

Micro Focus Fortify WebInspect

ソフトウェアバージョン: 21.2.0
Windows®オペレーティングシステム

ユーザガイド

マニュアルリリース日: 2021年11月
ソフトウェアリリース日: 2021年11月



保証と著作権

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

<https://www.microfocus.com>

保証

Micro Focus、関連会社、およびライセンサ(「Micro Focus」)の製品およびサービスに対する保証は、当該製品およびサービスに付属する保証書に明示的に規定されたものに限られます。本書のいかなる内容も、当該保証に新たに保証を追加するものではありません。Micro Focusは、本書に技術的または編集上の誤りまたは不備があっても責任を負わないものとします。本書の内容は、将来予告なしに変更されることがあります。

権利の制限

機密性のあるコンピュータソフトウェアです。別途指定されている場合を除き、これらの所有、使用、または複製には、Micro Focusからの有効な使用許諾が必要です。商用コンピュータソフトウェア、コンピュータソフトウェアに関する文書類、および商用アイテムの技術データは、FAR 12.211および12.212の規定に従い、ベンダーの標準商用ライセンスに基づいて米国政府に使用許諾が付与されます。

著作権表示

© Copyright 2004-2021 Micro Focus or one of its affiliates

商標に関する通知

このドキュメントに含まれるすべての商標、サービス名、製品名、およびロゴは、当該所有者に属するものとします。

マニュアルの更新

このマニュアルのタイトルページには次の識別情報が含まれています。

- ソフトウェアのバージョン番号
- ドキュメントのリリース日(ドキュメントが更新されるごとに変更されます)
- ソフトウェアリリース日(このバージョンのソフトウェアのリリース日)

このドキュメントは6月 23, 2022に作成されました。最近の更新を確認したり、ドキュメントが最新版であるかどうかを確認したりする場合は、次のページにアクセスしてください。

<https://www.microfocus.com/support/documentation>

このオンラインヘルプのPDF版について

このドキュメントは、オンラインヘルプのPDF版です。このPDFファイルを使用すると、ヘルプ情報から複数のトピックを簡単に印刷したり、オンラインヘルプをPDF形式で読んだりすることができます。このコンテンツはもともとオンラインヘルプとしてWebブラウザで表示するために作成されたため、一部のトピックが正しく書式設定されていない場合があります。このPDF版では、一部の対話型トピックが存在しない場合があります。それらのトピックは、オンラインヘルプ内から正常に印刷できます。

目次

| | |
|---|----|
| 序文 | 24 |
| Micro Focus Fortifyカスタマサポートへのお問い合わせ | 24 |
| その他情報 | 24 |
| マニュアルセットについて | 24 |
| Fortify製品の機能に関するビデオ | 25 |
| 変更ログ | 26 |
| 第1章: 紹介 | 34 |
| 検出事項について | 34 |
| Fortify WebInspectの概要 | 34 |
| Web探索および監査 | 34 |
| レポート | 35 |
| 手動ハッキング制御 | 35 |
| 概要と修復 | 35 |
| スキャンポリシー | 35 |
| ソートとカスタマイズが可能なビュー | 36 |
| 企業全体における利用状況の機能 | 36 |
| Webサービススキャン機能 | 36 |
| エクスポートウィザード | 36 |
| Web Service Test Designer | 36 |
| APIスキャン | 37 |
| API検出 | 37 |
| 統合機能 | 37 |
| 強化されたサードパーティの商用アプリケーション脅威エージェント | 37 |
| ハッカーレベルのインサイト | 38 |
| Fortify WebInspect Enterpriseについて | 38 |
| Fortify WebInspect Enterpriseのコンポーネント | 38 |
| コンポーネントの説明 | 39 |
| FIPSの準拠 | 40 |
| Fortify WebInspect製品のFIPSの準拠について | 40 |
| FIPS準拠モードの選択 | 41 |
| 関連ドキュメント | 41 |
| すべての製品 | 41 |

| | |
|--|----|
| Micro Focus Fortify WebInspect | 42 |
| Micro Focus Fortify WebInspect Enterprise | 44 |
| 第2章: はじめに | 46 |
| システムの監査準備 | 46 |
| 機密データ | 46 |
| ファイアウォール、ウィルス対策ソフトウェア、および侵入検知システム | 46 |
| 考慮すべき影響 | 47 |
| 役に立つヒント | 47 |
| クイックスタート | 48 |
| SecureBaseの更新 | 49 |
| システムを監査用に準備する | 49 |
| スキャンの開始 | 49 |
| 第3章: WebInspectユーザインターフェース | 51 |
| アクティビティパネル | 51 |
| アクティビティパネルを閉じる | 52 |
| ボタンバー | 52 |
| スキャンに関連付けられたペイン | 54 |
| 開始ページ(Start Page) | 55 |
| ホーム(Home) | 55 |
| スキャンの管理 | 55 |
| スケジュールの管理(Manage Schedule) | 56 |
| メニューバー | 56 |
| [ファイル(File)]メニュー | 56 |
| [編集(Edit)]メニュー | 57 |
| [表示(View)]メニュー | 58 |
| [ツール(Tools)]メニュー | 58 |
| [スキャン(Scan)]メニュー | 59 |
| [エンタープライズサーバ(Enterprise Server)]メニュー | 60 |
| [レポート(Reports)]メニュー | 61 |
| [ヘルプ(Help)]メニュー | 61 |
| WebInspectのヘルプ(WebInspect Help) | 61 |
| 検索 | 61 |
| サポート(Support) >拡張機能の依頼(Request an Enhancement) | 61 |
| サポート(Support) >テクニカルサポートへのお問い合わせ(Contact Technical | 62 |

| | |
|---|----|
| Support) | |
| サポート(Support) > オープンTCブラウザ情報の取得(Get Open TC Browsers info) | 62 |
| サポート(Support) > アプリケーションスナップショットのクリップボードへのコピー(Copy Application Snapshot to Clipboard) | 62 |
| チュートリアル | 63 |
| WebInspectについて(About WebInspect) | 63 |
| ツールバー | 63 |
| スキャンツールバーで使用可能なボタン | 63 |
| 標準ツールバーで使用可能なボタン | 65 |
| [スキャンの管理(Manage Scans)]ツールバーで使用可能なボタン | 66 |
| ナビゲーションペイン | 67 |
| サイトビュー | 69 |
| 除外ホスト | 69 |
| 許可ホストの基準 | 70 |
| [シーケンス(Sequence)]ビュー | 71 |
| SPAカバレッジ(SPA Coverage) | 72 |
| 検索(Search)]ビュー | 73 |
| ステップモード(Step Mode)]ビュー | 74 |
| ナビゲーションペインのアイコン | 74 |
| ナビゲーションペインのショートカットメニュー | 76 |
| 情報ペイン | 78 |
| [スキャン情報(Scan Info)]パネル | 79 |
| ダッシュボード | 79 |
| Traffic Monitor | 80 |
| 添付ファイル(Attachments) | 80 |
| 誤検出(False Positives) | 81 |
| ダッシュボード | 82 |
| 進行状況バー | 83 |
| 進行状況バーの説明 | 83 |
| 進行状況バーの色 | 84 |
| アクティビティメータ | 84 |
| アクティビティメータの説明 | 85 |
| 脆弱性グラフィック | 85 |
| 統計パネルレスキャン | 85 |
| 統計パネル-Web探索 | 87 |
| 統計パネル-監査 | 87 |
| 統計パネル-ネットワーク | 87 |
| 添付ファイル(Attachments) -スキャン情報(Scan Info) | 89 |
| 誤検出(False Positives) | 89 |

| | |
|--|-----|
| 誤検出のインポート | 90 |
| 非アクティブ/アクティブの誤検出リスト | 90 |
| 誤検出のロード | 90 |
| 誤検出の操作 | 90 |
| セッション情報(Session Info)]パネル | 91 |
| 選択可能なオプション | 91 |
| 脆弱性(Vulnerability) | 95 |
| Webブラウザ(Web Browser) | 95 |
| HTTP要求(HTTP Request) | 95 |
| 要求で強調表示されるテキスト | 95 |
| HTTP応答(HTTP Response) | 95 |
| 応答で強調表示されるテキスト | 95 |
| スタックトレース(Stack Traces) | 96 |
| 詳細(Details) | 96 |
| ステップ(Steps) | 96 |
| リンク(Links) | 96 |
| コメント(Comments): セッション情報(Session Info) | 96 |
| テキスト(Text) | 97 |
| 非表示(Hiddens): セッション情報(Session Info) | 97 |
| フォーム(Forms): セッション情報(Session Info) | 97 |
| 電子メール(E-Mail) | 97 |
| スクリプト(Scripts) -セッション情報(Session Info) | 98 |
| 添付ファイル(Attachments) -セッション情報(Session Info) | 98 |
| 添付ファイルの表示 | 98 |
| セッションの添付ファイルの追加 | 99 |
| 添付ファイルの編集 | 99 |
| 攻撃情報(Attack Info) | 100 |
| Webサービス要求(Web Service Request) | 100 |
| Webサービス応答(Web Service Response) | 100 |
| XML要求(XML Request) | 100 |
| XML応答(XML Response) | 100 |
| ホスト情報(Host Info)]パネル | 100 |
| 選択可能なオプション | 101 |
| P3P情報(P3P Info) | 102 |
| P3Pユーザエージェント | 103 |
| AJAX | 103 |
| AJAXの動作 | 104 |
| 証明書(Certificates) | 104 |
| コメント(Comments) -ホスト情報(Host Info) | 104 |
| クッキー(Cookies) | 105 |
| 電子メール(E-Mails) -ホスト情報(Host Info) | 105 |

| | |
|--|-----|
| フォーム(Forms) -ホスト情報(Host Info) | 106 |
| 非表示(Hiddens) -ホスト情報(Host Info) | 106 |
| スクリプト(Scripts) -ホスト情報(Host Info) | 107 |
| 壊れたリンク(Broken Links) | 107 |
| サイト外リンク | 108 |
| パラメータ(Parameters) | 108 |
| サマリペイン | 109 |
| 検出事項(Findings)]タブ | 109 |
| 使用可能な列 | 110 |
| 脆弱性の重大度 | 111 |
| 検出事項の操作 | 112 |
| 未検出(Not Found)]タブ | 114 |
| スキャンログ(Scan Log)]タブ | 114 |
| サーバ情報(Server Information)]タブ | 115 |
| Micro Focus Fortify Monitor | 115 |
| 第4章:スキャンの操作 | 116 |
| ガイド付きスキャンの概要 | 116 |
| 事前定義テンプレート | 116 |
| モバイルテンプレート | 116 |
| ガイド付きスキャンの実行 | 117 |
| 事前定義テンプレート(標準、クリック、または詳細) | 117 |
| モバイルスキャンテンプレート | 117 |
| ネイティブスキャンテンプレート | 118 |
| 事前定義テンプレートの使用 | 118 |
| ガイド付きスキャンの起動 | 118 |
| レンダリングエンジンについて | 119 |
| サイトステージについて | 119 |
| Webサイトの検証 | 119 |
| スキャンタイプの選択 | 121 |
| ログインステージについて | 123 |
| ネットワーク認証ステップ | 123 |
| ネットワーク認証の設定 | 123 |
| アプリケーション認証のステップ | 124 |
| マスクされた値のサポート | 124 |
| 権限のエスカレーションなしでログインマクロを使用する(Using a Login Macro without Privilege Escalation) | 125 |
| 権限のエスカレーションのためにログインマクロを使用する(Using Login Macros for Privilege Escalation) | 125 |

| | |
|---|-----|
| Fortify WebInspect Enterpriseに接続した際にログインマクロを使用する (Using a Login Macro when Connected to Fortify WebInspect Enterprise) | 126 |
| ログインマクロを自動で作成する | 127 |
| ワークフローステージについて | 127 |
| Burp Proxy結果を追加するには | 128 |
| アクティブラーニングステージについて | 129 |
| Profilerの使用 | 129 |
| 設定ステージについて | 131 |
| ガイド付きスキャンでのMicro Focus UFT (Unified Functional Testing)ファイルのインポート | 134 |
| モバイルスキャンテンプレートの使用 | 135 |
| モバイルスキャンの起動 | 136 |
| カスタムユーザエージェントヘッダの作成 | 137 |
| サイトステージについて | 137 |
| Webサイトの検証 | 137 |
| スキャンタイプの選択 | 140 |
| ログインステージについて | 141 |
| ネットワーク認証ステップ | 141 |
| ネットワーク認証の設定 | 141 |
| アプリケーション認証のステップ | 142 |
| マスクされた値のサポート | 143 |
| 権限のエスカレーションなしでログインマクロを使用する(Using a Login Macro without Privilege Escalation) | 143 |
| 権限のエスカレーションのためにログインマクロを使用する(Using Login Macros for Privilege Escalation) | 144 |
| Fortify WebInspect Enterpriseに接続した際にログインマクロを使用する (Using a Login Macro when Connected to Fortify WebInspect Enterprise) | 145 |
| ログインマクロを自動で作成する | 145 |
| ワークフローステージについて | 146 |
| Burp Proxy結果の追加 | 147 |
| Burp Proxy結果の追加 | 147 |
| アクティブラーニングステージについて | 147 |
| Profilerの使用 | 148 |
| 設定ステージについて | 150 |
| ガイド付きスキャンでのMicro Focus UFT (Unified Functional Testing)ファイルのインポート | 153 |
| ネイティブスキャンテンプレートの使用 | 154 |
| モバイルデバイスのセットアップ | 155 |
| ガイド付きスキャンのステージ | 155 |
| サポートされるデバイス | 155 |

| | |
|---|-----|
| サポートされる開発エミュレータ | 155 |
| ネイティブスキャンの起動 | 156 |
| ネイティブモバイルステージについて | 156 |
| デバイス/エミュレータタイプの選択ステップ | 157 |
| プロファイルの選択 | 157 |
| モバイルデバイスのプロキシアドレスの設定 | 157 |
| 信頼された証明書の追加 | 158 |
| スキャンタイプの選択ステップ | 159 |
| ログインステージについて | 160 |
| ネットワーク認証ステップ | 160 |
| ネットワーク認証の設定 | 160 |
| クライアント証明書の設定 | 161 |
| アプリケーション認証のステップ | 162 |
| マスクされた値のサポート | 162 |
| 権限のエスカレーションなしでログインマクロを使用する(Using a Login Macro without Privilege Escalation) | 163 |
| 権限のエスカレーションのためにログインマクロを使用する(Using Login Macros for Privilege Escalation) | 163 |
| Fortify WebInspect Enterpriseに接続した際にログインマクロを使用する(Using a Login Macro when Connected to Fortify WebInspect Enterprise) | 164 |
| マクロのテスト(Testing the Macro) | 165 |
| アプリケーションステージについて | 165 |
| アプリケーションの実行ステップ | 165 |
| 許可ホストとRESTfulエンドポイントの最終決定 | 165 |
| 設定ステージについて | 166 |
| 最終確認ステップ | 166 |
| 設定の検証とスキャンの開始 | 167 |
| スキャン後のステップ | 169 |
| APIまたはWebサービススキャンの実行 | 169 |
| APIスキャン | 170 |
| Webサービススキャン | 170 |
| APIスキャンウィザードの開始 | 170 |
| 次に行う作業 | 171 |
| APIスキャンの設定 | 171 |
| 次に行う作業 | 172 |
| Webサービススキャンの設定 | 172 |
| WSDLファイルの使用 | 173 |
| 既存のWSDLファイルの使用 | 173 |
| 次に行う作業 | 173 |
| APIスキャンおよびWebサービススキャンのプロキシの設定 | 173 |
| 次に行う作業 | 174 |

| | |
|--|-----|
| APIスキャンおよびWebサービススキャンの認証の設定 | 174 |
| ネットワーク認証の設定 | 174 |
| Postman環境設定の表示および調整 | 175 |
| 次に行う作業 | 176 |
| APIスキャンおよびWebサービススキャンのスキャン詳細の設定 | 176 |
| APIスキャンのポリシーの選択 | 176 |
| Web Service Test Designerの起動 | 176 |
| APIスキャンおよびWebサービススキャンの追加の設定 | 177 |
| 次に行う作業 | 178 |
| その後の作業 | 178 |
| 基本スキャンの実行(Webサイトスキャン) | 178 |
| 基本スキャンのオプション | 178 |
| 認証とコネクティビティ | 182 |
| カバレッジと徹底性 | 185 |
| 詳細スキャン設定(Detailed Scan Configuration) | 187 |
| Profiler | 187 |
| 設定(Settings) | 188 |
| Webフォームの自動入力(Auto fill Web forms) | 188 |
| 許可ホストの追加(Add Allowed Hosts) | 188 |
| 識別された誤検出を再利用する(Reuse Identified False Positives) | 189 |
| サンプルマクロ | 189 |
| トラフィック分析(Traffic Analysis) | 189 |
| メッセージ | 189 |
| その後の作業(Congratulations) | 189 |
| Fortify WebInspect Enterpriseスキャンテンプレートへのアップロード | 190 |
| 設定の保存 | 190 |
| レポートの生成 | 190 |
| Site List Editorの使用 | 191 |
| プロキシプロファイルの設定 | 191 |
| PACファイルを使用してプロキシを設定する | 192 |
| プロキシを明示的に設定する(Explicitly configure proxy) | 192 |
| 許可ホストの指定 | 192 |
| 許可ホストの指定 | 193 |
| 許可ホストの編集 | 193 |
| マルチユーザログインスキャン | 194 |
| 作業を開始する前に | 194 |
| 既知の制限事項 | 194 |
| プロセスの概要 | 195 |
| マルチユーザログインのスキャンの設定 | 195 |
| 資格情報の追加 | 196 |

| | |
|--|-----|
| 資格情報の編集 | 197 |
| 資格情報の削除 | 197 |
| 2要素認証の使用 | 198 |
| 2要素認証を使用するスキャンの仕組み | 198 |
| テクノロジプレビュー | 198 |
| 推奨 | 198 |
| 既知の制限事項 | 199 |
| プロセスについて | 199 |
| 対話型スキャン | 200 |
| 対話型スキャンの設定 | 200 |
| 「フォルダに限 定」に関する制限 | 202 |
| JavaScriptインクルードファイル | 202 |
| ログインマクロ | 202 |
| ワークフローマクロ | 202 |
| エンタープライズスキャンの実 行 | 203 |
| スキャン対象ホスト(Hosts to Scan)]リストの編集 | 205 |
| リストのエクスポート | 206 |
| スキャンの開始 | 206 |
| 手動スキャンの実行 | 206 |
| 権限のエスカレーションスキャンについて | 207 |
| 権限のエスカレーションスキャンの2つのモード | 208 |
| スキャン時の動作について | 208 |
| 制限のあるページを識別するために使用される正規表現パターン | 208 |
| Web探索プログラムの制限設定によって権限のエスカレーションスキャンに及 ぶ影響 | 209 |
| 乱数を含むパラメータによって権限のエスカレーションスキャンに及 ぶ影響 | 210 |
| シングルページアプリケーションスキャンについて | 210 |
| テクノロジプレビュー | 211 |
| シングルページアプリケーションの課 題 | 211 |
| SPAサポートの有効化 | 211 |
| スキャンステータス | 212 |
| スキャンマネージャの情報の更新 | 213 |
| 保存したスキャンを開く | 213 |
| スキャンの比 較 | 214 |
| スキャンを比較するためのスキャンの選択 | 214 |
| スキャンダッシュボードの確認 | 215 |
| スキャンの説明 | 215 |
| ベン図 | 216 |

| | |
|--|-----|
| 脆弱性棒グラフ | 216 |
| スキーム、ホスト、およびポートの違いがスキャン比較に及ぼす影響 | 216 |
| 比較モード | 217 |
| セッションフィルタリング | 217 |
| セッション情報(Session Info)パネルの使用 | 217 |
| サマリペインを使用した脆弱性の詳細の確認 | 218 |
| 脆弱性のグループ化とソート | 218 |
| 脆弱性のフィルタリング | 218 |
| 脆弱性の操作 | 219 |
| スキャンの管理 | 219 |
| スキャンのスケジュール | 221 |
| スケジュールされたスキャンの時間間隔の設定 | 222 |
| スケジュールされたスキャンの管理 | 222 |
| レポートの選択 | 224 |
| レポート設定を行う | 225 |
| スケジュールされているスキャンの停止 | 227 |
| スケジュールされたスキャンのステータス | 227 |
| スキャンのエクスポート | 228 |
| スキャン詳細のエクスポート | 229 |
| Software Security Centerへのスキャンのエクスポート | 231 |
| Webアプリケーションファイアウォール(WAF)への保護ルールのエクスポート | 232 |
| スキャンのインポート | 233 |
| 誤検出のインポート | 233 |
| レガシWebサービススキャンのインポート | 234 |
| インポート/エクスポート設定の変更 | 235 |
| エンタープライズサーバからのスキャンのダウンロード | 235 |
| ログファイルがダウンロードされない | 236 |
| エンタープライズサーバへのスキャンのアップロード | 236 |
| エンタープライズサーバでのスキャンの実行 | 236 |
| エンタープライズサーバとの間での設定の転送 | 237 |
| Fortify WebInspect Enterpriseスキャンテンプレートの作成 | 237 |
| Fortify WebInspect設定ファイルの作成 | 238 |
| スキャンの発行(Fortify WebInspect Enterprise接続) | 239 |
| Fortify Software Security Centerへの脆弱性の統合 | 240 |
| 最初のスキャン | 241 |

| | |
|--|-----|
| 2回目のスキャン | 242 |
| 3回目のスキャン | 242 |
| 4回目のスキャン | 242 |
| Fortify Software Security Centerとの同期 | 243 |
| | |
| 第5章: WebInspectの機能の使用 | 244 |
| 再テストと再スキャン | 244 |
| 脆弱性の再テスト | 244 |
| 再テストのステータスについて | 245 |
| 失敗した脆弱性およびサポート対象外の脆弱性に関する推奨事項 | 246 |
| すべての脆弱性の再テスト | 246 |
| 特定の重大度を持つすべての脆弱性の再テスト | 246 |
| 選択した脆弱性の再テスト | 247 |
| グループ化されたカテゴリの再テスト | 247 |
| 再テストのスキャンの再テスト | 248 |
| 再テストのスキャンログ | 248 |
| 比較ビュー | 248 |
| 再テストのスキャンの保持または削除 | 248 |
| サイトの再スキャン | 249 |
| スキャンの再利用 | 250 |
| 再利用のオプション | 250 |
| 改善スキャンと脆弱性の再テストの違い | 250 |
| スキャンの再利用に関するガイドライン | 250 |
| スキャンの再利用 | 251 |
| 増分スキャン | 251 |
| ベースラインスキャンと増分スキャンのマージ | 251 |
| 継続的監査または遅延監査による増分スキャン | 252 |
| マクロの使用 | 253 |
| ワークフローマクロの選択 | 254 |
| Web Macro Recorderの使用 | 254 |
| Web Macro Recorder with Macro Engine 6.1 | 254 |
| セッションベースのWeb Macro Recorder | 255 |
| Traffic Monitor (Traffic Viewer) | 255 |
| Traffic Viewerのトラフィックセッションデータ | 255 |
| Traffic Viewerでのトラフィックの表示 | 255 |
| Server Profiler | 256 |
| Server Profilerの使用 | 256 |
| 結果の検査 | 257 |
| 基本スキャン(Basic Scan) | 257 |

| | |
|--------------------------------------|-----|
| 1つ以上の脆弱性の操作 | 258 |
| グループの操作 | 259 |
| 重大度について | 260 |
| ナビゲーションペインでの操作 | 260 |
| Webサービススキャン | 260 |
| 検索(Search)]ビュー | 261 |
| サマリペインのフィルタとグループの使用 | 262 |
| フィルタの使用 | 263 |
| フィルタを使用しない場合 | 263 |
| 「Method:Get」でフィルタされている場合 | 263 |
| 複数のフィルタの指定 | 264 |
| フィルタ基準 | 264 |
| グループの使用 | 265 |
| Webサービスの監査 | 266 |
| セッション情報(Session Info)]パネルで使用可能なオプション | 266 |
| 脆弱性スクリーンショットの追加と表示 | 268 |
| 選択したセッションのスクリーンショットの表示 | 269 |
| すべてのセッションのスクリーンショットの表示 | 269 |
| 脆弱性の編集 | 269 |
| 脆弱なセッションの編集 | 270 |
| 脆弱性のロールアップ | 272 |
| ロールアップされた脆弱性の挙動 | 272 |
| ロールアップのガイドライン | 272 |
| 脆弱性のロールアップ | 273 |
| ロールアップの取り消し | 274 |
| 誤検出としてマーク | 274 |
| 脆弱性としてマーク | 275 |
| フォローアップのためのセッションへのフラグ設定 | 275 |
| 選択したセッションのフラグの表示 | 275 |
| すべてのセッションのフラグの表示 | 275 |
| スキャンメモ | 276 |
| セッションのメモ | 276 |
| 選択したセッションのメモの表示 | 276 |
| すべてのセッションのメモの表示 | 277 |
| 脆弱性のメモ | 277 |
| 選択したセッションのメモの表示 | 277 |
| すべてのセッションのメモの表示 | 278 |

| | |
|---------------------------------------|-----|
| 削除された項目の回復 | 278 |
| Micro Focus ALMへの脆弱性の送信 | 278 |
| 送信される追加情報 | 279 |
| データ実行防止の無効化 | 280 |
| レポートの生成 | 280 |
| レポートの保存 | 281 |
| 詳細レポートのオプション | 281 |
| レポートビューア | 282 |
| メモの追加 | 283 |
| 標準レポート | 283 |
| レポートの管理 | 285 |
| コンプライアンステンプレート | 286 |
| 設定の管理 | 295 |
| 設定ファイルの作成 | 296 |
| 設定ファイルの編集 | 296 |
| 設定ファイルの削除 | 296 |
| 設定ファイルのインポート | 296 |
| 設定ファイルのエクスポート | 296 |
| 保存した設定ファイルを使用したスキャン | 297 |
| SmartUpdate | 297 |
| SmartUpdateの実行(インターネットに接続している場合) | 298 |
| Fortify WebInspectを更新せずにチェックをダウンロードする | 299 |
| SmartUpdateの実行(オフライン) | 299 |
| WebSphere Portalに関するFAQ | 300 |
| コマンドライン実行 | 302 |
| CLIの起動 | 302 |
| Fortify WebInspect on DockerのCLI制限 | 302 |
| WI.exeの使用 | 303 |
| オプション | 303 |
| 例 | 318 |
| Seleniumログインマクロの例 | 319 |
| 応答状態ルールの例 | 319 |
| スキャンのマージ | 319 |
| コマンドライン引数のハイフン | 320 |
| 終了コード | 320 |
| WIScanStopper.exeの使用 | 320 |
| MacroGenServer.exeの使用 | 321 |

| | |
|--|-----|
| オプション | 321 |
| 正規表現 | 323 |
| 正規表現の拡張 | 324 |
| 正規表現タグ | 324 |
| 正規表現演算子 | 325 |
| 例 | 325 |
| Fortify WebInspect REST API | 326 |
| Fortify WebInspect REST APIとは | 326 |
| Fortify WebInspect REST APIの設定 | 326 |
| Fortify WebInspect REST API Swagger UIへのアクセス | 329 |
| Swagger UIの使用 | 329 |
| フィールドレベルの詳細の取得 | 330 |
| Fortify WebInspectの自動化 | 331 |
| Fortify WebInspectのアップデートとAPI | 331 |
| Postmanコレクションによるスキャン | 331 |
| Postmanとは何か | 331 |
| Postmanコレクションの利点 | 332 |
| Postman変数に関する既知の制限事項 | 332 |
| Postmanスキャンのオプション | 332 |
| Postmanの前提条件 | 332 |
| Postmanでのクライアント証明書の使用 | 332 |
| Postmanコレクションの準備のヒント | 333 |
| 有効な応答の確保 | 333 |
| 要求の順序 | 333 |
| 認証の処理 | 334 |
| スタティック認証の使用 | 334 |
| ダイナミック認証の使用 | 334 |
| Postmanログインマクロの使用 | 335 |
| Postmanの自動設定 | 335 |
| Postmanのサンプルスクリプト | 335 |
| ダイナミックトークン用のPostmanログインの手動設定 | 335 |
| ダイナミックトークンとは何か | 335 |
| 作業を開始する前に | 336 |
| プロセスの概要 | 336 |
| ログイン要求の識別と分離 | 336 |
| 正規表現を使用したログアウト条件の作成 | 336 |
| Bearerトークンの応答状態ルールの作成 | 337 |
| APIキーの応答状態ルールの作成 | 338 |
| WI.exeまたはWebInspect REST APIを使用したPostman APIスキャン | 338 |
| プロセス | 339 |

| | |
|---------------------------------------|-----|
| Postmanスキャンのトラブルシューティング | 340 |
| Selenium WebDriverとの統合 | 340 |
| 既知の制限事項 | 340 |
| プロセスの概要 | 341 |
| Seleniumスクリプトへのプロキシの追加 | 342 |
| 長所 | 342 |
| 短所 | 343 |
| サンプルコード | 343 |
| CLIの使用 | 345 |
| Fortify WebInspect geckodriver.exeの使用 | 346 |
| 長所 | 346 |
| 短所 | 346 |
| Selenium WebDriver環境のインストール | 346 |
| コマンドラインからのテスト | 346 |
| Seleniumコマンドの作成 | 347 |
| Fortify WebInspectへのファイルのアップロード | 350 |
| CLIの使用 | 350 |
| APIの使用 | 350 |
| Seleniumコマンドの使用 | 350 |
| WI.exeを使用したスキャンの実行 | 350 |
| APIを使用したマクロの作成 | 351 |
| Burp API拡張機能について | 352 |
| Burp API拡張機能を使用するメリット | 352 |
| サポートされるバージョン | 353 |
| Burp API拡張機能の使用 | 353 |
| Burp拡張機能のロード | 353 |
| Fortify WebInspectへの接続 | 355 |
| スキャンのリストの更新 | 357 |
| Burpでのスキャンの操作 | 357 |
| BurpからWebInspectへの項目の送信 | 360 |
| WebInspect SDKについて | 361 |
| 監査拡張機能/カスタムエージェント | 362 |
| SDKの機能 | 362 |
| インストールの推奨事項 | 362 |
| WebInspect SDKのインストール | 363 |
| インストールの検証 | 363 |
| インストール後の作業 | 364 |
| ページまたはディレクトリの追加 | 364 |
| バリエーションの追加 | 365 |

| | |
|---|-----|
| Fortify Monitor: Enterprise Serverセンサの設定 | 365 |
| センサとして設定後(After Configuring as a Sensor) | 366 |
| ブラックアウト期間 | 366 |
| 除外の作成 | 367 |
| 例1 | 368 |
| 例2 | 368 |
| 例3 | 368 |
| 例4 | 369 |
| Internet Protocolバージョン6 | 369 |
| 第6章: デフォルトのスキャン設定 | 370 |
| スキャン設定: 方法 | 370 |
| スキャンモード(Scan Mode) | 370 |
| Web探索および監査モード(Crawl and Audit Mode) | 371 |
| Web探索および監査の詳細(Crawl and Audit Details) | 371 |
| ナビゲーション | 372 |
| SSL/TLSプロトコル(SSL/TLS Protocols) | 373 |
| スキャン設定: 全般 | 374 |
| スキャンの詳細(Scan Details) | 374 |
| Web探索の詳細 | 376 |
| スキャン設定: JavaScript | 380 |
| JavaScriptの設定 | 380 |
| スキャン設定: リクエスタ | 382 |
| リクエスタパフォーマンス(Requestor Performance) | 382 |
| リクエスタ設定(Requestor Settings) | 383 |
| コネクティビティの喪失が検出された場合にスキャンを停止する(Stop Scan if Loss of Connectivity Detected) | 384 |
| スキャン設定: セッション除外 | 385 |
| 除外または拒否するファイル拡張子 | 386 |
| 除外 MIMEタイプ | 386 |
| その他の除外/拒否基準 | 386 |
| 基準の編集 | 387 |
| 基準の追加 | 387 |
| スキャン設定: 許可ホスト | 389 |
| 許可ホスト設定の使用 | 389 |
| 許可されたドメインの追加 | 390 |
| ドメインの編集または削除 | 390 |
| スキャン設定: HTTP解析 | 390 |

| | |
|---|-----|
| オプション | 391 |
| CSRF | 395 |
| CSRFについて | 395 |
| CRSFトークンの使用 | 396 |
| Fortify WebInspectでのCSRF認識の有効化 | 396 |
| スキャン設定: カスタムパラメータ | 396 |
| URLの書き換え | 397 |
| RESTfulサービス | 397 |
| スキャン時に使用されていないルールの自動シードを有効にする(Enable automatic seeding of rules that were not used during scan) | 398 |
| URLパラメータのダブルエンコード(Double Encode URL Parameters) | 399 |
| パスマトリックスパラメータ | 399 |
| パスセグメントの定義 | 400 |
| ルールの特別な要素 | 400 |
| アスタリスクプレースホルダ | 401 |
| プレースホルダを使用する利点 | 402 |
| 複数のルールが1つのURLに一致する場合 | 402 |
| スキャン設定: フィルタ | 402 |
| オプション | 403 |
| キーワードの検索および置換のためのルールの追加 | 403 |
| スキャン設定: クッキー/ヘッダ | 404 |
| 標準のヘッダパラメータ | 404 |
| カスタムヘッダの追加 | 405 |
| カスタムヘッダの追加 | 405 |
| カスタムクッキーの追加 | 405 |
| カスタムクッキーの追加 | 405 |
| スキャン設定: プロキシ | 406 |
| オプション | 406 |
| スキャン設定: 認証 | 408 |
| スキャンにはネットワーク認証が必要(Scan Requires Network Authentication) | 408 |
| 認証メソッド | 408 |
| 認証資格情報 | 408 |
| クライアント証明書 | 409 |
| WebInspectツール用のプロキシ設定ファイルの編集 | 410 |
| マクロ検証を有効にする(Enable Macro Validation) | 410 |
| フォーム認証にログインマクロを使用する(Use a login macro for forms authentication) | 411 |
| ログインマクロパラメータ(Login Macro Parameters) | 411 |
| 起動マクロを使用する(Use a startup macro) | 411 |

| | |
|--|-----|
| マルチユーザログイン(Multi-user Login) | 412 |
| スキャン設定: ファイルが見つからない | 413 |
| オプション | 413 |
| スキャン設定: ポリシー | 415 |
| ポリシーの作成 | 415 |
| ポリシーの編集 | 415 |
| ポリシーのインポート | 415 |
| ポリシーの削除 | 416 |
| スキャン設定: ユーザエージェント | 416 |
| プロファイルおよびユーザエージェント文字列 | 416 |
| ナビゲータインターフェース設定 | 417 |
| 第7章: Web探索設定 | 418 |
| Web探索設定: リンク解析 | 418 |
| 特殊リンク識別子の追加 | 418 |
| Web探索設定: リンクソース | 418 |
| リンク解析とは | 419 |
| パターンベースの解析 | 419 |
| DOMベースの解析 | 419 |
| フォームアクション、スクリプトインクルード、およびスタイルシート | 424 |
| その他のオプション | 425 |
| リンクソース設定の制限 | 426 |
| Web探索設定: セッション除外 | 426 |
| 除外または拒否するファイル拡張子 | 426 |
| 除外/拒否するファイル拡張子の追加 | 426 |
| 除外MIMEタイプ | 427 |
| 除外するMIMEタイプの追加 | 427 |
| その他の除外/拒否基準 | 427 |
| デフォルトの基準の編集 | 427 |
| 除外/拒否基準の追加 | 428 |
| 第8章: 監査設定 | 431 |
| 監査設定: セッション除外 | 431 |
| 除外または拒否するファイル拡張子 | 431 |
| 除外/拒否するファイル拡張子の追加 | 431 |
| 除外MIMEタイプ | 432 |
| 除外するMIMEタイプの追加 | 432 |
| その他の除外/拒否基準 | 432 |

| | |
|--|-----|
| デフォルトの基準の編集 | 432 |
| 除外/拒否基準の追加 | 433 |
| 監査設定:攻撃除外 | 435 |
| 除外パラメータ | 435 |
| 除外するパラメータの追加 | 435 |
| 除外クッキー(Excluded Cookies) | 435 |
| 特定のクッキーの除外 | 436 |
| 除外ヘッダ(Excluded Headers) | 436 |
| 特定のヘッダの除外 | 436 |
| Audit Inputs Editor | 437 |
| 監査設定:攻撃式 | 437 |
| 追加の正規表現言語 | 438 |
| 監査設定:脆弱性フィルタリング | 438 |
| 脆弱性フィルタの追加 | 439 |
| サイト外の脆弱性の抑止 | 439 |
| 監査設定:スマートスキャン | 439 |
| スマートスキャンの有効化 | 440 |
| HTTP応答で正規表現を使用する(Use regular expressions on HTTP responses) | 440 |
| サーバアナライザのフィンガープリント法を使用し、サンプリングを要求する(Use server analyzer fingerprinting and request sampling) | 440 |
| カスタムサーバ/アプリケーションタイプの定義(Custom server/application type definitions) | 440 |
| 第9章:アプリケーション設定 | 442 |
| アプリケーション設定:全般 | 442 |
| 全般(General) | 442 |
| WebInspect Agent | 445 |
| アプリケーション設定:データベース | 446 |
| スキャン/レポートストレージの接続設定 | 446 |
| SQL Serverデータベース特権 | 446 |
| SQL Server Standard Editionの設定 | 446 |
| スキャン表示の接続設定 | 447 |
| Site Explorer用のスキャンデータの作成 | 447 |
| アプリケーション設定:ディレクトリ | 448 |
| Fortify WebInspectファイルの保存場所の変更 | 448 |
| アプリケーション設定:ライセンス | 448 |
| ライセンスの詳細 | 448 |

| | |
|--|-----|
| Micro Focusへの直接接続 | 449 |
| APLSへの接続 | 449 |
| LIMへの接続 | 450 |
| アプリケーション設定: Server Profiler | 450 |
| モジュール | 451 |
| アプリケーション設定: ステップモード | 453 |
| アプリケーション設定: 2要素認証 | 453 |
| テクノロジレビュー | 453 |
| 2要素認証コントロールセンター | 454 |
| モバイルアプリケーション | 454 |
| Fortify2FAモバイルアプリのインストールと設定 | 455 |
| アプリケーション設定: ログ記録 | 461 |
| アプリケーション設定: プロキシ | 462 |
| プロキシサーバを使用しない | 462 |
| プロキシサーバを使用する | 462 |
| プロキシの設定 | 463 |
| アプリケーション設定: レポート | 464 |
| オプション | 464 |
| ヘッダとフッタ | 465 |
| アプリケーション設定: テレメトリ | 465 |
| テレメトリについて | 466 |
| テレメトリの有効化 | 466 |
| テレメトリ経由のスキャンのアップロード | 466 |
| アップロード間隔の設定 | 466 |
| オンディスクキャッシュサイズの設定 | 467 |
| 送信する情報のカテゴリの特定 | 467 |
| アプリケーション設定: センサとしての実行 | 467 |
| センサ | 467 |
| アプリケーション設定: SQLデータベース設定の上書き | 469 |
| データベース設定の上書き(Override Database Settings) | 469 |
| SQLデータベースの設定 | 469 |
| アプリケーション設定: スマートアップデート | 470 |
| オプション | 470 |
| アプリケーション設定: サポートチャネル | 470 |
| サポートチャネルを開く | 471 |
| アプリケーション設定: Micro Focus ALM | 471 |
| ALMライセンスの使用 | 471 |

| | |
|-----------------------------------|-----|
| 作業を開始する前に | 471 |
| プロファイルの作成 | 471 |
| | |
| 第10章: 参照リスト | 473 |
| Fortify WebInspectのポリシー | 473 |
| ベストプラクティス | 473 |
| タイプ別 | 475 |
| カスタム | 476 |
| 危険 | 476 |
| 非推奨になったチェックおよびポリシー | 477 |
| スキャンログのメッセージ | 478 |
| HTTPステータスコード | 502 |
| | |
| 第11章: トラブルシューティング | 506 |
| WebInspectのトラブルシューティング | 506 |
| コネクティビティに関する問題 | 506 |
| スキャン初期化の失敗 | 507 |
| スキャン設定の問題 | 508 |
| アラートのトラブルシューティング | 508 |
| テクノロジプレビュー | 508 |
| アラートの無効化 | 508 |
| アラートのトラブルシューティングの表 | 509 |
| ログインマクロのテスト | 510 |
| 実行される検証テスト | 510 |
| トラブルシューティングのヒント | 510 |
| Fortify WebInspectのアンインストール | 511 |
| 削除のオプション | 511 |
| | |
| マニュアルのフィードバックの送信 | 513 |

序文

Micro Focus Fortifyカスタマサポートへのお問い合わせ

サポートWebサイトでは以下を実行できます。

- ライセンスとエンタイトルメントの管理
- 技術サポートリクエストの作成と管理
- ドキュメントおよびナレッジの記事の参照
- ソフトウェアのダウンロード
- コミュニティの検索

<https://www.microfocus.com/support>

その他の情報

Fortifyソフトウェア製品の詳細については、次のリンクを参照してください。

<https://www.microfocus.com/cyberres/application-security>

マニュアルセットについて

Fortifyソフトウェアマニュアルセットには、すべてのFortifyソフトウェア製品およびコンポーネントのインストールガイド、ユーザガイド、および展開ガイドが含まれています。また、新機能、既知の問題、最新情報を説明する技術ノートおよびリリースノートも提供されています。これらのドキュメントの最新バージョンには、次のMicro Focus製品マニュアルWebサイトからアクセスできます。

<https://www.microfocus.com/support/documentation>

リリース間のマニュアル更新のお知らせを受け取るには、Micro FocusコミュニティのFortify製品情報を購読してください。

<https://community.microfocus.com/cyberres/fortify/w/fortify-product-announcements>

Fortify製品の機能に関するビデオ

Fortify Unplugged YouTubeチャンネルで、Fortifyの製品と機能を紹介したビデオをご覧いただけます。

<https://www.youtube.com/c/FortifyUnplugged>

変更ログ

次の表に、このドキュメントに加えられた変更を示します。このマニュアルの改訂版がソフトウェアリースの切り替え時に発行されるのは、その変更が製品の機能に影響する場合だけです。

| ソフトウェアリース/ドキュメントバージョン | 変更点 |
|-----------------------|---|
| 21.2.0 | <p>追加:</p> <ul style="list-style-type: none">2要素認証を使用するスキャンに関する内容。「"2要素認証の使用" ページ198」と「"アプリケーション設定: 2要素認証" ページ453」を参照してください。 <p>更新:</p> <ul style="list-style-type: none">スキャン設定の 自動応答状態ルール(Auto Response State Rules) オプション。「"スキャン設定: HTTP解析" ページ390」を参照してください。スキャンログのメッセージの応答状態ルールと外部相関に関するエントリ。「"スキャンログのメッセージ" ページ478」を参照してください。Postmanスキャン情報のPostman変数に関する既知の制限。「"Postmanコレクションによるスキャン" ページ331」を参照してください。マルチユーザログインに関する内容に2要素認証が含まれました。「"マルチユーザログインスキャン" ページ194」と「"スキャン設定: 認証" ページ408」を参照してください。対話型スキャンに関する内容で2要素認証が除外されました。「"対話型スキャン" ページ200」を参照してください。ガイド付きスキャンと基本スキャンに関する内容の、2要素認証を含むマクロに関する重要な情報。次のトピックを参照してください。<ul style="list-style-type: none">"事前定義テンプレートの使用" ページ118"モバイルスキャンテンプレートの使用" ページ135"ネイティブスキャンテンプレートの使用" ページ154"基本スキャンの実行(Webサイトスキャン)" ページ178 |

| ソフトウェアリリース/ ドキュメントバージョン | 変更点 |
|----------------------------|---|
| | <ul style="list-style-type: none"> API検出の説明を含む機能のリスト。「"Fortify WebInspectの概要" ページ34」を参照してください。 |
| 21.1.0 | <p>追加:</p> <ul style="list-style-type: none"> ユーザエージェントの新しいスキャン設定ページに関する内容。「"スキャン設定: ユーザエージェント" ページ416」を参照してください。 アラートレベルのスキャンログのメッセージのトラブルシューティングに関する内容。「"アラートのトラブルシューティング" ページ508」を参照してください。 HTTP/2サポートを有効にするためのアプリケーション設定。「"アプリケーション設定: 全般" ページ442」。 <p>更新:</p> <ul style="list-style-type: none"> Webサービススキャンに関する内容にAPIスキャンが含まれました。次のトピックを参照してください。 <ul style="list-style-type: none"> "WebInspectユーザインターフェース" ページ51 "開始ページ(Start Page)" ページ55 "APIまたはWebサービススキャンの実行" ページ169 " [ファイル(File)]メニュー" ページ56 "ツールバー" ページ63 "スキャンのスケジュール" ページ221 [スキャンログ(Scan log)]タブとログメッセージの、アラートレベルのメッセージに関する情報。「" [スキャンログ(Scan Log)]タブ" ページ114」と「"スキャンログのメッセージ" ページ478」を参照してください。 機能のリストにHacker-level Insightsが含まれました。「"Fortify WebInspectの概要" ページ34」を参照してください。 サイト認証に関する内容の、マクロにおけるマスクされた変数のサポート。次のトピックを参照してください。 <ul style="list-style-type: none"> "基本スキャンの実行(Webサイトスキャン)" ページ178 "事前定義テンプレートの使用" ページ118 |

| ソフトウェアリース/ ドキュメントバージョ ン | 変更点 |
|-------------------------------|---|
| | <p>変更点</p> <ul style="list-style-type: none"> ・ "モバイルスキャンテンプレートの使用" ページ135 ・ "ネイティブスキャンテンプレートの使用" ページ154 ・ "スキャン設定:認証" ページ408 ・ ポリシーのリストの、NIST-SP80053R5ポリシーの説明。「"WI.exeの使用" ページ303」と「"Fortify WebInspectのポリシー" ページ473」を参照してください。 ・ WI.exeに関する内容の、Postman環境ファイルオプションと終了コード。「"WI.exeの使用" ページ303」を参照してください。 ・ Postmanに関する内容の、クライアント証明書の使用に関するプロセス。「"Postmanコレクションによるスキャン" ページ331」を参照してください。 ・ システムの監査準備に関する有益なヒントの、CAPTCHAに関する情報。「"システムの監査準備" ページ46」を参照してください。 ・ Swagger UIに関する内容の、エンドポイントに関するフィールドレベルの詳細の取得に関する情報。「"Fortify WebInspect REST API" ページ326」を参照してください。 <p>削除:</p> <ul style="list-style-type: none"> ・ Selenium IDEマクロへの参照。 ・ 基本スキャンウィザードから、APIスキャンオプションと設定。 ・ zero.webappsecurity.comでのWebサービスのスキャンに関するトピック。 ・ WISwag.exeツールの使用に関するトピック。 ・ WI.exeに関する内容から、[Web探索の再利用(Reuse Crawl)]オプションと[Web探索改善の再利用(Reuse Crawl Remediation)]オプション。 |
| 20.2.0 | <p>更新:</p> <ul style="list-style-type: none"> ・ 冗長なページ検出設定の説明の、新しいオプション。「"スキャン設定:全般" ページ374」を参照してください。 ・ SPAサポート設定の説明の、新しいオプション。次のトピックを参照してください。 <ul style="list-style-type: none"> ・ "スキャン設定:JavaScript" ページ380 |

| ソフトウェアリース/ ドキュメントバージョ ン | 変更点 |
|-------------------------------|---|
| | <ul style="list-style-type: none"> "事前定義テンプレートの使用" ページ118 "モバイルスキャンテンプレートの使用" ページ135 Postman前提条件情報で、Newmanパス変数をインストールする必要がある場所が明確化されました。「"Postmanの前提条件" ページ332」を参照してください。 SQL Server Standard Editionの設定手順の、接続情報を手動で入力する方法に関する重要な内容。「"SQL Server Standard Editionの設定" ページ446」を参照してください。 アプリケーション設定の、OpenSSLエンジンを使用するための新しいオプション。「"アプリケーション設定: 全般" ページ442」を参照してください。 ポリシーのリストの、API、CWE Top 25、およびOWASP ASVS (Application Security Verification Standard)ポリシーの説明。「"Fortify WebInspectのポリシー" ページ473」を参照してください。 トラブルシューティングセクションにOpenSSL欠陥に関するコネクティビティの問題が含まれました。「"WebInspectのトラブルシューティング" ページ506」を参照してください。 ネットワーク認証オプションにADFS CBT認証が含まれました。次のトピックを参照してください。 <ul style="list-style-type: none"> "基本スキャンの実行(Webサイトスキャン)" ページ178 "事前定義テンプレートの使用" ページ118 "モバイルスキャンテンプレートの使用" ページ135 "ネイティブスキャンテンプレートの使用" ページ154 "APIまたはWebサービススキャンの実行" ページ169 "スキャン設定: 認証" ページ408 ""アプリケーション設定: Server Profiler" ページ450 ""WI.exeの使用" ページ303 ""MacroGenServer.exeの使用" ページ321 <p>削除:</p> <ul style="list-style-type: none"> MacroGenServer.exeアプリケーションで使用可能なオプションの |

| ソフトウェアリース/ ドキュメントバージョ ン | 変更点 |
|-------------------------------|---|
| | <p>リストから、-engineオプション。</p> <ul style="list-style-type: none"> スキャン設定: セッションストレージに関するトピック。 |
| 20.1.0 / 2020年6月 | <p>更新:</p> <ul style="list-style-type: none"> レンダリングエンジンオプションの基本スキャンとガイド付きスキャンに関するトピックで新しい言い回しが採用されました。次のトピックを参照してください。 <ul style="list-style-type: none"> "基本スキャンの実行 (Webサイトスキャン)" ページ178 "事前定義テンプレートの使用" ページ118 "モバイルスキャンテンプレートの使用" ページ135 Postmanログインの手動設定で、ダイナミックトークンの説明が含まれ、サンプルコードの問題が修正されました。「"ダイナミックトークン用のPostmanログインの手動設定" ページ335」を参照してください。 <p>削除:</p> <ul style="list-style-type: none"> システムの監査準備中に、ファイアウォール、ウィルス対策ソフトウェア、および侵入検知システムで例外を許可することに関する記述。 |
| 20.1.0 | <p>追加:</p> <ul style="list-style-type: none"> スキャンのサイトツリーをJSON形式とCSV形式にエクスポートするためのCLIオプション。「"WI.exeの使用" ページ303」を参照してください。 スキャンでSeleniumログインマクロを使用するためのCLIオプション。「"WI.exeの使用" ページ303」を参照してください。 <p>更新:</p> <ul style="list-style-type: none"> トラブルシューティングセクションにC++再配布可能ファイルに関する既知の問題が含まれました(リースノートにはすでに記載)。「"WebInspectのトラブルシューティング" ページ506」を参照してください。 再テストと再スキャンに関するトピックで、更新された再テスト機能とその使い方が説明されています。次のトピックを参照してください。 |

| ソフトウェアリース/ ドキュメントバージョ ン | 変更点 |
|-------------------------------|--|
| | <ul style="list-style-type: none"> • "再テストと再スキャン" ページ244 • "脆弱性の再テスト" ページ244 • " [スキャン(Scan)]メニュー" ページ59 • サマリペインと脆弱性の再テストに言及しているトピックで、単一の検出事項(Findings)タブと更新された再テスト機能が文書化されています。次のトピックを参照してください。 <ul style="list-style-type: none"> • "WebInspectユーザインターフェース" ページ51 • "サマリペイン" ページ109 • " 検出事項(Findings)]タブ" ページ109 • " 未検出(Not Found)]タブ" ページ114 • " [スキャンログ(Scan Log)]タブ" ページ114 • " [サーバ情報(Server Information)]タブ" ページ115 • "サマリペインのフィルタとグループの使用" ページ262 • "脆弱性のロールアップ" ページ272 • "ナビゲーションペイン" ページ67 • "結果の検査" ページ257 • "スキャンの比較" ページ214 • "再テストと再スキャン" ページ244 • "削除された項目の回復" ページ278 • "セッションのメモ" ページ276 • "フォローアップのためのセッションへのフラグ設定" ページ275 • " [セッション情報(Session Info)]パネル" ページ91 • "Fortify Software Security Centerへの脆弱性の統合" ページ240 • " [スキャン情報(Scan Info)]パネル" ページ79 • "Webサービスの監査" ページ266 • "添付ファイル(Attachments) -スキャン情報(Scan Info)" ページ |

| ソフトウェアリース/ ドキュメントバージョ ン | 変更点 |
|-------------------------------|--|
| | <p>89</p> <ul style="list-style-type: none">"添付ファイル(Attachments) - セッション情報(Session Info)" ページ98"脆弱性スクリーンショットの追加と表示" ページ268"脆弱性のメモ" ページ277"脆弱性の編集" ページ269"アプリケーション設定: 全般" ページ442"誤検出(False Positives)" ページ89"Burp API拡張機能の使用" ページ353Postmanコレクションに関するトピックの、Postmanスキャンの実行およびPostmanスキャンの改善に関する新しいCLIオプション。次のトピックを参照してください。<ul style="list-style-type: none">"Postmanコレクションによるスキャン" ページ331"Postmanコレクションの準備のヒント" ページ333"ダイナミックトークン用のPostmanログインの手動設定" ページ335Postmanコレクションを使用するスキャンの実行"WI.exeの使用" ページ303基本スキャンとガイド付きスキャンの使用手順における、ブラウザとWeb Macro Recorder技術に関するさまざまな細かな変更。次のトピックを参照してください。<ul style="list-style-type: none">"基本スキャンの実行(Webサイトスキャン)" ページ178"事前定義テンプレートの使用" ページ118"モバイルスキャンテンプレートの使用" ページ135"ネイティブスキャンテンプレートの使用" ページ154ナビゲーションペインの説明に [SPAカバレッジ(SPA Coverage)] ビューが含まれました。「"ナビゲーションペイン" ページ67」を参照してください。Web Macro Recorderツールの説明。「"Web Macro Recorderの |

| ソフトウェアリース/ ドキュメントバージョ ン | 変更点 |
|-------------------------------|--|
| | <p>使用"ページ254"を参照してください。</p> <ul style="list-style-type: none">ポリシーのリストの、PCI Software Security Framework 1.0ポリ シーの説明。「"Fortify WebInspectのポリシー" ページ473」を参 照してください。 <p>削除:</p> <ul style="list-style-type: none">License and Infrastructure Managerの使用に関する付録。この 情報は、『<i>Micro Focus Fortify License and Infrastructure Manager Installation and Usage Guide</i>』で参照できるようにな りました。「アプリケーション設定: 全般」から、デフォルトのWeb Macro Recorderを選択するための設定。ツールバー、[スキャン(Scan)]メニュー、およびスキャンログのメッ セージに関するトピックから、[スキップ(Skip)]ボタンに関連する情 報。[スキャン(Scan)]メニューとスキャンの再利用に関するトピックか ら、Web探索の再利用およびWeb探索改善の再利用機能。 |

第1章：紹介

Micro Focus Fortify WebInspect™ 21.2.0は、自動化されたWebアプリケーション、API、およびWebサービスの脆弱性スキャンツールです。Fortify WebInspectは、スキャン技術の最新の進化形として、あらゆるエンタープライズ環境に適応するWebアプリケーションセキュリティ製品を提供します。スキャンを開始すると、Fortify WebInspectはWebアプリケーションのすべてのエリアをダイナミックにカタログするエージェントを割り当てます。これらのエージェントは、検出事項を分析する主要なセキュリティエンジンに結果を報告します。その後、Fortify WebInspectは「脅威エージェント」を起動して、収集された情報を評価し、攻撃アルゴリズムを適用して潜在的な脆弱性の存在と相対的な重大度を判断します。このスマートなアプローチにより、Fortify WebInspectは特定のアプリケーション環境に適応する適切なスキャンリソースを継続的に適用します。

検出事項について

Fortify WebInspectの検出事項は、実際の脆弱性ではなく潜在的な脆弱性と見なす必要があります。アプリケーションはどれも固有であり、どの機能も特有のコンテキスト内で実行されます。そのコンテキストを最もよく理解できるのは開発チームです。開発者に直接確認することなく、疑わしい動作が脆弱性と見なされるかどうかを完全に判断できる技術はありません。

次も参照

["Fortify WebInspectの概要" 下](#)

Fortify WebInspectの概要

Fortify WebInspectで実行できる操作、およびWebInspectからもたらされる組織へのメリットについて、次に簡単に説明します。

Web探索および監査

Fortify WebInspectでは、セキュリティ上の弱点を明らかにするために、2つの基本モードを使用します。

- Web探索とは、Fortify WebInspectでターゲットWebサイトの構造を識別するプロセスです。基本的に、Web探索はURL上にアクセスできるリンクがなくなるまで実行されます。
- 監査とは、実際の脆弱性スキャンです。Web探索と監査を組み合わせて1つの機能にしたもの、スキャンと呼びます。

レポート

Fortify WebInspectレポートを使用して、整理された有益なアプリケーション情報を取得します。レポートの詳細をカスタマイズしたり、各レポートに含める情報のレベルを決定したり、特定の対象ユーザ向けにレポートを作成したりすることができます。カスタマイズしたレポートはテンプレートとして保存することもできます。これにより、同じレポート基準を使用して、更新情報を反映したレポートを生成することが可能になります。レポートは、PDF、HTML、Excel、Raw、RTF、またはテキスト形式で保存できます。また、脆弱性データのグラフィックサマリを含めることもできます。

手動ハッキング制御

Fortify WebInspectでは、サイトで実際に何が起こっているかを確認し、真の攻撃環境をシミュレートできます。Fortify WebInspect機能を使用すると、脆弱性のあるページのコードを表示し、サーバ要求を変更して直ちに再送信することができます。

概要と修復

情報ペインには、ナビゲーションペインまたはサマリペインのいずれかで選択した脆弱性に関するすべての概要と修復情報が表示されます。詳細については、「["ナビゲーションペイン" ページ67](#)」および「["サマリペイン" ページ109](#)」を参照してください。

また、参考資料が提示され、パッチへのリンク、将来の問題を防止するための指示、および脆弱性ソリューションも示されています。新しい攻撃やエクスプロイトコードは毎日作成されるため、Fortifyによって概要と修復情報のデータベースが頻繁に更新されます。Fortify WebInspectツールバーの [スマートアップデート(Smart Update)] でデータベースを更新して最新の脆弱性解決情報を反映させることも、起動時に自動的に更新を確認することもできます。詳細については、「["SmartUpdate" ページ297](#)」および「["アプリケーション設定:スマートアップデート" ページ470](#)」を参照してください。

スキャンポリシー

組織のニーズに合わせてスキャンポリシーを編集およびカスタマイズして、Fortify WebInspectのスキャン所要時間を短縮できます。Fortify WebInspectポリシーの設定方法に関する詳細については、Policy Managerのヘルプまたは『*Micro Focus Fortify WebInspect Tools Guide*』を参照してください。

ソートとカスタマイズが可能なビュー

スキャンを実行または表示する場合、Fortify WebInspectウィンドウの左のナビゲーションペインには、[サイト(Site)]、[シーケンス(Sequence)]、[検索(Search)]、および[ステップモード(Step Mode)]の各ボタンがあり、このボタンでナビゲーションペインに表示されるコンテンツ(または「ビュー」)を決定できます。

- ・[サイト(Site)]ビューには、Fortify WebInspectによって決定された、スキャン対象サイトの階層ファイル構造が表示されます。また、リソースごとに、サーバから返されたHTTPステータスコードと検出された脆弱性の数も表示されます。
- ・[シーケンス(Sequence)]ビューには、Fortify WebInspectによって自動スキャンまたは手動Web探索(ステップモード)中に検出された順序でサーバリソースが表示されます。
- ・検索ビューでは、指定した基準に一致するセッションを検索できます。詳細については、「["検索\(Search\)"\]ビュー" ページ261](#)」を参照してください。
- ・ステップモードは、[サイト(Site)]ビューまたは[シーケンス(Sequence)]ビューのいずれかから選択したセッションを起点にして、サイト内を手動で移動するために使用されます。詳細については、「["手動スキャンの実行" ページ206](#)」を参照してください。

企業全体における利用状況の機能

統合スキャンでは、企業全体の観点からWebプレゼンスの包括的な概要が提供され、ネットワーク上のすべてのWeb対応アプリケーションのアプリケーションスキャンを実行できます。

Webサービススキャン機能

Webサービスの脆弱性を包括的にスキャンします。Webサービス/SOAPオブジェクトが含まれているアプリケーションを評価できます。

エクスポート ウィザード

Fortify WebInspectの堅牢で設定可能なXMLエクスポートツールを使用すると、ユーザはスキャン中に検出されたあらゆる情報を(標準化されたXML形式で)エクスポートできます。これには、コメント、非表示フィールド、JavaScript、クッキー、Webフォーム、URL、要求、およびセッションが含まれます。ユーザは、エクスポートする情報のタイプを指定できます。

Web Service Test Designer

Web Service Test Designerでは、Webサービススキャンの実行時にFortify WebInspectから送信される値が入ったWebサービステスト設計ファイル(<ファイル名>.wsd)を作成できます。

APIスキャン

Fortify WebInspectでは、REST APIアプリケーションのスキャンは次のようにサポートされます:

- APIスキャンウィザードを使用して、ユーザインターフェースでAPIスキャンを設定します。詳細については、「["APIまたはWebサービススキャンの実行" ページ169](#)」を参照してください。
- WebInspect REST APIを使用して、REST API定義をスキャンします。詳細については、「["Fortify WebInspect REST API" ページ326](#)」を参照してください。
- API要求のPostmanコレクションを使用して、スキャンを開始します。詳細については、「["Postmanコレクションによるスキャン" ページ331](#)」を参照してください。

API検出

API検出では、スキャン中に検出されたSwaggerスキーマまたはOpenAPIスキーマのエンドポイントが既存のスキャンに追加され、自動状態検出を使用してエンドポイントに認証が適用されます。また、一般的なAPIフレームワークのデフォルトの場所にプローブが送信され、スキーマが検出されます。

統合機能

Fortify WebInspectは、最も広く使用されているアプリケーションセキュリティ開発およびテストツールと統合できます。これには以下のものが含まれます。

- Burp (詳細については、「["Burp API拡張機能について" ページ352](#)」を参照してください。)
- Postman (詳細については、「["Postmanコレクションによるスキャン" ページ331](#)」を参照してください。)
- Selenium WebDriver (詳細については、「["Selenium WebDriverとの統合" ページ340](#)」を参照してください。)

強化されたサードパーティの商用アプリケーション脅威エージェント

Fortify WebInspectを使用すれば、ユーザは業界をリードするアプリケーションプラットフォームを含むあらゆるWebアプリケーションのセキュリティスキャンを実行できます。Fortify WebInspectを使用する標準的な商用アプリケーション脅威エージェントには、次のようなものがあります:

- Adobe ColdFusion
- Adobe JRun
- Apache Tomcat
- IBM Domino
- IBM WebSphere
- Microsoft.NET

- Oracle Application Server
- Oracle WebLogic

ハッカーレベルのインサイト

Fortify WebInspectでは、スキャン中にアプリケーションで検出されたライブラリにフラグが設定されます。この情報により、開発者やセキュリティ専門家はアプリケーションの全体的なセキュリティ状態に関するコンテキストを把握できます。これらの検出事項が必ずしもセキュリティの脆弱性を示しているとは限りませんが、通常、攻撃者は既知の弱点やパターンを特定しようとすると、ターゲットの偵察を実行するということに注意することが重要です。

Fortify WebInspect Enterpriseについて

Micro Focus Fortify WebInspect Enterpriseは、一元管理されたデータベースを持つシステムマネージャによって制御されるFortify WebInspectセンサの分散ネットワークを採用しています。必要に応じて、Fortify WebInspect EnterpriseをFortify Software Security Centerと統合し、WebサイトとWebサービスのダイナミックスキャンを通して検出された情報をFortify Software Security Centerに提供できます。

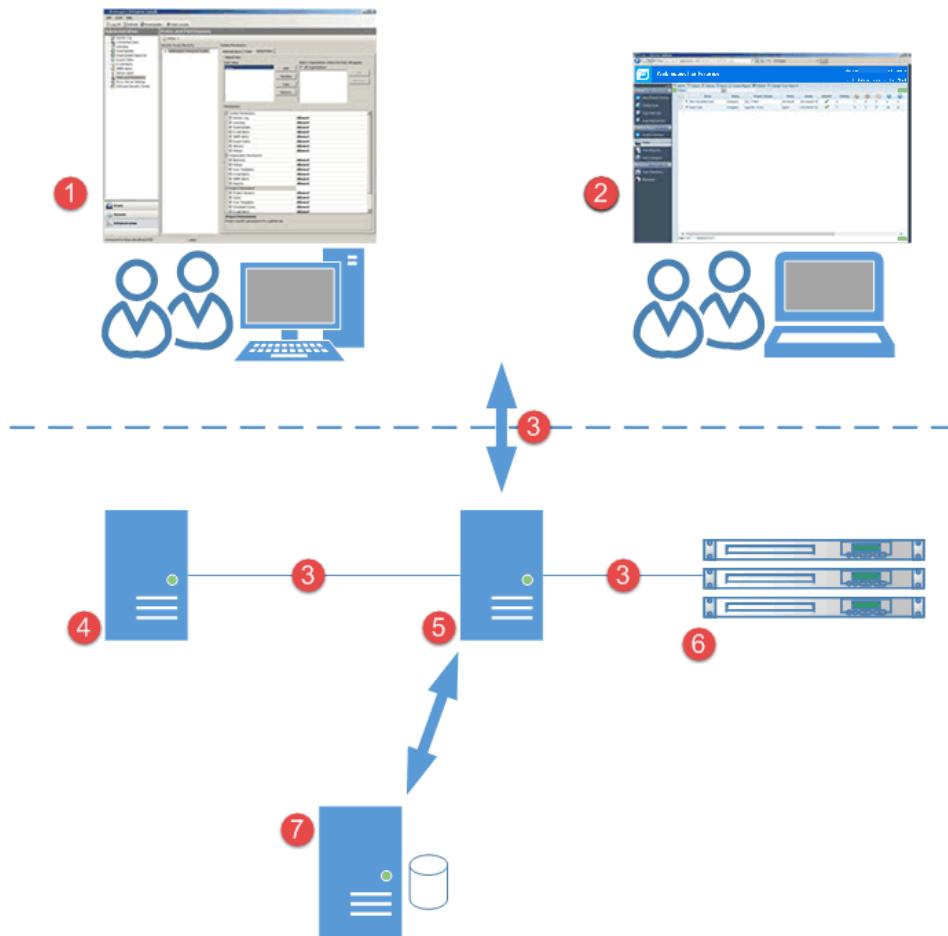
この革新的なアーキテクチャにより、次の操作を実行できます。

- 任意の数のFortify WebInspectセンサを使用して多数の自動化セキュリティスキャンを実行し、WebアプリケーションとSOAPサービスをスキャンします。
- 組織全体にわたる大規模または小規模なFortify WebInspect展開を管理し、製品のアップデート、スキャンポリシー、スキャン許可、ツールの使用状況、およびスキャン結果のすべてをFortify WebInspect Enterpriseコンソールから一元的に管理します。
- 新しいWebアプリケーションと既存のWebアプリケーションを追跡、管理、および検出し、それらに関連付けられたすべてのアクティビティを監視します。
- 必要に応じて、スキャンデータをFortify Software Security Centerにアップロードします。
- Fortify WebInspectまたはFortify WebInspect Enterpriseコンソールを使用して、スキャンとブラックアウト期間を個別にスケジュールしたり、スキャンを手動で起動したり、リポジトリ情報を更新したりします。詳細については、「["ブラックアウト期間" ページ366](#)」を参照してください。
- ユーザ用に一元的に定義された役割を使用することによって、社外秘扱いのコンポーネントやデータの表示を制限します。
- スキャン結果、レポート、および傾向分析の一元管理されたデータベースを通して、組織のリスクとポリシー・コンプライアンスの正確な全体像を把握します。
- サードパーティ製品との統合と、カスタマイズされたWebベースのフロントエンドの展開を、Webサービスアプリケーションプログラミングインターフェース(API)を使用して促進します。

Fortify WebInspect Enterpriseのコンポーネント

次の図は、Fortify WebInspect Enterpriseシステムの主要なコンポーネントを示しています。これには、Fortify WebInspect Enterpriseアプリケーション、データベース、センサ、およびユーザ

が含まれます。



コンポーネントの説明

次の表に、Fortify WebInspect Enterpriseのユーザインターフェースとアーキテクチャの説明を示します。

| 項目 | コンポーネント | 説明 |
|----|--------------------------|--|
| 1 | Windowsコンソールのユーザインターフェース | このコンソールは、管理機能、ポリシー編集、およびツールキットを提供するシンクライアントアプリケーションです。 |
| 2 | Webコンソールのユーザインターフェース | このコンソールは、ユーザ機能を提供するブラウザベースのアプリケーションです。これは、管理機能、ポリシー編集、またはツールキットを備えていません。 |
| 3 | HTTPまたはHTTPS | Fortify WebInspect Enterpriseコンポーネントでは、これら |

| 項目 | コンポーネント | 説明 |
|----|--|--|
| | | の通信プロトコルが使用されます。 |
| 4 | Fortify Software Security Center (オプション) | Fortify Software Security Centerと統合すると、すべてのスタティックスキャンとダイナミックスキャンの中央リポジトリにスキャンを発行できます。これにより、ある程度一元管理されたアカウント(ただし、許可は依然として独立して管理される)、スキャン要求を送信する機能、およびスタンダードインストールに比べてより広範囲のレポートングが提供されます。 |
| 5 | Fortify WebInspect Enterprise Manager | これは、IISアプリケーションプラットフォームを使用したMicrosoft Windowsサーバです。ユーザ認証と権限付与、データリポジトリ、およびリモートスキャンスケジューリングを主な機能とするWebサービスです。 |
| 6 | センサ | これらのWebInspectセンサは、Microsoft WindowsまたはWindows Serverオペレーティングシステムにインストールされます。センサは、GUIがなく、Webコンソールで設定されたりモートスキャンを実行します。Webコンソールを使用して、スキャン設定、結果、レポート、および更新のすべてを制御します。 |
| 7 | Microsoft SQL Server | このMicrosoft Windowsサーバは、すべてのユーザ、許可、および管理設定を格納するSQLデータベースを備えています。このデータベースには、すべてのスキャンデータとレポートングも保存されます。 |

FIPSの準拠

Fortify WebInspectおよびFortify WebInspect Enterpriseは、通常モードまたはFIPS準拠モードで実行できます。

Fortify WebInspect製品のFIPSの準拠について

FIPS準拠モードでは、Fortify WebInspectプログラムは連邦情報処理標準(FIPS)に準拠するためには必要な暗号化規格を満たします。FIPS準拠モードで実行している場合、アメリカ国立標準技術研究所(NIST)によって確立されたAESアルゴリズムを使用してデータが暗号化されます。これには、Fortify WebInspectとのデータの送受信や、保存されたスキャンデータが含まれます。

FIPS準拠は、デフォルトのFortify WebInspect製品で使用されるものとは異なる暗号化モジュールを使用するため、FIPS準拠のインストールでは、FIPS非準拠のインストールで生成

されたスキャンデータにアクセスできません。以前にFIPS非準拠のFortify WebInspectのインストールを使用していて、FIPS準拠環境でFortify WebInspectを実行する場合は、Micro Focus FIPSマイグレーションツールを使用してデータを復号化してから、AESアルゴリズムを使用して再暗号化しない限り、FIPS非準拠のインストールで生成したスキャンデータは使用できません。環境内でFortify WebInspectの複数のインスタンスを実行しているときに、それらのインスタンス間でデータを共有する場合、インスタンスはすべてFIPS準拠またはFIPS非準拠のいずれかでなければなりません。

Fortify WebInspect、Fortify WebInspect Enterprise、およびFortify WebInspect AgentはすべてFIPS準拠モードを備えています。

FIPS準拠モードの選択

Fortify WebInspectをFIPS準拠環境にインストールすると、Fortify WebInspectを通常モードまたはFIPS準拠モードで実行するオプションがトリガれます。あるモードから別のモードに切り替えできないため、このオプションを選択する前に、FIPS非準拠のデータとの後方互換性を維持する必要がある依存関係が存在しないことを確認してください。FIPS準拠モードで実行している場合、Fortify WebInspectの日常の動作における変化に気付くことはありません。

関連ドキュメント

このトピックでは、Micro Focus Fortifyソフトウェア製品に関する情報を提供するドキュメントについて説明します。

メモ: Micro Focus Fortify製品マニュアルは <https://www.microfocus.com/support/documentation>にあります。ほとんどのガイドは、PDF形式とHTML形式の両方で提供されています。製品ヘルプは、Fortify LIM製品およびFortify WebInspect製品内で利用できます。

すべての製品

次のドキュメントには、すべての製品の一般情報が記載されています。特に明記されていない限り、これらのドキュメントはMicro Focus製品マニュアルのWebサイトで入手できます。

| ドキュメント/ファイル名 | 説明 |
|---|--|
| <i>About Micro Focus Fortify Product Software Documentation</i> | このドキュメントでは、Micro Focus Fortify製品マニュアルにアクセスする方法について説明します。 |
| <i>About_Fortify_Docs_<version>.pdf</i> | メモ: このドキュメントは製品のダウンロードにのみ含まれています。 |
| <i>Micro Focus Fortify License and</i> | このドキュメントでは、Fortify License and |

| ドキュメント/ファイル名 | 説明 |
|--|---|
| <i>Infrastructure Manager Installation and Usage Guide</i> LIM_Guide_<version>.pdf | Infrastructure Manager (LIM)をインストール、設定、および使用する方法について説明します。これはローカルWindowsサーバへのインストールも、Dockerプラットフォーム上のコンテナイメージとしての使用も可能です。 |
| <i>Micro Focus Fortify Software System Requirements</i> Fortify_Sys_Req_<version>.pdf | このドキュメントでは、このバージョンのFortifyソフトウェアでサポートされている環境および製品の詳細を提供します。 |
| <i>Micro Focus Fortify Software Release Notes</i> FortifySW_RN_<version>.pdf | このドキュメントでは、本リリースのFortifyソフトウェアに加えられた変更の概要と、製品マニュアルの他の場所には含まれていない重要な情報について説明します。 |
| <i>What's New in Micro Focus Fortify Software <version></i> Fortify_Whats_New_<version>.pdf | このドキュメントでは、Fortifyソフトウェア製品の新機能について説明します。 |

Micro Focus Fortify WebInspect

次のドキュメントでは、Fortify WebInspectに関する情報を提供します。特に明記されていない限り、これらのドキュメントはMicro Focus製品マニュアルのWebサイト <https://www.microfocus.com/documentation/fortify-webinspect>で入手できます。

| ドキュメント/ファイル名 | 説明 |
|--|---|
| <i>Micro Focus Fortify WebInspect Installation Guide</i> WI_Install_<version>.pdf | このドキュメントでは、Fortify WebInspectの概要と、Fortify WebInspectのインストールと製品ライセンスの有効化に関する手順について説明します。 |
| <i>Micro Focus Fortify WebInspect User Guide</i> WI_Guide_<version>.pdf | このドキュメントでは、Fortify WebInspectを設定および使用してWebアプリケーションおよびWebサービスをスキャンおよび分析する方法について説明します。 |

メモ: このドキュメントは、Fortify WebInspectヘルプのPDF版です。このPDFファイルを使用すると、ヘルプ情報から複数のトピックを簡単に印

| ドキュメント/ファイル名 | 説明 |
|---|--|
| | 刷したり、ヘルプをPDF形式で読んだりすることができます。このコンテンツはもともとヘルプとしてWebブラウザで表示するために作成されたため、一部のトピックが正しく書式設定されていない場合があります。また、このPDF版では、一部の対話型トピックやリンクされたコンテンツが存在しない場合があります。 |
| <i>Micro Focus Fortify WebInspect on Docker User Guide</i> WI_Docker_Guide_<version>.pdf | このドキュメントでは、Dockerプラットフォーム上のコンテナイメージとして利用可能なFortify WebInspectをダウンロード、設定、および使用する方法について説明します。この製品のフルバージョンは、コマンドラインインターフェース(CLI)またはアプリケーションプログラミングインターフェース(API)を使用して設定されたヘッダレスセンサとして、自動プロセスで使用することを目的としています。Fortify ScanCentral DASTセンサとして実行することもでき、Fortify Software Security Centerと連携させて使用できます。 |
| <i>Micro Focus Fortify WebInspect Tools Guide</i> WI_Tools_Guide_<version>.pdf | このドキュメントでは、Fortify WebInspectおよびFortify WebInspect EnterpriseにパッケージされたFortify WebInspect診断および侵入テストツールおよび設定ユーティリティの使用方法について説明します。 |
| <i>Micro Focus Fortify WebInspect Agent Installation Guide</i> WI_Agent_Install_<version>.pdf | このドキュメントでは、サポートされているアプリケーションサーバ上のサポートされているJava Runtime Environment (JRE)で実行されるアプリケーションのために、またはサポートされているバージョンのIIS上のサポートされている.NET Frameworkで実行されるサービスまたはアプリケーションのために、Fortify WebInspect Agentをインストールする方法を説明します。 |
| <i>Micro Focus Fortify WebInspect Agent Rulepack Kit Guide</i> WI_Agent_Rulepack_Guide_<version>.pdf | このドキュメントでは、Fortify WebInspect Agent Rulepack Kitの検出機能について説明します。Fortify WebInspect Agent Rulepack KitはFortify WebInspect Agent上で実行され、ソフトウェアセキュリティの脆弱性がないか、実行中のコードを監視できます。Fortify WebInspect Agent Rulepack |

| ドキュメント/ファイル名 | 説明 |
|--------------|--|
| | Kitは、ダイナミックな結果をスタティックな結果につなげるのに役立つランタイム技術を提供します。 |

Micro Focus Fortify WebInspect Enterprise

次のドキュメントは、Fortify WebInspect Enterpriseに関する情報を提供します。特に明記されていない限り、これらのドキュメントはMicro Focus製品マニュアルのWebサイト <https://www.microfocus.com/documentation/fortify-webinspect-enterprise>で入手できます。

| ドキュメント/ファイル名 | 説明 |
|---|--|
| <i>Micro Focus Fortify WebInspect Enterprise Installation and Implementation Guide</i> WIE_Install_<version>.pdf | このドキュメントではFortify WebInspect Enterpriseの概要と、Fortify WebInspect Enterpriseのインストール、Fortify Software Security CenterおよびFortify WebInspectとの統合、およびインストールのトラブルシューティングの手順について説明します。また、Fortify WebInspect Enterpriseシステムのコンポーネント(Fortify WebInspect Enterpriseのアプリケーション、データベース、センサ、ユーザなど)の設定方法についても説明します。 |
| <i>Micro Focus Fortify WebInspect Enterprise User Guide</i> WIE_Guide_<version>.pdf | このドキュメントでは、Fortify WebInspect Enterpriseを使用してFortify WebInspectセンサの分散ネットワークを管理し、WebアプリケーションおよびWebサービスをスキャンおよび分析する方法について説明します。 |
| <i>Micro Focus Fortify WebInspect Tools Guide</i> | メモ: このドキュメントはFortify WebInspect EnterpriseヘルプのPDF版です。このPDFファイルを使用すると、ヘルプ情報から複数のトピックを簡単に印刷したり、ヘルプをPDF形式で読んだりすることができます。このコンテンツはもともとヘルプとしてWebブラウザで表示するために作成されたため、一部のトピックが正しく書式設定されていない場合があります。また、このPDF版では、一部の対話型トピックやリンクされたコンテンツが存在しない場合があります。 |

| ドキュメント/ファイル名 | 説明 |
|----------------------------------|------------------------|
| WI_Tools_Guide_ <version>.pdf | ユーティリティの使用方法について説明します。 |

第2章：はじめに

この章では、Fortify WebInspectをすぐに使い始めることができるよう、お使いのシステムを監査用に準備し、SecureBaseを更新して、スキャンを開始する方法について説明します。

システムの監査準備

Fortify WebInspectは、実際のおよび潜在的なセキュリティの脆弱性がないかWebサイト全体を厳正に調査する、積極的なWebアプリケーションアナライザです。程度の差こそあれ、この手順は侵入型です。適用するFortify WebInspectポリシーと選択するオプションによっては、サーバとアプリケーションのスループットと効率に影響する場合があります。最も積極的なポリシーを使用する場合は、サーバを監視しながら制御された環境でこの分析を実行することをFortifyはお勧めします。

機密データ

Fortify WebInspectでは、アプリケーションとサーバ間で送信されたアプリケーションデータがすべてキャプチャおよび表示されます。使用しているアプリケーション内で自分が認識していない機密データが検出されることさえあるかもしれません。Fortifyでは、機密データに関する次のいずれかのベストプラクティスに従うことをお勧めします。

- Fortify WebInspectでのテスト中は、実際のユーザ名やパスワードなどの潜在的な機密データを使用しない。
- 潜在的な機密データへのアクセスを許可されていないユーザがFortify WebInspectスキャン、関連するアーティファクト、およびデータストアにアクセスできないようにする。

ネットワーク認証資格情報はWebInspectに表示されず、設定に保存される際に暗号化されます。

ファイアウォール、ウィルス対策ソフトウェア、および侵入検知システム

WebInspectでは、攻撃をサーバに送信し、結果を分析して保存します。このようなアクティビティを防止するために、Webアプリケーションファイアウォール(WAF)、ウィルス対策ソフトウェア、ファイアウォール、および侵入検知/防止システム(IDS/IPS)が用意されています。そのため、脆弱性のスキャンを実行する際に、これらのツールが問題になることがあります。

まず、これらのツールは、WebInspectによるサーバのスキャンに干渉する可能性があります。WebInspectからサーバに送信される攻撃が傍受されて、サーバへの要求が失敗する可能性があります。サーバがその攻撃に対して脆弱な場合は、検出漏れが発生する可能性があります。

第二に、結果や攻撃がWebInspect製品内にある場合、ディスク上にローカルにキャッシュされている場合、またはデータベース内にある場合、これらのツールによって特定されて検疫されることがあります。WebInspectで使用される作業ファイルまたはデータベース内のデータが検疫されると、WebInspectでの結果に矛盾が生じる可能性があります。また、このような検疫済みのファイルとデータによって、予期しない動作が発生する可能性もあります。

この種の問題は環境に固有のものですが、McAfee IPSは両方の種類の問題の原因となることが知られており、WAFはどれも最初の問題の原因となります。Fortifyでは、これらのツールに関連する他の問題も確認されています。

スキャンの実行中にこのような問題が発生した場合、Fortifyではスキャン中、WAF、ウィルス対策ソフトウェア、ファイアウォール、およびIDS/IPSツールを無効にすることをお勧めします。この方法が信頼できるスキャン結果を確実に取得できる唯一の方法です。

考慮すべき影響

どの種類の監査でも、Fortify WebInspectによって多数のHTTP要求が送信されますが、その多くには「無効」パラメータが含まれています。処理速度の遅いシステムでは、要求の量のせいで他のユーザからのアクセス速度が低下したり、アクセスが拒否されたりすることがあります。また、侵入検知システムを使用している場合は、多数の不正アクセス試行が識別されることになります。

徹底スキャンを実行するため、Fortify WebInspectでは、アプリケーション内にあるすべてのページ、フォーム、ファイル、およびフォルダの識別が試みられます。サイトのWeb探索中にフォームを送信するオプションを選択すると、Fortify WebInspectによって、検出されたすべてのフォームが入力されて送信されます。これにより、アプリケーション内でFortify WebInspectのシームレスな移動が可能になりますが、次のような結果が生じる場合があります。

- 通常、ユーザがフォームを送信すると、アプリケーションで電子メールや電子掲示板の投稿が作成されて、(製品サポートまたは販売グループ宛などに)送信されるようになっている場合、Fortify WebInspectでもプローブの一環としてこれらのメッセージが生成されます。
- 通常のフォーム送信によってデータベースにレコードが追加されるようになっている場合、Fortify WebInspectから送信されるフォームによって擬似的なレコードが作成されます。

スキャンの監査段階で、Fortify WebInspectは、アプリケーションの問題を特定するため、考えられるあらゆるパラメータを操作して、何度もフォームを再送信します。これにより、作成されるメッセージとデータベースレコードの数が大幅に増加します。

役に立つヒント

- クライアントから送信されたフォームに基づいてバックエンドサーバ(データベース、LDAPなど)にレコードを書き込むシステムの場合、運用システムを監査する前にデータベースをバックアップして、監査の完了後に再インストールするFortify WebInspectユーザもいます。これを実施できない場合は、監査後にサーバにクエリを実行して、Fortify WebInspectから送信された1つ以上のフォーム値を含むレコードを検索して削除できます。これらの値は、Web Form Editorを開くことで特定できます。
- ユーザが送信したフォームに応答して電子メールメッセージが生成される場合は、電子メールサーバを無効にすることを検討してください。または、すべての電子メールをキューにリ

ダイレクトしてから、監査後に、Fortify WebInspectから送信されたフォームに応答して生成されたこれらの電子メールを手動で確認して削除することもできます。

- Fortify WebInspectは、最大75の同時HTTP要求を送信してから、最初の要求に対するHTTP応答を待機するように設定できます。デフォルトのスレッド数設定は、Web探索では5、監査では10です(別々のリクエスタを使用する場合)。環境によっては、アプリケーションまたはサーバに障害が発生しないように、より小さい値を指定する必要があります。詳細については、「["スキャン設定:リクエスタ" ページ382](#)」を参照してください。
- 何らかの理由で、Fortify WebInspectで特定のディレクトリに対してWeb探索と攻撃をしない場合は、Fortify WebInspect設定の除外URL機能を使用して、これらのディレクトリを指定する必要があります(「["スキャン設定:セッション除外" ページ385](#)」を参照)。また、特定のファイルタイプとMIMEタイプを除外することもできます。
- デフォルトでは、Fortify WebInspectは、Webアプリケーションで一般的に見られる多くのバイナリファイル(イメージやドキュメントなど)を無視するように設定されています。これらのドキュメントは、Web探索や攻撃ができないため、監査する価値はありません。これらのドキュメントをバイパスすることにより、監査速度が大幅に向上します。専有ドキュメントが使用中である場合は、ドキュメントのファイル拡張子を決定し、Fortify WebInspectのデフォルト設定内で除外します。Web探索中にFortify WebInspectの動作が極端に遅くなったり、停止したりした場合は、バイナリドキュメントをダウンロードしようとしたことが原因である可能性があります。
- フォーム送信の場合、事前にパッケージ化されたファイルから抽出されたデータがFortify WebInspectによって送信されます。特定の値(ユーザ名やパスワードなど)が必要な場合は、FortifyのWeb Form Editorでファイルを作成し、そのファイルをFortify WebInspectで識別する必要があります。
- 対話型のスキャンを実行する場合を除き、CAPTCHAソフトウェアはオフにしてください。CAPTCHAはWebアプリケーションでの自動化を防止するように設計されているため、Webアプリケーションの自動スキャンに干渉する可能性があります。
- Fortify WebInspectでは、サーバへのファイルのアップロードを試行することで、特定の脆弱性がテストされます。これがサーバで許可された場合、この脆弱性はFortify WebInspectによってスキャンレポートに記録され、このファイルの削除が試みられます。ただし、サーバ側でファイルの削除が阻止されることがあります。このため、スキャン後の保守では、「CreatedByHP」で始まる名前のファイルを検索して削除することを日常業務の一環としてください。

次も参照

["Fortify WebInspectの概要" ページ34](#)

["クイックスタート" 下](#)

クイックスタート

このトピックでは、Fortify WebInspectを使い始める際に役立つ情報を提供します。さらに詳しい情報へのリンクも含まれています。

SecureBaseの更新

Fortify WebInspectの脆弱性のカタログに関する最新の情報を確実に取得するには、次の手順に従って脆弱性データベースを更新します。

1. Fortify WebInspectを起動します。

メモ: Fortify WebInspectが、Fortify WebInspect Enterpriseの対話型コンポーネントとしてインストールされている場合、およびエンタープライズサーバが現在このFortify WebInspectモジュールを使用してスキャンを実行している場合は、Fortify WebInspectを起動できません。次のメッセージが表示されます：「WebInspectを起動できません。許可が拒否されました。(Unable to start WebInspect. Permission denied.)」

2. 開始ページ(Start Page)で、[スマートアップデートの開始(Start Smart Update)]をクリックします。
[スマートアップデート(Smart Update)]ウィンドウが開き、使用可能な更新が一覧表示されます。
3. [更新(Update)]をクリックします。

メモ: 製品を使用するたびに更新を行います。プログラムを起動するたびにスマートアップデートを実行するアプリケーション設定を選択できます。詳細については、「["アプリケーション設定:スマートアップデート" ページ470](#)」を参照してください。

オフラインのWebInspectの更新手順を含む詳細については、「["SmartUpdate" ページ297](#)」を参照してください。

システムを監査用に準備する

監査を実行する前に、Webサイトに与える潜在的な影響、および正常な監査のための準備作業に注意してください。詳細については、「["システムの監査準備" ページ46](#)」を参照してください。

スキャンの開始

データベースを更新すると、Webアプリケーションのセキュリティ脆弱性を判断する準備が整います。

Fortify WebInspectの開始ページ(Start Page)で、次のいずれかの選択肢をクリックします。

- ガイド付きスキャンの開始（「["ガイド付きスキャンの概要" ページ116](#)」を参照してください）
- 基本スキャンの開始（「["基本スキャンの実行\(Webサイトスキャン\)" ページ178](#)」を参照してください）
- APIスキャンの開始（「["APIまたはWebサービススキャンの実行" ページ169](#)」を参照してください）

- エンタープライズスキャンの開始（「["エンタープライズスキャンの実行" ページ203](#)」を参照してください）

次も参照

["システムの監査準備" ページ46](#)

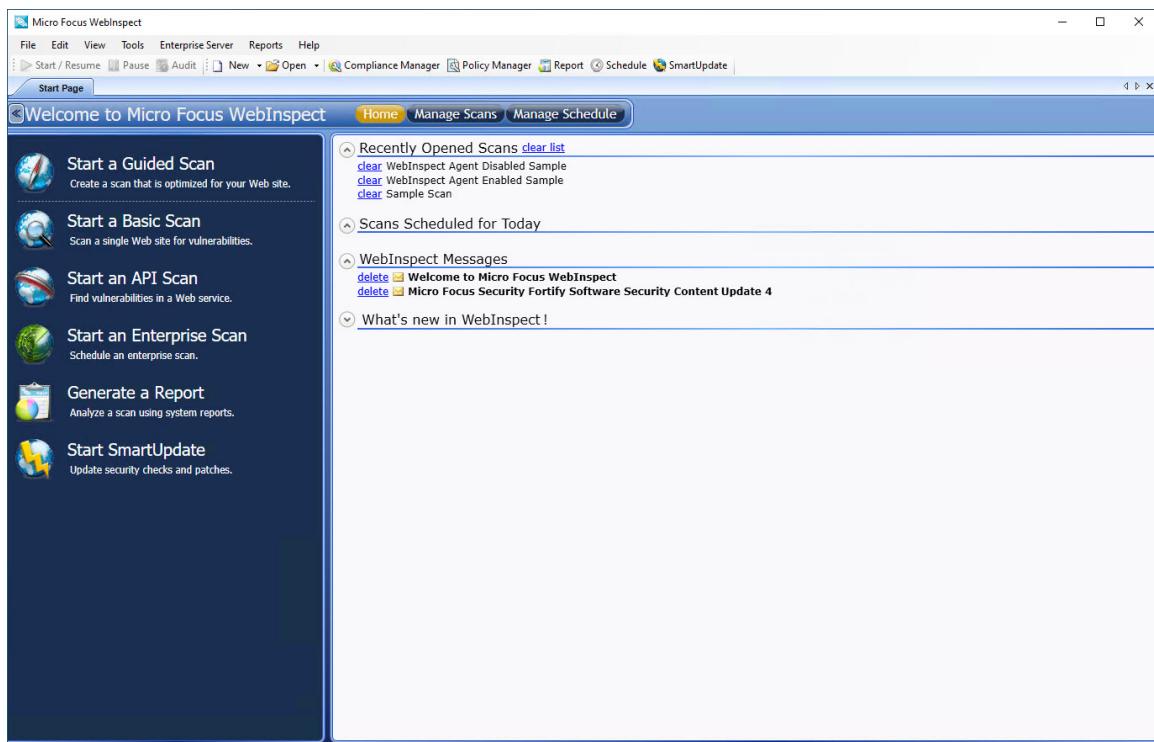
["WebInspectユーザインターフェース" ページ51](#)

第3章: WebInspectユーザインターフェース

Fortify WebInspectを初めて開始するときには、以下に示すように、アプリケーションで [開始ページ(Start Page)] が表示されます。

[開始ページ(Start Page)] のイメージ

メモ: Fortify WebInspectがエンタープライズサーバに接続されている場合は、[SmartUpdate] ボタンの右側に「WebInspect Enterprise WebConsole」というラベルのボタンがあります。このボタンによってWebコンソールが起動します。



アクティビティパネル

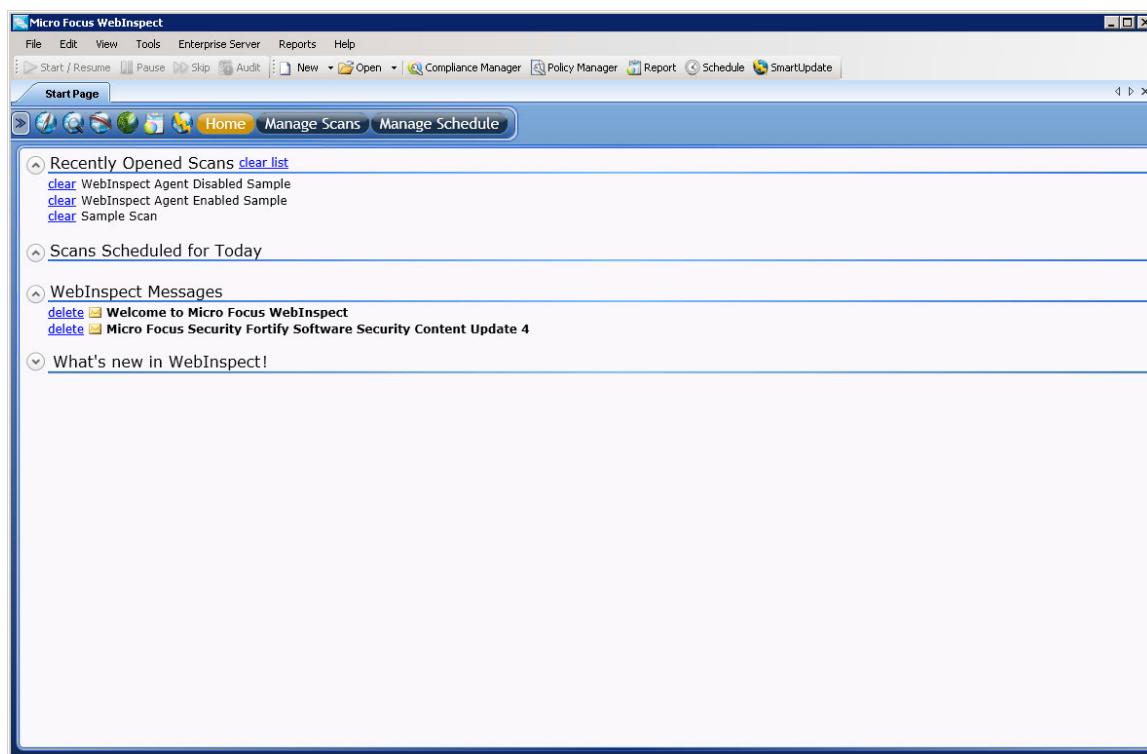
左側のペイン(アクティビティパネル)には、以下の主要な機能へのハイパーリンクが表示されます。

- ガイド付きスキャンの開始(「"ガイド付きスキャンの概要" ページ116」を参照してください)
- 基本スキャンの開始(「"基本スキャンの実行(Webサイトスキャン)" ページ178」を参照してください)
- APIスキャンの開始(「"APIまたはWebサービススキャンの実行" ページ169」を参照してください)

- エンタープライズスキャンの開始(「"エンタープライズスキャンの実行" ページ203」を参照してください)
- レポートの生成(「"レポートの生成" ページ280」を参照してください)
- SmartUpdateの開始(「"SmartUpdate" ページ297」を参照してください)

アクティビティパネルを閉じる

ペインの上のバーの左矢印をクリックすると、アクティビティパネルを閉じることができます。
アクティビティパネルがない 開始ページ(Start Page)】のイメージ



ボタンバー

右側のペインの内容は、次のイメージで示されているボタンバーで選択したボタンによって決まります。

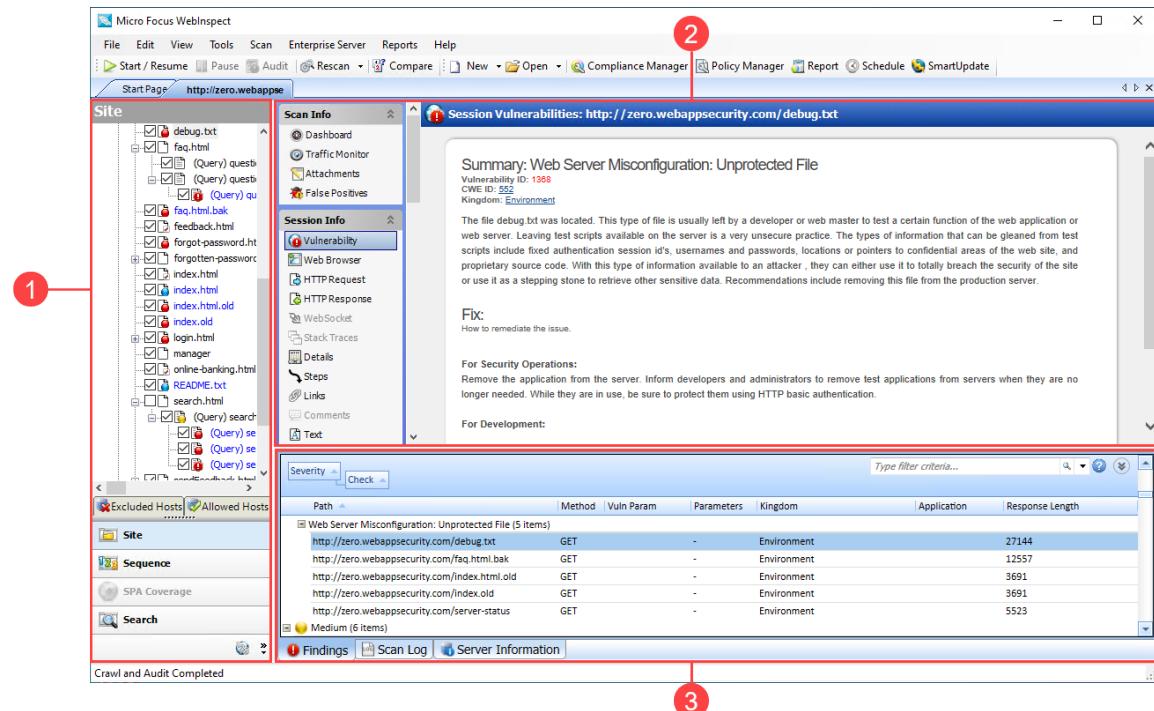


次の表で、選択肢について説明します。

| ボタン | 表示されるリスト |
|----------------------------|--|
| ホーム(Home) | <p>最近開いたスキャンのリストと、今日実行予定のスキャン、最近生成されたレポート、およびMicro Focusサーバからダウンロードされたメッセージが表示されます。</p> <p>ポインタをスキャン名の上に置くと、Fortify WebInspectにスキャンに関する概要情報が表示されます。スキャン名をクリックすると、Fortify WebInspectの別のタブでスキャンが開かれます。</p> |
| スキャンの管理 | 以前に実行したスキャンのリストが表示されます。スキャンを開いたり、名前変更したり、削除したりできます。[接続(Connections)]をクリックして、ローカル(自分のマシン上のSQL Server Express Editionデータベースに保存されているスキャン)またはリモート(自分のマシン上またはネットワーク上の別の場所に設定されたSQL Server Standard Editionデータベースに保存されているスキャン)、またはその両方のデータベースを選択します。詳細については、「 "スキャンの管理" ページ219 」を参照してください。 |
| スケジュールの管理(Manage Schedule) | 実行予定のスキャンのリストを表示します。スキャンをスケジュールに追加したり、スケジュールされたスキャンを編集または削除したり、手動でスキャンを開始したりできます。詳細については、「 "スケジュールされたスキャンの管理" ページ222 」を参照してください。 |

スキャンに関連付けられたペイン

スキャンを開くか実行するたびに、Fortify WebInspectは、ターゲットサイトの名前または説明のラベルが付いたタブを開きます。この作業エリアは、次の図に示されている3つの領域に分かれています。



| 項目 | 説明 |
|----|------------|
| 1 | ナビゲーションペイン |
| 2 | 情報ペイン |
| 3 | サマリペイン |

同時に多数のスキャンを開いていて、すべてのタブを表示するスペースがない場合は、タブバーの最右端にある矢印 をクリックしてタブをスクロールできます。選択したタブを閉じるには、Xをクリックします。

次も参照

["メニューバー" ページ56](#)

["ツールバー" ページ63](#)

["開始ページ\(Start Page\)" 次のページ](#)

"ナビゲーションペイン" ページ67

"サマリペイン" ページ109

"情報ペイン" ページ78

開始ページ(Start Page)

開始ページ(Start Page)]の左側のペインには、Webサイト、API、またはWebサービスの脆弱性スキャンに関連するアクティビティのリストが表示されます。

- ガイド付きスキャンの開始(「"ガイド付きスキャンの概要" ページ116」を参照してください)
- 基本スキャンの開始(「"基本スキャンの実行(Webサイトスキャン)" ページ178」を参照してください)
- APIスキャンの開始(「"APIまたはWebサービススキャンの実行" ページ169」を参照してください)
- エンタープライズスキャンの開始(「"エンタープライズスキャンの実行" ページ203」を参照してください)
- レポートの生成(「"レポートの生成" ページ280」を参照してください)
- SmartUpdateの開始(「"SmartUpdate" ページ297」を参照してください)

右側のペインの内容は、ボタンバーのボタンによって制御されます。



ホーム(Home)

ホーム(Home)]が選択されている場合(デフォルト)、Fortify WebInspectに以下のリストが表示されます。

- 最近開かれたスキャン。
ポイントをスキャン名の上に置くと、Fortify WebInspectにスキャンに関する概要情報が表示されます。スキャン名をクリックすると、Fortify WebInspectの別のタブでスキャンが開かれます。
- 今日実行予定のスキャン
- 最近生成されたレポート
- Micro Focusサーバからダウンロードされたメッセージ

スキャンの管理

スキャンの管理(Manage Scans)]が選択されている場合、以前に実行されたスキャンのリストがFortify WebInspectに表示されます。スキャンを開いたり、名前変更したり、削除したりできます。接続(Connections)]をクリックして、ローカル(自分のマシン上のSQL Server

Express Editionデータベースに保存されているスキャン)またはリモート(SQL Server データベース(設定されている場合)に保存されているスキャン)、またはその両方のデータベースを選択します。詳細については、「["スキャンの管理" ページ219](#)」を参照してください。

スケジュールの管理(Manage Schedule)

「スケジュールの管理(Manage Schedule)」が選択されている場合、スケジュールされたスキャンのリストがFortify WebInspectに表示されます。スキャンをスケジュールに追加したり、スケジュールされたスキャンを編集または削除したり、手動でスキャンを開始したりできます。詳細については、「["スケジュールされたスキャンの管理" ページ222](#)」を参照してください。

次も参照

["WebInspectユーザインターフェース" ページ51](#)

メニューバー

メニューオプションは次のとおりです。

- ・ " [ファイル(File)]メニュー" 下
- ・ " [編集(Edit)]メニュー" 次のページ
- ・ " [表示(View)]メニュー" ページ58
- ・ " [ツール(Tools)]メニュー" ページ58
- ・ " [スキャン(Scan)]メニュー" ページ59
- ・ " [エンタープライズサーバ(Enterprise Server)]メニュー" ページ60
- ・ " [レポート(Reports)]メニュー" ページ61
- ・ " [ヘルプ(Help)]メニュー" ページ61

「ファイル(File)」メニュー

「ファイル(File)」メニューのコマンドについて、次の表で説明します。

| コマンド | 説明 |
|------------------|---|
| 新規(New) | ガイド付きスキャン、基本スキャン、APIスキャン、またはエンタープライズスキャンを選択できます。次いで関連するスキャンウィザードが起動して、スキャン開始のプロセスのステップを示します。 |
| 開く(Open) | スキャンまたは生成されたレポートを開くことができます。 |
| スケジュール(Schedule) | 「スケジュールされたスキャンの管理(Manage Scheduled Scans)」ウィンドウを開きます。このウィンドウでは、スケジュールされたスキャンを追加、編集、または削除できます。 |

| コマンド | 説明 |
|-------------------------|--|
| スキャンのインポート(Import Scan) | スキャンファイルをインポートできます。 |
| エクスポート(Export) | <p>このコマンドは、スキャンを含むタブが選択されている場合にのみ使用できます。以下を実行できます。</p> <ul style="list-style-type: none"> スキャンのエクスポート(Export a scan) スキャン詳細のエクスポート(Export scan details) Software Security Centerへのスキャンのエクスポート(Export a scan to Software Security Center) Webアプリケーションファイアウォール(WAF)への保護ルールのエクスポート(Export protection rules to a web application firewall (WAF)) |
| タブを閉じる(Close Tab) | <p>複数のタブが開いている場合に、選択したタブを閉じます。</p> <p>ヒント: 開いている任意のタブを右クリックし、以下のコンテキストメニューのオプションを使用できます。</p> <ul style="list-style-type: none"> 閉じる-クリックしたタブを閉じます。 これ以外をすべて閉じる(Close All But This) -クリックしたタブを除くすべてのタブを閉じます。 すべて閉じる(Close All) -すべてのタブを閉じます <p>同様に、中央クリックまたは<code><CTRL>+<F4></code>を使用して、1つのタブを閉じることができます。</p> <p>再テストスキャンのためにタブを閉じる場合、スキャンの保持に関するプロンプトが表示されることがあります。詳細については、「"脆弱性の再テスト" ページ244」を参照してください。</p> |
| 終了(Exit) | Fortify WebInspectプログラムを閉じます。 |

編集(Edit)】メニュー

【編集(Edit)】メニューのコマンドについて、次の表で説明します。

| コマンド | 説明 |
|--------------|---|
| デフォルトのスキャン設定 | 【デフォルト設定(Default Settings)】ウィンドウを表示し、スキャンに使用するオプションを選択または変更できるようにします。 |

| コマンド | 説明 |
|-----------------------------------|--|
| (Default Scan Settings) | |
| 現在のスキャン設定 (Current Scan Settings) | 現在のスキャンのオプションを選択または変更できる設定ウィンドウを表示します。このコマンドは、スキャンを含むタブが選択されている場合にのみ使用できます。 |
| 設定の管理 (Manage Settings) | 設定ファイルを追加、編集、または削除できるウィンドウを開きます。 |
| アプリケーション設定 (Application Settings) | 「アプリケーション設定 (Application Settings)」ウィンドウを表示します。このウィンドウでは、Fortify WebInspectアプリケーションの操作を制御するオプションを選択または変更できます。詳細については、「 "アプリケーション設定" ページ442 」を参照してください。 |
| URLのコピー (Copy URL) | 選択したURLをWindowsクリップボードにコピーします。このコマンドは、スキャンを含むタブが選択されている場合にのみ使用できます。 |
| スキャンログのコピー (Copy Scan Log) | (選択したタブのスキャン用に)ログをWindowsクリップボードにコピーします。このコマンドは、スキャンを含むタブが選択されている場合にのみ使用できます。 |

「表示 (View)」メニュー

「表示 (View)」メニューのコマンドについて、次の表で説明します。

| コマンド | 説明 |
|------------------|---|
| 折り返し (Word Wrap) | HTTP要求およびHTTP応答を表示するときに、表示エリアの右側の余白にソフトリターンを挿入します。このコマンドは、スキャンを含むタブが選択されている場合にのみ使用できます。 |
| ツールバー (Toolbars) | 表示するツールバーを選択できます。詳細については、「 "ツールバー" ページ63 」を参照してください。 |

「ツール (Tools)」メニュー

「ツール (Tools)」メニューには、ツールアプリケーションを起動するコマンドが含まれています。

[スキャン(Scan)]メニュー

[スキャン(Scan)]メニューは、スキャンを含むタブにフォーカスがある場合にのみメニューバーに表示されます。[スキャン(Scan)]メニューのコマンドについて、次の表で説明します。

| コマンド | 説明 |
|-------------------------|---|
| 開始/再開 (Start/Resume) | スキャンを開始します。または、処理を一時停止した後で再開します。 |
| 一時停止 (Pause) | Web探索または監査を停止します。スキャンを続行するには、[再開(Resume)]をクリックします。 |
| 監査(Audit) | Web探索を実行したサイトの脆弱性を評価します。このコマンドは、Web探索の完了後、またはステップモードを終了した後に使用します。 |
| 再スキャン (Rescan) | <p>選択したスキャンで最後に使用された設定が事前入力された状態で[スキャンウィザード(Scan Wizard)]を起動します。</p> <p>[再スキャン(Rescan)]ドロップダウンメニューでは、次の項目を実行できます。</p> <ul style="list-style-type: none"> もう一度スキャンする(Scan Again)(「"サイトの再スキャン" ページ249」を参照) 脆弱性の再テスト(Retest Vulnerabilities)(「"脆弱性の再テスト" ページ244」を参照) 増分の再利用(Reuse Incremental)(「"増分スキャン" ページ251」を参照) 改善の再利用(Reuse Remediation)(「"スキャンの再利用" ページ250」を参照) |
| 比較(Compare) | 同じターゲットに対する2つの異なるスキャンによって明らかになった脆弱性を比較します。「 "スキャンの比較" ページ214 」を参照してください。 |

[エンタープライズサーバ(Enterprise Server)]メニュー

[エンタープライズサーバ(Enterprise Server)]メニューには、次のコマンドが含まれています。

| コマンド | 説明 |
|--|--|
| [WebInspect Enterpriseへの接続(Connect to WebInspect Enterprise)]または[切断(Disconnect)] | Fortify WebInspect Enterpriseサーバへの接続を確立または解除します。 |
| スキャンのダウンロード(Download Scan) | サーバからハードドライブにコピーするスキャンを選択できるようにします。 |
| スキャンの発行(Publish Scan) | ダイアログボックスが表示され、そこで脆弱性を確認して、エンタープライズサーバに送信できます。次いで脆弱性はMicro Focus Fortify Software Security Centerサーバに送信されます。詳細については、「 "スキャンの発行(Fortify WebInspect Enterprise接続)" ページ239 」を参照してください。 メモ: このオプションは、Fortify WebInspect EnterpriseがFortify Software Security Centerと統合されている場合にのみ使用できます。 |
| スキャンのアップロード(Upload Scan) | サーバにデータを転送するスキャンを選択できます。ほとんどの場合、これは、アプリケーション設定「スキャンの自動アップロード(auto upload scans)」が選択されていない場合に使用されます。 |
| 設定の転送(Transfer Settings) | Fortify WebInspect設定ファイルを選択してサーバに転送できます。サーバで、これらの設定に基づいてスキャンテンプレートが作成されます。また、スキャンテンプレートを選択してFortify WebInspectに転送することもできます。これにより、テンプレートに基づいて設定ファイルが作成されます。詳細については、「 "エンタープライズサーバとの間での設定の転送" ページ237 」を参照してください。 |
| WebConsole | Fortify WebInspect Enterprise Webコンソールアプリケーションを起動します。 |

| コマンド | 説明 |
|--|--|
| Enterprise Serverについて(About Enterprise Server) | Fortify WebInspect Enterpriseに関する情報を表示します。 |

メモ: スタンドアロンライセンスを使用するFortify WebInspectインストールシステムは、ユーザーがFortify WebInspect Enterprise内の役割のメンバーである限り、いつでもエンタープライズサーバに接続できます。

〔レポート(Reports)〕メニュー

〔レポート(Reports)〕メニューのコマンドについて、次の表で説明します。

| コマンド | 説明 |
|--------------------------|--|
| レポートの生成(Generate Report) | Report Generatorを起動します。 |
| レポートの管理(Manage Reports) | 標準レポートおよびカスタムレポートの種類の一覧が表示されます。カスタム設計されたレポートの名前変更、削除、またはエクスポートと、レポート定義ファイルのインポートを行えます。 |

〔ヘルプ(Help)〕メニュー

〔ヘルプ(Help)〕メニューには、このトピックで説明するコマンドが表示されます。

WebInspectのヘルプ(WebInspect Help)

このコマンドは、ヘルプファイルを開きます。

検索

このコマンドは、ヘルプファイルを開き、左ペインに検索オプションを表示します。

サポート(Support) > 拡張機能の依頼(Request an Enhancement)

サポートチャネルが有効になっている場合(「["アプリケーション設定: サポートチャネル" ページ 470](#)」を参照)、このコマンドは、拡張機能の依頼をMicro Focusに送信するためのウインドウ

を開きます。

サポート (Support) > テクニカルサポートへのお問い合わせ (Contact Technical Support)

このコマンドは、Fortifyカスタマサポートに連絡するための手順を表示します。

サポート (Support) > オープンTCブラウザ情報の取得 (Get Open TC Browsers info)

このメニュー命令は、(スキャンが完了しない場合など)スキャンに関する問題をトラブルシューティングするためにFortifyカスタマサポートと共同で作業する際に使用します。このコマンドは、スキャン中にTruClientブラウザのスナップショットとログを照合します。スキャン中はブラウザは非表示になり、メモリダンプにプロセスは現れません。そのため、これらのスナップショットは、スキャン中にFortify WebInspectが検出した内容のブラウザビューを提供します。

このコマンドを使用するには:

1. [ヘルプ(Help)]> [サポート(Support)]> [オープンTCブラウザ情報の取得 (Get Open TC Browsers info)]を選択します。
2. 参照ボタン([...])をクリックし、照合されたファイルを保存する場所を選択します。
3. [テlemetryへのアップロード(Upload to Telemetry)]を選択して、照合されたファイルを完了時に自動的にMicro Focusにアップロードします。
4. [照合(Collate)]をクリックします。

スキャンGUIDの名前を使用してフォルダが作成され、照合されたスナップショットとログがフォルダ内に配置されます。

サポート (Support) > アプリケーションスナップショットのクリップボードへのコピー (Copy Application Snapshot to Clipboard)

このメニュー命令は、Fortify WebInspectの問題を診断するためにFortifyカスタマサポートと共同で作業する際に使用します。このオプションは、Fortify WebInspectのメモリダンプを作成し、Windowsデバッガツールを使用してダンプ分析を実行できるようにします。

このコマンドを使用するには:

1. [ヘルプ(Help)]> [サポート(Support)]> [アプリケーションスナップショットのクリップボードへのコピー(Copy Application Snapshot to Clipboard)]を選択します。
2. メッセージ全体を受信したら、メモ帳を開き、<CTRL>+<V>を押して内容をファイルに貼り付けます。

チュートリアル

このコマンドを使用して、チュートリアルおよび他のFortify WebInspectドキュメントをダウンロードできます。

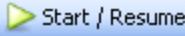
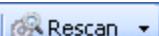
WebInspectについて(About WebInspect)

このコマンドは、ライセンス情報、許可ホスト、属性など、Fortify WebInspectアプリケーションに関する情報を表示します。

ツールバー

Fortify WebInspectウィンドウには、2つのツールバー(スキャンツールバーと標準ツールバー)があります。ツールバーを表示または非表示にするには、[表示(View)]メニューから[ツールバー(Toolbars)]を選択します。

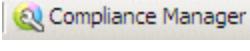
スキャンツールバーで使用可能なボタン

| ボタン | 機能 |
|--|--|
|  Start / Resume | スキャンを一時停止してからスキャンを再開できます。完了したスキャンには、(タイムアウトまたはその他のエラーによる)未送信のセッションが含まれていることがあります。[開始(Start)]をクリックすると、Fortify WebInspectはそれらのセッションの再送信を試行します。 |
|  Pause | 実行中のスキャンを中断します。スキャンを続行するには、[開始/再開(Start/Resume)]ボタンをクリックします。 |
|  Audit | Web探索のみのスキャンまたはステップモードスキャンを実行する場合は、実行後にこのボタンをクリックして監査を実行できます。詳細については、「 手動スキャンの実行 ページ206」を参照してください。 |
|  Rescan ▾ | <p>このボタンは、スキャンを含むタブを選択した場合にのみ表示されます。[再スキャン(Rescan)]ドロップダウンメニューでは、次の項目を実行できます。</p> <ul style="list-style-type: none"> もう一度スキャンする(Scan Again)(「サイトの再スキャン ページ249」を参照) 脆弱性の再テスト(Retest Vulnerabilities)(「脆弱性の再 |

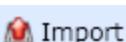
| ボタン | 機能 |
|--|--|
| | <p>"テスト" ページ244を参照)</p> <ul style="list-style-type: none"> 増分の再利用(Reuse Incremental)("増分スキャン" ページ251を参照) 改善の再利用(Reuse Remediation)("スキャンの再利用" ページ250を参照) <p>詳細については、"再テストと再スキャン" ページ244を参照してください。</p> |
|  Compare | <p>このボタンは、スキャンを含むタブを選択した場合にのみ表示されます。これにより、同じターゲットに対する2つの異なるスキャンによって明らかになった脆弱性を比較できます。詳細については、"スキャンの比較" ページ214を参照してください。</p> |
|  Run in WebInspect Enterprise | <p>このボタンは、Fortify WebInspectがFortify WebInspect Enterpriseに接続されており、フォーカスがあるタブでスキャンが開いている場合にのみ表示されます。スキャン設定をFortify WebInspect Enterpriseに送信できます。これにより、スキャン要求が作成され、次に利用可能なセンサのスキャンキューに入れられます。詳細については、"エンタープライズサーバでのスキャンの実行" ページ236を参照してください。</p> |
|  Synchronize | <p>このボタンは、Fortify WebInspect Enterpriseに接続した後でのみ表示されます。Fortify Software Security Centerアプリケーションとバージョンを指定できます。Fortify WebInspectは次にFortify Software Security Centerから脆弱性のリストをダウンロードし、ダウンロードした脆弱性と現在のスキャンで検出された脆弱性を比較し、適切なステータス(新規(New)]、既存(Existing)]、再導入(Reintroduced)]、または 未検出(Not Found)])を割り当てます。詳細については、"Fortify Software Security Centerへの脆弱性の統合" ページ240を参照してください。</p> <p>メモ: このオプションは、Fortify WebInspect EnterpriseがFortify Software Security Centerと統合されている場合にのみ使用できます。</p> |
|  Publish | <p>このボタンは、Fortify WebInspect Enterpriseに接続した後でのみ表示され、Fortify WebInspectとFortify Software Security Centerを同期した後で有効になります。Fortify WebInspect EnterpriseからFortify Software Security Center</p> |

| ボタン | 機能 |
|-----|---|
| | <p>にアプリケーションバージョンデータをアップロードします。</p> <p>メモ: このオプションは、Fortify WebInspect EnterpriseがFortify Software Security Centerと統合されている場合にのみ使用できます。</p> |

標準ツールバーで使用可能なボタン

| ボタン | 機能 |
|--|--|
|  New | ガイド付きスキャン、基本スキャン、APIスキャン、またはエンタープライズスキャンを選択できます。次いで関連するスキャンウィザードが起動して、スキャン開始のプロセスのステップを示します。 |
|  Open | スキャンまたはレポートを開くことができます。 |
|  Compliance Manager | Compliance Managerを起動します。 |
|  Policy Manager | Policy Managerを起動します。 |
|  Report | Report Generatorを起動します。 |
|  Schedule | スキャンが特定の日時に実行されるようにスケジュールを設定できます。詳細については、「 "スキャンのスケジュール" ページ 221 」を参照してください。 |
|  SmartUpdate | 中央のMicro Focusデータベースと通信して、ご使用のシステムに適用できるアップデートがあるかどうかを判別し、アップデートがある場合はアップデートをインストールできるようにします。詳細については、「 "SmartUpdate" ページ 297 」を参照してください。 |
|  WebInspect Enterprise WebConsole | Fortify WebInspect Enterprise Webコンソールアプリケーションを起動します。このボタンは、Fortify WebInspect Enterpriseに接続している場合にのみ表示されます。 |

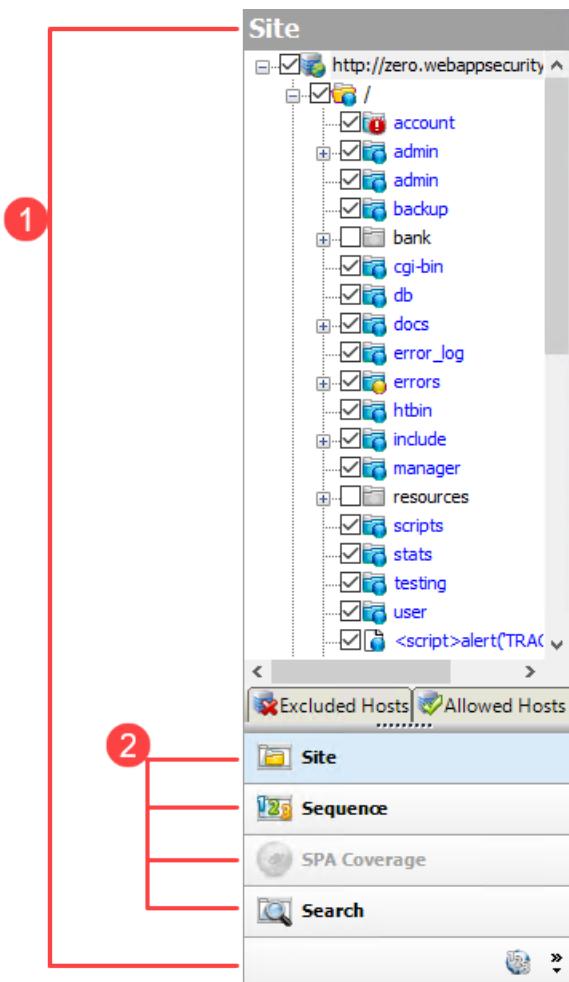
「スキャンの管理(Manage Scans)」ツールバーで使用可能なボタン

| ボタン | 機能 |
|---|--|
|  Open | スキャンを開くには、1つ以上のスキャンを選択して [開く(Open)]をクリックします(または、単にリスト内のエントリをダブルクリックします)。Fortify WebInspectによってスキャンデータがロードされ、それぞれのスキャンは個別のタブに表示されます。 |
|  Rescan ▾ | 選択したスキャンで最後に使用された設定が取り込まれた状態でスキャンウィザードを起動するには、[再スキャン(Rescan)]> [もう一度スキャンする(Scan Again)]をクリックします。 前回のスキャンで明らかになった脆弱性を含むセッションのみを再スキャンするには、スキャンを選択して、[再スキャン(Rescan)]> [脆弱性の再テスト(Retest Vulnerabilities)]をクリックします。 詳細については、「 "再テストと再スキャン" ページ244 」を参照してください。 |
|  Rename | 選択したスキャンの名前を変更するには、[名前変更(Rename)]をクリックします。 |
|  Delete | 選択したスキャンを削除するには、[削除>Delete)]をクリックします。 |
|  Import | スキャンをインポートするには、[インポート(Import)]をクリックします。 |
|  Export ▾ | スキャンのエクスポート、スキャンの詳細のエクスポート、Fortify Software Security Centerへのスキャンのエクスポート、またはWAF (Webアプリケーションファイアウォール)への保護ルールのエクスポートを行うには、[エクスポート(Export)]のドロップダウン矢印をクリックします。 |
|  Compare | スキャンを比較するには、(<Ctrl>を押しながらクリックして) 2つのスキャンを選択し、[比較(Compare)]をクリックします。詳細については、「 "スキャンの比較" ページ214 」を参照してください。 |
|  Connections | デフォルトでは、ローカルSQL Server Express Editionと設定 |

| ボタン | 機能 |
|---|--|
| | 済みのSQL Server Standard Editionに保存されているスキーマがすべてFortify WebInspectによって一覧表示されます。一方または両方のデータベースを選択する、またはSQL Server接続を指定するには、[接続(Connections)]をクリックします。 |
|  Refresh | 必要に応じて、[更新(Refresh)]をクリックして表示を更新します。 |
|  Columns | 表示する列を選択するには、[列(Column)]をクリックします。[上へ移動(Move Up)]ボタンと[下へ移動(Move Down)]ボタンを使用して列を表示する順序を並べ替えたり、[スキャンの管理(Manage Scans)]リストで、単に列見出しをドラッグアンドドロップしたりすることができます。 |

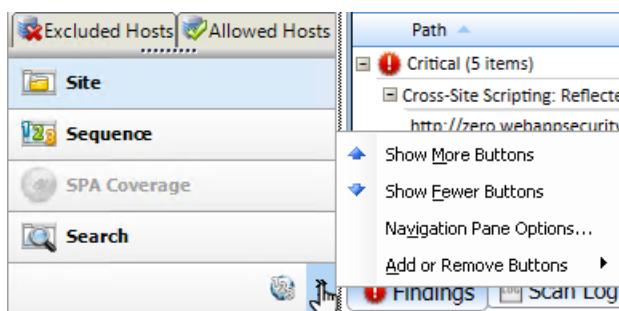
ナビゲーションペイン

スキャンを実行または表示すると、Fortify WebInspectウィンドウの左側にナビゲーションペインが表示されます。ナビゲーションペインに表示される内容(または「ビュー」)を決定する[サイト(Site)]ボタン、[シーケンス(Sequence)]ボタン、[SPAカバレッジ(SPA Coverage)]ボタン、[検索(Search)]ボタン、および[ステップモード(Step Mode)]ボタンが含まれています。



| 項目 | 説明 |
|----|------------|
| 1 | ナビゲーションペイン |
| 2 | 表示を変更するボタン |

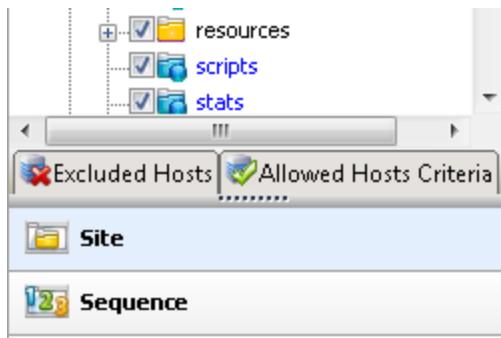
すべてのボタンが表示されていない場合は、ボタンリストの下部にあるドロップダウン矢印をクリックし、[他のボタンを表示 (Show More Buttons)]を選択します。



サイトビュー

Fortify WebInspectのナビゲーションペインにはWebサイトまたはWebサービスの階層構造だけが表示され、それに加えて脆弱性が検出されたセッションが表示されます。サイトのWeb探索中、Fortify WebInspectでは各セッションの横のチェックボックスが選択され(デフォルト)、セッションの監査も行われることが示されます。Web探索と監査を順次実行する場合(サイトが完全にWeb探索されてから監査される場合)、監査を開始する前に関連するチェックボックスをオフにすることで、セッションを監査から除外できます。

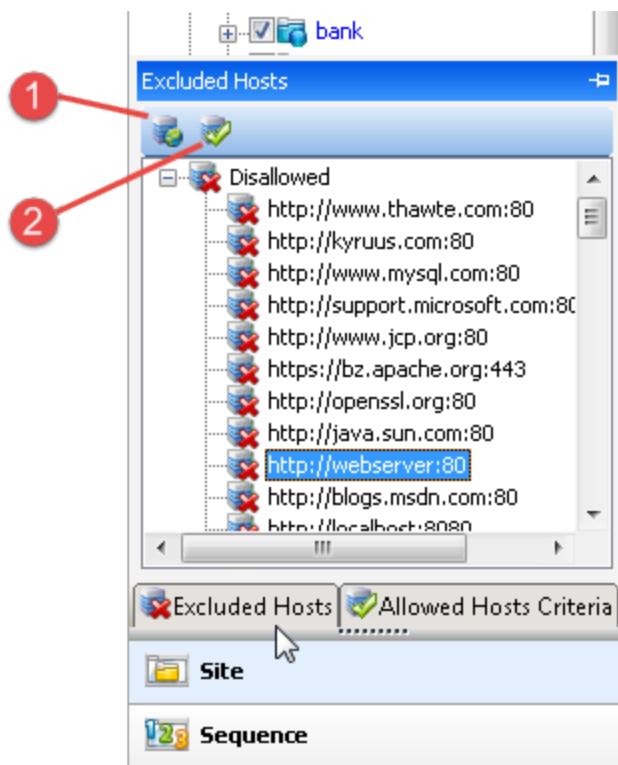
サイトビューには、**除外ホスト(Excluded Hosts)**と**許可ホストの基準(Allowed Hosts Criteria)**という2つのポップアップタブもあります。



除外ホスト

除外ホスト(Excluded Hosts)タブをクリックする(またはその上にポインタを置く)と、タブには許可されていないすべてのホストの一覧が表示されます。これらは、ターゲットサイト内の任意の場所から参照できるホストですが、**許可ホスト(Allowed Hosts)**設定(「デフォルトまたは現在のスキャン設定(Default/Current Scan Settings)」>「スキャン設定(Scan Settings)」>「許可ホスト(Allowed Hosts)」)で指定されていないので、スキャンできません。

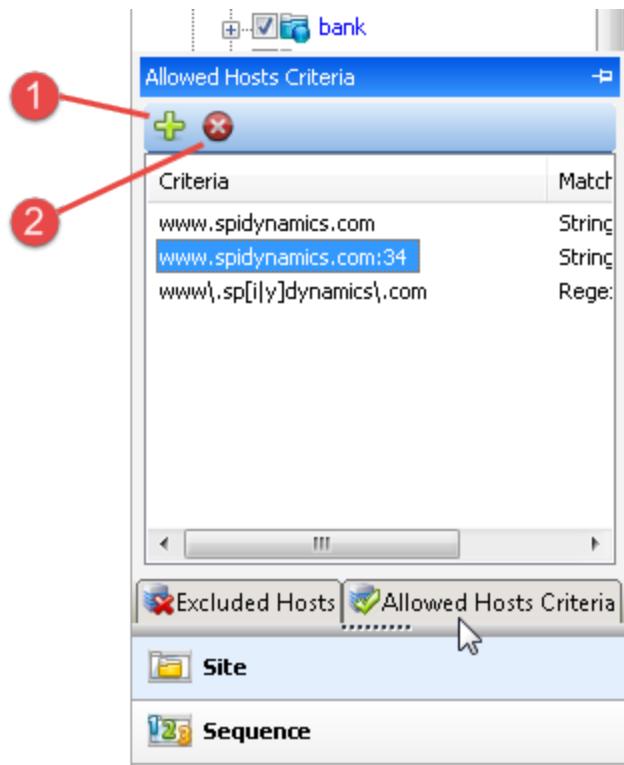
除外ホスト(Excluded Hosts)タブを使用して、除外ホストを選択し、「**スキャンに追加(Add to scan)**」または**許可ホストの基準を追加(Add allowed host criteria)**をクリックできます。



| 項目 | 説明 |
|----|---|
| 1 | スキャンに追加-ホストをスキャンに追加すると、ホストルートディレクトリを表すノードがサイトツリー内に作成されます。Fortify WebInspectは、そのセッションをスキャンします。 |
| 2 | 許可ホストの基準を追加-許可ホストの基準にホストを追加すると、現在のスキャン設定(Current Scan Settings)の許可ホストの一覧にURLが追加されます。Fortify WebInspectは、そのホストへの後続のリンクをスキャンに含めます。ただし、Fortify WebInspectがすでにそのホストへのリンクを含む唯一のリソースをスキャンした後で、許可ホストの基準にホストを追加した場合、追加されたホストはスキャンされません。 |

許可ホストの基準

許可ホストの基準(Allowed Hosts Criteria)タブをクリックする(またはその上にポインタを置く)と、Fortify WebInspectのスキャン設定(許可ホスト(Allowed Hosts)の下)で指定されたURL(または正規表現)がタブに表示されます。削除(Delete)または許可ホストの基準を追加(Add allowed host criteria)をクリックすると、Fortify WebInspectで現在の設定(Current Settings)ダイアログボックスが開き、許可ホストの基準(リテラルURLまたはURLを表す正規表現)を追加、編集、または削除できます。



| 項目 | 説明 |
|----|--|
| 1 | 許可ホストの基準を追加-エントリを追加すると、Fortify WebInspectでは基準に一致するホストへの後続のリンクをスキャンに含めます。ただし、Fortify WebInspectがすでにそのホストへのリンクを含む唯一のリソースをスキャンした後で、ホストを指定した場合、追加されたホストはスキャンされません。 |
| 2 | 削除-許可ホストの一覧からエントリを削除した場合でも、Fortify WebInspectですでに検出したリソースはすべてスキャンに含まれます。 |

後でスキャンするためにこれらの設定を保存するには、[設定(Settings)]ウィンドウの左ペインの下にある[設定に名前を付けて保存(Save settings as)]を選択します。

除外ホストまたは許可ホストの基準を変更する前に、スキャンを一時停止する必要があります。さらに、スキャンを一時停止したポイントによっては、追加または削除されたホストのスキャンが期待どおりに行われない可能性があります。たとえば、Fortify WebInspectがすでに追加されたホストへのリンクを含む唯一のリソースをスキャンした後で、許可ホストを追加した場合、追加されたホストはスキャンされません。

シーケンス(Sequence)]ビュー

[シーケンス(Sequence)]ビューには、スキャン中にFortify WebInspectが検出した順序でサーバリソースが表示されます。

メモ: [サイト(Site)]ビューと[シーケンス(Sequence)]ビューのどちらにおいても、青いテキストで示されるのは、リンクを介して検出されたリソースではなく、Fortify WebInspectによって「推測された」ディレクトリまたはファイルです。たとえば、Fortify WebInspectは、ターゲットWebサイトに「backup」という名前のディレクトリが含まれているかどうかを検出する試行の際、要求「GET /backup/ HTTP/1.1」を常時送信します。

SPAカバレッジ(SPA Coverage)

[SPAカバレッジ(SPA Coverage)]ビューは、SPAサポートがスキャンに対して有効になっている場合にのみ使用できます。このビューには、Web探索プログラムがWeb探索中に操作したページ内の要素が表示されます。

SPA Coverage

Total: 138

| URL | Display Name | Selector |
|-----------------------------------|-------------------------------------|--|
| http://localhost:8080/WebGoat/... | Cross-Site Scripting (XSS) | //a[normalize-space(string(.))=...] |
| http://localhost:8080/WebGoat/... | Stage 5: Reflected XSS | //a[@id='Stage5ReflectedXSS'] |
| http://localhost:8080/WebGoat/... | Denial of Service from Multiple ... | //a[@id='DenialOfServicefrom...'] |
| http://localhost:8080/WebGoat/... | Admin Functions | //a[normalize-space(string(.))=...] |
| http://localhost:8080/WebGoat/... | Challenge | //a[normalize-space(string(.))=...] |
| http://localhost:8080/WebGoat/... | LAB: Client Side Filtering | //a[@id='LABClientSideFiltering'] |
| http://localhost:8080/WebGoat/... | XML Injection | //a[@id='XMLInjection'] |
| http://localhost:8080/WebGoat/... | The CHALLENGE | //a[@id='TheCHALLENGE'] |
| http://localhost:8080/WebGoat/... | Report Card | //a[@id='ReportCard'] |
| http://localhost:8080/WebGoat/... | Hijack a Session | //a[@id='HijackaSession'] |
| http://localhost:8080/WebGoat/... | Stage 4: Parameterized Query #2 | //a[@id='Stage4Parameterized...'] |
| http://localhost:8080/WebGoat/... | Tomcat Configuration | //a[@id='TomcatConfiguration'] |
| | Denial of Service | //span[normalize-space(string(.))=...] |
| http://localhost:8080/WebGoat/... | Command Injection | //a[@id='CommandInjection'] |
| http://localhost:8080/WebGoat/... | Useful Tools | //a[@id='UsefulTools'] |
| http://localhost:8080/WebGoat/... | Access Control Flaws | //a[normalize-space(string(.))=...] |
| http://localhost:8080/WebGoat/... | Blind Numeric SQL Injection | //a[@id='BlindNumericSQLInjec...'] |
| http://localhost:8080/WebGoat/... | Stage 2: Add Business Layer A... | //a[@id='Stage2AddBusinessL...'] |
| | Insecure Storage | //span[normalize-space(string(.))=...] |
| http://localhost:8080/WebGoat/... | Session Fixation | //a[@id='SessionFixation'] |
| http://localhost:8080/WebGoat/... | Fail Open Authentication Scheme | //a[@id='FailOpenAuthenticati...'] |
| http://localhost:8080/WebGoat/... | General | //a[normalize-space(string(.))=...] |
| | | |

Site

Sequence

SPA Coverage

Search

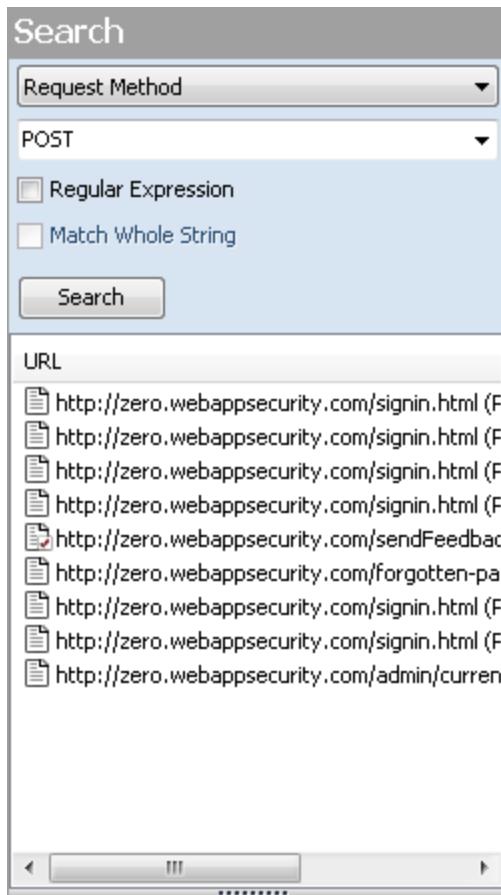
[SPAカバレッジ(SPA Coverage)]ビューには、要素が検出されたURLと、次の追加情報が一覧表示されます。

- 表示名(Display Name)** - 表示されるテキスト、記号、リンク、HTMLタグ名、または検出された要素に関連する他のUI情報。
- セレクタ(Selector)** - ページ内の要素のXPathの場所。これは、要素に対する操作の検索と実行に使用されます。

詳細については、「"シングルページアプリケーションスキャンについて" ページ210」を参照してください。

検索(Search)]ビュー

検索(Search)]ビューでは、すべてのセッションでさまざまなHTTPメッセージコンポーネントを検索できます。たとえば、ドロップダウンリストから **要求メソッド(Request Method)**]を選択し、検索文字列として **POST**]を指定すると、Fortify WebInspectはHTTP要求がPOSTメソッドを使用しているすべてのセッションを一覧表示します。



検索(Search)]ビューを使用するには:

1. ナビゲーションペインで、**検索(Search)**]をクリックします(ペインの下部)。すべてのボタンが表示されてはいない場合は、ボタンリストの下部にある **ボタンの設定 (Configure Buttons)**]ドロップダウンリストをクリックし、**他のボタンを表示 (Show More Buttons)**]を選択します。
2. 一番上のリストから、検索するエリアを選択します。
3. コンボボックスで、検索する文字列を入力または選択します。
4. 文字列が正規表現を表している場合は、**正規表現 (Regular Expression)**]チェックボックスをオンにします。詳細については、「"正規表現" ページ323」を参照してください。

- 検索文字列と完全に一致する文字列全体をHTTPメッセージ内で検索するには、**文字列全体を照合する(Match Whole String)** チェックボックスをオンにします。完全一致では、大文字と小文字は区別されません。

メモ: このオプションは、特定の検索ターゲットには使用できません。

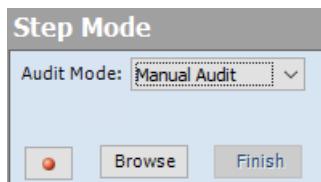
- 検索(Search)]をクリックします。

[ステップモード(Step Mode)]ビュー

ステップモードは、[サイト(Site)]ビューまたは[シーケンス(Sequence)]ビューで選択したセッションから始めて、サイト内を手動で移動する場合に使用します。

次のステップに従って、サイトをステップごとに移動します。

- [サイト(Site)]または[シーケンス(Sequence)]ビューで、セッションを選択します。
- [ステップモード(Step Mode)]ボタンをクリックします。
ボタンが表示されていない場合は、[ボタンの設定(Configure Buttons)]ドロップダウンをクリックし、[他のボタンを表示>Show More Buttons]を選択します。
- ナビゲーションペインに[ステップモード(Step Mode)]が表示されたら、[監査モード]リストから[ブラウズ時に監査する(Audit as you browse)]か[手動監査(Manual Audit)]を選択します。[手動監査(Manual Audit)]をお勧めします。



- [記録(Record)] [] をクリックします。
- [参照(Browse)] をクリックします。
選択したブラウザが開き、選択したセッションに関連付けられている応答が表示されます。必要な数のページを引き続き参照できます。
- 完了したら、Fortify WebInspectに戻って[完了(Finish)]をクリックします。
新しいセッションがナビゲーションペインに追加されます。
- ステップ3で[手動監査(Manual Audit)]を選択した場合は、[Audit]をクリックします。
Fortify WebInspectは、ステップモードで追加(または置換)したセッションを含む、監査されていないすべてのセッションを監査します。

ナビゲーションペインのアイコン

次の表を使用して、ナビゲーションペインに表示されるリソースを識別します。

ナビゲーションペインで使用されるアイコン

| アイコン | 説明 |
|------|---|
| | サーバ/ホスト: サイトのツリー構造の最上位を表します。 |
| | 青色のフォルダ: Web探索ではなく「推測」によって検出されたフォルダです。 |
| | 黄色のフォルダ: Webサイト上でコンテンツを使用できるフォルダです。 |
| | 灰色のフォルダ: パスの切り捨てによる項目の検出を示すフォルダです。親が検出されると、フォルダはプロパティに応じて青または黄色で表示されます。 |
| | ファイル。 |
| | クエリまたはポスト。 |
| | DOMイベント。 |

フォルダまたはファイルに重なって表示されるアイコンは、検出された脆弱性を示します

| アイコン | 説明 |
|------|---|
| | 感嘆符付きの赤い点は、オブジェクトに重大な脆弱性が含まれていることを示します。攻撃者は、サーバ上でコマンドを実行したり、個人情報を取得および変更したりできる可能性があります。 |
| | 赤色の点は、オブジェクトに高レベルの脆弱性が含まれていることを示します。一般に、ソースコード、Webルート外のファイル、および機密性の高いエラーメッセージの表示が可能になります。 |
| | 金色の点は、オブジェクトに中程度レベルの脆弱性が含まれていることを示します。これらは通常、HTML以外のエラーや、機密性が高い可能性がある問題です。 |
| | 青色の点は、オブジェクトに低レベルの脆弱性が含まれていることを示します。これらは通常注目すべき問題、またはより高いレベルの問題になる可能性のある問題です。 |
| | 青色の円の中にある「i」は、情報項目を示します。これらは、サイト内の興味深い点、または特定のアプリケーションやWebサーバです。 |
| | 赤色のチェックマークは、「ベストプラクティス」違反を示します。 |

ナビゲーションペインのショートカットメニュー

「サイト(Site)」ビューまたは「シーケンス(Sequence)」ビューの使用中にナビゲーションペインで項目を右クリックすると、ショートカットメニューに次のオプションが表示されます。

- **子の展開*(Expand Children*)** - (「サイト(Site)」ビューのみ)サイトツリーのブランチノードを展開します。
- **子の折りたたみ*(Collapse Children*)** - (「サイト(Site)」ビューのみ)ブランチノードを上位ノードに短縮します。
- **すべてをオン(Check All*)** - (「サイト(Site)」ビューのみ)親ノードとすべての子のチェックボックスをオンにします。
- **すべてをオフ(Uncheck All*)** - (「サイト(Site)」ビューのみ)親ノードとすべての子のチェックボックスをオフにします。
- **セッションレポートの生成*(Generate Session Report*)** - (「サイト(Site)」ビューのみ)選択したセッションの概要情報、攻撃の要求と攻撃の応答、URLとのリンク、コメント、フォーム、電子メールアドレス、およびチェックの説明を示すレポートを作成します。
- **サイトツリーのエクスポート*(Export Site Tree*)** - (「サイト(Site)」ビューのみ)指定した場所にXML形式でサイトツリーを保存します。
- **URLのコピー(Copy URL)** - URLをWindowsのクリップボードにコピーします。
- **ブラウザで表示(View in Browser)** - HTTP応答をブラウザで表示します。
- **リンク(Links)** - (「サイト(Site)」ビューのみ)選択したリソースへのリンクが含まれている、ターゲットサイトのすべてのリソースを一覧表示します。リンクは、HTMLタグ、スクリプト、またはHTMLフォームによってレンダリングできます。また、選択したセッションのHTTP応答内のリンクによって参照されるすべてのリソースも(「リンク先(Linked To)」の下に)一覧表示されます。表示されているリンクをダブルクリックすると、Fortify WebInspectによって、ナビゲーションペインのフォーカスが、参照されているセッションに移動します。または、Webブラウザでセッションを表示することにより、リンクされたリソースを参照することもできます(「Webブラウザ(Web Browser)」をクリック)。
- **追加(Add)** - Fortify WebInspectスキャン以外の方法(手動検査、その他のツールなど)で検出された場所を情報として追加できます。その後、検出された脆弱性をそれらの場所に追加して、サイトのより完全な説明を分析用にアーカイブできます。
 - **ページ(Page)** - 個別のURL(リソース)。
 - **ディレクトリ(Directory)** - ページのコレクションを含むフォルダ。
「ページ(Page)」または「ディレクトリ(Directory)」を選択すると、ディレクトリまたはページに名前を付けてHTTP要求と応答を編集するためのダイアログボックスが表示されます。
 - **バリエーション(Variation)** - その場所の特定の属性を一覧にした場所のサブノード。たとえば、*login.asp*の場所には、「(Query)
Username=12345&Password=12345&Action=Login」というバリエーションがあります。バリエーションは、サブノードに加えて脆弱性が付加されている可能性があるという点で、他の場所と同じです。

「**バリエーション(Variation)**」を選択すると、「**バリエーションの追加 (Add Variation)**」ダイアログボックスが表示されます。このダイアログボックスでは、バリエーション属性の編集、PostまたはQueryの指定、およびHTTP要求と応答の編集を行うことができます。

- **脆弱性(Vulnerability)** -セキュリティ上の特定の脅威。

「**脆弱性(Vulnerability)**」を選択すると、「**脆弱性の編集(Edit Vulnerabilities)**」ダイアログボックスが表示されます。このダイアログボックスでは、バリエーション属性の編集、PostまたはQueryの指定、およびHTTP要求と応答の編集を行うことができます。詳細については、「["脆弱性の編集" ページ269](#)」を参照してください。

- **脆弱性の編集(Edit Vulnerabilities)** -手動で追加した場所を編集したり、脆弱性を編集したりすることができます。詳細については、「["脆弱性の編集" ページ269](#)」を参照してください。
- **場所の削除(Remove Location)** -選択したセッションをナビゲーションペイン(「**サイト(Site)**」ビューと「**シーケンス(Sequence)**」ビューの両方)から削除し、関連する脆弱性もすべて削除します。

メモ: 削除された場所(セッション)およびそれに関連する脆弱性を回復できます。詳細については、「["削除された項目の回復" ページ278](#)」を参照してください。

- **誤検出としてマーク(Mark as False Positive)** -脆弱性に誤検出のフラグを付け、メモを追加できます。
- **送信先(Send to)** -Fortify WebInspectのアプリケーション設定で指定されたプロファイルを使用して、選択した脆弱性を欠陥に変換し、Micro Focus Application Lifecycle Management (ALM)に割り当てることができます。
- **サーバの削除(Remove Server)** -ナビゲーションペインからサーバを削除し、残りのスキャンアクティビティにそのサーバを含めないようにします。このコマンドは、サーバを右クリックした場合にのみ表示されます。
- **Web探索(Crawl)** -選択したURLのWeb探索を再実行します。
- **添付ファイル(Attachments)** -選択したセッションに関連するメモの作成、フォローアップのためのセッションへのフラグ付け、脆弱性のメモの追加、脆弱性スナップショットの追加を行うことができます。
- **ツール(Tools)** -使用可能なツールのサブメニューを表示します。
- **現在のセッションでフィルタ(Filter by Current Session)** -サマリペイン内の項目の表示を、選択したセッションのSummaryDataIDを持つ項目に制限します。

*ナビゲーションペインで「**サイト(Site)**」ビューを使用している場合のみ、ショートカットメニューにコマンドが表示されます。

次も参照

["WebInspectユーザインターフェース" ページ51](#)

["検索\(Search\)\]ビュー" ページ261](#)

["結果の検査" ページ257](#)

情報ペイン

スキャンを実行または表示する際、情報ペインに、3つの折りたたみ可能な情報パネルと、1つの情報表示エリアが表示されます。

The screenshot shows the WebInspect interface with the following callouts:

- Scan Info panel (left): A tree view showing 'Dashboard', 'Traffic Monitor', 'Attachments', and 'Failures'. The 'Failures' node is highlighted with a red circle containing the number 1.
- Session Info panel (left): A tree view showing 'Vulnerability', 'Web Browser', 'HTTP Request', 'HTTP Response', 'Stack Traces', 'Details', 'Steps', 'Links', 'Comments', 'Text', 'Hidden', 'Forms', 'E-mail', 'Scripts', 'Attachments', and 'Attack Info'. The 'Links' node is highlighted with a red circle containing the number 2.
- Host Info panel (left): A tree view showing 'P2P Info', 'AJAX', 'Certificates', 'Comments', 'Cookies', 'E-mail', 'For', 'Hidden', 'Scripts', and 'Broken Links'. The 'For' node is highlighted with a red circle containing the number 3.
- Information Area (right): A large panel titled 'Session Vulnerabilities: http://zero.webappsecurity.com/stats/'. It displays a list of vulnerabilities: 'Access Control: Unprotected File', 'Privacy Violation: Autocomplete', 'Credential Management: Insecure Transmission', and 'Transport Layer Protection: Unencrypted Login Form'. Below this, a specific vulnerability is expanded: 'Summary: Access Control: Unprotected File' with ID 10229, CWE ID 548, and Kingdom: Environment. It describes the risk of sensitive information being accessible through log files and suggests remediation steps. A red circle containing the number 4 is positioned above the 'Fix' section.

| 項目 | 説明 |
|----|--|
| 1 | 「スキャン情報(Scan Info)」パネル ("スキャン情報(Scan Info)"]パネル" 次のページを参照してください) |
| 2 | 「セッション情報(Session Info)」パネル ("セッション情報(Session Info)"]パネル" ページ91を参照してください) |
| 3 | 「ホスト情報(Host Info)」パネル ("ホスト情報(Host Info)"]パネル" ページ100を参照してください) |
| 4 | 情報表示エリア |

左側の列にあるこれらの3つの情報パネルの1つで項目をクリックし、表示する情報のタイプを選択します。

ヒント: 脆弱性情報を表示する際にリンクをたどる場合、ナビゲーションペインで強調表示されたセクションをクリックすると戻ることができます。

次も参照

["サマリペイン" ページ109](#)

["WebInspectユーザインターフェース" ページ51](#)

["ナビゲーションペイン" ページ67](#)

[" \[スキャン情報\(Scan Info\)\]パネル" 下](#)

[" \[セッション情報\(Session Info\)\]パネル" ページ91](#)

[" \[ホスト情報\(Host Info\)\]パネル" ページ100](#)

[スキャン情報(Scan Info)]パネル

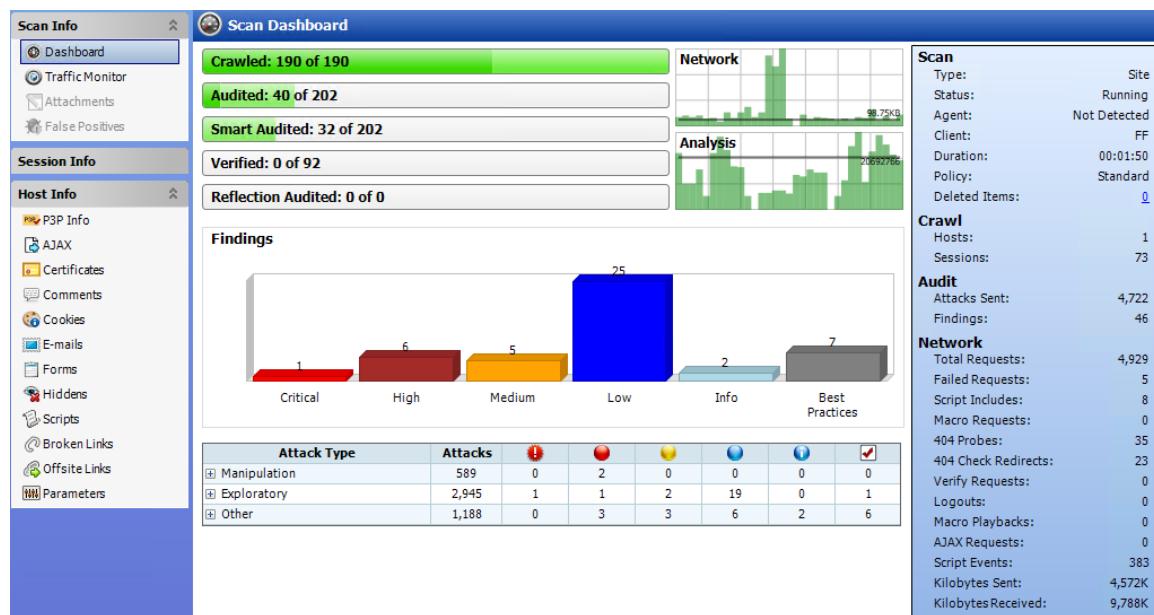
[スキャン情報(Scan Info)]パネルには、次の選択肢があります。

- ダッシュボード
- Traffic Monitor
- 添付ファイル
- 誤検出

ダッシュボード

[ダッシュボード(Dashboard)]を選択すると、スキャン結果のリアルタイムの概要とスキャン進行状況のグラフィックが表示されます。このセクションは [デフォルト(Default)]または [現在の設定(Current)]でこのオプションを選択した場合にのみ表示されます。詳細については、「["ダッシュボード" ページ82](#)」を参照してください。

ダッシュボードのイメージ



Traffic Monitor

Fortify WebInspectのナビゲーションペインには、通常、WebサイトまたはWebサービスの階層構造だけが表示され、それに加えて脆弱性が検出されたセッションが表示されます。Traffic MonitorまたはTraffic Viewerを使用すると、Fortify WebInspectによって送信されたすべてのHTTP要求と、Webサーバから受信した関連するHTTP応答を表示および確認できます。

Traffic MonitorまたはTraffic Viewerは、スキャンの実行前にTraffic Monitorロギングが有効になっている場合にのみ利用できます。

詳細については、「["Traffic Monitor \(Traffic Viewer\)" ページ255](#)」を参照してください。

添付ファイル(Attachments)

「**添付ファイル(Attachments)**」を選択すると、スキャンに追加されたすべてのセッションのメモ、脆弱性のメモ、フォローアップ用フラグ、および脆弱性スクリーンショットの一覧が表示されます。各添付ファイルは、特定のセッションに関連付けられています。このフォームには、スキャンメモ(特定のセッションではなく、スキャン全体に適用されるメモ)も一覧表示されます。

スキャンメモを作成したり、既存の添付ファイルを編集または削除したりできます。

スキャンメモを作成するには、(情報表示エリアの) **追加(Add)** メニューをクリックします。

添付ファイルを編集するには、添付ファイルを選択して **編集(Edit)** をクリックします。

Fortify WebInspectユーザインターフェースの他のエリアで添付ファイルを作成するには、次のいずれかを実行します。

- ナビゲーションペインでセッションを右クリックし、ショートカットメニューから **添付ファイル(Attachments)** を選択します。

- ・ サマリペインの [検出事項(Findings)] タブで URL を右クリックし、ショートカットメニューから [添付ファイル(Attachments)] を選択します。

Micro Focus Application Lifecycle Management (ALM) に不具合を送信すると、Fortify WebInspect によってメモが自動的にセッションに追加されます。

詳細については、「"添付ファイル(Attachments) - スキャン情報(Scan Info)" ページ89」を参照してください。

添付ファイルのイメージ

誤検出(False Positives)

この機能は、Fortify WebInspect が脆弱性を含むものとして最初にフラグを立てたものの、後でユーザが誤検出と判断したすべての URL を一覧表示します。このオプションは、誰かが実際に誤検出として脆弱性を指定するまでは表示されません。

誤検出に関連付けられた URL をクリックすると、ユーザが脆弱性を削除した際に入力されたメモが表示されます。

脆弱性を再割り当てし、[誤検出(False Positive)] リストから URL を削除するには、URL を選択して [脆弱性としてマーク(Mark as Vulnerability)] をクリックします。

以前のスキャンから、誤検出として特定された脆弱性のリストをインポートできます。続いて、Fortify WebInspect は、以前のスキャンで検出されたこれらの誤検出を、現在のスキャンで検出された脆弱性と相関させ、新たに出現した脆弱性に誤検出のフラグを設定します。

詳細については、「"誤検出(False Positives)" ページ89」を参照してください。

誤検出のイメージ

The screenshot shows the 'Scan False Positives' interface. The left sidebar has tabs for 'Scan Info', 'Session Info', and 'Attachments'. The main panel shows a table of false positives with columns for Risk, URL, Vulnerability, State, and Source. The table lists several items, including:

- Vulnerability: Backup File (Appended .bak) (1 item)
- Vulnerability: Possible Server Path Disclosure (unix) (1 item)
- Vulnerability: Form Auto Complete Active (1 item)
- Vulnerability: Potential filename found in comments (1 item)

次も参照

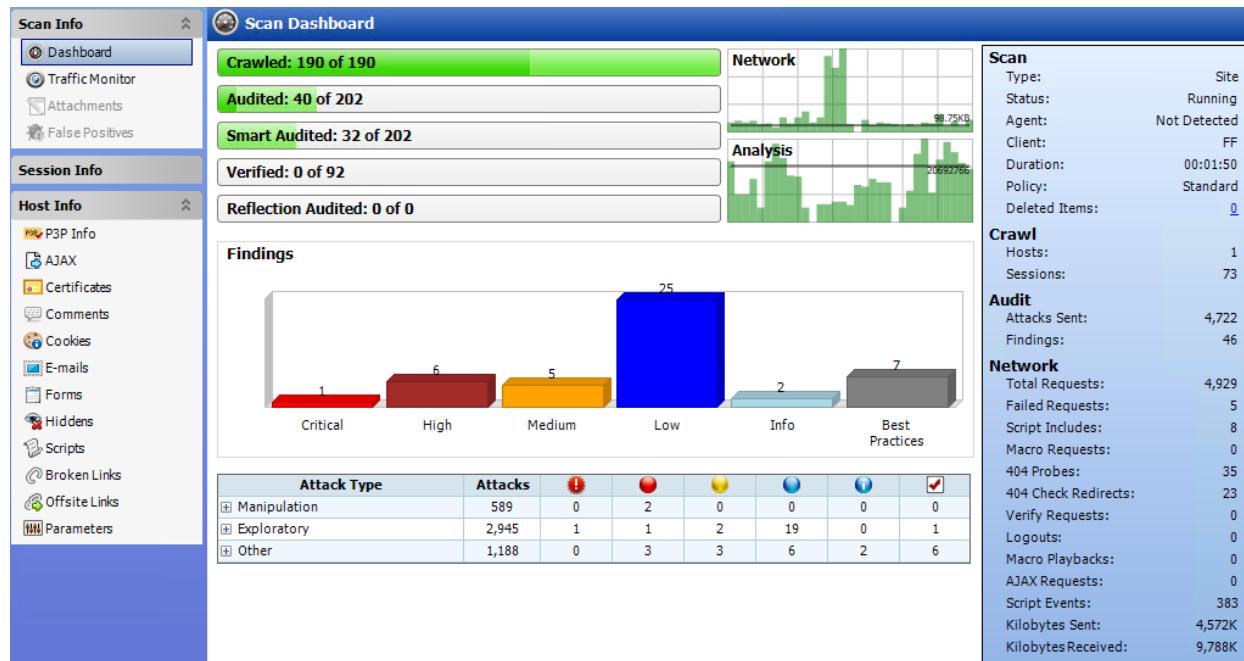
- "[セッション情報(Session Info)]パネル" ページ91
- "[ホスト情報(Host Info)]パネル" ページ100
- "WebInspectユーザインターフェース" ページ51
- "ダッシュボード" 下
- "Traffic Monitor (Traffic Viewer)" ページ255
- "添付ファイル(Attachments) -スキャン情報(Scan Info)" ページ89

ダッシュボード

「ダッシュボード(Dashboard)」を選択すると、スキャン結果のリアルタイムの概要とスキャン進行状況のグラフィックが表示されます。

ダッシュボードのイメージ

次のイメージは、スキャンが進行中のスキャンダッシュボードを示しています。



進行状況バー

各バーは、そのスキャンフェーズにおける進行状況を表します。



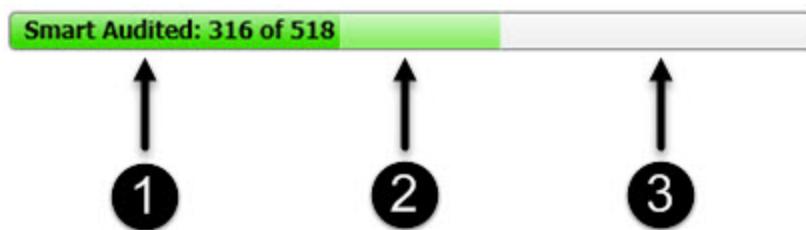
進行状況バーの説明

次の表に、進行状況バーの説明を示します。

| 進行状況バー | 説明 |
|----------------------|---|
| Web探索済み (Crawled) | Web探索済みのセッションの数 / Web探索するセッションの総数。 |
| 監査済み (Audited) | 監査済みのセッションの数 / 監査するセッションの総数。 総数には、スマート監査によって処理されるサーバタイプに関連するもの |

| 進行状況バー | 説明 |
|----------------------------|--|
| | 以外のすべてのチェックが含まれます。 |
| スマート監査済み(Smart Audited) | <p>スマート監査を使用して監査済みのセッションの数/スマート監査のセッションの総数。</p> <p>スマート監査では、Fortify WebInspectが、Webアプリケーションをホストしているサーバのタイプを検出します。Fortify WebInspectは、サーバタイプに固有のチェックを実行し、サーバタイプに対して有効でないチェックを回避します。</p> |
| 検証済み(Verified) | <p>検証済みの永続的XSS脆弱セッションの数/検証する永続的XSS脆弱セッションの総数。</p> <p>永続的XSS監査が有効になっている場合は、Fortify WebInspectが、脆弱なすべてのセッションに対して2件目の要求を送信し、過去に行つたプローブに対するすべての応答を検査します。プローブが特定された場合は、Fortify WebInspectがそれらのページ間のリンクを内部的に記録します。</p> |
| 反射監査済み(Reflection Audited) | <p>監査済みの永続的XSS脆弱リンク済みセッションの数/監査する永続的XSS脆弱リンク済みセッションの総数。</p> <p>永続的XSS監査が有効になっている場合は、永続的XSSの検証ステップで検出されたリンク済みセッションを監査するために必要な作業を表します。</p> |

進行状況バーの色

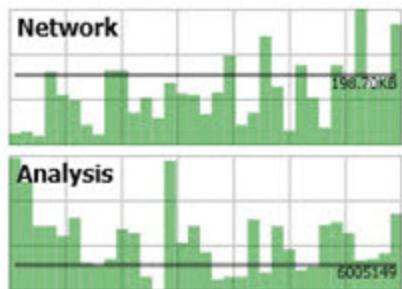


1. 濃い緑色は、処理されたセッションを表します。
2. 薄い緑色は、除外、中止、または拒否されたセッション(処理対象と見なされていたが、設定などの理由でスキップされたセッション)を表します。
3. 薄い灰色は、未処理のセッションを表します。

アクティビティメータ

Fortify WebInspectは、スキャンで発生しているアクティビティに関する情報をポーリングして、アクティビティメータにデータを表示します。このデータは、スキャンアクティビティのリアルタイムス

ナップショットを表します。この情報は、スキャンが停止しているのか、活発に動作しているのかを判断するのに役立ちます。



アクティビティメータの説明

次の表に、アクティビティメータの説明を示します。

| メータ | 説明 |
|---------------------|--|
| ネットワーク (Network) | Fortify WebInspectによって送受信されるデータの量。 グラフには、このデータが過去1秒間に送受信されたB、KB、またはMB単位で表示されます。 |
| 分析(Analysis) | すべてのスレッドの処理において、Fortify WebInspectによって1秒あたりに実行される作業の量。 |

脆弱性グラフィック

次の表に、脆弱性棒グラフとグリッドの説明を示します。

| グラフィック | 説明 |
|----------|---------------------------------------|
| 脆弱性グラフ | スキャンに対して特定された重大度レベルごとの問題の総数。 |
| 攻撃統計グリッド | 攻撃の種類と監査エンジン別に分類された、行われた攻撃と検出された問題の数。 |

統計パネルスキャン

次の表に、統計パネルの [スキャン(Scan)] セクションの説明を示します。

| 項目 | 説明 |
|-----------|---|
| タイプ(Type) | スキャンのタイプ: [サイト(Site)]、[サービス(Service)]、または [サイト再テスト(Site Retest)]。 |
| スキャンステータ | ステータス: [実行中(Running)]、[一時停止(Paused)]、または [完 |

| 項目 | 説明 |
|------------------------|---|
| ス(Scan Status) | 了(Complete)]。 |
| エージェント(Agent) | Fortify WebInspect Agentを意味し、[検出(Detected)]または[未検出(Not Detected)]のどちらかを示します。特定のチェック(SQLインジェクション、コマンド実行、クロスサイトスクリプティングなど)に対して、Fortify WebInspect Agentは、Fortify WebInspect HTTP要求を傍受し、ターゲットモジュールでランタイム分析を実行します。この分析によって脆弱性が存在することが確認されると、Fortify WebInspect AgentはHTTP応答にスタックトレースを追加します。開発者は、このスタックトレースを分析して、改善が必要なエリアを調査できます。 |
| クライアント(Client) | スキャン用に指定されたレンダリングエンジン。オプションを次に示します。 <ul style="list-style-type: none"> IE (Internet Explorer) FF (Firefox) iPhone iPad Android Windows Phone Windows RT |
| 期間(Duration) | スキャンが実行されている時間の長さ(スキャンが異常終了した場合は間違っている可能性があります)。 |
| ポリシー(Policy) | スキャンに使用されるポリシーの名前。 |
| 削除された項目(Deleted Items) | ユーザがスキャンから削除したセッションと脆弱性の数。 セッションを削除するには、ナビゲーションペインでセッションを右クリックし、ショートカットメニューから[場所の削除(Remove Location)]を選択します。詳細については、「 "ナビゲーションペイン" ページ67 」を参照してください。 脆弱性を削除するには、サマリペインで脆弱性を右クリックし、ショートカットメニューから[脆弱性を無視(Ignore Vulnerability)]を選択します。詳細については、「 "サマリペイン" ページ109 」を参照してください。 削除されたセッションまたは脆弱性を復元するには: <ol style="list-style-type: none"> スキャンダッシュボードで、削除された項目に関連付けられた番号をクリックします。 |

| 項目 | 説明 |
|----|---|
| | <p>削除された項目の回復(Recover Deleted Items)]ウィンドウが表示されます。</p> <ol style="list-style-type: none"> ドロップダウンメニューから 脆弱性(Vulnerabilities)]または セッション(Sessions)]のどちらかを選択します。 1つ以上の項目を選択します。 回復(Recover)]をクリックします。 |

統計パネル-Web探索

次の表に、統計パネルの [Web探索(Crawl)] セクションの説明を示します。

| 項目 | 説明 |
|-----------------|---|
| ホスト(Hosts) | スキャンに含まれるホストの数。 |
| セッション(Sessions) | セッションの総数(AJAX要求、スクリプトとスクリプトフレームのインクルード、およびWSDLインクルードを除く)。 |

統計パネル-監査

次の表に、統計パネルの [監査(Audit)] セクションの説明を示します。

| 項目 | 説明 |
|---------------------|--------------------------------|
| 送信攻撃数(Attacks Sent) | 送信された攻撃の総数。 |
| 問題数(Issues) | 検出された問題の総数(すべての脆弱性とベストプラクティス)。 |

統計パネル-ネットワーク

次の表に、統計パネルの [ネットワーク(Network)] セクションの説明を示します。

| 項目 | 説明 |
|-----------------------|------------|
| 要求の総数(Total Requests) | 行われた要求の総数。 |
| 失敗要求数(Failed) | 失敗した要求の総数。 |

| 項目 | 説明 |
|--------------------------------------|---|
| Requests) | |
| スクリプトインクルード数 (Script Includes) | スクリプトインクルードの総数。 |
| マクロ要求数 (Macro Requests) | マクロ実行の一部として行われた要求の総数。 |
| 404プローブ (404 Probes) | 「ファイルが見つからない」ステータスを判断するために発行された「ファイルが見つからない」プローブの数。 |
| 404チェックリダイレクト数 (404 Check Redirects) | 404プローブがリダイレクトになった回数。 |
| 検証要求数 (Verify Requests) | 保存されたパラメータの検出のために行われた要求。 |
| ログアウト数 (Logouts) | ログアウトが検出され、ログインマクロが実行された回数。 |
| マクロ再生数 (Macro Playbacks) | マクロが実行された回数。 |
| AJAX要求数 (AJAX Requests) | 発行されたAJAX要求の総数。 |
| スクリプトイ벤트数 (Script Events) | 処理されたスクリプトイベントの総数。 |
| 送信キロバイト数 (Kilobytes Sent) | 送信されたキロバイトの総数。 |
| 受信キロバイト数 (Kilobytes Received) | 受信されたキロバイトの総数。 |

次も参照

- " [スキャン情報(Scan Info)] パネル" ページ79
- " [セッション情報(Session Info)] パネル" ページ91
- " [ホスト情報(Host Info)] パネル" ページ100

添付ファイル(Attachments) -スキャン情報(Scan Info)

「添付ファイル(Attachments)」を選択すると、スキャンに追加されたすべてのセッションのメモ、脆弱性のメモ、フォローアップ用フラグ、および脆弱性スクリーンショットの一覧が表示されます。各添付ファイルは、特定のセッションに関連付けられています。このフォームには、スキャンメモ(特定のセッションではなく、スキャン全体に適用されるメモ)も一覧表示されます。

スキャンメモを作成したり、既存の添付ファイルを編集または削除したりできます。

添付ファイルを表示するには、添付ファイルを選択して「表示(View)」をクリックします(または単に添付ファイルをダブルクリックします)。

スキャンメモを作成するには、(情報表示エリアの)「追加(Add)」メニューをクリックします。詳細については、「"情報ペイン" ページ78」を参照してください。

添付ファイルを編集するには、添付ファイルを選択して「編集(Edit)」をクリックします。スクリーンショットは編集できないことに注意してください。

これらの機能は、添付ファイルを右クリックし、ショートカットメニューからオプションを選択して使用することもできます。「セッションへ移動(Go to session)」を選択すると、「セッション情報-添付ファイル(Session Info - Attachments)」ペインが開き、その添付ファイルに関連付けられているセッションがナビゲーションペインで強調表示されます。

Fortify WebInspectユーザインターフェースの他のエリアで添付ファイルを作成するには、次のいずれかを実行します。

- ナビゲーションペインでセッションを右クリックし、ショートカットメニューから「添付ファイル(Attachments)」を選択します。詳細については、「"ナビゲーションペイン" ページ67」を参照してください。
- サマリペインの「検出事項(Findings)」タブでURLを右クリックし、ショートカットメニューから「添付ファイル(Attachments)」を選択します。詳細については、「"検出事項(Findings)タブ" ページ109」を参照してください。

Micro Focus Application Lifecycle Management (ALM)に不具合を送信すると、Fortify WebInspectによってメモが自動的にセッションに追加されます。

次も参照

- " [スキャン情報(Scan Info)] パネル" ページ79

誤検出(False Positives)

この機能は、Fortify WebInspectが脆弱性を含むものとして最初にフラグを立て、後でユーザが誤検出と判断したすべてのURLを一覧表示します。

誤検出のインポート

また、以前のスキャンで分析により誤検出として判断された脆弱性のリストをインポートすることができます。続いて、Fortify WebInspectは、以前のスキャンで検出されたこれらの誤検出を、現在のスキャンで検出された脆弱性と関連させ、新たに出現した脆弱性に誤検出のフラグを設定します。

たとえば、クロスサイトスクリプティングの脆弱性がスキャン番号1でURL <http://www.mysite.com/foo/bar>に検出され、さらに分析を行った後、いずれかのユーザがそれに誤検出のフラグを立てたとします。スキャン番号1の誤検出を www.mysite.comのスキャン番号2にインポートした場合に、2番目のスキャンで同じURL (<http://www.mysite.com/foo/bar>)でクロスサイトスクリプティングの脆弱性が検出されると、Fortify WebInspectは自動的にその脆弱性を誤検出に変更します。

非アクティブ/アクティブの誤検出リスト

インポートされた誤検出は、「非アクティブな誤検出 (Inactive False Positives)」というラベルのリストに最初にロードされます。そのリスト内の誤検出が現在のスキャンの脆弱性と一致する場合、その項目は「非アクティブな誤検出 (Inactive False Positives)」リストから「アクティブな誤検出 (Active False Positives)」リストに移動されます。一致しない項目は、「非アクティブな誤検出 (Inactive False Positives)」リストに残ります。

誤検出のロード

他のスキャンからの誤検出をいつでも現在のスキャンに手動でロードできます。または、スキャンの開始中に、特定のファイルから誤検出をロードするようにスキャンウィザードに指示することができます。この場合、Fortify WebInspectは、スキャン中に誤検出が検出されるとその誤検出を関連させます。スキャンの実行中に一致した誤検出を(スキャンダッシュボードで)確認することもできます。

誤検出の操作

1. 「スキャン情報 (Scan Info)」パネルから「誤検出 (False Positives)」を選択します。
2. 必要に応じて、脆弱性の説明の横にあるプラス記号 $+$ をクリックして、関連付けられているURLと状態を表示します。
3. URLをクリックすると、ユーザが脆弱性を削除した際に入力された可能性のあるコメントが(情報ペインの下部)に表示されます。
4. 他のスキャンから誤検出をインポートするには、「誤検出のインポート (Import False Positives)」をクリックします。
5. 誤検出を脆弱性に戻す場合は、「アクティブな誤検出 (Active False Positive)」リストから項目を選択し、「脆弱性としてマーク (Mark as Vulnerability)」をクリックします。
6. 「非アクティブな誤検出 (Inactive False Positive)」リストから項目を削除するには、項目を選択して「非アクティブから削除 (Remove From Inactive)」をクリックします。
7. 誤検出に関連付けられたコメントを編集するには、項目を選択して「コメントの編集 (Edit Comment)」をクリックします。

脆弱性を誤検出として指定する方法については、「"ナビゲーションペインのショートカットメニュー" ページ76」または「"検出事項(Findings)】タブ" ページ109」を参照してください。

Fortify WebInspectウィンドウの詳細については、「"WebInspectユーザインターフェース" ページ51」を参照してください。

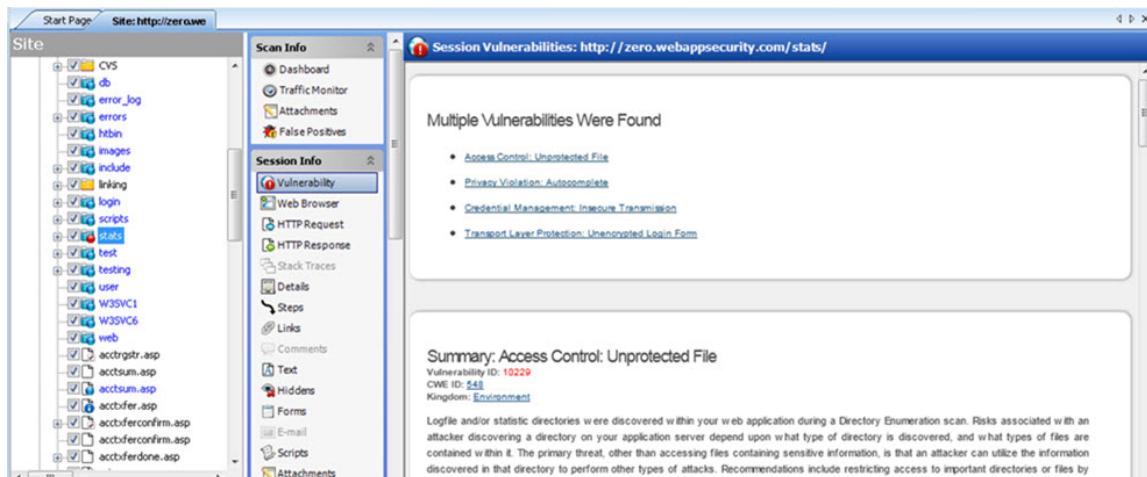
【セッション情報(Session Info)】パネル

Fortify WebInspectでは、ナビゲーションペインの【サイト(Site)】ビューまたは【シーケンス(Sequence)】ビューを使用して、スキャンで作成された各セッションがリストされます。セッションを選択し、【セッション情報(Session Info)】パネルでオプションを1つクリックして、そのセッションに関する関連情報を表示します。

次のスキャンの例では、Fortify WebInspectがHTTP要求 GET /stats/stats.html HTTP/1.1を送信しています。

脆弱性を表示するには:

1. ナビゲーションペインで【Stats.html】を選択します。
2. 【セッション情報(Session Info)】パネルで、【脆弱性(Vulnerability)】をクリックします。



選択可能なオプション

次の表に、【セッション情報(Session Info)】パネルで使用可能なオプションを一覧にします。一部のオプションは、特定のスキャン(基本スキャンまたはWebサービススキャン)でのみ表示されます。また、選択されているセッションに関するオプションのみが有効になります。たとえば、セッションにフォームが含まれていない場合には【フォーム(Forms)】は選択できません。

| オプション | 説明 |
|--------------------|--------------------------------------|
| 脆弱性(Vulnerability) | ナビゲーションペインで選択されているセッションの脆弱性情報を表示します。 |
| Webブラウザ | ナビゲーションペインで選択されているセッションで、Webブラウザによって |

| オプション | 説明 |
|----------------------------|---|
| (Web Browser) ¹ | レンダリングされたサーバ応答を表示します。 |
| HTTP要求 (HTTP Request) | Fortify WebInspectから、スキャン対象のサイトをホストするサーバに送信された生HTTP要求を表示します。 |
| HTTP応答 (HTTP Response) | Fortify WebInspectの要求に対するサーバの生HTTP応答を表示します。 応答に1つ以上の攻撃署名(脆弱性が検出されたことを示す)が含まれている場合は、次のいずれかのボタンをクリックして攻撃署名を切り替えることができます。  |
| | Flash (.swf)ファイルを選択した場合、Fortify WebInspectはバイナリデータの代わりにHTMLを表示します。これにより、Fortify WebInspectは読み取り可能なフォーマットでリンクを表示できます。 |
| スタックトレース (Stack Traces) | この機能は、Fortify WebInspect Agentがターゲットサーバにインストールされ、実行されているときにこのエージェントをサポートするように設計されています。 特定のチェック(SQLインジェクション、コマンド実行、クロスサイトスクリプティングなど)の場合、Fortify WebInspect AgentはFortify WebInspect HTTP要求を傍受し、ターゲットモジュールでランタイム分析を実行します。この分析によって脆弱性が存在することが確認されると、Fortify WebInspect AgentはHTTP応答にスタックトレースを追加します。開発者は、このスタックトレースを分析して、改善が必要なエリアを調査できます。 |
| 詳細(Details) ¹ | 要求および応答の詳細(応答のサイズや要求のメソッドなど)を一覧にします。[応答(Response)]セクションには、コンテンツタイプの2つのエンティ、つまり返されるものと検出されたものが含まれていることに注意してください。[返されるコンテンツタイプ(Returned Content Type)]は、HTTP応答のContent-Typeエンティティヘッダーフィールドで指定されたメディアタイプを示します。[検出されたコンテンツタイプ(Detected Content Type)]は、Fortify WebInspectによって判別された実際のコンテンツタイプを示します。 |
| ステップ(Steps) ¹ | ナビゲーションペインで選択されているセッションまたはサマリペインで選択されているURLに到達するためにFortify WebInspectがたどったルートを表示します。親セッション(リストの一番上)から始まり、それ以降にア |

| オプション | 説明 |
|-----------------------------|---|
| | クセスしたURLが順番に表示され、スキャン方法に関する詳細が提供されます。 |
| リンク(Links) ¹ | このオプションでは、選択したリソースへのリンクを含むターゲットサイトのすべてのリソースが(「リンク元(Linked From)」の下に)一覧表示されます。リンクは、HTMLタグ、スクリプト、またはHTMLフォームによってレンダリングできます。また、選択したセッションのHTTP応答内のリンクによって参照されるすべてのリソースも(「リンク先(Linked To)」の下に)一覧表示されます。 |
| コメント(Comments) ¹ | HTTP応答に埋め込まれているすべてのコメントを(HTML形式で)表示します。 |
| テキスト(Text) ¹ | ナビゲーションペインで選択されているセッションのHTTP応答に含まれるすべてのテキストを表示します。 |
| 非表示(Hiddens) ¹ | コントロールタイプが「hidden」の各入力要素の名前属性を表示します。 |
| フォーム(Forms) ¹ | ブラウザがフォームをレンダリングするために解釈するHTMLを表示します。 |
| 電子メール(E-mail) ¹ | 応答に含まれるすべての電子メールアドレスを表示します。 |
| スクリプト(Scripts) ¹ | サーバ応答に埋め込まれているクライアントサイドのスクリプトをすべて表示します。 |
| 添付ファイル(Attachments) | <p>選択されているオブジェクトに関連付けられているすべてのメモ、フラグ、およびスクリーンショットを表示します。</p> <p>添付ファイルを作成するには、次のいずれかを実行できます。</p> <ul style="list-style-type: none"> ナビゲーションペインでセッション(基本またはガイド付きスキャン)、操作、または脆弱性(Webサービススキャン)を右クリックし、ショートカットメニューから「添付ファイル(Attachments)」を選択します。 サマリペインの「検出事項(Findings)」タブでURLを右クリックし、ショートカットメニューから「添付ファイル(Attachments)」を選択します。 ナビゲーションペインでセッション(基本スキャン)、操作、または脆弱性(Webサービススキャン)を選択し、「セッション情報(Session Info)」パネルから「添付ファイル(Attachments)」を選択し、(情報ペインの)「追加(Add)」メニューをクリックします。 |

| オプション | 説明 |
|--|---|
| | Micro Focus Application Lifecycle Management (ALM)に問題を送信するたびに、Fortify WebInspectによってメモがセッション情報に自動的に追加されます。 |
| 攻撃情報 (Attack Info) ¹ | 攻撃シーケンス番号、URL、使用されている監査エンジンの名前、および脆弱性テストの結果が表示されます。攻撃情報は、通常、攻撃が検出されたセッションではなく、攻撃が作成されたセッションに関連付けられます。選択された脆弱なセッションに関する攻撃情報が表示されない場合は、親セッションを選択してから、[攻撃情報(Attack Info)]をクリックします。 |
| XML要求(XML Request) ² | 要求に埋め込まれているSOAPエンベロープが表示されます(Webサービススキャンで操作を選択した場合に使用可能)。 |
| XML応答(XML Response) ² | 応答に埋め込まれているSOAPエンベロープが表示されます(Webサービススキャンで操作を選択した場合に使用可能)。 |
| Webサービス要求(Web Service Request) ² | 要求に埋め込まれているWebサービススキーマと値が表示されます(Webサービススキャンで操作を選択した場合に使用可能)。 |
| Webサービス応答(Web Service Response) ² | 応答に埋め込まれているWebサービススキーマと値が表示されます(Webサービススキャンで操作を選択した場合に使用可能)。 |

¹基本スキャンまたはガイド付きスキャンのみ

² Webサービススキャンのみ

ほとんどのオプションでは、情報ペイン上部に検索機能が表示され、指定するテキストを検索できます。正規表現を使用して検索を実行するには、[正規表現(Regex)]ボタンを選択してから [検索(Find)]をクリックします。

ヒント: 脆弱性情報を表示する際にリンクをたどる場合、ナビゲーションペインで強調表示されたセッションをクリックすると戻ることができます。

次も参照

["WebInspectユーザインターフェース" ページ51](#)

["ホスト情報\(Host Info\)"\]パネル" ページ100](#)

["ナビゲーションペイン" ページ67](#)

["スキャン情報\(Scan Info\)"\]パネル" ページ79](#)

["サマリペイン" ページ109](#)

["正規表現" ページ323](#)

脆弱性 (Vulnerability)

このオプションを選択すると、ナビゲーションペインで選択したセッション、またはサマリペインで選択した脆弱性の脆弱性情報が表示されます。通常、脆弱性の説明、脆弱性ID、CWE (Common Weakness Enumeration) ID、界、影響(この脆弱性による影響)、および脆弱性の修復方法に関する指示が含まれます。

Webブラウザ (Web Browser)

このオプションを選択すると、ナビゲーションペインで選択したセッションのサーバ応答が、Webブラウザによってレンダリングされる形で表示されます。

HTTP要求 (HTTP Request)

このオプションを選択すると、Fortify WebInspectによってスキャン中のサイトのホストサーバに送信された(ナビゲーションペインで選択したセッションに関する)生のHTTP要求が表示されます。

要求で強調表示されるテキスト

HTTP要求で、Fortify WebInspectは次のようにテキストを強調表示します。

- 黄色の強調表示は、GET、POST、またはPUTステータス行とクッキーヘッダを示します。
- 赤色の強調表示は、攻撃ペイロードと脆弱性(検出された場合)を示します。

HTTP応答 (HTTP Response)

このオプションは、ナビゲーションペインで選択したセッションに関する、Fortify WebInspectの要求に対するサーバの生のHTTP応答を表示します。

応答に1つ以上の攻撃署名(脆弱性が検出されたことを示す)が含まれている場合は、次のいずれかのボタンをクリックして攻撃署名を切り替えることができます。



Flash (.swf)ファイルを選択した場合、Fortify WebInspectはバイナリデータの代わりにHTMLを表示します。これにより、Fortify WebInspectは読み取り可能なフォーマットでリンクを表示できます。

応答で強調表示されるテキスト

HTTP応答で、Fortify WebInspectは赤色の強調表示を使用して、検出された脆弱性を示します。

スタックトレース(Stack Traces)

この機能は、Fortify WebInspect Agentがターゲットサーバにインストールされ、実行されているときにこのエージェントをサポートするように設計されています。

特定のチェック(SQLインジェクション、コマンド実行、クロスサイトスクリプティングなど)の場合、Fortify WebInspect AgentはFortify WebInspect HTTP要求を傍受し、ターゲットモジュールでランタイム分析を実行します。この分析によって脆弱性が存在することが確認されると、Fortify WebInspect AgentはHTTP応答にスタックトレースを追加します。開発者は、このスタックトレースを分析して、改善が必要なエリアを調査できます。

詳細(Details)

このオプションは、ナビゲーションペインで選択したセッションの要求と応答の詳細(応答のサイズや要求メソッドなど)を一覧表示します。

【応答(Response)】セクションには、コンテンツタイプの2つのエントリ、つまり返されたものと検出されたものが含まれていることに注意してください。【返されるコンテンツタイプ(Returned Content Type)】は、HTTP応答のContent-Typeエンティティヘッダーフィールドで指定されたメディアタイプを示します。【検出されたコンテンツタイプ(Detected Content Type)】は、Fortify WebInspectによって判別された実際のコンテンツタイプを示します。

ステップ(Steps)

このオプションを選択すると、ナビゲーションペインで選択したセッションまたはサマリペインで選択したURLに到達するために、Fortify WebInspectがたどったルートが表示されます。親セッション(リストの一番上)から始まり、それ以降にアクセスしたURLが順番に表示され、スキャン方法に関する詳細が提供されます。

リンク(Links)

このオプションでは、選択したリソースへのリンクを含むターゲットサイトのすべてのリソースが(【リンク元(Linked From)】の下に)一覧表示されます。リンクは、HTMLタグ、スクリプト、またはHTMLフォームによってレンダリングできます。

また、選択したセッションのHTTP応答内のリンクによって参照されるすべてのリソースも(【リンク先(Linked To)】の下に)一覧表示されます。

表示されているリンクをダブルクリックすると、ナビゲーションペインのフォーカスが、参照されているセッションに移動します。または、Webブラウザでセッションを表示することにより、リンクされたリソースを参照することもできます(【Webブラウザ(Web Browser)】をクリック)。詳細については、「["ナビゲーションペイン" ページ67](#)」を参照してください。

コメント(Comments): セッション情報(Session Info)

このオプションは、ナビゲーションペインで選択されたセッションのHTTP応答に埋め込まれたすべてのコメントを表示します。

開発者が、サイトのセキュリティを侵害するために使用可能な重要な情報をコメントに残す場合があります。たとえば、テーブル内のフィールドの必須の順序についてのコメント、といった一見無害な情報が、サイトのセキュリティを侵害するのに必要となる重大な情報を攻撃者に与えてしまうことがあります。

情報ペインの最上部にある **検索(Search)**]機能を使用して、指定したテキストを探します。正規表現を使用して検索を実行するには、**正規表現(Regex)**]ボタンを選択してから **検索(Find)**]をクリックします。

コメントをクリップボードにコピーするには、テキストを強調表示して、ショートカットメニューから **コピー(Copy)**]を選択します。

テキスト(Text)

このオプションは、ナビゲーションペインで選択されているセッションのHTTP応答に含まれるすべてのテキストを表示します。詳細については、「["ナビゲーションペイン" ページ67](#)」を参照してください。

非表示(Hiddens): セッション情報(Session Info)

Fortify WebInspectは、すべてのフォームを分析し、「非表示」タイプのすべてのコントロール(レンダリングされていないが、フォームで送信される値を持つコントロール)を一覧表示します。しばしば開発者は非表示のコントロールにパラメータを含めますが、攻撃者がこれを編集して再送信する可能性があります。

情報ペインの最上部にある **検索(Search)**]機能を使用して、指定したテキストを探します。正規表現を使用して検索を実行するには、**正規表現(Regex)**]ボタンを選択してから **検索(Find)**]をクリックします。

HTMLテキストをクリップボードにコピーするには、テキストを強調表示して、ショートカットメニューから **コピー(Copy)**]を選択します。

フォーム(Forms): セッション情報(Session Info)

Fortify WebInspectは、ナビゲーションペインで選択されたセッションに対して検出されたすべてのHTMLフォームを一覧表示します。

情報ペインの最上部にある **検索(Search)**]機能を使用して、指定したテキストを探します。正規表現を使用して検索を実行するには、**正規表現(Regex)**]ボタンを選択してから **検索(Find)**]をクリックします。

フォームをクリップボードにコピーするには、テキストを強調表示して、ショートカットメニューから **コピー(Copy)**]を選択します。

Fortify WebInspectウィンドウの詳細については、「["WebInspectユーザインターフェース" ページ51](#)」を参照してください。

電子メール(E-Mail)

Fortify WebInspectは、ナビゲーションペインから選択されたセッションに含まれるすべての電子メールアドレスを一覧表示します。

情報ペインの最上部にある [検索(Search)] 機能を使用して、指定したテキストを探します。正規表現を使用して検索を実行するには、[正規表現(Regex)] ボタンを選択してから [検索(Find)] をクリックします。

電子メールアドレスをクリップボードにコピーするには、テキストを強調表示して、ショートカットメニューから [コピー(Copy)] を選択します。

スクリプト (Scripts) - セッション情報 (Session Info)

Fortify WebInspectは、セッションで検出されたスクリプトをすべて一覧表示します。

情報ペインの最上部にある [検索(Search)] 機能を使用して、指定したテキストを探します。正規表現を使用して検索を実行するには、[正規表現(Regex)] ボタンを選択してから [検索(Find)] をクリックします。詳細については、「["正規表現" ページ323](#)」を参照してください。

スクリプトをクリップボードにコピーするには、テキストを強調表示して、ショートカットメニューから [コピー(Copy)] を選択します。

Fortify WebInspect ウィンドウの詳細については、「["WebInspectユーザインターフェース" ページ51](#)」を参照してください。

添付ファイル(Attachments) - セッション情報 (Session Info)

次の添付ファイルをセッションに関連付けることができます。

- セッションのメモ
- フォローアップ用 フラグセッション
- 脆弱性のメモ
- 脆弱性のスクリーンショット

メモ: メモをスキャンに関連付け、[スキャン情報(Scan Info)] パネルで [添付ファイル(Attachments)] を選択して、そのスキャンに追加されたすべての添付ファイルを表示することもできます。

[添付ファイル(Attachments)] を選択すると、選択したセッションに関連付けられているすべてのメモ、フラグ、およびスクリーンショットの一覧が表示されます。

添付ファイルの表示

添付ファイルを表示するには:

- 添付ファイルを選択して [表示(View)] をクリックします(または単に添付ファイルをダブルクリックします)。

セッションの添付ファイルの追加

セッションの添付ファイルを追加するには:

- 次のいずれかを実行してセッションを選択します。
 - サマリペインの [検出事項(Findings)] タブで、脆弱なURLを右クリックします。詳細については、「"検出事項(Findings)タブ" ページ109」を参照してください。
 - ナビゲーションペインで、セッションまたはURLを右クリックします。詳細については、「"ナビゲーションペイン" ページ67」を参照してください。
- ショートカットメニューで [添付ファイル(Attachments)] をクリックし、添付ファイルの種類を選択します。

メモ: 別の方法として、ナビゲーションペインでセッションを選択し、[セッション情報(Session Info)] パネルで [添付ファイル(Attachments)] をクリックし、(情報表示エリア内の) [追加(Add)] メニューからコマンドを選択します。詳細については、「"情報ペイン" ページ78」を参照してください。

- 選択した添付ファイルの種類に関連するコメントを入力します。
- 1つ以上の脆弱性の横にあるチェックボックスをオンにします。
- [脆弱性スクリーンショット(Vulnerability Screenshot)] を選択した場合:
 - [名前(Name)] ボックスにスクリーンショットの名前を入力します。最大長は、40文字です。
 - [参照(Browse)] ボタン [...] をクリックしてグラフィックファイルを見つけるか、イメージをメモリにキャプチャした場合は、[クリップボードからコピー(Copy from Clipboard)] をクリックします。
- [OK] をクリックします。

添付ファイルの編集

添付ファイルを編集するには:

- 次のいずれかを実行します。
 - スキャンに追加された添付ファイルをすべて表示するには、[スキャン情報(Scan Info)] パネルで [添付ファイル(Attachments)] をクリックします。
 - 特定のセッションに追加された添付ファイルのみを表示するには、[セッション情報(Session Info)] パネルで [添付ファイル(Attachments)] をクリックし、ナビゲーションペインでセッションをクリックします。サマリペインでURLを選択することもできます。
- 添付ファイルを選択し、[編集(Edit)] をクリックします。
- 必要に応じてコメントを変更します。

メモ: スクリーンショットの添付ファイルは編集できません。

- [OK] をクリックします。

ヒント: 追加、編集、表示、および削除機能は、情報表示エリア内の添付ファイルを右クリックし、ショートカットメニューからオプションを選択して使用することもできます。

攻撃情報(Attack Info)

このオプションを使用すると、ナビゲーションペインで選択されたセッションに関して、攻撃シーケンス番号、URL、使用されている監査エンジンの名前、および脆弱性テストの結果が表示されます。

攻撃情報は、通常、攻撃が検出されたセッションではなく、攻撃が作成されたセッションに関連付けられます。選択された脆弱なセッションに関する攻撃情報が表示されない場合は、親セッションを選択してから、**攻撃情報(Attack Info)**]をクリックします。

Webサービス要求(Web Service Request)

このオプションを選択すると、要求に埋め込まれているWebサービススキーマと値が表示されます(Webサービススキャンで操作を選択した場合に使用可能)。Webサービススキャン中にのみ使用できます。

Webサービス応答(Web Service Response)

このオプションを選択すると、応答に埋め込まれているWebサービススキーマと値が表示されます(Webサービススキャンで操作を選択した場合に使用可能)。Webサービススキャン中にのみ使用できます。

XML要求(XML Request)

このオプションを選択すると、選択した要求に埋め込まれている関連XMLスキーマが表示されます(WebサービススキャンでWSDLオブジェクトを選択した場合に使用可能)。

XML応答(XML Response)

このオプションを選択すると、ナビゲーションペインで選択したセッションの応答に埋め込まれている関連XMLスキーマが表示されます(WebサービススキャンでWSDLオブジェクトを選択した場合に使用可能)。

[ホスト情報(Host Info)]パネル

この折りたたみ可能なパネルに一覧表示されている項目をクリックすると、サイト(またはホスト)のWeb探索または監査中に検出されたその項目タイプのすべてのインスタンスがFortify WebInspectに表示されます。

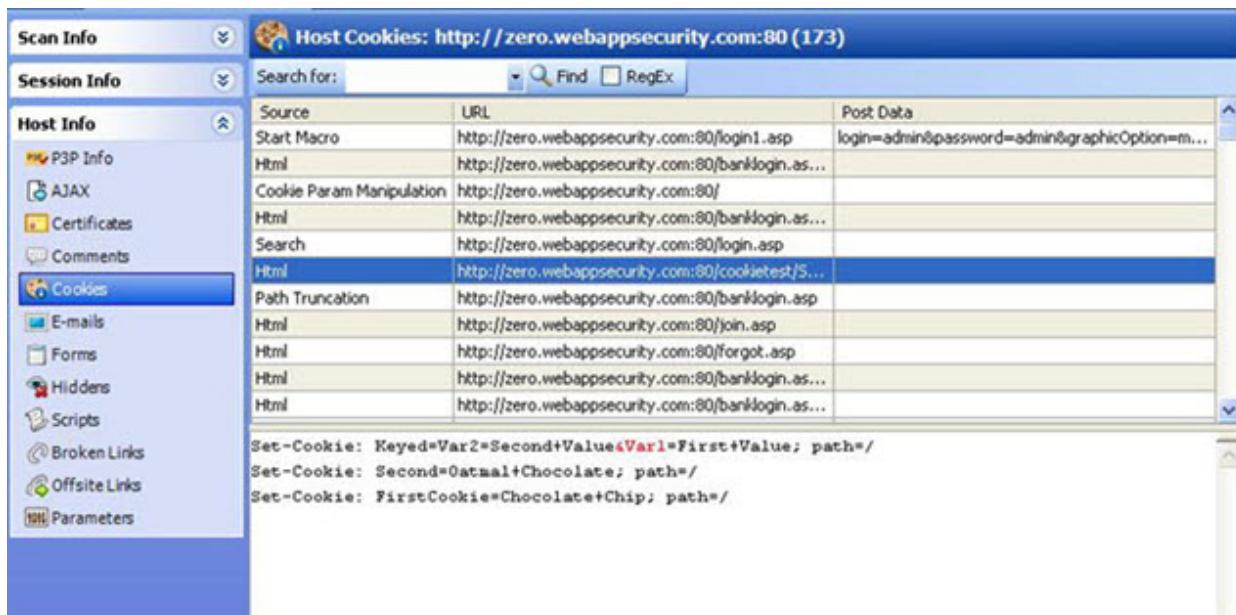
項目をダブルクリックすると、その項目を含むセッションがナビゲーションペインで強調表示されます。項目(電子メールアドレスなど)をクリップボードにコピーするには、テキストを強調表示して、ショートカットメニューから**コピー(Copy)**]を選択します。

ほとんどの場合、情報ペインの最上部にある [検索(Search)]機能を使用して、指定したテキストを探します。正規表現を使用して検索を実行するには、[正規表現(Regex)]ボタンを選択してから [検索(Find)]をクリックします。

メモ: Webサービススキャンを実行している場合、[ホスト情報(Host Info)]パネルは表示されません。

次の図で、[クッキー(Cookies)]を選択すると、クッキーが検出されたすべてのセッションのリストが表示されます。リストから項目を選択すると、選択したセッションに関連付けられたクッキーがFortify WebInspectに表示されます。

[ホスト情報(Host Info)]パネルのイメージ



選択可能なオプション

[ホスト情報(Host Info)]オプションについて、次の表で説明します。

| オプション | 説明 |
|-------------------|--|
| P3P情報(P3P Info) | P3P (Platform for Privacy Preferences Project)情報を表示します。詳細については、「 "P3P情報(P3P Info)" 次のページ 」を参照してください。 |
| AJAX | AJAXエンジンとAJAX要求を含むすべてのページのリストを表示します。詳細については、「 "AJAX" ページ103 」を参照してください。 |
| 証明書(Certificates) | サイトに関連付けられているすべての証明書のリストを表示します。詳細については、「 "証明書(Certificates)" ページ104 」を参照してください。 |

| オプション | 説明 |
|--------------------------|---|
| コメント (Comments) | コメントを含むすべてのURLのリストを表示します。詳細については、「 "コメント(Comments) -ホスト情報(Host Info)" ページ104 」を参照してください。 |
| クッキー (Cookies) | クッキーを含むすべてのURLのリストを表示します。詳細については、「 "クッキー(Cookies)" ページ105 」を参照してください。 |
| 電子メール(E-Mails) | 応答に電子メールアドレスを含むすべてのURLのリストを表示します。詳細については、「 "電子メール(E-Mails) -ホスト情報(Host Info)" ページ105 」を参照してください。 |
| フォーム(Forms) | フォームを含むすべてのURLのリストを表示します。詳細については、「 "フォーム(Forms) -ホスト情報(Host Info)" ページ106 」を参照してください。 |
| 非表示 (Hiddens) | コントロールタイプが「hidden」の入力要素を含むすべてのURLのリストを表示します。詳細については、「 "非表示(Hiddens) -ホスト情報(Host Info)" ページ106 」を参照してください。 |
| スクリプト | サーバの応答に埋め込まれるクライアントサイドスクリプトを含むすべてのURLのリストを表示します。詳細については、「 "スクリプト(Scripts) -ホスト情報(Host Info)" ページ107 」を参照してください。 |
| 壊れたリンク (Broken Links) | 存在しないターゲットへのハイパーリンクを含むすべてのURLのリストを表示します。詳細については、「 "壊れたリンク(Broken Links)" ページ107 」を参照してください。 |
| サイト外リンク | 他のサイトへのハイパーリンクを含むすべてのURLのリストを表示します。詳細については、「 "サイト外リンク" ページ108 」を参照してください。 |
| パラメータ (Parameters) | 埋め込みパラメータを含むすべてのURLのリストを表示します。詳細については、「 "パラメータ(Parameters)" ページ108 」を参照してください。 |

P3P情報 (P3P Info)

このオプションには、P3P (Platform for Privacy Preferences Project)情報が表示されます。

World Wide Web ConsortiumのP3Pにより、Webサイトで、ユーザエージェントが自動的に取得して簡単に解釈可能な標準形式でプライバシープラクティスを表現できます。P3Pユーザエージェントを使用すると、ユーザはサイトプラクティスを(マシンと人の両方が読み取り可能な形式で)受信したり、必要に応じてこれらのプラクティスに基づいて意思決定を自動化したりすることができます。そのため、ユーザは、アクセスする各サイトでプライバシーポリシーを読む必要がありません。

P3P準拠のWebサイトでは、収集する情報の種類とその情報の使用方法がポリシーで宣言されます。P3P対応のWebブラウザでは、このポリシーをユーザの保存された環境設定と比較することで、実行する操作を決定できます。たとえば、ユーザは自身の閲覧習慣に関する情報が収集されないようにブラウザの環境設定を行うことができます。この目的でクッキーを使用することがポリシーに記載されているWebサイトにユーザがアクセスすると、ブラウザによってクッキーが自動的に拒否されます。

P3Pユーザエージェント

Microsoft Internet Explorer 6では、P3Pプライバシーポリシーを表示し、P3Pポリシーを独自の設定と比較して、特定のサイトからのクッキーを許可するかどうかを決定できます。

<http://www.privacybird.com/>で入手できるPrivacy Bird(元はAT&Tが開発)は、完全な機能を備えたP3Pユーザエージェントであり、ユーザがアクセスする各Webサイトで自動的にプライバシーポリシーの検索を行います。次いで、ポリシーと、保存されているユーザのプライバシー環境設定とを比較し、矛盾が発生した場合はユーザに通知します。

次も参照

["ホスト情報\(Host Info\)"\]パネル" ページ100](#)

AJAX

AJAXは、Asynchronous JavaScript and XMLHttpRequestの頭字語です。

このオプションを選択すると、Fortify WebInspectには、AJAXエンジンとAJAX要求を含むすべてのページが表示されます。

| Type | URL |
|-----------|---|
| AJAX Page | http://officerdoofy:80/SampleWebSite/AlwaysVisibleControl/AlwaysVisibleControl.aspx |
| AJAX Page | http://officerdoofy:80/SampleWebSite/HoverMenu/HoverMenu.aspx |
| AJAX Page | http://officerdoofy:80/SampleWebSite/NumericUpDown/NumericUpDown.aspx |
| AJAX Page | http://officerdoofy:80/SampleWebSite/PopupControl/PopupControl.aspx |
| AJAX Page | http://officerdoofy:80/SampleWebSite/Rating/Rating.aspx |
| AJAX Page | http://officerdoofy:80/SampleWebSite/ReorderList/ReorderList.aspx |
| AJAX Page | http://officerdoofy:80/SampleWebSite/TextBoxWatermark/TextBoxWatermark.aspx |
| AJAX Page | http://officerdoofy:80/SampleWebSite/ToggleButton/ToggleButton.aspx |
| AJAX Page | http://officerdoofy:80/SampleWebSite/UpdatePanelAnimation/UpdatePanelAnimation.aspx |
| AJAX Page | http://officerdoofy:80/SampleWebSite/ValidatorCallout/ValidatorCallout.aspx |
| AJAX Page | http://officerdoofy:80/SampleWebSite/AlwaysVisibleControl/AlwaysVisibleControl.aspx |
| AJAX Page | http://officerdoofy:80/SampleWebSite/CascadingDropDown/CascadingDropDown.aspx |
| AJAX Page | http://officerdoofy:80/SampleWebSite/ConfirmButton/ConfirmButton.aspx |
| AJAX Page | http://officerdoofy:80/SampleWebSite/DiminDimin/DiminDimin.aspx |

This page uses AJAX in script

このビューには、2種類のAJAX行項目があります。

- AJAXページ(上の図を参照)
- 要求

リスト内の項目をクリックすると、Fortify WebInspectに、「This page uses AJAX in script」と表示される(ページタイプの場合)か、クエリおよび/またはPOSTデータパラメータが一覧表示されます(要求タイプの場合)。

AJAXの動作

AJAXは、それ単体の技術ではなく、HTMLまたはXHTML、カスケーディングスタイルシート、JavaScript、ドキュメントオブジェクトモデル、XML、XSLT、XMLHttpRequestオブジェクトなどの既存の技術の組み合わせです。これらの技術をAJAXモデルで組み合わせると、Webアプリケーションはブラウザページ全体を再ロードせずに、ユーザインターフェースを迅速かつインクリメンタルに更新できます。

ブラウザは、セッションの最初にWebページをロードする代わりに、AJAXエンジンをロードします。これはユーザインターフェースのレンダリングとサーバとの通信の両方を担当します。通常ならHTTP要求が生成されるはずの各ユーザアクションは、代わりにAJAXエンジンに対するJavaScript呼び出しの形を取ります。サーバとの通信を必要としないユーザアクション(たとえば、単純なデータ検証、メモリ内のデータの編集、および一部のナビゲーションさえ)への応答は、エンジンによって処理されます。エンジンがサーバと通信する必要がある場合(処理用のデータの送信、追加のインターフェースコードのロード、または新しいデータの取得)、エンジンによってこれらの要求が非同期に、通常はXMLを使用して発行されます。ユーザとアプリケーションのやり取りが停止することはありません。

証明書(Certificates)

証明書は、特定のWebサイトが安全であり、本物であると明言します。これにより、他のどのWebサイトも元の安全なサイトを偽ることができなくなります。セキュリティ証明書によって識別情報が公開鍵に関連付けられます。証明書の所有者だけが、対応する秘密鍵を知っています。これにより、所有者は「デジタル署名」を作成したり、対応する公開鍵で暗号化された情報を復号化したりすることができます。

コメント(Comments) - ホスト情報(Host Info)

開発者が、サイトのセキュリティを侵害するために使用可能な重要な情報をコメントに残す場合があります。たとえば、テーブル内のフィールドの必須の順序についてのコメント、といった一見無害な情報が、サイトのセキュリティを侵害するのに必要となる重大な情報を攻撃者に与えてしまうことがあります。

検出されたコメントを表示するには:

1. [ホスト情報(Host Info)]パネルから [コメント(Comments)]を選択し、コメントが含まれているすべてのURLを一覧にします。
2. [URL]をクリックして、そのURLに含まれるコメントを表示します。
3. エントリをダブルクリックして、コメントを含むセッションをナビゲーションペインで探します。

フォーカスが、[セッション情報(Session Info)]パネルの[コメント(Comments)]選択肢に切り替わります。

情報ペインの最上部にある[検索(Search)]機能を使用して、指定したテキストを探します。正規表現を使用して検索を実行するには、[正規表現(Regex)]ボタンを選択してから[検索(Find)]をクリックします。

コメントをクリップボードにコピーするには、テキストを強調表示して、ショートカットメニューから[コピー(Copy)]を選択します。

URLをダブルクリックすると、そのURLを含むセッションがナビゲーションペインで強調表示されます。

クッキー(Cookies)

クッキーには、後で使用するためにサーバによってクライアント上に保存された情報(ユーザの優先設定や設定情報など)が含まれています。クッキーには基本形式が2種類あります。個別のファイルと、1つの連続ファイル内のレコードです。たいてい複数のセットが存在します。これは、異なる場所に複数のブラウザがインストールされていることの結果です。多くの場合、「忘れられた」クッキーには、他人に見られたくない暴露情報が含まれています。

検出されたクッキーを表示するには:

1. [ホスト情報(Host Info)]パネルから[クッキー(Cookies)]を選択し、Web探索または監査中にクッキーが検出されたすべてのURLを一覧表示します。
2. URLをクリックして、そのURLに含まれるクッキーを表示します。
3. エントリをダブルクリックして、クッキーを含むセッションをナビゲーションペインで探します。

情報ペインの最上部にある[検索(Search)]機能を使用して、指定したテキストを探します。正規表現を使用して検索を実行するには、[正規表現(Regex)]ボタンを選択してから[検索(Find)]をクリックします。

クッキーをクリップボードにコピーするには、テキストを強調表示して、ショートカットメニューから[コピー(Copy)]を選択します。

URLをダブルクリックすると、そのURLを含むセッションがナビゲーションペインで強調表示されます。

電子メール(E-Mails) - ホスト情報(Host Info)

Fortify WebInspectは、スキャン中に検出された電子メールアドレスをすべて一覧表示します。電子メールアドレスを表示するには:

1. [ホスト情報(Host Info)]パネルから[電子メール(E-mail)]を選択し、電子メールアドレスを含むすべてのURLを一覧表示します。
2. URLをクリックすると、そのURLに含まれる電子メールアドレスが表示されます。
3. エントリをダブルクリックして、電子メールアドレスを含むセッションをナビゲーションペインで探します。

します。[セッション情報(Session Info)]パネルの[電子メール(E-mail)]選択項目にフォーカスが切り替わります。

情報ペインの最上部にある[検索(Search)]機能を使用して、指定したテキストを探します。正規表現を使用して検索を実行するには、[正規表現(Regex)]ボタンを選択してから[検索(Find)]をクリックします。

電子メールアドレスをクリップボードにコピーするには、テキストを強調表示して、ショートカットメニューから[コピー(Copy)]を選択します。

URLをダブルクリックすると、そのURLを含むセッションがナビゲーションペインで強調表示されます。

フォーム(Forms) - ホスト情報(Host Info)

Fortify WebInspectは、スキャン中に検出されたHTMLフォームをすべて一覧表示します。

1. [ホスト情報(Host Info)]パネルから[フォーム(Forms)]を選択し、フォームが含まれているすべてのURLを一覧表示します。
2. URLをクリックすると、そのURLに含まれるフォームのソースHTMLが表示されます。
3. エントリをダブルクリックして、フォームを含むセッションをナビゲーションペインで探します。
[セッション情報(Session Info)]パネルの[フォーム(Forms)]選択項目にフォーカスが切り替わります。

情報ペインの最上部にある[検索(Search)]機能を使用して、指定したテキストを探します。正規表現を使用して検索を実行するには、[正規表現(Regex)]ボタンを選択してから[検索(Find)]をクリックします。

フォームをクリップボードにコピーするには、テキストを強調表示して、ショートカットメニューから[コピー(Copy)]を選択します。

URLをダブルクリックすると、そのURLを含むセッションがナビゲーションペインで強調表示されます。

非表示(Hiddens) - ホスト情報(Host Info)

Fortify WebInspectは、すべてのフォームを分析し、「非表示」タイプのすべてのコントロール(レンダリングされていないが、フォームで送信される値を持つコントロール)を一覧表示します。しばしば開発者は非表示のコントロールにパラメータを含めますが、攻撃者がこれを編集して再送信する可能性があります。

1. [ホスト情報(Host Info)]パネルから[非表示(Hiddens)]を選択し、非表示のコントロールを含むすべてのURLを一覧表示します。
2. URLをクリックすると、そのURLに含まれる「非表示」のコントロールの名前と値の属性が表示されます。
3. エントリをダブルクリックして、非表示のコントロールを含むセッションをナビゲーションペインで探します。
[セッション情報(Session Info)]パネルの[非表示(Hiddens)]選択項目にフォーカスが切り替わります。

情報ペインの最上部にある **検索(Search)**]機能を使用して、指定したテキストを探します。正規表現を使用して検索を実行するには、**正規表現(Regex)**]ボタンを選択してから **検索(Find)**]をクリックします。

HTMLテキストをクリップボードにコピーするには、テキストを強調表示して、ショートカットメニューから **コピー(Copy)**]を選択します。

URLをダブルクリックすると、そのURLを含むセッションがナビゲーションペインで強調表示されます。

スクリプト (Scripts) - ホスト情報 (Host Info)

Fortify WebInspectは、スキャン中に検出されたスクリプトをすべて一覧表示します。検出されたスクリプトを表示するには:

1. **ホスト情報(Host Info)**]パネルから **スクリプト(Scripts)**]を選択し、スクリプトが含まれているすべてのURLを一覧表示します。
2. URLをクリックして、そのURLに含まれるスクリプトを表示します。
3. エントリをダブルクリックして、スクリプトを含むセッションをナビゲーションペインで探します。

情報ペインの最上部にある **検索(Search)**]機能を使用して、指定したテキストを探します。正規表現を使用して検索を実行するには、**正規表現(Regex)**]ボタンを選択してから **検索(Find)**]をクリックします。

スクリプトをクリップボードにコピーするには、テキストを強調表示して、ショートカットメニューから **コピー(Copy)**]を選択します。

URLをダブルクリックすると、そのURLを含むセッションがナビゲーションペインで強調表示されます。

Fortify WebInspectウィンドウの詳細については、「["WebInspectユーザインターフェース" ページ 51](#)」を参照してください。

次も参照

["ホスト情報\(Host Info\)" パネル](#) ページ 100

["ナビゲーションペイン"](#) ページ 67

["正規表現"](#) ページ 323

壊れたリンク(Broken Links)

Fortify WebInspectは、サイト上の正常に機能しないハイパーテインクのすべてを検索して文書化します。壊れたリンクを探すには:

1. **ホスト情報(Host Info)**]パネルから **壊れたリンク(Broken Links)**]を選択し、正常に機能しないハイパーテインクを含むすべてのURLを一覧にします。
2. エントリをダブルクリックして、壊れたリンクを含むセッションをナビゲーションペインで探します。フォーカスが、**セッション情報(Session Info)**]パネルの **HTTP応答(HTTP Response)**]選択肢に切り替わります。

情報ペインの最上部にある [検索(Search)] 機能を使用して、指定したテキストを探します。正規表現を使用して検索を実行するには、[正規表現(Regex)] ボタンを選択してから [検索(Find)] をクリックします。

HTMLテキストをクリップボードにコピーするには、テキストを強調表示して、ショートカットメニューから [コピー(Copy)] を選択します。

URLをダブルクリックすると、そのURLを含むセッションがナビゲーションペインで強調表示されます。

サイト外リンク

Fortify WebInspectは、他のサイトへのハイパーアリンクをすべて検索して文書化します。

他のサイトへのハイパーアリンクを調べるには:

1. [ホスト情報(Host Info)] パネルから [サイト外リンク(Offsite Links)] を選択し、他のサイトへのハイパーアリンクが含まれているすべてのURLを一覧表示します。
2. エントリをダブルクリックして、サイト外リンクを含むセッションをナビゲーションペインで探しします。オーカスが、[セッション情報(Session Info)] パネルの [HTTP応答(HTTP Response)] 選択肢に切り替わります。

情報ペインの最上部にある [検索(Search)] 機能を使用して、指定したテキストを探します。正規表現を使用して検索を実行するには、[正規表現(Regex)] ボタンを選択してから [検索(Find)] をクリックします。

HTMLテキストをクリップボードにコピーするには、テキストを強調表示して、ショートカットメニューから [コピー(Copy)] を選択します。

URLをダブルクリックすると、そのURLを含むセッションがナビゲーションペインで強調表示されます。

Fortify WebInspect ウィンドウの詳細については、「["WebInspectユーザインターフェース" ページ 51](#)」を参照してください。

パラメータ(Parameters)

パラメータには、次のいずれかを指定できます。

- HTTP要求のURLの一部として送信される(または別のヘッダに含まれる)クエリ文字列。
- Postメソッドを使用して送信されるデータ。

パラメータを含むすべてのURLを一覧表示するには:

1. [ホスト情報(Host Info)] パネルから [パラメータ(Parameters)] を選択します。
2. URLをクリックして、そのURLに含まれるパラメータを表示します。
3. エントリをダブルクリックして、パラメータを含むセッションをナビゲーションペインで探しします。 詳細については、「["ナビゲーションペイン" ページ 67](#)」を参照してください。

情報ペインの最上部にある [検索(Search)] 機能を使用して、選択したURLから、指定したテキストを検索します。正規表現を使用して検索を実行するには、[正規表現(Regex)]

ボタンを選択してから [検索(Find)]をクリックします。詳細については、「["正規表現" ページ 323](#)」を参照してください。

テキストをクリップボードにコピーするには、テキストを強調表示して、ショートカットメニューから [コピー(Copy)]を選択します。

URLをダブルクリックすると、そのURLを含むセッションがナビゲーションペインで強調表示されます。

Fortify WebInspectウィンドウの詳細については、「["WebInspectユーザインターフェース" ページ 51](#)」を参照してください。

次も参照

["ホスト情報\(Host Info\)"\]パネル" ページ100](#)

サマリペイン

スキャンを実行または表示するときには、ウィンドウの下部にある横長のサマリペインを使用して、まとめて表示される脆弱性リソースを確認し、脆弱性情報に素早くアクセスし、Fortify WebInspectログ記録情報を確認します。

このペインには以下のタブがあります。

- ・検出事項(Findings) (「["検出事項\(Findings\)"\]タブ" 下](#)」を参照)
- ・未検出(Not Found) (「["未検出\(Not Found\)"\]タブ" ページ114](#)」を参照)
- ・スキャンログ(Scan Log) (「["スキャンログ\(Scan Log\)"\]タブ" ページ114](#)」を参照)
- ・サーバ情報(Server Information) (「["サーバ情報\(Server Information\)"\]タブ" ページ115](#)」を参照)

次も参照

["WebInspectユーザインターフェース" ページ51](#)

["サマリペインのフィルタとグループの使用" ページ262](#)

["脆弱性の再テスト" ページ244](#)

["脆弱性のロールアップ" ページ272](#)

検出事項(Findings)]タブ

[検出事項(Findings)]タブには、Webアプリケーションの監査中に検出された各脆弱性に関する情報が一覧表示されます。

このタブには、スキャン中に検出された懸案事項の情報も表示されます。これらは脆弱性とは見なされませんが、サイトまたは特定のアプリケーションやWebサーバにおける興味深い事項を示します。

さらに、このタブには、スキャン中に検出されたベストプラクティスの問題も含まれています。同様に、これらは脆弱性とは見なされませんが、Web開発で一般的に認められるベストプラクティスに関連し、サイト品質とサイト開発のセキュリティに関する全体的なプラクティス(またはその欠如)の指標となります。

メモ: 検出事項(Findings)】タブで結果をグループ化し、フィルタ処理することもできます。詳細については、「"サマリペインのフィルタとグループの使用" ページ262」を参照してください。

使用可能な列

データの複数の列を表示できます。表示する情報を選択するには、列ヘッダバーを右クリックし、ショートカットメニューから【列(Columns)】を選択します。

使用可能な列は次のとおりです。

- **重大度(Severity):** 脆弱性の相対的な評価(低(low)から重大(critical)まで)。関連するアイコンについては、以下を参照してください。
- **チェック(Check):** 特定の脆弱性に対するFortify WebInspectプローブ。たとえば、クロスサイトスクリプティング、暗号化されていないログインフォームなどです。
- **チェックID (Check ID):** 特定の脆弱性の有無をチェックする、Fortify WebInspectプローブの識別番号。たとえば、チェックID 742は、データベースサーバのエラーメッセージについてテストします。
- **パス(Path):** リソースへの階層パス。
- **メソッド(Method):** 攻撃に使用されるHTTPメソッド。
- **スタック(Stack):** Fortify WebInspect Agentから取得したスタックトレース情報。列は、スキャン中にFortify WebInspect Agentが有効になっている場合にのみ使用できます。
- **脆弱なパラメータ(Vuln Param):** 脆弱なパラメータの名前。
- **パラメータ(Parameters):** パラメータの名前、およびそれらに割り当てられた値。
- **手動(Manual):** 脆弱性が手動で作成された場合は、チェックマークが表示されます。
- **重複(Duplicates):** 同じソースに対して追跡可能な、Fortify WebInspect Agentによって検出された脆弱性。列は、スキャン中にFortify WebInspect Agentが有効になっている場合にのみ使用できます。
- **場所(Location):** パスとパラメータ。
- **CWE ID:** 脆弱性に関連付けられたCommon Weakness Enumeration識別子。
- **界(Kingdom):** Fortify Software Security Research Groupが開発したソフトウェアセキュリティエラーの分類を使用して、この脆弱性が分類されるカテゴリ。
- **アプリケーション(Application):** 脆弱性が見つかったアプリケーションまたはフレームワーク(ASP.NETやMicrosoft IISサーバなど)。
- **保留中ステータス(Pending Status):** このスキャンが発行されると仮定した場合のステータス(自動的にFortify WebInspectによって、または手動で割り当てられる)。
- **発行済みステータス(Published Status):** 以前に発行されている場合の、Software Security Centerに存在するステータス。
- **再現性(Reproducible):** 取り得る値は、[再現済み(Reproduced)]、[未検出/修復済み(Not Found/Fixed)]、または[新規(New)]です。列は、サイト再テスト(脆弱性の再テスト)でのみ使用できます。
- **応答長(Response Length):** 脆弱なセッションの応答サイズ(バイト単位)。
- **再テストのステータス(Retest Status):** 1つ以上の問題で実行された検証スキャンのステータス。この列は、再テストスキャンでのみ使用できます。詳細については、「["脆弱性の再テスト" ページ244](#)」を参照してください。

脆弱性の重大度

検出事項(Findings)タブの脆弱性の重大度は、次のアイコンで示されます。

| | | | |
|----|---|---|---|
| 重大 | 高 | 中 | 低 |
|----|---|---|---|



検出事項の操作

リスト内の項目をクリックすると、関連するセッションがナビゲーションペインで強調表示され、関連する情報が情報ペインに表示されます。詳細については、「["ナビゲーションペイン" ページ67](#)」および「["情報ペイン" ページ78](#)」を参照してください。

セッションを選択し、「**セッション情報 (Session Info)**」パネルからオプションを選択して、関連する情報を表示することもできます。

PostパラメータおよびQueryパラメータの場合は、「**パラメータ (Parameters)**」列のエントリをクリックすると、パラメータのより分かりやすい概要が表示されます。

リスト内の項目を右クリックすると、ショートカットメニューを使用して次の操作を実行できます。

- **URLのコピー (Copy URL)** - URLをWindowsのクリップボードにコピーします。
- **選択した項目のコピー (Copy Selected Item(s))** - 選択した項目のテキストをWindowsクリップボードにコピーします。
- **すべての項目のコピー (Copy All Items)** - すべての項目のテキストをWindowsクリップボードにコピーします。
- **エクスポート (Export)** - すべての項目または選択した項目を含むカンマ区切り値(csv)ファイルを作成し、Microsoft Excelで表示します。
- **ブラウザで表示 (View in Browser)** - HTTP応答をブラウザで表示します。
- **現在の値によるフィルタ (Filter by Current Value)** - 選択した基準を満たす脆弱性だけを表示するよう制限します。たとえば、「**メソッド (Method)**」列で「Post」を右クリックして、「**現在の値によるフィルタ (Filter by Current Value)**」を選択すると、Postメソッドを使用したHTTP要求を送信して検出された脆弱性だけがリストに表示されます。

メモ: フィルタ基準は、サマリペインの右上隅のコンボボックスに表示されます。または、このコンボボックスを使用してフィルタ基準を手動で入力または選択することもできます。

追加の詳細および構文ルールについては、「["サマリペインのフィルタとグループの使用" ページ262](#)」を参照してください。

- **SSCステータスの変更 (Change SSC Status)** - Fortify Software Security Centerに発行する前に脆弱性/問題のステータスを変更します。

メモ: このオプションは、Fortify Software Security Centerと統合されたFortify WebInspect Enterpriseに接続している場合にのみ使用できます。

- **重大度の変更 (Change Severity)** - 重大度レベルを変更できます。
- **脆弱性の編集 (Edit Vulnerability)** - 脆弱性の編集(Edit Vulnerabilities)ダイアログボックスが表示され、脆弱性のさまざまな特性を変更できます。詳細については、「["脆弱性の編集" ページ269](#)」を参照してください。

- **脆弱性のロールアップ(Rollup Vulnerabilities)** -複数の脆弱性が選択されている場合に使用できます。選択した脆弱性を、Fortify WebInspect、Fortify WebInspect Enterprise、およびレポート内で「[Rollup]」というタグの接頭部を持つ单一インスタンスにロールアップできます。詳細については、「["脆弱性のロールアップ" ページ272](#)」を参照してください。

メモ: ロールアップされた脆弱性を選択した場合、このメニューのオプションは「**脆弱性のロールアップを元に戻す(Undo Rollup Vulnerabilities)**」になります。

- **再テスト(Retest)** -選択した1つ以上の脆弱性、すべての脆弱性、または特定の重大度の脆弱性の再テストを実行します。詳細については、「["脆弱性の再テスト" ページ244](#)」を参照してください。
- **マーク付けする(Mark as)** -脆弱性に誤検出(メモを追加可能)または無視のフラグを設定します。どちらの場合も、その脆弱性はリストから削除されます。[スキャン情報(Scan Info)]パネルで「**誤検出(False Positives)**」を選択すると、すべての誤検出のリストを表示できます。[スキャン情報(Scan Info)]パネルで「**ダッシュボード(Dashboard)**」を選択し、統計情報列で削除済み項目のハイパーキー付きの数値をクリックすると、誤検出された脆弱性と無視された脆弱性のリストを表示できます。

メモ: 「誤検出」および「無視」の脆弱性を回復できます。詳細については、「["削除された項目の回復" ページ278](#)」を参照してください。

- **送信(Send to)** -脆弱性を欠陥に変換し、Micro Focus Application Lifecycle Management (ALM)データベースに追加します。
- **場所の削除(Remove Location)** -選択したセッションをナビゲーションペイン(「**サイト(Site)**」ビューと「**シーケンス(Sequence)**」ビューの両方)から削除し、関連する脆弱性もすべて削除します。

メモ: 削除された場所(セッション)およびそれに関連する脆弱性を回復できます。詳細については、「["削除された項目の回復" ページ278](#)」を参照してください。

- **Web探索(Crawl)** -選択したURLのWeb探索を再実行します。
- **ツール(Tools)** -使用可能なツールのサブメニューを表示します。
- **添付ファイル(Attachments)** -選択したセッションに関連するメモの作成、フォローアップのためのセッションへのフラグ付け、脆弱性のメモの追加、または脆弱性スクリーンショットの追加を行うことができます。

グループ見出しを右クリックすると、ショートカットメニューで次の操作を実行できます。

- **すべてのグループの縮小/展開(Collapse/Expand All Groups)**
- **グループの縮小/展開(Collapse/Expand Group)**
- **選択した項目のコピー(Copy Selected Item(s))**
- **すべての項目のコピー(Copy All Items)**
- **重大度の変更(Change Severity)**
- **マーク付けする(Mark as)**
- **送信(Send to)**
- **場所の削除(Remove Location)**

「未検出(Not Found)」タブ

このタブは、Fortify WebInspect Enterpriseに接続した後、かつスキャンをSoftware Security Centerと同期させた後にのみ表示されます。特定のアプリケーションバージョンで前回のスキャンによって検出されたが、現在のスキャンでは検出されていない脆弱性が一覧表示されます。これらの脆弱性はダッシュボード上のカウントには含まれないため、ナビゲーションペインの「サイト(Site)」ビューや「シーケンス(Sequence)」ビューには表示されません。

ショートカットメニューのオプション、グループ化、およびフィルタリング機能は、「検出事項(Findings)」タブで示されている機能のサブセットです。

「スキャンログ(Scan Log)」タブ

Fortify WebInspectスキャンアクティビティに関する情報を表示するには、「スキャンログ(Scan Log)」タブを使用します。たとえば、Webアプリケーションに対して特定の監査手法が適用される時刻がここに一覧表示されます。さらに、スキャンに影響を与えるかねない潜在的な問題についての洞察を与えるアラートレベルのメッセージが「スキャンログ(Scan Log)」に表示されます。

| Scan Log | | |
|----------------------|-------|---|
| Time | Level | Message |
| 1/6/2020 4:06:07 PM | Info | Scan Start, ScanID:267ae8e1-553f-4b34-a05b-1264380ff9aa Version:20.1.0.53, Source:WebInspect.exe: |
| 1/6/2020 4:06:08 PM | Info | Loading Debug DLL: |
| 1/6/2020 4:27:09 PM | Info | Verify Audit Start: |
| 1/6/2020 4:27:10 PM | Info | Verify Audit Stop: |
| 1/6/2020 4:27:17 PM | Info | Scan Complete, ScanID:267ae8e1-553f-4b34-a05b-1264380ff9aa: |
| 1/15/2020 9:29:19 AM | Info | Loading Debug DLL: |
| 1/15/2020 2:25:11 PM | Info | Loading Debug DLL: |
| 1/15/2020 2:25:11 PM | Info | Loading Debug DLL: |

「アプリケーション設定(Application Settings)」ウィンドウの「ログ記録(Logging)」オプションを使用して、ログレベル(、デバッグ、情報、警告、エラー、または重大)を選択できます。詳細については、「[「アプリケーション設定: ログ記録」ページ461](#)」を参照してください。

ペイン上部の「エラー(Errors)」、「警告(Warnings)」、「メッセージ(Messages)」の各ボタンを使用して、表示されるメッセージの種類をフィルタできます。

ヒント: アラートレベルのメッセージは、「警告(Warnings)」フィルタに含まれます。

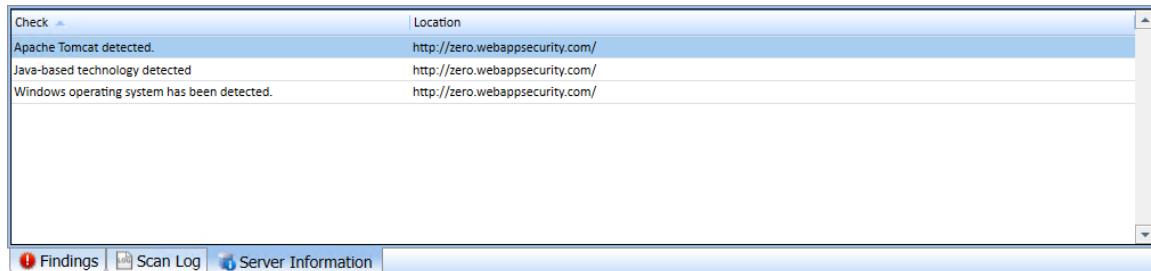
スキャンログの特定のエントリに関する詳細情報を表示するには、エントリを選択して「詳細(Detail)」をクリックします。

また、エントリを右クリックして、ショートカットメニューから次のオプションを選択することもできます。

- 選択した行をクリップボードにコピーする(Copy selected row to clipboard)。
- すべての項目をクリップボードにコピーする(Copy all items to clipboard)。
- このメッセージの詳細を確認する(Get more information about this message)。

【サーバ情報(Server Information)】タブ

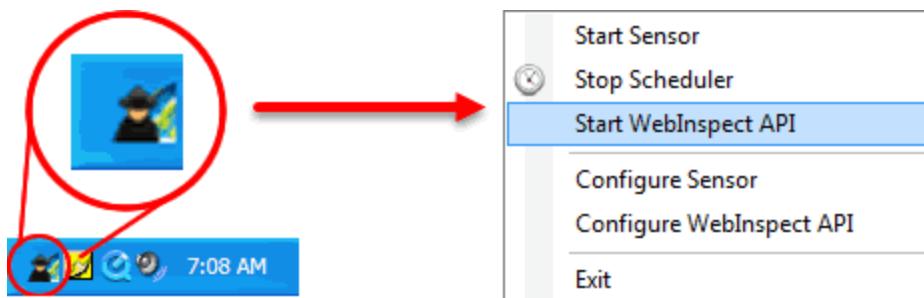
【サーバ(Server)】タブには、サーバに関する重要な項目が一覧表示されます。項目またはイベントはサーバごとに1回だけ表示されます。



Micro Focus Fortify Monitor

Micro Focus Fortify Monitorプログラムは、タスクバーの通知エリアのアイコンとして表示されます。このプログラムのコンテキストメニューから、次の操作を実行できます。

- センサーハードウェアの開始/停止
- スケジューラサービスの開始/停止
- エンタープライズサーバセンサの設定
- WebInspect APIの開始/設定



特定のイベントが発生するたびにポップアップメッセージも表示されます。

この機能の主な対象は、Fortify WebInspectをスタンドアロンスキャナとしてインストールするものの、後でFortify WebInspect Enterpriseに接続するつもりのユーザです。

第4章: スキャンの操作

この章では、Fortify WebInspectが実行できる各種スキャンと、それらのスキャンの実行方法について説明します。スキャンのスケジュール手順と、完了したスキャンのインポート、エクスポート、および管理の手順が収録されています。

ガイド付きスキャンの概要

ガイド付きスキャンを使用すると、最良のステップでアプリケーションに合わせてスキャンを設定できます。

左ペインにガイド付きスキャンの進行状況が表示されるため、スキャンの設定を指定するときに進行状況を簡単に確認できます。右ペインには、各 ウィザードページ上のスキャンオプションが表示されます。

ガイド付きスキャン ウィザードでは、次の操作を実行できます。

- アプリケーションへのコネクティビティを検証する
- アプリケーション全体またはワークフローのみをテストする
- ログイン手順を記録する
- 推奨される設定変更を確認する

ガイド付きスキャンはテンプレートに基づいています。事前定義テンプレートとモバイルテンプレートのどちらを使用するかを選択できます。

事前定義テンプレート

次に挙げる3つの事前定義テンプレートオプションから選択できます。

- **標準スキャン**: このオプションは、カバレッジを重視する場合に使用します。大規模なサイトにこのテンプレートを使用すると数日かかる場合があります。
- **クイックスキャン**: このオプションは、深く掘り下げるよりも適用範囲の広さとパフォーマンスを重視する場合に使用します。非常に大規模なサイトに特に適しています。
- **徹底スキャン**: サイト上で徹底的なWeb探索を実行するために使用します。これらの設定を使用する場合は、サイトを各部に分割して、サイトの小部分だけをスキャンすることをお勧めします。大規模なサイトにはお勧めしません。

モバイルテンプレート

次の2つのモバイルテンプレートオプションの中から選択できます。

- **モバイルスキャン**: このオプションは、Fortify WebInspectまたはFortify WebInspect Enterpriseのインスタンスがインストールされているマシンからモバイルサイトをスキャンする場

合に使用します。このオプションを選択すると、Fortify WebInspectまたはFortify WebInspect Enterpriseにより、サイト全体ではなくモバイルバージョンのサイトがフェッチされます。

- **ネイティブスキャン:** このオプションは、ネイティブモバイルアプリケーションを手動でWeb探索し、Webトラフィックをワークフローマクロとしてキャプチャする場合に使用します。モバイルアプリケーションを実行しているAndroid、Windows、またはiOSデバイスまたはソフトウェアエミュレータ(AndroidおよびiOSのみ)でトラフィックを生成します。

ガイド付きスキャンテンプレートを選択すると、左ペインにステージとステップが表示されます。このペインでは、これらの間を簡単に移動して、スキャンの設定を指定できます。

次も参照

["事前定義テンプレートの使用"次のページ](#)

["モバイルスキャンテンプレートの使用"ページ135](#)

["ネイティブスキャンテンプレートの使用"ページ154](#)

ガイド付きスキャンの実行

左ペインにガイド付きスキャンの進行状況が表示されるため、スキャンの設定を指定するときに進行状況を簡単に確認できます。右ペインには、各ウィザードページ上のスキャンオプションが表示されます。

ガイド付きスキャンの最初のページには、実行するスキャンのタイプを選択するオプションが表示されます。3つの主要なタイプから選択できます。

事前定義テンプレート(標準、クイック、または詳細)

次に挙げる3つの事前定義テンプレートオプションから選択できます。

- **標準スキャン:** デフォルトのスキャン設定は、パフォーマンスよりもカバレッジを重視して設計されています。これらの設定を使用して大規模なサイトをWeb探索するには数日かかる場合があります。
- **クイックススキャン:** 深く掘り下げるよりも、範囲の広さとパフォーマンスを重視したスキャン。非常に大規模なサイトに特に適しています。
- **徹底スキャン:** 徹底スキャンの設定は、サイトの徹底的なWeb探索を実行するように設計されています。これらの設定を使用する場合は、サイトをいくつかの部分に分割して、サイトの小部分だけをスキャンすることをお勧めします。大規模なサイトにはお勧めしません。

詳細については、「["事前定義テンプレートの使用"次のページ](#)」を参照してください。

モバイルスキャンテンプレート

このテンプレートは、Webアプリケーションのスキャン中にモバイルデバイスをエミュレートします。

詳細については、「["モバイルスキャンテンプレートの使用"ページ135](#)」を参照してください。

ネイティブスキャンテンプレート

このテンプレートは、ネイティブモバイルアプリケーションを手動でWeb探索し、Webトライアックをワークフローマクロとしてキャプチャします。

詳細については、「["ネイティブスキャンテンプレートの使用" ページ154](#)」を参照してください。

次も参照

["ガイド付きスキャンの概要" ページ116](#)

["Fortify WebInspectのポリシー" ページ473](#)

事前定義テンプレートの使用

ガイド付きスキャンウィザードでは、Webサイトのスキャンに必要なステージとステップを順に実行します。前のステップまたはステージに戻る必要がある場合は、[戻る]ナビゲーションボタンをクリックするか、ガイド付きスキャンツリー内のステップをクリックして、そこに直接移動します。

重要! SQL Expressデータベースを使用して複数のスキャンを実行する場合、SQL Expressの制限が原因で期待する結果を得られないことがあります。そのため、SQL Expressを使用するインストールでは、同時(または並行)スキャンの実行をお勧めしません。

ガイド付きスキャンの起動

ガイド付きスキャンを起動するには:

- Fortify WebInspectのユーザは、左側のペインの [ガイド付きスキャンの開始(Start a Guided Scan)]オプションをクリックするか、またはメニューバーから [ファイル(File)]> [新規(New)]> [ガイド付きスキャン(Guided Scan)]を選択します。
- Fortify WebInspect Enterpriseのユーザは、Webコンソールで [アクション(Actions)]の下にある [ガイド付きスキャン(Guided Scan)]をクリックします。

ガイド付きスキャンウィザードが起動し、ガイド付きスキャンテンプレートのリストが表示されます。次に挙げる3つの事前定義テンプレートオプションから選択できます。

- 標準スキャン:** このオプションは、カバレッジを重視する場合に使用します。大規模なサイトにこのテンプレートを使用すると数日かかる場合があります。
- クイックスキャン:** このオプションは、深く掘り下げるよりも適用範囲の広さとパフォーマンスを重視する場合に使用します。非常に大規模なサイトに特に適しています。
- 徹底スキャン:** サイト上で徹底的なWeb探索を実行するために使用します。これらの設定を使用する場合は、サイトを各部に分割して、サイトの小部分だけをスキャンすることをお勧めします。大規模なサイトにはお勧めしません。

いずれかの事前定義テンプレートを選択します。

レンダリングエンジンについて

選択するレンダリングエンジンによって、ガイド付きスキャンの設定時に新しいマクロの記録または既存のマクロの編集を行うときに開かれるWeb Macro Recorderが決まります。レンダリングエンジンのオプションは次のとおりです。

- **セッションベース(Session-based)** - このオプションを選択すると、セッションベースのWeb Macro Recorderが指定されます。これはInternet Explorerブラウザテクノロジを使用します。
- **Macro Engine 6.1 (推奨) (Macro Engine 6.1 (recommended))** - このオプションを選択すると、Web Macro Recorder with Macro Engine 6.1が指定されます。これはTruClientテクノロジとFirefoxテクノロジを使用します。

サイトステージについて

サイトステージでは、次の操作を行います。

- スキャンするWebサイトの検証
- スキャンタイプの選択

Webサイトの検証

Webサイトを検証するには:

1. [開始URL(Start URL)]ボックスで、スキャンするサイトの完全なURLまたはIPアドレスを入力または選択します。

URLを入力する場合は、正確に入力する必要があります。たとえば「MYCOMPANY.COM」と入力すると、Fortify WebInspectおよびFortify WebInspect EnterpriseはWWW.MYCOMPANY.COMなどのバリエーションはスキャンしません(許可ホスト(Allowed Hosts)]設定で代替URLを指定している場合を除く)。

無効なURLまたはIPアドレスを指定すると、エラーが発生します。階層ツリー内の特定の位置からスキャンを実行する場合は、スキャンの開始点(<http://www.myserver.com/myapplication/>など)を追加します。

IPアドレスによるスキャンでは、(相対パスではなく)完全修飾URLを使用するリンクを追跡しません。

メモ: Fortify WebInspectでは、WebサイトスキャンおよびWebサービススキャンでIPv6(Internet Protocolバージョン6)アドレスがサポートされています。開始URLを指定する場合は、IPv6アドレスを括弧で囲む必要があります。次に例を示します。

- `http://[::1]`
Fortify WebInspectは「localhost」をスキャンします。
- `http://[fe80::20c:29ff:fe32:bae1]/subfolder/`

Fortify WebInspectは、指定されたアドレスのホストのスキャンを「subfolder」ディレクトリから開始します。

- [http://\[fe80::20c:29ff:fe32:bae1\]:8080/subfolder/](http://[fe80::20c:29ff:fe32:bae1]:8080/subfolder/)

Fortify WebInspectは、ポート8080で実行されているサーバのスキャンを「subfolder」から開始します。

Fortify WebInspectおよびFortify WebInspect Enterpriseでは、IPV4 (Internet Protocol バージョン4)とIPV6 (Internet Protocol バージョン6)の両方がサポートされています。IPV6 アドレスは括弧で囲む必要があります。

2. (オプション)スキャン範囲を特定のエリアに限定するには、[「**フォルダに限定 (Restrict to Folder)**」] チェックボックスをオンにし、リストから次のいずれかのオプションを選択します。

[**ディレクトリのみ(自己) (Directory only (self))**]。Fortify WebInspectおよびFortify WebInspect Enterpriseは、指定されたURLのみをWeb探索または監査(またはその両方)します。たとえば、このオプションを選択してwww.mycompany/one/two/というURLを指定すると、Fortify WebInspectおよびFortify WebInspect Enterpriseは「two」ディレクトリのみを評価します。

[**ディレクトリおよびサブディレクトリ(Directory and subdirectories)**]。Fortify WebInspect およびFortify WebInspect Enterpriseは、指定されたURLでWeb探索または監査(またはその両方)を開始しますが、ディレクトリツリーでそれよりも上位のディレクトリにはアクセスしません。

[**ディレクトリおよび親ディレクトリ(Directory and parent directories)**]。Fortify WebInspectおよびFortify WebInspect Enterpriseは、指定されたURLでWeb探索または監査(またはその両方)を開始しますが、ディレクトリツリーでそれよりも下位のディレクトリにはアクセスしません。

[**「**フォルダに限定 (Restrict to folder)**」スキャンオプションの制限**については、「["「**フォルダに限定**」に関する制限" ページ202](#)」を参照してください。

3. [**検証(Verify)**]をクリックします。

Webサイトが、共通アクセスカード(CAC)を使用してクライアント証明書で認証するように設定されている場合、ガイド付きスキャンでは次のメッセージが表示されます。

サイト<URL>がクライアント証明書を要求しています。今すぐ設定しますか? (The site <URL> is requesting a client certificate. Would you like to configure one now?)

CACを使用してクライアント証明書を設定するには:

- a. [**はい(Yes)**]をクリックします。

[**クライアント証明書の選択 (Select a Client Certificate)**] ウィンドウが表示されます。

- b. [**証明書ストア(Certificate Store)**]で、**現在のユーザ(Current User)**を選択します。

使用可能な証明書のリストが [**証明書(Certificate)**] エリアに表示されます。

- c. 「(SmartCard)」というプレフィックスが付いた証明書を見つけて選択します。

証明書の詳細とPINフィールドが、 [**証明書情報(Certificate Information)**] エリアに表示されます。

- d. PINが必要な場合は [**PIN**] フィールドにCACのPINを入力し、 [**テスト(Test)**] をクリックします。

メモ: PINが必要な場合に、この時点でPINを入力しないと、スキャン中にPINの入力を求められるたびに、Windowsの[セキュリティ]ウィンドウにPINを入力する必要があります。

4. プロキシサーバ経由でターゲットサイトにアクセスする必要がある場合は、メイン画面の左下にある[プロキシ(Proxy)]をクリックして[プロキシ設定(Proxy Settings)]エリアを表示し、[プロキシ設定(Proxy Settings)]リストからオプションを選択します。
 - 直接接続(プロキシ無効)(Direct Connection (proxy disabled))
 - プロキシ設定の自動検出(Auto detect proxy settings): WPAD (Web Proxy Autodiscovery Protocol)を使用してプロキシ自動設定ファイルを見つけ、このファイルを使用してブラウザのWebプロキシ設定を行います。
 - システムのプロキシ設定を使用する(Use System proxy settings): ローカルマシンからプロキシサーバ情報をインポートします。
 - Firefoxプロキシ設定を使用する(Use Firefox proxy settings): Firefoxからプロキシサーバ情報をインポートします。
 - PACファイルを使用してプロキシ設定を行う(Configure proxy settings using a PAC File): PAC (Proxy Automatic Configuration)ファイルからプロキシ設定をロードします。このオプションを選択した場合は、[編集(Edit)]をクリックしてPACの場所(URL)を入力します。
 - プロキシを明示的に設定する(Explicitly configure proxy settings): 指示に従ってプロキシサーバ設定を指定します。このオプションを選択した場合は、表示されるフィールドにプロキシ情報を入力します。

メモ: ブラウザのプロキシ設定を使用することにしても、プロキシサーバ経由のインターネットアクセスが保証されるわけではありません。Firefoxブラウザの接続設定が[プロキシーを使用しない]に設定されている場合、またはInternet Explorerの[LANにプロキシサーバを使用する]設定が選択されていない場合、プロキシサーバは使用されません。

Webサイトまたはディレクトリ構造のスクリーンショットが表示されたら、開始URLへの接続の検証が正常に完了しています。

5. 次へ(Next)]をクリックします。
[スキャンタイプの選択(Choose Scan Type)]ウィンドウが表示されます。

スキャンタイプの選択

1. [スキャン名(Scan Name)]ボックスにスキャンの名前を入力します。
2. 次のいずれかのスキャンタイプを選択します。
 - 標準(Standard):** Fortify WebInspectおよびFortify WebInspect Enterpriseは自動分析を実行し、ターゲットURLから開始します。これは標準的なスキャン開始方法です。

- **ワークフロー(Workflows)**: このオプションを選択すると、ガイド付きスキャンにワークフローステージが追加されます。
3. [スキャン方法(Scan Method)]エリアで、次のいずれかのスキャン方法を選択します。
- **Web探索のみ(Crawl Only)**。このオプションを選択すると、サイトの階層データ構造が完全にマッピングされます。Web探索が完了したら、[監査(Audit)]をクリックしてアプリケーションの脆弱性を評価できます。
 - **Web探索および監査(Crawl and Audit)**。Fortify WebInspectおよびFortify WebInspect Enterpriseは、サイトの階層データ構造をマッピングし、各リソース(ページ)を監査します。選択したデフォルト設定に応じて、各リソースの検出時またはサイト全体のWeb探索後に監査を実行できます。Web探索および監査の同時実行と順次実行の詳細については、「["スキャン設定: 方法" ページ370](#)」を参照してください。
 - **監査のみ(Audit Only)**。Fortify WebInspectおよびFortify WebInspect Enterpriseは、選択されたポリシーの手法を脆弱性リスクの判断に適用しますが、WebサイトのWeb探索は行いません。サイト上のリンクをたどることも評価することもありません。
4. [ポリシー(Policy)]エリアの [ポリシー(Policy)]リストからポリシーを選択します。ポリシーの管理については、『*Micro Focus Fortify WebInspect Tools Guide*』の「Policy Manager」の章を参照してください。
5. [Web探索のカバレッジ(Crawl Coverage)]エリアで、[Web探索のカバレッジ(Crawl Coverage)]スライダを使用してカバレッジのレベルを選択します。Web探索のカバレッジレベルの詳細については、「["カバレッジと徹底性" ページ185](#)」を参照してください。
6. [シングルページアプリケーション(Single-Page Applications)]エリアで、SPA (single-page application)のWeb探索および監査のオプションを選択します。有効にすると、DOMスクリプトエンジンは、Web探索中に、JavaScriptインクルード、フレームとiframeのインクルード、CSSファイルインクルード、およびAJAX呼び出しを検索してから、それらのイベントによって生成されたすべてのトラフィックを監査します。[シングルページアプリケーション(Single-Page Applications)]のオプションは次のとおりです。
- **自動(Automatic)** - Fortify WebInspectがSPAフレームワークを検出すると、自動的にSPAサポートモードに切り替わります。
 - **有効(Enabled)** - SPAフレームワークがターゲットアプリケーションで使用されていることを示します。
- 注意!** SPAサポートは、シングルページアプリケーションに対してのみ有効にするべきです。SPAサポートを有効にしてSPA以外のWebサイトをスキャンすると、スキャンが遅くなります。
- **無効(Disabled)** - SPAフレームワークがターゲットアプリケーションで使用されていないことを示します。
- 詳細については、「["シングルページアプリケーションスキャンについて" ページ210](#)」を参照してください。
7. [次へ(Next)]ボタンをクリックします。
- ログインステージが表示され、左側のペインでネットワーク認証が強調表示されます。

ログインステージについて

スキャンするアプリケーションにログイン資格情報が必要な場合は、ログインステージを使用して、既存のログインマクロを選択するか、スキャンで使用するログインマクロを記録できます。

アプリケーションにログイン資格情報が必要ない場合は、値を割り当てずに各オプションをクリックするか、ガイド付きスキャンツリーの「[アプリケーション(Application)]」をクリックして次のステージにスキップすることで、ガイド付きスキャンウィザードのこのセクションをスキップできます。

このステージでは、次の操作を実行できます。

- ネットワークの権限付与の設定
- アプリケーションの権限付与の設定
- ログインマクロの作成または割り当て

ネットワーク認証ステップ

アプリケーションでネットワークまたはアプリケーションレベルの認証が必要な場合は、ここで割り当てることができます。

ネットワーク認証の設定

ネットワークでユーザ認証が必要な場合は、ここで設定できます。ネットワークでユーザ認証が不要な場合は、[次へ(Next)]ナビゲーションボタン、またはガイド付きスキャンツリーの次の該当ステップをクリックして続行します。

ネットワーク認証を設定するには:

1. [ネットワーク認証(Network Authentication)]チェックボックスをクリックします。
2. 認証メソッドのドロップダウンリストから、メソッドを選択します。認証メソッドは次のとおりです。
 - ADFS CBT
 - 自動(Automatic)
 - 基本(Basic)
 - ダイジェスト(Digest)
 - Kerberos
 - ネゴシエート(Negotiate)
 - NT LAN Manager (NTLM)
3. ネットワーク認証にクライアント証明書を使用するには、[クライアント証明書(Client Certificate)]を選択します。

4. 証明書ストア(Certificate Store)]エリアで、次のいずれかを選択してから、[マイ(My)]または[ルート(Root)]ラジオボタンを選択します。
 - [ローカルマシン(Local Machine)]。Fortify WebInspectは、証明書ストア(Certificate Store)]エリアで選択した内容に基づいて、ローカルマシン上の証明書を使用します。
 - [現在のユーザ(Current User)]。Fortify WebInspectは、証明書ストア(Certificate Store)]エリアで選択した内容に基づいて、現在のユーザの証明書を使用します。
 5. 証明書情報(Certificate Information)]エリアに証明書の詳細を表示するには、証明書を選択します。
 6. [次へ(Next)]ボタンをクリックします。
- 「アプリケーション認証(Application Authentication)」ページが表示されます。

アプリケーション認証のステップ

サイトで認証が必要な場合は、このステップを使用してログインマクロを作成、選択、または編集することにより、ログインプロセスを自動化してサイトのカバレッジを拡大できます。ログインマクロは、アプリケーションにアクセスしてログインするために必要なアクティビティの記録です。通常は、ユーザ名とパスワードを入力し、[ログイン]や[ログオン]などのボタンをクリックします。

ログインマクロを使用するスキャンの[スキャン設定: 認証(Scan Settings: Authentication)]で「マクロ検証を有効にする(Enable macro validation)」が選択されている場合、Fortify WebInspectはスキャンの開始時点でログインマクロをテストして、ログインが成功したことを確認します。マクロが無効で、アプリケーションへのログインに失敗した場合、スキャンは停止し、エラーメッセージがスキャンログファイルに書き込まれます。詳細とトラブルシューティングのヒントについては、「["ログインマクロのテスト" ページ510](#)」を参照してください。

重要! 2要素認証を含むマクロを使用する場合は、スキャンを開始する前に、2要素認証アプリケーションの設定を行う必要があります。詳細については、「["アプリケーション設定: 2要素認証" ページ453](#)」を参照してください。

ログインマクロでは、次のオプションを使用できます。

- "[権限のエスカレーションなしでログインマクロを使用する\(Using a Login Macro without Privilege Escalation\)](#)" 次のページ
- "[権限のエスカレーションのためにログインマクロを使用する\(Using Login Macros for Privilege Escalation\)](#)" 次のページ
- "[Fortify WebInspect Enterpriseに接続した際にログインマクロを使用する\(Using a Login Macro when Connected to Fortify WebInspect Enterprise\)](#)" ページ126

マスクされた値のサポート

Web Macro Recorderで値がマスクされたパラメータがマクロで使用されている場合、Fortify WebInspectでガイド付きスキャンを設定するときにも、それらの値はマスクされます。

権限のエスカレーションなしでログインマクロを使用する(Using a Login Macro without Privilege Escalation)

ログインマクロを使用するには:

1. **このサイトでログインマクロを使用する(Use a login macro for this site)**] チェックボックスをオンにします。
 2. 次のいずれかを実行します。
 - 事前に記録されたログインマクロを使用するには、省略記号ボタン([...])をクリックして、保存されているマクロを参照します。
 - **ログインマクロ(Login Macro)**] フィールドに表示されている既存のログインマクロを編集するには、**編集(Edit)**] をクリックします。
 - 新しいマクロを記録するには、**作成(Create)**] をクリックします。
 3. **次へ(Next)**] ボタンをクリックします。
- 標準スキャンを選択した場合は、**最適化タスク(Optimization Tasks)**] ページが表示されます。ワークフロースキャンを選択した場合は、**ワークフローの管理(Manage Workflows)**] ページが表示されます。

権限のエスカレーションのためにログインマクロを使用する(Using Login Macros for Privilege Escalation)

権限のエスカレーションポリシーか、有効な権限のエスカレーションチェックを含む別のポリシーを選択した場合、高い権限を持つユーザアカウント用のログインマクロが少なくとも1つ必要です。詳細については、「["権限のエスカレーションスキャンについて" ページ207](#)」を参照してください。

ログインマクロを使用するには:

1. **高い権限のユーザアカウントログインマクロ(High-Privilege User Account Login Macro)**] チェックボックスをオンにします。このログインマクロは、サイト管理者やモデレータアカウントなど、より高い権限を持つユーザアカウント用です。
2. 次のいずれかを実行します。
 - 事前に記録されたログインマクロを使用するには、省略記号ボタン([...])をクリックして、保存されているマクロを参照します。
 - **ログインマクロ(Login Macro)**] フィールドに表示されている既存のログインマクロを編集するには、**編集(Edit)**] をクリックします。
 - 新しいマクロを記録するには、**作成(Create)**] をクリックします。

新しいログインマクロの記録 や既存のログインマクロの使用の詳細については、『*Micro Focus Fortify WebInspect Tools Guide*』の「Web Macro Recorder」の章を参照してください。

最初のマクロを記録または選択して 次へ(Next)]の矢印をクリックすると、低い権限のログインマクロを設定する(Configure Low Privilege Login Macro)]プロンプトが表示されます。

3. 次のいずれかを実行します。

- 認証モードでスキャンを実行するには、【はい(Yes)】をクリックします。詳細については、「["権限のエスカレーションスキャンについて" ページ207](#)」を参照してください。ガイド付きスキャンが [ログインマクロの選択(Select Login Macro)] ウィンドウに戻り、低い権限のログインマクロを作成または選択できるようになります。ステップ4に進みます。
- スキャンを非認証モードで実行するには、【いいえ(No)】をクリックします。詳細については、「["権限のエスカレーションスキャンについて" ページ207](#)」を参照してください。アプリケーション認証のステップが完了しました。標準スキャンを選択した場合は、最適化タスク(Optimization Tasks)]ページが表示されます。ワークフロースキャンを選択した場合は、[ワークフローの管理(Manage Workflows)]ページが表示されます。

4. **低い権限のユーザーアカウントログインマクロ(Low-Privilege User Account Login Macro)** チェックボックスをオンにします。このログインマクロは、サイトコンテンツのビューアやコンシューマなど、低い権限のユーザーアカウント用です。

5. 次のいずれかを実行します。

- 事前に記録されたログインマクロを使用するには、省略記号ボタン([...])をクリックして、保存されているマクロを参照します。
- [ログインマクロ(Login Macro)] フィールドに表示されている既存のログインマクロを編集するには、**編集(Edit)**をクリックします。
- 新しいマクロを記録するには、**作成(Create)**をクリックします。

新しいログインマクロの記録 や既存のログインマクロの使用の詳細については、『*Micro Focus Fortify WebInspect Tools Guide*』の「Web Macro Recorder」の章を参照してください。

6. 2つ目のマクロを記録または選択した後、**次へ(Next)**]ボタンをクリックします。

標準スキャンを選択した場合は、最適化タスク(Optimization Tasks)]ページが表示されます。ワークフロースキャンを選択した場合は、[ワークフローの管理(Manage Workflows)]ページが表示されます。

Fortify WebInspect Enterpriseに接続した際にログインマクロを使用する(Using a Login Macro when Connected to Fortify WebInspect Enterprise)

Fortify WebInspect Enterpriseに接続されているFortify WebInspectの場合は、Fortify WebInspect Enterpriseマクロリポジトリからログインマクロをダウンロードして使用できます。

マクロをダウンロードするには:

1. [このサイトでログインマクロを使用する(Use a login macro for this site)] チェックボックスをオンにします。
2. [ダウンロード(Download)] をクリックします。
[Fortify WebInspect Enterpriseからマクロをダウンロードする(Download a Macro from Fortify WebInspect Enterprise)] ウィンドウが表示されます。
3. ドロップダウンリストから [アプリケーション(Application)] と [バージョン(Version)] を選択します。
4. [マクロ(Macro)] ドロップダウンリストからリポジトリマクロを選択します。
5. [OK] をクリックします。

メモ: リポジトリマクロを選択すると、[最終確認(Final Review)] ページの [自動でスキャンをWIEにアップロードする(Automatically Upload Scan to WIE)] の [アプリケーション(Application)] と [バージョン(Version)] が自動的に同期されます。

ログインマクロを自動で作成する

ユーザ名とパスワードを入力して、Fortify WebInspectでログインマクロを自動的に作成できます。

メモ: 権限のエスカレーションおよびマルチユーザログインスキャンに対して、また、セッションベースのレンダリングエンジンを使用するスキャンに対して自動でログインマクロを作成することはできません。

ログインマクロを自動的に作成するには:

1. [ログインマクロの自動生成(Auto-gen Login Macro)] を選択します。
2. [ユーザ名(Username)] フィールドにユーザ名を入力します。
3. [パスワード>Password)] フィールドにパスワードを入力します。

オプションで、[テスト(Test)] をクリックして、ログインフォームの検索、マクロの生成、マクロ検証テストの実行を行ってから、ガイド付きスキャンウィザードの次のステージに進みます。完了前に検証テストをキャンセルする必要がある場合は、[キャンセル(Cancel)] をクリックします。

重要! ワークフローステージまたはガイド付きスキャンの拡張カバレッジ(Enhanced Coverage)タスクで自動的に生成されたマクロを使用するには、[テスト(Test)] をクリックしてマクロを生成する必要があります。

マクロが無効で、アプリケーションへのログインが失敗すると、エラーメッセージが表示されます。詳細とトラブルシューティングのヒントについては、「["ログインマクロのテスト" ページ510](#)」を参照してください。

ワークフローステージについて

ワークフローステージは、サイトステージで [スキャンタイプ(Scan Type)] として [ワークフロー(Workflows)] を選択した場合にのみ表示されます。標準(Standard)を選択した場合、

ワークフローステージは表示されません。ワークフローマクロを作成すると、マクロで指定したページをFortify WebInspectで確実に監査できます。Fortify WebInspectはマクロに含まれているURLのみを監査し、監査中に検出されたハイパーアリンクはたどりません。ログアウト署名は不要です。この種のマクロは、アプリケーションの特定のサブセクションに焦点を当てるために最もよく使用されます。

重要! ログインマクロを、ワークフローマクロまたは起動マクロ、あるいはその両方と組み合わせて使用する場合、すべてのマクロは同じ種類である必要があります。すべてが.webmacroファイルであるか、すべてがBurp Proxyキャプチャであるかのどちらかです。同じスキャンで異なる種類のマクロを使用することはできません。

ワークフローの設定を完了するには、[ワークフロー(Workflows)]テーブルで次のいずれかをクリックします。

- **記録(Record)**]。Web Macro Recorderが開き、マクロを作成できます。
- **編集(Edit)**]。Web Macro Recorderが開き、選択したマクロがロードされます。
- **削除(Delete)**]。選択したマクロが削除されます(ただしディスクからは削除されません)。
- **インポート(Import)**]。標準のファイル選択ウィンドウが開き、以前に記録した.webmacroファイルまたはBurp Proxyキャプチャを選択できます。

メモ: コンピュータにMicro Focus UFT (Unified Functional Testing)がインストールされている場合は、Fortify WebInspectがこれを自動的に検出し、UFT .usrファイルをインポートするためのオプションが表示されます。

「"ガイド付きスキャンでのMicro Focus UFT (Unified Functional Testing)ファイルのインポート" ページ134」を参照してください。

- **エクスポート(Export)**]。標準のファイル選択ウィンドウが開き、記録したマクロを保存できます。

ワークフローマクロを指定して再生すると、[ワークフロー(Workflows)]テーブルにそのマクロが表示され、許可ホストが「ガイド付きスキャン(Guided Scan)」>「ワークフロー(Workflows)」>「ワークフロー(Workflows)」>「マネージャワークフロー(Manager Workflow)」ページに追加されます。特定のホストへのアクセスを有効または無効にできます。詳細については、「"スキャン設定: 許可ホスト" ページ389」を参照してください。

Burp Proxy結果を追加するには

Burp Proxyセキュリティテストを実行した場合、テスト中に収集されたトラフィックをワークフローマクロにインポートできます。これにより、同じエリアの再スキャンにかかる時間が短縮されます。

ワークフローマクロにBurp Proxy結果を追加するには:

1. 「ワークフロー(Workflows)」画面が表示されていない場合は、「ガイド付きスキャン(Guided Scan)」ツリーの「ワークフローの管理(Manage Workflows)」ステップをクリックします。
2. 「インポート(Import)」ボタンをクリックします。
「マクロのインポート(Import Macro)」ファイルセレクタが表示されます。

3. ファイルの種類ボックスのフィルタを [Webマクロ(*.webmacro)(Web Macro (*.webmacro))] から [Burp Proxy (*.*)] に変更します。
4. Burp Proxyファイルに移動し、目的のファイルを選択します。
5. [開く(Open)] をクリックします。

アクティブラーニングステージについて

アクティブラーニングステージでは次の操作が実行されます。

- WebInspect Profilerが実行され、設定を変更する必要があるかどうかが確認されます。
- 必要に応じてスキャン最適化オプションを設定します。

Profilerの使用

WebInspect Profilerは、ターゲットWebサイトの事前テストを実行し、特定の設定を変更すべきかどうかを判断します。変更が必要だと思われる場合、Profilerは提案のリストを返します。これらの提案は、受け入れることも拒否することもできます。

たとえば、Profilerは、サイトに入るための権限付与が必要であるものの、有効なユーザ名とパスワードが指定されていないことを検出するかもしれません。そのままスキャンを続行して著しく質の低い結果を得るのではなく、Profilerの提案に従って、続行する前に必要な情報を設定することができます。

同様に、設定では、Fortify WebInspectが「ファイルが見つからない」の検出を実行しないように指定されていることもあります。このプロセスは、存在しないリソースをクライアントから要求されてもステータス「404 Not Found」を返さないWebサイトで役に立ちます(代わりにステータス「200 OK」が返される場合がありますが、応答にはファイルが見つからないというメッセージが含まれます)。Profilerは、このような手法がターゲットサイトに実装されていると判断した場合、この特徴に対応できるようにFortify WebInspect設定を変更することを推奨します。

Profilerを起動するには:

1. [プロファイル(Profile)] をクリックします。

Profilerが実行されます。詳細については、「["Server Profiler" ページ256](#)」を参照してください。

結果は、[設定(Settings)] セクションの [スキャンの最適化(Optimize scan for)] ボックスに表示されます。

2. [スキャンの最適化(Optimize scan for)] ドロップダウンボックスに表示される提案を受け入れるかまたは拒否します。提案を拒否するには、ドロップダウンメニューから [なし(None)] または代わりの提案を選択します。
3. 必要に応じて、要求された情報を入力します。
4. [次へ(Next)] ボタンをクリックします。

Profilerを実行していない場合でも、いくつかのオプションが表示されることがあります。これについてには、以降のセクションで説明します。

Webフォームの自動入力(Autofill Web Forms)

Fortify WebInspectがターゲットサイトのスキャン中に検出されるフォームの入力コントロールの値を送信するようにするには、[Web探索時のWebフォームの自動入力(Auto-fill Web forms during crawl)]を選択します。Fortify WebInspectは、事前パッケージ化されたデフォルトファイル、またはWeb Form Editorを使用して作成したファイルから値を抽出します。『Micro Focus Fortify WebInspect Tools Guide』の「Web Form Editor」の章を参照してください。以下を実行できます。

1. 省略記号ボタン(...)をクリックして、ファイルを見つけてロードします。
2. [編集(Edit)]をクリックして、選択したファイル(またはデフォルト値)をWeb Form Editorで編集します。
3. [作成(Create)]をクリックしてWeb Form Editorを開き、ファイルを作成します。

許可ホストの追加(Add Allowed Hosts)

[許可ホスト(Allowed Host)]設定は、Web探索して監査するドメインを追加する場合に使用します。Webプレゼンスで複数のドメインが使用されている場合は、それらのドメインをここに追加します。詳細については、「["スキャン設定:許可ホスト" ページ389](#)」を参照してください。

許可するドメインを追加するには:

1. [追加(Add)]をクリックします。
2. [許可ホストの指定(Specify Allowed Host)]ウィンドウで、URL(またはURLを表す正規表現)を入力し、[OK]をクリックします。

識別された誤検出を再利用する(Reuse Identified False Positives)

誤検出に変更された脆弱性を含むスキャンを選択します。このスキャンで検出された脆弱性がこれらの誤検出と一致する場合、脆弱性は誤検出に変更されます。詳細については、「["誤検出\(False Positives\)" ページ89](#)」を参照してください。

識別された誤検出を再利用するには:

1. [誤検出のインポート(Import False Positives)]を選択します。
2. [スキャンの選択(Select scans)]をクリックします。
3. 現在スキャンしている同じサイトからの誤検出を含むスキャンを1つ以上選択します。
4. [OK]をクリックします。

サンプルマクロの適用(Apply Sample Macro)

Fortify WebInspectのサンプルシンキングアプリケーション(zero.webappsecurity.com)では、Webフォームログインが使用されています。このサイトをスキャンする場合は、[サンプルマクロの適用(Apply sample macro)]を選択して、ログインスクリプトを含む事前パッケージ化されたマクロを実行します。

トラフィック分析(Traffic Analysis)

Web Proxyツールを使用してFortifyにより発行されたHTTP要求とターゲットサーバから返された応答を検査するには、[Web Proxyの起動およびWeb Proxy経由でのトラフィックの送信(Launch and Direct Traffic through Web Proxy)]を選択します。

Fortify WebInspectはWebサイトのスキャン中に、Webサイトの階層構造を明らかにするセッションと、脆弱性が検出されたセッションのみをナビゲーションペインに表示します。ただし **[Traffic Monitorを有効にする(Enable Traffic Monitor)]**を選択すると、Fortify WebInspectでは **[Traffic Monitor]**ボタンが **[スキャン情報(Scan Info)]**パネルに追加されます。これにより、Fortify WebInspectが送信した各HTTP要求と、サーバから受信した関連HTTP応答を表示して確認できます。

メッセージ

Profilerが変更を推奨しない場合は、ガイド付きスキャンウィザードに「設定の変更は推奨されません。現在のスキャン設定はこのサイトに最適です。(No settings changes are recommended. Your current scan settings are optimal for this site.)」というメッセージが表示されます。

[次へ(Next)]をクリックします。

[最終確認(Final Review)]ページが表示され、左側のペインで **詳細オプションの設定(Configure Detailed Options)**が強調表示されます。

設定ステージについて

詳細オプションを設定するには、次の設定を指定します。

識別された誤検出を再利用する(Reuse Identified False Positives)

Fortify WebInspectによってすでに識別されている誤検出を再利用するには、**誤検出(False Positives)**ボックスをオンにします。

トラフィック分析(Traffic Analysis)

1. Web Proxyツールを使用するには、**[Web Proxyの起動およびWeb Proxy経由でのトラフィックの送信(Launch and Direct Traffic through Web Proxy)]**を選択して、Fortify WebInspectが発行したHTTP要求と、ターゲットサーバから返された応答を調べます。
Web Proxyはスタンドアロンの自己完結型プロキシサーバであり、デスクトップ上で設定および実行できます。Web Proxyを使用すると、スキャナ、Webブラウザ、またはHTTP要求を送信してサーバから応答を受信する他のツールからのトラフィックを監視できます。Web Proxyは、デバッグと侵入スキャンのためのツールです。サイトのブラウズ中に、すべての要求とサーバの応答を確認できます。
2. Fortify WebInspectによって送信された各HTTP要求と、サーバから受信した関連HTTP応答を表示および確認するには、**[Traffic Monitor]**ボックスを選択します。

Fortify WebInspectはWebサイトのスキャン中に、Webサイトの階層構造を明らかにしたセッションと、脆弱性が検出されたセッションのみを表示します。ただし **[Traffic Monitorを有効にする(Enable Traffic Monitor)]**を選択すると、Fortify WebInspectではFortify WebInspectが送信した各HTTP要求と、サーバから受信した関連HTTP応答を表示して確認できます。

3. **[次へ(Next)]**をクリックします。

[設定の検証とスキャンの開始(Validate Settings and Start Scan)]ページが表示され、左側のペインで **詳細オプションの設定(Configure Detailed Options)**が強調表示されます。

設定の検証とスキャンの開始(Validate Settings and Start Scan)

このページのオプションを使用すると、現在のスキャン設定を保存することができます。また、WebInspectがWebInspect Enterpriseと統合されている場合は、WebInspect Enterpriseとやり取りすることができます。

1. スキャン設定をXMLファイルとして保存するには、[ここをクリックして設定を保存する(Click here to save settings)]を選択します。標準の名前を付けて保存(Save as)]ウィンドウを使用して、ファイルに名前を付けて保存します。
2. WebInspectがWebInspect Enterpriseと統合されている場合は、ツールバーに[テンプレート(Templates)]セクションが表示されます。次の表の説明に従って操作を進めます。

| 目的の作業 | その場合の手順 |
|--|--|
| <p>現在のスキャン設定をテンプレートとしてWebInspect Enterpriseデータベースに保存する</p> <p>メモ: 既存のテンプレートを編集する場合、[保存(Save)]を実行すると、実際には更新が行われます。設定の編集を保存したり、テンプレート名を変更したりすることができます。ただし、アプリケーション、バージョン、またはグローバルテンプレートの設定は変更できません。</p> | <ol style="list-style-type: none"> 次のいずれかを実行します。 <ul style="list-style-type: none"> ツールバーの[テンプレート(Templates)]セクションで[保存(Save)]をクリックします。 [ここをクリックしてテンプレートを保存する(Click here to save template)]を選択します。 [テンプレートの保存(Save Template)]ウィンドウが表示されます。 [アプリケーション(Application)]ドロップダウンリストからアプリケーションを選択します。 [バージョン(Version)]ドロップダウンリストからアプリケーションバージョンを選択します。 [テンプレート(Template)]フィールドに名前を入力します。 |
| <p>テンプレートからスキャン設定をロードする</p> | <ol style="list-style-type: none"> ツールバーの[テンプレート(Templates)]セクションで[ロード(Load)]をクリックします。 <p>現在のスキャン設定が失われるという確認メッセージが表示されます。</p> <ol style="list-style-type: none"> [はい(Yes)]をクリックします。 [テンプレートのロード(Load Template)]ウィンドウが表示されます。 |

| 目的の作業 | その場合の手順 |
|-------|---|
| | <p>c. [アプリケーション(Application)]ドロップダウンリストからアプリケーションを選択します。</p> <p>d. [バージョン-Version)]ドロップダウンリストからアプリケーションバージョンを選択します。</p> <p>e. [テンプレート(Template)]ドロップダウンリストからテンプレートを選択します。</p> <p>f. [ロード(Load)]をクリックします。</p> <p>ガイド付きスキャンがサイトステージに戻り、Webサイトの検証と、テンプレートからのステップごとの設定の実行が行えるようになります。</p> |

3. WebInspectがWebInspect Enterpriseと統合されている場合は、このページに [WebInspect Enterprise]セクションが表示されます。WebInspect Enterpriseを操作するには、次のようにします。
- [アプリケーション(Application)]ドロップダウンリストからアプリケーションを選択します。
 - [バージョン-Version)]ドロップダウンリストからアプリケーションバージョンを選択します。
 - 次の表の説明に従って操作を進めます。

| スキャンの実行方法 | その場合の手順 |
|--------------------------------|--|
| WebInspect Enterpriseでセンサを使用する | <ol style="list-style-type: none"> [WebInspect Enterpriseで実行(Run in WebInspect Enterprise)]を選択します。 [センサ(Sensor)]ドロップダウンリストからセンサを選択します。 スキャンの [優先度(Priority)]を選択します。 |
| WebInspectで | <ol style="list-style-type: none"> [WebInspectで実行(Run in WebInspect)]を選択します。 スキャン結果をWebInspect Enterpriseの指定したアプリケーションおよびバージョンに自動的にアップロードする場合は、 [WebInspect Enterpriseへの自動アップロード(Auto Upload to WebInspect Enterprise)]を選択します。 |

| スキャンの実行方法 | その場合の手順 |
|-----------|---|
| | <p>メモ: スキャンが正常に完了しない場合、WebInspect Enterpriseにはアップロードされません。</p> |

- 【今すぐスキャン(Scan Now)】エリアでスキャン設定を見直し、【スキャンの開始(Start Scan)】をクリックしてスキャンを開始します。

ガイド付きスキャンでのMicro Focus UFT (Unified Functional Testing)ファイルのインポート

Micro Focus Unified Functional Testingアプリケーションがインストールされている場合、Fortify WebInspectがこのアプリケーションを検出し、ワークフロースキャンにUTFファイル(.usr)をインポートして、スキャンの完全性と攻撃露呈部分を拡張できるようにします。詳細については、Micro Focus Webサイトの「[Unified Functional Testing](#)」を参照してください。

UTF (.usr)ファイルをFortify WebInspect ガイド付きスキャンにインポートするには:

- ガイド付きスキャンを起動し、【スキャンタイプ(Scan Type)】として【ワークフロースキャン(Workflow Scan)】を選択します。【ワークフロースキャン(Workflows scan)】オプションの下に、「Micro Focus Unified Functional Testingが検出されました(Micro Focus Unified Functional Testing has been detected)」という追加テキストが表示されます。スクリプトをインポートして、セキュリティテストの完全性を強化できます。
- 【次へ(Next)】ボタンをクリックします。
- 【認証(Authentication)】セクションで、【アプリケーション認証(Application Authentication)】が自動的に選択されます。指示に従ってフィールドに入力します。
- 【ワークローの管理(Manage Workflows)】画面で【インポート(Import)】をクリックします。【スクリプトのインポート(Import Scripts)】ダイアログボックスが表示されます。【スクリプトのインポート(Import Scripts)】ダイアログボックスでは、次の操作を実行できます。
 - ファイル名を入力します。
 - クリックしてファイルを参照し、拡張子が usr のファイルを見つけます。ファイルタイプのドロップダウンから **Micro Focus Unified Functional Testing** を選択し、ファイルに移動します。
 - 【編集(Edit)】をクリックして、Micro Focus Unified Functional Testing アプリケーションを起動します。
- (オプション) 【スクリプトのインポート(Import Scripts)】ダイアログボックスでは、次のいずれかのオプションを選択できます。
 - インポート中に Micro Focus Unified Functional Testing UI を表示する(Show Micro Focus Unified Functional Testing UI during import)
 - インポート後にスクリプトの結果を開く(Open script result after import)

6. インポートするファイルを選択し、[インポート(Import)]をクリックします。ファイルが正常にインポートされると、そのファイルが[ワークフロー(Workflows)]テーブルに表示されます。
7. [ワークフロー(Workflows)]テーブルから次のいずれかを選択します。
 - **記録(Record)** - Web Macro Recorderを起動します。詳細については、『Micro Focus Fortify WebInspect Tools Guide』の「Web Macro Recorder」の章を参照してください。
 - **編集(Edit)** - Web Macro Recorderを使用してファイルを変更できます。『Micro Focus Fortify WebInspect Tools Guide』の「Web Macro Recorder」の章を参照してください。
 - **削除(Delete)** - [ワークフロー(Workflows)]テーブルからスクリプトを削除します。
 - **インポート(Import)** - 別のファイルをインポートします。
 - **エクスポート(Export)** - 指定した名前と場所を使用して.webmacro形式でファイルを保存します。
8. [次へ(Next)]ボタンをクリックします。

最初の usrスクリプトファイルがリストに追加されると、その名前(またはデフォルト名)が[ワークフロー(Workflows)]テーブルに表示され、[許可ホスト(Allowed Hosts)]テーブルがペインに追加されます。

別の usrスクリプトファイルを追加すると、許可ホストがさらに追加されます。有効になっているホストは、このホストが追加されたワークフロー usrファイルだけでなく、一覧にされているすべてのワークフロー usrスクリプトファイルに対して使用可能になります。ガイド付きスキャンでは、対応するチェックボックスがオンであるかどうかに関係なく、一覧にされているすべてのワークフローファイルが再生成され、一覧にされているすべての許可ホストに対して要求が行われます。許可ホストのチェックボックスがオフになっている場合、Fortify WebInspectはそのホストからの応答をWeb探索または監査します。チェックボックスがオフの場合、Fortify WebInspectは、そのホストからの応答をWeb探索または監査しません。また、特定のワークフロー usrスクリプトでパラメータが使用されている場合は、そのワークフローマクロがリストで選択されると、[マクロパラメータ(Macro Parameters)]テーブルが表示されます。必要に応じてパラメータの値を編集します。
9. [ワークフロー(Workflows)]テーブルの変更または追加が完了したら、ガイド付きスキャン ウィザードで次に進み、設定を完了してスキャンを実行します。新しいログインマクロの記録または既存のログインマクロの使用の詳細については、『Micro Focus Fortify WebInspect Tools Guide』の「Web Macro Recorder」の章を参照してください。

次も参照

["ガイド付きスキャンの概要" ページ116](#)

モバイルスキャンテンプレートの使用

モバイルスキャンテンプレートを使用してモバイルWebサイトスキャンを作成すると、Fortify WebInspectまたはFortify WebInspect Enterprise内から、デスクトップバージョンのブラウザを使用してWebサイトのモバイルバージョンをスキャンできます。

モバイルスキャンは、Webサイトスキャンとほぼ同じであり、事前定義テンプレートの1つを使用して標準、徹底、またはクイックスキャンを実行するときに検出する設定オプションを反映します。唯一の違いは、ブラウザでモバイルブラウザをエミュレートできるようにするためにユーザエージェントヘッダを選択する必要がある点です。

Fortify WebInspectおよびFortify WebInspect Enterpriseには4つのモバイルユーザエージェントのオプションがあり、その中から選択することができますが、カスタムオプションを作成することができます。別のバージョンのAndroid、Windows Phone、または他のモバイルデバイス用のユーザエージェントを作成することができます。ユーザエージェントヘッダの作成については、「["カスタムユーザエージェントヘッダの作成"次のページ](#)」を参照してください。

重要! SQL Expressデータベースを使用して複数のスキャンを実行する場合、SQL Expressの制限が原因で期待する結果を得られないことがあります。そのため、SQL Expressを使用するインストールでは、同時(または並行)スキャンの実行をお勧めしません。

モバイルスキャンの起動

モバイルスキャンを起動するには:

1. ガイド付きスキャンを開始します。
 - a. Fortify WebInspectの場合は、Fortify WebInspectの「開始ページ(Start page)」で、[ガイド付きスキャンの開始(Start a Guided Scan)]をクリックします。
 - b. Fortify WebInspect Enterpriseの場合は、Webコンソールの「アクション(Actions)」で[ガイド付きスキャン(Guided Scan)]をクリックします。
2. [モバイルテンプレート(Mobile Templates)]セクションで[モバイルスキャン(Mobile Scan)]を選択します。
3. ツールバーの[モバイルクライアント(Mobile Client)]アイコンをクリックします。
4. 使用するレンダリングエンジンを選択します。選択するレンダリングエンジンによって、ガイド付きスキャンの設定時に新しいマクロの記録または既存のマクロの編集を行うときに開かれるWeb Macro Recorderが決まります。レンダリングエンジンのオプションは次のとおりです。
 - **セッションベース(Session-based)** -このオプションを選択すると、セッションベースのWeb Macro Recorderが指定されます。これはInternet Explorerブラウザテクノロジを使用します。
 - **Macro Engine 6.1 (推奨) (Macro Engine 6.1 (recommended))** -このオプションを選択すると、Web Macro Recorder with Macro Engine 6.1が指定されます。これはTruClientテクノロジとFirefoxテクノロジを使用します。
5. レンダリングエンジンからサイトに提供するエージェント文字列を表すユーザエージェントを選択します。独自のユーザ文字列を作成した場合は、[カスタム(Custom)]として表示されます。ユーザエージェントがリストにない場合は、カスタムユーザエージェントを作成できます。「カスタムユーザエージェントヘッダの作成」を参照してください。

ガイド付きスキャンウィザードで[ネイティブモバイルステージ: Webサイトの検証(Native Mobile Stage: Verify Web Site)]の最初のステップが表示されます。

カスタムユーザエージェントヘッダの作成

Fortify WebInspectおよびFortify WebInspect Enterpriseには、Android、Windows、およびiOSデバイス用のユーザエージェントが含まれています。いずれかのオプションを使用する場合には、カスタムユーザエージェントヘッダを作成する必要はありません。Webブラウザに別のモバイルデバイスまたは特定のOSバージョンを名乗らせるには、カスタムユーザエージェントヘッダを作成します。

カスタムユーザエージェントを作成するには:

1. ガイド付きスキャンのツールバーで **詳細(Advanced)**]アイコンをクリックします。
 2. [スキャン設定(Scan Settings)]ウィンドウが表示されます。
 3. [スキャン設定(Scan settings)]列で、**クッキー/ヘッダ(Cookies/Headers)**]を選択します。
 4. 設定エリアの **カスタムヘッダの追加(Append Custom Headers)**]セクションで、User-Agent文字列をダブルクリックします。
[カスタムヘッダの指定(Specify Custom Header)]ボックスが表示されます。
 5. 「User-Agent:」と入力し、その後に目的のデバイスのユーザエージェントヘッダ文字列を入力します。
 6. [OK]をクリックします。
- これで、新しいカスタムユーザエージェントをモバイルクライアントとして選択できるようになりました。

サイトステージについて

サイトステージでは、次の操作を行います。

- スキャンするWebサイトの検証
- スキャンタイプの選択

Webサイトの検証

Webサイトを検証するには:

1. **開始URL(Start URL)**]ボックスで、スキャンするサイトの完全なURLまたはIPアドレスを入力または選択します。
URLを入力する場合は、正確に入力する必要があります。たとえば「MYCOMPANY.COM」と入力すると、Fortify WebInspectおよびFortify WebInspect EnterpriseはWWW.MYCOMPANY.COMなどのバリエーションはスキャンしません(許可ホスト(Allowed Hosts)]設定で代替URLを指定している場合を除く)。
無効なURLまたはIPアドレスを指定すると、エラーが発生します。階層ツリー内の特定の位置からスキャンを実行する場合は、スキャンの開始点(<http://www.myserver.com/myapplication/>など)を追加します。

IPアドレスによるスキャンでは、(相対パスではなく)完全修飾URLを使用するリンクを追跡しません。

Fortify WebInspectおよびFortify WebInspect Enterpriseでは、IPv4 (Internet Protocol バージョン4)とIPv6 (Internet Protocol バージョン6)の両方がサポートされています。IPv6 アドレスは括弧で囲む必要があります。

メモ: Fortify WebInspectでは、WebサイトスキャンおよびWebサービススキャンでIPv6 (Internet Protocol バージョン6)アドレスがサポートされています。開始URLを指定する場合は、IPv6アドレスを括弧で囲む必要があります。次に例を示します。

- `http://[::1]`
Fortify WebInspectは「localhost」をスキャンします。
- `http://[fe80::20c:29ff:fe32:bae1]/subfolder/`
Fortify WebInspectは、指定されたアドレスのホストのスキャンを「subfolder」ディレクトリから開始します。
- `http://[fe80::20c:29ff:fe32:bae1]:8080/subfolder/`
Fortify WebInspectは、ポート8080で実行されているサーバのスキャンを「subfolder」から開始します。

2. (オプション)スキャン範囲を特定のエリアに限定するには、「**フォルダに限定 (Restrict to Folder)**」チェックボックスをオンにし、リストから次のいずれかのオプションを選択します。

- **ディレクトリのみ(自己) (Directory only (self))**。Fortify WebInspectおよびFortify WebInspect Enterpriseは、指定されたURLのみをWeb探索または監査(またはその両方)します。たとえば、このオプションを選択して`www.mycompany/one/two/`というURLを指定すると、Fortify WebInspectおよびFortify WebInspect Enterpriseは「two」ディレクトリのみを評価します。
- **ディレクトリおよびサブディレクトリ(Directory and subdirectories)**。Fortify WebInspectおよびFortify WebInspect Enterpriseは、指定されたURLでWeb探索または監査(またはその両方)を開始しますが、ディレクトリツリーでそれよりも上位のディレクトリにはアクセスしません。
- **ディレクトリおよび親ディレクトリ(Directory and parent directories)**。Fortify WebInspectおよびFortify WebInspect Enterpriseは、指定されたURLでWeb探索または監査(またはその両方)を開始しますが、ディレクトリツリーでそれよりも下位のディレクトリにはアクセスしません。

「**フォルダに限定 (Restrict to folder)**」スキャンオプションの制限については、「[「**フォルダに限定**」に関する制限](#)」ページ202を参照してください。

3. **検証(Verify)**をクリックします。

Webサイトが、共通アクセスカード(CAC)を使用してクライアント証明書で認証するように設定されている場合、ガイド付きスキャンでは次のメッセージが表示されます。

サイト <URL> がクライアント証明書を要求しています。今すぐ設定しますか? (The site <URL> is requesting a client certificate. Would you like to configure one now?)

CACを使用してクライアント証明書を設定するには:

- a. [はい(Yes)]をクリックします。
クライアント証明書の選択(Select a Client Certificate)]ウィンドウが表示されます。
- b. 証明書ストア(Certificate Store)]で、**現在のユーザ(Current User)**]を選択します。
使用可能な証明書のリストが 証明書(Certificate)]エリアに表示されます。
- c. 「(SmartCard)」というプレフィックスが付いた証明書を見つけて選択します。
証明書の詳細とPINフィールドが、 証明書情報(Certificate Information)]エリアに表示されます。
- d. PINが必要な場合は PIN]フィールドにCACのPINを入力し、 **テスト(Test)**]をクリックします。

メモ: PINが必要な場合に、この時点でPINを入力しないと、スキャン中にPINの入力を求められるたびに、Windowsの [セキュリティ] ウィンドウにPINを入力する必要があります。

4. プロキシサーバ経由でターゲットサイトにアクセスする必要がある場合は、メイン画面の左下にある **プロキシ(Proxy)**]をクリックして **プロキシ設定(Proxy Settings)**]エリアを表示し、 **プロキシ設定(Proxy Settings)**]リストからオプションを選択します。
 - **直接接続(プロキシ無効)(Direct Connection (proxy disabled))**
 - **プロキシ設定の自動検出(Auto detect proxy settings):** WPAD (Web Proxy Autodiscovery Protocol)を使用してプロキシ自動設定ファイルを見つけ、このファイルを使用してブラウザのWebプロキシ設定を行います。
 - **システムのプロキシ設定を使用する(Use System proxy settings):** ローカルマシンからプロキシサーバ情報をインポートします。
 - **Firefoxプロキシ設定を使用する(Use Firefox proxy settings):** Firefoxからプロキシサーバ情報をインポートします。
 - **PACファイルを使用してプロキシ設定を行う(Configure proxy settings using a PAC File):** PAC (Proxy Automatic Configuration)ファイルからプロキシ設定をロードします。このオプションを選択した場合は、**編集(Edit)**]をクリックしてPACの場所(URL)を入力します。
 - **プロキシを明示的に設定する(Explicitly configure proxy settings):** 指示に従ってプロキシサーバ設定を指定します。このオプションを選択した場合は、表示されるフィールドにプロキシ情報を入力します。

メモ: ブラウザのプロキシ設定を使用することにしても、プロキシサーバ経由のインターネットアクセスが保証されるわけではありません。Firefoxブラウザの接続設定が [プロキシーを使用しない]に設定されている場合、またはInternet Explorerの [LANにプロキシサーバを使用する]設定が選択されていない場合、プロキシサーバは使用されません。

Webサイトまたはディレクトリ構造のスクリーンショットが表示されたら、開始URLへの接続の検証が正常に完了しています。

5. [次へ(Next)]をクリックします。

[スキャンタイプの選択(Choose Scan Type)]ウィンドウが表示されます。

スキャンタイプの選択

1. [スキャン名(Scan Name)]ボックスにスキャンの名前を入力します。
2. 次のいずれかのスキャンタイプを選択します。
 - **標準(Standard)**: Fortify WebInspectおよびFortify WebInspect Enterpriseは自動分析を実行し、ターゲットURLから開始します。これは標準的なスキャン開始方法です。
 - **ワークフロー(Workflows)**: このオプションを選択すると、ガイド付きスキャンにワークフローステージが追加されます。
3. [スキャン方法(Scan Method)]エリアで、次のいずれかのスキャン方法を選択します。
 - **Web探索のみ(Crawl Only)**: このオプションを選択すると、サイトの階層データ構造が完全にマッピングされます。Web探索が完了したら、[監査(Audit)]をクリックしてアプリケーションの脆弱性を評価できます。
 - **Web探索および監査(Crawl and Audit)**: Fortify WebInspectおよびFortify Enterpriseは、サイトの階層データ構造をマッピングし、各リソース(ページ)を監査します。選択したデフォルト設定に応じて、各リソースの検出時またはサイト全体のWeb探索後に監査を実行できます。Web探索および監査の同時実行と順次実行の詳細については、「["Web探索および監査モード\(Crawl and Audit Mode\)" ページ371](#)」を参照してください。
 - **監査のみ(Audit Only)**: Fortify WebInspectおよびFortify WebInspect Enterpriseは、選択されたポリシーの手法を適用して脆弱性リスクを判断しますが、WebサイトのWeb探索は行いません。サイト上のリンクをたどることも評価することもありません。
4. [ポリシー(Policy)]エリアの[ポリシー(Policy)]リストからポリシーを選択します。ポリシーの管理については、『*Micro Focus Fortify WebInspect Tools Guide*』の「Policy Manager」の章を参照してください。
5. [Web探索のカバレッジ(Crawl Coverage)]エリアで、[Web探索のカバレッジ(Crawl Coverage)]スライダを使用してカバレッジのレベルを選択します。Web探索のカバレッジレベルの詳細については、「["カバレッジと徹底性" ページ185](#)」を参照してください。
6. [シングルページアプリケーション(Single-Page Applications)]エリアで、SPA (single-page application)のWeb探索および監査のオプションを選択します。有効にすると、DOMスクリプトエンジンは、Web探索中に、JavaScriptインクルード、フレームとiframeのインクルード、CSSファイルインクルード、およびAJAX呼び出しを検索してから、それらのイベントによって生成されたすべてのトラフィックを監査します。[シングルページアプリケーション(Single-Page Applications)]のオプションは次のとおりです。
 - **自動(Automatic)** - Fortify WebInspectがSPAフレームワークを検出すると、自動的にSPAサポートモードに切り替わります。

- **有効(Enabled)** - SPAフレームワークがターゲットアプリケーションで使用されていることを示します。

注意! SPAサポートは、シングルページアプリケーションに対してのみ有効にするべきです。SPAサポートを有効にしてSPA以外のWebサイトをスキャンすると、スキャンが遅くなります。

- **無効(Disabled)** - SPAフレームワークがターゲットアプリケーションで使用されていないことを示します。

詳細については、「["シングルページアプリケーションスキャンについて" ページ210](#)」を参照してください。

7. [次へ(Next)]ボタンをクリックします。

ログインステージが表示され、左側のペインでネットワーク認証が強調表示されます。

ログインステージについて

スキャンするアプリケーションにログイン資格情報が必要な場合は、ログインステージを使用して、既存のログインマクロを選択するか、スキャンで使用するログインマクロを記録できます。

アプリケーションにログイン資格情報が必要ない場合は、値を割り当てずに各オプションをクリックするか、ガイド付きスキャンツリーの「[アプリケーション(Application)]」をクリックして次のステージにスキップすることで、ガイド付きスキャンウィザードのこのセクションをスキップできます。

このステージでは、次の操作を実行できます。

- ネットワークの権限付与の設定
- アプリケーションの権限付与の設定
- ログインマクロの作成または割り当て

ネットワーク認証ステップ

アプリケーションでネットワークまたはアプリケーションレベルの認証が必要な場合は、ここで割り当てることができます。

ネットワーク認証の設定

ネットワークでユーザ認証が必要な場合は、ここで設定できます。ネットワークでユーザ認証が不要な場合は、[次へ(Next)]ナビゲーションボタン、またはガイド付きスキャンツリーの次の該当ステップをクリックして続行します。

ネットワーク認証を設定するには:

1. [ネットワーク認証(Network Authentication)] チェックボックスをクリックします。
2. 認証メソッドのドロップダウンリストから、メソッドを選択します。認証メソッドは次のとおりです。
 - ADFS CBT
 - 自動(Automatic)
 - 基本(Basic)
 - ダイジェスト(Digest)
 - Kerberos
 - ネゴシエート(Negotiate)
 - NT LAN Manager (NTLM)
3. ネットワーク認証にクライアント証明書を使用するには、[クライアント証明書(Client Certificate)]を選択します。

メモ: クライアント証明書をWindowsフォンに追加できますが、後でその証明書を削除するには、Windowsフォンをデフォルト設定に戻すしかありません。
4. [証明書ストア(Certificate Store)] エリアで、次のいずれかを選択してから、[マイ(My)] または [ルート(Root)] ラジオボタンを選択します。
 - [ローカルマシン(Local Machine)]。Fortify WebInspectは、証明書ストア(Certificate Store)] エリアで選択した内容に基づいて、ローカルマシン上の証明書を使用します。
 - [現在のユーザー(Current User)]。Fortify WebInspectは、証明書ストア(Certificate Store)] エリアで選択した内容に基づいて、現在のユーザーの証明書を使用します。
5. [証明書情報(Certificate Information)] エリアに証明書の詳細を表示するには、証明書を選択します。
6. [次へ(Next)] ボタンをクリックします。

[アプリケーション認証(Application Authentication)] ページが表示されます。

アプリケーション認証のステップ

サイトで認証が必要な場合は、このステップを使用してログインマクロを作成、選択、または編集することにより、ログインプロセスを自動化してサイトのカバレッジを拡大できます。ログインマクロは、アプリケーションにアクセスしてログインするために必要なアクティビティの記録です。通常は、ユーザ名とパスワードを入力し、[ログイン] や [ログオン]などのボタンをクリックします。

ログインマクロを使用するスキャンの [スキャン設定: 認証(Scan Settings: Authentication)] で [マクロ検証を有効にする(Enable macro validation)] が選択されている場合、Fortify WebInspectはスキャンの開始時点でログインマクロをテストして、ログインが成功したことを確認します。マクロが無効で、アプリケーションへのログインに失敗した場合、スキャンは停止し、

エラーメッセージがスキャンログファイルに書き込まれます。詳細とトラブルシューティングのヒントについては、「["ログインマクロのテスト" ページ510](#)」を参照してください。

重要! 2要素認証を含むマクロを使用する場合は、スキャンを開始する前に、2要素認証アプリケーションの設定を行う必要があります。詳細については、「["アプリケーション設定: 2要素認証" ページ453](#)」を参照してください。

ログインマクロでは、次のオプションを使用できます。

- ・ "権限のエスカレーションなしでログインマクロを使用する(Using a Login Macro without Privilege Escalation)" 下
- ・ "権限のエスカレーションのためにログインマクロを使用する(Using Login Macros for Privilege Escalation)" 次のページ
- ・ "Fortify WebInspect Enterpriseに接続した際にログインマクロを使用する(Using a Login Macro when Connected to Fortify WebInspect Enterprise)" ページ145

マスクされた値のサポート

Web Macro Recorderで値がマスクされたパラメータがマクロで使用されている場合、Fortify WebInspectでガイド付きスキャンを設定するときにも、それらの値はマスクされます。

権限のエスカレーションなしでログインマクロを使用する(Using a Login Macro without Privilege Escalation)

ログインマクロを使用するには:

1. **【このサイトでログインマクロを使用する(Use a login macro for this site)】** チェックボックスをオンにします。
2. 次のいずれかを実行します。
 - ・ 事前に記録されたログインマクロを使用するには、省略記号ボタン([...])をクリックして、保存されているマクロを参照します。
 - ・ **【ログインマクロ(Login Macro)】** フィールドに表示されている既存のログインマクロを編集するには、**【編集(Edit)】**をクリックします。
 - ・ 新しいマクロを記録するには、**【作成(Create)】**をクリックします。

新しいログインマクロの記録や既存のログインマクロの使用の詳細については、『*Micro Focus Fortify WebInspect Tools Guide*』の「Web Macro Recorder」の章を参照してください。

3. **【次へ(Next)】** ボタンをクリックします。

標準スキャンを選択した場合は、**【最適化タスク(Optimization Tasks)】** ページが表示されます。ワークフロースキャンを選択した場合は、**【ワークフローの管理(Manage Workflows)】** ページが表示されます。

権限のエスカレーションのためにログインマクロを使用する(Using Login Macros for Privilege Escalation)

権限のエスカレーションポリシーか、有効な権限のエスカレーションチェックを含む別のポリシーを選択した場合、高い権限を持つユーザーアカウント用のログインマクロが少なくとも1つ必要です。詳細については、「["権限のエスカレーションスキャンについて" ページ207](#)」を参照してください。

ログインマクロを使用するには:

1. **高い権限のユーザーアカウントログインマクロ(High-Privilege User Account Login Macro)** チェックボックスをオンにします。このログインマクロは、サイト管理者やモデレータアカウントなど、より高い権限を持つユーザーアカウント用です。
2. 次のいずれかを実行します。
 - 事前に記録されたログインマクロを使用するには、省略記号ボタン([...])をクリックして、保存されているマクロを参照します。
 - ログインマクロ(Login Macro) フィールドに表示されている既存のログインマクロを編集するには、**編集(Edit)**をクリックします。
 - 新しいマクロを記録するには、**作成(Create)**をクリックします。

新しいログインマクロの記録や既存のログインマクロの使用の詳細については、『*Micro Focus Fortify WebInspect Tools Guide*』の「Web Macro Recorder」の章を参照してください。

最初のマクロを記録または選択して 次へ(Next)の矢印をクリックすると、**低い権限のログインマクロを設定する(Configure Low Privilege Login Macro)** プロンプトが表示されます。

3. 次のいずれかを実行します。
 - 認証モードでスキャンを実行するには、**はい(Yes)**をクリックします。詳細については、「["権限のエスカレーションスキャンについて" ページ207](#)」を参照してください。ガイド付きスキャンが「ログインマクロの選択(Select Login Macro)」ウィンドウに戻り、低い権限のログインマクロを作成または選択できるようになります。ステップ4に進みます。
 - スキャンを非認証モードで実行するには、**いいえ(No)**をクリックします。詳細については、「["権限のエスカレーションスキャンについて" ページ207](#)」を参照してください。アプリケーション認証のステップが完了しました。標準スキャンを選択した場合は、**最適化タスク(Optimization Tasks)** ページが表示されます。ワークフロースキャンを選択した場合は、**ワークフローの管理(Manage Workflows)** ページが表示されます。
4. **低い権限のユーザーアカウントログインマクロ(Low-Privilege User Account Login Macro)** チェックボックスをオンにします。このログインマクロは、サイトコンテンツのビューアやコンシューマなど、低い権限のユーザーアカウント用です。

5. 次のいずれかを実行します。

- 事前に記録されたログインマクロを使用するには、省略記号ボタン([...])をクリックして、保存されているマクロを参照します。
- 【ログインマクロ(Login Macro)】フィールドに表示されている既存のログインマクロを編集するには、【編集(Edit)】をクリックします。
- 新しいマクロを記録するには、【作成(Create)】をクリックします。

新しいログインマクロの記録や既存のログインマクロの使用の詳細については、『*Micro Focus Fortify WebInspect Tools Guide*』の「Web Macro Recorder」の章を参照してください。

6. 2つ目のマクロを記録または選択した後、【次へ(Next)】ボタンをクリックします。

標準スキャンを選択した場合は、【最適化タスク(Optimization Tasks)】ページが表示されます。ワークフロースキャンを選択した場合は、【ワークフローの管理(Manage Workflows)】ページが表示されます。

Fortify WebInspect Enterpriseに接続した際にログインマクロを使用する(Using a Login Macro when Connected to Fortify WebInspect Enterprise)

Fortify WebInspect Enterpriseに接続されているFortify WebInspectの場合は、Fortify WebInspect Enterpriseマクロリポジトリからログインマクロをダウンロードして使用できます。

マクロをダウンロードするには:

- 【このサイトでログインマクロを使用する(Use a login macro for this site)】チェックボックスをオンにします。
- 【ダウンロード(Download)】をクリックします。
【Fortify WebInspect Enterpriseからマクロをダウンロードする(Download a Macro from Fortify WebInspect Enterprise)】ウィンドウが表示されます。
- ドロップダウンリストから【アプリケーション(Application)】と【バージョン(Version)】を選択します。
- 【マクロ(Macro)】ドロップダウンリストからリポジトリマクロを選択します。
- 【OK】をクリックします。

メモ: リポジトリマクロを選択すると、【最終確認(Final Review)】ページの【自動でスキャンをWIEにアップロードする(Automatically Upload Scan to WIE)】の【アプリケーション(Application)】と【バージョン(Version)】が自動的に同期されます。

ログインマクロを自動で作成する

ユーザ名とパスワードを入力して、Fortify WebInspectでログインマクロを自動的に作成できます。

メモ: 権限のエスカレーションおよびマルチユーザログインスキャンに対して、また、セッションベースのレンダリングエンジンを使用するスキャンに対して自動でログインマクロを作成することはできません。

ログインマクロを自動的に作成するには:

1. [ログインマクロの自動生成(Auto-gen Login Macro)]を選択します。
2. [ユーザ名(Username)]フィールドにユーザ名を入力します。
3. [パスワード>Password)]フィールドにパスワードを入力します。

オプションで、[テスト(Test)]をクリックして、ログインフォームの検索、マクロの生成、マクロ検証テストの実行を行ってから、ガイド付きスキャンウィザードの次のステージに進みます。完了前に検証テストをキャンセルする必要がある場合は、[キャンセル(Cancel)]をクリックします。

重要! ワークフローステージまたはガイド付きスキャンの拡張カバレッジ(Enhanced Coverage)タスクで自動的に生成されたマクロを使用するには、[テスト(Test)]をクリックしてマクロを生成する必要があります。

マクロが無効で、アプリケーションへのログインが失敗すると、エラーメッセージが表示されます。詳細とトラブルシューティングのヒントについては、「["ログインマクロのテスト" ページ510](#)」を参照してください。

ワークフローステージについて

ワークフローステージは、サイトステージで[スキャンタイプ(Scan Type)]として[ワークフロー(Workflows)]を選択した場合にのみ表示されます。[標準(Standard)]を選択した場合、ワークフローステージは表示されません。

ワークフローマクロを作成すると、マクロで指定したページをFortify WebInspectで確実に監査できます。Fortify WebInspectはマクロに含まれているURLのみを監査し、監査中に検出されたハイパーアリンクはたどりません。

サイトのユースケースごとに1つずつ、複数のワークフローマクロを作成できます。ログアウト署名は不要です。この種のマクロは、アプリケーションの特定のサブセクションに焦点を当てるために最もよく使用されます。複数のマクロを選択すると、すべてのマクロが同一路由に含まれます。複数のマクロを選択できるほかに、Burp Proxyキャプチャをインポートしてスキャンに追加することもできます。

重要! ログインマクロを、ワークフローマクロまたは起動マクロ、あるいはその両方と組み合わせて使用する場合、すべてのマクロは同じ種類である必要があります。すべてが.webmacroファイルであるか、すべてがBurp Proxyキャプチャであるかのどちらかです。同じスキャンで異なる種類のマクロを使用することはできません。

ワークフローの設定を完了するには、[ワークフロー(Workflow)]テーブルで次のいずれかをクリックします。

- [記録(Record)]。Web Macro Recorderが開き、マクロを作成できます。
- [編集(Edit)]。Web Macro Recorderが開き、選択したマクロがロードされます。
- [削除>Delete)]。選択したマクロが削除されます(ただしディスクからは削除されません)。
- [インポート(Import)]。標準のファイル選択ウィンドウが開き、以前に記録した.webmacroファイルまたはBurp Proxyキャプチャを選択できます。

メモ: コンピュータにMicro Focus UFT (Unified Functional Testing)がインストールされている場合は、Fortify WebInspectがこれを自動的に検出し、UFT .usrファイルをインポートするためのオプションが表示されます。

詳細については、「["ガイド付きスキャンでのMicro Focus UFT \(Unified Functional Testing\)ファイルのインポート" ページ153](#)」を参照してください。

- 記録したマクロをエクスポートします。マクロを選択または記録した後で、許可ホストを必要に応じて指定できます。標準のファイル選択ウィンドウが開き、記録したマクロを保存できます。

ワークフローマクロを指定して再生すると、[ワークフロー(Workflows)]テーブルにそのマクロが表示され、許可ホストが [ガイド付きスキャン\(Guided Scan\)](#)]> [ワークフロー(Workflows)]> [ワークフロー(Workflows)]> [マネージャワークフロー(Manager Workflow)]ページに追加されます。特定のホストへのアクセスを有効または無効にできます。詳細については、「["スキャン設定: 許可ホスト" ページ389](#)」を参照してください。

Burp Proxy結果の追加

Burp Proxyセキュリティテストを実行した場合、テスト中に収集されたトラフィックをワークフローマクロにインポートできます。これにより、同じエリアの再スキャンにかかる時間が短縮されます。

Burp Proxy結果の追加

ワークフローマクロにBurp Proxy結果を追加するには:

- [ワークフロー(Workflows)]画面が表示されていない場合は、[ガイド付きスキャン\(Guided Scan\)](#)ツリーの [ワークフローの管理(Manage Workflows)]ステップをクリックします。
- [インポート(Import)]ボタンをクリックします。
[マクロのインポート(Import Macro)]ファイルセレクタが表示されます。
- ファイルの種類ボックスのフィルタを [Webマクロ(*.webmacro)(Web Macro (*.webmacro))]から [Burp Proxy (*.*)]に変更します。
- Burp Proxyファイルに移動し、目的のファイルを選択します。
- [開く(Open)]をクリックします。

アクティブラーニングステージについて

アクティブラーニングステージでは次の操作が実行されます。

- WebInspect Profilerが実行され、設定を変更する必要があるかどうかが確認されます。
- 必要に応じてスキャン最適化オプションを設定します。

Profilerの使用

WebInspect Profilerは、ターゲットWebサイトの事前テストを実行し、特定の設定を変更すべきかどうかを判断します。変更が必要だと思われる場合、Profilerは提案のリストを返します。これらの提案は、受け入れることも拒否することもできます。

たとえば、Profilerは、サイトに入るために権限付与が必要であるものの、有効なユーザ名とパスワードが指定されていないことを検出するかもしれません。そのままスキャンを続行して著しく質の低い結果を得るのではなく、Profilerの提案に従って、続行する前に必要な情報を設定することができます。

同様に、設定では、Fortify WebInspectが「ファイルが見つからない」の検出を実行しないように指定されていることもあります。このプロセスは、存在しないリソースをクライアントから要求されてもステータス「404 Not Found」を返さないWebサイトで役に立ちます(代わりにステータス「200 OK」が返される場合がありますが、応答にはファイルが見つからないというメッセージが含まれます)。Profilerは、このような手法がターゲットサイトに実装されていると判断した場合、この特徴に対応できるようにFortify WebInspect設定を変更することを推奨します。

Profilerを起動するには:

1. 「プロファイル(Profile)」をクリックします。

Profilerが実行されます。詳細については、「["Server Profiler" ページ256](#)」を参照してください。

結果は、「**設定(Settings)**」セクションの「**スキャンの最適化(Optimize scan for)**」ボックスに表示されます。

2. 必要に応じて、要求された情報を入力します。
3. 「**次へ(Next)**」ボタンをクリックします。

Profilerを実行していない場合でも、いくつかのオプションが表示されることがあります。これについては、以降のセクションで説明します。

Webフォームの自動入力(Autofill Web Forms)

Fortify WebInspectがターゲットサイトのスキャン中に検出されるフォームの入力コントロールの値を送信するようにするには、「**Web探索時のWebフォームの自動入力(Auto-fill Web forms during crawl)**」を選択します。Fortify WebInspectは、事前パッケージ化されたデフォルトファイル、またはWeb Form Editorを使用して作成したファイルから値を抽出します。『*Micro Focus Fortify WebInspect Tools Guide*』の「**Web Form Editor**」の章を参照してください。以下を実行できます。

1. ブラウザボタンをクリックして、ファイルを見つけてロードします。
2. 「**編集(Edit)**」をクリックして、選択したファイル(またはデフォルト値)をWeb Form Editorで編集します。
3. 「**作成(Create)**」をクリックしてWeb Form Editorを開き、ファイルを作成します。

許可ホストの追加(Add Allowed Hosts)

「**許可ホスト(Allowed Host)**」設定は、Web探索して監査するドメインを追加する場合に使用します。Webプレゼンスで複数のドメインが使用されている場合は、それらのドメインをここ

に追加します。詳細については、「["スキャン設定: 許可ホスト" ページ389](#)」を参照してください。

許可するドメインを追加するには:

1. **追加(Add)**]をクリックします。
2. **許可ホストの指定(Specify Allowed Host)**]ウィンドウで、URL (またはURLを表す正規表現)を入力し、**OK**]をクリックします。

識別された誤検出を再利用する(Reuse Identified False Positives)

誤検出に変更された脆弱性を含むスキャンを選択します。このスキャンで検出された脆弱性がこれらの誤検出と一致する場合、脆弱性は誤検出に変更されます。詳細については、「["誤検出\(False Positives\)" ページ89](#)」を参照してください。

識別された誤検出を再利用するには:

1. **誤検出のインポート(Import False Positives)**]を選択します。
2. **スキャンの選択(Select scans)**]をクリックします。
3. 現在スキャンしている同じサイトからの誤検出を含むスキャンを1つ以上選択します。
4. **OK**]をクリックします。

サンプルマクロの適用(Apply Sample Macro)

Fortify WebInspectのサンプルバシキングアプリケーション(zero.webappsecurity.com)では、Webフォームログインが使用されています。このサイトをスキャンする場合は、**サンプルマクロの適用(Apply sample macro)**]を選択して、ログインスクリプトを含む事前パッケージ化されたマクロを実行します。

トラフィック分析(Traffic Analysis)

Web Proxyツールを使用してFortifyにより発行されたHTTP要求とターゲットサーバから返された応答を検査するには、**Web Proxyの起動およびWeb Proxy経由でのトラフィックの送信(Launch and Direct Traffic through Web Proxy)**]を選択します。

Fortify WebInspectはWebサイトのスキャン中に、Webサイトの階層構造を明らかにするセッションと、脆弱性が検出されたセッションのみをナビゲーションペインに表示します。ただし **Traffic Monitorを有効にする(Enable Traffic Monitor)**]を選択すると、Fortify WebInspectでは **Traffic Monitor**]ボタンが **スキャン情報(Scan Info)**]パネルに追加されます。これにより、Fortify WebInspectが送信した各HTTP要求と、サーバから受信した関連HTTP応答を表示して確認できます。

メッセージ

Profilerが変更を推奨しない場合は、ガイド付きスキャンウィザードに「設定の変更は推奨されません。現在のスキャン設定はこのサイトに最適です。(No settings changes are recommended. Your current scan settings are optimal for this site.)」というメッセージが表示されます。

次へ(Next)]をクリックします。

最終確認(Final Review)]ページが表示され、左側のペインで **詳細オプションの設定(Configure Detailed Options)**]が強調表示されます。

設定ステージについて

詳細オプションを設定するには、次の設定を指定します。

識別された誤検出を再利用する(Reuse Identified False Positives)

Fortify WebInspectによってすでに識別されている誤検出を再利用するには、**誤検出(False Positives)**]ボックスをオンにします。

トラフィック分析(Traffic Analysis)

1. Web Proxyツールを使用するには、[Web Proxyの起動およびWeb Proxy経由でのトラフィックの送信(Launch and Direct Traffic through Web Proxy)]を選択して、Fortify WebInspectが発行したHTTP要求と、ターゲットサーバから返された応答を調べます。

Web Proxyはスタンドアロンの自己完結型プロキシサーバであり、デスクトップ上で設定および実行できます。Web Proxyを使用すると、スキヤナ、Webブラウザ、またはHTTP要求を送信してサーバから応答を受信するその他のツールからのトラフィックを監視できます。Web Proxyは、デバッグと侵入スキャンのためのツールです。サイトのブラウズ中に、すべての要求とサーバの応答を確認できます。

2. Fortify WebInspectによって送信された各HTTP要求と、サーバから受信した関連HTTP応答を表示および確認するには、[Traffic Monitor]ボックスを選択します。

Fortify WebInspectはWebサイトのスキャン中に、Webサイトの階層構造を明らかにしたセッションと、脆弱性が検出されたセッションのみを表示します。ただし [Traffic Monitorを有効にする(Enable Traffic Monitor)]を選択すると、Fortify WebInspectではFortify WebInspectが送信した各HTTP要求と、サーバから受信した関連HTTP応答を表示して確認できます。

3. 次へ(Next)]をクリックします。

設定の検証とスキャンの開始(Validate Settings and Start Scan)]ページが表示され、左側のペインで 詳細オプションの設定(Configure Detailed Options)]が強調表示されます。

設定の検証とスキャンの開始(Validate Settings and Start Scan)

このページのオプションを使用すると、現在のスキャン設定を保存することができます。また、WebInspectがWebInspect Enterpriseと統合されている場合は、WebInspect Enterpriseとやり取りすることができます。

1. スキャン設定をXMLファイルとして保存するには、[ここをクリックして設定を保存する(Click here to save settings)]を選択します。標準の [名前を付けて保存(Save as)] ウィンドウを使用して、ファイルに名前を付けて保存します。
2. WebInspectがWebInspect Enterpriseと統合されている場合は、ツールバーに [テンプレート(Templates)] セクションが表示されます。次の表の説明に従って操作を進めます。

| 目的の作業 | その場合の手順 |
|---------------------|------------------|
| 現在のスキャン設定をテンプレートとして | a. 次のいずれかを実行します。 |

| 目的の作業 | その場合の手順 |
|---|--|
| <p>WebInspect Enterpriseデータベースに保存する</p> <p>メモ: 既存のテンプレートを編集する場合、[保存(Save)]を実行すると、実際には更新が行われます。設定の編集を保存したり、テンプレート名を変更したりすることができます。ただし、アプリケーション、バージョン、またはグローバルテンプレートの設定は変更できません。</p> | <ul style="list-style-type: none"> ◦ ツールバーの [テンプレート(Templates)]セクションで [保存(Save)]をクリックします。 ◦ [ここをクリックしてテンプレートを保存する(Click here to save template)]を選択します。 <p>[テンプレートの保存(Save Template)]ウィンドウが表示されます。</p> <ol style="list-style-type: none"> b. [アプリケーション(Application)]ドロップダウンリストからアプリケーションを選択します。 c. [バージョン-Version)]ドロップダウンリストからアプリケーションバージョンを選択します。 d. [テンプレート(Template)]フィールドに名前を入力します。 |
| <p>テンプレートからスキャン設定をロードする</p> | <ol style="list-style-type: none"> a. ツールバーの [テンプレート(Templates)]セクションで [ロード(Load)]をクリックします。 <p>現在のスキャン設定が失われるという確認メッセージが表示されます。</p> <ol style="list-style-type: none"> b. [はい(Yes)]をクリックします。 <p>[テンプレートのロード(Load Template)]ウィンドウが表示されます。</p> <ol style="list-style-type: none"> c. [アプリケーション(Application)]ドロップダウンリストからアプリケーションを選択します。 d. [バージョン-Version)]ドロップダウンリストからアプリケーションバージョンを選択します。 e. [テンプレート(Template)]ドロップダウンリストからテンプレートを選択します。 f. [ロード(Load)]をクリックします。 |

| 目的の作業 | その場合の手順 |
|-------|---|
| | ガイド付きスキャンがサイトステージに戻り、Webサイトの検証と、テンプレートからのステップごとの設定の実行が行えるようになります。 |

3. WebInspectがWebInspect Enterpriseと統合されている場合は、このページに [WebInspect Enterprise] セクションが表示されます。WebInspect Enterpriseを操作するには、次のようにします。
 - [アプリケーション(Application)] ドロップダウンリストからアプリケーションを選択します。
 - [バージョン(Version)] ドロップダウンリストからアプリケーションバージョンを選択します。
 - 次の表の説明に従って操作を進めます。

| スキャンの実行方法 | その場合の手順 |
|--------------------------------|---|
| WebInspect Enterpriseでセンサを使用する | <ol style="list-style-type: none"> [WebInspect Enterpriseで実行(Run in WebInspect Enterprise)]を選択します。 [センサ(Sensor)] ドロップダウンリストからセンサを選択します。 スキャンの [優先度(Priority)] を選択します。 |
| WebInspectで | <ol style="list-style-type: none"> [WebInspectで実行(Run in WebInspect)]を選択します。 スキャン結果をWebInspect Enterpriseの指定したアプリケーションおよびバージョンに自動的にアップロードする場合は、 [WebInspect Enterpriseへの自動アップロード(Auto Upload to WebInspect Enterprise)]を選択します。 <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> メモ: スキャンが正常に完了しない場合、WebInspect Enterpriseにはアップロードされません。 </div> |

4. [今すぐスキャン(Scan Now)] エリアでスキャン設定を見直し、[スキャンの開始(Start Scan)] をクリックしてスキャンを開始します。

ガイド付きスキャンでのMicro Focus UFT (Unified Functional Testing)ファイルのインポート

Micro Focus Unified Functional Testingアプリケーションがインストールされている場合、Fortify WebInspectがこのアプリケーションを検出し、ワークフロースキャンにUFTファイル(.usr)をインポートして、スキャンの完全性と攻撃露呈部分を拡張できるようにします。詳細については、Micro Focus Webサイトの「[Unified Functional Testing](#)」を参照してください。

UFT (.usr)ファイルをFortify WebInspect ガイド付きスキャンにインポートするには:

1. ガイド付きスキャンを起動し、[スキャンタイプ(Scan Type)]として [ワークフロースキャン (Workflows Scan)]を選択します。[ワークフロースキャン(Workflows scan)]オプションの下に、「Micro Focus Unified Functional Testingが検出されました(Micro Focus Unified Functional Testing has been detected)」という追加テキストが表示されます。スクリプトをインポートして、セキュリティテストの完全性を強化できます。
2. [次へ(Next)]ボタンをクリックします。
3. [認証(Authentication)]セクションで、[アプリケーション認証(Application Authentication)]が自動的に選択されます。指示に従ってフィールドに入力します。
4. [ワークフローの管理(Manage Workflows)]画面で [インポート(Import)]をクリックします。[スクリプトのインポート(Import Scripts)]ダイアログボックスが表示されます。[スクリプトのインポート(Import Scripts)]ダイアログボックスでは、次の操作を実行できます。
 - ファイル名を入力します。
 - クリックしてファイルを参照し、拡張子が usr のファイルを見つけます。ファイルタイプのドロップダウンから [Micro Focus Unified Functional Testing]を選択し、ファイルに移動します。
 - [編集(Edit)]をクリックして、Micro Focus Unified Functional Testing アプリケーションを起動します。
5. (オプション) [スクリプトのインポート(Import Scripts)]ダイアログボックスでは、次のいずれかのオプションを選択できます。
 - インポート中に Micro Focus Unified Functional Testing UI を表示する(Show Micro Focus Unified Functional Testing UI during import)
 - インポート後にスクリプトの結果を開く(Open script result after import)
6. インポートするファイルを選択し、[インポート(Import)]をクリックします。ファイルが正常にインポートされると、そのファイルが [ワークフロー(Workflows)] テーブルに表示されます。
7. [ワークフロー(Workflows)] テーブルから次のいずれかを選択します。
 - [記録(Record)] - Web Macro Recorderを起動します。詳細については、『*Micro Focus Fortify WebInspect Tools Guide*』の「Web Macro Recorder」の章を参照してください。
 - [編集(Edit)] - Web Macro Recorderを使用してファイルを変更できます。『*Micro Focus Fortify WebInspect Tools Guide*』の「Web Macro Recorder」の章を参照してください。

- 削除(Delete) - [ワークフロー(Workflows)]テーブルからスクリプトを削除します。
 - インポート(Import) -別のファイルをインポートします。
 - エクスポート(Export) -指定した名前と場所を使用して.webmacro形式でファイルを保存します。
8. [次へ(Next)]ボタンをクリックします。
- 最初の usrスクリプトファイルがリストに追加されると、その名前(またはデフォルト名)が [ワークフロー(Workflows)]テーブルに表示され、[許可ホスト(Allowed Hosts)]テーブルがペインに追加されます。
- 別の usrスクリプトファイルを追加すると、許可ホストがさらに追加されます。有効になっているホストは、このホストが追加されたワークフロー usrファイルだけでなく、一覧にされているすべてのワークフロー usrスクリプトファイルに対して使用可能になります。ガイド付きスキャンでは、対応するチェックボックスがオンであるかどうかに関係なく、一覧にされているすべてのワークフローファイルが再生され、一覧にされているすべての許可ホストに対して要求が行われます。許可ホストのチェックボックスがオンになっている場合、Fortify WebInspectはそのホストからの応答をWeb探索または監査します。チェックボックスがオフの場合、Fortify WebInspectは、そのホストからの応答をWeb探索または監査しません。また、特定のワークフロー usrスクリプトでパラメータが使用されている場合は、そのワークフローマクロがリストで選択されると、[マクロパラメータ(Macro Parameters)]テーブルが表示されます。必要に応じてパラメータの値を編集します。
9. [ワークフロー(Workflows)]テーブルの変更または追加が完了したら、ガイド付きスキャン ウィザードで次に進み、設定を完了してスキャンを実行します。新しいログインマクロの記録または既存のログインマクロの使用の詳細については、『Micro Focus Fortify WebInspect Tools Guide』の「Web Macro Recorder」の章を参照してください。

次も参照

["ガイド付きスキャンの概要" ページ116](#)

ネイティブスキャンテンプレートの使用

Fortify WebInspectおよびFortify WebInspect Enterpriseを使用して、AndroidまたはiOSのアプリまたはサービスで生成されたバックエンドトラフィックをスキャンできます。トラフィックは、Android、Windows、またはiOSデバイス上でアプリケーションを実行するか、AndroidまたはiOSエミュレータを介してソフトウェアを実行することで生成できます。

ガイド付きスキャン ウィザードでは、アプリケーションのバックエンドトラフィックのスキャンに必要なステージとステップを順に実行します。前のステップまたはステージに戻る必要がある場合は、[戻る] ナビゲーションボタンをクリックするか、ガイド付きスキャンツリー内のステップをクリックして、そこに直接移動します。

重要! SQL Expressデータベースを使用して複数のスキャンを実行する場合、SQL Expressの制限が原因で期待する結果を得られないことがあります。そのため、SQL Expressを使用するインストールでは、同時(または並行)スキャンの実行をお勧めしません。

モバイルデバイスのセットアップ

ネイティブスキャンの実行では、セキュリティ保護されたプロキシと連動するようにモバイルデバイスを設定する必要があります。この設定を行うには、以下の手順を実行する必要があります。

- モバイルデバイス/エミュレータプロキシのセットアップ(「[モバイルデバイスのプロキシアドレスの設定](#)」[ページ157](#)」を参照してください)
- 信頼された証明書のインストール(「[信頼された証明書の追加](#)」[ページ158](#)」を参照してください)

ガイド付きスキャンのステージ

モバイルテンプレートを使用したガイド付きスキャンは、4つまたは5つのステージで構成され、各ステージには1つ以上のステップが含まれています。これらのステージは次のとおりです。

ネイティブモバイル: デバイスまたはエミュレータを選択し、デバイスまたはエミュレータのプロキシを設定し、実行するスキャンのタイプを選択します。

ログイン: モバイルアプリケーションのバックエンドで必要な場合に認証のタイプを定義します。

アプリケーション: アプリを実行し、Webトラフィックを記録し、スキャンに含めるホストとRESTfulエンドポイントを特定します。

設定: 選択内容を確認して検証し、スキャンを実行します。

サポートされるデバイス

Fortify WebInspectおよびFortify WebInspect Enterpriseは、Android、Windows、およびiOSデバイス上のバックエンドトラフィックのスキャンをサポートしています。

Androidデバイスのサポート

Androidベースの携帯電話やタブレットなど、あらゆるAndroidデバイス。

Windowsデバイスのサポート

WindowsフォンやSurfaceタブレットなど、あらゆるWindowsデバイス。

iOSデバイスのサポート

iPhoneやiPadなど、最新バージョンのiOSを実行しているあらゆるiOSデバイス。

サポートされる開発エミュレータ

AndroidおよびiOSデバイスのサポートに加えて、お使いの開発環境でAndroidまたはiOSエミュレータを介してアプリケーションを実行できます。デバイスエミュレータを介して生成されたトラフィックをスキャンする場合、開発マシンがFortify WebInspectまたはFortify WebInspect

Enterpriseと同じネットワーク上に存在し、Fortify WebInspectまたはFortify WebInspect Enterpriseと開発マシンの間にプロキシが設定されていることを確認する必要があります。

ネイティブスキャンの起動

ネイティブスキャンを起動するには、デバイスまたはエミュレータがFortify WebInspectと同じネットワーク上にあることを確認する必要があります。また、プロキシ接続を正常に作成するためには、Fortify WebInspectを実行しているマシン上のポートに対する権限とアクセスが必要になります。

ネイティブスキャンを起動するには:

1. Fortify WebInspectまたはFortify WebInspect Enterpriseを開きます。
2. ガイド付きスキャンを開始します。
 - Fortify WebInspectの場合は、Fortify WebInspectの「開始ページ(Start page)」で、「ガイド付きスキャンの開始(Start a Guided Scan)」をクリックします。
 - Fortify WebInspect Enterpriseの場合は、Webコンソールの「アクション(Actions)」で、「ガイド付きスキャン(Guided Scan)」をクリックします。
3. 「モバイルテンプレート(Mobile Templates)」セクションで「ネイティブスキャン(Native Scan)」を選択します。
ガイド付きスキャンウィザードに、ネイティブモバイルステージの最初のステップである「デバイス/エミュレータの選択(Choose Device/Emulator)」が表示されます。

ネイティブモバイルステージについて

プロセスの最初のステージは、ネイティブモバイルステージです。このステージでは、次の操作を行います。

- プロキシ接続を使用するためにデバイスまたはエミュレータを設定します。
- Fortify WebInspectまたはFortify WebInspect Enterpriseのインスタンスと同じネットワークにデバイスまたはエミュレータをログオンさせます。
- デバイスまたはエミュレータにクライアント証明書をインストールします。
- 今後参照できるようにスキャンに名前を付けます。
- スキャン方法を選択します。
- スキャンポリシーを選択します。
- Web探索のカバレッジを選択します。

デバイス/エミュレータタイプの選択ステップ

ガイド付きスキャンを起動すると、次の表で説明するオプションが表示されます。

| オプション | 説明 |
|--|---|
| プロファイル(Profile) | スキャンするデバイスまたはエミュレータのタイプ。ドロップダウンメニューからタイプを選択します。詳細については、「 "プロファイルの選択" 下 」を参照してください。 |
| モバイルデバイス/エミュレータプロキシ (Mobile Device/Emulator Proxy) | デバイスまたはエミュレータとテスト対象のWebサービスまたはアプリケーション間のトラフィックをリスンするために、Fortify WebInspectまたはFortify WebInspect Enterpriseが作成するプロキシのIPアドレスとポート番号。IPアドレスまたはポート(あるいはその両方)が他のアクセティビティ用に予約されていない限り、デフォルト設定を使用します。詳細については、「 "モバイルデバイスのプロキシアドレスの設定" 下 」を参照してください。 |
| 信頼された証明書 (Trusted Certificate) | デバイスまたはエミュレータのクライアント証明書を取得するためのポートとURL。デバイスまたはエミュレータに証明書をダウンロードしてインストールするには、「 "信頼された証明書の追加" 次のページ 」を参照してください。 |

プロファイルの選択

デバイスプロファイルを設定するには、[プロファイル]ドロップダウンテキストボックスから次のいずれかを選択します。

- iOSデバイス(iOS Device) - 最新バージョンのiOSを実行しているiPadまたはiPhone。
- iOSシミュレータ(iOS Simulator) - iOS SDKの一部であるiOSエミュレータ。
- Androidデバイス(Android Device) - Androidオペレーティングシステムを実行している携帯電話またはタブレット。
- Androidエミュレータ(Android Emulator) - Android SDKの一部であるAndroidエミュレータ。
- Windowsデバイス(Windows Device) - WindowsフォンまたはSurfaceタブレット。

モバイルデバイスのプロキシアドレスの設定

[モバイルデバイス/エミュレータプロキシ(Mobile Device/Emulator Proxy)]セクションには、デバイスまたはエミュレータとFortify WebInspectまたはFortify WebInspect Enterprise間のプロキシ接続を確立するために使用されるホストIPアドレスとポート番号が一覧表示されます。システムでIPアドレスまたはポート番号が使用できない場合を除き、推奨される設定を使用します。

メモ: プロキシの設定後にサーバに接続できなかったりインターネットにアクセスできなかったりする場合は、ネイティブモバイルステージで指定されたファイアウォールのポートを開くか変更する必要がある場合があります。それでも機能しない場合は、別のIPアドレスの選択が必要になる可能性があります。Fortify WebInspect/WebInspect Enterpriseインターフェースに表示されるIPアドレスでは、アドレスをクリックすることで、ドロップダウンリストから代替アドレスを選択できます。

iOSデバイスでプロキシを設定するには:

1. [設定(Settings)]アプリケーションを実行します。
2. [Wi-Fi]を選択します。
3. Fortify WebInspectまたはFortify WebInspect Enterpriseへの接続に使用するWi-Fiネットワークを選択します。
4. [HTTPプロキシ(HTTP Proxy)]セクションまでスクロールダウンして、[手動(Manual)]を選択します。
この画面には、デバイスが接続されているネットワークのネットワーク設定オプションが表示されます。
5. さらに下にスクロールし、Fortify WebInspectまたはFortify WebInspect Enterpriseによって提供されるサーバのIPアドレスとポート番号を入力します。この情報が表示されない場合は、「["デバイスエミュレータタイプの選択ステップ"前のページ](#)」を参照してください。
6. Fortify WebInspectまたはFortify WebInspect Enterpriseで、[信頼された証明書(Trusted Certificate)]セクションの[検証(Verify)]ボタンをクリックし、接続が適切に動作していることを確認します。
[検証(Verify)]アクティビティの進行状況バーが表示されます。
7. デバイスでデフォルトのブラウザを起動して任意のサイトにアクセスし、Fortify WebInspectまたはFortify WebInspect Enterpriseがバックエンドトラフィックを認識できることを確認します。
すべてが正しく設定されている場合、しばらくすると、[検証(Verify)]アクティビティの進行状況バーにトラフィックが正常に検証されたことが示されます。
8. [OK]をクリックして検証の進行状況バーを閉じ、[次へ(Next)]をクリックしてスキャンタイプを選択します。

AndroidまたはWindowsデバイスでプロキシを設定するには、オペレータの指示に従ってください。

信頼された証明書の追加

サイトで安全な接続が必要な場合、スキャンを実行するたびに、Fortify WebInspectまたはFortify WebInspect Enterpriseはお使いのデバイスまたはエミュレータ用に固有のクライアント証明書を生成します。デバイス(またはエミュレータ)の証明書リポジトリに証明書をインストールする必要があります。

メモ: クライアント証明書をWindowsフォンに追加できますが、後でその証明書を削除するには、Windowsフォンをデフォルト設定に戻すしかありません。

証明書を追加するには、次の3つの方法があります。

- ガイド付きスキャンの [信頼された証明書(Trusted Certificate)] セクションからQRコードをスキャンします(QRリーダーソフトウェアが必要になります)。
- デバイスまたはデバイスエミュレータの組み込みブラウザにアドレスを入力します。
- 後で適用するために証明書をシステムクリップボードにコピーします(デバイスエミュレータでスキャンする場合に使用されます)。

ニーズに最適なオプションを選択します。

メモ: スキャンの完了後、デバイスのリポジトリから証明書を削除する必要があります。「["スキャン後のステップ" ページ169](#)」を参照してください。

iOSデバイスまたはエミュレータに証明書を追加するには:

- QRコードをスキャンするか、提供されたURLをブラウザに入力すると、[プロファイルのインストール(Install Profile)] ページが表示されます。

メモ: WebInspectルートの証明書のステータスは、これをルートチェーンに追加するまで、「信頼されていない(Not Trusted)」と表示されます。

- [インストール(Install)] ボタンをタップします。

証明書が信頼されていないことを示す警告画面が表示されます。デバイスまたはエミュレータの証明書リポジトリに証明書を追加すると、警告は表示されなくなります。

- [警告(Warning)] 画面で [インストール(Install)] をタップします。

表示が変更され、デバイスまたはエミュレータが接続されている現在のネットワークが表示されます。Fortify WebInspectまたはFortify WebInspect Enterpriseと同じネットワークに接続されていることを確認します。

スキャンタイプの選択ステップ

ネイティブモバイルステージの最初の部分でFortify WebInspectまたはFortify WebInspect Enterpriseで動作するデバイスまたはエミュレータを設定したら、実行するスキャンのタイプを選択する必要があります。

次の表の説明に従ってオプションを設定します。

| オプション | 説明 |
|-------------------------|---|
| スキャン名 (Scan Name) | 後で [スキャンの管理(Manage Scans)] ページでスキャンを識別できるように、スキャンの名前を入力します。 |
| スキャン方法 (Scan Method) | 次のリストから目的のスキャンのタイプを選択します。 <ul style="list-style-type: none"> Web探索のみ(Crawl Only): 指定したワークフローの攻撃露呈部分をマッピングします。 |

| オプション | 説明 |
|-----------------------------|---|
| | <ul style="list-style-type: none"> Web探索および監査(Crawl and Audit):指定したワークフローの攻撃露呈部分をマッピングし、脆弱性をスキャンします。 監査のみ(Audit Only): 指定したワークフローの攻撃のみ行います。 |
| ポリシー | ドロップダウンメニューからスキャンのポリシーを選択します。ポリシーの詳細については、「 "Fortify WebInspectのポリシー" ページ473 」を参照してください。ポリシーの作成と編集の詳細については、『 <i>Micro Focus Fortify WebInspect Tools Guide</i> 』の「Policy Manager」の章を参照してください。 |
| Web探索のカバレッジ(Crawl Coverage) | 「Web探索のカバレッジ(Crawl Coverage)」スライダを使用して、カバレッジのレベルを選択します。 |

ログインステージについて

スキャンするアプリケーションにログイン資格情報が必要な場合は、ログインステージを使用して、既存のログインマクロを選択するか、スキャンで使用するログインマクロを記録できます。

アプリケーションにログイン資格情報が必要ない場合は、値を割り当てずに各オプションをクリックするか、ガイド付きスキャンツリーの次のステップをクリックして次のステージにスキップすることで、ガイド付きスキャンウィザードのこのセクションをスキップできます。

このステージでは、次の操作を実行できます。

- ネットワークの権限付与の設定
- アプリケーションの権限付与の設定
- ログインマクロの作成または割り当て

ネットワーク認証ステップ

アプリケーションでネットワークまたはアプリケーションレベルの認証が必要な場合は、ここで割り当てることができます。

ネットワーク認証の設定

ネットワークでユーザ認証が必要な場合は、ここで設定できます。ネットワークでユーザ認証が不要な場合は、次へ(Next)】ナビゲーションボタン、またはガイド付きスキャンツリーの次の該当ステップをクリックして続行します。

ネットワーク認証を設定するには:

1. [ネットワーク認証(Network Authentication)] チェックボックスをクリックします。
2. 認証メソッドのドロップダウンリストから、メソッドを選択します。認証メソッドは次のとおりです。
 - ADFS CBT
 - 自動
 - 基本(Basic)
 - ダイジェスト(Digest)
 - Kerberos
 - ネゴシエート(Negotiate)
 - NT LAN Manager (NTLM)
3. [ユーザ名(User Name)]と[パスワード>Password)]に入力します。

クライアント証明書の設定

ユーザ名とパスワードではなくクライアント証明書を受け入れるようにネットワークが設定されている場合、要求に応じてクライアント証明書を提供するようにFortify WebInspectまたはFortify WebInspect Enterpriseを設定できます。

クライアント証明書を設定するには:

1. [クライアント証明書(Client Certificate)] チェックボックスを選択します。
2. 次のいずれかを実行します。
 - コンピュータにとってローカルで、コンピュータ上のすべてのユーザにとってグローバルな証明書を使用するには、[ローカルマシン(Local Machine)]を選択します。
 - コンピュータ上のユーザーアカウントにとってローカルな証明書を使用するには、[現在のユーザ(Current User)]を選択します。

メモ: 共通アクセスカード(CAC)リーダで使用される証明書はユーザ証明書であり、[現在のユーザ(Current User)]に保管されます。

3. 次のいずれかを実行します。
 - 「個人」(「マイ」)証明書ストアから証明書を選択するには、ドロップダウンリストから[マイ(My)]を選択します。
 - 信頼されたルート証明書を選択するには、ドロップダウンリストで[ルート(Root)]を選択します。
4. Webサイトは共通アクセスカード(CAC)リーダを使用しますか?
 - 「はい」の場合は、次の手順を実行します。
 - i. [証明書(Certificate)]リストから、「(SmartCard)」というプレフィックスが付いた証明書を選択します。

選択した証明書に関する情報とPINフィールドが「証明書情報(Certificate Information)」エリアに表示されます。

- ii. PINが必要な場合は、[PIN]フィールドにCACのPINを入力します。

メモ: PINが必要な場合に、この時点ではPINを入力しないと、スキャン中にPINの入力を求められるたびに、Windowsの「セキュリティ」ウィンドウにPINを入力する必要があります。

- iii. [テスト(Test)]をクリックします。

正しいPINを入力した場合は、成功メッセージが表示されます。

- 「いいえ」の場合は、[証明書(Certificate)]リストから証明書を選択します。
- 選択した証明書に関する情報が「証明書(Certificate)」リストの下に表示されます。

アプリケーション認証のステップ

サイトで認証が必要な場合は、このステップを使用してログインマクロを作成、選択、または編集することにより、ログインプロセスを自動化してサイトのカバレッジを拡大できます。ログインマクロは、アプリケーションにアクセスしてログインするために必要なアクティビティの記録です。通常は、ユーザ名とパスワードを入力し、[ログイン]や[ログオン]などのボタンをクリックします。

ログインマクロを使用するスキャンの「スキャン設定: 認証(Scan Settings: Authentication)」で「マクロ検証を有効にする(Enable macro validation)」が選択されている場合、Fortify WebInspectはスキャンの開始時点でログインマクロをテストして、ログインが成功したことを確認します。マクロが無効で、アプリケーションへのログインに失敗した場合、スキャンは停止し、エラーメッセージがスキャンログファイルに書き込まれます。詳細とトラブルシューティングのヒントについては、「["ログインマクロのテスト" ページ510](#)」を参照してください。

重要! 2要素認証を含むマクロを使用する場合は、スキャンを開始する前に、2要素認証アプリケーションの設定を行う必要があります。詳細については、「["アプリケーション設定: 2要素認証" ページ453](#)」を参照してください。

ログインマクロでは、次のオプションを使用できます。

- "["権限のエスカレーションなしでログインマクロを使用する\(Using a Login Macro without Privilege Escalation\)" 次のページ](#)
- "["権限のエスカレーションのためにログインマクロを使用する\(Using Login Macros for Privilege Escalation\)" 次のページ](#)
- "["Fortify WebInspect Enterpriseに接続した際にログインマクロを使用する\(Using a Login Macro when Connected to Fortify WebInspect Enterprise\)" ページ164](#)
- "["マクロのテスト\(Testing the Macro\)" ページ165](#)

マスクされた値のサポート

Web Macro Recorderで値がマスクされたパラメータがマクロで使用されている場合、Fortify WebInspectでガイド付きスキャンを設定するときにも、それらの値はマスクされます。

権限のエスカレーションなしでログインマクロを使用する(Using a Login Macro without Privilege Escalation)

ログインマクロを使用するには:

1. **このサイトでログインマクロを使用する(Use a login macro for this site)**] チェックボックスをオンにします。
2. 次のいずれかを実行します。
 - 事前に記録されたログインマクロを使用するには、省略記号ボタン([...])をクリックして、保存されているマクロを参照します。
 - ログインマクロ(Login Macro)] フィールドに表示されている既存のログインマクロを編集するには、**編集(Edit)**] をクリックします。
 - 新しいマクロを記録するには、**作成(Create)**] をクリックします。
3. **次へ(Next)**] ボタンをクリックします。
アプリケーション認証のステップが完了しました。アプリケーションステージに進み、アプリケーションを実行します。

権限のエスカレーションのためにログインマクロを使用する(Using Login Macros for Privilege Escalation)

権限のエスカレーションポリシーか、有効な権限のエスカレーションチェックを含む別のポリシーを選択した場合、高い権限を持つユーザーアカウント用のログインマクロが少なくとも1つ必要です。詳細については、「["権限のエスカレーションスキャンについて" ページ207](#)」を参照してください。ログインマクロを使用するには:

1. **高い権限のユーザーアカウントログインマクロ(High-Privilege User Account Login Macro)**] チェックボックスをオンにします。このログインマクロは、サイト管理者やモデレータアカウントなど、より高い権限を持つユーザーアカウント用です。
2. 次のいずれかを実行します。
 - 事前に記録されたログインマクロを使用するには、省略記号ボタン([...])をクリックして、保存されているマクロを参照します。
 - ログインマクロ(Login Macro)] フィールドに表示されている既存のログインマクロを編集するには、**編集(Edit)**] をクリックします。
 - 新しいマクロを記録するには、**作成(Create)**] をクリックします。

新しいログインマクロの記録や既存のログインマクロの使用の詳細については、『*Micro Focus Fortify WebInspect Tools Guide*』の「Web Macro Recorder」の章を参照してください。

最初のマクロを記録または選択して [次へ(Next)] の矢印をクリックすると、低い権限のログインマクロを設定する([Configure Low Privilege Login Macro])プロンプトが表示されます。

3. 次のいずれかを実行します。
 - 認証モードでスキャンを実行するには、[はい(Yes)]をクリックします。詳細については、「["権限のエスカレーションスキャンについて" ページ207](#)」を参照してください。
ガイド付きスキャンが [ログインマクロの選択(Select Login Macro)] ウィンドウに戻り、低い権限のログインマクロを作成または選択できるようになります。ステップ4に進みます。
 - スキャンを非認証モードで実行するには、[いいえ(No)]をクリックします。詳細については、「["権限のエスカレーションスキャンについて" ページ207](#)」を参照してください。
アプリケーション認証のステップが完了しました。アプリケーションステージに進みます。
4. [低い権限のユーザーアカウントログインマクロ(Low-Privilege User Account Login Macro)] チェックボックスをオンにします。このログインマクロは、サイトコンテンツのビューアやコンシューマなど、低い権限のユーザーアカウント用です。
5. 次のいずれかを実行します。
 - 事前に記録されたログインマクロを使用するには、省略記号ボタン([...])をクリックして、保存されているマクロを参照します。
 - [ログインマクロ(Login Macro)] フィールドに表示されている既存のログインマクロを編集するには、[編集(Edit)]をクリックします。
 - 新しいマクロを記録するには、[作成(Create)]をクリックします。

新しいログインマクロの記録や既存のログインマクロの使用の詳細については、『*Micro Focus Fortify WebInspect Tools Guide*』の「Web Macro Recorder」の章を参照してください。
6. 2つ目のマクロを記録または選択した後、[次へ(Next)] ボタンをクリックします。
アプリケーション認証のステップが完了しました。アプリケーションステージに進み、アプリケーションを実行します。

Fortify WebInspect Enterpriseに接続した際にログインマクロを使用する(Using a Login Macro when Connected to Fortify WebInspect Enterprise)

Fortify WebInspect Enterpriseに接続されているFortify WebInspectの場合は、Fortify WebInspect Enterpriseマクロリポジトリからログインマクロをダウンロードして使用できます。

1. [このサイトでログインマクロを使用する(Use a login macro for this site)] チェックボックスをオンにします。
2. [ダウンロード(Download)]をクリックします。
Fortify WebInspect Enterpriseからマクロをダウンロードする([Download a Macro from Fortify WebInspect Enterprise]) ウィンドウが表示されます。
3. ドロップダウンリストから [アプリケーション(Application)] と [バージョン(Version)] を選択します。

4. [マクロ(Macro)] ドロップダウンリストからリポジトリマクロを選択します。
5. [OK] をクリックします。

メモ: リポジトリマクロを選択すると、最終確認(Final Review)ページの [自動でスキャンをWIEにアップロードする(Automatically Upload Scan to WIE)] の [アプリケーション(Application)] と [バージョン(Version)] が自動的に同期されます。

マクロのテスト (Testing the Macro)

オプションで、[テスト(Test)] をクリックして、ログインフォームの検索とマクロ検証テストの実行を行ってから、ガイド付きスキャンウィザードの次のステージに進みます。完了前に検証テストをキャンセルする必要がある場合は、[キャンセル(Cancel)] をクリックします。

マクロが無効で、アプリケーションへのログインが失敗すると、エラーメッセージが表示されます。詳細とトラブルシューティングのヒントについては、「["ログインマクロのテスト" ページ510](#)」を参照してください。

アプリケーションステージについて

アプリケーションステージでは、アプリケーションを実行します。アプリケーションステージ中に、以下の操作を実行します。

- モバイルアプリケーションを実行して、Webトラフィックを生成および収集します。
- 含めるホストとRESTfulエンドポイントを指定します。

アプリケーションの実行ステップ

アプリケーションを実行してWebトラフィックを生成および収集するには:

1. [記録(Record)] ボタンをクリックします。
2. アプリケーションを実行し、顧客が行うようにインターフェースを移動します。
3. 十分なトラフィックが生成されたら、[停止(Stop)] ボタンをクリックします。
4. ワークフローを確認するには、[再生(Play)] をクリックします。

許可ホストとRESTfulエンドポイントの最終決定

アプリケーションを実行してWebトラフィックを収集すると、許可ホストと潜在的なRESTfulエンドポイントのリストが生成されます。

監査に含めるホストを選択するには、[許可ホスト(Allowed Hosts)] テーブルの [有効(Enabled)] 列のチェックボックスをクリックします。

RESTfulエンドポイントのリストは、RESTfulエンドポイントになる可能性のあるすべての組み合わせを一覧表示することで生成されます。[有効(Enabled)] チェックボックスを選択して、リストから実際のRESTfulエンドポイントを選択します。より可能性の高いサブセットだけを示すようリストを縮小するには、[検出(Detect)] ボタンをクリックします。ヒューリスティックが適用さ

れ、可能性の低い結果の一部がフィルタで除外されます。結果のリストで [有効(Enabled)] チェックボックスを選択します。

Fortify WebInspectまたはFortify WebInspect EnterpriseですべてのRESTfulエンドポイントが見つからなかった場合は、手動で追加できます。

新しいRESTfulエンドポイントルールを設定するには:

1. [新規ルール(New Rule)] ボタンをクリックします。
RESTfulエンドポイントテーブルに新しいルール入力ボックスが表示されます。
2. 入力ボックスのサンプルフォーマットに従って、RESTfulエンドポイントを入力します。

RESTfulエンドポイントのリストをインポートするには:

1. [インポート(Import)] ボタンをクリックします。
ファイルセレクタが表示されます。
2. Webアプリケーション記述言語(.wadl)ファイルを選択します。
3. [OK]をクリックします。

設定ステージについて

最終ステージでは、収集したトラフィックの監査方法に影響を与えるいくつかのオプションを設定できます。使用可能なオプションは、選択した内容によって異なります。

最終確認ステップ

詳細オプションの設定

詳細オプションの設定ステップでは、詳細オプションを設定できます。これらのオプションは、ガイド付きスキャンウィザードでの選択内容に依存するため、スキャンごとに変わります。次のようなオプションがあります。

識別された誤検出を再利用する(Reuse Identified False Positives)]。以前のスキャンを選択して、すでに誤検出として識別されている脆弱性を特定します。

トラフィック分析(Traffic Analysis)]。自己完結型のプロキシサーバをデスクトップで使用できます。これを使用すると、サーバとの間でHTTP要求の送信と応答の受信を行うスキャナ、ブラウザ、または他のツールからのトラフィックを監視できます。Traffic Monitorを有効にし、Fortify WebInspectナビゲーションペインにWebサイトまたはWebサービスの階層構造を表示することもできます。これにより、Fortify WebInspectによって送信されたすべてのHTTP要求と、サーバから受信した関連するHTTP応答を表示および確認できます。

スキャンモード(Scan Mode)]。Web探索のみの機能。このオプションでは、検出(パスの切り捨て)を設定できます。パスの切り捨てにより、ファイル名のない既知のディレクトリに対して要求を行うことができます。これにより、ディレクトリ一覧を表示できます。また、[パッシブ分析(キーワード検索)(Passive Analysis (Keyword Search))]オプションを選択して、Webサーバからのすべての応答(エラーメッセージ、ディレクトリリスト、クレジットカード番号など)について、Webサイトで適切に保護されていないかどうかを調べることもできます。

設定の検証とスキャンの開始

このページのオプションを使用すると、現在のスキャン設定を保存することができます。また、WebInspectがWebInspect Enterpriseと統合されている場合は、WebInspect Enterpriseとやり取りすることができます。

1. スキャン設定をXMLファイルとして保存するには、[ここをクリックして設定を保存する(Click here to save settings)]を選択します。標準の[名前を付けて保存(Save as)]ウィンドウを使用して、ファイルに名前を付けて保存します。
2. WebInspectがWebInspect Enterpriseと統合されている場合は、ツールバーに[テンプレート(Templates)]セクションが表示されます。次の表の説明に従って操作を進めます。

| 目的の作業 | その場合の手順 |
|--|--|
| <p>現在のスキャン設定をテンプレートとしてWebInspect Enterpriseデータベースに保存する</p> <p>メモ: 既存のテンプレートを編集する場合、[保存(Save)]を実行すると、実際には更新が行われます。設定の編集を保存したり、テンプレート名を変更したりすることができます。ただし、アプリケーション、バージョン、またはグローバルテンプレートの設定は変更できません。</p> | <ol style="list-style-type: none"> 次のいずれかを実行します。 <ul style="list-style-type: none"> ツールバーの[テンプレート(Templates)]セクションで[保存(Save)]をクリックします。 [ここをクリックしてテンプレートを保存する(Click here to save template)]を選択します。 [テンプレートの保存(Save Template)]ウィンドウが表示されます。 [アプリケーション(Application)]ドロップダウンリストからアプリケーションを選択します。 [バージョン(Version)]ドロップダウンリストからアプリケーションバージョンを選択します。 [テンプレート(Template)]フィールドに名前を入力します。 |
| <p>テンプレートからスキャン設定をロードする</p> | <ol style="list-style-type: none"> ツールバーの[テンプレート(Templates)]セクションで[ロード(Load)]をクリックします。 <p>現在のスキャン設定が失われるという確認メッセージが表示されます。</p> <ol style="list-style-type: none"> [はい(Yes)]をクリックします。 <p>[テンプレートのロード(Load Template)]ウィンドウが表示されます。</p> |

| 目的の作業 | その場合の手順 |
|-------|---|
| | <p>す。</p> <p>c. [アプリケーション(Application)]ドロップダウンリストからアプリケーションを選択します。</p> <p>d. [バージョン-Version)]ドロップダウンリストからアプリケーションバージョンを選択します。</p> <p>e. [テンプレート(Template)]ドロップダウンリストからテンプレートを選択します。</p> <p>f. [ロード(Load)]をクリックします。</p> <p>ガイド付きスキャンがサイトステージに戻り、Webサイトの検証と、テンプレートからのステップごとの設定の実行が行えるようになります。</p> |

3. WebInspectがWebInspect Enterpriseと統合されている場合は、このページに[WebInspect Enterprise]セクションが表示されます。WebInspect Enterpriseを操作するには、次のようにします。
- [アプリケーション(Application)]ドロップダウンリストからアプリケーションを選択します。
 - [バージョン-Version)]ドロップダウンリストからアプリケーションバージョンを選択します。
 - 次の表の説明に従って操作を進めます。

| スキャンの実行方法 | その場合の手順 |
|--------------------------------|--|
| WebInspect Enterpriseでセンサを使用する | <ol style="list-style-type: none"> [WebInspect Enterpriseで実行(Run in WebInspect Enterprise)]を選択します。 [センサ(Sensor)]ドロップダウンリストからセンサを選択します。 スキャンの[優先度(Priority)]を選択します。 |
| WebInspectで | <ol style="list-style-type: none"> [WebInspectで実行(Run in WebInspect)]を選択します。 スキャン結果をWebInspect Enterpriseの指定したアプリケーションおよびバージョンに自動的にアップロードする場合は、[WebInspect Enterpriseへの自動アップ |

| スキャンの実行方法 | その場合の手順 |
|-----------|--|
| | <p>ロード(Auto Upload to WebInspect Enterprise)]を選択します。</p> <p>メモ: スキャンが正常に完了しない場合、WebInspect Enterpriseにはアップロードされません。</p> |

4. [今すぐスキャン(Scan Now)]エリアでスキャン設定を見直し、[スキャンの開始(Start Scan)]をクリックしてスキャンを開始します。

スキャン後のステップ

スキャンを完了してFortify WebInspectまたはFortify WebInspect Enterpriseを実行したら、Android、Windows、またはiOSデバイスまたはエミュレータを以前の状態にリセットする必要があります。次のステップは、iOSデバイスを開始前の状態にリセットする方法を示しています。他のデバイスおよびエミュレータのステップは類似していますが、実行しているOSのバージョンによって異なります。

iOSデバイスでFortify証明書を削除するには:

[設定(Settings)]アプリケーションを実行します。

1. [設定(Settings)]列から [全般(General)]を選択します。
2. リストの一一番下までスクロールして、[プロファイルWebInspectルート(Profile WebInspect Root)]を選択します。
3. [削除(Remove)]ボタンをタップします。

iOSデバイスのプロキシ設定を削除するには:

1. [設定(Settings)]アプリケーションを実行します。
2. [設定(Settings)]列から [Wi-Fi]を選択します。
3. [ネットワーク(Network)]の名前をタップします。

サーバのIPアドレスとポート番号を削除します。

次も参照

["ガイド付きスキャンの概要" ページ116](#)

APIまたはWebサービススキャンの実行

APIスキャンウィザードを使用して、APIスキャンまたはWebサービススキャンを設定します。

重要! SQL Expressデータベースを使用して複数のスキャンを実行する場合、SQL Expressの制限が原因で期待する結果を得られないことがあります。そのため、SQL Expressを使用するインストールでは、同時(または並行)スキャンの実行をお勧めしません。

APIスキャン

APIスキャンの場合、Fortify WebInspectがREST API定義からマクロを作成し、自動分析を実行します。

重要! Postman APIスキャンを設定する場合は、次に進む前に前提条件のソフトウェアがインストールされていることを確認してください。ダイナミックトークンを使用したダイナミック認証の設定など、Postmanコレクションファイルの使用に関する詳細については、「["Postmanコレクションによるスキャン" ページ331](#)」を参照してください。

Webサービススキャン

Webサービススキャンの場合、Fortify WebInspectはWSDLサイトをWeb探索し、検出した各操作の各パラメータに値を送信します。これらの値はファイルから抽出されますが、そのファイルはWeb Service Test Designerを使用して作成する必要があります。次に、Fortify WebInspectは、SQLインジェクションなどの脆弱性を検出するために各パラメータを攻撃して、サイトを監査します。

Webサービス脆弱性スキャンとその他のタイプのスキャンアクションの違いについては、「["Webサービスの監査" ページ266](#)」を参照してください。

APIスキャンウィザードの開始

APIスキャンまたはWebサービススキャンの設定を開始するには:

1. Fortify WebInspectの [開始ページ(Start Page)] で [APIスキャンの開始(Start an API Scan)] をクリックします。
APIスキャンウィザードの [ステップ1(Step 1)] が開きます。
2. [スキャン名(Scan Name)] ボックスにスキャンの名前を入力します。

ヒント: APIスキャンウィザードで表示される任意のウィンドウで、(ウィンドウの下部にある) [設定(Settings)] をクリックして、デフォルトの設定を変更するか、または以前に保存した設定ファイルをロードすることができます。変更はすべてこのスキャンにのみ適用され、デフォルト設定ファイルに保持されることはありません。変更を行い、デフォルト設定として維持するには、Fortify WebInspect の [編集(Edit)] メニューをクリックし、[デフォルトのスキャン設定(Default Scan Settings)] を選択します。

次に行う作業

次のいずれかを実行します。

- APIスキャンを設定するには、「["APIスキャンの設定" 下](#)」に進みます。
- Webサービススキャンを設定するには、「["Webサービススキャンの設定" 次のページ](#)」に進みます。

APIスキャンの設定

APIスキャンウィザードの [ステップ1(Step 1)] でAPIスキャンを設定できます。

APIスキャンを設定するには:

1. [APIスキャン(API Scan)]を選択します。

重要! API定義にアクセスするためにHTTP権限付与資格情報(基本的なアクセス認証またはBearerトークンなど)が必要な場合には、スキャン開始前に、「["カスタムヘッダの追加" ページ405](#)」の説明に従って、[スキャン設定: クッキー/ヘッダ(Scan Settings: Cookies/Headers)]でこの情報をカスタムヘッダとして追加する必要があります。

ヘッダの例:

```
Authorization: Basic YWxhZGRpbjpvcGVuc2VzYW1l
Authorization: \sBearer\s(?<Token>[^\\r\\n]*)\\r\\n
```

2. [APIタイプ(API Type)]リストでスキャンするAPIタイプを選択します。オプションは、[Open API](Swaggerとも呼ばれる)、[Postman]、および [OData]です。
3. 次の表の説明に従って操作を進めます。

| APIのタイプ... | 操作手順 |
|------------------|---|
| Open APIまたはOData | <p>[API定義URL (API Definition URL)]ボックスに、Open APIまたはOData定義ファイルのURLを次の例に示すように指定します。</p> <p>http://172.16.81.36/v1</p> <p>ヒント: あるいは、ローカルマシンに保存されている定義ファイルのフルパスを貼り付けることもできます。</p> <p>メモ: Fortify WebInspectでは、これらのAPIタイプで次の定義とプロトコルがサポートされています。</p> <ul style="list-style-type: none">OpenAPI Specificationバージョン2.0および3.0 (旧称 Swagger Specification) 詳細については、Swagger Webサイト(http://swagger.io/)にアクセスしてください。 |

| APIのタイプ... | 操作手順 |
|------------|---|
| | <ul style="list-style-type: none"> Open Data (OData)プロトコル(バージョン2、3、および4)。詳細については、OData Webサイト(http://www.odata.org/)にアクセスしてください。 |
| Postman | <p>次のいずれかを実行します。</p> <ul style="list-style-type: none"> ワークフローコレクションをインポートするには、をクリックし、ドロップダウンリストから [ワークフロー(Workflow)]を選択して、Postmanコレクションファイルをインポートします。 認証コレクションをインポートするには、をクリックし、ドロップダウンリストから [認証(Authentication)]を選択し、Postmanコレクションファイルをインポートします。 環境ファイルをインポートするには、をクリックし、ドロップダウンリストから [環境(Environment)]を選択し、Postman環境ファイルをインポートします。 <p>ファイルはコレクションファイルのリストに追加されます。追加のコレクションファイルをインポートするには、このステップを繰り返します。</p> <p>重要! インポートできる認証コレクションファイルと環境ファイルはそれぞれ1つのみです。ワークフローコレクションファイルは複数インポートできます。</p> |

次に行う作業

次のいずれかを実行します。

- プロキシを設定する場合は、「["APIスキャンおよびWebサービススキャンのプロキシの設定"次のページ](#)」に進みます。
- 認証を設定するには、[\[次へ\(Next\)\]](#)をクリックし、「["APIスキャンおよびWebサービススキャンの認証の設定" ページ174](#)」に進みます。

Webサービススキャンの設定

APIスキャンウィザードの [ステップ1(Step 1)] でWebサービススキャンを設定できます。

WSDLファイルの使用

WSDL (Web Service Definition Language)ファイルを使用して設定を行うには:

1. [Webサービススキャンを設定する(Configure a Web Service Scan)]を選択します。
2. 次のいずれかを実行します。
 - WSDLファイルのフルパスと名前を入力または選択します。
 - をクリックして標準のファイル選択ダイアログボックスを開き、WSDLファイルを選択します。

メモ: この時点でWSDLファイルをインポートし、後でWeb Service Test Designerを起動して、サービスの各操作の値を含むファイルを設定します。

既存のWSDファイルの使用

既存のWSD (Webサービステスト設計)ファイルを使用して設定を行うには:

1. **既存のデザインファイルを使用してスキャンする(Scan with Existing Design File)**を選択します。
2. をクリックして標準のファイル選択ダイアログボックスを開き、Web Service Test Designerを使用して以前に作成したWSDファイルを選択します。

メモ: 選択したファイルには、サービスの各操作の値が含まれています。

次に行う作業

次のいずれかを実行します。

- プロキシを設定する場合は、「["APIスキャンおよびWebサービススキャンのプロキシの設定" 下](#)」に進みます。
- 認証を設定するには、[「次へ\(Next\)」](#)をクリックし、「["APIスキャンおよびWebサービススキャンの認証の設定" 次のページ](#)」に進みます。

APIスキャンおよびWebサービススキャンのプロキシの設定

プロキシサーバ経由でターゲットサイトにアクセスする必要がある場合は、APIスキャンウィザードの [ステップ1(Step 1)] でプロキシを設定できます。

プロキシ設定を行うには:

- [ネットワークプロキシ(Network Proxy)]を選択し、[プロキシプロファイル\(Proxy Profile\)](#)リストからオプションを選択します。
- [\[自動検出\(Auto Detect\)\]](#): WPAD (Web Proxy Autodiscovery)プロトコルを使用してプロキシ自動設定ファイルを探し、これを使用してブラウザのWebプロキシ設定を行いま

す。

- **システムプロキシを使用(Use System Proxy)**: ローカルマシンからプロキシサーバ情報を取り込みます。
- **PACファイルを使用(Use PAC File)**: PAC (Proxy Automatic Configuration)ファイルからプロキシ設定をロードします。このオプションを選択した場合は、**編集(Edit)**をクリックしてPACの場所(URL)を入力します。
- **明示的なプロキシ設定を使用(Use Explicit Proxy Settings)**: プロキシサーバ設定を指定します。このオプションを選択した場合は、**編集(Edit)**をクリックしてプロキシ情報を入力します。
- **Mozilla Firefoxを使用(Use Mozilla Firefox)**: Firefoxからプロキシサーバ情報をインポートします。

メモ: ブラウザのプロキシ設定を使用することにしても、プロキシサーバ経由のインターネットアクセスが保証されるわけではありません。Firefoxブラウザの接続設定が「**プロキシーを使用しない**」に設定されている場合、またはInternet Explorerの「**LANにプロキシサーバを使用する**」設定が選択されていない場合、プロキシサーバは使用されません。

次に行う作業

認証を設定するには、**次へ(Next)**をクリックし、「["APIスキャンおよびWebサービススキャンの認証の設定" 下](#)」に進みます。

APIスキャンおよびWebサービススキャンの認証の設定

APIスキャンウィザードの「**ステップ2(Step 2)**」でネットワーク認証を設定できます。Postman APIスキャンを実行する場合、「**ステップ1(Step 1)**」で選択したコレクションファイルがスキャンウィザードによって検証され、このページにPostman環境設定が表示されます。設定を確認し、必要に応じて調整できます。

ネットワーク認証の設定

Webサーバのネットワーク認証を設定するには:

- **ネットワーク認証(Network Authentication)**を選択し、認証メソッドを選択して、ネットワーク資格情報を入力します。認証メソッドは次のとおりです。
 - ADFS CBT
 - 自動(Automatic)
 - 基本(Basic)
 - ダイジェスト(Digest)
 - Kerberos

- ネゴシエート(Negotiate)
- NT LAN Manager (NTLM)

Postman環境設定の表示および調整

メモ: Postman環境設定は、Postman APIスキャンを実行する場合にのみ使用できます。

Postmanコレクションファイルの検証が正常に完了すると、コレクションファイルに含まれるセッションのリストが [Postman設定(Postman Configuration)] エリアに表示されます。認証セッションが指定されている場合、それらのセッションは認証(Auth)セッションとして事前に選択されます。その他のすべてのセッションは、監査(Audit)セッションとして事前に選択されます。また、検出された認証のタイプがトークン戦略(Token Strategy)として一覧にされ、オプションとしてなし(None)、[スタティック(Static)]、または [ダイナミック(Dynamic)] があります。

メモ: 認証(Auth)セッションは、スキャンの認証に使用されます。監査(Audit)セッションは、スキャンで監査されます。

必要に応じて設定を調整します。

1. 必要に応じてセッションのタイプを変更するには、[認証(Auth)] または [監査(Audit)] チェックボックスをオンにします。
2. Postman認証設定を次のように変更します。
 - スタティック(Static)認証の場合は、[カスタムヘッダトークン(Custom Header Token)] ボックスにトークンを入力します。
 - ダイナミック(Dynamic)認証の場合は、次の手順を実行します。
 - [応答トークン(Response Token)] ボックスの右側にある [正規表現(カスタム)(Regex (Custom))] オプションを選択して、[応答トークン名(Response Token Name)] ボックスにカスタム正規表現を入力します。
 - [要求トークン名(Request Token Name)] ボックスの右側にある [正規表現(カスタム)(Regex (Custom))] オプションを選択して、[要求トークン名(Request Token Name)] ボックスにカスタム正規表現を入力します。
 - [ログアウト条件(Logout Condition)] ボックスの右側にある [自動検出を使用する(Use Auto Detect)] オプションをオフにして、[ログアウト条件(Logout Condition)] ボックスに新しいログアウト条件文字列を入力します。

Postmanのダイナミック認証の詳細については、「["ダイナミックトークン用のPostmanログインの手動設定" ページ335](#)」を参照してください。

重要! Postman認証設定を変更した場合、APIスキャンウィザードの [ステップ1(Step 1)] に戻って [次へ(Next)] をもう一度クリックしないと、変更は検証されません。

次に行う作業

スキャンの詳細を設定するには、[次へ\(Next\)】をクリックし、「"APIスキャンおよびWebサービススキャンのスキャン詳細の設定" 下」に進みます。](#)

APIスキャンおよびWebサービススキャンのスキャン詳細の設定

APIスキャンおよびWebサービススキャンのデフォルトポリシーはAPIポリシーです。APIスキャン ウィザードの [\[ステップ3\(Step 3\)\]](#)で、別のポリシーを選択するか、またはスキャンの他のオプションを選択できます。

APIスキャンのポリシーの選択

デフォルトでは、APIスキャンではAPIポリシーが選択されています。ただし、必要に応じて別のポリシーを選択できます。

別のポリシーを選択するには:

1. **監査の深さ(ポリシー)(Audit Depth (Policy))** エリアで、ドロップダウンリストからポリシーを選択します。
2. 「["APIスキャンおよびWebサービススキャンの追加の設定" 次のページ](#)」に進みます。

Web Service Test Designerの起動

デザインテストファイルを作成する場合、Web Service Test Designerの起動を求めるメッセージが表示されます。Designerを使用してWSDファイルを作成するまで、APIスキャンウィザードは先に進みません。

Web Service Test Designerを起動するには::

1. **【デザイン(Design)】**をクリックします。
Web Service Test Designerが開き、インポートされたWSDLが表示されます。
2. 必要に応じてファイルを編集します。
詳細については、Web Service Test Designerのヘルプまたは『*Micro Focus Fortify WebInspect Tools Guide*』を参照してください。
3. Web Service Test DesignerでWSDファイルを保存します。
4. 「["APIスキャンおよびWebサービススキャンの追加の設定" 次のページ](#)」に進みます。

APIスキャンおよびWebサービススキャンの追加の設定

必要に応じて、次の表の説明に従って [設定(Settings)] セクションで追加設定を選択または設定できます。

| 目的の作業... | 手順... |
|---|---|
| スタンダロンプロキシサーバを使用する | <p>[Web Proxyの起動およびWeb Proxy経由でのトラフィックの送信(Launch and Direct Traffic through Web Proxy)]を選択します。</p> <p>メモ: このオプションは、スケジュールしている場合は使用できません。</p> |
| スキャン中にFortify WebInspectから送信されたすべてのHTTP要求をキャプチャして表示する | <p>[Traffic Monitorを有効にする(Enable Traffic Monitor)]を選択します。</p> |
| すでに識別されている誤検出を再利用する | <ol style="list-style-type: none">[誤検出のインポート(Import False Positives)]を選択します。[スキャンを選択(select scans)]リンクをクリックして、誤検出のインポート元のスキャンを1つまたは複数選択します。 |
| 許可ホストを追加する | <ol style="list-style-type: none">[許可ホストの追加(Add Allowed Hosts)]セクションで [追加(Add)]をクリックします。[許可ホストの指定(Specify Allowed Host)]ダイアログボックスで、URL (またはURLを表す正規表現)を入力します。<p>メモ: URLを指定する場合は、プロトコル指定子 (http://やhttps://など)を含めないでください。</p>許可ホストの正規表現を入力した場合は、[正規表現を使用する(Use Regular Expression)]を選択します。<p>ヒント: 正規表現の作成のヒントについては、  (許可ホスト(Allowed Host)]ボックスの右側)をクリックします。</p>[OK]をクリックします。 |

| 目的の作業... | 手順... |
|----------|---|
| | URLが [許可ホスト(Allowed Hosts)] リストに追加されます。 |

次に行う作業

設定を保存するには、スキャンを実行するかスキャンをスケジュールして、[次へ(Next)]をクリックし、「[その後の作業" 下](#)」に進みます。

その後の作業

1. このスキャンを再度実行する予定の場合は、設定をXMLファイルに保存できます。[保存(Save)]ハイパーリンクをクリックして、ファイルに名前を付けて保存します。Webサービススキャンウィザードでスキャンを開始するときに、(ウィンドウ下部にある) [設定(Settings)]をクリックしてこの設定ファイルをロードできます。
2. スキャンをスケジュールする場合は、スキャン完了時にレポートを生成することを選択できます。[レポートの生成(Generate Report)]チェックボックスをオンにしてから、[レポートの選択(Select reports)]ハイパーリンクをクリックします。
3. [スキャン(Scan)]をクリックします(スキャンをスケジュールする場合は[スケジュール(Schedule)]をクリックします)。

基本スキャンの実行(Webサイトスキャン)

このウィンドウおよびそれ以降のウィンドウにデフォルトで表示されるオプションは、Fortify WebInspectのデフォルト設定から抽出されます。行う変更はすべて、このスキャンにのみ使用されます。ウィンドウ下部の [設定(デフォルト)(Settings (Default))]をクリックしてFortify WebInspectの全設定にアクセスする場合も、選択する内容はすべて一時的なものになります。デフォルト設定を変更するには、[編集(Edit)]メニューから [デフォルトのスキャン設定(Default Scan Settings)]を選択する必要があります。詳細については、「["デフォルトのスキャン設定" ページ370](#)」を参照してください。

重要! SQL Expressデータベースを使用して複数のスキャンを実行する場合、SQL Expressの制限が原因で期待する結果を得られないことがあります。そのため、SQL Expressを使用するインストールでは、同時(または並行)スキャンの実行をお勧めしません。

基本スキャンのオプション

1. [スキャン名(Scan Name)]ボックスに、スキャンの名前または簡単な説明を入力します。

2. 次のいずれかのスキャンモードを選択します。

- **Web探索のみ(Crawl Only):** サイトの階層データ構造が完全にマッピングされます。Web探索が完了したら、**監査(Audit)**をクリックしてアプリケーションの脆弱性を評価できます。
- **Web探索および監査(Crawl and Audit):** サイトの階層データ構造がマッピングされ、各リソース(ページ)が監査されます。選択したデフォルト設定に応じて、各リソースの検出時またはサイト全体のWeb探索後に監査を実行できます。Web探索および監査の同時実行と順次実行の詳細については、「["Web探索および監査モード\(Crawl and Audit Mode\)" ページ371](#)」を参照してください。
- **監査のみ(Audit Only):** 選択されているポリシーの手法を適用して脆弱性リスクを判断しますが、WebサイトのWeb探索は実行されません。サイト上のリンクをたどることも評価することもありません。
- **手動(Manual):** アクセス先として選んだのがアプリケーションのどのセクションであれ、Internet Explorerを使用してそこに手動で移動できます。Fortify WebInspectはサイト全体のWeb探索を実行せず、サイト内を手動で移動中に検出したリソースに関する情報のみを記録します。この機能は、Webフォームのログオンページからサイトに入る場合、または調査するアプリケーションの個別のサブセットまたは部分を定義する場合に最もよく使用されます。サイト内を移動し終わったら、結果を監査して、記録したサイトのその部分に関連するセキュリティ脆弱性を評価できます。

メモ: スキャンをスケジュールするときには、手動モードは使用できません。

3. **レンダリングエンジン(Rendering Engine)**ドロップダウンリストからレンダリングエンジンを選択します。選択するレンダリングエンジンによって、スキャンの設定時に新しいマクロの記録または既存のマクロの編集を行うときに開かれるWeb Macro Recorderが決まります。オプションは次のとおりです。

- **Macro Engine 6.1 (推奨) (Macro Engine 6.1 (recommended))** -このオプションを選択すると、Web Macro Recorder with Macro Engine 6.1が指定されます。これはTruClientテクノロジとFirefoxテクノロジを使用します。
- **セッションベース(Session-based)** -このオプションを選択すると、セッションベースのWeb Macro Recorderが指定されます。これはInternet Explorerブラウザテクノロジを使用します。

メモ: 手動モードでレンダリングエンジンを設定することはできません。手動モードでは、セッションベースのテクノロジが使用されます。

4. 次のいずれかのスキャンタイプを選択します。

- **標準スキャン(Standard Scan):** ターゲットURLから始めて、自動分析を実行します。これは標準的なスキャン開始方法です。
- **手動スキャン(Manual Scan):** (ステップモードとも呼ばれます) アクセス先として選んだのがアプリケーションのどのセクションであれ、Internet Explorerを使用してそこに手動で移動できます。この選択項目は、手動スキャンモードを選択している場合にのみ表示されます。

- **リストドリブンスキャン(List-Driven Scan)**: スキャン対象 URLのリストを使用してスキャンを実行します。各URLは完全修飾であり、プロトコル(`http://`または`https://`など)が含まれている必要があります。カンマ区切りリスト形式または1行に1つずつURLを指定したテキストファイルを使用できます。
 - リストをインポートするには、[インポート(Import)]をクリックします。
 - Site List Editorを使用してリストを作成または編集するには、[管理(Manage)]をクリックします。詳細については、「["Site List Editorの使用" ページ191](#)」を参照してください。
- **ワークフロードリブンスキャン(Workflow-Driven Scan)**: 以前に記録したマクロに含まれているURLのみを監査し、監査中に検出されたハイパーリンクはたどりません。ログアウト署名は不要です。この種のマクロは、アプリケーションの特定のサブセクションに焦点を当てるために最もよく使用されます。複数のマクロを選択すると、すべてのマクロが同一スキャンに含まれます。.webmacroファイルまたはBurp Proxyキャプチャを使用できます。詳細については、「["ワークフローマクロの選択" ページ254](#)」を参照してください。

重要! ログインマクロを、ワークフローマクロまたは起動マクロ、あるいはその両方と組み合わせて使用する場合、すべてのマクロは同じ種類である必要があります。すべてが.webmacroファイルであるか、すべてがBurp Proxyキャプチャであるかのどちらかです。同じスキャンで異なる種類のマクロを使用することはできません。

5. 次の表の説明に従って操作を進めます。

| 選択する項目... | 行う手順... |
|-----------------------|---|
| 標準スキャン(Standard Scan) | <p>a. [開始URL(Start URL)]ボックスで、調査するサイトの完全なURLまたはIPアドレスを入力または選択します。</p> <p>URLを入力する場合は、正確に入力する必要があります。たとえば「MYCOMPANY.COM」と入力すると、Fortify WebInspectはWWW.MYCOMPANY.COMなどのバリエーションはスキャンしません([許可ホスト(Allowed Hosts)]設定で代替URLを指定している場合を除く)。</p> <p>無効なURLまたはIPアドレスを指定すると、エラーが発生します。階層ツリー内の特定の位置からスキャンを実行する場合は、スキャンの開始点(<code>http://www.myserver.com/myapplication/</code>など)を追加します。</p> <p>IPアドレスによるスキャンでは、(相対パスではなく)完全修飾URLを使用するリンクは追跡しません。</p> <p>Fortify WebInspectでは、IPV4 (Internet Protocolバージョン4)とIPV6 (Internet Protocolバージョン6)の両方がサポートされています。IPV6アドレスは括弧で囲む必要があります。詳細について</p> |

| 選択する項目 ... | 行う手順... |
|--------------------------------------|--|
| | <p>は、「"Internet Protocolバージョン6" ページ369」を参照してください。</p> <p>b. 【フォルダに限 定(Restrict to folder)】を選択した場合は、ドロップダウンリストから選択したエリアにスキャン範囲を制限できます。次の選択肢があります。</p> <ul style="list-style-type: none"> ◦ ディレクトリのみ(Directory only) - Fortify WebInspectは、指定されたURLだけをWeb探索または監査(またはその両方)します。たとえば、このオプションを選択して <code>www.mycompany/one/two/</code>というURLを指定すると、Fortify WebInspectは「two」ディレクトリのみを評価します。 ◦ ディレクトリおよびサブディレクトリ(Directory and subdirectories) - Fortify WebInspectは、指定されたURLで Web探索または監査(またはその両方)を開始しますが、ディレクトリツリーでそれよりも上位のディレクトリにはアクセスしません。 ◦ ディレクトリおよび親ディレクトリ(Directory and parent directories) - Fortify WebInspectは、指定されたURLでWeb探索または監査(またはその両方)を開始しますが、ディレクトリツリーでそれよりも下位のディレクトリにはアクセスしません。 <p>【【フォルダに限 定(Restrict to folder)】スキャンオプションの制限について</p> <p>は、「"【フォルダに限 定】に関する制限" ページ202」を参照してください。</p> |
| 手動スキャン(Manual Scan) | <p>開始URLを入力し、必要に応じて 【フォルダに限 定(Restrict to folder)】を選択します。前に説明した「標準スキャン」を参照してください。</p> <p>メモ: 手動モードでレンダリングエンジンを設定することはできません。手動モードでは、セッションベースのテクノロジが使用されます。</p> |
| リストドリブンスキャン(List-Driven Scan) | <p>次のいずれかを実行します。</p> <ul style="list-style-type: none"> ◦ 【インポート(Import)】をクリックし、スキャンするURLのリストを含むテキストファイルまたはXMLファイルを選択します。 ◦ 【管理(Manage)】をクリックし、URLのリストを作成または変更します。 |

| 選択する項目 ... | 行う手順... |
|--|--|
| ワークフロードリブンスキャン (Workflow-Driven Scan) | <p>次のいずれかを実行します。</p> <ul style="list-style-type: none"> 【管理(Manage)】をクリックして、マクロを選択、編集、記録、インポート、エクスポート、または削除します。 【記録(Record)】をクリックしてマクロを作成します。 <p>メモ: 複数のマクロを1つのスキャンに含めることができます。</p> |

6. 次へ(Next)】をクリックします。

認証とコネクティビティ

1. プロキシサーバ経由でターゲットサイトにアクセスする必要がある場合は、【ネットワークプロキシ(Network Proxy)】を選択し、【プロキシプロファイル(Proxy Profile)】リストからオプションを選択します。
 - 【自動検出(Auto Detect)】: WPAD (Web Proxy Autodiscovery)プロトコルを使用してプロキシ自動設定ファイルを探し、これを使用してブラウザのWebプロキシ設定を行います。
 - 【システムプロキシを使用(Use System Proxy)】: ローカルマシンからプロキシサーバ情報をインポートします。
 - 【PACファイルを使用(Use PAC File)】: PAC (Proxy Automatic Configuration)ファイルからプロキシ設定をロードします。このオプションを選択した場合は、【編集(Edit)】をクリックしてPACの場所(URL)を入力します。詳細については、「["プロキシプロファイルの設定" ページ191](#)」を参照してください。
 - 【明示的なプロキシ設定を使用(Use Explicit Proxy Settings)】: プロキシサーバ設定を指定します。このオプションを選択した場合は、【編集(Edit)】をクリックしてプロキシ情報を入力します。詳細については、「["プロキシプロファイルの設定" ページ191](#)」を参照してください。
 - 【Mozilla Firefoxを使用(Use Mozilla Firefox)】: Firefoxからプロキシサーバ情報をインポートします。

メモ: ブラウザのプロキシ設定を使用することにしても、プロキシサーバ経由のインターネットアクセスが保証されるわけではありません。Firefoxブラウザの接続設定が【プロキシーを使用しない】に設定されている場合、またはInternet Explorerの【LANにプロキシサーバを使用する】設定が選択されていない場合、プロキシサーバは使用されません。

2. サーバ認証が必要な場合は、[ネットワーク認証(Network Authentication)]を選択します。次に、認証メソッドを選択し、ネットワーク資格情報を入力します。認証メソッドは次のとおりです。
 - ADFS CBT
 - 自動(Automatic)
 - 基本(Basic)
 - ダイジェスト(Digest)
 - Kerberos
 - ネゴシエート(Negotiate)
 - NT LAN Manager (NTLM)
3. Webサイトのクライアント証明書を設定するには、[設定(Settings)]>[認証(Authentication)]をクリックし、次の手順に従って続行します。
 - a. [クライアント証明書(Client Certificates)]エリアで、[有効化(Enable)]チェックボックスをオンにします。
 - b. [選択>Select)]をクリックします。
[クライアント証明書(Client Certificates)]ウィンドウが開きます。
 - c. 次のいずれかを実行します。
 - コンピュータにとってローカルで、コンピュータ上のすべてのユーザーにとってグローバルな証明書を使用するには、[ローカルマシン(Local Machine)]を選択します。
 - コンピュータ上のユーザーアカウントにとってローカルな証明書を使用するには、[現在のユーザー(Current User)]を選択します。

メモ: 共通アクセスカード(CAC)リーダで使用される証明書はユーザ証明書であり、[現在のユーザー(Current User)]に保管されます。
 - d. 次のいずれかを実行します。
 - 「個人」(「マイ」)証明書ストアから証明書を選択するには、ドロップダウンリストから[マイ(My)]を選択します。
 - 信頼されたルート証明書を選択するには、ドロップダウンリストで[ルート(Root)]を選択します。
 - e. WebサイトではCACリーダを使用しますか。
 - 「はい」の場合は、次の手順を実行します。
 - A. [証明書(Certificate)]リストから、「(SmartCard)」というプレフィックスが付いた証明書を選択します。
選択した証明書に関する情報とPINフィールドが[証明書情報(Certificate Information)]エリアに表示されます。
 - B. PINが必要な場合は、[PIN]フィールドにCACのPINを入力します。

メモ: PINが必要な場合に、この時点でPINを入力しないと、スキャン中にPINの入力を求められるたびに、Windowsの[セキュリティ]ウィンドウにPINを入力する必要があります。

- C. [テスト(Test)]をクリックします。
正しいPINを入力した場合は、成功メッセージが表示されます。
- 「いいえ」の場合は、[証明書(Certificate)]リストから証明書を選択します。
選択した証明書に関する情報が[証明書(Certificate)]リストの下に表示されます。
 - f. [OK]をクリックします。
4. ターゲットサイトにログインできる1つ以上のユーザ名とパスワードが含まれている記録済みマクロを使用するには、[サイト認証(Site Authentication)]を選択します。そのマクロには「ログアウト条件」も含まれている必要があります。これは、予期せぬログアウトが発生した場合にそれを示し、Fortify WebInspectがこのマクロを再実行して再びログインできるようにするためのものです。

Web Macro Recorderで値がマスクされたパラメータがマクロで使用されている場合、Fortify WebInspectで基本スキャンを設定するときにも、それらの値はマスクされます。

ログインマクロを使用するスキャンの[スキャン設定:認証(Scan Settings: Authentication)]で[マクロ検証を有効にする(Enable macro validation)]が選択されている場合、Fortify WebInspectはスキャンの開始時点でログインマクロをテストして、ログインが成功したことを確認します。マクロが無効で、アプリケーションへのログインに失敗した場合、スキャンは停止し、エラーメッセージがスキャンログファイルに書き込まれます。詳細とトラブルシューティングのヒントについては、「["ログインマクロのテスト" ページ 510](#)」を参照してください。

重要! 2要素認証を含むマクロを使用する場合は、スキャンを開始する前に、2要素認証アプリケーションの設定を行う必要があります。詳細については、「["アプリケーション設定:2要素認証" ページ453](#)」を参照してください。

次の表の説明に従って操作を進めます。

| 目的... | 手順... |
|------------------------------------|---|
| 事前に記録されたWeb Macro Recorderマクロを使用する | <p>省略記号ボタン(...)をクリックしてマクロを選択します。</p> <p>マクロを選択した後で、Web Macro Recorderを使用してマクロを変更する場合は、[編集(Edit)]をクリックします。</p> <p>ヒント: マクロ名を消去するには、[サイト認証(Site Authentication)]チェックボックスをオフにします。</p> |

| 目的... | 手順... |
|--|--|
| 新しいマクロを作成する | <p>【記録(Record)】をクリックします。 Web Macro Recorderが開きます。</p> <p>メモ: Web Macro Recorderの使用法の詳細については、Web Macro Recorderのヘルプを参照してください。</p> |
| <p>ログインマクロを自動的に作成する</p> <p>メモ: 権限のエスカレーションおよびマルチユーザログインスキャン用のログインマクロは自動的に作成できません。</p> | <p>a. 【ログインマクロの自動生成(Auto-gen Login Macro)】を選択します。</p> <p>b. 【ユーザ名(Username)】フィールドにユーザ名を入力します。</p> <p>c. 【パスワード>Password)】フィールドにパスワードを入力します。</p> <p>オプションで、【テスト(Test)】をクリックして、ログインフォームの検索、マクロの生成、マクロ検証テストの実行を行ってから、スキャンウィザードの次のステージに進みます。完了前に検証テストをキャンセルする必要がある場合は、【キャンセル(Cancel)】をクリックします。</p> <p>マクロが無効で、アプリケーションへのログインが失敗すると、エラーメッセージが表示されます。詳細とトラブルシューティングのヒントについては、「"ログインマクロのテスト" ページ510」を参照してください。</p> |

5. 【次へ(Next)】をクリックします。

力バレッジと徹底性

1. Oracle Application Development Framework FacesのコンポーネントまたはIBM WebSphere Portalのいずれかを使用して構築されたアプリケーションの設定を最適化するには、【フレームワーク(Framework)】を選択し、【スキャンの最適化対象(Optimize scan for)】リストから【Oracle ADF Faces】または【WebSphere Portal】を選択します。Fortifyでは、他の設定オーバーレイを開発し、スマートアップデートを通じて提供することができます。
WebSphere Portalのスキャンの詳細については、「["WebSphere Portalに関するFAQ" ページ300](#)」を参照してください。
2. 【Web探索範囲(CrawlCoverage)】スライダを使用して、Web探索プログラム設定を指定します。

このスライダが使用可能かどうかは、選択したスキャンモードによって決まります。このスライダに関連付けられているラベルも、選択した内容に応じて異なります。このスライダが使用可能な場合、スライダではWeb探索の4つの位置から1つを選択できます。それぞれの位置は、特定の設定コレクションを表しており、次のラベルで示されています。

徹底(Thorough)

徹底Web探索とは、次の設定を使用する自動Web探索です。

- 冗長ページ検出(Redundant Page Detection): **オフ(OFF)**
- 単一URL最大ヒット数(Maximum Single URL Hits): **10**
- Webフォーム最大送信数(Maximum Web Form Submissions): **7**
- ページあたりの最大スクリプトイベント数(Maximum Script Events Per Page): **2000**
- セッションあたりの許容ダイナミックフォーム数(Number of Dynamic Forms Allowed Per Session): **無制限(Unlimited)**
- ヒット数にパラメータを含める(Include Parameters In Hit Count): **True**

デフォルト(Default)

デフォルトのWeb探索とは、次の(デフォルトスキャン)設定を使用する自動Web探索です。

- 冗長ページ検出(Redundant Page Detection): **オフ(OFF)**
- 単一URL最大ヒット数(Maximum Single URL Hits): **5**
- Webフォーム最大送信数(Maximum Web Form Submissions): **3**
- ページあたりの最大スクリプトイベント数(Maximum Script Events Per Page): **1000**
- セッションあたりの許容ダイナミックフォーム数(Number of Dynamic Forms Allowed Per Session): **無制限(Unlimited)**
- ヒット数にパラメータを含める(Include Parameters In Hit Count): **True**

中程度(Moderate)

標準的なWeb探索とは、次の設定を使用する自動Web探索です。

- 冗長ページ検出(Redundant Page Detection): **オフ(OFF)**
- 単一URL最大ヒット数(Maximum Single URL Hits): **5**
- Webフォーム最大送信数(Maximum Web Form Submissions): **2**
- ページあたりの最大スクリプトイベント数(Maximum Script Events Per Page): **300**
- セッションあたりの許容ダイナミックフォーム数(Number of Dynamic Forms Allowed Per Session): **1**
- ヒット数にパラメータを含める(Include Parameters In Hit Count): **False**

クイック(Quick)

クイックWeb探索では、次の設定が使用されます。

- 冗長ページ検出(Redundant Page Detection): **オン(ON)**
- 単一URL最大ヒット数(Maximum Single URL Hits): 3
- Webフォーム最大送信数(Maximum Web Form Submissions): 1
- ページあたりの最大スクリプトイベント数(Maximum Script Events Per Page): 100
- セッションあたりの許容ダイナミックフォーム数(Number of Dynamic Forms Allowed Per Session): 0
- ヒット数にパラメータを含める(Include Parameters In Hit Count): **False**

「**設定(Settings)**」]をクリックして(「**詳細設定(Advanced Settings)**」]ダイアログボックスを開き)、設定を変更して、スライダに4つある位置の1つで定められている設定と対立した場合、スライダにはカスタマイズされたカバレッジ設定(Customized Coverage Settings)という名前の5つ目の位置が作成されます。

- 監査深度(ポリシー)(Audit Depth (Policy))]リストからポリシーを選択します。
このリストが使用可能かどうかは、スキャンウィザードのステップ1で選択したスキャンモードによって決まります。ポリシーの詳細については、「["Fortify WebInspectのポリシー" ページ 473](#)」を参照してください。
- 次へ(Next)]をクリックします。

詳細スキャン設定(Detailed Scan Configuration)

Profiler

Fortify WebInspectは、ターゲットWebサイトの事前テストを実行し、特定の設定を変更すべきかどうかを判断します。変更が必要だと思われる場合、Profilerは提案のリストを返します。これらの提案は、受け入れることも拒否することもできます。

たとえば、Server Profilerは、サイトに入るための権限付与が必要であるものの、有効なユーザ名とパスワードが指定されていないことを検出するかもしれません。そのままスキャンを続行して著しく質の低い結果を得るのではなく、Server Profilerの提案に従って、続行する前に必要な情報を設定することができます。

同様に、設定では、Fortify WebInspectが「ファイルが見つからない」の検出を実行しないように指定されていることもあります。このプロセスは、存在しないリソースをクライアントから要求されてもステータス「404 Not Found」を返さないWebサイトで役に立ちます(代わりにステータス「200 OK」が返される場合がありますが、応答にはファイルが見つからないというメッセージが含まれます)。Profilerは、このような手法がターゲットサイトに実装されていると判断した場合、この特徴に対応できるようにFortify WebInspect設定を変更することを推奨します。

このページにアクセスするたびにProfilerを起動するには、「**Profilerを自動的に実行する(Run Profiler Automatically)**」]を選択します。

Profilerを手動で起動するには、[プロファイル(Profile)]をクリックします。詳細については、「["Server Profiler" ページ256](#)」を参照してください。

結果が[設定(Settings)]セクションに表示されます。

設定(Settings)

- 提案を受諾または拒否します。拒否するには、対応するチェックボックスをオフにします。
- 必要に応じて、要求された情報を入力します。
- [次へ(Next)]をクリックします。

Profilerを実行しない場合でも、いくつかのオプションが表示されることがあります。以下のものが含まれます。

- Webフォームの自動入力(Auto fill Web forms)
- 許可ホストの追加(Add allowed hosts)
- 識別された誤検出を再利用する(Reuse identified false positives)
- サンプルマクロの適用(Apply sample macro)
- トラフィック分析(Traffic analysis)

Webフォームの自動入力(Auto fill Web forms)

Fortify WebInspectがターゲットサイトのスキャン中に検出されるフォームの入力コントロールの値を送信するようにするには、[Web探索時のWebフォームの自動入力(Auto-fill Web forms during crawl)]を選択します。Fortify WebInspectは、事前パッケージ化されたデフォルトファイル、またはWeb Form Editorを使用して作成したファイルから値を抽出します。以下を実行できます。

- 省略記号ボタン...をクリックして、ファイルを見つけてロードします。
- [編集(Edit)][Edit]をクリックして、選択したファイル(またはデフォルト値)をWeb Form Editorで編集します。
- [作成(Create)][Create]をクリックしてWeb Form Editorを開き、ファイルを作成します。

許可ホストの追加(Add Allowed Hosts)

[許可ホスト(Allowed Host)]設定は、Web探索して監査するドメインを追加する場合に使用します。Webプレゼンスで複数のドメインが使用されている場合は、それらのドメインをここに追加します。詳細については、「["スキャン設定:許可ホスト" ページ389](#)」を参照してください。

許可するドメインを追加するには:

- [追加(Add)]をクリックします。
- [許可ホストの指定(Specify Allowed Host)]ウィンドウで、URL(またはURLを表す正規表現)を入力し、[OK]をクリックします。

許可ホストの追加または編集の詳細については、「["許可ホストの指定" ページ192](#)」を参照してください。

識別された誤検出を再利用する(Reuse Identified False Positives)

誤検出に変更された脆弱性を含むスキャンを選択します。このスキャンで検出された脆弱性がこれらの誤検出と一致する場合、脆弱性は誤検出に変更されます。詳細については、「["誤検出\(False Positives\)" ページ89](#)」を参照してください。

識別された誤検出を再利用するには:

1. **誤検出のインポート(Import False Positives)**]を選択します。
2. **【スキャンの選択(Select Scans)**]をクリックします。
3. 現在スキャンしている同じサイトからの誤検出を含むスキャンを1つ以上選択します。
4. **OK]**をクリックします。

メモ: スキャンのスケジューリング時 やエンタープライズスキャンの実行時に誤検出をインポートすることはできません。

サンプルマクロ

Fortify WebInspectのサンプルバンキングアプリケーション(zero.webappsecurity.com)では、Webフォームログインが使用されています。このサイトをスキャンする場合は、**サンプルマクロの適用(Applied sample macro)**]を選択して、ログインスクリプトを含むサンプルマクロを実行します。

トラフィック分析(Traffic Analysis)

Web Proxyツールを使用してFortifyにより発行されたHTTP要求とターゲットサーバから返された応答を検査するには、**【Web Proxyの起動およびWeb Proxy経由でのトラフィックの送信(Launch and Direct Traffic through Web Proxy)**]を選択します。

Fortify WebInspectはWebサイトのスキャン中に、Webサイトの階層構造を明らかにするセッションと、脆弱性が検出されたセッションのみをナビゲーションペインに表示します。ただし **【Traffic Monitorを有効にする(Enable Traffic Monitor)**]を選択すると、Fortify WebInspectでは **【Traffic Monitor】**ボタンが **【スキャン情報(Scan Info)**]パネルに追加されます。これにより、Fortify WebInspectが送信した各HTTP要求と、サーバから受信した関連HTTP応答を表示して確認できます。

メッセージ

Profilerが変更を推奨しない場合は、スキャンウィザードに「設定の変更は推奨されません。現在のスキャン設定はこのサイトに最適です。(No settings changes are recommended. Your current scan settings are optimal for this site.)」というメッセージが表示されます。

その後の作業(Congratulations)

このウィンドウに表示される内容は、選択内容と設定によって異なります。

Fortify WebInspect Enterpriseスキャンテンプレートへのアップロード

エンタープライズサーバ(Fortify WebInspect Enterprise)に接続している場合、このスキャンの設定をFortify WebInspect Enterpriseに送信できます。これにより、スキャンテンプレートが作成されます。ただし、スキャンテンプレートを作成できる役割が自分に割り当てられている必要があります。

設定の保存

このスキャン用に設定した内容を保存しておき、将来のスキャンで設定を再利用できます。

レポートの生成

スキャンをスケジュールしている場合は、スキャン完了時にレポートを生成することをFortify WebInspectに対して指示できます。

1. [レポートの生成(Generate Reports)]を選択します。
2. [レポートの選択>Select reports)]ハイパーキーをクリックします。
3. (オプション) [お気に入り(Favorites)]リストからレポートを選択します。
「お気に入り」は、1つ以上のレポートとその関連パラメータの単なる名前付きコレクションです。レポートおよびパラメータを選択した後でお気に入りを作成するには、[お気に入り(Favorites)]リストをクリックして、[お気に入りに追加(Add to favorites)]を選択します。
4. 1つ以上のレポートを選択します。
5. 要求できるパラメータの情報を入力します。必須のパラメータは赤で囲まれます。
6. [次へ(Next)]をクリックします。
7. [ファイル名の自動生成(Automatically Generate Filename)]を選択すると、レポートファイルの名前は<reportname> <date/time>.<extension>の形式になります。たとえば、pdf形式でコンプライアンスレポートを作成し、そのレポートが4月5日の6:30に生成される場合、ファイル名は「Compliance Report 04_05_2009 06_30.pdf」になります。これは、反復スキャンの場合に便利です。
レポートは、生成されるレポート用にアプリケーション設定で指定されたディレクトリに書き込まれます。
8. [ファイル名の自動生成(Automatically Generate Filename)]を選択しなかった場合は、[ファイル名(Filename)]ボックスにファイルの名前を入力します。
9. [エクスポート形式(Export Format)]リストからレポート形式を選択します。
10. 複数のレポートを選択した場合は、[レポートを1つに集約(Aggregate reports into one report)]を選択することで、すべてのレポートを1つに結合できます。
11. レポートに使用するヘッダとフッタを定義するテンプレートを選択し、必要に応じて要求されたパラメータを指定します。
12. [完了(Finished)]をクリックします。
13. [スケジュール(Schedule)]をクリックします。

Site List Editorの使用

基本スキャンウィザードを使用してリストドリブンスキャンを実行する場合、Site List Editorを使用してURLのリストを作成または編集できます。

Site List Editorにアクセスするには:

- 基本スキャンウィザードの [リストドリブンスキャン(List-Driven Scan)] オプションの下にある [管理(Manage)] をクリックします。

個々のURLを手動で追加するには:

- [追加(Add)] をクリックします。
- スキャンに追加するURLを入力します。プロトコルを指定しない場合、エディタによって URLの先頭に「http://」が追加されます。
- 必要に応じて、操作を繰り返します。

テキストファイルまたはXMLファイルに指定されているURLを追加するには:

- [インポート(Import)] をクリックします。
- 標準のファイル選択ウィンドウを使用して、ファイルを見つけて [開く(Open)] をクリックします。
- 必要に応じて、操作を繰り返します。

メモ: エディタでは重複はチェックされません。2つのリストをインポートし、両方のリストに同じURLが含まれている場合、そのURLは2回リストに含められます。

また、各URLにはプロトコル(http://またはhttps://など)が含まれている必要があります。手動での入力とは異なり、インポートされたURLの先頭にはプロトコルは自動的に追加されません。

エントリを編集するには:

- URLをクリックします。

エントリを削除するには:

- URLを選択し、[削除(Delete)] をクリックします。

次も参照

["基本スキャンの実行\(Webサイトスキャン\)" ページ178](#)

プロキシプロファイルの設定

基本スキャンを実行し、PAC (Proxy Automatic Configuration) ファイルからプロキシ設定を使用するか、明示的なプロキシ設定(Explicit Proxy Settings)を指定する場合は、[プロキシプロファイル(Proxy Profile)] ウィンドウでプロキシオプションを設定できます。

「プロキシプロファイル(Proxy Profile)」ウィンドウにアクセスするには:

- 基本スキャンウィザードの「ネットワークプロキシ(Network Proxy)」にある「編集(Edit)」をクリックします。

PACファイルを使用してプロキシを設定する

プロキシ設定をPAC (Proxy Automatic Configuration)ファイルからロードします。「URL」ボックスにファイルの場所を指定します。

プロキシを明示的に設定する(Explicitly configure proxy)

要求された情報を入力することによって、プロキシを設定します。

1. 「サーバ(Server)」ボックスにプロキシサーバのURLまたはIPアドレスを入力し、続いて「ポート(Port)」ボックスにポート番号(8080など)を入力します。
2. 「タイプ(Type)」リストから、プロキシサーバ経由のTCPトラフィックを処理するプロトコルを選択します。
 - SOCKS4
 - SOCKS5
 - 標準(Standard)
3. 認証が必要な場合は、「認証(Authentication)」リストからタイプを選択します。
 - 自動
 - 基本(Basic)
 - ダイジェスト(Digest)
 - Kerberos
 - ネゴシエート(Negotiate)
 - NT LAN Manager (NTLM)
4. プロキシサーバで認証が必要な場合は、適格なユーザ名とパスワードを入力します。
5. 特定のIPアドレス(内部テストサイトなど)にアクセスするためにプロキシサーバを使用する必要がない場合は、「プロキシをバイパスするサイト(Bypass Proxy For)」ボックスにアドレスまたはURLを入力します。エントリはカンマで区切ります。

次も参照

["基本スキャンの実行\(Webサイトスキャン\)" ページ178](#)

許可ホストの指定

Web探索するドメインを追加するには許可ホストを指定します。Webプレゼンスで複数のドメインが使用されている場合は、それらのドメインをここに追加します。たとえば、「Wexample.com」をスキャンする場合、「Wexample2.com」と「Wexample3.com」がWeb

プレゼンスの一部であり、かつそれらをWeb探索または監査に含めたいのであれば、それらのドメインをここに追加する必要があります。

この機能を使用して、指定したテキストが名前に含まれているドメインをスキャンすることもできます。たとえば、スキャンターゲットとして「www.myco.com」を指定し、許可ホストとして「myco」と入力したとします。Fortify WebInspectは、ターゲットサイトをスキャンして「myco」を含むURLへのリンクを検出すると、そのリンクをたどってそのサイトのサーバをスキャンします。この処理は、すべてのリンク先のサイトがスキャンされるまで繰り返されます。この仮説例では、Fortify WebInspectによって次のドメインがスキャンされます。

- www.myco.com:80
- contact.myco.com:80
- www1.myco.com
- ethics.myco.com:80
- contact.myco.com:443
- wow.myco.com:80
- mycocorp.com:80
- www.interconnection.myco.com:80

ポート番号を指定する場合は、許可ホストが完全に一致する必要があることに注意してください。

許可ホストの指定

許可ホストを指定(追加)するには:

1. 基本スキャンウィザードの [詳細スキャン設定(Detailed Scan Configuration)] ページで、[追加(Add)] をクリックします。
2. [許可ホストの指定(Specify Allowed Host)] ダイアログボックスで、URL (またはURLを表す正規表現)を入力します。

メモ: URLを指定する場合は、プロトコル指定子 (http://やhttps://など)を含めないでください。

3. 許可ホストの正規表現を入力した場合は、[正規表現を使用する(Use Regular Expression)] を選択します。

正規表現の作成のヒントについては、 ([許可ホスト(Allowed Host)] ボックスの右側)をクリックします。

4. [OK] をクリックします。

許可ホストの編集

許可ホストを編集するには:

1. 基本スキャンウィザードの [詳細スキャン設定(Detailed Scan Configuration)] ページでホストを選択し、[編集(Edit)] をクリックします。

2. [許可ホストの編集(Edit Allowed Host)]ダイアログボックスで、URL (またはURLを表す正規表現)を編集します。

メモ: URLを編集する場合は、プロトコル指定子 (http://やhttps://など)を含めないでください。

3. [OK]をクリックします。

次も参照

["基本スキャンの実行\(Webサイトスキャン\)" ページ178](#)

マルチユーザログインスキャン

ユーザごとに1つのアクティブルoginセッションのみを許可するアプリケーションでは、マルチスレッドスキャンができません。複数のログインが行われると、スレッドどうしによって相互の状態が無効にされ、スキャン時間が遅くなります。

この問題を解決するには、ログインマクロに記録された資格情報をパラメータに変換し、同じアプリケーション特権を持つ複数のログインアカウントを使用します。[スキャンの設定:認証(Scan Settings: Authentication)]ウィンドウの[マルチユーザログイン(Multi-user Login)]オプションを使用すると、ログインマクロ内のユーザ名とパスワードをパラメータ化し、スキャンで使用する複数のユーザ名とパスワードのペアを定義できます。2要素認証が必要な場合は、電話番号、電子メール、および電子メールパスワードをパラメータ化することもできます。

このアプローチを使用すると、複数のスレッドでスキャンを実行できます。スレッドごとにログインセッションが異なるため、スキャン時間が短縮されます。

作業を開始する前に

マルチユーザログインスキャンを設定するには、パラメータ化されたログインマクロを使用する必要があります。詳細については、『*Micro Focus Fortify WebInspect Tools Guide*』の「Web Macro Recorder」の章の「パラメータの操作」トピックを参照してください。

既知の制限事項

マルチユーザログイン機能には、次の既知の制限事項が適用されます。

- この機能を使用する場合、Fortify WebInspectはログイン関連の複数のSecurebaseチェックを検出しません。
- この機能は現在、共有リクエスタスレッドのみをサポートしています。Web探索と監査の別個のスレッドでデフォルトのスキャン設定を使用することは、サポートされていません。詳細については、「["スキャン設定:リクエスタ" ページ382](#)」を参照してください。
- ログインしている複数のユーザ間でスキャンの作業が等しく分散されません。たとえば、1人の設定済みユーザがスキャンアクティビティの最大75%を使用し、他のすべてのユーザが残りの25%のスキャンアクティビティに割り当たられる場合があります。

プロセスの概要

マルチユーザログインスキャンを設定するには、次の表で説明されているプロセスを使用します。

| ステージ | 説明 |
|------|--|
| 1. | <p>共有リクエスタを目的のユーザ数に設定します。詳細については、「"スキャン設定: リクエスタ" ページ382」を参照してください。</p> <p>重要! 共有リクエスタスレッドの数が、設定されたユーザの数を超えないようにする必要があります。有効なユーザを持たないリクエスタスレッドでは、スキャンの実行時間が長くなります。複数のユーザを設定する場合は、最初のユーザとして、パラメータ化されたマクロ内のオリジナルのユーザ名とパスワードをカウントすることを忘れないでください。</p> |
| 2. | <p>パラメータ化されたユーザ名とパスワードを含むログインマクロを使用してください。2要素認証が必要な場合は、必要に応じて、電話番号、電子メール、および電子メールパスワードをパラメータ化します。詳細については、『<i>Micro Focus Fortify WebInspect Tools Guide</i>』の「Web Macro Recorder」の章の「パラメータの操作」トピックを参照してください。</p> |
| 3. | <p>基本スキャンウィザードまたはガイド付きスキャンウィザードで、「"マルチユーザログインのスキャンの設定" 下」の説明に従って、マルチユーザのチェックボックスを有効にします。</p> |
| 4. | <p>「"資格情報の追加" 次のページ」の説明に従って、複数のユーザの資格情報を追加します。</p> |
| 5. | <p>通常どおりにスキャンウィザードを進め、スキャンを実行します。</p> |

マルチユーザログインのスキャンの設定

マルチユーザログインスキャンを設定するには:

- 次のいずれかを実行します。
 - 基本スキャンウィザードでは、[編集(Edit)]> [現在のスキャン設定(Current Scan Settings)]をクリックします。次に、[スキャン設定(Scan Settings)]> [認証(Authentication)]を選択します。
 - ガイド付きスキャンウィザードでは、リボンの[詳細設定(Advanced)]をクリックし、[スキャン設定(Scan Settings)]> [認証(Authentication)]を選択します。

2. [フォーム認証にログインマクロを使用する(Use a login macro for forms authentication)] チェックボックスを選択します。

重要! マルチユーザログインオプションを有効にするには、このチェックボックスをオンにする必要があります。

3. 次のいずれかを実行します。

- 新しいマクロを記録するには、通常どおり [記録(Record)] をクリックしてログインマクロを記録します。

メモ: ガイド付きスキャンの場合は、ログインマクロを記録するための別のステージが含まれているため、[記録(Record)] ボタンを使用できません。マクロを記録した後、資格情報をパラメータ化する必要があります。

- 既存のマクロを使用するには、[...] をクリックして、すでにパラメータ化された資格情報を持つ保存済みマクロを選択します。

4. [マルチユーザログイン(Multi-user Login)] チェックボックスをオンにします。

メモ: スキャンを実行する前に [マルチユーザログイン(Multi-user Login)] チェックボックスをオフにすると、スキャン中に追加の資格情報が使用されません。Fortify WebInspectは、ログインマクロに記録されたオリジナルの資格情報のみを使用します。

5. 次のように続行します。

- ユーザの資格情報を追加するには、「"資格情報の追加" 下」に進みます。
- ユーザの資格情報を編集するには、「"資格情報の編集" 次のページ」に進みます。
- ユーザの資格情報を削除するには、「"資格情報の削除" 次のページ」に進みます。

6. ユーザの資格情報を設定した後、通常どおりにスキャンウィザードを進め、スキャンを実行します。

資格情報の追加

資格情報を追加するには:

1. [マルチユーザログイン(Multi-user Login)] で、[追加(Add)] をクリックします。
[マルチユーザ資格情報入力(Multi-user Credential Input)] ダイアログボックスが表示されます。
2. [ユーザ名(Username)] ボックスに、ユーザ名を入力します。
3. [パスワード>Password)] ボックスに、対応するパスワードを入力します。
4. 2要素認証が必要な場合は、必要に応じて次の表の説明に従って操作を進めます。

| この資格情報ボックスの場合 ... | これを入力 ... |
|----------------------------|------------------------------------|
| 電話番号(Phone Number) | ユーザ名に対応する電話番号(SMS応答を受信するため) |
| 電子メール>Email) | ユーザ名に対応する電子メールアドレス(電子メール応答を受信するため) |
| 電子メールパスワード>Email Password) | 電子メールアドレスのパスワード(電子メール応答を受信するため) |

5. [OK]をクリックします。
6. 追加するユーザログインごとにステップ1-5を繰り返します。

重要! 共有リクエスタスレッドの数が、設定されたユーザの数を超えないようにする必要があります。有効なユーザを持たないリクエスタスレッドでは、スキャンの実行時間が長くなります。複数のユーザを設定する場合は、最初のユーザとして、パラメータ化されたマクロ内のオリジナルのユーザ名とパスワードをカウントすることを忘れないでください。詳細については、「["スキャン設定: リクエスタ" ページ382](#)」を参照してください。

資格情報の編集

資格情報を編集するには:

1. [マルチユーザログイン(Multi-user Login)]で、テーブル内のエントリを選択し、[編集(Edit)]をクリックします。
[マルチユーザ資格情報入力(Multi-user Credential Input)]ダイアログボックスが表示されます。
2. 必要に応じて資格情報を編集します。
3. [OK]をクリックします。

資格情報の削除

資格情報を削除するには:

1. [マルチユーザログイン(Multi-user Login)]で、削除するテーブル内のエントリを選択します。
2. [削除>Delete)]をクリックします。

2要素認証の使用

2要素認証は、「自分が知っているもの」の要素として定義される通常のパスワードを、次のいずれかを使用して補います。

- SMSまたは電子メールで送信されるワンタイムパスコード(OTP)など、自分が所有しているもの
- 指紋、顔、または網膜など、自分の体の一部

この2つ目の認証要素はセキュリティを向上させますが、それを実装するWebアプリケーションの自動スキャンを行う際の複雑さが増大します。

Fortifyエンジニアは、Fortify WebInspectとMacro Engine 6.1を使用するWeb Macro Recorderにより、2要素認証の「自分が所有しているもの」の要素を自動化する方法とプロセスを開発しました。

2要素認証を使用するスキャンの仕組み

Fortify WebInspectにはNode.jsサーバが含まれており、これを設定して、アプリケーションサーバから受信するSMSおよび電子メールの応答をコントロールセンターで処理できます。また、SMS応答をコントロールセンターに転送するモバイルアプリケーションもあります。コントロールセンターは応答をキューに登録し、認証が必要になったら、適切なTruClientブラウザに転送します。

テクノロジプレビュー

この機能はテクノロジプレビューとして提供されます。

テクノロジプレビュー機能は現在サポートされていないため、完全に機能しない可能性があります。また、運用環境での展開には適しません。ただし、これらの機能は、将来的には完全なサポートを提供できることを目指すために広く拡大することを主な目的として、便宜的に提供されています。

推奨

Fortifyでは、テスト用電話とテスト用電子メールアドレスのみを使用するよう強くお勧めします。プライバシー上の懸念があるため、個人用の電話や電子メールアドレスは使用しないでください。

既知の制限事項

次の既知の制限事項が2要素認証機能に適用されます。

- UIDL (Unique ID Listing)をサポートするPOP3サーバだけがサポートされています。
- 現在サポートされているのはAndroid携帯電話のみです。
- 携帯電話では、Fortify WebInspectがインストールされているのと同じサブネット内のWi-Fiに接続する必要があります。

プロセスについて

次の表では、2要素認証を使用してスキャンを実行するプロセスについて説明します。

| ステージ | 説明 |
|------|--|
| 1. | <p>2要素認証のFortify WebInspectアプリケーション設定で、次の操作を実行します。</p> <ul style="list-style-type: none">• 2要素認証コントロールセンターを設定する• モバイルアプリケーションを設定する(SMS応答を使用する場合) <p>詳細については、「"アプリケーション設定: 2要素認証" ページ453」を参照してください。</p> |
| 2. | <p>Macro Engine 6.1を使用するWeb Macro Recorderでログインマクロを記録して、次のように変更します。</p> <ol style="list-style-type: none">1. 2要素認証(Two-factor authentication)]グループステップを追加および設定します。 メモ: [SMS]または[電子メール(email)]の応答のグループステップを設定する必要があります。グループステップには、2FAを待機する(Wait for 2FA)]ステップが含まれます。このステップも設定する必要があります。2. オプションで、ユーザ名、パスワード、電話番号、電子メール、および電子メールパスワードのパラメータを作成します。2要素認証のパラメータを使用すると、マルチユーザログインスキャンを実行できます。3. 2FAを待機する(Wait for 2FA)]ステップを設定します。4. 汎用オブジェクトアクション(Generic Object Action)]ステップを追加し、それをタイプ(Type)]ステップとして設定します。5. 汎用オブジェクトアクション(Generic Object Action)]ステップを追加し、それをクリック(Click)]ステップとして設定します。 |

| ステージ | 説明 |
|------|--|
| | 詳細については、『 <i>Micro Focus Fortify WebInspect Tools Guide</i> 』を参照してください。 |
| 3. | Web Macro Recorderで、ログインマクロを再生します。 |
| 4. | オプションで、マルチユーザログインスキャンを実行する場合は、[スキャン設定:認証(Scan Settings: Authentication)]ウィンドウに、ユーザ名、パスワード、電話番号、電子メール、および電子メールパスワードの資格情報を追加します。詳細については、「 "マルチユーザログインスキャン" ページ194 」と「 "スキャン設定:認証" ページ408 」を参照してください。 |
| 5. | Fortify WebInspectで、マクロを使用してスキャンを実行します。 |

対話型スキャン

CAPTCHAなど、特定のタイプのアンチスキャンテクノロジを使用するWebアプリケーションでは、WebInspectで対話型のスキャン設定が必要になります。対話型スキャンでは、認証のためのユーザ入力を求めるブラウザウィンドウが表示されます。入力フィールドが検出された場合にのみ一時停止する自動対話型スキャンを設定できます。この一時停止は、入力フィールドが検出されたリクエスタスレッドにのみ影響します。残りのスレッドには影響しません。

対話型スキャン設定は、CAPTCHA、RSA IDトークンフィールド、仮想PINパッド、仮想キーボード、およびPINまたは入力がダイナミックで変化する共通アクセスカード(CAC)リーダに対して機能します。

ヒント: スタティックPINでCACリーダを使用するWebサイトでは、CAC証明書を使用するようにスキャンを設定できます。次のいずれかのトピックを参照してください。

- ["スキャン設定:認証" ページ408](#)
- ["基本スキャンの実行\(Webサイトスキャン\)" ページ178](#)
- ["ネイティブスキャンテンプレートの使用" ページ154](#)
- ["モバイルスキャンテンプレートの使用" ページ135](#)
- ["事前定義テンプレートの使用" ページ118](#)

メモ: 2要素認証では、対話型スキャンは不要です。2要素認証を使用して、完全に自動化されたスキャンを設定できます。詳細については、「["2要素認証の使用" ページ198](#)」を参照してください。

対話型スキャンの設定

次の表で、対話型スキャンを設定するためのプロセスについて説明します。

| ステージ | 説明 |
|------|---|
| 1. | <p>次のようにWebフォーム入力ファイルを準備します。</p> <ol style="list-style-type: none"> 1. Web Form Editorツールにフィールド名を記録するか入力します。 2. フォーム名を右クリックし、対話型としてマークする(Mark As Interactive)を選択します。 3. Webフォーム入力ファイルを保存します。 <p>詳細については、『<i>Micro Focus Fortify WebInspect Tools Guide</i>』の「Web Form Editor」の章を参照してください。</p> |
| 2. | <p>ダイナミックPINを必要とするクライアント側証明書を使用していますか。</p> <ul style="list-style-type: none"> 「はい」の場合は、Internet Explorerを起動して、クライアント側の証明書が一覧表示されていることを確認するか、手動でインポートします。 <p>この操作により、証明書が一時的にWindowsの証明書ストアにロードされます。</p> <p>メモ: ハードウェアトークンに接続し、要求されたPINを入力すると、これが自動的に行われます。</p> <ul style="list-style-type: none"> 「いいえ」の場合は、ステージ3にスキップします。 |
| 3. | <p>対話型スキャンモードのスキャン方法を次のように設定します。</p> <ol style="list-style-type: none"> 1. スキャン設定: 方法(Scan Settings: Method) ウィンドウを開きます。 2. Webフォームの自動入力(Auto fill web forms) フィールドで、ステージ1で作成したWebフォーム入力ファイルを指定します。 3. スキャン中にWebフォーム値の入力を要求する(対話型モード)(Prompt for web form values during scan (interactive mode)) チェックボックスをオンにします。 4. タグ付けされた入力に対してのみプロンプトを表示する(Only prompt for tagged inputs) チェックボックスをオンにします。 <p>メモ: この最後のチェックボックスが選択されていない場合は、サイトで検出されたすべての入力に対してプロンプトが表示されます。</p> |
| 4. | <p>ダイナミックPINを必要とするクライアント側証明書を使用していますか。</p> <ul style="list-style-type: none"> 「はい」の場合は、次の手順に従って、クライアント側証明書を使用するように認証を設定します。 <ol style="list-style-type: none"> a. スキャン設定: 認証(Scan Settings: Authentication) ウィンドウを開きます。 |

| ステージ | 説明 |
|------|--|
| | <p>b. [クライアント証明書(Client Certificates)]エリアで 有効にする]チェックボックスをオンにして、ユーザの証明書を参照して選択します。</p> <p>Fortify WebInspectでは、この証明書がタイムアウトして、要求されたPINの入力に失敗するまで、またはハードウェアトークンが削除され、Windowsで証明書がストアから削除されるまで、この証明書が使用されます。</p> <ul style="list-style-type: none"> 「いいえ」の場合は、ステージ5にスキップします。 |
| 5. | <p>スキャン設定を保存して、それらの設定をFortify WebInspectスキャンで使用します。</p> <p>重要! 必要に応じて、ポップアップを確認してフォームの値を入力する必要があります。</p> |

「フォルダに限定」に関する制限

このトピックでは、JavaScriptのインクルードファイルが検出されるか、ログインマクロまたはワークフローマクロが使用される場合の、「**フォルダに限定(Restrict to folder)**」スキャンオプションに関する制限について説明します。

JavaScriptインクルードファイル

スキャン中に、Web探索プログラムとJavaScriptエンジンは、外部のJavaScriptインクルードファイルにアクセスすることができます。これらのファイルはアクティブに監査されないので、攻撃がHTTP経由で送信されることはありません。ただし、パッシブな調査によってJavaScriptインクルードファイルの問題が明らかになり、これらのファイルがサイトツリーに一覧表示されることがあります。

ログインマクロ

ログインマクロを使用する場合、そのマクロで要求されるセッションはサイトツリーに一覧表示されます。セッションはパッシブに監査されます。つまり、攻撃は送信されませんが、弱い暗号化、暗号化されないログインフォームなどの脆弱性が明らかになる可能性があります。

ワークフローマクロ

[Web探索および監査(Crawl and Audit)]スキャンまたは[Web探索のみ(Crawl Only)]スキャンでワークフローマクロを使用する場合、スキャンは「**フォルダに限定(Restrict to folder)**」オプションに違反する可能性があります。ワークフローマクロに含まれるURLにアクセスすることを希望していると見なされます。

エンタープライズスキャンの実行

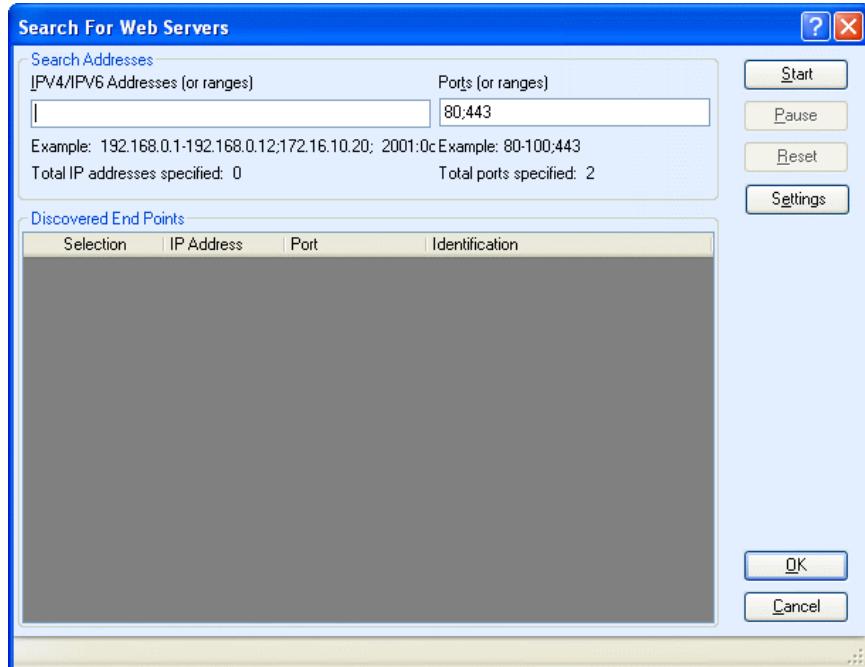
エンタープライズスキャンは、Webプレゼンスの包括的な概観を企業ネットワークの観点から提供します。Fortify WebInspectを使用すると、ある範囲のIPアドレスで使用可能なすべてのポートが自動的に検出されます。その後、検出された全サーバから脆弱性を評価するサーバを選択できます。

エンタープライズスキャンを開始するには:

1. 次のいずれかを実行して、エンタープライズスキャンウィザードを起動します。
 - Fortify WebInspectの [開始ページ(Start Page)] で、[エンタープライズスキャンの開始(Start an Enterprise scan)] をクリックします。
 - [ファイル(File)] > [新規作成(New)] > [エンタープライズスキャン(Enterprise Scan)] の順にクリックします。
 - (ツールバーの) [新規(New)] アイコンでドロップダウン矢印をクリックし、[エンタープライズスキャン(Enterprise Scan)] を選択します。
 - Fortify WebInspectの [開始ページ(Start Page)] で、[スケジュールされたスキャンの管理(Manage Scheduled Scans)] をクリックし、[追加(Add)] をクリックしてから [エンタープライズスキャン(Enterprise Scan)] を選択します。
2. エンタープライズスキャンウィザードのステップ1で、スキャンを実行するタイミングを指定します。次の選択肢があります。
 - **即時(Immediately)**: スケジュールされたスキャンウィザードを終了するとすぐにスキャンが実行されます。
 - **日時指定で1回実行(Run Once Date / Time)**: スキャンを開始する日時を変更します。ドロップダウン矢印をクリックすると、日付を選択するカレンダを表示できます。
 - **定期実行スケジュール(Recurrence Schedule)**: スライダを使用して、頻度(毎日(Daily)、毎週(Weekly)、または毎月(Monthly))を選択します。次に、スキャンを開始する時刻を指定し、(毎週(Weekly)または毎月(Monthly))の場合はその他のスケジュール情報を指定します。
3. [次へ(Next)] をクリックします。
4. エンタープライズスキャンウィザードのステップ2で、[エンタープライズスキャン名(Enterprise Scan Name)] ボックスに、このエンタープライズスキャンの固有名を入力します。
5. この時点で、以下の1つ以上の機能を実行できます。
 - 指定したIPアドレスとポートの範囲内で使用可能なすべてのサーバを検出するように Fortify WebInspectに指示します。

Webサーバを検出するには:

- i. [検出(Discover)]をクリックします。
[Webサーバの検索(Search for Web Servers)]ウィンドウが表示されます。



- ii. [IPV4/IPv6アドレス(または範囲)(IPV4/IPv6 Addresses (or ranges))]ボックスに、1つ以上のIPアドレスまたはIPアドレスの範囲を入力します。
 - 複数のアドレスを区切るには、セミコロンを使用します。
例: 172.16.10.3;172.16.10.44;188.23.102.5
 - 範囲の開始IPアドレスと終了IPアドレスを区切るには、ダッシュまたはハイフンを使用します。
例: 10.2.1.70-10.2.1.90。

メモ: IPv6アドレスは括弧で囲む必要があります。「["Internet Protocolバージョン6" ページ369](#)」を参照してください。
- iii. [ポート(または範囲)(Ports (or ranges))]ボックスに、スキャンするポートを入力します。
 - 複数のポートを区切るには、セミコロンを使用します。
例: 80;8080;443
 - 範囲の開始ポートと終了ポートを区切るには、ダッシュまたはハイフンを使用します。
例: 80-8080。
- iv. (オプション) [設定(Settings)]をクリックして、検出プロセスで使用するソケットとタイムアウトのパラメータの数を変更します。
- v. [開始(Start)]をクリックして検出プロセスを開始します。
結果が [検出されたエンドポイント(Discovered End Points)] エリアに表示されます。

- [IPアドレス(IP Address)]列のエントリをクリックして、そのサイトをブラウザで表示します。
 - [識別(Identification)]列のエントリをクリックして、[セッションプロパティ(Session Properties)]ウィンドウを開きます。このウィンドウでは、生の要求と応答を表示できます。
- vi. サーバをリストから削除するには、[選択(Selection)]列の対応するチェックボックスをオフにします。
 - vii. [OK]をクリックします。
[スキャン対象ホスト(Hosts to Scan)]リストにIPアドレスが表示されます。
- スキャンするホストの個別のURLまたはIPアドレスを入力します。
スキャンするURLまたはIPアドレスのリストを手動で入力するには:
 - i. [追加(Add)]をクリックします。
スキャンウィザードが開きます。
 - ii. 「["基本スキャンの実行\(Webサイトスキャン\)" ページ178](#)」で説明されている情報を入力します。
 - iii. 他の各サーバに対して同じ手順を繰り返します。
 - スキャンするサーバのリストをインポートします(前に作成したリストを使用)。
以前にエンタープライズスキャン機能またはWeb Discoveryツールを使用してサーバを検出し、その検出事項をテキストファイルにエクスポートした場合は、[インポート(Import)]をクリックして、保存されたファイルを選択することにより、それらの結果をロードできます。

[スキャン対象ホスト(Hosts to Scan)]リストの編集

上記の1つ以上の方針を使用してサーバのリストを作成した後、リストを変更できます。

特定のスキャンの設定を変更するには:

1. サーバを選択します。
2. [編集(Edit)]をクリックします。
スキャンウィザードが開きます。
3. 設定を変更します。
4. ([基本スキャンの編集(Edit Basic Scan)]ウィンドウで) [完了(Finish)]をクリックします。

リストからサーバを削除するには:

1. サーバを選択します。
2. [削除>Delete)]をクリックします。

リストのエクスポート

【スキャン対象ホスト(Hosts to Scan)】リストを保存するには:

1. 【エクスポート(Export)】をクリックします。
2. 標準のファイル選択 ウィンドウを使用して、ファイル名と場所を指定します。

スキャンの開始

エンタープライズスキャンを開始するには、【スケジュール(Schedule)】をクリックします。各サーバのスキャン結果が、完了時にデフォルトのScansフォルダに自動的に保存されます。サーバの名前、日付、およびタイムスタンプがファイル名に含まれます。

メモ: Fortify WebInspectライセンスにより、特定のIPアドレスまたはアドレス範囲のスキャンがユーザーに許可されます。ライセンスで許可されていないIPアドレスがサーバにある場合、そのサーバはスキャンに含まれません。

手動スキャンの実行

手動スキャン(ステップモードとも呼ばれる)は、Internet Explorerを使用して、アクセス対象として選択したアプリケーションの任意のセクションに手動で移動できる基本スキャンオプションです。サイト全体のWeb探索は実行されず、サイト内を手動で移動中に検出したリソースに関する情報のみを記録します。この機能は、Webフォームのログオンページからサイトに入る場合、または調査するアプリケーションの個別のサブセットまたは部分を定義する場合に最もよく使用されます。サイト内を移動し終わったら、結果を監査して、記録したサイトのその部分に関連するセキュリティ脆弱性を評価できます。

手動スキャンを実行するには:

1. Fortify WebInspectの【開始ページ(Start Page)】で、【基本スキャンの開始(Start A Basic Scan)】を選択します。
2. スキャン方法として【手動(Manual)】を選択し、基本スキャンウィザードで説明される基本スキャンの設定手順に従います。詳細については、「["基本スキャンの実行\(Webサイトスキャン\)" ページ178](#)」を参照してください。
3. 【スキャン(Scan)】をクリックします。
4. Internet Explorerが開いたら、Internet Explorerを使用してサイト内を移動し、記録するエリアにアクセスします。

ヒント: セッションを記録せずにアプリケーションの特定のエリアにアクセスする場合は、Fortify WebInspectに戻り、ナビゲーションペインの【ステップモード(Step Mode)】ビューに表示される【一時停止(Pause)】ボタン  をクリックします。セッション記録を再開するには、【記録(Record)】ボタン  をクリックします。詳細については、「["ナビゲーションペイン" ページ67](#)」を参照してください。

5. 完了したら、ブラウザを閉じます。

Fortify WebInspectのナビゲーションペインに「ステップモード(Step Mode)」ビューが表示されます。



6. 次のいずれかを実行します。

- アプリケーションのブラウズを再開するには、セッションを選択して「**ブラウズ(Browse)**」をクリックします。
- セッションをスキャンにインポートするには、**完了(Finish)**をクリックします。個々のセッションをインポートから除外するには、対応するチェックボックスをオフにします。

7. 記録されたセッションを監査するには、(ツールバーの)  Auditをクリックします。

権限のエスカレーションスキャンについて

権限のエスカレーション脆弱性は、プログラミングエラーや設計上の欠陥から生じ、攻撃者にアプリケーションとそのデータへの昇格されたアクセス権を付与します。Fortify WebInspectでは、同じスキャンで、低い権限または未認証のWeb探索に続いて、高い権限のWeb探索と

監査を行って、権限のエスカレーション脆弱性を検出できます。Fortify WebInspectには、権限のエスカレーションポリシーと共に、カスタムポリシーを含む他のポリシーで有効にできる権限のエスカレーションチェックが含まれています。ガイド付きスキャンでは、権限のエスカレーションチェックが有効なポリシーが選択されると、Fortify WebInspectがそれを自動的に検出し、必要なログインマクロの入力を求めるプロンプトを表示します。

権限のエスカレーションスキャンの2つのモード

Fortify WebInspectでは2つのモードで権限のエスカレーションスキャンを実行できます。これは、使用するログインマクロの数によって決まります。

- 認証モード-このモードでは、低い権限によるアクセス用と、高い権限によるアクセス用の、2つのログインマクロを使用します。このモードでは、低い権限によるWeb探索の後に、高い権限によるWeb探索と監査が続きます。このタイプのスキャンは、ガイド付きスキャンを使用して実行できます。詳細については、「["ガイド付きスキャンの実行" ページ117](#)」を参照してください。

メモ: ガイド付きスキャンで、Webサイトの拡張カバレッジ(Enhance Coverage of Your Web Site)機能を権限のエスカレーションポリシーと一緒に合わせて使用している場合、高い権限のログインマクロで認証されている間は、探索された場所が収集されます。

- 未認証モード-このモードでは、高い権限のログインマクロのみを使用します。このモードでは、低い権限によるWeb探索は、実際には未認証のWeb探索です。このスキャンで検出される権限のエスカレーションは、未認証から高い権限に移行するものです。このタイプのスキャンは、(高い権限のログインマクロのみを提供して)ガイド付きスキャンウィザードを使用して実行するか、基本スキャンウィザードを使用して実行することができます。詳細については、「["基本スキャンの実行\(Webサイトスキャン\)" ページ178](#)」を参照してください。

スキャン時の動作について

権限のエスカレーションチェックを有効にしたスキャンを実行する場合、Fortify WebInspectはまずサイトに対して低い権限によるWeb探索を実行します。このWeb探索では、Webサイトの階層構造は[サイト(Site)]ビューに表示されません。サマリペインにも脆弱性は表示されません。ただし、サマリペインの[スキャンログ(Scan Log)]タブをクリックすると、スキャンが実際に動作していることを確認できます。ログには、「スキャンの開始(Scan Start)」時刻と「LowPrivilegeCrawlStart」時刻を示すメッセージが記録されます。サイトに対する低い権限によるWeb探索が完了すると、高い権限によるWeb探索と監査のスキャンフェーズが実行されます。このフェーズでは、[サイト(Site)]ビューに情報が入力され、検出された脆弱性がサマリペインに表示されます。詳細については、「["サマリペイン" ページ109](#)」を参照してください。

制限のあるページを識別するために使用される正規表現パターン

「禁止(Forbidden)」、「制限付き(Restricted)」、または「アクセス拒否(Access Denied)」などのテキストを使用してブロックされる、制限のあるページがサイトに含まれる場合、権限のエスカレーションチェックには、これらのページが現在のユーザに対して禁止されていることを判断するための正規表現パターンが含まれます。したがって、これらのページは権限のエスカレー

ションに対して脆弱なものとして特定されません。ただし、組み込みの正規表現パターンに一致しない、権限を制限する他のテキストがサイトで使用されている場合は、独自のテキストパターンを含むように正規表現を変更する必要があります。変更しない場合、これらのページに対する権限のエスカレーションチェックで誤検出が発生するおそれがあります。

権限の制限パターンに合わせた正規表現の変更

1. [編集(Edit)] > [デフォルトのスキャン設定(Default Scan Settings)] の順にクリックします。
[デフォルト設定(Default Settings)] ウィンドウが表示されます。
2. [監査設定(Audit Settings)] グループで、[攻撃の除外(Attack Exclusions)] を選択します。
3. [Audit Inputs Editor...] をクリックします。
Audit Inputs Editor が表示されます。
4. [入力のチェック(Check Inputs)] を選択します。
5. [11388権限のエスカレーション(11388 Privilege Escalation)] のチェックを選択します。
[権限の制限パターン(Privilege Restriction Patterns)] が右側のペインに表示されます。デフォルトのパターンは次のとおりです。
'forbidden|restricted|access\sdenied|(:operation\snot\s(:allowed|permitted|authorized))|(:you\s(:do\snot|don't)\ shave\s(:access|permission|authorization))|(:you\s(:are\snot|aren't)\s(:allowed|permitted|authorized))'
6. 正規表現構文を使用して、サイトで使用されている、禁止されているアクションを表す新しい単語を追加します。
7. [OK] をクリックして、変更した [入力のチェック(Check Inputs)] を保存します。
8. [OK] をクリックして、[デフォルト設定(Default Settings)] ウィンドウを閉じます。

Web探索プログラムの制限設定によって権限のエスカレーションスキャンに及ぶ影響

Fortify WebInspectは、スキャン中に各パラメータ値を監査します。したがって、権限のエスカレーションスキャンは、Web探索プログラムを制限する次のような設定の影響を受けます。

- 1つのURLの最大ヒット数を以下に制限する(Limit maximum single URL hits to)
- ヒット数にパラメータを含める(Include parameters in hit count)
- Webフォームの最大送信数を以下に制限する(Limit maximum Web form submission to)
- 冗長ページ検出の実行(Perform redundant page detection)

たとえば、[1つのURLの最大ヒット数を以下に制限する(Limit maximum single URL hits to)] に1を設定し、サイトに次のようなリンクが含まれているとします。

```
index.php?id=2
index.php?id=1
index.php?id=3
```

ここで、Fortify WebInspectは高い権限によるスキャンの際に「index.php?id=1」を検出し、低い権限によるスキャンの際に「index.php?id=3」を検出します。このシナリオでは、Fortify WebInspectは「index.php?id=1」に対して権限のエスカレーション脆弱性のマークを付けます。この脆弱性は誤検出です。

詳細については、「"スキャン設定: 全般" ページ374」を参照してください。

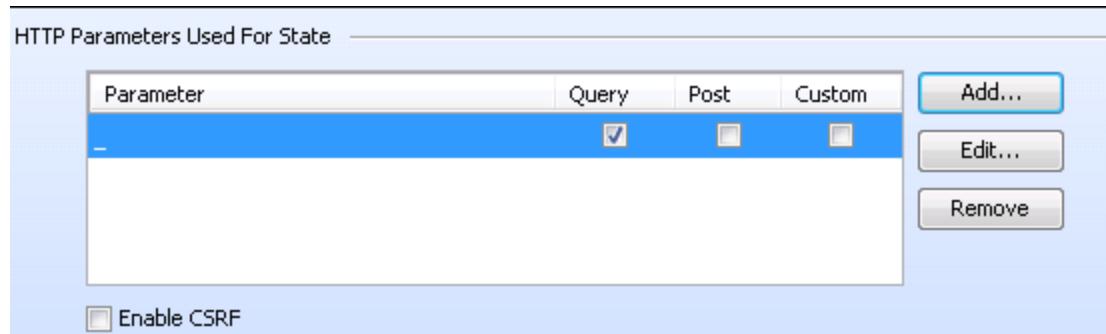
乱数を含むパラメータによって権限のエスカレーションスキャンに及ぶ影響

サイトに乱数を含むパラメータが含まれている場合は、そのパラメータを「状態に使用されるHTTPパラメータ(HTTP Parameters Used For State)」のリストに追加して、このようなセッションを監査から除外し、誤検出の数を減らすことができます。

たとえば、次のパラメータがあるとします。

```
index.php?_=1440601463586  
index.php?_=1440601465662  
index.php?_=1440601466365
```

次のように、このパラメータを「状態に使用されるHTTPパラメータ(HTTP Parameters Used For State)」のリストに追加します。



詳細については、「"スキャン設定: HTTP解析" ページ390」を参照してください。

次も参照

["基本スキャンの実行\(Webサイトスキャン\)" ページ178](#)

["事前定義テンプレートの使用" ページ118](#)

["モバイルスキャンテンプレートの使用" ページ135](#)

["ネイティブスキャンテンプレートの使用" ページ154](#)

シングルページアプリケーションスキャンについて

このトピックでは、アプリケーションのDOM (Document Object Model)のWeb探索および監査のためのSPA (シングルページアプリケーション)のサポートについて説明します。

重要! このバージョンのSPAサポートは、テクノロジプレビューとして提供されています。

テクノロジプレビュー

テクノロジプレビュー機能は現在サポートされていないため、完全に機能しない可能性があります。また、運用環境での展開には適しません。ただし、これらの機能は、将来的には完全なサポートを提供できることを目指すために広く拡大することを主な目的として、便宜的に提供されています。

シングルページアプリケーションの課題

開発者は、JavaScriptフレームワーク(Angular、Ext JS、Ember.jsなど)を使用してSPAを構築します。これらのフレームワークを使用することで開発者のアプリケーション構築は容易になりますが、セキュリティテスト担当者がセキュリティ脆弱性を検出するためにアプリケーションをスキャンすることが難しくなります。

従来のサイトで使用されているシンプルなバックエンドサーバレンダリングでは、サーバサイドで完全なHTML Webページが構築されます。SPAおよびその他の「Web 2.0」サイトで使用されているのは、フロントエンドDOMレンダリング、またはフロントエンドとバックエンドのDOMレンダリングの組み合わせです。SPAでは、ユーザがメニュー項目を選択すると、ページ全体を消去し、新しいコンテンツで再作成することができます。ただし、メニュー項目を選択するイベントで、サーバに対する新しいページの要求が生成されることはありません。サーバからページを再ロードすることなく、コンテンツの更新が行われます。

従来の脆弱性テストでは、新しいコンテンツをトリガしたイベントにより、SPAで以前に監査のために収集された他のイベントが破壊される可能性があります。WebInspectではSPAのサポートによって、SPAでの脆弱性テストの課題に対する解決策を提供します。

SPAサポートの有効化

SPAサポートを有効にすると、DOMスクリプトエンジンは、Web探索中に、JavaScriptインクルード、フレームとiframeのインクルード、CSSファイルインクルード、およびAJAX呼び出しを検索してから、それらのイベントによって生成されたすべてのトランザクションを監査します。

SPAサポートは、スキャン設定またはガイド付きスキャンで有効にできます。

注意! SPAサポートは、シングルページアプリケーションに対してのみ有効にするべきです。SPAサポートを有効にしてSPA以外のWebサイトをスキャンすると、スキャンが遅くなります。

次も参照

["スキャン設定: JavaScript" ページ380](#)

["事前定義テンプレートの使用" ページ118](#)

["モバイルスキャンテンプレートの使用" ページ135](#)

["ネイティブスキャンテンプレートの使用" ページ154](#)

スキャンステータス

特に指定されていない限り、スキャンステータスはデータベースから直接読み込まれます。次の表で、スキャンステータスについて説明します。

ヒント: ほとんどのスキャンステータスに関しては、ステータスの理由はスキャンログで確認できます。

| ステータス | 説明 |
|---------------------|---|
| 完了 | スキャンが完了しました。 |
| 未完了 (Incomplete) | ユーザがスキャンを一時停止して閉じました。スキャンの実行は完了していません。 |
| 中斷 (Interrupted) | テスト中のアプリケーションやデータベースとのコネクティビティの問題など、環境上の問題があります。 |
| ロック状態 | Fortify WebInspectの別のインスタンスによってスキャンが開始済みです。スキャンは実行中であり、そのハートビート機能は期限が切れていません。 メモ: リモートSQL Server(フルバージョン)にのみ適用されます。 |
| 開く | ローカルマシンのユーザが、Fortify WebInspectでスキャンを開いています。ユーザは現在のユーザの場合もあれば(その場合は「スキャン(Scan)」タブにスキャンが表示される)、同じマシン上の別のユーザの場合もあります(ターミナルサービスを使用している場合など)。スキャンデータベースに保存されている状態は無視されます。 |
| 一時停止 (Paused) | ユーザがスキャンを一時停止しました。 |
| 実行中 (Running) | スキャンは現在ローカルマシンで実行されています。 メモ: このステータスには、スケジュールされたスキャンと、コマンドラインインターフェース(CLI)を介して開始されたスキャンが含まれます。 |

スキャンマネージャの情報の更新

スキャンマネージャは、現在表示されているスキャンに関するリアルタイムのステータス情報を提供することを目的としていませんが、次の3つの重要な例外があります。

- 新しいスキャンが作成されたか、開かれた場合。この場合、スキャンマネージャは新しいスキャンを一覧に示し、「オープン(Open)」ステータスを表示します。
- 現在のユーザによって以前に開かれたスキャンが閉じられた場合。たとえば、ユーザがスキャンを開くか作成した後、それを閉じます。スキャンマネージャ内でそのスキャンのステータスが更新され、閉じられた時点でのスキャンのステータスが反映されます(「完了(Completed)」や「未完了(Incomplete)」など)。その単一のスキャンに対してのみ、すべての統計情報が更新されます。
- スキャンが開かれている間、[期間(Duration)]フィールドが常に正確で使用可能であるとは限りません。したがって、スキャンの状態が「オープン(Open)」、「実行中(Running)」、または「ロック状態(Locked)」の場合、[期間(Column)]列には値がないことが示されます(数字ではなく、「-」が表示されます)。

それ以外のステータス変更や更新されたカウント情報を表示するには、更新ボタンをクリックする必要があります。

次も参照

["スケジュールされたスキャンのステータス" ページ227](#)

保存したスキャンを開く

次のいずれかの手順を使用して、前回のスキャンの結果を含む保存済みファイルを開きます。

メニューまたはツールバーの使用:

- [ファイル(File)] > [開く(Open)] > [スキャン(Scan)]の順にクリックします。
- [開く(Open)]ボタンのドロップダウン矢印をクリックし、[スキャン(Scan)]を選択します。

[開始ページ(Start Page)]タブから:

- [基本スキャンの開始(Start a Basic Scan)]をクリックします。
- ホームページで、[最近開いたスキャン(Recently Opened Scans)]リスト内のエントリをクリックします。
- [スキャンの管理(Manage Scans)]ペインでスキャンを選択し、[開く(Open)]をクリックします(またはスキャン名をダブルクリックします)。

スキャンデータがロードされ、別のタブに表示されます。

スキャンの比較

ターゲットが同じ2つの異なるスキャンから判明した脆弱性を比較し、この情報を次の目的で使用できます。

- 修復を検証する: 最初のスキャンで検出された脆弱性と、脆弱性の修復後に同じサイトに対して実行した別のスキャンで検出された脆弱性と比較します。
- スキャンヘルスをチェックする: スキャン設定を変更し、それらの変更によって攻撃露呈部分が広がっていないか検証します。
- 新しい脆弱性を検索する: 更新版のサイトが新しい脆弱性をもたらしていないか判断します。
- 問題を調査する: 誤検出や見落とされた脆弱性などのアノマリを追跡します。
- 権限付与アクセスを比較する: 2つの異なるユーザーアカウントを使用してスキャンを実行し、両方のアカウントで固有のまたは共通の脆弱性を検出します。

メモ: 両方のスキャンからのデータは、同じデータベースタイプ(SQL Server Express EditionまたはSQL Server Standard/Enterprise Edition)に保存する必要があります。

スキャンを比較するためのスキャンの選択

2つのスキャンを比較するには、次のいずれかを実行します。

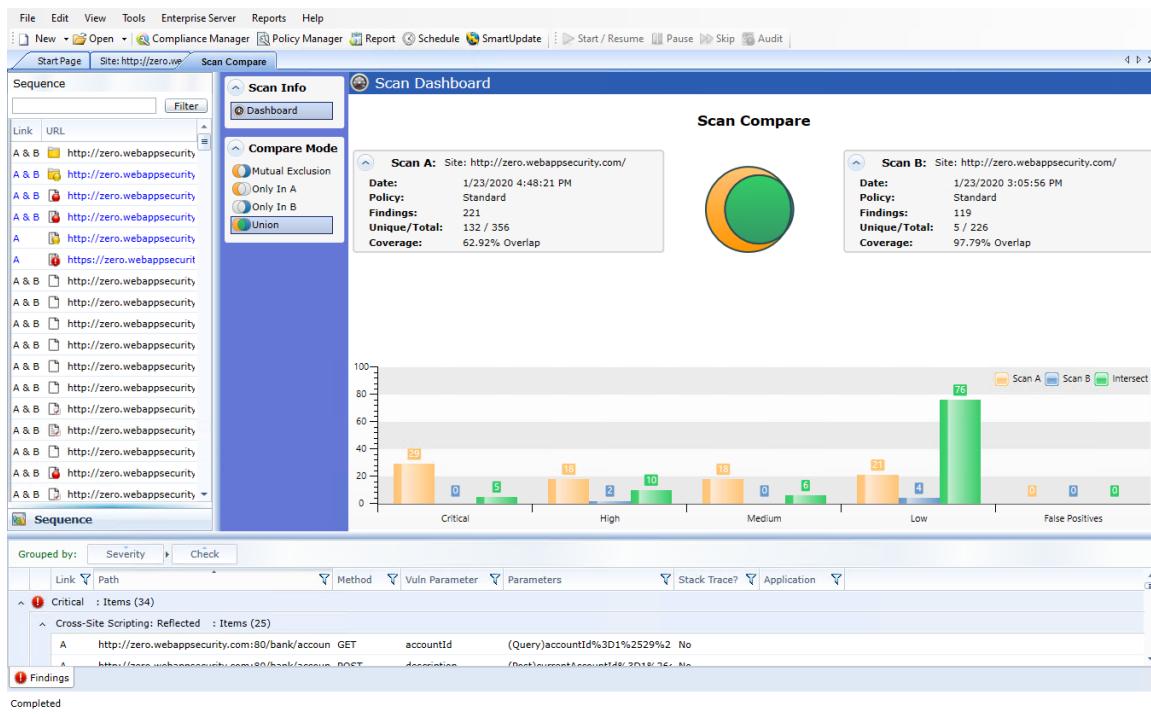
- 【スキャンの管理(Manage Scans)】ページで、2つのスキャンを選択し、【比較(Compare)】をクリックします。
- 開いているスキャン(比較ではスキャンAになる)を含むタブから:
 - 【比較(Compare)】をクリックします。
 - 【スキャンの比較(Scan Comparison)】ウィンドウのリストからスキャンを選択します。このスキャンが比較ではスキャンBになります。
 - 【比較(Compare)】をクリックします。

メモ: 開いているスキャンが「site retest」(【再スキャン(Rescan)】> 【脆弱性の再テスト(Retest Vulnerabilities)】)の場合は、Fortify WebInspectが比較対象の親スキャンを自動的に選択します。たとえば、「zero」という名前のスキャンを作成し、そのスキャンの脆弱性を検証した場合は、結果のスキャンに(デフォルトで)「site retest - zero」という名前が付けられます。再テストスキャンが開いている状態で、【比較(Compare)】を選択すると、Fortify WebInspectが「site retest - zero」を親スキャン「zero」と比較します。

選択したスキャンの開始URLが異なる場合や異なるスキャンポリシーが使用されている場合、または、スキャンのタイプが異なる場合(基本スキャンとWebサービススキャンなど)は、警告メッセージが表示されます。続行を選択することも、機能を終了することもできます。

どちらかのスキャンが実行中は、比較を実行できません。

スキャン比較のイメージ



スキャンダッシュボードの確認

スキャン比較結果はスキャンダッシュボードに表示されます。

スキャンの説明



【スキャンA (Scan A)】ボックスと【スキャンB (Scan B)】ボックスに、スキャンに関する次の情報が表示されます。

- **スキャンA (Scan A)またはスキャンB (Scan B):** スキャンの名前。
- **日付 (Date):** オリジナルのスキャンが実行された日付と時刻。
- **ポリシー (Policy):** スキャンに使用されたポリシー。詳細については、「["Fortify WebInspectのポリシー" ページ473](#)」を参照してください。
- **検出事項 (Findings):** 検出事項 (Findings) タブで特定された問題と検出された誤検出の総数。
- **固有/合計 (Unique/Total):** このスキャン用に作成された固有のセッションの数 (つまり、もう一方のスキャンではなく、このスキャンで出現したセッションの数) を、このスキャンのセッション

の総数と比較します。

- **カバレッジ(Coverage):** 両方のスキャンに共通するセッションの割合。

ベン図

ベン図は、スキャンA(黄色の円)のセッションカバレッジとスキャンB(青色の円)のセッションカバレッジを示しています。2つのセットの交差は緑色のオーバーラップで表されます(以前のリリースでは、ベン図は脆弱性のオーバーラップを表していました)。

ベン図は、セット間の実際の関係を反映して拡大/縮小されます。

セッションカバレッジのオーバーラップの例を以下に示します。

| | | | | |
|------|--------|--------|-------------|-------|
| | | | | |
| 交差なし | 50%の交差 | AがBを包含 | AのほとんどがBと交差 | 完全な交差 |

脆弱性棒グラフ

脆弱性の重大度のそれぞれと誤検出を別々のグループにすると、スキャンダッシュボードの下部に、スキャンA、スキャンB、およびそれらの交差(交差(Intersect))で検出された脆弱性の数を示す棒グラフのセットが表示されます。ベン図と同じ色分けが使用されます。これらの棒グラフが、選択された [比較モード(Compare Mode)]に基づいて変化することはありません。

スキーム、ホスト、およびポートの違いがスキャン比較に及ぼす影響

別々のサーバ上でホストされている2つの重複サイトからのスキャンを比較する場合、Fortify WebInspectはスキーム、ホスト、およびポートを無視しません。

たとえば、次のサイトのペアは、スキーム、ホスト、またはポートの違いにより、スキャン比較で相関性がありません。

- **スキーム**
 - サイトA - <http://zero.webappsecurity.com/>
 - サイトB - <https://zero.webappsecurity.com/>
- **ホスト**
 - サイトA - <http://dev.foo.com/index.html?par1=123&par2=123>
 - サイトB - <http://qa.foo.com/index.html?par1=123&par2=123>
- **ポート**
 - サイトA - <http://zero.webappsecurity.com:80/>
 - サイトB - <http://zero.webappsecurity.com:8080/>

比較モード

スキャンダッシュボードの左側にある [比較モード(Compare Mode)] セクションで次のいずれかのオプションを選択して、左側のペインの [シーケンス(Sequence)] エリアに別のデータを表示できます(スキャンダッシュボード内のデータには影響しません)。

- **相互除外(Mutual Exclusion)**: スキャンAまたはスキャンBに出現するものの、両方のスキャンには出現しないセッションを一覧にします。
- **Aのみ(Only In A)**: スキャンAにのみ出現するセッションを一覧にします。
- **Bのみ(Only in B)**: スキャンBにのみ出現するセッションを一覧にします。
- **結合(Union) (デフォルト)**: スキャンAとスキャンBのいずれかまたは両方に出現するセッションを一覧にします。

セッションfiltrリング

[シーケンス(Sequence)] ペインには、選択された比較モードと一致する各セッションが一覧表示されます。URLの左側にあるアイコンは、そのセッションの脆弱性(もしあれば)の重大度を示します。重大度アイコンは次のとおりです。

| 重大 | 高 | 中 | 低 |
|---|---|---|---|
|  |  |  |  |

[シーケンス(Sequence)] ペインの上部で、filtrタを指定して [filtrタ(Filter)] をクリックすると、表示されるセッションのセットを次の方法で制限できます。

- URLは、「次の文字で始まる」の一一致として、先頭の文字のみを入力できます。エントリは、プロトコル(http://またはhttps://)で始まる必要があります。
- URLを引用符で囲んで完全一致を検索できます。エントリは、引用符とプロトコル("http://または"https://)で始まる必要があります。
- 入力する文字列の先頭または末尾にワイルドカード文字としてアスタリスク(*)を使用できます。
- 入力する文字列の先頭と末尾の両方にアスタリスク(*)を使用できます。一致するには、アスタリスクの間の文字列が含まれている必要があります。
- 疑問符(?)の後に完全なクエリパラメータ文字列を入力して、そのクエリパラメータと一致する文字列を検索できます。

[セッション情報(Session Info)] パネルの使用

[シーケンス(Sequence)] ペインでセッションを選択すると、[比較モード(Compare Mode)] オプションの下で [セッション情報(Session Info)] パネルが開きます。セッションを選択した状態で、[セッション情報(Session Info)] パネルでオプションを選択すると、[セッション情報(Session Info)] パネルの右側に、そのセッションに関する詳細が表示されます。セッションに

両方のスキャンのデータが含まれている場合は、[Webブラウザ(Web Browser)]、[HTTP要求(HTTP Request)]、[ステップ(Steps)]などの一部の機能に関するデータが分割ビューに表示されます(左側がスキャンAで右側がスキャンB)。

メモ: [ステップ(Steps)]オプションは、[シーケンス(Sequence)]ペインで選択されたセッションまたはサマリペインで選択されたURLに到達するためにFortify WebInspectがたどったパスを表示します。親セッション(リストの一番上)から始まり、それ以降にアクセスしたURLが順番に表示され、スキャン方法に関する詳細が提供されます。スキャン比較では、セッションのステップのいずれかがスキャン間で異なる場合に、[両方(In Both)]列が[ステップ(Steps)]テーブルに(最初の列として)追加されます。特定のステップの列内の[はい(Yes)]の値は、スキャンAとスキャンBの両方のそのセッションでステップが同じであることを示します。特定のステップの列内の[いいえ(No)]の値は、スキャンAとスキャンBのそれぞれのそのセッションでステップが異なることを示します。

サマリペインを使用した脆弱性の詳細の確認

スキャンを比較する場合は、ウィンドウの下部にある水平のサマリペインに、脆弱なリソースの一元管理されたテーブルが表示され、脆弱性情報に素早くアクセスできます。テーブルの上の水平区切り線をドラッグすると、サマリペインの表示と非表示にする区画を増やすことができます。

[検出事項(Findings)]タブに表示される一連のエントリ(行)は、テーブルの[リンク(Link)]列に反映されているように、[比較モード(Compare Mode)]で選択されたオプションによって異なります。

脆弱性のグループ化とソート

脆弱性のグループ化とソートについては、「["サマリペイン" ページ109](#)」と「["サマリペインのフィルタとグループの使用" ページ262](#)」を参照してください。

脆弱性のフィルタリング

任意の列見出しの右側にあるフィルタアイコン()をクリックしてフィルタを開き、フィルタリング後に脆弱性(行)をテーブルに残すために満たすべき、その列に関するさまざまな条件を選択することができます。使用可能な条件には、列内の現在の値の一式が含まれます。また、その列の内容に関する論理式を指定することもできます。

たとえば、[Vulnパラメータ(Vuln Parameter)]列のフィルタで、次のように想定します。

1. チェックボックスの一一番上のセットをそのままにします。
2. [次の値の行を表示する>Show rows with value that]テキストの下で、ドロップダウンメニューから[次の値を含む]を選択します。
3. ドロップダウンメニューの下にあるテキストボックスに「Id」と入力します。
4. [フィルタ]をクリックします。

次に、[Vulnパラメータ(Vuln Parameter)]列に「Id」というテキストを含む行だけがテーブルに表示されます。これには、[Vulnパラメータ(Vuln Parameter)]の値が「accountId」や「payeeId」である行、または、「Id」を含むその他のエントリが含まれます。

複数の列にフィルタを指定できます(1回につき1つの列に指定)。それらのフィルタがすべて適用されます。

列のフィルタが指定されている場合、そのアイコンは未使用のフィルタのアイコンより濃い青色になります。

フィルタを素早くクリアするには、指定するフィルタが開いている間に「**フィルタのクリア(Clear Filter)**」をクリックします。

脆弱性の操作

サマリペインで項目を右クリックすると、次のコマンドを含むショートカットメニューが表示されます。

- **URLのコピー(Copy URL)**: URLをWindowsのクリップボードにコピーします。
- **選択した項目をコピー(Copy Selected Item(s))**: 選択した項目のテキストをWindowsのクリップボードにコピーします。
- **すべての項目をコピー(Copy All Items)**: すべての項目のテキストをWindowsのクリップボードにコピーします。
- **エクスポート(Export)**: すべての項目または選択した項目を含むカンマ区切り値(csv)ファイルを作成し、Microsoft Excelで表示します。
- **ブラウザで表示(View in Browser)**: ブラウザでHTTP応答をレンダリングします。

メモ: PostパラメータおよびQueryパラメータの場合は、「**パラメータ(Parameters)**」列のエントリをクリックすると、パラメータのより分かりやすい概要が表示されます。

次も参照

["サマリペイン" ページ109](#)

["サマリペインのフィルタとグループの使用" ページ262](#)

スキャンの管理

スキャンを管理するには:

1. 開始ページ(Start Page)で、「**スキャンの管理(Manage Scans)**」をクリックします。



スキャンの一覧が、開始ページ(Start Page)の右側のペインに表示されます。

デフォルトでは、自分のマシン上のSQL Server Express Editionと、SQL Server Standard Edition(設定されている場合)に保存されているスキャンがすべてFortify WebInspectによって一覧表示されます。スキャンの現在の状態は「**ステータス(Status)**」列に示されます。詳細については、「["スキャンステータス" ページ212](#)」を参照してください。

2. (オプション)列見出しに基づいてスキャンをカテゴリにグループ化するには、見出しをドラッグしてグループ化エリアにドロップします。

3. ツールバーのボタンを使用して、次に示す機能を実行します。

- スキャンを開くには、1つ以上のスキャンを選択して [開く(Open)]をクリックします(または、単にリスト内のエントリをダブルクリックします)。Fortify WebInspectによってスキャンデータがロードされ、それぞれのスキャンは個別のタブに表示されます。
- 選択したスキャンで最後に使用された設定が取り込まれた状態でスキャンウィザードを起動するには、[再スキャン(Rescan)]> [もう一度スキャンする(Scan Again)]をクリックします。
- スキャンを再利用するには、[再スキャン(Rescan)]をクリックし、ドロップダウンメニューから目的の再利用オプションを選択します。詳細については、「["スキャンの再利用" ページ250](#)」を参照してください。
- 前回のスキャンで明らかになった脆弱性を含むセッションのみを再スキャンするには、スキャンを選択して、[再スキャン(Rescan)]> [脆弱性の再テスト(Retest Vulnerabilities)]をクリックします。
- スキャンをマージするには、(<Ctrl>を押しながらクリックして) 2つのスキャンを選択し、右クリックして [マージ(Merge)]を選択します。詳細については、「["増分スキャン" ページ251](#)」を参照してください。
- 選択したスキャンの名前を変更するには、[名前変更(Rename)]をクリックします。
- 選択したスキャンを削除するには、[削除>Delete)]をクリックします。
- スキャンをインポートするには、[インポート(Import)]をクリックします。
- スキャンまたはスキャンの詳細をエクスポートしたり、スキャンをSoftware Security Centerにエクスポートしたり、保護ルールをWebアプリケーションファイアウォール(WAF)にエクスポートしたりするには、[エクスポート(Export)]のドロップダウンボタンをクリックします。
- スキャンを比較するには、(<Ctrl>を押しながらクリックして) 2つのスキャンを選択し、[比較(Compare)]をクリックします。
- デフォルトでは、ローカルSQL Server Express Editionと設定済みのSQL Server Standard Editionに保存されているスキャンがすべてFortify WebInspectによって一覧表示されます。一方または両方のデータベースを選択する、またはSQL Server接続を指定するには、[接続(Connections)]をクリックします。
- 必要に応じて、[更新(Refresh)]をクリックして表示を更新します。
- 表示する列を選択するには、[列(Column)]をクリックします。[上へ移動(Move Up)]ボタンと[下へ移動(Move Down)]ボタンを使用して列を表示する順序を並べ替えたり、[スキャンの管理(Manage Scans)]リストで、単に列見出しをドラッグアンドドロップしたりすることができます。

メモ: また、エントリを右クリックしてショートカットメニューからコマンドを選択することで、これらの機能のほとんどを実行できます。レポートの生成も選択できます。詳細については、「["レポートの生成" ページ280](#)」を参照してください。

次も参照

["スケジュールされたスキャンの管理" 次のページ](#)

["開始ページ\(Start Page\)" ページ55](#)

スキャンのスケジュール

基本スキャン、APIスキャン、またはエンタープライズスキャンを、選択した日時に実行するためのスケジュールを設定できます。

選択したオプションと設定は特別なファイルに保存されます。これは、Fortify WebInspectの起動(必要な場合)とスキャンの開始を行うWindowsサービスによってアクセスされます。スキャンの開始が指定されている時刻にFortify WebInspectが実行されている必要はありません。

メモ: スケジュールされたスキャンの完了後、これにアクセスするには、[開始ページ\(Start Page\)](#)タブを選択して[\[スキャンの管理\(Manage Scans\)\]](#)をクリックします。

スキャンをスケジュール設定するには:

1. 次のいずれかを実行します。
 - Fortify WebInspectツールバーの[\[スケジュール\(Schedule\)\]](#)アイコンをクリックします。
 - Fortify WebInspectの[\[開始ページ\(Start Page\)\]](#)で、[\[スケジュールされたスキャンの管理\(Manage Scheduled Scans\)\]](#)をクリックします。
2. [\[スケジュールされたスキャンの管理\(Manage Scheduled Scans\)\]](#)ウインドウが表示されたら、[\[追加\(Add\)\]](#)をクリックします。
3. [\[スキャンのタイプ\(Type of Scan\)\]](#)グループで、次のいずれかを選択します。
 - [\[Webサイトスキャン\(Web Site Scan\)\]](#)
 - [\[APIスキャン\(API Scan\)\]](#)
 - [\[エンタープライズスキャン\(Enterprise Scan\)\]](#)
4. スキャンを1回だけ実行するには、[\[1度だけ実行\(Run Once\)\]](#)を選択し、[\[開始日\(Start Date\)\]](#)と[\[時刻\(Time\)\]](#)を編集します。ドロップダウン矢印をクリックすると、カレンダーを使用して日付を選択できます。
5. サイトを定期的にスキャンするには:
 - a. [\[繰り返し\(Recurring\)\]](#)(または[\[繰り返しスケジュール\(Recurrence Schedule\)\]](#))を選択し、開始時刻を指定して頻度([毎日\(Daily\)](#)、[毎週\(Weekly\)](#)、[毎月\(Monthly\)](#))を選択します。
 - b. [\[毎週\(Weekly\)\]](#)または[\[毎月\(Monthly\)\]](#)を選択した場合は、要求される追加の情報を入力します。
6. [\[次へ\(Next\)\]](#)をクリックします。

次も参照

["基本スキャンの実行\(Webサイトスキャン\)" ページ178](#)

["APIまたはWebサービススキャンの実行" ページ169](#)

["エンタープライズスキャンの実行" ページ203](#)

["スケジュールされたスキャンの時間間隔の設定" 下](#)

スケジュールされたスキャンの時間間隔の設定

スキャンを実行する時間を設定したり、定期的なスキャンを設定したりするには:

1. [スキャンのタイプ(Type of Scan)]グループで、次のいずれかを選択します。
 - 基本スキャン(Basic Scan)
 - APIスキャン(API Scan)
 - エンタープライズスキャン(Enterprise Scan)
2. スキャンを今すぐ実行するには、[即時(Immediately)]を選択します。
3. 後日または後刻に一度だけスキャンを実行するには:
 - a. [一度だけ実行(Run Once)]を選択します。
 - b. スキャンを開始する日時を変更します。

ヒント: ドロップダウン矢印をクリックして、日付を選択するためのカレンダを表示します。
4. サイトを定期的にスキャンするには:
 - a. [定期的(Recurring)]を選択します。
 - b. スキャンを開始する時刻を指定します。
 - c. 頻度を[毎日(Daily)]、[毎週(Weekly)]、または[毎月(Monthly)]から選択します。
5. [次へ(Next)]をクリックします。

次も参照

["基本スキャンの実行\(Webサイトスキャン\)" ページ178](#)

["APIまたはWebサービススキャンの実行" ページ169](#)

["エンタープライズスキャンの実行" ページ203](#)

スケジュールされたスキャンの管理

指定した日時にスキャンを実行するように、Fortify WebInspectに指示できます。選択したオプションと設定は特別なファイルに保存されます。これは、Fortify WebInspectの起動(必要な場合)とスキャンの開始を行うWindowsサービスによってアクセスされます。スキャンの開始が指定されている時刻にFortify WebInspectが実行されている必要はありません。

メモ: スケジュールされたスキャンが完了しても、Fortify WebInspectの[開始ページ(Start Page)]に表示される[最近のスキャン(Recent Scans)]一覧には表示されません。スケジュールされたスキャンの完了後、これにアクセスするには、[開始ページ(Start Page)]を

選択して [スキャンの管理(Manage Scans)]をクリックします。

開始ページ(Start Page)]で、[スケジュールの管理(Manage Schedule)]をクリックします。



以前にスケジュールされたスキャンの一覧が、開始ページ(Start Page)]の右側のペインに表示されます。

スキャンの現在の状態は [ステータス(Status)]列に示されます。詳細については、「["スケジュールされたスキャンのステータス" ページ227](#)」を参照してください。

以下のタスクを実行できます。

スキャンの削除

- 一覧からスキャンを削除するには、スキャンを選択して [削除(Delete)]をクリックします。

スキャン設定の編集

- スケジュールされたスキャンの設定を編集するには、スキャンを選択して [編集(Edit)]をクリックします。

スキャンをすぐに実行する

- スケジュールされた時間を持たずに入力スキャンをすぐに実行するには、スキャンを選択して [開始(Start)]をクリックします(または、スキャンを右クリックしてショートカットメニューから [スキャンの開始(Start Scan)]を選択します)。すべてのスケジュールされたスキャンと同様に、スキャンはバックグラウンドで実行され、タブには表示されません。

スケジュールされたスキャンを停止する

- スケジュールされたスキャンを停止するには、実行中のスキャンを選択して [停止(Stop)]をクリックします(または、実行中のスキャンを右クリックしてショートカットメニューから [スキャンの終了(Stop Scan)]を選択します)。

スキャンのスケジュール

スキャンをスケジュール設定するには:

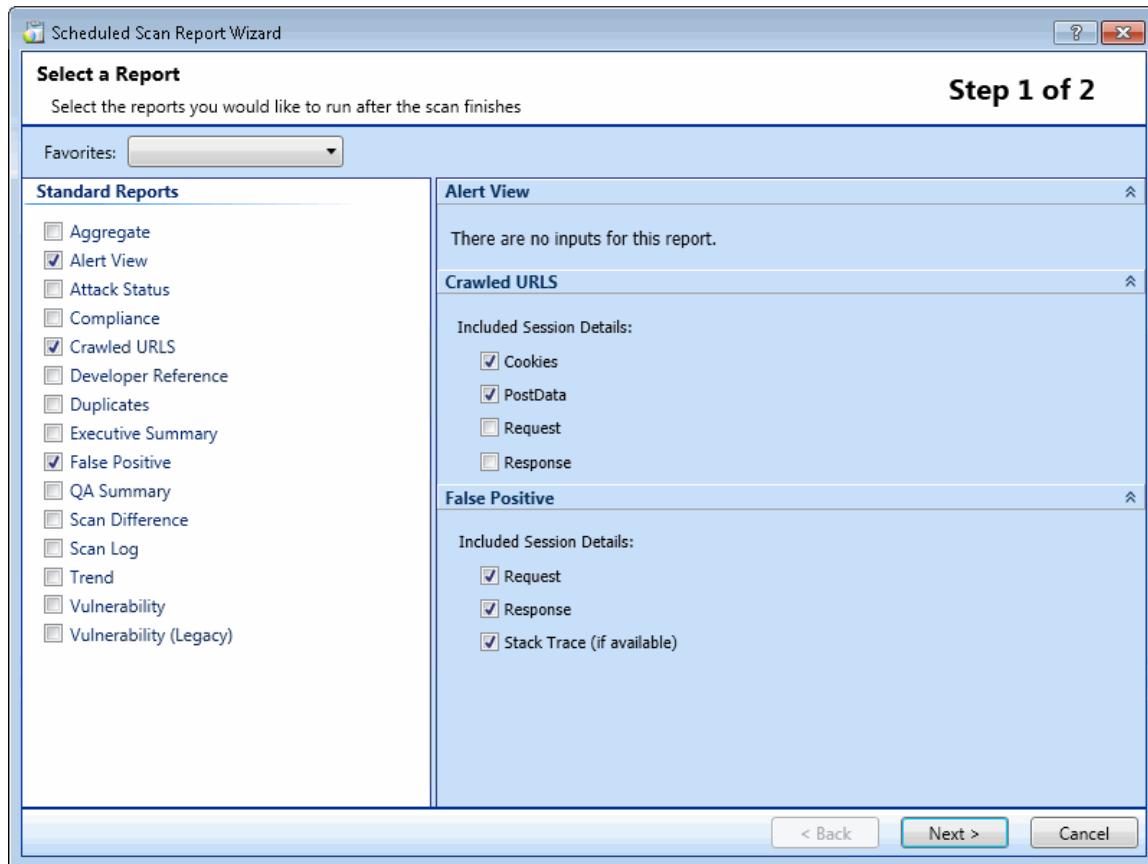
- [追加(Add)]をクリックします。
- [スキャンのタイプ(Type of Scan)]グループで、次のいずれかを選択します。
 - 基本スキャン(Basic Scan)
 - Webサービススキャン(Web Service Scan)
 - エンタープライズスキャン(Enterprise Scan)
- スキャンを実行するタイミングを指定します。次の選択肢があります。
 - 即時(Immediately)
 - 1回実行(Run Once): スキャンを開始する日時を変更します。ドロップダウン矢印をクリックすると、日付を選択するカレンダを表示できます。

- 定期実行スケジュール(Recurrence Schedule): スライダを使用して、頻度(毎日(Daily)、毎週(Weekly)、または毎月(Monthly))を選択します。次に、スキャンを開始する時刻を指定し、(毎週(Weekly)]または[毎月(Monthly)]の場合は)その他のスケジュール情報を指定します。
- [次へ(Next)]をクリックします。
 - 選択したスキャンのタイプの設定を入力します。
 - WebサイトおよびWebサービススキャンの場合に限り、スキャンの最後にレポートを実行するように選択できます。
 - [レポートの生成(Generate Reports)]を選択し、[レポートの選択(Select Reports)]ハイパーアリンクをクリックします。
 - (下の)「レポートの選択」に進んでください。
 - レポートを生成せずにスキャンをスケジュール設定するには、[スケジュール(Schedule)]をクリックします。

レポートの選択

スケジュールされたスキャンにレポートを含めるように選択した場合は、[スケジュールされたスキャンのレポートウィザード(Scheduled Scan Report Wizard)]が表示されます。

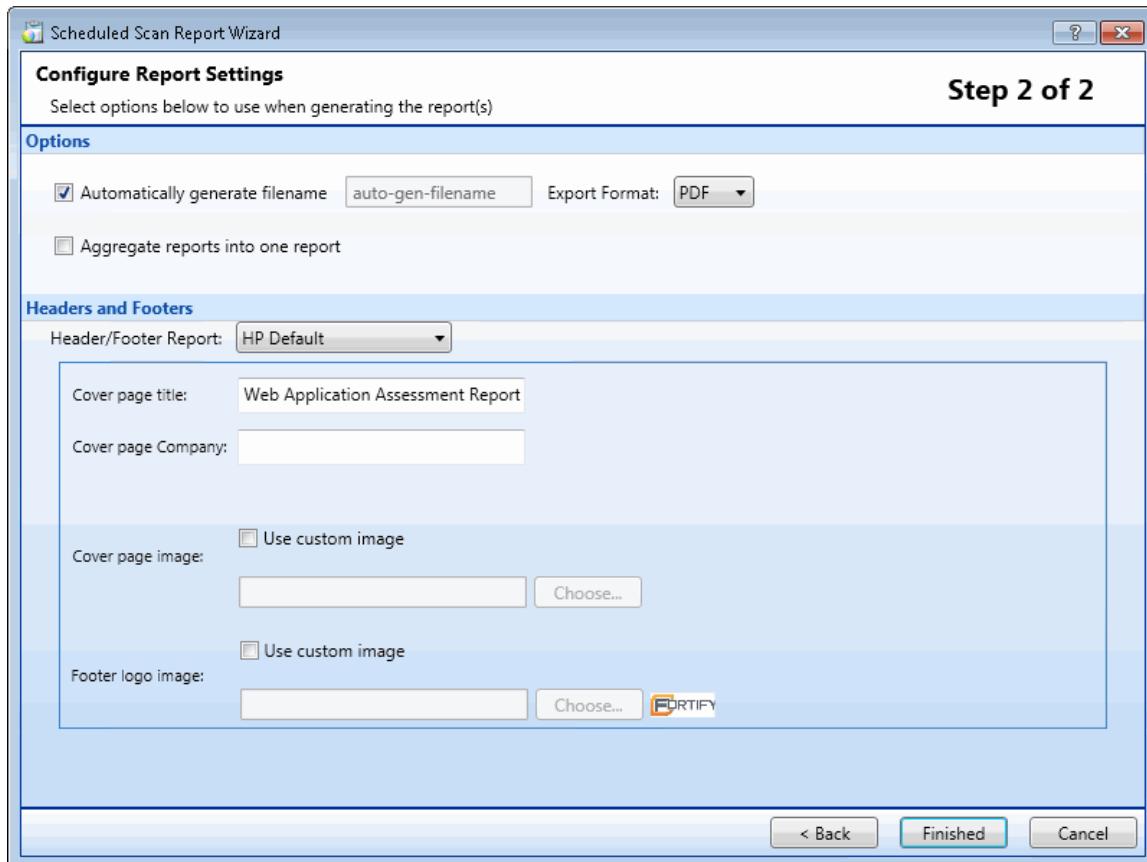
[スケジュールされたスキャンのレポートウィザード(Scheduled Scan Report Wizard)](ステップ1/2)のイメージ



1. (オプション) お気に入り(Favorites) リストからレポートを選択します。
「お気に入り」は、1つ以上のレポートとその関連パラメータの単なる名前付きコレクションです。レポートおよびパラメータを選択した後でお気に入りを作成するには、お気に入り(Favorites) リストをクリックして、お気に入りに追加(Add to favorites)を選択します。
2. 1つ以上のレポートを選択します。
3. 要求できるパラメータの情報を入力します。必須のパラメータは赤で囲まれます。
4. 次へ(Next)をクリックします。
[レポート設定(Configure Report Settings)] ウィンドウが表示されます。

レポート設定を行う

「スケジュールされたスキャンのレポートウィザード(Scheduled Scan Report Wizard)」(ステップ2/2)のイメージ



- 「ファイル名の自動生成(Automatically Generate Filename)」を選択すると、レポートファイルの名前は<reportname> <date/time>.<extension>の形式になります。たとえば、pdf形式でコンプライアンスレポートを作成し、そのレポートが4月5日の6:30に生成される場合、ファイル名は「Compliance Report 04_05_2009 06_30.pdf」になります。これは、反復スキャンの場合に便利です。
レポートは、生成されるレポート用にアプリケーション設定で指定されたディレクトリに書き込まれます。
- 「ファイル名の自動生成(Automatically Generate Filename)」を選択しなかった場合は、「ファイル名(Filename)」ボックスにファイルの名前を入力します。
- 「エクスポート形式(Export Format)」リストからレポート形式を選択します。
- 複数のレポートを選択した場合は、「レポートを1つに集約(Aggregate reports into one report)」を選択することで、すべてのレポートを1つに結合できます。
- レポートに使用するヘッダとフッタを定義するテンプレートを選択し、必要に応じて要求されたパラメータを指定します。
- 「完了(Finished)」をクリックします。
- 「スケジュール(Schedule)」をクリックします。

次も参照

["開始ページ\(Start Page\)" ページ55](#)

["スキャンの管理" ページ219](#)

["スケジュールされたスキャンのステータス" 次のページ](#)

スケジュールされているスキャンの停止

スケジュールされているスキャンを実行中に停止するには、[スケジュールの管理(Manage Schedule)]リストからスキャンを選択して、 Stop をクリックします(またはスキャンを右クリックしてショートカットメニューから [スキャンの停止(Stop Scan)]を選択します)。

停止したスキャンを再開するには、[スケジュールの管理(Manage Schedule)]リストからスキャンを選択して、 Start をクリックします(またはスキャンを右クリックしてショートカットメニューから [スキャンの開始(Start Scan)]を選択します)。

スケジュールされたスキャンのステータス

スケジュールされたスキャンそれぞれのステータスは、[スケジュールの管理(Manage Schedule)]ペインの [前回の実行のステータス>Last Run Status] 列に表示されます。次の表に、それぞれのステータスの定義を示します。

| ステータス | 定義 |
|-------------------------------|---|
| 失敗(Failure) | Fortify WebInspectはスキャンを実行できませんでした。 |
| 成功(Success) | スキャンが実行され、エラーはありませんでした。 |
| 未実行(Not Yet Run) | スキャンは、スケジュールされた時刻に実行するためにキューに登録されていますが、まだ実行されていません。 |
| スキップ済み(Skipped) | サービスが一時的にダウンしたため、スケジュールされたスキャンが実行されませんでした。 |
| 停止中(Stopping) | ユーザが [停止(Stop)] ボタンをクリックしましたが、スキャンはまだ停止していません。 |
| 停止済み(Stopped) | スキャンはユーザによって停止されました。 |
| 実行中(Running) | スケジュールされたスキャンが進行中です。 |
| 実行中、エラーあり(Running with Error) | スキャンを停止できませんでした。詳細についてはログを参照してください。 |

スキャンのエクスポート

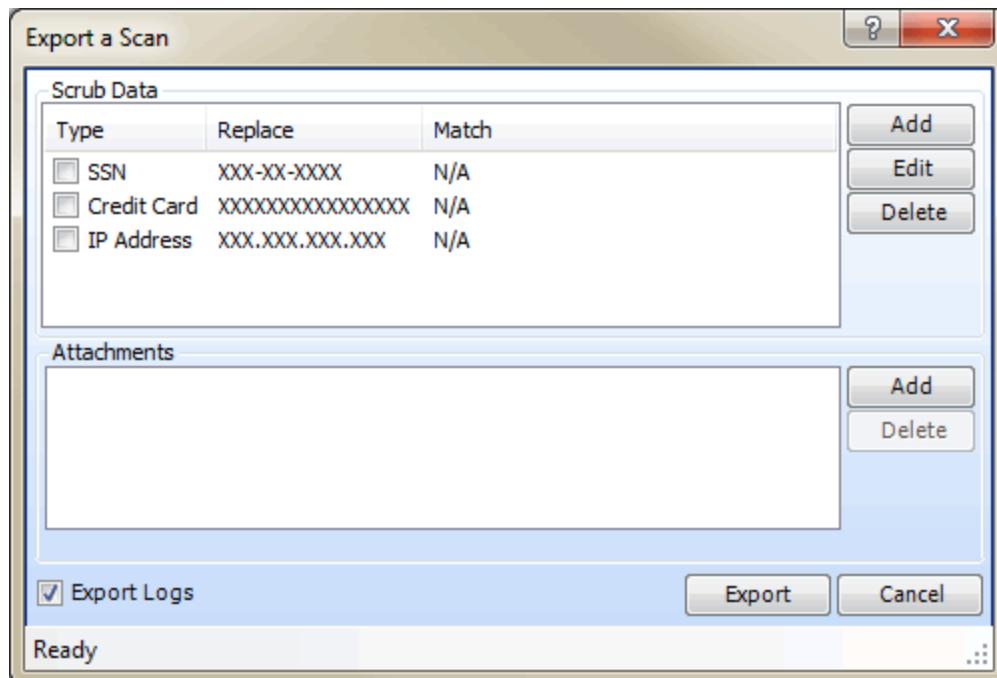
スキャンのエクスポート機能を使用して、Fortify WebInspectのWeb探索または監査時に収集された情報を保存します。

メモ: Fortify Software Security Centerにエクスポートする場合、.fpr形式にエクスポートした後で、.fprファイルをFortify Software Security Centerに手動でアップロードする必要があります。Fortifyでは、Fortify WebInspect FPRアーティファクトとFortify WebInspect Enterprise FPRアーティファクトの両方をFortify Software Security Centerの同じアプリケーションバージョンにアップロードすることはサポートしていません。

スキャンをエクスポートするには、以下のステップに従います。

1. 次のいずれかを実行します。
 - スキャンを開き(または開いているスキャンを含むタブをクリックし)、[ファイル(File)]>[エクスポート(Export)]をクリックして、[スキャン(Scan)]または[スキャンをSoftware Security Centerへ(Scan to Software Security Center)]を選択します。
 - 開始ページ(Start Page)]の[スキャンの管理(Manage Scans)]ペインでスキャンを選択し、[エクスポート(Export)]ボタンのドロップダウン矢印をクリックして、[スキャンのエクスポート(Export Scan)]または[Software Security Centerへのスキャンのエクスポート(Export Scan to Software Security Center)]を選択します。

[スキャンのエクスポート(Export a Scan)]ウィンドウ(または[Software Security Centerへのスキャンのエクスポート(Export Scan to Software Security Center)]ウィンドウ)が表示されます。



2. [スクラブデータ(Scrub Data)]グループには、デフォルトで、社会保障番号、クレジットカード番号、またはIPアドレスとしてフォーマットされた文字列内の各数字をXに置き換える、編集不可の3つの正規表現関数が含まれています。検索および置換機能を含めるには、関連するチェックボックスをオンにします。この機能により、機密データがエクスポートに含まれないようにすることができます。
3. スクラブデータ関数を作成するには:
 - a. [追加(Add)]をクリックします。
 - b. [スクラブ項目の追加(Add Scrub Entry)]ウィンドウで、[タイプ(Type)]リストから[正規表現(Regex)]または[リテラル(Literal)]を選択します。
 - c. [一致(Match)]ボックスに、検索する文字列(または文字列を表す正規表現)を入力します。正規表現を使用する場合は、省略記号ボタン [...]をクリックしてRegular Expression Editorを開き、正規表現を作成およびテストできます。
 - d. [置換(Replace)]ボックスに、[一致(Match)]文字列で指定したターゲットを置き換える文字列を入力します。
 - e. [OK]をクリックします。
4. Software Security Centerにエクスポートする場合は、ステップ7に進みます。
5. 添付ファイルを含める場合:
 - a. [添付ファイル(Attachments)]グループで、[追加(Add)]をクリックします。
 - b. 標準のファイル選択ウィンドウを使用して、添付するファイルを含むディレクトリに移動します。
 - c. ファイルを選択し、[開く(Open)]をクリックします。
6. スキャンのログファイルを含めるには、[ログのエクスポート(Export Logs)]を選択します。
7. [エクスポート(Export)]をクリックします。
8. 標準のファイル選択ウィンドウを使用して場所を選択し、[保存(Save)]をクリックします。

次も参照

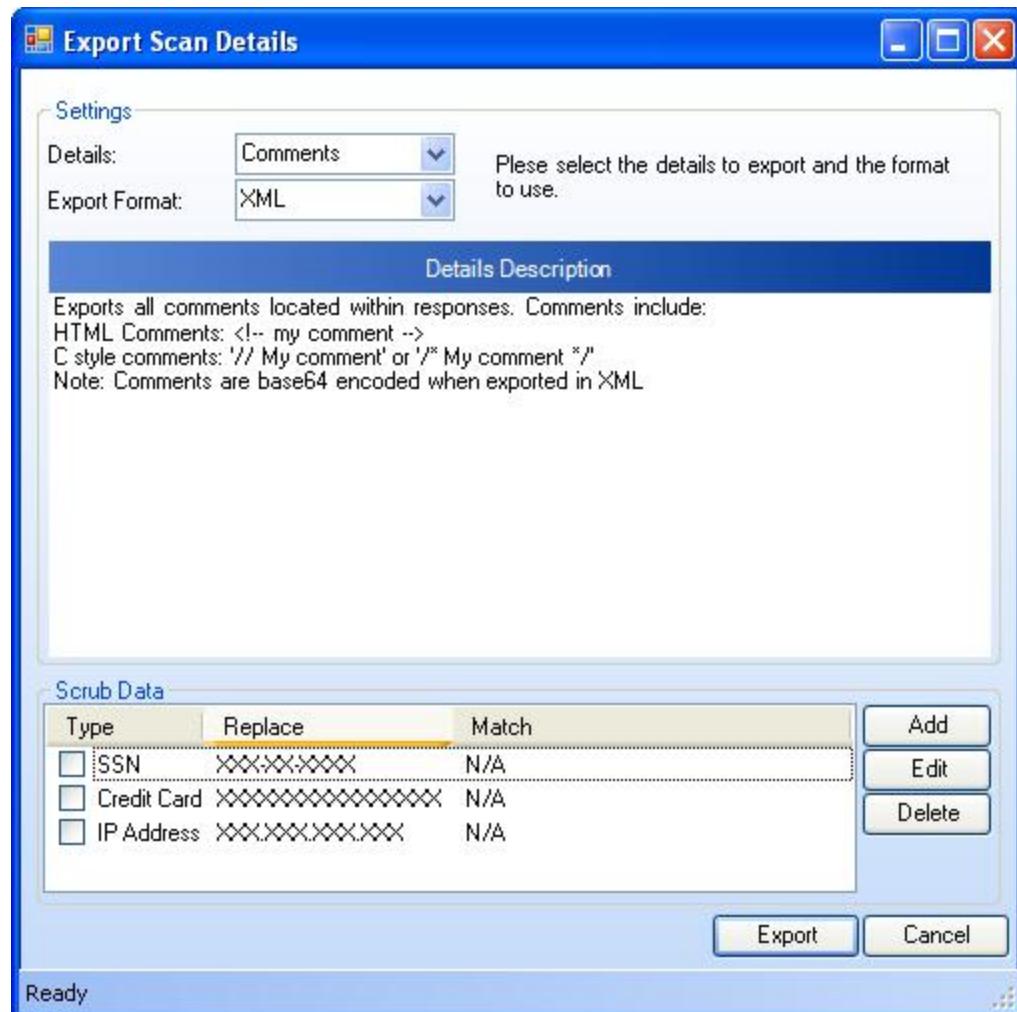
["スキャンのインポート" ページ233](#)

["スキャン詳細のエクスポート" 下](#)

スキャン詳細のエクスポート

この機能を使用して、Fortify WebInspectのWeb探索または監査時に収集された情報を保存します。

1. スキャンを開くか、スキャンを含むタブをクリックします。
 2. [ファイル(File)] > [エクスポート(Export)] > [スキャンの詳細(Scan Details)]の順にクリックします。
- [スキャン詳細のエクスポート(Export Scan Details)]ウィンドウが表示されます。



3. [詳細(Details)]リストから、エクスポートする情報のタイプを選択します。オプションは次のとおりです。
- コメント(Comments)
 - 電子メール(Emails)
 - 完全(すべての詳細)(Full (all details))
 - 非表示フィールド(Hidden Fields)
 - サイト外リンク(Offsite Links)
 - パラメータ(Parameters)
 - 要求(Requests)
 - スクリプト(Script)
 - セッション(Sessions)
 - 設定されているクッキー(Set Cookies)

- URL(URLs)
- 脆弱性(Vulnerabilities)
- Web探索のダンプ(Web Crawl Dump)
- サイトツリーのダンプ(Site Tree Dump)
- Webフォーム(Web Forms)

メモ: 一部の選択肢はWebサービススキャンでは使用できません。

4. [エクスポート形式(Export Format)]リストから形式(テキストまたはXML)を選択します。
5. [スクラブデータ(Scrub Data)]グループには、デフォルトで、社会保障番号、クレジットカード番号、またはIPアドレスとしてフォーマットされた文字列内の各数字をXに置き換える、編集不可の3つの正規表現関数が含まれています。データタイプにこの検索および置換機能を含めるには、関連するチェックボックスをオンにします。この機能により、機密データがエクスポートに含まれないようにすることができます。
6. スクラブデータ関数を作成するには:
 - a. [追加(Add)]をクリックします。
 - b. [スクラブ項目の追加(Add Scrub Entry)]ウィンドウで、[タイプ(Type)]リストから[正規表現(Regex)]または[リテラル(Literal)]を選択します。
 - c. [一致(Match)]ボックスに、検索する文字列(または文字列を表す正規表現)を入力します。正規表現を使用する場合は、省略記号ボタン...をクリックしてRegular Expression Editorを開き、正規表現を作成およびテストできます。
 - d. [置換(Replace)]ボックスに、[一致(Match)]文字列で指定したターゲットを置き換える文字列を入力します。
 - e. [OK]をクリックします。
7. [エクスポート(Export)]をクリックします。
8. 標準のファイル選択ウィンドウを使用して、エクスポートするファイルの名前と場所を指定し、[保存(Save)]をクリックします。

次も参照

["スキャンのエクスポート" ページ228](#)

Software Security Centerへのスキャンのエクスポート

この機能を使用すると、Fortify Software Security Centerで利用できる形式(.fpr形式)でFortify WebInspectスキャンの結果をエクスポートできます。

メモ: .fpr形式にエクスポートした後、その.fprファイルをFortify Software Security Centerに手動でアップロードする必要があります。Fortifyでは、Fortify WebInspect FPRアーティファクトとFortify WebInspect Enterprise FPRアーティファクトの両方をFortify Software

Security Centerの同じアプリケーションバージョンにアップロードすることはサポートしていません。

1. 次のいずれかを実行します。
 - スキャンを開き(または開いているスキャンを含むタブをクリックし)、[ファイル(File)]>[エクスポート(Export)]>[スキャンをSoftware Security Centerへ(Scan to Software Security Center)]をクリックします。
 - 開始ページ(Start Page)]の[スキャンの管理(Manage Scans)]ペインでスキャンを選択し、[エクスポート(Export)]ボタンのドロップダウン矢印をクリックして、[Software Security Centerへのスキャンのエクスポート(Export Scan to Software Security Center)]を選択します。
[Software Security Centerへのスキャンのエクスポート(Export Scan to Software Security Center)]ウィンドウが表示されます。
2. [スクラブデータ(Scrub Data)]グループには、デフォルトで、社会保障番号、クレジットカード番号、またはIPアドレスとしてフォーマットされた文字列内の各数字をXに置き換える、編集不可の3つの正規表現関数が含まれています。検索および置換機能を含めるには、関連するチェックボックスをオンにします。この機能により、機密データがエクスポートに含まれないようにすることができます。
3. スクラブデータ関数を作成するには:
 - a. [追加(Add)]をクリックします。
 - b. [スクラブ項目の追加(Add Scrub Entry)]ウィンドウで、[タイプ(Type)]リストから[正規表現(Regex)]または[リテラル(Literal)]を選択します。
 - c. [一致(Match)]ボックスに、検索する文字列(または文字列を表す正規表現)を入力します。正規表現を使用する場合は、省略記号ボタン...をクリックしてRegular Expression Editorを開き、正規表現を作成およびテストできます。
 - d. [置換(Replace)]ボックスに、[一致(Match)]文字列で指定したターゲットを置き換える文字列を入力します。
 - e. [OK]をクリックします。
4. [エクスポート(Export)]をクリックします。
5. 標準のファイル選択ウィンドウを使用して場所を選択し、[保存(Save)]をクリックします。

Webアプリケーションファイアウォール(WAF)への保護ルールのエクスポート

Webアプリケーションのスキャン中にFortify WebInspectによって検出された脆弱性に基づく完全なエクスポート(.xml)ファイルを生成して保存するには:

1. 対象となるスキャンを開き(または開いているスキャンを含むタブをクリックし)、[ファイル(File)]>[エクスポート(Export)]>[保護ルールをWebアプリケーションファイアウォールへ(Protection Rules to Web Application Firewall)]をクリックします。

2. [ファイル(File)] > [エクスポート(Export)] > [スキャン(Scan)] オプションと同じ方法でスクラブデータのタイプを指定します。[スクラブデータ(Scrub Data)] グループには、デフォルトで、社会保障番号、クレジットカード番号、またはIPアドレスとしてフォーマットされた文字列内の各数字をXに置き換える、編集不可の3つの正規表現関数が含まれています。データタイプにこの検索および置換機能を含めるには、関連するチェックボックスをオンにします。この機能により、機密データがエクスポートに含まれないようにすることができます。
 3. [エクスポート(Export)] をクリックします。
 4. エクスポートしたデータを保存するパスとファイル名を指定し、[保存(Save)] をクリックします。
- 完全なエクスポート(.xml)ファイルが、指定どおりに保存されます。

スキャンのインポート

スキャンをインポートするには:

1. [ファイル(File)] > [スキャンのインポート(Import Scan)] をクリックします。
2. 標準のファイル選択 ウィンドウを使用して、[ファイルの種類(Files Of Type)] リストから次のいずれかのオプションを選択します。
 - スキャンファイル(*.scan) - 7.0 以降のバージョンの Fortify WebInspect で設計または作成されたスキャンファイル。
 - SPAファイル(*.spa) - 7.0 より前のバージョンの Fortify WebInspect によって作成されたスキャンファイル。
3. ファイルを選択し、[開く(Open)] をクリックします。

スキャンと一緒に添付ファイルをエクスポートした場合、その添付ファイルがインポートされて、インポートされたスキャンのサブディレクトリに保存されます。デフォルトの場所は、

C:\Users\<username>\AppData\HP\HP

WebInspect\ScanData\Imports\<DirectoryName>\<filename> です。この場合、DirectoryName は、エクスポートまたはインポートされたスキャンの ID 番号です。

次も参照

["スキャンのエクスポート" ページ228](#)

誤検出のインポート

以前のスキャンから、誤検出として分析された脆弱性のリストをインポートできます。その後、Fortify WebInspect では、以前のスキャンで検出されたこれらの誤検出を、現在のスキャンで検出された脆弱性と関連させ、新たに出現した脆弱性に誤検出のフラグを設定します。

現在スキャンしているのと同じサイトから誤検出を含むスキャンを選択します。

メモ: スキャンのスケジューリング時やエンタープライズスキャンの実行時に誤検出をインポートすることはできません。

誤検出をインポートするには:

1. 現在実行中のスキャンの [スキャン情報(Scan Info)] パネルで、**誤検出(False Positives)** を選択します。
[スキャンの誤検出(Scan False Positives)] ウィンドウが表示されます。
2. **誤検出のインポート(Import False Positives)** をクリックします。
誤検出をインポートするスキャンの選択(Select a Scan to Import False Positives) ウィンドウが表示されます。
3. 誤検出のインポート元のスキャン(複数可)のチェックボックスを選択して、**OK** をクリックします。
誤検出のインポート中(Importing False Positives) ウィンドウが表示され、インポートの進行状況が表示されます。
4. インポートが完了したら、次のいずれかを実行します。
 - **詳細(Details)** をクリックして、インポートのログファイルを表示します。
 - **閉じる(Close)** をクリックして、[スキャンの誤検出(Scan False Positives)] ウィンドウに誤検出を表示します。

レガシWebサービススキャンのインポート

Fortify WebInspect 10.00以降では、9.00より前のバージョンのFortify WebInspectで作成されたWebサービススキャンに対して最小限のサポートを提供します。これらのスキャンには、現在のユーザインターフェースで適切にレンダリングするために必要な情報がすべて含まれているわけではなく、次のような特性があります。

- ツリービューに正しい構造が表示されない場合があります。
- 操作がツリービューに表示されない場合でも、脆弱性リストに脆弱性が表示されます。これらの脆弱性を選択し、脆弱性情報、および要求と応答を表示できます。
- XmlGridには何も表示されません。
- 再スキャン機能により、Webサービススキャンウィザードが起動され、選択したWSDLがすでに入力されている状態で最初のオプションが選択されます。これにより、Web Service Test Designerがページ3で強制的に開かれます。
- 「脆弱性レビュー」機能は無効になっている必要があります。
- すべてのレポートは、以前のFortify WebInspectリリースと同様に機能します。
- スキャンビューは「ReadOnly」モードでレンダリングされます。このモードでは、**開始(Start)** ボタン、**監査(Audit)** ボタン、および**現在の設定(Current Settings)** ボタンが無効になります。

Fortify では、Webサービスを再スキャンすることをお勧めします。

インポート/エクスポート設定の変更

スキャンアクションごとに異なる設定が必要な場合は、XMLファイルに設定を保存し、必要に応じてその設定をロードできます。また、Fortify WebInspectの出荷時のデフォルト設定を再ロードすることもできます。

ヒント: [設定の管理(Manage Settings)] ウィンドウからスキャン設定ファイルを作成、編集、削除、インポート、およびエクスポートすることもできます。 [編集(Edit)] をクリックし、[設定の管理(Manage Settings)] を選択します。

設定をインポート、エクスポート、または復元するには:

1. [編集(Edit)] > [デフォルト設定(Default Settings)] をクリックします。
[デフォルト設定(Default Settings)] ウィンドウが表示されます。
2. 設定をエクスポートするには:
 - a. 左ペインの下部にある [設定に名前を付けて保存(Save settings as)] をクリックします。
 - b. [Save Scan Settings (スキャン設定の保存)] ウィンドウで、フォルダを選択してファイル名を入力します。
 - c. [保存(Save)] をクリックします。
3. 設定をインポートするには:
 - a. 左ペインの下部にある [ファイルから設定をロード(Load settings from file)] をクリックします。
 - b. [スキャン設定ファイルを開く(Open Scan Settings File)] ウィンドウで、ファイルを選択します。
 - c. [開く(Open)] をクリックします。
4. 出荷時のデフォルト設定を復元するには:
 - a. 左ペインの下部にある [出荷時のデフォルト設定を復元(Restore factory defaults)] をクリックします。
 - b. 選択内容を確認するプロンプトが表示されたら、[はい(Yes)] をクリックします。

エンタープライズサーバからのスキャンのダウンロード

次の手順を使用して、エンタープライズサーバ(Fortify WebInspect Enterprise)からFortify WebInspectにスキャンをダウンロードします。

1. [エンタープライズサーバ(Enterprise Server)] メニューをクリックし、[スキャンのダウンロード(Download Scan)] を選択します。
2. [スキャンのダウンロード(Download Scan)] ウィンドウで、使用可能なスキャンのリストから1つ以上のスキャンを選択します。
3. [OK] をクリックします。

ダウンロードしたスキャンは、[スキャンの管理 (Manage Scans)] ペインのスキャンのリストに追加されます。スキャンの日付は、サイトが最初にスキャンされた日付ではなく、スキャンをダウンロードした日付になります。詳細については、「["スキャンの管理" ページ219](#)」を参照してください。

ログファイルがダウンロードされない

トランザクションファイルを含むログファイルは、Fortify WebInspect EnterpriseからFortify WebInspectにセンサススキャナをダウンロードする際にダウンロードされません。スキャンのログファイルを取得して表示するには、Fortify WebInspect Enterpriseからスキャンを手動でエクスポートしてから、そのスキャンをFortify WebInspectにインポートする必要があります。詳細については、「["スキャンのインポート" ページ233](#)」を参照してください。

次も参照

["エンタープライズサーバへのスキャンのアップロード" 下](#)

エンタープライズサーバへのスキャンのアップロード

Fortify WebInspectからエンタープライズサーバ(Fortify WebInspect Enterprise)へスキャンファイルをアップロードするには、次の手順を使用します。

1. Fortify WebInspectの [エンタープライズサーバ(Enterprise Server)] メニューをクリックして、[スキャンのアップロード(Upload Scan)] を選択します。
2. [スキャンのアップロード(Upload Scan(s))] ウィンドウで、[スキャン名(Scan Name)] 列から1つ以上のFortify WebInspectスキャンを選択します。

メモ: 別のデータベースのスキャンにアクセスするには、[接続(Connections)] をクリックし、データベースアプリケーション設定で [スキャン表示の接続設定(Connection Settings for Scan Viewing)] のオプションを変更します。
3. スキャンごとに、該当するドロップダウンリストからアプリケーションおよびバージョンを選択します。
プログラムはスキャンファイルの「スキャンURL」を基に正しいアプリケーションとバージョンの選択を試みますが、代わりのものを自分で選択しても構いません。
4. [アップロード(Upload)] をクリックします。

次も参照

["エンタープライズサーバからのスキャンのダウンロード" 前のページ](#)

エンタープライズサーバでのスキャンの実行

この機能は、Fortify WebInspect Enterpriseではなく、Fortify WebInspectでスキャンを設定することを望むユーザ向けです。設定を変更してFortify WebInspectでスキャンを実行し、最適な設定が得られるまでこのプロセスを繰り返すことができます。その後、開いているスキャン

の設定をFortify WebInspect Enterpriseに送信すると、スキャン要求が作成され、次に利用可能なセンサのスキャンキューに配置されます。

WebInspect Enterpriseでスキャンを実行するには:

1. スキャンを開きます。
2. エンタープライズサーバに接続していない場合は、[エンタープライズサーバ(Enterprise Server)]メニューをクリックして、[WebInspect Enterpriseに接続する(Connect to WebInspect Enterprise)]を選択します。
3. [スキャン(Scan)]メニューをクリックし、[WebInspect Enterpriseで実行(Run in WebInspect Enterprise)]を選択します(またはツールバーの適切なボタンをクリックします)。
4. [WebInspect Enterpriseでスキャンを実行(Run Scan in WebInspect Enterprise)]ダイアログボックスで、スキャンの名前を入力します。
5. [アプリケーション(Application)]と[バージョン(Version)]を選択します。
6. [OK]をクリックします。

すべての許可チェックに合格するとスキャンが作成され、スキャンに割り当てる優先度は、役割で許可されている最高の優先度に設定されます(最大3で、これがデフォルトです)。

エンタープライズサーバとの間での設定の転送

この機能は、次の目的で使用します。

- Fortify WebInspect設定ファイルに基づいてFortify WebInspect Enterpriseスキャンテンプレートを作成し、Fortify WebInspectからエンタープライズサーバ(Fortify WebInspect Enterprise)にそのテンプレートをアップロードする。
- エンタープライズサーバのスキャンテンプレートに基づいてFortify WebInspect設定ファイルを作成し、Fortify WebInspectにその設定ファイルをダウンロードする。

Fortify WebInspect設定ファイルとFortify WebInspect Enterpriseスキャンテンプレートの形式は同じではありません。一方の形式のすべての設定がもう一方の形式で複製されるわけではありません。変換手順の説明の後の警告に注意してください。

Fortify WebInspect Enterpriseスキャンテンプレートの作成

Fortify WebInspect Enterpriseスキャンテンプレートを作成するには:

1. Fortify WebInspectの[エンタープライズサーバ(Enterprise Server)]メニューをクリックし、[転送設定(Transfer Settings)]を選択します。
2. [転送設定(Transfer Settings)]ウィンドウで、[ローカル設定ファイル(Local Settings File)]リストからFortify WebInspect設定ファイルを選択します。
3. (オプション) [表示(View)]をクリックして、Fortify WebInspect設定ファイルに表示される設定を確認します。続行するには、[閉じる(Close)]をクリックします。

メモ: これは読み込み専用ファイルです。変更は保持されません。

4. Fortify WebInspect Enterpriseでテンプレートの転送先となるアプリケーションおよびバージョンを選択します。
5. 必要に応じて、[更新(Refresh)]をクリックして、リストに最新の設定ファイルとスキャンテンプレートが含まれていることを確認します。
6. 作成するスキャンテンプレートの名前を入力します。既存のテンプレートの名前を複製することはできません。
7. [アップロード(Upload)]をクリックします。

Fortify WebInspectから抽出されないテンプレート設定はすべて、Fortify WebInspect Enterpriseテンプレートのデフォルト設定を使用します。

- スキャンテンプレートでは、Fortify WebInspect設定ファイルで使用されるポリシーは指定されません。代わりに、「Use Any」オプションが含まれます。
- Fortify WebInspect設定ファイルに含まれているクライアント証明書情報はスキャンテンプレートに転送されますが、証明書は送信されません。
- すべてのFortify WebInspect設定は、Fortify WebInspect Enterpriseで使用されていない場合でもスキャンテンプレートに保持されます。したがって、元の設定ファイルから作成したスキャンテンプレートに基づいて、後でFortify WebInspect設定ファイルを作成すると、Fortify WebInspect設定は保持されます。

Fortify WebInspect設定ファイルの作成

Fortify WebInspect設定ファイルを作成するには

1. Fortify WebInspectの[エンタープライズサーバ(Enterprise Server)]メニューをクリックし、[転送設定(Transfer Settings)]を選択します。
2. Fortify WebInspect Enterpriseでテンプレートの転送元となるアプリケーションおよびバージョンを選択します。
3. [転送の設定(Transfer Settings)]ウィンドウで、リストからスキャンテンプレートを選択します。
4. (オプション) [表示(View)]をクリックして、Fortify WebInspect設定ファイルに表示される設定を確認します。続行するには、[閉じる(Close)]をクリックします。

メモ: これは読み込み専用ファイルです。変更は保持されません。

5. 必要に応じて、[更新(Refresh)]をクリックして、リストに最新の設定ファイルとスキャンテンプレートが含まれていることを確認します。
6. [ダウンロード(Download)]をクリックします。
7. 標準のファイル選択ウィンドウを使用して、設定ファイルに名前を付け、保存先を選択し、[保存(Save)]をクリックします。

Fortify WebInspect設定ファイルでは、スキャンテンプレートで使用されるポリシーは指定されません。代わりに、標準ポリシーが指定されます。

スキャンの発行 (Fortify WebInspect Enterprise接続)

メモ: このトピックは、Fortify WebInspect EnterpriseがFortify Software Security Centerと統合されている場合にのみ適用されます。

Fortify WebInspect Enterpriseを介して、Fortify WebInspectからFortify Software Security Centerのサーバにスキャンデータを送信するには、次の手順に従います。

メモ: 同じWebサイトまたはアプリケーションに対して複数のスキャンを実行する際にFortify Software Security Centerの脆弱性のステータスを管理する方法については、「["Fortify Software Security Centerへの脆弱性の統合"次のページ](#)」を参照してください。

1. Fortify WebInspect EnterpriseとFortify Software Security Centerを設定します。
2. Fortify WebInspectでスキャンを実行します(または、インポートまたはダウンロードしたスキャンを使用します)。
3. [エンタープライズサーバ(Enterprise Server)]メニューをクリックして、[WebInspect Enterpriseへの接続(Connect to WebInspect Enterprise)]を選択します。資格情報の送信を求めるプロンプトが表示されます。
4. フォーカスされているタブでスキャンが開かれていて、そのスキャンのみを発行する場合:
 - a.  Synchronize をクリックします。
 - b. アプリケーションとバージョンを選択し、[OK]をクリックします。
 - c. 結果を検査します。サマリペインに「発行済みステータス(Published Status)」と「保留中のステータス(Pending Status)」を示すカラムが表示されます。「発行済みステータス」は、このスキャンが最後にFortify WebInspect Enterpriseに発行された時の脆弱性のステータスです。「保留中のステータス」は、このスキャンが発行された後の脆弱性のステータスが何になるかを示します。一部の「保留中のステータス」は、脆弱性が解決済みか、それともまだ存在しているか示すために変更することができます(次のステップ7を参照)。また、[未検出(Not Found)]という名前の新しいタブが表示されます。このタブには、前回のスキャンでは検出されたものの、現在のスキャンでは検出されていない脆弱性が含まれています。脆弱性にスクリーンショットやコメントを追加したり、脆弱性に誤検出または無視のマークを付けたりすることができます。また、脆弱性を確認して再テストし、スキャン結果を変更して発行の準備を行うことができます。
 - d.  Publish をクリックします。ステップ7に進みます。
5. スキャンのリストから選択するには:
 - a. [エンタープライズサーバ(Enterprise Server)]メニューをクリックして、[スキャンの発行(Publish Scan)]を選択します。
 - b. [スキャンをSoftware Security Centerに発行する(Publish Scan(s) to Software Security Center)]ダイアログボックスで、1つ以上のスキャンを選択します。
 - c. アプリケーションとバージョンを選択します。

- d. 次へ(Next)]をクリックします。Fortify WebInspectはFortify Software Security Centerと自動的に同期します。
6. Fortify WebInspectには、ステータスおよび重大度別に分類された、発行される脆弱性の数の一覧が表示されます。

ステータスを判断するために、Fortify WebInspectは以前に送信された脆弱性(Fortify Software Security Centerと同期して取得されたもの)を現在のスキャンで報告された脆弱性と比較します。これがアプリケーションのあるバージョンに対して初めて送信されたスキャンである場合、すべての脆弱性は「新規(New)」になります。

脆弱性が以前に報告されているものの現在のスキャンに含まれていない場合、「未検出(Not Found)」のマークが付けられます。見つからなかった理由が、修復されたためか、それともスキャンの設定が異なっているからなのかを判断する必要があります(たとえば、別のスキャンポリシーを使用していた場合や、サイトの別の部分をスキャンした場合、スキャンを途中で終了した場合などがあります)。結果を調べるときに(ステップ4c)、最初のスキャンを除くすべての脆弱性で検出された個々の脆弱性の「保留中のステータス」を変更できます(サマリペインで脆弱性を右クリック)。ただし、発行時に、Fortify WebInspectが残りの「未検出(Not Found)」の脆弱性を処理する方法を指定する必要があります。

Fortify Software Security Centerでこれらの「未検出(Not Found)」の脆弱性を保持する(脆弱性が依然として存在することを示すため)には、**保持: スキャンでまだ「未検出」とマークされているすべての脆弱性をまだ存在していると見なす(Retain: Assume all vulnerabilities still marked "Not Found" in the scan are still present)**を選択します。

これらの脆弱性を削除する(修復済みであることを示す)には、**解決: スキャンでまだ「未検出」とマークされているすべての脆弱性を修復済みと見なす(Resolve: Assume all vulnerabilities still marked "Not Found" in the scan are fixed)**を選択します。

7. このスキャンが、Fortify Software Security Centerで開始されたスキャン要求に応じて実行された場合は、**スキャンを、現在のアプリケーションバージョンに対する「進行中」スキャン要求に関連付ける(Associate scan with an "In Progress" scan request for the current application version)**を選択します。
8. **発行(Publish)**をクリックします。

Fortify Software Security Centerへの脆弱性の統合

メモ: このトピックは、Fortify WebInspect EnterpriseがFortify Software Security Centerと統合されている場合にのみ適用されます。

Fortify Software Security Centerは、ソフトウェアのセキュリティ脆弱性を特定し、順位付けて、修復する、緊密に統合されたソリューションから成るスイートです。これは、Fortify Static Code Analyzerを使用してスタティック分析を行い、Fortify WebInspectを使用してダイナミックなアプリケーションセキュリティテストを実施します。Fortify WebInspect Enterpriseは、複数のFortify WebInspectスキャナを管理し、Fortify Software Security Center内の個々のアプリ

ケーションバージョンに直接発行できるスキャン結果を相関させるための中央の場所を提供します。

Fortify WebInspect Enterpriseは、特定のFortify Software Security Centerアプリケーションバージョンのすべての脆弱性の履歴を保持します。Fortify WebInspectは、スキャンを実行した後、Fortify WebInspect Enterpriseと同期してその履歴を取得し、スキャンの脆弱性と履歴内の脆弱性を比較して、各脆弱性にステータスを割り当てます。次の表で、ステータスについて説明します。

| Fortify Software Security Centerのステータス | 説明 |
|--|---|
| 新規 (New) | 以前に報告されていない問題。 |
| 既存 (Existing) | すでに履歴にあるスキャンの脆弱性。 |
| 未検出 (Not Found) | 履歴にはあるものの、スキャンでは見つからない脆弱性。これは、(a)脆弱性が改善されて存在しなくなった、または(b)最新のスキャンで別の設定が使用されたか、サイトの別の部分がスキャンされたか、または他の何らかの理由で脆弱性が検出されなかつたために発生する可能性があります。 |
| 解決済み (Resolved) | 修復された脆弱性。 |
| 復活 (Reintroduced) | 以前に「解決済み (Resolved)」と報告されたが、現在のスキャンに表示される脆弱性。 |
| 依然として問題 (Still an Issue) | 現在のスキャンで「未検出 (Not Found)」であったが、実際には存在する脆弱性。 |

個々の脆弱性のFortify Software Security Centerのステータスを変更するには、[検出事項 (Findings)]タブで脆弱性を右クリックし、[保留中のステータスの変更 (Modify Pending Status)]を選択します。このオプションは、Fortify WebInspect Enterpriseに接続した後にのみ表示され、Fortify WebInspectをSoftware Security Centerと同期した後でのみ有効になります。

以下に、脆弱性をFortify Software Security Centerに統合するための仮想の一連のスキャンの例を示します。

最初のスキャン

1. Fortify WebInspectでターゲットサイトをスキャンします。この例では、1つの脆弱性 (Vuln A)のみ検出されたとします。
2. 結果を検査します。脆弱性にスクリーンショットやコメントを追加したり、脆弱性に誤検出または無視のマークを付けたりすることができます。脆弱性を確認、再テスト、および

削除することもできます。

3. Fortify Software Security Centerでスキャンをアプリケーションバージョンと同期してから、スキャンを発行します。

2回目のスキャン

1. 2回目のスキャンでVuln Aが再び明らかになり、さらに4つの脆弱性(Vuln B、C、D、およびE)も検出されます。
2. Fortify Software Security Centerでスキャンをアプリケーションバージョンと同期します。
3. 次に、結果を検査します。最初のスキャンを発行するときに監査データ(コメントやスクリーンショットなど)をVuln Aに追加した場合、そのデータは新しいスキャンにインポートされます。
4. スキャンをFortify Software Security Centerに発行します。Vuln Aには「既存」のマークが付けられ、Vuln BからEには「新規」のマークが付けられます。Fortify Software Security Centerシステムには5つの項目が存在することになります。

3回目のスキャン

1. 3回目のスキャンでは、Vuln B、C、およびDは検出されますが、Vuln AもVuln Eも検出されません。
2. Fortify Software Security Centerでスキャンをアプリケーションバージョンと同期します。
3. Vuln Aの再テスト後、実際にはVuln Aは存在すると判断します。その保留中のステータスを「依然として問題(Still an Issue)」に変更します。
4. Vuln Eの再テスト後、Vuln Eは存在しないと判断します。その保留中のステータスを「解決済み(Resolved)」に変更します。
5. スキャンをFortify Software Security Centerに発行します。Vuln B、C、およびDには「既存(Existing)」のマークが付けられます。Fortify Software Security Centerシステムには5つの項目が存在することになります。

4回目のスキャン

1. 4回目のスキャンでは、Vuln AもVuln Bも検出されません。このスキャンでは、Vuln C、D、E、およびFが検出されます。
2. Fortify Software Security Centerでスキャンをアプリケーションバージョンと同期します。
3. Vuln Eは以前に解決済みと宣言されたので、そのステータスは「復活(Reintroduced)」に設定されています。
4. 検出されなかった脆弱性を調べます(この例では、AとB)。脆弱性がまだ存在すると判断した場合は、保留中のステータスを「依然として問題(Still an Issue)」に更新します。再テストによって脆弱性が存在しないと確認された場合は、保留中のステータスを「解決済み(Resolved)」に更新します。
5. スキャンをFortify Software Security Centerに発行します。Vuln CおよびDは「Existing(既存)」のマークが付いたままになります。

Fortify Software Security Centerとの同期

メモ: このトピックは、Fortify WebInspect EnterpriseがFortify Software Security Centerと統合されている場合にのみ適用されます。

このダイアログボックスを使用して、アプリケーションとバージョンを指定し、Fortify Software Security Centerと同期します。Fortify WebInspectは次にFortify Software Security Centerから脆弱性のリストをダウンロードし、ダウンロードした脆弱性と現在のスキャンで検出された脆弱性を比較し、適切なステータス(「新規(New)」、「既存(Existing)」、「再導入(Reintroduced)」、または「未検出(Not Found)」)を割り当てます。詳細については、「["Fortify Software Security Centerへの脆弱性の統合" ページ240](#)」を参照してください。

Fortify Software Security Centerと同期するには:

1. ツールバーの **同期(Synchronize)**]をクリックします。
2. アプリケーションを選択します。
3. バージョンを選択します。
4. **OK**]をクリックします。

第5章: WebInspectの機能の使用

この章では、Server ProfilerやWeb Macro Recorderツールなど、Fortify WebInspectで使用できる特定のツールについて説明します。また、スキャン結果を検査し、スキャン中に検出された脆弱性を処理する方法も説明します。WebInspect API、正規表現、およびFortifyポリシーの使用法を説明します。この章には、コンプライアンスエンプレートとFortify WebInspectのレポート機能に関する情報も含まれています。

Fortify WebInspectで使用可能なすべてのツールの詳細については、『*Micro Focus Fortify WebInspect Tools Guide*』を参照してください。

再テストと再スキャン

Fortify WebInspectには、検出された脆弱性を再テストおよび再スキャンする複数の方法が用意されています。以下を実行できます。

- 個々の脆弱性、すべての脆弱性、または特定の重大度を持つすべての脆弱性を再テストする。詳細については、「["脆弱性の再テスト" 下](#)」を参照してください。
- サイト全体を再スキャンする。詳細については、「["サイトの再スキャン" ページ249](#)」を参照してください。
- 以前のスキャンのデータを新しいスキャンを支援するために再利用する。詳細については、「["スキャンの再利用" ページ250](#)」および「["増分スキャン" ページ251](#)」を参照してください。

脆弱性の再テスト

スキャンの実行と検出された脆弱性の報告が済むと、開発者がコードの修正とサイトの更新を行えるようになります。その後、元のスキャンを開いて再テストのスキャンを行うことで、次が修復されていることを確認できます。

- 選択した脆弱性
- すべての脆弱性
- 特定の重大度を持つすべての脆弱性

Fortify WebInspectは新しいスキャンを開始して、問題が修復されたかどうかを判断します。再テストのスキャンでは、元のスキャン名の前に「retest:」が付くので、元のスキャンと再テストのスキャンを簡単に識別できます。

再テストのスキャン中、再テストのキューに登録されている脆弱性はサマリペインの「検出事項(Findings)」タブに一覧表示され、「再テストのステータス(Retest Status)」列には再テストの結果が示されます。

重要! Fortifyでは、前のバージョンのFortify WebInspectを使用して作成されたスキャンで脆弱性を再テストすることはお勧めしません。前のバージョンからのスキャンの再テストは多

くのインスタンスで機能すると考えられますが、再テストの際に個々のチェックで同じ脆弱性にフラグが付けられるとは限らないため、常に信頼できるわけではありません。前のバージョンのFortify WebInspectからのスキャンを再テストする際に、チェックが同じ脆弱性にフラグを付けないとしても、脆弱性が改善されたことを意味するとは限りません。

再テストのステータスについて

次の表で、[再テストのステータス(Retest Status)]列に表示される値について説明します。

| ステータス | 説明 |
|---|---|
| 処理中 (Processing) | 脆弱性は現在再テスト中です。これは一時的なステータスで、再テストが完了すると最終的なステータスに置き換えられます。 |
| 検出済み (Detected) | 脆弱性は再テストのスキャンで再現されました。 |
| 検出なし、相関エラーの可能性 (Not Detected, Possible Correlation Failure) | 再テストのスキャン中に同じチェックIDを持つ脆弱性が検出されました が、再テスト中の検出事項と相関が一致しません。 |
| メモ: 相関とは、Fortify WebInspectが、同じパラメータまたは場所を 使用して脆弱性を固有に識別する方法を指します。 | |
| 検出なし(Not Detected) | 脆弱性は、テスト対象のパラメータまたは場所に存在しません。 |
| サポート対象外 | 脆弱性は再テストされませんでした。再テストは、この特定の脆弱性に 対してサポートされていません。詳細については、「 "失敗した脆弱性およびサポート対象外の脆弱性に関する推奨事項"次のページ 」を参照 してください。 |
| 失敗 | 特定の脆弱性の再テストが失敗しました。失敗の理由を示す次の失 敗ステータスも確認できます。 <ul style="list-style-type: none"> 失敗、トリガセッションが見つかりません(Failed, Trigger Session Not Found) 失敗、トリガセッションの応答がありません(Failed, Trigger Session Response Missing) 失敗、トリガセッションのステータスコードが異なります(Failed, Trigger Session Status Code Different) 詳細については、「 "失敗した脆弱性およびサポート対象外の脆弱性に関する推奨事項"次のページ 」を参照してください。 |

| ステータス | 説明 |
|--------------------------------|--|
| 依存関係の失敗 (Dependency Failed) | 元のスキャンに存在していた依存関係を検証スキャンで複製できなかつたため、再テストを完了できませんでした。 |

失敗した脆弱性およびサポート対象外の脆弱性に関する推奨事項

Fortifyでは、再テストのステータスが「失敗」または「サポート対象外」である脆弱性に対して、改善の再利用スキャン、または新しいスキャンの実行をお勧めします。改善の再利用スキャンの詳細については、「["スキャンの再利用" ページ250](#)」を参照してください。

すべての脆弱性の再テスト

スキャンのすべての脆弱性を再テストするには:

- 次のいずれかを実行します。
 - [スキャンの管理(Manage Scans)]リストでスキャンを右クリックして、[再スキャン(Rescan)]>[脆弱性の再テスト(Retest Vulnerabilities)]>[すべての再テスト(Retest All)]を選択します。
 - 開いているスキャンの[スキャン(Scan)]メニューで、[再スキャン(Rescan)]ドロップダウンリストをクリックして、[脆弱性の再テスト(Retest Vulnerabilities)]>[すべての再テスト(Retest All)]を選択します。
 - 開いているスキャンのサマリペインの[検出事項(Findings)]タブで脆弱性を右クリックし、[再テスト(Retest)]>[すべての再テスト(Retest All)]を選択します。

元のスキャン名の前に「retest:」が付けられて、再テストのスキャンが開始します。

特定の重大度を持つすべての脆弱性の再テスト

スキャンの特定の重大度を持つすべての脆弱性を再テストするには:

- 次のいずれかを実行します。
 - [スキャンの管理(Manage Scans)]リストでスキャンを右クリックして、[再スキャン(Rescan)]>[脆弱性の再テスト(Retest Vulnerabilities)]>[重大度別の再テスト(Retest by Severity)]を選択します。
 - 開いているスキャンの[スキャン(Scan)]メニューで、[再スキャン(Rescan)]ドロップダウンリストをクリックして、[脆弱性の再テスト(Retest Vulnerabilities)]>[重大度別の再テスト(Retest by Severity)]を選択します。
 - 開いているスキャンのサマリペインの[検出事項(Findings)]タブで脆弱性を右クリックし、[再テスト(Retest)]>[重大度別の再テスト(Retest by Severity)]を選択します。
- 特定の重大度([重大(Critical)]、[高(High)]、[中(Medium)]、[低(Low)])を選択します。

メモ: ある重大度がコンテキストメニューにない場合、スキャンにはその重大度の脆弱性がありません。

元のスキャン名の前に「retest:」が付けられて、再テストのスキャンが開始します。

選択した脆弱性の再テスト

選択した1つ以上の脆弱性を再テストするには:

1. 開いているスキャンのサマリペインの [検出事項(Findings)] タブで、次のいずれかを実行します。
 - 1つの脆弱性を再テストするには、その脆弱性を右クリックします。
 - 複数の脆弱性を再テストするには、<CTRL>キーを押しながら脆弱性をクリックしてそれらを選択し、次いで右クリックします。
2. [再テスト(Retest)] > [選択した脆弱性の再テスト(Retest Selected)] を選択します。

元のスキャン名の前に「retest:」が付けられて、再テストのスキャンが開始します。

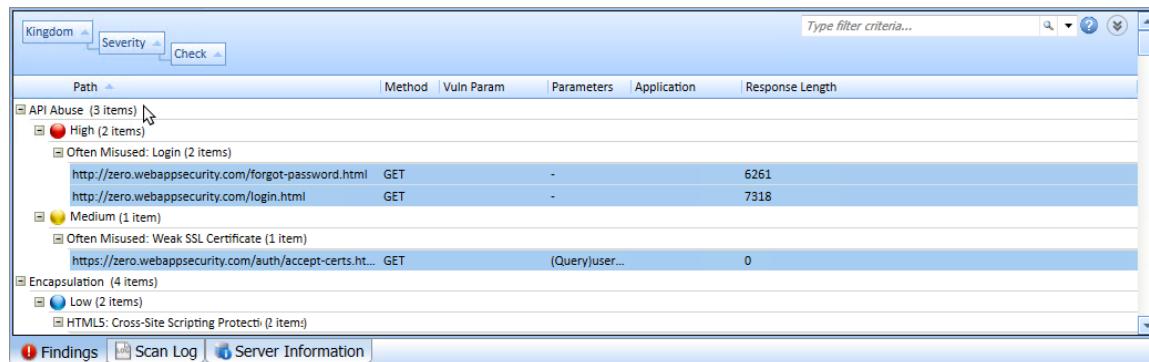
グループ化されたカテゴリの再テスト

検出事項がカテゴリにグループ化されている場合は、グループを選択して、そのカテゴリ内のすべての項目を再テストできます。

グループを再テストするには:

1. 再テストするグループを選択します。

グループ内のすべての検出事項が選択されます。たとえば、次のイメージでは、検出事項が「界(Kingdom)」、「重大度(Severity)」、「チェック(Check)」の順でグループ化されています。[APIの誤用] グループが選択されているため、そのカテゴリ内のすべての検出事項が選択されています。



| Path | Method | Vuln Param | Parameters | Application | Response Length |
|---|--------|----------------|------------|-------------|-----------------|
| API Abuse (3 items) | | | | | |
| High (2 items) | | | | | |
| Often Misused: Login (2 items) | | | | | |
| http://zero.webappsecurity.com/forgot-password.html | GET | | | 6261 | |
| http://zero.webappsecurity.com/login.html | GET | | | 7318 | |
| Medium (1 item) | | | | | |
| Often Misused: Weak SSL Certificate (1 item) | | | | | |
| https://zero.webappsecurity.com/auth/accept-certs.ht... | GET | (Query)user... | | 0 | |
| Encapsulation (4 items) | | | | | |
| Low (2 items) | | | | | |
| HTML5: Cross-Site Scripting Protection (2 items) | | | | | |

2. 右クリックし、[再テスト(Retest)] > [選択した脆弱性(Selected)] を選択します。

ヒント: グループを右クリックすると、カテゴリ内のすべての検出事項を選択し、コンテキストメニューを表示することができます。

グループの詳細については、「"サマリペインのフィルタとグループの使用" ページ262」を参照してください。

再テストのスキャンの再テスト

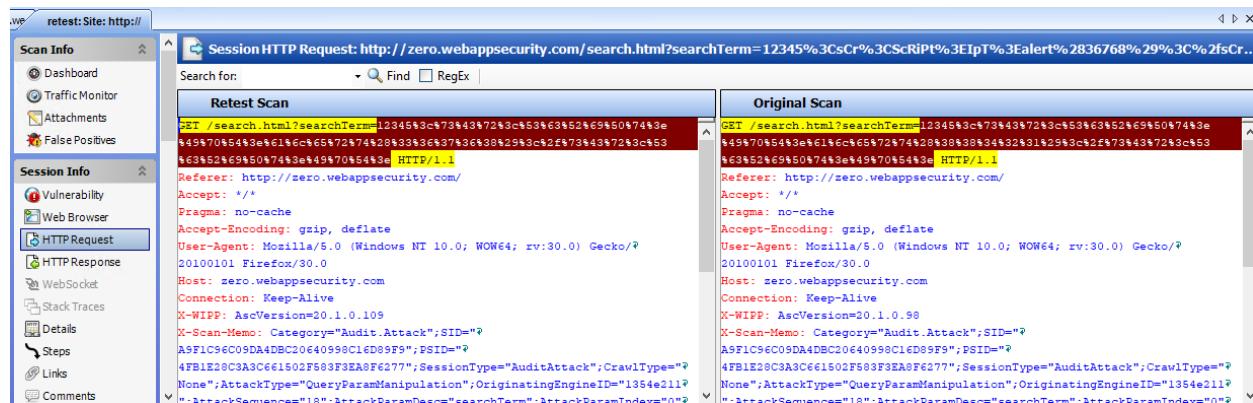
元のスキャンを再テストするのと同じ方法で、再テストのスキャンの検出事項を再テストできます。ただし、再テストできるのは、再テストのステータスが「検出済み(Detected)」の検出事項のみです。それ以外の再テストのステータスを持つ検出事項は再テストされません。

再テストのスキャンログ

スキャンの多数の検出事項を再テストする場合は、再テストのスキャンの「スキャンログ(Scan Log)」タブで結果のスナップショットを確認できます。

比較ビュー

再テストのスキャンで脆弱性を選択する場合、両方のスキャンからの特定のデータをデュアルペインビューで確認できます。[HTTP要求(HTTP Request)]、[HTTP応答(HTTP Response)]、または[ステップ(Steps)]を選択して、再テストのスキャンと元のスキャンを比較するデュアルペインビューを表示します。元のスキャンが使用できない場合は、再テストのスキャンのデータだけが表示されます。



[HTTP要求(HTTP Request)]ビューおよび[HTTP応答(HTTP Response)]ビューでデータを検索するには:

1. [検索対象(Search for)]フィールドに検索用語を入力します。
2. 必要に応じて、検索条件で正規表現を使用するには、[RegEx]オプションを選択します。
3. [検索(Find)]をクリックします。

データが見つかった場合は、再テストのスキャンと元のスキャンの両方で強調表示されます。

詳細については、「"HTTP要求(HTTP Request)" ページ95」、「"HTTP応答(HTTP Response)" ページ95」、および「"ステップ(Steps)" ページ96」を参照してください。

再テストのスキャンの保持または削除

開いているスキャンを閉じると、Fortify WebInspectはそれが再テストのスキャンであるかどうかを検出します。次の条件が満たされた場合は、スキャンの保持についてプロンプトが表示さ

れます。

- 再テストのスキャンである。
- 親スキャンがスキャンデータベースに存在する。
- 以前にそのスキャンのプロンプトが表示されたことがない。

これらの条件が満たされた場合、「スキャン"retest:<ScanName>"を保持しますか? (Do you want to keep the scan "retest:<ScanName>?)」というメッセージが表示されます。これらの条件を満たす再テストのスキャンのタブを複数閉じると、再テストのスキャンごとにプロンプトが表示されます。

次のいずれかを実行します。

- 再テストのスキャンを保持するには、[はい(Yes)]をクリックします。
スキャンが保存され、[最近開いたスキャン(Recently Opened Scans)]リストに追加されます。さらに、プロンプトが再び表示されないようにスキャンの設定にフラグが付きます。このフラグは、スキャンがエクスポートされて、別のスキャンデータベースにインポートされた場合でも保持されます。
- 再テストのスキャンを削除するには、[いいえ(No)]をクリックします。
[スキャンの削除(Deleting Scans)]ウィンドウが表示されます。スキャンが削除されたら、[完了(Done)]をクリックします。

サイトの再スキャン

再スキャン機能を使用すると、開いたスキャンまたは選択したスキャンから、元のスキャン設定が事前に読み込まれたスキャンウィザードに簡単に移行できます。更新されたサイトに対して(元のスキャンで使用されたのと同じ設定を使用して)同一のスキャンを実行して、以前に検出された脆弱性が修復されていることと、別の脆弱性が入り込んでいないことを確認できます。また、一部の設定を微調整して、Web探索または監査を改善することもできます。

スキャンの再利用にも2つのオプションがあります。[贈分の再利用(Reuse Incremental)]と[改善の再利用(Reuse Remediation)]です。詳細については、「["スキャンの再利用"次のページ](#)」を参照してください。

再スキャン機能は、スキャンツールバーの[再スキャン(Rescan)]ボタンと、[スキャンの管理(Manage Scans)]ペインで選択したスキャンに対する[再スキャン(Rescan)]ボタン(およびショートカットメニュー)の2箇所で利用できます。

1. 次のいずれかを実行します。
 - スキャンを開き、[再スキャン(Rescan)]をクリックして[スキャンを再度実行(Scan Again)]を選択します。
 - Fortify WebInspectの開始ページ(Start Page)で、[スキャンの管理(Manage Scans)]をクリックします。その後スキャンを選択して[再スキャン(Rescan)]をクリックします。
2. スキャンウィザードを使用して、元のスキャンに使用した設定を変更することもできます。

メモ: スキャン名はデフォルトで「<original_scan_name>-1」に設定されます。再スキャンの再スキャンを実行する場合、デフォルト名に追加される整数は1ずつインクリメントされます。

3. スキャンウィザードの最後のステップで、[スキャン(Scan)]をクリックします。

スキャンの再利用

スキャンの再利用では、以前のスキャンのデータを新しいスキャンを支援するために使用します。再利用スキャンには、次の2つのスキャンが関係しています。

- **再利用スキャン。** 実行しようとしている新しいスキャンです。
- **ソーススキャンまたはベースラインスキャン。** 再利用スキャンの完了に必要な作業と時間を短縮するためにデータが使用されるスキャンです。

再利用のオプション

スキャンの再利用には、4つのオプションがあります。

- **増分の再利用(Reuse Incremental)** -新しい攻撃露呈部分を見つけます。このスキャンでは通常のWeb探索を実行し、各セッションをベースラインスキャンと比較します。ベースラインスキャンに存在しなかった新しいセッションだけが監査されます。詳細については、「["増分スキャン"次のページ](#)」を参照してください。
- **改善の再利用(Reuse Remediation)** -ベースラインスキャンで検出された脆弱性を探します。このスキャンでは、ベースラインスキャンでフラグが設定されたチェックのみを含むポリシーが作成され、このカスタムポリシーを使用してサイトが再び監査されます。したがって、このスキャンでは、ベースラインスキャンでフラグが設定されたチェックだけが調査されます。

改善スキャンと脆弱性の再テストの違い

改善スキャンでは、ベースラインスキャンでフラグが設定された脆弱性に直接由来する縮小されたポリシーを、ベースラインスキャンで脆弱だったセッションだけでなく、改善スキャンのすべてのセッションに適用します。

たとえば、ベースラインスキャンにおいて、セッションAでクロスサイトスクリプティング(XSS)が検出され、セッションBでは検出されなかったとします。その後、セッションAではXSSが修復されたものの、セッションBではこれが作成されました。脆弱性の再テストのオプションではセッションBの脆弱性を発見できませんが、改善スキャンなら発見できます。したがって改善スキャンでは、以前に検出された脆弱性に関して、すべての既知の攻撃露呈部分が評価されます。

スキャンの再利用に関するガイドライン

スキャンを再利用する場合は、次のガイドラインに従います。

- **再利用スキャンを実行するマシンでベースラインスキャンが利用できる必要があります。**
- **ベースラインスキャンは、再利用スキャンと同じデータベースに存在する必要があります。**

スキャンの再利用

スキャンを再利用するには:

1. 次のいずれかを実行します。
 - 開いているスキャンから [再スキャン(Rescan)] をクリックし、ドロップダウンメニューから目的の再利用オプションを選択します。
 - [スキャンの管理(Manage Scans)] ページでスキャンを右クリックして [再スキャン(Rescan)] をクリックし、必要な再利用オプションをメニューから選択します。
 - [スキャンの管理(Manage Scans)] ページでスキャンを選択して [再利用(Rescan)] をクリックし、必要な再利用オプションをドロップダウンメニューから選択します。
2. 再スキャンのオプションの詳細については、「["再利用のオプション"前のページ](#)」を参照してください。

ヒント: 増分スキャンでは、新しい攻撃露呈部分を検出するために設定を変更することが役に立つ場合があります。ただし、改善スキャンの場合、設定の変更はお勧めしません。

メモ: デフォルトでは、選択した再利用スキャンのタイプがベースラインスキャン名の前に付加され、末尾に-1が追加されます。

3. スキャンウィザードの最後のステップで、[スキャン(Scan)] をクリックします。

次も参照

["増分スキャン"下](#)

増分スキャン

増分スキャンを使用すると、時間の経過とともに変化するWebアプリケーションのエリアを検索および監査すると同時に、すべての検出事項を单一のスキャンに保持できます。このようにするには、増分スキャンを実行し、それらのスキャンをベースラインスキャンにマージする必要があります。増分スキャンとベースラインスキャンの詳細については、「["スキャンの再利用"前のページ](#)」を参照してください。

ベースラインスキャンと増分スキャンのマージ

ベースラインスキャンと増分スキャンを单一のスキャンにマージできます。その後、結合したスキャンの攻撃露呈部分を今後の増分スキャンのために使用できます。

増分スキャンを実行した後、増分スキャンとベースラインスキャンを選択し、右クリックすると、[マージ(Merge)] オプションが表示されます。

重要! 増分スキャンの派生元のベースラインスキャンをクリックして、[マージ(Merge)] オプションが有効になっていることを確認する必要があります。

「マージ(Merge)」をクリックすると、増分スキャンがベースラインスキャンにマージされます。ベースラインスキャンに、2つのスキャンの和集合が含まれるようになります。マージされた後のスキャンは新しいベースラインスキャンになります。増分-マージ-増分-マージを無期限に継続的に実行することで、継続的監査または遅延監査のプロセスを作成できます。詳細については、「["継続的監査または遅延監査による増分スキャン" 下](#)」を参照してください。

スキャンをマージするには:

1. 「スキャンの管理(Manage Scans)」ページで、ベースラインスキャンと増分スキャンを選択します。
2. 右クリックして「マージ(Merge)」を選択します。

スキャンをマージすると、ベースラインスキャンと増分スキャンのIDを含むログエントリがスキャンログに書き込まれます。

継続的監査または遅延監査による増分スキャン

増分スキャンにより、継続的監査または遅延監査を実行することができます。

継続的監査による増分

増分スキャンを使用して、継続的監査のプロセスを導入できます。このプロセスは次のようになります。

1. ベースラインスキャンを作成します。
2. 増分スキャンが必要な場合:
 - a. ベースラインスキャンから増分監査スキャンを作成します。このスキャン中に、新しい露呈部分が監査されます。
 - b. 増分スキャンをベースラインスキャンとマージします。マージされたスキャンが新しいベースラインスキャンになります。詳細については、「["ベースラインスキャンと増分スキャンのマージ" 前のページ](#)」を参照してください。
 - c. 増分スキャンを削除します。
 - d. ステップ2に戻ります。

遅延監査による増分

増分スキャンを使用して、延期監査のプロセスを導入できます。このプロセスは次のようになります。

1. ベースラインスキャンを作成します。
2. 新しい増分スキャンが必要な場合:
 - a. ベースラインスキャンからWeb探索のみの増分スキャンを作成します。
 - b. 増分スキャンをベースラインスキャンとマージします。マージされたスキャンが新しいベースラインスキャンになります。詳細については、「["ベースラインスキャンと増分スキャンのマージ" 前のページ](#)」を参照してください。
 - c. 増分スキャンを削除します。
 - d. 新しい攻撃露呈部分が見つかった場合に、ベースライン監査を再開し、新しい露

呈部分を監査します。

- e. ステップ2に戻ります。

次も参照

["スキャンの再利用" ページ250](#)

マクロの使用

マクロとは、Webサイトにアクセスしてログインするときに発生するイベントを記録したものです。その後、この記録を使用してスキャンを開始するようにFortify WebInspectに指示できます。セッションベースのWeb Macro RecorderツールまたはWeb Macro Recorder with Macro Engine 6.1ツールを使用してログインマクロを記録することも、基本スキャンウィザードまたはガイド付きスキャンウィザードで作成することができます。基本スキャンまたはガイド付きスキャンで作成されたマクロは、どちらのタイプのスキャンでも使用できます。

マクロは2種類あります。

- ログインマクロは、Webサイトにアクセスしてログインするときに発生するイベントをWeb Macro Recorderツールを使用して記録したものです。その後、この記録を使用してスキャンを開始するようにFortify WebInspectに指示できます。
ログインマクロを使用するスキャンの [スキャン設定: 認証 (Scan Settings: Authentication)] で [マクロ検証を有効にする(Enable macro validation)] が選択されている場合、Fortify WebInspectはスキャンの開始時点でログインマクロをテストして、ログインが成功したことを確認します。マクロが無効で、アプリケーションへのログインに失敗した場合、スキャンは停止し、エラーメッセージがスキャンログファイルに書き込まれます。詳細とトラブルシューティングのヒントについては、「["ログインマクロのテスト" ページ510](#)」を参照してください。
- ワークフローマクロは、Webサイト内を移動する場合に発生するHTTPイベントをWeb Macro Recorderツールを使用して記録したものです。Fortify WebInspectは、以前に記録したマクロに含まれているURLのみを監査し、監査中に検出されたハイパーアリンクはたどりません。

マクロに記録されるアクティビティにより、スキャン設定は無効になります。たとえば [除外URL (Excluded URL)] 設定にURLを指定してから、マクロの作成時にそのURLに実際に移動すると、Fortify WebInspectでサイトのWeb探索と監査を行うときに、その除外は無視されます。

メモ: 記録されたマクロにクッキーヘッダが組み込まれている場合、マクロの再生時にそれがFortify WebInspectから送信されることはありません。基本スキャンまたはガイド付きスキャンで記録されたマクロは、どちらのタイプのスキャンでも使用できます。

次も参照

["スキャン設定: 認証" ページ408](#)

["ガイド付きスキャンの実行" ページ117](#)

["基本スキャンの実行 \(Webサイトスキャン\)" ページ178](#)

["ワークフローマクロの選択" 下](#)

["Web Macro Recorderの使用" 下](#)

ワークフローマクロの選択

ワークフロードライブ型のスキャンを実行する場合、Webサイトのナビゲートに使用される、1つ以上のマクロを選択または作成できます。

- **記録(Record)**] - Web Macro Recorderが開き、マクロを作成できます
- **編集(Edit)**] - Web Macro Recorderが開き、選択したマクロがロードされます
- **削除(Remove)**] - 選択したマクロを削除します(ただし、ディスクからは削除されません)
- **インポート(Import)**] - 標準のファイル選択ウィンドウが開き、以前に記録した.webmacroファイルまたはBurp Proxyキャプチャを選択できます。

重要! ログインマクロを、ワークフローマクロまたは起動マクロ、あるいはその両方と組み合わせて使用する場合、すべてのマクロは同じ種類である必要があります。すべてが.webmacroファイルであるか、すべてがBurp Proxyキャプチャであるかのどちらかです。同じスキャンで異なる種類のマクロを使用することはできません。

- **エクスポート(Export)**] - 標準のファイル選択ウィンドウが開き、記録したマクロを保存できます

マクロを選択または記録したら、必要に応じて許可ホストを指定できます。

次も参照

["マクロの使用" 前のページ](#)

Web Macro Recorderの使用

Fortify WebInspectには、2つのバージョンのWeb Macro Recorderツールがあります。

- Web Macro Recorder with Macro Engine 6.1
- セッションベースのWeb Macro Recorder

Web Macro Recorderツールはいくつかの方法で起動でき、ガイド付きスキャンまたは基本スキャンの設定中や、「スタンドアロン」モードとして知られるいずれかのスキャンの外部でも可能です。詳細については、Web Macro Recorderのヘルプまたは『Micro Focus Fortify WebInspect Tools Guide』の「Web Macro Recorder」の章を参照してください。

Web Macro Recorder with Macro Engine 6.1

Fortify WebInspectには、2つのWeb Macro Recorder with Macro Engine 6.1ツールが含まれています。1つはログインマクロ用、もう1つはワークフローマクロ用です。このドキュメントでは、特定のログイン関連およびワークフロー関連のコンテンツを除き、これらの2つのツールは一般に「Web Macro Recorder」と呼ばれます。

Web Macro Recorder with Macro Engine 6.1ツールは、TruClientテクノロジを使って設計されました。イベントベースの機能とFirefoxブラウザのテクノロジを使用してマクロを記録および再生します。

セッションベースのWeb Macro Recorder

Fortify WebInspectにはセッションベースのWeb Macro Recorderツールが含まれています。1つはログインマクロ用、もう1つはワークフローマクロ用です。このドキュメントで、これらの2つのツールは、特定のログイン関連およびワークフロー関連のコンテンツを除き、一般に「セッションベースのWeb Macro Recorder」と呼ばれます。

セッションベースのWeb Macro Recorderは、Internet Explorerブラウザテクノロジ(IEテクノロジとも呼ばれます)を使用してマクロを記録および再生します。

次も参照

["マクロの使用" ページ253](#)

Traffic Monitor (Traffic Viewer)

Fortify WebInspectのナビゲーションペインには、通常、WebサイトまたはWebサービスの階層構造だけが表示され、それに加えて脆弱性が検出されたセッションが表示されます。Traffic MonitorまたはTraffic Viewerを使用すると、Fortify WebInspectによって送信されたすべてのHTTP要求と、Webサーバから受信した関連するHTTP応答を表示および確認できます。

スキャン実行前にTraffic Monitorのログ記録が有効になっていなかった場合、Traffic MonitorとTraffic Viewerは使用できません。この機能は、デフォルト設定で有効にするか(編集(Edit)]> デフォルト設定(Default Settings)]> 設定(Settings)]> 全般(General)]をクリック)、またはスキャンウィザードでスキャンを開始するときに有効にすることができます(詳細なスキャン設定(Detailed Scan Configuration)]ウインドウの 設定(Settings)]で [Traffic Monitorの有効化(Enable Traffic Monitor)]を選択)。

Traffic Viewerのトラフィックセッションデータ

元のTraffic Monitorは、スタンドアロンのTraffic Viewerツールになりました。Traffic Viewerには、元のTraffic MonitorとWebProxyツールの両方の機能が組み込まれています。スタンドアロンのTraffic Viewerのトラフィックセッションファイルの形式は、Traffic Monitorの形式とは異なります。スタンドアロンのTraffic Viewerツールの詳細については、Traffic Viewerツールのオンラインヘルプまたは『Micro Focus Fortify WebInspect Tools Guide』を参照してください。

Traffic Viewerでのトラフィックの表示

Traffic Viewerでトラフィックセッションデータを表示するには:

- 開いているスキャンの [スキャン情報(Scan Info)] パネルで、[Traffic Monitor]をクリックします。

Traffic Viewerツールが開き、ビューにトラフィックセッションデータが表示されます。

次も参照

[" \[スキャン情報\(Scan Info\)\] パネル" ページ79](#)

Server Profiler

Server Profilerを使用してWebサイトの事前テストを行い、Fortify WebInspectの特定の設定を変更する必要があるかどうかを判断します。変更が必要だと思われる場合、Profilerは提案のリストを返します。これらの提案は、受け入れることも拒否することもできます。

たとえば、Server Profilerは、サイトに入るための権限付与が必要であるものの、有効なユーザー名とパスワードが指定されていないことを検出するかもしれません。そのままスキャンを続行して著しく質の低い結果を得るのではなく、Server Profilerのプロンプトに従って、続行する前に必要な情報を設定することができます。

同様に、設定では、Fortify WebInspectが「ファイルが見つからない」の検出を実行しないように指定されていることもあります。このプロセスは、存在しないリソースをクライアントから要求されてもステータス「404 Not Found」を返さないWebサイトで役に立ちます(代わりにステータス「200 OK」が返される場合がありますが、応答にはファイルが見つからないというメッセージが含まれます)。Profilerは、このような手法がターゲットサイトに実装されていると判断した場合、この特徴に対応できるようにFortify WebInspect設定を変更することを推奨します。

Server Profilerは、ガイド付きスキャン中に選択することも、[アプリケーション(Application)]設定で有効にすることもできます。詳細については、「["アプリケーション設定: Server Profiler" ページ450](#)」を参照してください。

Server Profilerの使用

次の2つの方法のいずれかを使用して、Server Profilerを起動します。

ツールとしてのServer Profilerの起動

次のステップに従って、Server Profilerを起動します。

1. Fortify WebInspectの[ツール(Tools)]メニューをクリックし、[ServerProfiler]を選択します。
2. [URL]ボックスで、URLまたはIPアドレスを入力または選択します。
3. (オプション)必要に応じて、[サンプルサイズ(Sample Size)]を変更します。大規模なWebサイトでは、要件を十分に分析するために、デフォルトのセッション数を超えるセッションが必要な場合があります。
4. [分析(Analyze)]をクリックします。
Profilerは、提案の一覧(または変更が不要であるというステートメント)を返します。
5. 提案を拒否するには、関連するチェックボックスのチェックを外します。
6. ユーザ入力が必要な提案については、要求された情報を入力してください。

7. (オプション)変更した設定をファイルに保存するには:
 - a. **設定の保存(Save Settings)**]をクリックします。
 - b. 標準のファイル選択ウィンドウを使用して、設定をSettingsディレクトリのファイルに保存します。

スキャンの開始時にServer Profilerを起動する

スキャンの開始時にProfilerを起動するには、次のステップに従います。

1. 次のいずれかの方法でスキャンを開始します。
 - Fortify WebInspectの **開始ページ(Start Page)**]で、**基本スキャンの開始(Start a Basic Scan)**]をクリックします。
 - **ファイル(File)**] > **新規(New)**] > **基本スキャン(Basic Scan)**]をクリックします。
 - (ツールバーの) **新規(New)**]アイコンでドロップダウン矢印をクリックして、**基本スキャン(Basic Scan)**]を選択します。
 - Fortify WebInspectの **開始ページ(Start Page)**]で、**スケジュールされたスキャンの管理(Manage Scheduled Scans)**]をクリックし、**追加(Add)**]をクリックしてから **基本スキャン(Basic Scan)**]を選択します。
2. スキャンウィザードのステップ4(詳細スキャン設定)で、**プロファイル(Profile)**]をクリックします(**Profilerを自動的に実行する(Run Profiler Automatically)**]が選択されている場合を除く)。
Profilerは、提案の一覧(または変更が不要であるというステートメント)を返します。
3. 提案を拒否するには、関連するチェックボックスのチェックを外します。
4. ユーザ入力が必要な提案については、要求された情報を入力してください。
5. **次へ(Next)**]をクリックします。

結果の検査

このトピックでは、基本スキャンとWebサービススキャンの結果の検査について説明します。

基本スキャン(Basic Scan)

基本スキャンを開始するとすぐに、Fortify WebInspectではWebアプリケーションのスキャンが開始し、各セッションを示すアイコンがナビゲーションペインに表示されます(**サイト(Site)**]ビューまたは**シーケンス(Sequence)**]ビューのいずれかを使用)。また、存在する可能性のある脆弱性もサマリペインの**検出事項(Findings)**]タブで報告されます。詳細については、「["ナビゲーションペイン" ページ67](#)」と「["検出事項\(Findings\)タブ" ページ109](#)」を参照してください。

サマリペインに一覧表示されているURLをクリックすると、関連するセッションがナビゲーションペインで強調表示され、関連する情報が情報ペインに表示されます。詳細については、「["情報ペイン" ページ78](#)」を参照してください。

脆弱なセッションを検出した攻撃が攻撃情報に一覧表示されない場合があります。つまり、ナビゲーションペインで脆弱なセッションを選択してから、[セッション情報(Session Info)]パネルで [攻撃情報(Attack Info)]をクリックしたときに、攻撃情報が情報ペインに表示されません。これは、攻撃情報は通常、攻撃が検出されたセッションではなく、攻撃が作成されたセッションに関連付けられているためです。このような場合は、親セッションを選択してから、[攻撃情報(Attack Info)]をクリックします。詳細については、「["セッション情報\(Session Info\)"パネル](#) ページ91」を参照してください。

1つ以上の脆弱性の操作

サマリペインで1つ以上の脆弱性を右クリックすると、ショートカットメニューを使用して次の操作を実行できます。

- **URLのコピー(Copy URL)** - URLをWindowsのクリップボードにコピーします。
- **選択した項目のコピー(Copy Selected Item(s))** - 選択した項目のテキストをWindowsクリップボードにコピーします。
- **すべての項目のコピー(Copy All Items)** - すべての項目のテキストをWindowsクリップボードにコピーします。
- **エクスポート(Export)** - 項目をCSVファイルにコピーします。
- **ブラウザで表示(View in Browser)** - 1つの脆弱性が選択されている場合に使用できます。ブラウザでHTTP応答をレンダリングします。
- **現在の値によるフィルタ(Filter by Current Value)** - 1つの脆弱性が選択されている場合に使用できます。選択した基準を満たす脆弱性だけを表示するよう制限します。たとえば、[メソッド(Method)]列で「Post」を右クリックして、**現在の値によるフィルタ(Filter by Current Value)**を選択すると、Postメソッドを使用したHTTP要求を送信して検出された脆弱性だけがリストに表示されます。

メモ: フィルタ基準は、サマリペインの右上隅のコンボボックスに表示されます。または、このコンボボックスを使用してフィルタ基準を手動で入力または選択することもできます。追加の詳細および構文ルールについては、「["サマリペインのフィルタとグループの使用" ページ262](#)」を参照してください。

- **重大度の変更(Change Severity)** - 重大度レベルを変更できます。
- **脆弱性の編集** - 1つの脆弱性が選択されている場合に使用できます。脆弱性の編集(Edit Vulnerabilities)ダイアログが表示され、脆弱性のさまざまな特性を変更できます。詳細については、「["脆弱性の編集" ページ269](#)」を参照してください。
- **脆弱性のロールアップ(Rollup Vulnerabilities)** - 複数の脆弱性が選択されている場合に使用できます。選択した脆弱性を、Fortify WebInspect、Fortify WebInspect Enterprise、およびレポート内で「[Rollup]」というタグの接頭部を持つ单一インスタンスにロールアップできます。詳細については、「["脆弱性のロールアップ" ページ272](#)」を参照してください。

メモ: ロールアップされた脆弱性を選択した場合、このメニューオプションは **脆弱性のロールアップを元に戻す(Undo Rollup Vulnerabilities)**になります。

- **再テスト(Retest)** - 選択した1つ以上の検出事項、すべての検出事項、または特定の重大度の検出事項の再テストを実行します。詳細については、「["脆弱性の再テスト" ページ](#)

[244](#)」を参照してください。

- マーク付けする(Mark as) - 脆弱性に誤検出(メモを追加可能)または無視のフラグを設定します。どちらの場合も、その脆弱性はリストから削除されます。[スキャン情報(Scan Info)]パネルで [誤検出(False Positives)]を選択すると、すべての誤検出のリストを表示できます。[スキャン情報(Scan Info)]パネルで [ダッシュボード(Dashboard)]を選択し、統計情報列で削除済み項目のハイパーアリンク付きの数値をクリックすると、誤検出された脆弱性と無視された脆弱性のリストを表示できます。

メモ: 「誤検出」および「無視」の脆弱性を回復できます。詳細については、「["削除された項目の回復" ページ278](#)」を参照してください。

- 送信(Send to) - 脆弱性を欠陥に変換し、Micro Focus Application Lifecycle Management(ALM)データベースに追加します。
- 場所の削除(Remove Location) - 選択したセッションをナビゲーションペイン([サイト(Site)]ビューと [シーケンス(Sequence)]ビューの両方)から削除し、関連する脆弱性もすべて削除します。

メモ: 削除された場所(セッション)およびそれに関連する脆弱性を回復できます。詳細については、「["削除された項目の回復" ページ278](#)」を参照してください。

- Web探索(Crawl) - 1つの脆弱性が選択されている場合に使用できます。選択したURLのWeb探索を再実行します。
- ツール - 1つの脆弱性が選択されている場合に使用できます。使用可能なツールのサブメニューを示します。
- 添付ファイル(Attachments) - 1つの脆弱性が選択されている場合に使用できます。選択したセッションに関連するメモの作成、フォローアップのためのセッションへのフラグ付け、脆弱性のメモの追加、脆弱性スクリーンショットの追加を行うことができます。

グループの操作

グループを右クリックすると、ショートカットメニューで次の操作を実行できます。

- すべてのグループの縮小/展開(Collapse/Expand All Groups)
- グループの縮小/展開(Collapse/Expand Group)
- URLのコピー(Copy URL)
- 選択した項目のコピー(Copy Selected Item(s))
- すべての項目のコピー(Copy All Items)
- エクスポート
- 重大度の変更(Change Severity)
- 脆弱性のロールアップ(Rollup Vulnerabilities)
- マーク付けする(Mark as)
- 送信(Send to)
- 場所の削除(Remove Location)

重大度について

サマリペインに一覧表示されている脆弱性の相対的な重大度は、次の表で説明するよう に、関連付けられたアイコンによって識別されます。

| アイコン | 説明 |
|---|---|
|  重大 | 攻撃者がサーバ上でコマンドを実行したり、個人情報を取得および変更したりできる可能性がある脆弱性。 |
|  高 | 一般に、ソースコード、Webルート外のファイル、および機密性の高いエラーメッセージの表示が可能になります。 |
|  中 | 機密性が高い可能性のあるHTML以外のエラーまたは問題を示します。 |
|  低 | 注目すべき問題、またはより高いレベルの問題になる可能性のある問題。 |
|  情報 | サイト内の興味深い点、または特定のアプリケーションやWebサーバの検出。 |
|  ベストプラクティス | Web開発で一般的に認められるベストプラクティスに関する問題で、サイト品質とサイト開発のセキュリティに関する全体的なプラクティス(またはその欠如)を示す可能性があります。 |

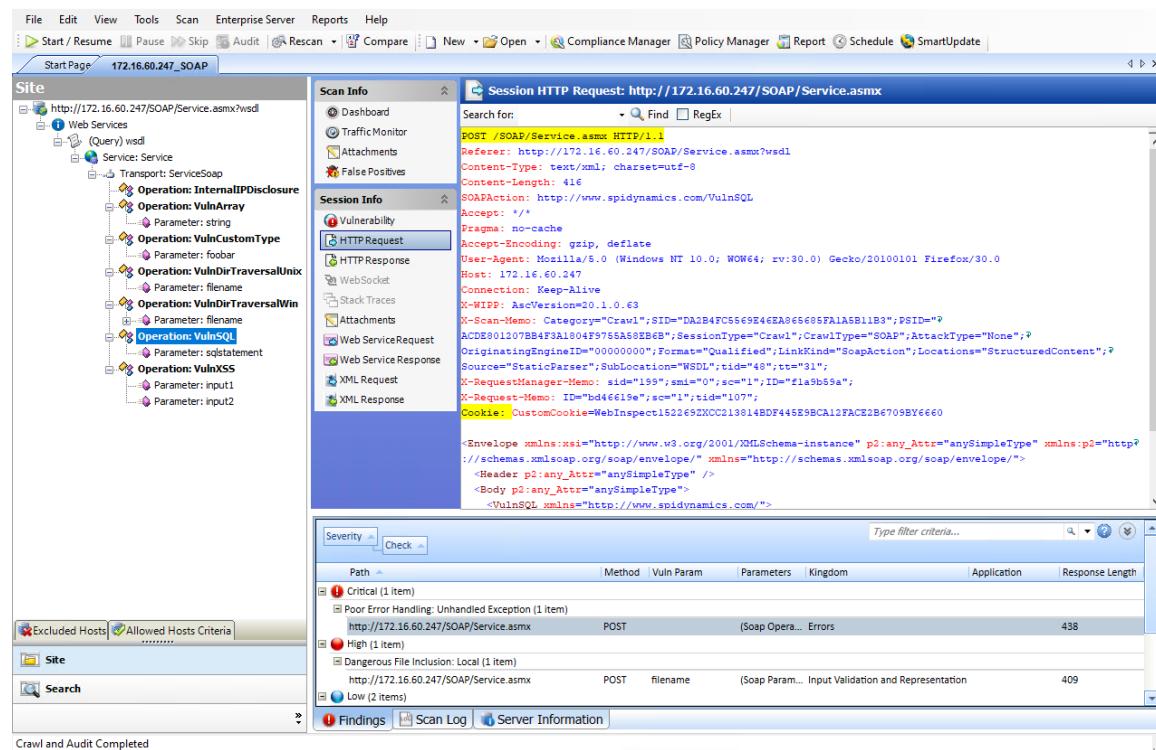
ナビゲーションペインでの操作

ナビゲーションペインでオブジェクトまたはセッションを選択し、[セッション情報(Session Info)] パネルで使用可能なオプションを使用してセッションを調査することもできます。詳細については、「["ナビゲーションペイン" ページ67](#)」および「["セッション情報\(Session Info\)"\] パネル" ページ91](#)」を参照してください。

Webサービスススキャン

Webサービスは、(ユーザではなく)他のアプリケーションと通信し、情報の要求に応答するプログラムです。ほとんどのWebサービスは、SOAP (Simple Object Access Protocol)を使用して、Webサービスと、情報要求を開始したクライアントWebアプリケーションとの間でXMLデータを送信します。XMLは、構造化されたデータの記述と格納を行うフレームワークを提供します。クライアントWebアプリケーションは、返されたデータをすぐに理解し、その情報をエンドユーザに表示できます。

Webサービススキャンのイメージ



WebサービスにアクセスするクライアントWebアプリケーションは、WSDL (Web Services Definition Language)ドキュメントを受け取り、サービスとの通信方法を理解します。WSDLドキュメントには、Webサービスに含まれるプロシージャ、それらのプロシージャに必要なパラメータ、およびクライアントWebアプリケーションが受け取る戻り情報のタイプが記述されています。

ナビゲーションペイン、またはサマリペインの [検出事項(Findings)] タブでセッションオブジェクトを選択した後、[セッション情報(Session Info)] パネルからオプションを選択できます。詳細については、「"ナビゲーションペイン" ページ67」、「" 検出事項(Findings)]タブ" ページ109」、および「" [セッション情報(Session Info)] パネル" ページ91」を参照してください。

次も参照

["再テストと再スキャン" ページ244](#)

["Webサービスの監査" ページ266](#)

["脆弱性の編集" ページ269](#)

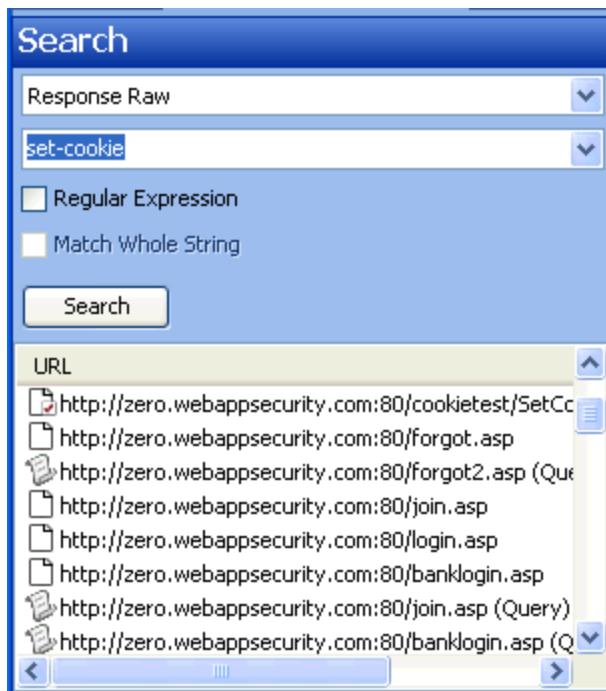
["WebInspectユーザインターフェース" ページ51](#)

["削除された項目の回復" ページ278](#)

[検索(Search)] ビュー

[検索(Search)] ビューでは、すべてのセッションでさまざまなHTTPメッセージコンポーネントを検索できます。たとえば、ドロップダウンから [応答の生データ(Response Raw)] を選択し、

検索文字列として「**set-cookie**」を指定すると、HTTP応答の生データに「set-cookie」コマンドが含まれるすべてのセッションが一覧表示されます。



「検索(Search)」ビューを使用するには:

1. ナビゲーションペインで、「**検索(Search)**」をクリックします(ペインの下部)。詳細については、「["ナビゲーションペイン" ページ67](#)」を参照してください。
すべてのボタンが表示されてはいない場合は、ボタンリストの下部にある「**ボタンの設定** (Configure Buttons)」ドロップダウンリストをクリックし、「**他のボタンを表示** (Show More Buttons)」を選択します。
2. 一番上のリストから、検索するエリアを選択します。
3. コンボボックスで、検索する文字列を入力または選択します。
4. 文字列が正規表現を表している場合は、「**正規表現(Regular Expression)**」チェックボックスをオンにします。詳細については、「["正規表現" ページ323](#)」を参照してください。
5. 検索文字列と完全に一致する文字列全体をHTTPメッセージ内で検索するには、「**文字列全体を照合する(Match Whole String)**」チェックボックスをオンにします。完全一致では、大文字と小文字は区別されません。
このオプションは、特定の検索ターゲットには使用できません。
6. 「**検索(Search)**」をクリックします。

次も参照

["WebInspectユーザインターフェース" ページ51](#)

サマリペインのフィルタとグループの使用

このトピックでは、サマリペインでフィルタおよびグループを使用する方法について説明します。

フィルタの使用

指定した基準に一致する項目のサブセットを表示するには、次の2つの方法のいずれかを使用します。

- ペインの右上隅にあるコンボボックスを使用してフィルタ基準を入力します。

メモ: フィルタ基準ボックスをクリックして $<CTRL> + <Space>$ を押すと、使用可能なすべてのフィルタ基準のpopupアップリストが表示されます。次に、その基準の値を入力します。

- 任意の列の値を右クリックし、ショートカットメニューから「現在の値でフィルタ(Filter by Current Value)」を選択します。

このフィルタ機能は、サマリペインの「スキャンログ(Scan Log)」を除くすべてのタブで使用できます。

フィルタを使用しない場合

次の例は、「検出事項(Findings)」タブで項目にフィルタが適用されていない状態を示しています。

フィルタが適用されていないサマリペインのイメージ

| Severity | Path | Method | Vuln Param | Parameters | Kingdom | Application | Response Length |
|---|-----------------|---------------------------|----------------|-------------------------------------|---------|-------------|-----------------|
| 1 Critical (5 items) | | | | | | | |
| Cross-Site Scripting: Reflected (3 items) | | | | | | | |
| http://zero.webappsecurity.com/faq.html | GET | question | (Query)ques... | Input Validation and Representation | | 7794 | |
| http://zero.webappsecurity.com/search.html | GET | searchTerm | (Query)sear... | Input Validation and Representation | | 7754 | |
| http://zero.webappsecurity.com/sendFeedback.html | POST | name | (Post)name=... | Input Validation and Representation | | 6689 | |
| Poor Error Handling: Unhandled Exception (1 item) | | | | | | | |
| http://zero.webappsecurity.com/account/ | GET | - | Errors | | | 15204 | |
| Findings | Scan Log | Server Information | | | | | |

「Method:Get」でフィルタされている場合

次の例は、フィルタ基準ボックスに「Method:Get」と入力した後に表示された内容です。

フィルタが適用されているサマリペインのイメージ

| Severity | Path | Method | Vuln Param | Parameters | Kingdom | Application | Response Length |
|--|-----------------|---------------------------|----------------|-------------------------------------|---------|-------------|-----------------|
| 1 Critical (4 items) | | | | | | | |
| Cross-Site Scripting: Reflected (2 items) | | | | | | | |
| http://zero.webappsecurity.com/faq.html | GET | question | (Query)ques... | Input Validation and Representation | | 7794 | |
| http://zero.webappsecurity.com/search.html | GET | searchTerm | (Query)sear... | Input Validation and Representation | | 7754 | |
| Poor Error Handling: Unhandled Exception (1 item) | | | | | | | |
| http://zero.webappsecurity.com/account/ | GET | - | Errors | | | 15204 | |
| Privacy Violation: Social Security Number (1 item) | | | | | | | |
| Findings | Scan Log | Server Information | | | | | |

コンボボックスにフィルタ基準(Method:Get)が表示されており、ここに赤いXも表示されていることに注意してください。このXをクリックするとフィルタが削除され、フィルタ適用前のリストが再び表示されます。

複数のフィルタの指定

フィルタ基準コンボボックスに基準を入力するときに複数のフィルタを指定するには、フィルタをカンマで区切ります(「Parameter:noteid, Method:GET」など)。

フィルタ基準

次の識別子を入力できます。

- application -脆弱性が検出されたアプリケーションまたはフレームワーク
- check -チェック名
- checkid - SecureBaseからのチェックID番号
- cookienamerp - HTTP応答のクッキーの名前
- cookienamerq - HTTP要求のクッキーの名前
- cookievaluerp - HTTP応答のクッキーの値
- cookievaluerq - HTTP要求のクッキーの値
- cwe - CWE (Common Weakness Enumeration) ID
- duplicates - Fortify WebInspect Agentにより検出された重複
- filerq - HTTP要求のファイル名と拡張子
- headernamerp - HTTP応答ヘッダ名
- headernamerq - HTTP要求ヘッダ名
- headervaluerp - HTTP応答ヘッダ値
- headervaluerq - HTTP要求ヘッダ値
- kingdom - 7つの有害な界の値(詳細については、「["アプリケーション設定:全般" ページ 442](#)」を参照)。
- location -リソースを識別するパスとパラメータ
- manual -手動で追加された場所(構文はmanual:Trueまたはmanual:False)
- method - HTTPメソッド(GET、POST)
- methodrq - HTTP要求で指定されたメソッド
- parameters - HTTP要求で指定されたパラメータ
- path -リソースを識別するパス(パラメータなし)
- pendstatus -スキャンがFortify Software Security Centerに発行される場合のステータス
- rawrp -生のHTTP応答
- rawrq -生のHTTP要求
- responselength -脆弱なセッションの応答サイズ(バイト単位)
- reteststatus -再テストステータスの値(値のリストについては、「["脆弱性の再テスト" ページ 244](#)」を参照)。

- sessiondataid -セッションデータ識別子(ナビゲーションペインでセッションを右クリックし、観在のセッションでフィルタ(Filter by Current Session)]を選択します)
- severity -脆弱性に割り当てられた重大度(critical、high、medium、low)
- stack - Fortify WebInspect Agentから返されるスタックトレース(構文はstack:Trueまたはstack:False)
- statuscode - HTTPステータスコード
- typeq -要求のタイプ: query、post、またはSOAP
- vparam -脆弱性パラメータ

グループの使用

列ヘッダに基づいて、項目をカテゴリにグループ化できます。これを行うには、ヘッダをドラッグして、ペイン上部のグループエリアにドロップするだけです。

次の画像の検出事項は、重大度別にグループ化され、次にチェック名別にグループ化されています。

グループを使用したサマリペインのイメージ

列ヘッダを右クリックすると、グループ化とフィルタリングに関連する次のショートカットメニュー項目が表示されます。

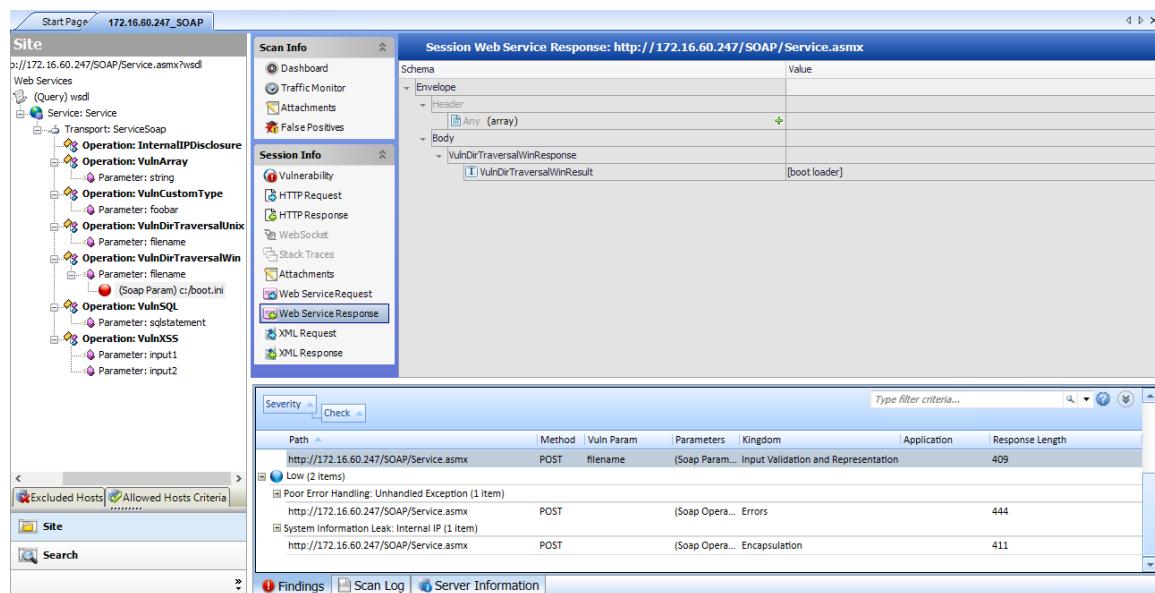
- [フィールドでグループ化(Group by Field)]-選択したフィールドに基づいて脆弱性をグループ化します。
- [ボックスでグループ化(Group by Box)]-列ヘッダに基づいてグループを編成できる「グループ基準(Group By)」エリアが表示されます。
- [列(Column)]-表示する列を選択できます。
- [デフォルトビューとして保存(Save as Default View)]-現在のグループ化方法をすべてのスキャンのデフォルトとして保存します。
- [デフォルトビューにリセット(Reset Default View)]-グループ化方法を、作成したデフォルトビューに戻します。
- [出荷時設定にリセット(Reset Factory Settings)]-グループ化方法を元のビューに戻します(重大度(Severity)> チェック(Check))。

Webサービスの監査

Webサービスは、(ユーザではなく)他のアプリケーションと通信し、情報の要求に応答するプログラムです。ほとんどのWebサービスは、SOAP (Simple Object Access Protocol)を使用して、Webサービスと、情報要求を開始したクライアントWebアプリケーションとの間でXMLデータを送信します。Webページの表示方法のみを記述するHTMLとは異なり、XMLは構造化されたデータを記述して、それを含めるためのフレームワークを提供します。クライアントWebアプリケーションは、返されたデータをすぐに理解し、その情報をエンドユーザに表示できます。

WebサービスにアクセスするクライアントWebアプリケーションは、WSDL (Web Services Description Language)ドキュメントを受け取り、サービスとの通信方法を理解します。WSDLドキュメントには、Webサービスに含まれるプログラミングされたプロシージャ、これらのプロシージャに必要なパラメータ、およびクライアントWebアプリケーションが受け取る戻り情報のタイプが記述されています。

Webサービススキャンのイメージ



「セッション情報(Session Info)」パネルで使用可能なオプション

次の表に、「セッション情報(Session Info)」パネルで使用可能なオプションを示します。

| オプション | 定義 |
|------------------------|--|
| 脆弱性 (Vulnerability) | ナビゲーションペインで選択されているセッションの脆弱性情報を表示します。詳細については、「 "ナビゲーションペイン" ページ67 」を参照してください。 |

| オプション | 定義 |
|----------------------------|--|
| HTTP要求 (HTTP Request) | Fortify WebInspectから、スキャン対象のサイトをホストするサーバに送信された生HTTP要求を表示します。 |
| HTTP応答 (HTTP Response) | Fortify WebInspectの要求に対するサーバの生HTTP応答を表示します。 メモ: Flash (.swf)ファイルを選択した場合、Fortify WebInspectはバイナリデータの代わりにHTMLを表示します。これにより、Fortify WebInspectは読み取り可能なフォーマットでリンクを表示できます。 |
| スタックトレース (Stack Traces) | この機能は、Fortify WebInspect Agentがターゲットサーバにインストールされ、実行されているときにこのエージェントをサポートするように設計されています。特定のチェック(SQLインジェクション、コマンド実行、クロスサイトスクリプティングなど)の場合、Fortify WebInspect AgentはFortify WebInspect HTTP要求を傍受し、ターゲットモジュールでランタイム分析を実行します。この分析によって脆弱性が存在することが確認されると、Fortify WebInspect AgentはHTTP応答にスタックトレースを追加します。開発者は、このスタックトレースを分析して、改善が必要なエリアを調査できます。 |
| 添付ファイル (Attachments) | 選択されているセッションに関連付けられているすべてのメモ、フラグ、およびスクリーンショットを表示します。 添付ファイルを作成するには、次のいずれかを実行します。 <ul style="list-style-type: none"> ナビゲーションペインで操作または脆弱性を右クリックし、ショートカットメニューから 添付ファイル(Attachments) を選択します。 サマリペインの 検出事項(Findings) タブでURLを右クリックし、ショートカットメニューから 添付ファイル(Attachments) を選択します。詳細については、「"サマリペイン" ページ109」を参照してください。 ナビゲーションペインで操作または脆弱性を選択し、セッション情報(Session Info) パネルから 添付ファイル(Attachments) を選択し、(情報ペインの) 追加(Add) メニューをクリックします。 Micro Focus Application Lifecycle Management (ALM)に問題を送信するたびに、Fortify WebInspectによってメモがセッション情報に自動的に追加されます。 |
| Webサービス要求 (Web) | 要求のSOAPエンベロープ、ヘッダ、および本文要素を、開かれたビューで表示します。 |

| オプション | 定義 |
|---------------------------------|--|
| Service Request) | |
| Webサービス応答(Web Service Response) | 応答のSOAPエンvelope、ヘッダ、および本文要素を、開かれたビューで表示します。 |
| XML要求(XML Request) | 要求に埋め込まれている関連XMLスキーマが表示されます(WebサービススキャンでWSDLオブジェクトを選択した場合に使用可能)。 |
| XML応答(XML Response) | 応答に埋め込まれている関連XMLスキーマが表示されます(WebサービススキャンでWSDLオブジェクトを選択した場合に使用可能)。 |

Webサービス脆弱性スキャンの実行方法の詳細については、「["APIまたはWebサービススキャンの実行" ページ169](#)」を参照してください。

脆弱性スクリーンショットの追加と表示

脆弱性スクリーンショットを追加するには:

- 次のいずれかを実行して脆弱性を選択します。
 - サマリペインの [検出事項(Findings)] タブで、脆弱なURLを右クリックします。詳細については、「["検出事項\(Findings\)"\]タブ" ページ109](#)」を参照してください。
 - ナビゲーションペインで、脆弱なセッションまたはURLを右クリックします。詳細については、「["ナビゲーションペイン" ページ67](#)」を参照してください。
- ショートカットメニューで、[添付ファイル(Attachments)]> [脆弱性スクリーンショットの追加(Add Vulnerability Screenshot)]をクリックします。

メモ: もう1つの方法として、脆弱性を選択し、[セッション情報(Session Info)] パネルで [添付ファイル(Attachments)] をクリックしてから、(情報表示エリアの) [追加(Add)] メニューでコマンドを選択する方法があります。詳細については、「["情報ペイン" ページ78](#)」を参照してください。

- 複数の脆弱性があるセッションを選択した場合は、1つ以上の脆弱性の横にあるチェックボックスをオンにします。
- [名前(Name)] ボックスにスクリーンショットの名前(最大40文字)を入力します。
- 次のいずれかの方法でイメージファイルを選択します。
 - 参照ボタン  をクリックし、標準のファイル選択ウィンドウでファイルを選択します。
 - [クリップボードからコピー(Copy from Clipboard)] をクリックして、Windowsクリップボードの内容を保存します。

メモ: 複数の脆弱性を選択した場合でも、指定できるイメージファイルは1つだけです。

6. (オプション)選択した脆弱性スクリーンショットに関連するメモを入力します。
7. [OK]をクリックします。

選択したセッションのスクリーンショットの表示

[セッション情報(Session Info)]パネルの [添付ファイル(Attachments)]をクリックすると、選択したセッションのメモ、フラグ、およびスクリーンショットを表示できます。

すべてのセッションのスクリーンショットの表示

[スキャン情報(Scan Info)]パネルの [添付ファイル(Attachments)]をクリックすると、すべてのセッションのメモ、フラグ、およびスクリーンショットを表示できます。

次も参照

["脆弱性のメモ" ページ277](#)

["フォローアップのためのセッションへのフラグ設定" ページ275](#)

["スキャンメモ" ページ276](#)

脆弱性の編集

Fortify WebInspectがアプリケーションの脆弱性を評価した後、以下のようなさまざまな理由で結果を編集および保存できます。

- セキュリティ-HTTP要求**または応答にパスワード、アカウント番号、またはその他の機密データが含まれている場合は、スキャン結果を組織内の他のユーザが利用できるようにする前に、この情報を削除または変更できます。
- 訂正**-Fortify WebInspectが「誤検出」を報告する場合があります。これは、Fortify WebInspectが脆弱性の可能性を示す兆候を検出したが、開発者がさらに調査することにより、問題が実際には存在しないと判断された場合に発生します。セッションから脆弱性を削除するか、セッション全体を削除できます。または、その報告を誤検出として指定することもできます。([サイト(Site)]または [シーケンス(Sequence)]ビューでセッションを右クリックし、**誤検出としてマーク(Mark As False Positive)**]を選択)。

- 重大度の変更** - Fortify WebInspectの脆弱性のランク付けが適切ではないと思われる場合は、次のスケールを使用して別のレベルを割り当てることができます。

| 範囲 | 重大度 |
|----------|-----|
| 0 - 9 | 通常 |
| 10 | 情報 |
| 11 - 25 | 低 |
| 26 - 50 | 中 |
| 51 - 75 | 高 |
| 76 - 100 | 重大 |

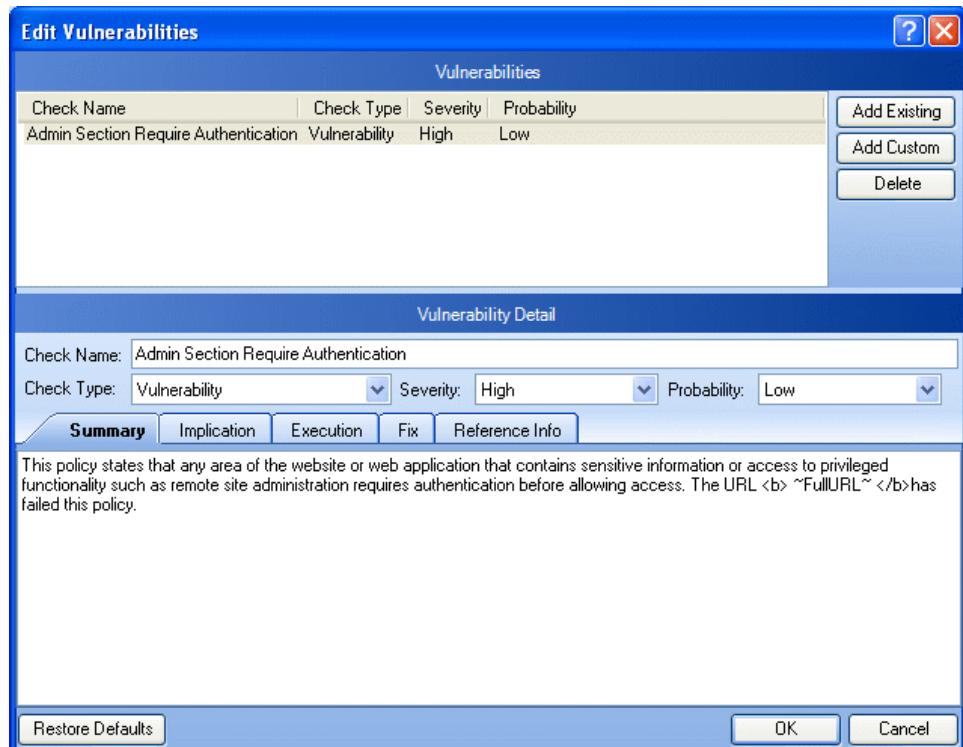
- レコードの保持** - 各々の脆弱性に関連付けられたレポートフィールド(サマリ(Summary)、実行(Execution)、推奨(Recommendation)、実装(Implementation)、修復(Fixes)、および参照(References))を変更できます。たとえば、実際に問題を修復した方法を説明するパラグラフを「修復(Fixes)」セクションに追加できます。
- 拡張** - 新しい脆弱性を検出した場合、その脆弱性を定義して、カスタム脆弱性としてセッションに追加できます。

脆弱なセッションの編集

脆弱なセッションを編集するには:

- 次のいずれかを実行してセッションを選択します。
 - サマリペインの「検出事項(Findings)」タブで、脆弱なURLを右クリックします。または、ナビゲーションペインで、セッションまたはURLを右クリックします。
- ショートカットメニューから「脆弱性の編集(Edit Vulnerability)」を選択します。

脆弱性の編集(Edit Vulnerabilities)】ウィンドウが開きます。



3. セッションに複数の脆弱性が含まれる場合は、1つの脆弱性を選択します。
4. 既存の脆弱性(つまり、データベースに存在する脆弱性)をセッションに追加するには、**既存のものを追加(Add Existing)**】をクリックします。
 - a. **既存の脆弱性の追加(Add Existing Vulnerability)**】ウィンドウで、脆弱性名の一部、または完全な脆弱性ID番号またはタイプを入力します。

メモ: *文字と%文字は、ワイルドカードとして使用でき、相互に交換可能です。ただし、ワイルドカードは、文字列の先頭、末尾、または先頭と末尾でのみ使用できます。文字列の中に含まれている場合(「mic*soft」など)、これらの文字はワイルドカードとして機能しません。
 - b. **検索(Search)**】をクリックします。
 - c. 検索によって返される脆弱性を1つ以上選択します。
 - d. **OK】**をクリックします。
5. カスタム脆弱性を追加するには、**カスタムの追加(Add Custom)**】をクリックします。次に、ステップ7の説明に従って脆弱性を編集できます。
6. 選択したセッションから脆弱性を削除するには、**削除(Delete)**】をクリックします。
7. 脆弱性を変更するには、**脆弱性の詳細(Vulnerability Detail)**】セクションから別のオプションを選択します。[サマリ(Summary)]、[意味(Implication)]、[実行(Execution)]、[修復(Fix)]、および[参照情報(Reference Info)]の各タブに表示される説明を変更することもできます。
8. **OK】**をクリックして変更を保存します。

脆弱性のロールアップ

一部のサイトには、サイト全体に特有の脆弱性のクラスが含まれています。たとえば、入力の検証がないために、サイト全体にわたり、すべてのパラメータに対するすべてのPOSTおよびGETメソッドに、クロスサイトスクリプティングの脆弱性が存在する場合があります。これは、サマリペインの「検出事項(Findings)」タブにクロスサイトスクリプティングの脆弱性が多数一覧表示されるという意味です。Fortify WebInspect、Fortify WebInspect Enterprise、およびレポートでは、開発チームの負担を軽減するため、このような脆弱性をロールアップして、先頭に「[Rollup]」というタグを付けた単一のインスタンスにできます。

ロールアップされた脆弱性の挙動

複数の脆弱性を選択してロールアップ機能を使用すると、最初に選択した脆弱性を除くすべての脆弱性は「無視」としてマーク付けされます。最初に選択された脆弱性はそのまま表示されて、ロールアップを代表します。選択した残りの脆弱性は「無視」としてマーク付けされますが、削除された項目の回復(Recover Deleted Items)】ウィンドウに無視された脆弱性として表示されることはありません。

注意! 脆弱性をロールアップすることは、それらの根本原因が同じであり、その根本原因を修復すればロールアップされたすべての脆弱性が修復されることを意味しています。以降のスキャンでは、ロールアップされた脆弱性が検出された場合、自動的に無視されます。ロールアップされた脆弱性の中に根本原因の異なるものがあっても、同様に無視されてしまいます。

ロールアップのガイドライン

脆弱性のロールアップには、次のガイドラインが適用されます。

- 脆弱性のロールアップを含むスキャンは、再スキャンと一緒に再テストができます。
- 一括再テストでは、表示されている脆弱性のみが再テストされます。残りの脆弱性は無視され、再テスト時にロールアップとして表示されません。
- ロールアップはスキャンに対してローカルであり、他のスキャンには伝播されません。
- ロールアップ機能は、ロールアップされていない複数の脆弱性を選択した場合にのみ使用できます。現在ロールアップされている脆弱性が誤って選択された場合、ショートカットメニューに「脆弱性のロールアップ(Rollup Vulnerability)」オプションは表示されません。
- ロールアップの取り消しは、現在ロールアップされている脆弱性を1つだけ選択した場合にのみ行うことができます。

脆弱性のロールアップ

脆弱性をロールアップするには:

1. サマリペインの [検出事項(Findings)] タブで、ロールアップする脆弱性を複数選択します。
2. 右クリックして、ショートカットメニューから [脆弱性のロールアップ(Rollup Vulnerabilities)] を選択します。

次の警告が表示されます。

これらの脆弱性をロールアップすることは、それらの根本原因が同じであり、その根本原因を修復すればロールアップされたすべての脆弱性が修復されることを意味しています。以降のスキャンでは、ロールアップされた脆弱性が検出された場合、自動的に無視されます。これらの脆弱性の中に根本原因の異なるものがあっても、同様に無視されてしまいます。続行しますか? (Rolling up these vulnerabilities indicates that they share the same root cause, and that fixing the root cause will fix all rolled up vulnerabilities. Future scans will automatically ignore rolled up vulnerabilities if found. If any of these vulnerabilities do not share the same root cause, they will still be ignored. Do you wish to continue?)

3. 次のいずれかを実行します。

- [OK]をクリックして、脆弱性をロールアップします。
- [キャンセル(Cancel)]をクリックして、脆弱性をそのままにします。

[OK]をクリックすると、選択した脆弱性が1つのインスタンスにロールアップされ、次に示すように、チェック名の前に「[Rollup]」というタグが付きます。さらに、同じ脆弱性の影響を受ける、ロールアップされたURLの詳細を含むメモが、[セッション情報(Session Info)] パネルの添付ファイルに追加されます。詳細については、「["選択したセッションのメモの表示" ページ277](#)」を参照してください。

| Severity | Check | Path | Method | Vuln Param | Parameters | Kingdom | Application | Response |
|---|--|--|--------|-----------------|-------------------------------------|-------------------------------------|-------------|----------|
| Critical (71 items) | | | | | | | | |
| ! | [Rollup] Cross-Site Scripting: Reflected (1 item) | http://zero.webappsecurity.com/acctxferconfirm.asp | POST | toAcct | (Post)fromA... | Input Validation and Representation | | 2362 |
| Access Control: Unprotected File (2 items) | | | | | | | | |
| | http://zero.webappsecurity.com/cgi.zip | GET | - | | Environment | | 51 | |
| | http://zero.webappsecurity.com/global.asa.bak | GET | - | | Environment | Microsoft IIS | 241 | |
| Cross-Site Scripting: Reflected (60 items) | | | | | | | | |
| | http://zero.webappsecurity.com/banklogin.asp | GET | err | (Query)err=l... | Input Validation and Representation | | 5008 | |
| | http://zero.webappsecurity.com/banklogin.asp | GET | err | (Query)err=... | Input Validation and Representation | ASP.NET | 5000 | |
| | http://zero.webappsecurity.com/cookieetest/ShowCook... | GET | - | | Input Validation and Representation | | 414 | |
| | http://zero.webappsecurity.com/cookieetest/ShowCook... | GET | - | | Input Validation and Representation | | 303 | |
| | http://zero.webappsecurity.com/cookieetest/ShowCook... | GET | - | | Input Validation and Representation | | 415 | |

ロールアップの取り消し

ロールアップ機能は、元に戻すことが可能です。ロールアップを取り消すには:

1. サマリペインの [検出事項(Findings)] タブで、ロールアップされた脆弱性を右クリックします。
2. [脆弱性のロールアップを取り消す(Undo Rollup Vulnerabilities)] を選択します。

ロールアップが元に戻され、脆弱性が [検出事項(Findings)] タブに表示されます。さらに、ロールアップされた脆弱性の詳細を含むメモが [セッション情報(Session info)] パネルの添付ファイルから削除されます。

メモ: Fortify Software Security Centerに発行されたスキャンのロールアップを取り消す場合、[セッション情報(Session Info)] パネルの添付ファイルに追加されたロールアップの詳細を含むメモは Fortify WebInspect から一時的に削除されますが、Fortify Software Security Centerとの同期後に再び表示されます。

次も参照

["検出事項\(Findings\)"\] タブ" ページ109](#)

誤検出としてマーク

セッションに脆弱性が含まれていると Fortify WebInspect が誤って判断したと思われる場合は、そのセッションからその脆弱性を削除できます。

誤検出としてマークするには:

1. 1つ以上のURLに関連付けられているチェックボックスをオンにします。
2. (オプション)コメントを入力します。
3. (オプション)誤検出と思える項目が見つかったことを Fortify カスタマサポート担当者に通知するには、[Micro Focus サポートに送信する(Send to Micro Focus Support)] を選択します。

このオプションを選択すると、[データアップロードのプレビュー(Preview Data Upload)] を選択することもできます。これをを利用して、Fortify カスタマサポートに送信するデータの内容を表示できます。その際、データを Windows クリップボードにコピーしたり、アップロードをキャンセルしたり、([OK] をクリックして) 続行させたりすることができます。

4. [OK] をクリックします。

ヒント: 誤検出としてマークされたすべてのセッションの一覧を表示するには、[スキャン情報(Scan Info)] パネルから [誤検出(False Positives)] を選択します。このオプションは、実際に脆弱性を誤検出として宣言するまでは表示されません。

脆弱性としてマーク

検出された脆弱性を、誰かが誤って誤検出として再分類したと思われる場合は、その脆弱性を元のセッションに復元できます。

- 1つ以上のURLに関連付けられているチェックボックスをオンにします。
- (オプション)コメントを入力します。
- 「OK」をクリックします。

フォローアップのためのセッションへのフラグ設定

フォローアップのためにセッションにフラグを付けるには:

- 次のいずれかを実行してセッションを選択します。
 - サマリペインの「検出事項(Findings)」タブで、脆弱なURLを右クリックします。
 - ナビゲーションペインで、セッションまたはURLを右クリックします。
- ショートカットメニューで、「添付ファイル(Attachments)」>「フォローアップのためのセッションへのフラグ設定(Flag Session for Follow Up)」をクリックします。

メモ: フォローアップのためにセッションにフラグを設定するもう1つの方法として、脆弱性またはセッションを選択し、「セッション情報(Session Info)」パネルで「添付ファイル(Attachments)」をクリックしてから、(情報表示エリアの)「追加(Add)」メニューをクリックする方法があります。

- 選択したセッションに関連するメモを入力します。
- 「OK」をクリックします。

選択したセッションのフラグの表示

「セッション情報(Session Info)」パネルの「添付ファイル(Attachments)」をクリックすると、選択したセッションのメモ、フラグ、およびスクリーンショットを表示できます。

すべてのセッションのフラグの表示

「スキャン情報(Scan Info)」パネルの「添付ファイル(Attachments)」をクリックすると、すべてのセッションのメモ、フラグ、およびスクリーンショットを表示できます。

スキャンメモ

スキャンメモを追加するには:

1. [スキャン情報(Scan Info)]パネルで [添付ファイル(Attachments)]をクリックします。
2. [追加(Add)]をクリックして [スキャンメモ(Scan Note)]を選択します。
3. [スキャンメモの追加(Add Scan Note)]ダイアログボックスで、スキャンに関連するメモを入力します。
4. [OK]をクリックします。

スキャンメモ(または添付ファイル)を削除するには:

1. 添付ファイルを選択します。
2. [削除(Delete)]をクリックします。

次も参照

["脆弱性スクリーンショットの追加と表示" ページ268](#)

["脆弱性のメモ" 次のページ](#)

["フォローアップのためのセッションへのフラグ設定" 前のページ](#)

セッションのメモ

セッションのメモを追加するには:

1. 次のいずれかを実行してセッションを選択します。
 - サマリペインの [検出事項(Findings)]タブで、脆弱なURLを右クリックします。
 - ナビゲーションペインで、セッションまたはURLを右クリックします。
2. ショートカットメニューで、[添付ファイル(Attachments)]> [セッションのメモの追加(Add Session Note)]をクリックします。

メモ: セッションのメモを追加するもう1つの方法として、脆弱性またはセッションを選択し、[セッション情報(Session Info)]パネルで [添付ファイル(Attachments)]をクリックしてから、(情報表示エリアの) [追加(Add)]メニューをクリックする方法があります。

3. 選択したセッションに関連するメモを入力します。
4. [OK]をクリックします。

選択したセッションのメモの表示

[セッション情報(Session Info)]パネルの [添付ファイル(Attachments)]をクリックすると、選択したセッションのメモ、フラグ、およびスクリーンショットを表示できます。

すべてのセッションのメモの表示

「スキャン情報(Scan Info)」パネルの「添付ファイル(Attachments)」をクリックすると、すべてのセッションのメモ、フラグ、およびスクリーンショットを表示できます。

次も参照

["検出事項\(Findings\)"\]タブ" ページ109](#)

["情報ペイン" ページ78](#)

["ナビゲーションペイン" ページ67](#)

脆弱性のメモ

脆弱性のメモを追加するには:

1. 次のいずれかを実行して脆弱性を選択します。
 - サマリペインの「検出事項(Findings)」タブで、脆弱なURLを右クリックします。詳細については、「["検出事項\(Findings\)"\]タブ" ページ109](#)」を参照してください。
 - ナビゲーションペインで、脆弱なセッションまたはURLを右クリックします。詳細については、「["ナビゲーションペイン" ページ67](#)」を参照してください。
2. ショートカットメニューで、「添付ファイル(Attachments)」>「脆弱性のメモの追加(Add Vulnerability Note)」をクリックします。

メモ: もう1つの方法として、脆弱性を選択し、「セッション情報(Session Info)」パネルで「添付ファイル(Attachments)」をクリックしてから、(情報表示エリアの)「追加(Add)」メニューをクリックする方法があります。詳細については、「["情報ペイン" ページ78](#)」を参照してください。

3. 複数の脆弱性があるセッションを選択した場合は、1つ以上の脆弱性の横にあるチェックボックスをオンにします。
4. 選択した脆弱性に関連するメモを入力します。
5. 「OK」をクリックします。

選択したセッションのメモの表示

「セッション情報(Session Info)」パネルの「添付ファイル(Attachments)」をクリックすると、選択したセッションのメモ、フラグ、およびスクリーンショットを表示できます。選択したセッションにロールアップされた脆弱性が含まれている場合、「説明(Description)」エリアのメモに、ロールアップされた、同一の脆弱性による影響を受けるURLの詳細が表示されます。詳細については、「["脆弱性のロールアップ" ページ272](#)」を参照してください。

すべてのセッションのメモの表示

【スキャン情報(Scan Info)】パネルの【添付ファイル(Attachments)】をクリックすると、すべてのセッションのメモ、フラグ、およびスクリーンショットを表示できます。

削除された項目の回復

セッションを削除するか、脆弱性を「無視」すると、Fortify WebInspectはその項目をナビゲーションペインから(【サイト(Site)】ビューと【シーケンス(Sequence)】ビューの両方で)、およびサマリペインの【検出事項(Findings)】タブから削除します。また、今後生成されるレポートからもこれらの項目が除外されます。

削除された項目の数は、ダッシュボード(【スキャン(Scan)】カテゴリの下)に表示されます。削除されたセッションと無視された脆弱性を復元するには:

1. 削除された項目(Deleted Items)】ヘッダの横に表示される、強調表示された数字をクリックします。
削除された項目の回復(Recover Deleted Items)】ウィンドウには、削除された項目のリストが表示されます。
2. 無視された脆弱性と削除されたセッションを切り替えるには、ドロップダウンリストをクリックします。
3. 回復する1つ以上の項目の横のチェックボックスをオンにします。
4. 項目の詳細情報を表示するには、【選択時に詳細を表示する(Show details when selected)】を選択します。
5. 【回復(Recover)】をクリックして、選択を確認するプロンプトが表示されたら【はい】をクリックします。

回復された脆弱性は、ナビゲーションペインの【サイト(Site)】ビューと【シーケンス(Sequence)】ビューに(親セッションとともに)再表示され、サマリペインの【検出事項(Findings)】タブにも再表示されます。復元されたセッションも、ナビゲーションペインに子セッションとその脆弱性とともに再表示されます。

次も参照

["セッション情報\(Session Info\)】パネル" ページ91](#)

Micro Focus ALMへの脆弱性の送信

1つ以上の脆弱性を不具合に変更して、それらをMicro Focus Application Lifecycle Management (ALM)データベースに追加できます。

脆弱性を不具合トラッキングシステムに送信するには:

1. ナビゲーションペインまたはサマリペインで脆弱性を右クリックします。詳細については、「["ナビゲーションペイン" ページ67](#)」および「["サマリペイン" ページ109](#)」を参照してください。

2. [送信先(Send to)]を選択して、[Micro Focus ALM]を選択します。
3. [送信先(Send to)]ダイアログボックスで、[プロファイル(Profile)]リストからプロファイルを選択します。

プロファイルを作成または編集する必要がある場合は、[管理(Manage)]をクリックして Fortify WebInspectの[アプリケーション設定(Application Settings)]にアクセスします。詳細については、「["アプリケーション設定: Micro Focus ALM" ページ471](#)」を参照してください。

メモ: 選択したプロファイルがFortify WebInspect脆弱性を(重大度レベルに基づいて)「発行しない(Do not publish)」にマップしている場合、脆弱性はエクスポートされません。

4. 以前に報告されている場合でも不具合を強制的に作成するには、[重複する不具合の割り当てを許可する(Allow duplicate defect assignment)]を選択します。
Fortify WebInspectは、同じスキャン内でのみ重複を認識します。サイトをスキャンして特定の脆弱性をALMIに送信する際に、そのスキャン中に再び同じ脆弱性が検出された場合、Fortify WebInspectが同じ脆弱性を送信しないようにすることができます。ただし、そのサイトに再びスキャンを行い、Fortify WebInspectが同じ脆弱性を再度検出した場合、Fortify WebInspectに以前のスキャンにおいて脆弱性がALMIに送信されたことをプログラムによって認識させることはできません。
5. 不具合の送信後にこのダイアログボックスを閉じるには、[完了したら閉じる(Close when finished)]を選択します。
6. 複数の脆弱性を選択した場合、ID番号の横のチェックボックスを外して脆弱性を除外できます。
7. [送信(Send)]をクリックします。

送信される追加情報

次の例が示しているように、Fortify WebInspectは、Micro Focus ALMIに欠陥が送信されたことを示すメモをセッション情報に追加します。

Defect #30 was created in Micro Focus ALM.

(Micro Focus ALMIにおいて不具合 #30が作成されました) Check ID: 182(チェックID: 182)

CheckName: Dan-o Log Information Disclosure(チェック名: Dan-oログ情報公開)

Profile: Thack(プロファイル: Thack)

Server URL: <http://qbakervm2003/qcbin>(サーバURL: <http://qbakervm2003/qcbin>)

Project: test3(プロジェクト: test3)

Priority: 3-High(優先度: 3-高)

Severity: 1-Low(重大度: 1-低)

メモ: 「Micro Focus ALMの認証でエラーが発生しました(Error authenticating with Micro Focus ALM)」というエラーメッセージが表示される場合は、「["データ実行防止の無効化"次のページ](#)」を参照してください。

データ実行防止の無効化

Micro Focus Application Lifecycle Management (ALM)と統合しようとすると、次のエラーメッセージが表示されることがあります。

Error authenticating with Micro Focus ALM.

その場合は、Microsoftのデータ実行防止(DEP)を無効にする必要があります。DEP設定の変更方法については、Windowsのマニュアルを参照してください。

レポートの生成

Report Generatorをさまざまな方法で起動できます。

- 開始ページ(Start Page)のクライアントエリアで、左ペインにある [レポートの生成 (Generate a Report)] をクリックする。
- Fortify WebInspectツールバーで [レポート(Reports)] をクリックする。
- [レポート(Reports)] メニューをクリックし、[レポートの生成(Generate Report)] を選択する。
- [スキャンの管理(Manage Scans)] フォームでスキャン名を右クリックし、[レポートの生成(Generate Report)] を選択する。
- スキャンを開いた状態で、[サイト(Site)] ビューでセッションを右クリックし、[セッションレポートの生成(Generate Session Report)] を選択する。詳細については、「["サイトビュー" ページ69](#)」を参照してください。
- スキャンをスケジューリングするときに。

レポートを生成するには:

- 上記のいずれかのオプションを使用してReport Generatorを起動します。
- [スキャンの選択(Select a Scan)] ウィンドウからスキャンを1つ以上選択します。
- (オプション) [詳細(Advanced)] (ウィンドウの下部にある)をクリックして、レポートの保存のオプションと、ヘッダとフッタのテンプレートを選択するためのオプションを選択します。
- [次へ(Next)] をクリックします。
- (オプション) [お気に入り(Favorites)] リストからレポートを選択します。

ヒント: 「お気に入り」は、1つ以上のレポートとその関連パラメータの単なる名前付きコレクションです。レポートおよびパラメータを選択した後でお気に入りを作成するには、[お気に入り(Favorites)] リストをクリックして、[お気に入りに追加(Add to favorites)] を選択します。

- 1つ以上のレポートを選択します。レポートの説明については、「["標準レポート" ページ283](#)」を参照してください。
- 要求できるパラメータの情報を入力します。感嘆符 ● は、必須パラメータを示します。

8. (1つのタブ上にすべてのレポートを結合するのではなく)個別のタブに各レポートを表示するには、[レポートを別のタブで開く(Open Reports in Separate Tabs)]を選択します。
9. [完了(Finish)]をクリックします。

レポートの保存

Fortify WebInspectによってレポートが生成および表示されたら、レポートビューアツールバーの[名前を付けて保存(Save As)]をクリックしてレポートを保存できます。

レポートは次の形式で保存できます。

- Adobe Portable Data Format (.pdf)
- ハイパーテキストマークアップ言語 (.html)
- ネイティブのFortify WebInspect内部形式 (.raw)
- リッチテキスト形式 (.rtf)
- テキスト (.txt)
- Microsoft Excel (.xls)

次も参照

["標準レポート" ページ283](#)

["詳細レポートのオプション" 下](#)

["コンプライアンステンプレート" ページ286](#)

["アプリケーション設定: レポート" ページ464](#)

詳細レポートのオプション

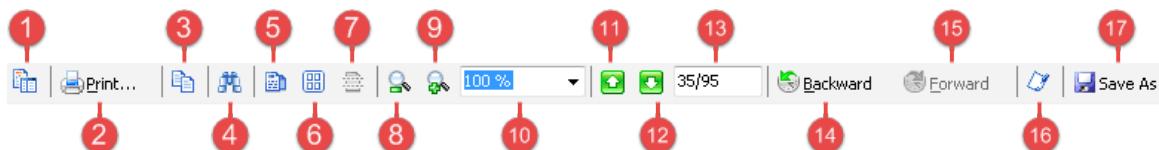
次の表に、詳細レポートのオプションの説明を示します。

| オプション | 説明 |
|--|---|
| レポートをディスクに保存する(Save reports to disk) | このオプションは、レポートをファイルに出力する場合に選択します。 |
| ファイル名を自動的に生成する(Automatically generate file name) | レポートをディスクに保存するときにこのオプションを選択すると、レポートファイルに<reportname> <date/time>.<extension>という形式の名前が付けられます。 たとえば、pdf形式でコンプライアンスレポートを作成し、そのレポートが4月5日の6:30に生成される場合、ファイル名は「Compliance Report 04_05_2009 06_30.pdf」になります。これは、反復スキャン |

| オプション | 説明 |
|---------------------------------------|---|
| | <p>の場合に便利です。</p> <ul style="list-style-type: none"> 複数のレポートタイプを選択した場合は、<reportname>が「Combined Reports」になります。 レポートは、生成されるレポート用にアプリケーション設定で指定されたディレクトリに書き込まれます。 <p>【ファイル名を自動的に生成する(Automatically generate filename)】を選択しない場合は、デフォルト名「auto-gen-filename」をファイル名に置き換えます。</p> |
| エクスポート形式 (Export Format) | レポート形式を選択します。 |
| ヘッダ/フッタレポート (Header/Footer Report) | レポートのヘッダとフッタの形式を選択してから、コンポーネントを入力または選択します。 |

レポートビューア

ツールバーを使用して、レポート内の移動、レポートの印刷と保存、メモの追加を行います。



| 項目 | 説明 |
|----|-----------|
| 1 | 目次の表示/非表示 |
| 2 | レポートの印刷 |
| 3 | コピー |
| 4 | 検索 |
| 5 | 単一ページビュー |
| 6 | 複数ページビュー |

| 項目 | 説明 |
|----|------------------------------------|
| 7 | 連続スクロール |
| 8 | ズームアウト |
| 9 | ズームイン |
| 10 | 倍率 |
| 11 | 前のページ |
| 12 | 次のページ |
| 13 | 現在のページ番号/ページの合計数 |
| 14 | 1ページ戻る |
| 15 | 1ページ進む |
| 16 | 注釈(「 メモの追加 」下)を参照) |
| 17 | レポートの保存 |

メモ: [戻る(Backward)]ボタンと [進む(Forward)]ボタンは、ブラウザの [戻る]ボタンと [進む]ボタンと同じように機能します。履歴リスト内の1ステップ分進むか、戻ります。

メモの追加

メモを追加するには:

1. [注釈(Annotation)]アイコンをクリックします。
2. 形式を選択します。
3. レポートにドラッグします。
4. メモを右クリックし、[プロパティ(Properties)]を選択します。
5. [テキスト(Text)]プロパティを選択し、メモの内容を入力します。

標準レポート

次の表に、使用可能な標準レポートの説明を示します。

| レポート | 説明 |
|---------------|--------------------------------|
| 集約(Aggregate) | このレポートは、複数スキャン向けに設計されています。報告する |

| レポート | 説明 |
|--------------------------------|---|
| | 重大度のカテゴリ、レポートセクション(サーバのコンテンツと脆弱性の詳細)、およびセッション情報(応答および要求)を選択できます。スタックトレースが利用可能な場合には、スタックトレースも報告できます。 |
| アラートビュー(Alert View) | このレポートでは、すべての脆弱性が重大度別に一覧にされ、脆弱性を発生させた各HTTP要求へのハイパーリンクが表示されます。また、各脆弱性を詳細に説明した付録も含まれています。 |
| 攻撃ステータス(Attack Status) | このレポートには、スキャン中に使用された各攻撃エージェント(チェック)について、脆弱性ID番号、チェック名、脆弱性の重大度、チェックがスキャンで有効になっていたかどうか、チェックが合格したかどうか(つまり、脆弱性が検出されたかどうか)、および(チェックが不合格の場合には)脆弱性が検出されたURLの数が一覧にされます。特定の重大度の脆弱性と、合格/不合格ステータスを報告することを選択できます。 |
| コンプライアンス(Compliance) | このレポートには、政府が定めた特定の規制や企業が定義したガイドラインにアプリケーションがどの程度準拠しているかを評価した定性分析が含まれています。 |
| Web探索済みURL(Crawled URL) | このレポートには、Web探索中に検出されたURLごとに、送信されたすべてのクッキーと生のHTTP要求および応答が一覧にされます。 |
| 開発者リファレンス(Developer Reference) | Webサイトで検出された各フォーム、JavaScript、電子メール、コメント、非表示のコントロール、およびクッキーの総数と詳細な説明が示されます。これらの参照タイプから1つ以上を選択できます。 |
| 重複(Duplicates) | このレポートには、Fortify WebInspect Agentにより検出され、同じソースに行き着く脆弱性に関する情報が記載されています。最初に、相關関係のない脆弱性の総数と固有の脆弱性の数を比較する棒グラフが表示されます。 |
| エグゼクティブサマリ(Executive Summary) | このレポートには、基本的な統計情報と、アプリケーションの脆弱性レベルを反映したグラフが表示されます。 |
| 誤検出(False Positives) | このレポートには、Fortify WebInspectによって最初は脆弱性として分類されたが、後でユーザが誤検出と判断したURLに関する情報が表示されます。 |
| QAの概要(QA) | このレポートには、破損したリンク、サーバエラー、外部リンク、および |

| レポート | 説明 |
|---|--|
| Summary) | タイムアウトを含むすべてのページのURLが一覧にされます。これらのカテゴリから1つ以上を選択できます。 |
| スキャンの差異 (Scan Difference) | このレポートでは、2つのスキャンが比較され、脆弱性、ページ、ファイルが見つからないという応答などが一方のWebサイトでだけ見られるといった相違が報告されます。 |
| スキャンログ(Scan Log) | スキャン中にFortify WebInspectによって実行されたアクティビティを順に示すリストです(情報はサマリペインの [スキャンログ(Scan Log)]タブに表示されます)。 |
| 傾向(Trend) | このレポートでは、脆弱性の解決に向けた開発チームの進捗状況を監視できます。たとえば、最初のスキャンの結果が保存され、チームが問題の修復を開始します。その後、毎週1回サイトを再スキャンして結果をアーカイブします。進行状況を定量化するには、現在までに実行したすべてのスキャンの結果を分析する傾向レポートを実行します。このレポートには、各スキャンの実行日付によって定義されたタイムラインに、脆弱性の数を重大度別に示すグラフが含まれています。重要: 信頼できる結果を得るために同じポリシーを使用して各スキャンを実行してください。 |
| 脆弱性(レガシ) (Vulnerability (Legacy)) | 各脆弱性と、改善に関する推奨事項を含む詳細なレポートです。 |
| 脆弱性 (Vulnerability) | このレポートにも、検出された脆弱性に関する詳細情報が重大度別に表示されます。 |

レポートの管理

レポート定義ファイルの名前変更、追加、削除、またはインポートを行うには、[レポートの管理(Manage Reports)]を使用します。

標準レポートに対する名前変更、削除、またはエクスポートは実行できません。

コンプライアンステンプレート

ここでは、使用可能なコンプライアンステンプレートについて説明します。他のテンプレートは、使用可能になった段階でSmartUpdateを介してダウンロードできます。

メモ: このリストは、お使いの製品に表示されるテンプレートと一致しない場合があります。このドキュメントの作成以降に、SmartUpdateによりテンプレートが追加されている可能性があります。

| テンプレート | 説明 |
|---------|--|
| 21CFR11 | <p>米国連邦規制基準第21編第11部(通常は「21 CFR 11」と略される)に、電子記録および電子署名に関する要件が記載されています。医療会社のコンプライアンスを支援するために、米国食品医薬品局(FDA)は、FDA規制によって保管および維持が義務付けられている記録の電子記録および電子署名の適切な使用に関するガイダンスを公開しています。このガイダンスには、「機関が、電子記録、電子署名、および電子記録に対して行われた手書きの署名が信用でき、信頼性が高く、紙の記録や紙に対して行われた手書きの署名と同等であると見なす基準」が記載されています。</p> <p>法律とFDAガイダンスにより、機密性の高い医療情報を扱う医療会社や医療機関は、電子記録と電子署名が信用でき、信頼性が高く、紙の記録や手書きの署名の同等の代用品であることを保証することが義務付けられています。機器、オペレータ、およびコンピュータ間の相互作用が当たり前になる中、情報の通信と保存を行う安全な手段を確立することが重要です。</p> |
| バーゼルIII | <p>バーゼルIIIは、世界中の中央銀行による検討事項の一環であり、スイスのバーゼルにあるバーゼル銀行監督委員会(BCBS)の下で、銀行と金融当局が国境を越えてリスク管理に取り組む方法の統一を図ることを目的としています。BCBSは、銀行業務のコンプライアンスに関する国際的なルール作成部門です。2004年、中央銀行の総裁と10か国蔵相会議(G10)の各国銀行監督機関の長が、バーゼルIIIとして広く知られている新しい自己資本の枠組みである「自己資本の計測と基準に関する国際的統一化:改訂された枠組み」の発行を承認しました。</p> <p>バーゼルIIIは、主に、銀行に対して、資本準備金を増やすか、信用リスクや運用リスクを組織的かつ効果的に管理できることを実証するよう求めています。この枠組みでは、運用リスクを「不適切なまたは機能不全の内部プロセス、人、およびシステムによって、または、外部的事象によって発生する損失のリスク」と定義し、不適切なシステムセキュリ</p> |

| テンプレート | 説明 |
|-----------|---|
| | <p>ティを介したハッキングや情報漏洩を損失事象として強調しています。世界中の銀行はグローバルな金融市場での運用リスクを管理する専門家ですが、オンライン銀行システムの運用と顧客データの安全性の確保に伴うリスクを理解して管理することには精通していません。</p> <p>効果的な情報セキュリティとシステムセキュリティを実践している銀行は、監督機関に対して、運用リスクの低減を通して資本準備金を削減する資格があることを実証できます。バーゼルIIの枠組みは、情報を保護するためのポリシーとプロセスの効果的なシステムが設けられていることと、これらのポリシーとプロセスへのコンプライアンスが保証されていることを実証するよう銀行に対して繰り返し求めていますが、銀行がセキュリティポリシーおよびプロセスを実装する方法については規範を示していません。国際標準のISO/IEC 17799 Code of Practice for Information Security Managementは、情報セキュリティの実装と維持に関するガイドラインを提供しており、バーゼルIIの文脈で情報セキュリティに関する運用リスクを管理および報告するためのモデルとして広く使用されています。</p> |
| CA OPPA | <p>カリフォルニア州オンラインプライバシー保護法(OPPA)は、2003年に制定され、カリフォルニア州の商用Webサイトのすべての企業と所有者に、個人情報の収集、使用、および共有に関するポリシーを明確に定めたプライバシーポリシーを目立つ場所に掲示し、遵守するように義務付けています。このポリシーは、サイト訪問者に関して収集された個人識別情報のカテゴリと、運営者が情報の共有先にできる第三者のカテゴリを識別します。</p> <p>カリフォルニア州の住人の非公開個人情報を収集するWebサイトを運営する企業、組織、または個人はこの法律の条項に制約されるため、カリフォルニア州OPPAは一般的な州の規制よりはるかに大きな影響を全国的に及ぼします。</p> |
| CASB 1386 | <p>カリフォルニア州上院法案第1386号は、米国内の州の中で最も具体的で制限的なプライバシー侵害報告要件を定めています。この法律は、正当な業務目的で非公開個人情報を保有する企業、組織、および個人に対して、個人情報が漏洩した場合に直ちに消費者に通知することを強制するために制定されました。また、この法律は、情報の侵害を通して被った損害について、民事裁判所で企業を訴える権利を消費者に与えています。カリフォルニア州の住人の非公開個人情報を保持する企業、組織、または個人は、この法律の条項に制約されます。</p> |
| COPPA | 児童オンラインプライバシー保護法(COPPA)は、13歳未満の子供に |

| テンプレート | 説明 |
|-------------------------|--|
| | <p>関する個人情報をオンライン収集から保護するために2000年に制定されました。COPPAの目的は、子供がしばしば簡単にWebにアクセスできることを認識した上で、子供のプライバシーと安全をオンラインで保護することです。この法律は、Webサイトの運営者がサイト上にプライバシーポリシーを掲載し、特定の状況下で子供の個人情報を収集する場合は親の同意を求めるという要件の概要を示すように義務付けています。</p> <p>この法律は、明らかに子供向けのWebサイトだけでなく、Webサイトの運営者が子供から個人情報を収集していることを自覚している、一般的な視聴者コンテンツを含むWebサイトにも適用されます。運営者は、自社のWebサイトまたはオンラインサービスのホームページと、子供から個人情報を収集する各エリアに、その情報取り扱いの通知へのリンクを掲載する必要があります。子供のエリアが別にある一般的な視聴者サイトの運営者は、子供のエリアのホームページにその通知へのリンクを掲載する必要があります。</p> |
| CWE Top 25 <version> | <p>CWE (Common Weakness Enumeration) Top 25 Most Dangerous Software Errors (CWE Top 25)は、MITREが作成した弱点のリストで、ソフトウェアの重大な脆弱性につながる可能性のある最も広がっている重大な弱点を示しています。MITREは、その方法論の概要を次のように説明しています。</p> <p>「このリストを作成するために、CWEチームは、公開済みのCVE (Common Vulnerabilities and Exposures)データ、NIST (National Institute of Standards and Technology) のNVD (National Vulnerability Database)内にある関連CWEマッピング、および各CVEに関連付けられたCVSS (Common Vulnerability Scoring System)スコアを利用するデータ駆動型のアプローチを使用しました。その上で、採点式を適用して各弱点が示すまん延度と危険度を決定しました。反復可能でスクリプト化されたプロセスとしてこのデータ駆動型のアプローチを使用し、最小限の労力で定期的にCWE Top 25リストを生成することができます。」</p> |
| DCID | この指令は、分類されたインテリジェンス情報を情報システムに保存、処理、および通信するためのセキュリティポリシーと手順を定めています。この指令の目的では、インテリジェンス情報とは、中央情報局長官の権限の下にある、隔離された機密情報とインテリジェンスへの特別なアクセスプログラムを指します。 |
| DoD Application | DISA FSO (Field Security Operations)は、アプリケーションSRRを実施して、アプリケーションがミッションを脅かす可能性のある攻撃に対して |

| テンプレート | 説明 |
|--|--|
| Security Checklist Version 2 | <p>合理的に安全であることの最低レベルの保証を、DISA、統合部隊、およびその他の国防総省(DoD)組織に提供します。ほとんどのミッションクリティカルなアプリケーションでは、その複雑さのせいで、アプリケーションSRRに割り当てられた時間枠内で考えられるすべてのセキュリティ機能と脆弱性の包括的なセキュリティレビューを行うことが不可能です。それにもかかわらず、最も一般的なアプリケーションの脆弱性に対処し、運用上許容できないリスクをもたらす情報保証(IA)問題を特定する上で、SRRは役立ちます。</p> <p>IA制御が開発ライフサイクルのすべてのフェーズで統合されることが理想的です。アプリケーションレビュープロセスを開発ライフサイクルに統合すれば、アプリケーションのセキュリティ、品質、および回復力を保証できます。通常、アプリケーションSRRはアプリケーションリリースの近くまたは後に実施されるため、アプリケーションSRRの検出事項の多くは、アプリケーションインフラストラクチャに対するパッチまたは変更を通して修復する必要があります。脆弱性によっては修正に大幅なアプリケーション変更を要することがあります。アプリケーションレビュープロセスを開発ライフサイクルに統合するのが早いほど、改善プロセスの中止が少なくなります。</p> |
| DoD Application Security and Development STIG <version> | <p>このコンプライアンステンプレートでは、Application Security and Development Security Technical Implementation Guide (STIG)のバージョン3、リリース2の該当するWebアプリケーションコンポーネントのすべてが報告されます。STIGは、アプリケーション開発ライフサイクル全体を通して使用するためのセキュリティガイダンスを提供します。国防情報システム局(DIS)は、アプリケーション開発プロセスのできるだけ早い段階でこれらのガイドラインを使用するようにサイトに奨励しています。</p> |
| DoD Control Correlation Identifier (CCI) | <p>国防情報システム局(DIS)のFSO (Field Security Operations)がCCI仕様を作成し、現在は、CCI仕様とCCIリストの保守を担当しています。</p> <p>CCI (Control Correlation Identifier)は、情報保証(IA)制御またはIAベストプラクティスを構成する単一のアクション可能な声明のそれぞれに標準の識別子と記述を提供します。</p> <p>CCIは大まかなポリシー表現と詳細な技術実装の間のギャップを埋めます。CCIでは、大まかなポリシーフレームワークで表現されたセキュリティ要件を分解し、その特定のセキュリティ制御の目的の遵守を判断するために評価する必要がある詳細なセキュリティ設定と明示的に関連付けることができます。セキュリティ要件をその原点(規制やIAフレームワークなど)から詳細な実装までを追跡できるこの能力を使用すれば、組織</p> |

| テンプレート | 説明 |
|-----------------------|---|
| | <p>は、複数のIAコンプライアンスフレームワークへのコンプライアンスを簡単に実証できます。また、CCIは、異種の技術をまたいで関連するコンプライアンス評価結果を客観的にロールアップして比較する手段も提供します。</p> <p>このレポートは、Micro Focus Fortify 7PK分類をDISA CCIにマップします。</p> |
| EUデータ保護 | <p>欧州委員会のデータ保護に関する指令は、個人データの処理に関するプライバシーに対する欧州連合市民の基本的権利を保護します。この指令の主な焦点は、受け入れ可能な個人データの使用と保護に置かれています。他のすべての欧州連合プライバシー立法と同様に、この指令でも、個人データを収集、保存、変更、または発信するにはデータの使用に関する市民の明確な同意と完全な開示を要求しています。また、欧州の組織から個人データの安全とプライバシーを適切に保護していない欧州連合以外の国や組織に個人データを転送することを禁じています。米国は、この指令に準拠する必要がある米国の組織向けのセーフハーバーフレームワークを策定しました。</p> |
| プライバシーおよび電子通信に関するEU指令 | <p>プライバシーおよび電子通信に関する欧州連合指令は、欧州連合の電子通信部門に適用される法律の広範な「電気通信一括法案」の一部です。この指令は、すべての加盟国が、公衆通信ネットワーク上で行われた通信と、このような通信に本来備わっている個人データと非公開データの機密性を保証しなければならないという欧州連合の基本原則を補強するものです。この指令は、物理通信ネットワークとその上で伝送される個人データに適用されます。</p> |
| FISMA | <p>米国連邦政府は、米国の経済と国家安全保障の利益に対する情報セキュリティの重要性を認識して、2002年の電子政府法を通過させました。この法律の第III編は、連邦情報セキュリティマネジメント法(FISMA)と題され、すべての米国連邦政府機関が機密性、整合性、および可用性という3つのセキュリティ目標を掲げた適切な情報セキュリティを情報システムの一部として実装する際に使用する標準とガイドラインの策定を米国標準技術局に委ねています。FISMAは、各連邦機関の長に、情報と情報システムの不正アクセス、使用、開示、中断、変更、または破壊に伴うリスクと損害の大きさに見合った情報セキュリティ保護を提供するように要求しています。保護は、機関だけでなく、機関の代わりに働く請負業者や他の組織にも適用される必要があります。</p> |
| 一般データ保護規則 | <p>EU一般データ保護規則(GDPR)は、データ保護指令95/46/ECに代わるもので、欧州全体のデータプライバシー法を調和させ、すべてのEU</p> |

| テンプレート | 説明 |
|----------|--|
| (GDPR) | <p>市民のデータプライバシーを保護および強化し、地域全体の組織がデータプライバシーにアプローチする方法を見直すように設計されています。2018年5月25日に施行されたGDPRは、個人データの処理方法に関するフレームワークを組織に提供しています。</p> <p>GDPR規制によると、個人データは「特定されたまたは特定可能な自然人（「データ主体」）に関する情報を意味します。特定可能な自然人とは、特に、名前、識別番号、位置データ、オンライン識別子などの識別子を参照したり、その自然人の物理的、生理的、遺伝的、精神的、経済的、文化的、または社会的アイデンティティに固有の1つ以上の要素を参照したりすることによって直接的または間接的に識別できる人のことです。」</p> <p>アプリケーションセキュリティに関連し、製品やサービスの設計や開発中に個人データを保護することを企業に要求するGDPRの条項を以下に示します。</p> <ul style="list-style-type: none"> 第25条、設計およびデフォルトでのデータ保護-「デフォルトで、処理の特定の目的ごとに必要な個人データのみが処理されることを保証するための適切な技術的および組織的手段」の実施が必要です。 第32条、処理のセキュリティ-企業は「個人データの偶発的または不当な破壊、紛失、改変、不正開示、またはアクセスから」システムおよびアプリケーションを保護する必要があります。 <p>このレポートは、アプリケーションセキュリティに関連して個人データの特定と保護を支援するためのフレームワークとして組織が使用する場合があります。</p> |
| GLBA | グラムリーチブライリー法(GLBA)では、金融機関が消費者の個人の金融情報を保護するように義務付けています。金融業界のWebアプリケーションセキュリティに影響を与える主な規定は、GLBAセーフガードルールです。 |
| HIPAA | Health Insurance Portability and Accountability Act (HIPAA: 医療保険の携行性と責任に関する法律)は、情報管理に関するさまざまな脅威や脆弱性からの個人の健康情報のプライバシーとセキュリティを義務付けています。 |
| ISO17799 | これは、情報セキュリティ管理に関して最も広く受け入れられている国際標準です。このポリシーは、組織とそのセキュリティポリシーのニーズを満たすコンプライアンスポリシーの策定のベースラインとして使用してください。 |

| テンプレート | 説明 |
|--------------------------|---|
| ISO27001 <version> | ISO/IEC 27001は、国際標準化機構および国際電気標準会議によって2005年10月に発行された情報セキュリティ管理システム標準です。基本的な目的は、継続的な改善アプローチを使用して、効果的な情報管理システムの確立と維持を支援することです。ISO 27001は、セキュリティ管理システム自体に関する要件を定めています。これは、ISO 17799とは対照的に、認定が提供される標準です。加えて、ISO 27001は、ISO 9001やISO 14001などの他の管理標準と「統一」されています。 |
| JPIPA | 日本は、2003年に、正当な目的のためにITと個人情報の有益性を保持しながら、個人の権利と個人情報を保護することを目的として、個人情報保護法(JPIPA)を施行しました。この法律は、日本の市民の個人情報を取り扱う企業の責任を規定し、準拠しない組織に対する罰金と罰則の可能性の概要を示しています。この法律は、企業に、個人情報の収集と使用の目的を伝達するように義務付けています。また、企業は、個人情報を開示、不正使用、または破壊から保護するための合理的な手順を講じる必要があります。 |
| NERC | 北米電力信頼度協議会(NERC)は、米国の電力システムが信頼でき、適切で、安全であることを保証する使命を持って1968年に設立されました。1998年にBill Clinton大統領が米国の国家経済と公共の福祉に不可欠なインフラストラクチャ産業を定義するために大統領決定指令63を発行した後、米国エネルギー省は8つの重要なインフラストラクチャ産業の1つとして指名された電力業界の調整機関としてNERCを指定しました。 |
| NIST 800-53 <version> | 米国連邦政府は、米国の経済と国家の利益に対する情報セキュリティの重要性を認識して、2002年の電子政府法を通過させました。この法律の第III編は、連邦情報セキュリティマネジメント法(FISMA)と題され、すべての米国連邦政府機関が機密性、整合性、および可用性という3つのセキュリティ目標を掲げた適切な情報セキュリティを情報システムの一部として実装する際に使用する標準とガイドラインの策定を米国標準技術局に委ねています。 |
| OMB | このポリシーは、2004年12月に行政管理予算局が連邦政府機関の公式Webサイトに関して定義した主要なアプリケーションセキュリティ部門を対象とします。これらのWebサイトは、連邦政府が全部または一部の資金を提供し、機関、請負業者、または機関に代わるその他の組織が運営する情報リソースです。政府の情報を開示したり、一般または特定の非連邦ユーザグループにサービスを提供して、機関の機能の適切な遂行をサポートしたりします。 |

| テンプレート | 説明 |
|------------------------|---|
| OWASP ASVS | <p>OWASP (Open Web Application Security Project) ASVS (Application Security Verification Standard)は、設計者、開発者、テスト担当者、セキュリティプロフェッショナル、ツールベンダー、および消費者が安全なアプリケーションを定義、構築、テスト、および検証するために使用できるアプリケーションセキュリティ要件またはテストのリストです。</p> <p>メモ: OWASP ASVSドキュメントのCWEカテゴリへのマッピングの中には、カテゴリの目的と一致しないものや、限定範囲で一致するものがあります。このテンプレートを使用して生成されたレポート内のCWEマッピングを確認してください。</p> |
| OWASP Top Ten <year> | <p>多くの政府機関が、Webアプリケーションのセキュリティの確保におけるベストプラクティスとして、OWASP Top Ten Webアプリケーション脆弱性のテストを推奨しています。</p> <p>メモ: 「Top Ten」以外のOWASPコンプライアンステンプレートも入手できます。</p> |
| PCIデータセキュリティ <version> | <p>クレジットカード業界(PCI)データセキュリティポリシーは、カード所有者データを保存、処理、または送信するすべてのPCIデータセキュリティのメンバー、業者、およびサービスプロバイダが、社内外のアプリケーションを含む、すべての購入したカスタムWebアプリケーションを検証するように義務付けています。</p> <p>メモ: 「データセキュリティ」以外のPCIコンプライアンステンプレートも入手できます。</p> |
| PIPEDA | <p>カナダの個人情報保護および電子文書法(PIPEDA)は、民間企業の管理下で個人情報を保護する新しい法律であり、商業活動の過程でのその情報の収集、使用、および開示に関するガイドラインを示しています。この法律は、カナダ規格協会が策定した10のプライバシー原則に基づいて、カナダのプライバシー委員会と連邦裁判所によって監視されています。2004年1月1日以降、カナダの企業はすべて、PIPEDAによって規定されたプライバシー原則を遵守する必要があります。この法律は、従来の紙ベースのビジネスとオンラインビジネスの両方を対象とします。</p> |
| セーフハーバー | <p>欧州委員会のデータ保護に関する指令は、欧州の組織から個人データの安全とプライバシーを適切に保護していない欧州連合以外の国や組織に個人データを転送することを禁じています。この包括的な欧州の法律の通過により、欧州連合の組織とデータを共有する米国内の</p> |

| テンプレート | 説明 |
|---------------------------|--|
| | <p>すべての企業および組織に規制の遵守が義務付けられ、これはさまざまな大西洋横断企業取引を混乱させかねませんでした。個人データのプライバシーの保護に対して米国と欧州連合の各国が取ったアプローチが異なるために、米国商務省は、欧州委員会と協力して、合理化された「セーフハーバー」フレームワークを策定しました。このフレームワークを通して、米国の組織はデータ保護に関する指令に準拠できます。</p> <p>セーフハーバーに参加している組織は、個人データが適切に使用、制御、および保護されていることを保証するために設計された7つの原則(通知、選択、転送、アクセス、セキュリティ、データ整合性、および実施)に準拠するように取り組む必要があります。ITにとって特に重要なのは次の点です。</p> <ul style="list-style-type: none"> 通知の原則では、組織は、個人情報を収集する目的をプライバシーポリシーなどを通して個人に通知する必要があります。 セキュリティの原則には、組織が個人データを保護するための合理的な予防措置を講じることが明記されています。 実施の原則では、組織が、包括的なセキュリティテストなどを通じて、セキュリティの義務が果たされていることを検証する手順を実施する必要があります。 |
| SANS CWE Top 25 <version> | <p>SANS (SysAdmin、Audit、Network、Security) Instituteは、1989年に共同研究および教育組織として設立されました。SANS CWE (Common Weakness Enumeration) Top 25 Most Dangerous Software Errorsは、深刻なソフトウェアの脆弱性につながる可能性のある最も普及している重大なプログラミングエラーのリストです。このようなエラーのせいで攻撃者がソフトウェアを完全に掌握して、データを盗んだり、ソフトウェアの機能を妨げたりすることが頻繁であるため、危険です。このコンプライアンステンプレートでは、このリストのすべての該当するWebアプリケーションコンポーネントが報告されます。</p> <p>メモ: 「CWE」以外のSANSコンプライアンステンプレートも入手できます。</p> |
| サーベンスオクスリー | 米国証券取引委員会(SEC)の管理下にあるサーベンスオクスリー法は、2002年7月30日に制定されました。この法律は、顧客の機密情報のプライバシーやセキュリティを強化するのではなく、財務記録の保護のための企業行動を規制することに焦点が当てられています。 |
| 英国のデータ保護 | 欧州委員会のデータ保護に関する指令は、個人データの処理に関するプライバシーに対する欧州連合市民の基本的権利を保護します。 |

| テンプレート | 説明 |
|-------------------|---|
| | <p>この指令の主な焦点は、受け入れ可能な個人データの使用と保護に置かれています。英国は、1998年のデータ保護法を通して、指令が定める保護を実施してきました。この法律の概要を以下に示します。</p> <ul style="list-style-type: none"> 個人データは、同意がある場合にのみ、公正かつ合法的に処理する必要があります。 個人データは、特定の合法的な目的でのみ取得し、それらの目的と相容れない方法では処理しないようにする必要があります。 個人データは、処理される目的に関して適切で、関連があり、過剰ではない必要があります。 個人データは、正確で、最新の状態に保つ必要があります。 いかなる目的のために処理される個人データも、必要以上に長く保持しないようにする必要があります。 個人データは、データ主体の権利に従って処理する必要があります。 個人データの不正なまたは不当な処理や個人データの偶発的な紛失、偶発的な破壊、または損害に対して、適切な技術的および組織的対策を講じる必要があります。 個人データは、欧州経済地域外の国または地域に転送しないようにする必要があります。ただし、その国または地域が個人データの処理に関するデータ主体の権利および自由に対する適切なレベルの保護を保証していない場合に限られます。 |
| WASC <version> | <p>このコンプライアンステンプレートは、Web Application Security Consortiumの脅威クラスに基づいて作成されています。WASCの脅威分類は、Webサイトのセキュリティに対する脅威を明確にして整理するための共同の取り組みです。全チェックポリシーと組み合わせて使用することにより、SecureBaseに付属の各脆弱性チェックを含むコンプライアンスレポートを生成できます。</p> |

設定の管理

この機能を使用すると、スキャン設定ファイルを作成、編集、削除、インポート、およびエクスポートできます。

また、[デフォルト設定(Default Settings)]ウィンドウから設定をロードして保存し、出荷時のデフォルト設定を復元することもできます。[編集(Edit)]をクリックし、[デフォルトのスキャン設定(Default Scan Settings)]を選択します。

Fortify WebInspectの **編集(Edit)**]メニューから **設定の管理(Manage Settings)**]を選択します。

設定の管理(Manage Settings)]ウィンドウが開きます。

設定ファイルの作成

設定ファイルを作成するには:

1. **追加(Add)**]をクリックします。
2. **新規設定の作成(Create New Settings)**]ウィンドウで設定を変更します。
3. 終了したら、**OK**]をクリックします。
4. 標準のファイル選択ダイアログボックスを使用して、ファイルに名前を付けて保存します。

設定ファイルの編集

設定ファイルを編集するには:

1. ファイルを選択します。
2. **編集(Edit)**]をクリックします。
3. **新規設定の作成(Create New Settings)**]ウィンドウで設定を変更します。
4. 終了したら、**OK**]をクリックします。

設定ファイルの削除

設定ファイルを削除するには:

1. ファイルを選択します。
2. **削除(Delete)**]をクリックします。

設定ファイルのインポート

設定ファイルをインポートするには:

1. **インポート(Import)**]をクリックします。
2. 標準のファイル選択ダイアログボックスを使用して設定ファイルを選択し、**開く(Open)**]をクリックします。

設定ファイルのエクスポート

設定ファイルをエクスポートするには:

1. ファイルを選択します。
2. **エクスポート(Export)**]をクリックします。

- 標準のファイル選択ダイアログボックスを使用して、ファイルに名前を付け、場所を選択します。
- 【保存(Save)】をクリックします。

保存した設定ファイルを使用したスキャン

保存した設定ファイルを使用してスキャンするには:

- Fortify WebInspectの【編集(Edit)】メニューから【デフォルト設定(Default Settings)】を選択します。
- 【デフォルト設定(Default Settings)】ウィンドウの下部の左側の列で、【ファイルから設定をロード(Load settings from file)】をクリックします。
- 標準のファイル選択ダイアログボックスを使用して、利用したい設定ファイルを選択し、【開く(Open)】をクリックします。

これで、選択したファイルがデフォルトの設定ファイルになります。

SmartUpdate

インターネットに接続しているインストール環境では、SmartUpdate機能がMicro Focusデータセンターと通信して、新規または更新されたアダプティブエージェント、脆弱性チェック、およびポリシー情報を確認します。SmartUpdateでは、Fortify WebInspectの最新バージョンを使用しているかどうかも確認され、新しいバージョンがダウンロード可能な場合には通知されます。

アプリケーションを起動するたびにSmartUpdateを実行するようにFortify WebInspectを設定できます(【編集(Edit)】メニューから【アプリケーション設定(Application Settings)】を選択し、【スマートアップデート(Smart Update)】を選択します)。

Fortify WebInspectユーザインターフェースからSmartUpdateをオンデマンドで実行することもできます。このためには、Fortify WebInspectの【開始ページ(Start Page)】から【SmartUpdateを開始(Start SmartUpdate)】を選択するか、【ツール(Tools)】メニューから【SmartUpdate】を選択するか、または標準ツールバーの【SmartUpdate】ボタンをクリックします。詳細については、「"ツール(Tools)】メニュー" ページ58」および「"ツールバー" ページ63」を参照してください。

インターネットに接続していないインストール環境の場合は、「"SmartUpdateの実行(オフライン)" ページ299」を参照してください。

注意! エンタープライズインストールの場合、Fortify WebInspectが使用する特定のファイルがSmartUpdateによって変更または置換されると、センササービスが停止し、センサで「オフライン」ステータスが表示されることがあります。Fortify WebInspectアプリケーションを起動し、サービスを再起動する必要があります。このためには、

1. [編集(Edit)] > [アプリケーション設定(Application Settings)] をクリックします。
2. [センサとして実行(Run as a Sensor)] を選択します。
3. [センサステータス(Sensor Status)] エリアの [開始(Start)] ボタンをクリックします。

SmartUpdateの実行(インターネットに接続している場合)

WebInspectがインターネットに接続している場合にSmartUpdateを実行するには:

1. 次のいずれかを実行します。
 - ツールバーで [SmartUpdate] をクリックします。
 - [ツール(Tools)] メニューから [SmartUpdate] を選択します。
 - Fortify WebInspectの [開始ページ(Start Page)] から [SmartUpdateの開始(Start SmartUpdate)] を選択します。アップデートが利用可能な場合は、[SmartUpdater] ウィンドウが開き、[サマリ(Summary)] タブが表示されます。[サマリ(Summary)] タブには、次のアイテムをダウンロードするための折りたたみ可能な別個のペインが最大3つ表示されます。
 - 新規チェックおよび更新されたチェック
 - Fortify WebInspectソフトウェア
 - SmartUpdateソフトウェア
2. 1つ以上のダウンロードオプションに対応するチェックボックスをオンにします。
3. (オプション) 更新されるチェックの詳細を表示するには
 - a. [チェックの詳細(Check Detail)] タブをクリックします。
左側のペインには、更新されるチェックのID、名前、およびバージョンを示すリストが表示されます。リストは [追加(Added)]、[更新(Updated)]、および [削除(Delete)] でグループ化されます。
 - b. 更新される特定のチェックを含むポリシーを確認するには、リストでそのチェックを選択します。
影響を受けるポリシーのリストが [関連ポリシー(Related Policies)] ペインに表示されます。
4. (オプション) 影響を受けるポリシーの詳細を表示するには
 - a. [ポリシーの詳細(Policy Detail)] タブをクリックします。
左側のペインに、更新の影響を受けるポリシーが英字順で一覧表示されます。

メモ: このリストには、更新されるチェックの影響を受けるポリシーだけが表示されます。 [ポリシーの詳細(Policy Detail)] タブには、アップデートに含まれている可能

性がある他のポリシー変更(ポリシーへの新しいチェックの関連付けまたはポリシー名の変更など)は表示されません。

- b. 特定のポリシーで更新されるチェックを表示するには、リストからポリシーを選択します。
[関連チェック(Related Checks)]ペインに、更新されるチェックのID、名前、およびバージョンを示すリストが表示されます。リストは [追加(Added)]、[更新(Updated)]、および [削除(Delete)] でグループ化されます。
- 5. アップデートをインストールするには、[ダウンロード(Download)]をクリックします。

Fortify WebInspectを更新せずにチェックをダウンロードする

スキャン中に特定のチェックを実行するには、エンジンの更新が必要です。最新バージョンの Fortify WebInspectを使用していない場合、スキャン中にSecureBaseのチェックの一部を実行できない可能性があります。すべて最新のチェックを使用してアプリケーションをテストするには、最新バージョンのFortify WebInspectを使用している必要があります。

SmartUpdateの実行(オフライン)

オフラインのWebInspectのSmartUpdateを実行するには、次の手順に従います。

| ステージ | 説明 |
|------|--|
| 1. | サポートケースを作成します。カスタマサポート担当者から、オフラインFTPサーバのURLとログイン資格情報が提供されます(必要な場合)。詳細については、「 "序文" ページ24 」を参照してください。 |
| 2. | インターネットにアクセスできるマシンで、オフラインFTPサーバにアクセスします。 |
| 3. | Fortify WebInspectのスタティックSmartUpdate ZIPファイルをダウンロードします。 |
| 4. | Fortify WebInspectがインストールされているマシンで、ZIPファイルからすべてのファイルを解凍します。 |
| 5. | Fortify WebInspectを閉じます。 |
| 6. | 解凍したSecureBase.sdfファイルおよびversion.txtファイルを、SecureBaseデータがあるディレクトリにコピーします。 <ul style="list-style-type: none"> • システムがFIPSに対応していない場合、デフォルトの場所は次のとおりです。 <ul style="list-style-type: none"> • C:\ProgramData\HP\HP WebInspect\SecureBase |

| ステージ | 説明 |
|------|--|
| | <ul style="list-style-type: none"> • C:\ProgramData\HP\HP WebInspect\SecureBase • システムがFIPS対応の場合、場所は次のとおりです。 <ul style="list-style-type: none"> • C:\ProgramData\HP\HP WebInspect\FIPS\SecureBase • C:\ProgramData\HP\HP WebInspect\FIPS\SecureBase <p>ヒント: Windowsでは、デフォルトではこれらのフォルダは表示されません。フォルダオプションを変更して隠しファイルを表示してください。</p> |

WebSphere Portalに関するFAQ

WebSphere Portalでアプリケーションが実行されているかどうかをどのように確認できますか?

通常、WebSphere PortalアプリケーションのURLは非常に長く、/wps/portalまたは/wps/myportalで始まり、その後にエンコードされたセクションが続きます。次に例を示します。

`http://myhost.com/wps/portal/internet/customers/home/!ut/p/b1/fY7BcoIwFAC_xS94T4QCx6Rpk6qlo20x5tIJShEIJoID0q-vnfFq97Yze1hQIEEdV8W-1zaozZ_rh6-HjkRfrhERBZ4-EKESBmde5ggzEEVxmbXNGW7-sIsKdgTW3c_B3xmpzBfnacLv6QuIfxVHKJGhmNfzToue8nWdKg4fx8jtaT9MJpB2zQPgqlp9GrADyey0tvvL1F95nftm_y0cbuw8Xbmvg2NN6412w1sQP27GAa3A09AEBJhmxxcnlWh1k8kverBIBQ!!/d14/d5/L2dBISEvZ0FBIS9nQSEh/`

サポートされているWebSphere Portalのバージョンを教えてください。

バージョン6.1以降がサポートされています。

Fortify WebInspectでWebSphere Portalアプリケーションをスキャンするために特別な設定が必要な理由は何ですか?

URLのエンコードセクションには、「ナビゲーション状態」が含まれています。これは、現在のページで要素を表示する方法に関する情報(.NetのVIEWSTATEに似ています)と、ナビゲーション履歴です。このナビゲーション履歴は、自動Web探索プログラムを使用するときに問題となります。Web探索プログラムが各リンクにアクセスすると、ナビゲーション状態が更新されます。これにより、Web探索プログラムがすでにアクセスした可能性のあるページ上のリンクが継続的に変化します。新しいリンクのように見えるので、Web探索プログラムはこれらのリンクにアクセスします。このようにして動作が無限に循環することになります。

WebSphere Portalオーバーレイが選択されている場合、Fortify WebInspectはURLのナビゲーション状態をデコードし、URLがすでにアクセス済みかどうかを判断できます。これにより、Web探索プログラムが同じページを何度も続けてアクセスすることが防げます。

Fortify WebInspectはナビゲーション状態をどのようにデコードしますか?

WebSphere Portal 6.1以降には、URLデコードサービスが含まれています。WebSphere Portalオーバーレイが選択されている場合、Fortify WebInspectはURLをデコードサービスに

渡し、応答を評価してこのURLがすでにアクセス済みであるかどうかを判断できます。デコードサービスはデフォルトでオンになっていますが、WebSphere Portalサーバの設定でオフにするともできます。Fortify WebInspectでサイトを適切にスキャンできるようにするには、デコードサービスを有効にする必要があります。

ナビゲーション状態とは特別なセッションIDでしょうか?

いいえ。ナビゲーション状態には、セッション情報は含まれていません。セッションはクッキーにより維持されます。

ログインマクロを記録する際の特別な手順はありますか?

クッキーJSESSIONIDおよびLtpaTokenを状態パラメータとして設定するようにしてください。

サイトツリーに深くネストされたフォルダが含まれているのはなぜですか?

現時点では、Fortify WebInspectのサイトツリーは、WebSphere Portal URLのナビゲーション状態を解析する方法を認識しません。各セクションはディレクトリとして扱われます。もちろん、これらは実際にはディレクトリではありません。通常、各プランチの最下位レベルにドリルダウンして、実際のコンテンツを確認する必要があります。

Fortify WebInspectがWebSphere Portalアプリケーションに対して実行できる攻撃のタイプに制限はありますか?

Fortify WebInspectは、WebSphere Portalアプリケーションに対してすべての操作攻撃を実行できます。これには、XSS、SQLインジェクション、CSRF、RFI、LFIなどが含まれます(ただし、これだけには限定されません)。Fortify WebInspectは、WebSphere Portalサイトをスキャンするときにサイト検索攻撃を実行しません。これには、バックアップファイル(.bak、.old)、隠しファイル、隠しディレクトリ、およびプラットフォーム固有の環境設定ファイルの検索が含まれます。除外されている理由は、ほとんどの要求が、デフォルトのポータルビューに対して200応答を返す結果になり、エラー応答と有効な応答を区別する方法がないためです。

WebSphere PortalサイトでWeb探索プログラムが正しく動作しているかどうかをどのように確認できますか?

Web探索プログラムが最適な状態で動作できるようにするため、WebSphere Portalデコードサービスを有効にし、サーバ上で到達可能にする必要があります。動作しているかどうかを確認するには、URLを手動でデコードします。サイトからURLをコピーし、次のように変更します。

```
http://myhost.com/wps/poc?uri=state: path with navigation  
state>&mode=download
```

XML応答が返されます。あるいは、WebSphere Portalオーバーレイが選択されている状態でサイトのスキャンを開始します。Traffic Monitorを有効にするか、Web Proxy経由でスキャンを実行します。デコーダサービスに対する次の形式での周期的な要求が確認できます。

```
http://myhost.com/wps/poc?uri=state: path with navigation  
state>&mode=download.
```

もう1つ考慮すべき点は、デコードサービスのパスをサーバ上で変更できる点です。これが当てはまる場合は、スキャン設定を手動で変更する必要があります。サポートについては、Fortifyカスタマサポートにお問い合わせください。

ナビゲーション状態マーカーも変更できます。デフォルトではこれは!ut/pです。サーバでこれをデフォルトから変更した場合、スキャン設定を手動で変更する必要があります。サポートについては、Fortifyカスタマサポートにお問い合わせください。

詳細については、「["序文" ページ24](#)」を参照してください。

コマンドライン実行

Fortify WebInspectには、コマンドラインインターフェース(CLI)を通して使用できる次のアプリケーションが含まれています。

- WI.exe -既存のマクロを使用するスキャンの設定と実行、スキャンファイルとレポートのエクスポート、スキャンのマージ、スキャンの再利用、既存のスキャンのログインマクロのテストができます。詳細については、「["WI.exeの使用" 次のページ](#)」を参照してください。
- WIScanStopper.exe -現在実行中のスキャンを停止することができます。詳細については、「["WIScanStopper.exeの使用" ページ320](#)」を参照してください。
- MacroGenServer.exe -ログインマクロを作成することができます。詳細については、「["MacroGenServer.exeの使用" ページ321](#)」を参照してください。

これらのアプリケーションは、Fortify WebInspectと同じディレクトリにインストールされます。デフォルトで、インストールディレクトリは次のとおりです。

C:\Program Files\Fortify\Fortify WebInspect

CLIの起動

CLIを起動するには:

- Windowsのコマンドプロンプト(cmd.exe)アプリケーションを右クリックし、**管理者として実行**を選択します。
管理者:コマンドプロンプト] ウィンドウが表示されます。

重要! コマンドプロンプトで、cdコマンドを使用して現在の作業ディレクトリをアプリケーションがインストールされているディレクトリに変更します。

Fortify WebInspect on DockerのCLI制限

コマンドラインインターフェースからアクセス可能な一部のパラメータと機能は、Fortify WebInspect on Dockerでサポートされていません。サポートされていない項目は、そのように示されています。

WI.exeの使用

プログラムWI.exeを使用して、コマンドラインインターフェース(CLI)で各種のFortify WebInspect機能を開始できます。コマンドを入力するときには次の構文を使用します。

```
wi.exe -u url [-api type] [-s file] [-ws file] [-Framework name] [-CrawlCoverage name] [-ps policyID | -pc path] [-ab|ac|an|ad|aa|ak|at creds] [-macro path] [-o|c] [-n name] [-e[abcdefghijklmnpst] file] [-x|xd|xa|xn] [-b filepath] [-db] [-d filepath -m filename] [-i[erxd] scanid | -ic scanid scanname | -im option scanid scanlist] [-r report_name -y report_type -w report_favorite -f report_export_file -g[phacxe] [-t compliance_template_file] [-v] [-?]
```

コマンドラインから複数のスキャンを実行するには、次のような形式でバッチファイルを作成して実行します。

```
c:
cd \program files\Fortify\Fortify WebInspect
wi.exe -u http://172.16.60.19 -ps 4
wi.exe -u http://www.mywebsite.com
wi.exe -u http://172.16.60.17
wi.exe -u http://172.16.60.16
```

オプション

次の表に、オプションの定義を示します。斜体で表示されている項目には値が必要です。

| カテゴリ | オプション | 定義 |
|------|----------|---|
| 全般 | -? | 使い方のヘルプを表示します。 |
| | -u {url} | <p>開始URLまたはIPアドレスを指定します。</p> <p>注意! -uパラメータを-s (設定ファイル)と一緒に使用する場合には、必要に応じて-x、-xa、-xd、または-xnパラメータを指定して、スキャンをフォルダに限定します。このように限定しないと、一定の条件下では無制限の監査が実行されることがあります。</p> <p>URLにアンパサンド(&)が含まれている場合は、URLを引用符で</p> |

| カテゴリ | オプション | 定義 |
|------|----------------|---|
| | | 囲む必要があります。 |
| | -api {type} | <p>スキャンするAPIタイプを指定します。 <i>type</i>の有効な値は次のとおりです。</p> <p>Swagger OData</p> <p>重要!次の例に示すように、SwaggerまたはOData定義ファイルのURLを指定する必要があります。</p> <pre>-u http://172.16.81.36/v1 -api Swagger</pre> |
| | -s {filename} | <p>設定ファイルを指定します。</p> <p>メモ: コマンドラインパラメータは、設定ファイルの値よりも優先されます。</p> |
| | -db | 設定ファイルで定義されているデータベースを使用することを指定します。省略すると、Fortify WebInspectではアプリケーション設定に定義されているデータベース接続がデフォルトで使用されます。 |
| | -ws {filename} | 使用するWebサービス設計ファイルを指定します。 |
| | -o | 監査専用スキャンを指定します。 |
| | -c | Web探索専用スキャンを指定します。 |
| | -n {name} | スキャン名を指定します。 |
| | -b {filepath} | 使用するSecureBaseファイルを指定します。パスには、フルパスとファイル名を指定します。 |
| | -d {filepath} | 指定したファイルパスにデータベースを |

| カテゴリ | オプション | 定義 |
|------------|-----------------------------|--|
| | | 移動します。 |
| | -m {filename} | 指定したファイル名にデータベースを移動します。 |
| | -v | 詳細出力を作成します。 |
| | -l | テレメトリデータの収集を無効にします(このスキャンのみ)。 |
| | -ie {scanid} | 指定したスキャンID (GUID)の設定済みスキャンを開始します。 |
| | -ir {scanid} | 指定したスキャンID (GUID)のスキャンを再開します。 |
| | -ix {scanid} | 指定したスキャンID (GUID)の既存スキャンを使用しますが、スキャンは続行されません。 |
| | -id {scanid} | 指定したスキャンID (GUID)のスキャンを削除します。 |
| | -ii {scanid} {file path} | スキャンをインポートします。 メモ: このパラメータは、Fortify WebInspect Dockerではサポートされていません。 |
| ルートフォルダに限定 | -x | スキャンをディレクトリのみ(自己)に限定します。 |
| | -xa | スキャンをディレクトリと親(先祖)に限定します。 |
| | -xd | スキャンをディレクトリとサブディレクトリ(子孫)に限定します。 |
| | -xn | 参照されている設定ファイルの「フォルダに限定」ルールを無視します。 フォルダに限定パラメータ(x xa xb xn)は、独自のカテゴリに含めることができます(レポートまたは出力として)。 |

| カテゴリ | オプション | 定義 |
|-------------|--|---|
| フレームワーク | <code>-framework {framework_name}</code> | フレームワークの名前を指定します。現在サポートされているのはOracle ADF Faces (Oracle)およびIBM WebSphere Portal (WebSpherePortal)のみです。いずれかのテクノロジを使用して構築されたアプリケーションのスキャンを最適化します。 |
| Web探索のカバレッジ | <code>-CrawlCoverage {Coveragename}</code> | スキャンのカバレッジのタイプを指定します。 <i>Coveragename</i> の値は次のとおりです。 Thorough = サイト全体を対象とした徹底的なWeb探索 Default = パフォーマンスよりもカバレッジに重点を置く Moderate = カバレッジと速度のバランスをとる Quick = 範囲とパフォーマンスに重点を置く |
| 監査ポリシー | <code>-ps {policy id}</code> | 使用する非カスタムポリシーを指定します。 <i>policy id</i> の値は次のとおりです。 ベストプラクティス 1 = 標準 1012 = OWASP Top 10 アプリケーションセキュリティリスク2013 1024 = SANS Top 25 2011 1025 = OWASP Top 10 2017 1027 = 一般データ保護規制 (GDPR) 1034 = DISA-STIGV4R9 1036 = DISA-STIGV4R10 1037 = CWE Top 25 1041 = OWASP Application Security Verification Standard (ASVS) 1043 = DISA-STIGV4R11 1044 = API |

| カテゴリ | オプション | 定義 |
|------|-------|--|
| | | <p>1045 = DISA-STIGV5R1 1046 = NIST-SP80053R5 1047 = CWE Top 25 2020</p> <p>タイプ別</p> <p>3 = SOAP 7 = ブランク 1001 = SQLインジェクション 1002 = クロスサイトスクリプティング 1005 = パッシブ 1008 = 重大 および 高 の 脆弱性 1010 = アグレッシブSQLインジェクション 1011 = NoSQLおよび Node.js 1013 = モバイル 1015 = Apache Struts 1016 = トランスポート層セキュリティ 1020 = 権限のエスカレーション 1021 = サーバサイド 1022 = クライアントサイド 1026 = DISA-STIG-V4R4 1029 = DISA-STIG-V4R5 1030 = DISA-STIG-V4R6 1031 = DISA-STIG-V4R7 1032 = DISA-STIGV4R8 1033 = WebSocket 1035 = PCI Software Security Framework 1.0 (PCI SSF 1.0)</p> <p>非推奨</p> <p>2 = 攻撃(非推奨) 4 = クイック(非推奨) 5 = セーフ(非推奨) 6 = 開発(非推奨) 16 = QA(非推奨) 17 = アプリケーション(非推奨) 18 = プラットフォーム(非推奨) 1009 = OWASP Top 10アプリケーションセキュリティリスク2010(非推奨) 1014 = OpenSSL Heartbleed(非推奨)</p> |

| カテゴリ | オプション | 定義 |
|------|----------------------|---|
| | | <p>1018 =標準(非推奨) 1019 =非推奨のチェック</p> <p>危険 1004 =全 チェック</p> |
| | -pc {policy path} | 使用するカスタムポリシーを指定します。パスには、フルパスとファイル名を指定します(例: C:\MyPolicies\MyCustomPolicy.policy)。 |
| 認証 | -ab "userid:pwd" | 基本モード(ユーザ名とパスワード)を指定します。 |
| | -ac "userid:pwd" | ADFS CBTモード(ユーザ名とパスワード)を指定します。 |
| | -an "userid:pwd" | NTLMモード(ユーザ名とパスワード)を指定します。 |
| | -ad "userid:pwd" | ダイジェストモード(ユーザ名とパスワード)を指定します。 |
| | -aa "userid:pwd" | 自動モード(ユーザ名とパスワード)を指定します。 |
| | -ak "userid:pwd" | Kerberosモード(ユーザ名とパスワード)を指定します。 |
| | -am {macro path} | 非推奨。-macroオプションを使用してください。 |
| | -at "{type} {token}" | <p>APIスキャンの認証モード(typeおよびtoken)を指定します。次に例を示します。</p> <p>-at "Basic YWxh0GRpbjpvcGVuc2VzYW1l"</p> <p>typeの認証モードは次のとおりです。</p> <p>Basic Bearer Digest</p> |

| カテゴリ | オプション | 定義 |
|------------------|--|--|
| | | HOBA Mutual Negotiate OAuth SCRAM-SHA-1 SCRAM-SHA-256 vapid <p>メモ: typeおよびtokenは、前に示したように二重引用符で囲む必要があります。</p> |
| マクロ | -macro {macro path} | Webマクロ認証のマクロ名とディレクトリパスを指定します。 |
| | -macro {url} {username} {password} | 認証用の自動生成マクロを作成します。 |
| ログインマクロ パラメータ | -ls "userid:pwd" | SmartCredentialsのユーザ名とパスワードを指定された値に置き換えます。 |
| | -lt "name0:value0;name1:value1; ...nameN:valueN" | 指定した名前に一致する既存のTruClientログインパラメータを置き換えます。 |
| 出力 | -ea {filepath} | スキャンを従来の完全なXML形式でエクスポートします。 |
| | -eb {filepath} | スキャンの詳細(完全)を従来のXML形式でエクスポートします。 |
| | -ec {filepath} | スキャンの詳細(コメント)を従来のXML形式でエクスポートします。 |
| | -ed {filepath} | スキャンの詳細(非表示フィールド)を従来のXML形式でエクスポートします。 |
| | -ee {filepath} | スキャンの詳細(スクリプト)を従来のXML形式でエクスポートします。 |
| | -ef {filepath} | スキャンの詳細(設定されているクッキー)を従来のXML形式でエクスポートします。 |

| カテゴリ | オプション | 定義 |
|------|-------------------------|--|
| | | トします。 |
| | -eg {filepath} | スキャンの詳細 (Webフォーム)を従来のXML形式でエクスポートします。 |
| | -eh {filepath} | スキャンの詳細 (URL)を従来のXML形式でエクスポートします。 |
| | -ei {filepath} | スキャンの詳細 (要求)を従来のXML形式でエクスポートします。 |
| | -ej {filepath} | スキャンの詳細 (セッション)を従来のXML形式でエクスポートします。 |
| | -ek {filepath} | スキャンの詳細 (電子メール)を従来のXML形式でエクスポートします。 |
| | -el {filepath} | スキャンの詳細 (パラメータ)を従来のXML形式でエクスポートします。 |
| | -em {filepath} | スキャンの詳細 (Webダンプ)を従来のXML形式でエクスポートします。 |
| | -en {filepath} | スキャンの詳細 (サイト外リンク)を従来のXML形式でエクスポートします。 |
| | -eo {filepath} | スキャンの詳細 (脆弱性)を従来のXML形式でエクスポートします。 |
| | -ep {filepath} | 指定したファイルにスキャンをFPR形式でエクスポートします。 |
| | -eq {format} {filepath} | スキャンの詳細をサイトツリーからエクスポートします。詳細は次のとおりです。 <ul style="list-style-type: none">要求が送信された日時 (ミリ秒単位)ホストパスメソッドステータスコード要求から応答までの間の経過時 |

| カテゴリ | オプション | 定義 |
|------|----------------|--|
| | | <p>間(ミリ秒 単位)</p> <p>SPA (シングルページアプリケーション)スキャンの場合:</p> <ul style="list-style-type: none"> CSV形式では、SPADisplayName列とSPASelector列が含まれます。 JSON形式では、SPADisplayNameおよびSPASelectorデータを含むSPAイベントが含まれます。 <p>詳細については、「"SPAカバレッジ (SPA Coverage)" ページ72」を参照してください。</p> <p>formatの値は次のとおりです。</p> <p>json csv</p> <p>エクスポートする値に二重引用符が含まれている場合は、エスケープ文字(二重引用符)がCSV出力に追加されます。たとえば、セレクタ"Sign in"には二重引用符が含まれているので、CSVファイルには次のように表示されます。</p> <pre>//a[normalize-space(string(.))="Sign in"]</pre> <p>ヒント: このオプションを、-ie、-ir、-ix、またはいずれかのスキャン開始オプションと組み合わせて、データを取得するスキャンを指定します。次に例を示します。</p> <pre>-ix {scan GUID} -eq {format} {filepath}</pre> |
| | -es {filepath} | 指定したファイルにスキャンを.scan形式 |

| カテゴリ | オプション | 定義 |
|------|---|--|
| | | 式でエクスポートします。 |
| | -et {filepath} | 指定したファイルにスキャンとログを.scan形式でエクスポートします。 |
| | -eu {filepath} | 他のすべての上書きを適用した後、指定したファイルにスキャン設定をエクスポートします。 |
| | | メモ: このパラメータではスキャンは実行されません。設定がエクスポートされ、終了します。 |
| レポート | <p>- r {report_name}</p> <p>複数のレポートを指定する場合は、レポート名をセミコロンで区切ります。すべてのレポートは1つのファイルにまとめられます。</p> | <p>実行するレポートの名前を指定します。report_nameの有効な値を次に示します。</p> <p>Aggregate Alert View Attack Status Compliance Crawled URLs Developer Reference Duplicates Executive Summary False Positive QA Summary Scan Difference Scan Log Trend Vulnerability Vulnerability (Legacy)</p> <p>メモ: スペースを含むレポート名は引用符で囲む必要があります。</p> |
| | -w {favorite_name} | 実行するレポートのお気に入りの名前を指定します。 |
| | -ag | レポートのお気に入りのレポートを集約します。 |
| | -y {report_type} | レポートのタイプ(StandardまたはCustom)を指定します。 |

| カテゴリ | オプション | 定義 |
|----------|---|--|
| | -f {export_file} | レポートを保存するファイルのパスとファイル名を指定します。 |
| | -gp | PDF (Portable Document Format) ファイルとしてエクスポートします。 |
| | -gh | HTMLファイルとしてエクスポートします。 |
| | -ga | 生のレポートファイルとしてエクスポートします。 |
| | -gc | RTF (リッチテキスト形式) ファイルとしてエクスポートします。 |
| | -gx | テキストファイルとしてエクスポートします。 |
| | -ge | Excelファイルとしてエクスポートします。 |
| | -t {filepath} | 使用するコンプライアンスエンプレートファイルを指定します。 |
| スキャンのマージ | -ic {scan id} {scan name} | <p>マージターゲットスキャンを作成します。詳細については、このトピックの「"スキャンのマージ" ページ319」を参照してください。</p> <p>メモ: このパラメータは、Fortify WebInspect Dockerではサポートされていません。</p> |
| | -im /o:{option} {merge target scan id} {source scan id1} {source scan id2} | <p>スキャンをマージします。詳細については、このトピックの「"スキャンのマージ" ページ319」を参照してください。<i>option</i>の選択肢は次のとおりです。</p> <ul style="list-style-type: none"> Replace -ターゲットセッションおよび脆弱性をソースセッションおよび脆弱性に置き換えます。 ReplaceMergeVulns -ターゲットセッションをソースセッションに置き換 |

| カテゴリ | オプション | 定義 |
|----------|---|---|
| | | <p>え、ソース脆弱性をターゲットスキャンに追加します。</p> <ul style="list-style-type: none"> Skip -両方のスキャンでセッションIDが同じ場合は、セッションや脆弱性をマージしません。 SkipMergeVulns -両方のスキャンでセッションIDが同じ場合は、ターゲットセッションを置き換えず、ソースから脆弱性をコピーします。 Smart -マージ時にソースおよびターゲットのポリシーと時刻を考慮します。 <div style="background-color: #e0e0e0; padding: 5px; margin-top: 10px;"> 重要! <code>-im</code> パラメータを使用する前にマージターゲットスキャンを作成するには、<code>-ic</code> パラメータを使用します。 </div> <div style="background-color: #e0e0e0; padding: 5px; margin-top: 10px;"> メモ: このパラメータは、Fortify WebInspect Dockerではサポートされていません。 </div> |
| スキャンの再利用 | <code>-iz /o:{option}</code> <code>{source scan id}</code> <code>{settings filename}</code> | <p>スキャンの再利用の設定を作成します。<code>option</code>の選択肢は次のとおりです。</p> <ul style="list-style-type: none"> Incremental -ソーススキャンと同じ設定を使用し、変更されたポリシーを適用します。これは、ソーススキャンでフラグを設定したチェックを無効にし、1回だけフラグを設定するポリシーです。このモードでは、新しいWeb探索対象部分のみが監査されます。新しいWeb探索が実行されますが、新しいセッションのみが監査されます。 Remediation -ソーススキャンと同じ設定を使用し、変更されたポリシーを適用します。これは、ソーススキャンでフラグを設定しなかった |

| カテゴリ | オプション | 定義 |
|---------------|--|--|
| | | <p>チェックを無効にするポリシーです。</p> <p><i>settings filename</i>は、作成する変更済み設定ファイルの名前です。</p> <p>メモ: このパラメータは、Fortify WebInspect Dockerではサポートされていません。</p> |
| スキャン検出事項の再テスト | <pre>-iv <guid> {[<severity> <vuln ID prefix>] ...} /s <file path></pre> | <p>スキャンを開始して検出事項を再テストするときに使用できる設定ファイルを作成します。重大度または固有のsessionCheckFoundID (またはその両方)を使って検出事項を再テストできます。重大度もsessionCheckFoundIDも指定しない場合は、ベーススキャンのすべての検出事項が再テストされます。パラメータの構成要素は次のとおりです。</p> <ul style="list-style-type: none"> • <guid>はベーススキャンIDです。これは必須です。 • <severity>は、再テストする脆弱性の重大度です。一覧に指定されている重大度のフラグが付いている、ベーススキャンのすべての脆弱性が再テストされます。重大度のオプションはCritical、High、Low、およびMediumです。 • <vuln ID prefix>は固有のsessionCheckFoundIDであり、SessionCheckFounds APIエンドポイントを使用して取得できます。詳細については、「Fortify WebInspect REST API Swagger UI」を参照してください。 <p>ヒント: sessionCheckFoundIDのプレフィックスを指定できます。たとえば、012fは</p> |

| カテゴリ | オプション | 定義 |
|-------------|---|--|
| | | <p>sessionCheckFoundID 012fa34124と一致します。</p> <ul style="list-style-type: none"> /s <file path>は、作成される脆弱性再テスト設定ファイルのディレクトリパスとファイル名です。このパラメータは必須であり、再テストを指定するため元のスキャンの設定を変更します。作成される新しい設定ファイルでは、再テストされる脆弱性が指定されます。 <p>重大度とsessionCheckFoundIDを任意の順序で指定したリストを指定できます。次の例は、有効なリストを示しています。</p> <p>Critical 3156 High 1234</p> <p>メモ: この機能はテクノロジプレビューです。テクノロジプレビュー機能は現在サポートされていないため、完全に機能しない可能性があります。また、運用環境での展開には適しません。ただし、これらの機能は、将来的には完全なサポートを提供できることを目指すために広く拡大することを主な目的として、便宜的に提供されています。</p> |
| ログインマクロのテスト | -it {scan id} | 既存のスキャンのログインマクロをテストします。 |
| Seleniumマクロ | -selenium_workflow {ArrayOfSelenium Command object} | <p>Seleniumワークフロースキャンを作成します。</p> <p>このコマンドを使用する際の完全なプロセスと手順については、「Selenium WebDriverとの統合」 ページ340を参照してください。</p> |

| カテゴリ | オプション | 定義 |
|-------------|---|--|
| | <code>-selenium_no_validation</code> | <p>スキャンを実行する前にSeleniumコマンドの検証を無効にします。</p> <p>重要! このパラメータを使用する場合は、1つ以上の許可ホストを指定する必要があります。</p> <p>詳細については、「"Selenium WebDriverとの統合" ページ340」を参照してください。</p> |
| | <code>-s1m {SeleniumCommand object}または @"PathToFilewithobject"</code> | <p>スキャンのSeleniumログインマクロを指定します。このオプションは、要素が1つのArrayOfSeleniumCommand objectか、SeleniumCommand objectを使用します。</p> <p>SeleniumCommand objectまたはArrayOfSeleniumCommand objectを含むファイルのパスを指定するには、<code>@"PathToFilewithobject"</code>を使用します。</p> <p>「"Seleniumログインマクロの例" ページ319」を参照してください。</p> <p>重要! LogoutCondition要素が必要です。</p> |
| Postmanスキャン | <code>-pwc {filename}</code> | <p>Postmanコレクションファイルを使用してスキャンを開始します。このオプションでは、カンマで区切られた複数のコレクションファイルが受け入れられます。次に例を示します。</p> <p><code>-pwc pcOne,pcTwo,pcThree</code></p> <p>詳細については、「"Postmanコレクションによるスキャン" ページ331」を参照してください。</p> |
| | <code>-pdac</code> | Postmanの自動設定を無効にします。これによりPostmanコレクションの自動設定または分析がスキャンの |

| カテゴリ | オプション | 定義 |
|--------|--|---|
| | | 前に実行されなくなります。 |
| | -plc {Collection path} | Postmanログインコレクションのパスを指定します。 |
| | -pls "logoutsignature" | ログアウト条件を指定します。このパラメータでは正規表現の拡張が受け入れられます。 重要! スペース文字は\sに置き換える必要があります。 |
| | -pec {filename} | スキャンで使用するPostman環境ファイルを指定します。 |
| 状態管理 | -rs {<ArrayOfResponseStateElement>} or "@{filepath}" | 応答状態ルールを指定します。このパラメータは、ArrayOfResponseStateElement要素またはファイルに保存されている応答状態ルールを受け入れます。これはBearerトークンおよびAPIキーに使用されます。 重要! ファイルに保存されている応答状態ルールを使用するには、@記号を使用してファイルパスを指定する必要があります。 例については、「 応答状態ルールの例 次のページ」を参照してください。 |
| その他の設定 | -ah {url} [, {url}, ...] | 許可ホストを一覧にします。URLは、スキーマ、ホスト、およびポート番号です。 |

例

次の例は、WebInspectホームディレクトリから実行される場合と同様のコマンドライン実行を示しています。

```
wi.exe -u www.anywebsite.com -ps 1 -ab MyUsername:Mypassword
```

```
wi.exe -u https://zero.webappsecurity.com
-s c:\program files\webinspect\scans\scripted\
```

```
-r "Executive Summary";Vulnerability -y Standard  
-f c:\program files\webinspect\scans\scripted\zero051105.xml -gx
```

ポリシーを指定しない場合、Fortify WebInspectはWebサイトのWeb探索を実行します(しかし監査は行いません)。

無効なポリシー番号を指定すると、Fortify WebInspectはスキャンを実行しません。

Seleniumログインマクロの例

Seleniumログインマクロオプションの例を次に示します。

```
-slm "<SeleniumCommand><Command>wi command\"</Command>  
<AllowedHosts><string>http://hostname/</string>  
</AllowedHosts><LogoutCondition>Access\sDenied</LogoutCondition>  
</SeleniumCommand>"
```

応答状態ルールの例

応答状態ルールの例を次に示します。

```
-rs "<ArrayOfResponseStateElement><ResponseStateElement><name>  
AutoDetect</name><ReplaceRegexes><string>Authorization:\sBearer\s  
(?<AutoDetect>[^r\n]*\r\n)</string></ReplaceRegexes>  
<SearchRegexes><string>"en": ""(?<AutoDetect> [-a-zA-Z0-9._  
~+/]+?)?"$</string></SearchRegexes>  
</ResponseStateElement></ArrayOfResponseStateElement>"
```

ヒント: 応答状態ルールは、Fortify WebInspectユーザインターフェースの「スキャン設定: HTTP解析(Scan Settings: HTTP Parsing)」で作成できます。その後、スキャン設定XMLファイルを開き、ResponseStateElementを見つけてコピーし、-rsパラメータに貼り付けることができます。応答状態ルールの詳細については、「["スキャン設定: HTTP解析"ページ390](#)」を参照してください。

次のコードは、ファイルに保存されている応答状態ルールを使用してPostmanスキャンを開始する例を示しています。

```
wi -pwc c:\BearerWorkflow.json -pdac -plc c:\BearerLogin.json -rs  
@c:\BearerResponseStateRule.txt -pls
```

スキャンのマージ

メモ: この機能は、Fortify WebInspect on Dockerではサポートされていません。

既存のスキャンにマージすることはできません。最初に「ic」パラメータを使用してマージターゲットを作成する必要があります。

マージするスキャンはスキャン日 の順にソートされ、その順序でマージされます。2つのスキャンでセッションIDが同一 の場合には情報が失われるため、順序は重要です。この問題が発生した場合、デフォルトでは、前のセッションおよび脆弱性は後のセッションおよび脆弱性で上書きされます。マージ時にこの問題を防ぐには、同じセッションIDの処理に関する別のオプションを選択できます。

メモ: マージは、2つのスキャンで同一 のセッションIDが少 数であるかまたはまったくない場合に最も有効に機能します。

すべてのマージスキャンオプションでは、ソーススキャンの監査ステータスが「完了(Complete)」のセッションだけがマージされます。セッション除外(監査から除外)はマージされません。詳細については、「["監査設定:攻撃除外" ページ435](#)」を参照してください。

コマンドライン引数のハイフン

コマンドライン引数(出力ファイルなど)でハイフンを使用できるのは、次のコマンドの「エクスポートパス」引数に示すように、引数を二重引用符で囲んだ場合だけです。

```
wi.exe -u http://zero.webappsecurity.com -ea "c:\temp\command-line-test-export.xml"
```

メモ: プロセスは、タスクマネージャに表示されるWI.exeです。スキャンデータは一時的に作業ディレクトリにキャッシュされ、その後スキャンディレクトリに移動されます。

終了コード

WI.exeアプリケーションは、次の表に示す終了コードの1つを返します。

| コード | 説明 |
|---------|--------------------|
| 0 | コマンドはエラーなしで完了しました。 |
| -1または-3 | エラーが発生しました。 |

WIScanStopper.exeの使用

WIScanStopper.exeアプリケーションを使用して、現在実行中のスキャンを停止できます。

メモ: この機能は、Fortify WebInspect on Dockerではサポートされていません。

実行中のスキャンを停止するには、コマンドラインで次のコマンドを入力します。

```
WIScanStopper {scanid}
```

WIScanStopper.exeアプリケーションは、指定されたスキャンID (GUID)のスキャンを停止します。このアプリケーションは、次の表に示す終了コードの1つを返します。

| コード | 説明 |
|-----|---|
| 0 | スキャンは正常に停止しました。 |
| 1 | 指定された引数はGUIDではありません。有効なスキャンID (GUID)を使用してコマンドを再試行してください。 |
| 2 | 指定されたGUIDのスキャンがマシンで実行されていることが検出されませんでした。スキャンID (GUID)を検証し、コマンドを再試行してください。 |
| 3 | スキャンの停止を待機中にタイムアウトが発生しました。 タイムアウトは60秒です。停止コマンドが送信されると、プロセスはスキャンが停止するまで待機します。60秒経過してもスキャンステータスが変わらない場合は、タイムアウトが発生し、プロセスからこのコードが返されます。 |
| 4 | その他の例外が発生しました。 |

ヒント: -ir {scanid} パラメータを指定した WI.exe アプリケーションを使用して、停止したスキャンを再開できます。詳細については、「["オプション" ページ303](#)」を参照してください。

MacroGenServer.exeの使用

MacroGenServer.exe アプリケーションにより、コマンドラインインターフェース(CLI)で開始 URL、ユーザ名、およびパスワードを指定して、ログインマクロを作成できます。次のテキストは、CLI でこのアプリケーションを使用するためのサンプル構文を示しています。

```
macrogenserver.exe -u http://zero.webappsecurity.com/login.html -mu username  
-mp password
```

オプション

次の表で、使用可能なオプションを定義します。

| パラメータ | 定義 |
|-------|---|
| -u | 開始 URLを指定します。このパラメータは必須です。 |
| -mu | ログインフォームのユーザ名を指定します。このパラメータは必須です。 重要! ユーザ名に特殊文字が含まれている場合は、文字列を二重引用符で囲む必要があります。ユーザ名に二重引用符文字が含まれている場合は、エスケープ文字を使用して、引用符をユーザ |

| パラメータ | 定義 |
|-------|--|
| | 名の一部として渡す必要があります。エスケープ文字を判別するには、使用している特定のコマンドラインインターフェースのマニュアルを参照してください。 |
| -mp | ログインフォームのパスワードを指定します。このパラメータは必須です。 重要! パスワードに特殊文字が含まれている場合は、文字列を二重引用符で囲む必要があります。パスワードに二重引用符文字が含まれている場合は、エスケープ文字を使用して、引用符をパスワードの一部として渡す必要があります。エスケープ文字を判別するには、使用している特定のコマンドラインインターフェースのマニュアルを参照してください。 |
| -m | ログインマクロの保存先のファイルパスを指定します。 |
| -ps | プロキシサーバのIPアドレスまたはホスト名を指定します。 例: macrogenserver.exe -u http://zero.webappsecurity.com -mu username -mp password -ps 127.0.0.1 -pp 8080 macrogenserver.exe -u http://zero.webappsecurity.com -mu username -mp password -ps myproxyhostname -pp 8080 |
| -pp | プロキシサーバポートを識別します。 |
| -at | ネットワーク認証タイプを指定します。オプションを次に示します。 <ul style="list-style-type: none"> • Basic • Digest • Ntlm • ADFS_CBT |
| -au | ネットワーク認証のユーザ名を指定します。 |
| -ap | ネットワーク認証のパスワードを指定します。 |
| -h | MacroGenServerアプリケーションのヘルプを表示します。 |

正規表現

正規表現のパターンを作成する際には、特殊なメタ文字とシーケンスが使用されます。次の表に、これらの文字の一部を示し、その簡単な使用例を示します。推奨する他の参照先として「Regular Expression Library」(<http://regexlib.com/Default.aspx>)があります。

作成した正規表現の構文を確認するには、Regular Expression Editorを使用してください(システムにインストールされている場合)。

| 文字 | 説明 |
|-------|--|
| \ | 次の文字を特殊文字としてマークします。/n/は文字「n」に一致します。シーケンス\n/は、改行文字に一致します。 |
| ^ | 入力または行の先頭に一致します。 文字クラスとともに使用すると、否定文字を意味します。たとえば、contentディレクトリ内の/content/enおよび/content/caを除くすべてを除外するには、/content[^(en ca)].*/.*を使用します。\\S \\D \\Wも参照してください。 |
| \$ | 入力または行の末尾に一致します。 |
| * | 先行する文字の0回以上の反復と一致します。/zo*/は「z」とも「zoo」とも一致します。 |
| + | 先行する文字の1回以上の反復と一致します。/zo+/は「zoo」に一致しますが、「z」には一致しません。 |
| ? | 先行する文字の0回または1回の出現と一致します。/a?ve?/は「never」の「ve」に一致します。 |
| . | 改行文字を除く任意の1文字に一致します。 |
| [xyz] | 文字セット。括弧内の任意の1文字に一致します。/[abc]/は「plain」の「a」に一致します。 |
| \b | スペースなどの単語境界に一致します。/ea*\b/は、「never early」の「er」に一致します。 |
| \B | 非単語境界に一致します。/ea*\B/は「never early」の中の「ear」と一致します。 |
| \d | 1つの数字に一致します。[0-9]と同じです。 |
| \D | 数字以外の1文字に一致します。[^0-9]と同じです。 |

| 文字 | 説明 |
|----|---|
| \f | 改ページ文字に一致します。 |
| \n | 改行文字に一致します。 |
| \r | キャリッジリターン文字に一致します。 |
| \s | スペース、タブ、改ページなどの空白に一致します。[\f\n\r\t\v]と同じです。 |
| \S | 空白文字以外の文字に一致します。[^ \f\n\r\t\v]と同じです。 |
| \w | アンダースコアを含む任意の単語文字に一致します。[A-Za-z0-9_]と同じです。 |
| \W | 任意の非単語文字に一致します。[^A-Za-z0-9_]と同じです。 |

通常の正規表現構文に対する拡張もFortify WebInspectの開発者により作成および実装されています。詳細については、「["正規表現の拡張" 下](#)」を参照してください。

正規表現の拡張

通常の正規表現(regex)構文に対する拡張がFortifyのエンジニアにより開発および実装されています。正規表現を作成する場合は、以下で説明するタグと演算子を使用できます。

正規表現タグ

- [STATUSCODE]
- [BODY]
- [ALL]
- [URI]
- [HEADERS]
- [COOKIES]
- [STATUSLINE]
- [STATUSDESCRIPTION]
- [SETCOOKIES]
- [METHOD]
- [REQUESTLINE]
- [VERSION]
- [POSTDATA]
- [TEXT]

正規表現演算子

- AND
- OR
- NOT
- []
- ()

例

- (a)ステータス行にステータスコード「200」が含まれており、かつ(b)メッセージ本文のどこかに「logged out」という語句が含まれている応答を検出するには、次の正規表現を使用します。

```
[STATUSCODE]200 AND [BODY]logged\sout
```

- 要求されたリソースが一時的に別のURI(リダイレクト)に存在することを示しており、かつ応答のどこかにパス「/Login.asp」への参照が含まれる応答を検出するには、次の正規表現を使用します。

```
[STATUSCODE]302 AND [ALL]Login.asp
```

- (a)ステータスコードが「200」、かつ「logged out」または「session expired」という語句が本文のどこかに含まれている、または(b)ステータスコード「302」、かつ応答のどこかにパス「/Login.asp」への参照が含まれている応答のいずれかを検出するには、次の正規表現を使用します。

```
( [STATUSCODE]200 AND [BODY]logged\sout OR [BODY]session\sexpired ) OR  
( [STATUSCODE]302 AND [ALL]Login.asp )
```

メモ:「開き」括弧または「閉じ」括弧の前後にスペース(ASCII 32)を含める必要があります。そうしないと、括弧が誤って正規表現の一部と見なされます。

- リダイレクトLocationヘッダのどこかに「login.aspx」が現れるリダイレクト応答を検出するには、次の正規表現を使用します。

```
[STATUSCODE]302 AND [HEADERS]Location:\slogin.aspx
```

- ステータス行のReason-Phrase部に特定の文字列(「Please Authenticate」など)が含まれる応答を検出するには、次の正規表現を使用します。

```
[STATUSDESCRIPTION]Please\sAuthenticate
```

次も参照

["正規表現" ページ323](#)

Fortify WebInspect REST API

このトピックでは、Fortify WebInspect REST APIに関する情報を提供します。

Fortify WebInspect REST APIとは

Fortify WebInspect REST APIは、プロキシとスキーナをリモート制御するための、システムとFortify WebInspect間のRESTfulインターフェースを提供します。Fortify WebInspectのインストール時に自動的にインストールされる、軽量Windowsサービス(WebInspect APIと呼ばれる)として動作します。Fortify Monitorツールを使用して、サービスを設定、開始、および停止します。Fortify WebInspect REST APIを使用して、既存の自動化スクリプトにセキュリティ監査機能を追加できます。

Fortify WebInspect REST APIは、業界標準のSwagger RESTful API Documentation Specificationバージョン2.0(現在はOpenAPI Specificationとして知られている)を使用して完全に記述され、文書化されています。Swaggerのマニュアルに、REST APIの使用を簡素化するための詳細なスキーマ、パラメータ情報、およびサンプルコードが記載されています。また、エンドポイントを運用環境で使用する前にテストする機能も提供されます。

重要! SQL Expressデータベースを使用して複数のスキャンを実行する場合、SQL Expressの制限が原因で期待する結果を得られないことがあります。そのため、SQL Expressを使用するインストールでは、同時(または並行)スキャンの実行をお勧めしません。

Fortify WebInspect REST APIの設定

Fortify WebInspect REST APIを使用する前に、それを設定する必要があります。

1. Windowsの[スタート]メニューから、[すべてのプログラム]>[Fortify]>[Fortify WebInspect]>[Micro Focus Fortify Monitor]の順にクリックします。
Micro Focus Fortify Monitorアイコンがシステムトレイに表示されます。
2. [Micro Focus Fortify Monitor]アイコンを右クリックして、[WebInspect APIの設定 (Configure WebInspect API)]を選択します。
[WebInspect APIの設定 (Configure WebInspect API)]ダイアログボックスが表示されます。
3. 次の表の説明に従って、APIサーバの設定を行います。

| 設定 | 値 |
|-----|---|
| ホスト | Fortify WebInspectとFortify WebInspect REST APIの両方が同 |

| 設定 | 値 |
|------------------------|---|
| | じマシン上に存在する必要があります。デフォルト設定の [+]は、FortifyWebInspect REST APIに、[ポート(Port)]フィールドで指定されたポート上のすべての要求を傍受するように指示するワイルドカードです。同じポート上で別のサービスを実行しており、APIサービス専用の特定のホスト名を定義したい場合は、この値を変更できます。 |
| ポート | 指定された値を使用するか、上/下矢印を使用して使用可能なポート番号に変更します。 |
| 認証 (Authentication) | <p>認証(Authentication)]ドロップダウンリストから、なし(None)、Windows、基本(Basic)、またはクライアント証明書(Client Certificate)を選択します。</p> <p>認証に対して基本(Basic)を選択した場合は、ユーザ名とパスワードを指定する必要があります。これには次の操作を行います。</p> <ol style="list-style-type: none"> 「パスワードの編集(Edit passwords)]ボタンをクリックし、テキストエディタを選択します。 <p>wircserver.keysファイルがテキストエディタで開きます。このファイルには、サンプルのユーザ名とパスワードのエントリが含まれています。</p> <pre>username1:password1 username2:password2</pre> <ol style="list-style-type: none"> サンプルを、サーバにアクセスするためのユーザ資格情報で置き換えます。追加の資格情報が必要な場合は、認証するユーザごとにユーザ名とパスワードをコロンで区切って追加します。1行あたりのユーザ名とパスワードは1つずつにする必要があります。 ファイルを保存します。 <p>認証に対してクライアント証明書(Client Certificate)を選択した場合は、まず、信頼された認証局(CA)から発行されたルートSSL証明書に基づいてクライアント証明書を生成してから、クライアントマシンにインストールする必要があります。</p> <div style="background-color: #e0e0e0; padding: 5px;"> <p>ヒント: Windowsソフトウェア開発キット(SDK)のMakeCertユーティリティなどのツールを使用して、クライアント証明書を作成できます。</p> </div> |

| 設定 | 値 |
|---------------------------|--|
| Use HTTPS (HTTPSを使用する) | <p>HTTPS接続を介してサーバにアクセスする場合に、このチェックボックスをオンにします。</p> <p>HTTPSを介してサーバを実行するには、サーバ証明書を作成してAPIサービスにバインドする必要があります。HTTPSを介してAPIをテストする自己署名証明書を素早く作成するには、Administrator PowerShellコンソールで次のスクリプトを実行します。</p> <pre>\$rootcertID = (New-SelfSignedCertificate -DnsName "DO NOT TRUST - WIRC Test Root CA", "localhost", "\$(env:computername)" -CertStoreLocation "cert:\LocalMachine\My").Thumbprint \$rootcert = (Get-Item -Path "cert:\LocalMachine\My\\$(\$rootcertID)") \$trustedRootStore = (Get-Item -Path "cert:\LocalMachine\Root") \$trustedRootStore.open("ReadWrite") \$trustedRootStore.add(\$rootcert) \$trustedRootStore.close() netsh http add sslcert ipport=0.0.0.0:8443 certhash=\$(\$rootcertID) appid="{160e1003-0b46-47c2-a2bc-01ea1e49b9dc}"</pre> <p>前述のスクリプトは、ローカルホストの証明書とコンピュータ名を作成して、その証明書を個人用ストアとルート認証局に配置し、ポート8443にバインドします。別のポートを使用する場合は、スクリプトで使用されるポートを指定します。</p> <p>重要! 前述のスクリプトによって作成された自己署名証明書は、テストにのみ使用してください。この証明書はローカルマシンでのみ機能し、認証局からの証明書のセキュリティは提供しません。運用環境では、認証局によって生成された証明書を使用してください。</p> |
| ログレベル | <p>収集するログ情報のレベルを選択します。</p> <p>ヒント: APIログファイルは、Windowsイベントビューアを使用して表示できます。ログファイルは、[アプリケーションとサービスのログ](Applications and Services Logs)] > [WebInspect API]にあります。</p> |

4. 次のいずれかを実行します。

- Fortify WebInspect REST APIサービスを開始し、API設定をテストするには、[APIのテスト(Test API)]をクリックします。
サービスが開始され、ブラウザが開いて、Fortify WebInspect REST API Swagger UIページに移動します。このページの詳細については、「["Fortify WebInspect REST API Swagger UIへのアクセス" 下](#)」を参照してください。
- API設定をテストせずにFortify WebInspect REST APIサービスを開始するには、[開始(Start)]をクリックします。

Fortify WebInspect REST API Swagger UIへのアクセス

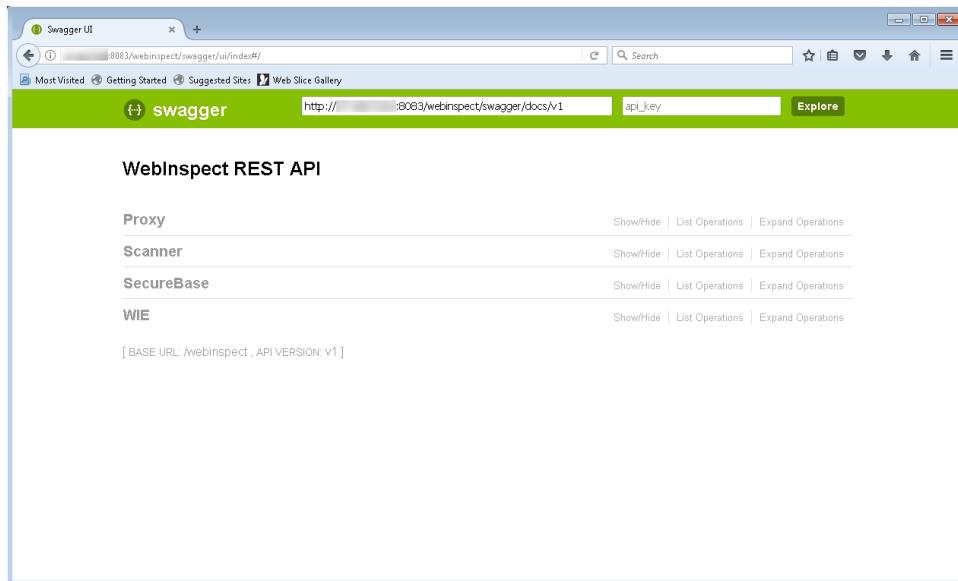
Fortify WebInspect REST API Swagger UIには、詳細なスキーマ、パラメータ情報、サンプルコード、およびエンドポイントのテスト機能を含む完全なマニュアルが付属しています。

この情報にアクセスするには:

1. Fortify WebInspect REST APIサービスを設定して起動したら、ブラウザを開きます。
2. アドレスフィールドに「`http://<hostname>:<port>/webinspect/api`」と入力し、<Enter>を押します。

例: Fortify WebInspect REST APIの設定時にデフォルト設定を使用した場合は、「`http://localhost:8083/webinspect/api`」と入力します。

WebInspect REST API Swagger UIページが表示されます。



Swagger UIの使用

Swagger UIを使用するには:

1. Swagger UIページで、エンドポイントカテゴリをクリックします。
2. 使用するエンドポイントメソッドをクリックします。

詳細なスキーマ、パラメータ情報、サンプルコード、およびエンドポイントのテスト機能が表示されます。

Swagger UI

8083/webinspect/swagger/ui/index#/WIE/WIE_Connection

Most Visited Getting Started Suggested Sites Web Slice Gallery

swagger http://:8083/webinspect/swagger/docs/v1 api_key Explore

WebInspect REST API

Proxy Show/Hide | List Operations | Expand Operations

Scanner Show/Hide | List Operations | Expand Operations

SecureBase Show/Hide | List Operations | Expand Operations

WIE Show/Hide | List Operations | Expand Operations

DELETE /wie/connection Release a WIE authorization token.

Implementation Notes: Release a WIE authorization token.

Response Class (Status 200): OK

Model: Example value: []

Response Content Type: application/json Try it out!

フィールドレベルの詳細の取得

一部のAPIエンドポイントには、設定可能な多数のフィールドがあります。これらのフィールドの詳細については、Swagger UIを参照してください。

フィールドレベルの詳細を表示するには:

- エンドポイントの「**パラメータ(Parameters)**」セクションで、**データ型(Data Type)**見出しの下の**モデル(Model)**をクリックします。

Parameters

| Parameter | Value | Description | Parameter Type | Data Type |
|-------------------|------------|---|----------------|---------------------|
| startScanSettings | (required) | Options used to start a scan. settingsName is required. overrides and reuseScan are optional. When reuseScan parameters are specified, settingsName should still be sent, but it is ignored and should be an empty value. In the scan reuse case the settings from the reused scan will be used. Overrides can be applied to reuse scan settings. | body | Model Example Value |

Parameter content type: application/json

Try it out!

すべてのエンドポイントフィールドの追加の詳細が表示されます。

| Parameters | | Description | Parameter Type | Data Type |
|------------------------------|-------|--|----------------|--|
| Parameter | Value | | | |
| startScanSettings (required) | | <p>Options used to start a scan.</p> <p><code>settingsName</code> is required. <code>overrides</code> and <code>reuseScan</code> are optional. When <code>reuseScan</code> parameters are specified, <code>settingsName</code> should still be sent, but it is ignored and should be an empty value. In the scan reuse case the settings from the reused scan will be used. Overrides can be applied to reuse scan settings.</p> | body | <p>Model Example Value</p> <pre>StartScanDescriptor { settingsName (string, optional), newSettingsName (string, optional), overrides (ScanSettingsOverrides, optional), reuseScan (ScanReuseOptions, optional), reuseFP (ReuseFalsePositives, optional), wise (WiseOptions, optional) } ScanSettingsOverrides { scanName (string, optional), startUrls (Array[string], optional), userAgent (UserAgentDescriptor, optional), webServiceScan (WebServiceScanDescriptor, optional), crawlAuditMode (string) = ['crawlOnly', 'auditOnly', 'crawlAndAudit'], crawlCoverageMode (string) = ['default', 'thorough', 'moderate', 'quick'], knownTechnology (KnownTechnologyDescriptor, optional), sharedThreads (integer, optional), crawlThreads (integer, optional), auditThreads (integer, optional), startOption (string) = ['url', 'macro'], loginMacroAutoGen (MacroGenDescriptor, optional), loginMacro (string, optional), workflowMacros (Array[string], optional), }</pre> |

Fortify WebInspectの自動化

Fortify WebInspect APIを使用して、既存の自動化スクリプトにFortify WebInspectを追加できます。ユーザエージェントがサービスルータにアクセスできる限り、スクリプトをFortify WebInspectとはまったく異なる環境に置くことができます。

Fortify WebInspectのアップデートとAPI

Fortify WebInspectをアップデートしたら、Fortify WebInspectユーザインターフェースを開いてからスキャンを開き、データベーススキーマの変更をスキャンデータベースに適用する必要があります。そうでない場合は、特定のAPIコマンドを実行するとエラーが表示される可能性があります。

Postmanコレクションによるスキャン

既存のPostman自動化テストスクリプト(コレクションとも呼ばれる)を使用して、REST APIアプリケーションのスキャンを実行できます。このトピックでは、Postmanおよび必要な追加のサードパーティソフトウェアに関する全般的な情報を提供します。

Postmanとは何か

PostmanはAPIの開発環境であり、APIの設計、協同、およびテストを実行できます。Postmanでは、API呼び出しのコレクションを作成することができ、各コレクションはサブフォルダおよび複数の要求に整理できます。コレクションをインポートおよびエクスポートできるため、開

発環境とテスト環境間でファイルを簡単に共有できます。NewmanなどのCollection Runnerを使用すると、テストを複数回反復して実行できるため、繰り返しテストに要する時間を短縮できます。

Postmanコレクションの利点

REST APIアプリケーションでは、ブラウザや自動ツールを操作する人間が使用できる形式ですべてのエンドポイントが公開されるわけではありません。多くの場合、特定の要求データのセットが指定されたさまざまなpost、put、およびgetを受け入れるエンドポイントのコレクションに過ぎません。これらのエンドポイントを正常に監査するには、APIに関する重要な詳細をFortify WebInspectが把握する必要があります。明確に定義されたPostmanコレクションでは、これらのエンドポイントを公開して、Fortify WebInspectでAPIアプリケーションを監査できるようにします。

Postman変数に関する既知の制限事項

Fortify WebInspectでは、Postmanのグローバル変数やデータ変数はサポートされていません。ただし、環境変数とコレクション変数、さらにコレクション内にあるローカル変数はサポートされています。

回避策として、グローバル変数とデータ変数を環境で指定できます。環境とは、Postman要求で使用できる変数のセットです。

Postmanスキャンのオプション

次のいずれかのオプションを使用して、Postmanスキャンを実行できます:

- APIスキャンウィザード(「["APIまたはWebサービススキャンの実行" ページ169](#)」を参照)
- WI.exeまたはFortify WebInspect REST API(「["WI.exeまたはWebInspect REST APIを使用したPostman APIスキャン" ページ338](#)」を参照)

Postmanの前提条件

Fortify WebInspectでスキャンを実行するには、Postmanコレクションバージョン2.0または2.1が必要です。さらに、NewmanコマンドラインCollection Runner、Node.js、およびNode Package Manager (NPM)をインストールする必要があります。特定のバージョン情報と追加の手順については、『*Micro Focus Fortify Software System Requirements*』を参照してください。

Postmanでのクライアント証明書の使用

Postmanスキャンの認証としてクライアント証明書を使用するには、証明書ファイル形式がWindowsでサポートされている必要があります。クライアント証明書がWindowsと互換性がない場合、証明書をWindowsと互換性のある形式に変換して、変換後のファイルをPostmanスキャンに使用できます。

次の表で、Postmanでクライアント証明書を変換および使用するプロセスについて説明します。

| ステージ | 説明 |
|------|--|
| 1. | OpenSSLなどのツールを使用して、証明書をWindows形式に変換します。 |
| 2. | Fortify WebInspectがインストールされているマシン上のWindows証明書ストアに、変換済みの証明書をインストールします。 |
| 3. | 【スキャン設定:認証(Scan Settings: Authentication)】に証明書を追加します。 詳細については、「 "スキャン設定:認証" ページ408 」を参照してください。 |

Postmanコレクションの準備のヒント

このトピックでは、優れたPostmanコレクションを作成するためのヒントを説明します。

有効な応答の確保

有効な応答を得るには、コレクションが完全で実行可能である必要があります。要求には次のものが含まれる必要があります:

- 有効な要求URL
- 正しいHTTPメソッド(POST、GET、PUT、PATCH、またはDELETE)
- APIを正しく実行するために必要な、有効なパラメータデータ
たとえば、「name」パラメータがある場合、デフォルトのデータ型「string」ではなく、「King Lear」または「Hamlet」のような実際のサンプルデータを指定する必要があります。

要求の順序

操作または要求の順序は重要であることに注意してください。たとえば、データに対してGET操作やDELETE操作を実行するには、事前にパラメータに対してサンプルデータを作成(またはPOST)する必要があります。

ヒント: Fortify WebInspectでコレクションの実行中にURLエラーが発生しないようにするには、コレクション内に正しい順序でAPI要求をバンドルした後、各要求をクリックしてから【保存(Save)】をクリックして、要求を個別に保存します。

認証の処理

APIで認証が必要な場合は、Postmanコレクションで設定する必要があります。認証を設定する場合は、次のガイドラインに従います:

- ユーザ資格情報は最新でなければならず、有効期限が切れていてはなりません。
- 環境を使用して認証情報を指定する場合は、Postmanコレクションで認証環境のタイプを選択します。
- コレクション内のすべての要求で認証が必要とは限らず、すべての要求で同じタイプの認証が必要であるとは限りません。ご使用のコレクションにこれが該当する場合は、コレクション内の各要求に適切な認証タイプを指定してください。

重要! スキャンでさまざまな認証タイプを使用中にセッション状態が失われた場合、正しく復元されません。セッション状態を適切に復元するには、単一の認証タイプでログインマクロまたはPostmanログインコレクションを使用します。

スタティック認証の使用

スタティック認証を使用する場合、Postmanコレクションでユーザ資格情報を名前と値のペアとしてハードコードする必要があります。Fortify WebInspectでは、コレクションファイルの解析時に、使用される認証タイプが判断され、コレクションからキーと名前と値が取得されます。その後、これらの値はスキャン設定に追加されます。

Fortify WebInspectでは、次のタイプのスタティック認証がサポートされています:

- APIキー
- 基本
- Bearerトークン
- ダイジェスト
- NTLM
- Oauth 1.0
- Oauth 2.0

ダイナミック認証の使用

ダイナミック認証を使用する場合、Bearerトークン認証変数またはAPIキー認証変数を、Postman環境ファイルまたはコレクションファイルのいずれかに保存する必要があります。たとえば、Bearerトークンでは{{bearerToken}}などの変数を使用できます。

応答状態ルールで正規表現を使用して、スキャン中にBearerトークンまたはAPIキーをダイナミックに指定する必要があります。応答状態ルールでは検索と置換のオプションが用意されており、トークンまたはキーを応答から取得して将来のセッションで使用することができます。詳細については、「["スキャン設定: HTTP解析" ページ390](#)」を参照してください。

Postmanログインマクロの使用

Fortify WebInspect REST APIまたはWi.exeで、Postmanコレクションファイルの形式のログインマクロとワークフローマクロを指定できます。たとえば、LoginBearer.jsonのようなログインマクロファイルを指定できます。ただし、ログインマクロを使用する場合は、正規表現The\stoken\sis\snot\svalidなどのログアウト条件も指定する必要があります。

Postmanの自動設定

スタティック認証の自動設定は、ユーザ名とパスワードがコレクションの認証セクションでハードコードされている場合など、認証値が既知の場合にサポートされています。自動設定が無効でない場合、Fortify WebInspectによってコレクションファイルの認証部分で有効な値が確認され、その値がスキャン設定に適用されます。

ダイナミック認証の自動設定では、ログインマクロと応答状態ルールの指定が自動的に試行されます。これは、BearerトークンまたはAPIキーが変数に保存されている場合に便利です。成功すると、Postmanコレクションの認証が検出されたことを示すメッセージが表示されます。Bearerトークンが検出されていても、安定した設定が作成されていない場合、自動設定に失敗したというメッセージが表示され、その理由が示されます。

重要! ダイナミック認証の自動設定は、Bearerトークン認証を使用する単純なケースでのみ機能します。

自動設定が失敗した場合は、認証を手動で設定する必要があります。詳細については、「["ダイナミックトークン用のPostmanログインの手動設定" 下](#)」を参照してください。

Postmanのサンプルスクリプト

Postman APIを活用するためのサンプルコードを<https://github.com/fortify/WebInspectAutomation>で入手できます。

PostmanコレクションのサンプルをGitHubのFortifyリポジトリ(<https://github.com/fortify/WebInspectAutomation/tree/master/PostmanSamples>)でダウンロードできます。

ダイナミックトークン用のPostmanログインの手動設定

このトピックでは、Postmanスキャンで自動設定が失敗した場合に、ダイナミック認証を手動で設定する方法について説明します。ダイナミック認証ではダイナミックトークンが使用されます。

ダイナミックトークンとは何か

ダイナミックトークンは、ソフトウェアによって生成される認証トークンであり、認証のインスタンスごとに固有です。トークンは短時間で作成でき、各インスタンスは個別に更新されます。

作業を開始する前に

手動ログインを設定するには、次の情報を把握している必要があります:

- アプリケーションで使用される認証のタイプ(Bearer、APIキー、OAuth 1.0、OAuth 2.0、クッキーなど)
- 正規表現の検索引数の作成方法

プロセスの概要

ログインを手動で設定するプロセスは、次の表のとおりです。

| ステージ | 説明 |
|------|---|
| 1. | 1つ以上のログイン要求を識別して、別々のPostmanコレクションに分離します。詳細については、「 "ログイン要求の識別と分離" 下 」を参照してください。 |
| 2. | ログアウト条件の正規表現を作成します。詳細については、「 "正規表現を使用したログアウト条件の作成" 下 」を参照してください。 |
| 3. | 応答状態ルールを作成します。詳細については、次を参照してください。 <ul style="list-style-type: none"> "Bearerトークンの応答状態ルールの作成" 次のページ "APIキーの応答状態ルールの作成" ページ338 <p>メモ: クッキーセッション管理では、応答状態ルールは必要ありません。</p> |

ログイン要求の識別と分離

ログイン要求を識別して分離するには:

- Postmanコレクションの内容を調べて、ログイン要求を識別します。

ヒント: 通常、ログイン要求はPostmanコレクションの最初の要求であり、認証トークンを取得するものです。ただし、認証には複数の要求が含まれる場合があります。

- この要求または複数の要求をコピーします。
- 要求を別々のファイルに貼り付けます。
- ファイルをPostmanコレクションとして保存します。

正規表現を使用したログアウト条件の作成

ログアウト条件を作成するには:

1. 認証を必要とする複数の要求を検索します。
2. 次のいずれかを実行します。
 - Bearerトークンの場合は、認証トークンを間違った値に置き換え、アプリケーションに送信する。
 - APIキーの場合は、アプリケーションに間違ったAPIKey値を送信する。
3. これらの要求からの応答を使用して、これらの応答に一致し、かつ有効なセッションと一致しない正規表現を作成します。

たとえば、ほとんどの場合に「unauthorized」という単語が表示される場合は、正規表現でその語を使用するのが最適です。次に例を示します。

```
[STATUSCODE]200 AND [BODY]unauthorized
```

間違ったAPIKey値を送信して、「{"status": "Access Deny"}」という応答が得られた場合、最適な正規表現は次のようなものかもしれません。

```
[BODY]Access\sDeny
```

Bearerトークンの応答状態ルールの作成

Bearerトークンの応答状態ルールを作成するには、2つの正規表現を作成する必要があります。

1つ目の正規表現では、すべての応答で認証トークンの更新を検索します。通常、このトークンは、プロセスのステージ1で識別されたログイン要求に対応するものです。

たとえば、次の応答には、「token」への参照があります。

```
{"success":true,"message":"Authentication  
successful!","token":"eyJhbGciOiJIUzI1NiIs  
InR5cCI6IkpXVCJ9.eyJ1c2VybmcFtZSI6ImFkbWluI  
iwiawF0IjoxNTg1NzQzNzkzLCJleHAiOjE1ODU3NDc  
z0TN9.i8uXa20JQt00t10jd1twRD76jTnsG-0xiU97 QWy6jkg"}
```

この応答に対して、次の正規表現を作成できます:

```
"token": "(?<Token>[-a-zA-Z0-9._~+/]+?=?)" }$
```

この正規表現では、(?<Token>[-a-zA-Z0-9._~+/]+?=?)によってトークンの値が識別されます。

メモ: XMLでは文字のエスケープが使用されます。XML形式で<および>を含む正規表現を使用する場合、<記号は<と>を使用してエスケープし、>記号は>を使用してエスケープします。

2つ目の正規表現で、このトークンを保存する場所を示します。Bearerトークンの場合、「Authorization: Bearer ...」ヘッダ内に配置されます。

Bearerトークンの例を次に示します:

```
"Authorization: \sBearer\s(?<Token>[^\\r\\n]*)\\r\\n"
```

この2つ目の正規表現では、1つ目の正規表現の値で置き換える値が(?<Token>[^\\r\\n]*))によって識別されます。

APIキーの応答状態ルールの作成

APIキーの応答状態ルールを作成するには、2つの正規表現を作成する必要があります。

1つ目の正規表現では、すべての応答で認証トークンの更新を検索します。通常、このトークンは、プロセスのステージ1で識別されたログイン要求に対応するものです。

たとえば、authのAPIキータイプのヘッダがあるとします。要求によって、ユーザ名とパスワードがパス「/Login」に送信され、次のような応答が返されます。

```
{"success":true,"APIToken": "tp8989ieupgrjynsfbnfgh9ysdopfghsprohjo"}
```

すべての保護された要求から、アクセスを承認するために「APIKey:」ヘッダが送信されます。

この応答に対して、次の正規表現を作成できます:

```
"APIToken": "(?<APIToken>[a-zA-Z0-9]+?)"}$
```

メモ: XMLでは文字のエスケープが使用されます。XML形式で<および>を含む正規表現を使用する場合、<記号は<とgt;を使用してエスケープし、>記号は>とlt;を使用してエスケープします。

2つ目の正規表現で、このトークンを保存する場所を示します。APIKeyの場合、カスタムヘッダの名前と値、またはカスタムクエリパラメータの名前と値を指定できます。

```
APIKey:\s(?<APIToken>[^\\r\\n]*)\\r\\n
```

Wi.exeまたはWebInspect REST APIを使用したPostman APIスキャン

このトピックでは、Fortify WebInspect REST APIまたはWi.exeでPostmanコレクションを使用してスキャンを実行するプロセスについて説明します。APIスキャンウィザードを使用してスキャンを実行するには、「["APIまたはWebサービススキャンの実行" ページ169](#)」を参照してください。

重要! Fortify WebInspectのREST API Postmanエンドポイントでは、SQL Expressを使用した並行スキャンの実行はサポートされていません。

プロセス

次の表で、Postmanコレクションを使用してスキャンを実行するプロセスについて説明します。

| ステージ | 説明 |
|------|---|
| 1. | <p>Postmanで次の操作を実行します:</p> <ol style="list-style-type: none"> このトピックでこれまでに説明したガイドラインに従って、Postmanコレクションファイルを作成します。 Postman内の各API呼び出しを個別に保存します。 「ランナ(Runner)」をクリックして、NewmanコマンドラインCollection Runnerを開きます。 |
| 2. | <p>NewmanコマンドラインCollection Runnerで次の操作を実行します:</p> <ol style="list-style-type: none"> Collection Runnerでコレクションを開いた状態で、API呼び出しが正しい実行順序であることを確認します。 「<Collection Name>を実行(Run <Collection Name>)」をクリックします。 各呼び出しからの応答を検査して、要求が成功したことを確認します。 |
| 3. | <p>Fortify WebInspectで次のいずれかを実行します:</p> <ul style="list-style-type: none"> Fortify WebInspect REST APIを使用するには: <ul style="list-style-type: none"> Fortify WebInspect APIを設定して起動します。「"Fortify WebInspect REST APIの設定" ページ326」を参照してください。 Swagger UIでPostman APIエンドポイントにアクセスします。「"Fortify WebInspect REST API Swagger UIへのアクセス" ページ329」を参照してください。 Swagger UIの指示に従ってエンドポイントを設定します。 Swagger UIまたは任意のAPIツールからエンドポイントサンプルスクリプトを実行します。 <p>重要! スキャン設定ファイルには、Postmanコレクション内のサイトへのアクセスを提供する適切な設定を含めます。たとえば、正しい許可ホスト、プロキシ設定などを含めます。設定ファイルを指定しない場合、Fortify WebInspectのデフォルトのスキャン設定がスキャンに適用されます。</p> Wi.exeを使用するには: <ul style="list-style-type: none"> 「"コマンドライン実行" ページ302」の説明に従って、CLIを起動します。 |

| ステージ | 説明 |
|------|--|
| | b. 「 "WI.exeの使用" ページ303 」で説明されているPostmanスキャンオプションを使用して、コマンドを作成します。 |
| 4. | エンドポイントまたはCLIコマンドによって、スキャンID (GUID)およびPostmanコレクションの結果が返されます。 |

Postmanスキャンのトラブルシューティング

Postmanコレクションを使用したスキャンの実行中に問題が発生した場合は、次のトラブルシューティングのヒントを使用します:

- スキャン設定でプロキシ設定を確認し、常にPostmanがプロキシ経由で実行され、テスト用のサイトにアクセスできるようにします。1つの方法として、プロキシ設定を使用して手動でNewmanを実行してみるという方法があります。
- 要求の結果を確認します。
 - 送信された要求の総数を表示して、Postmanファイル内の要求数と一致していることを確認します。
 - 失敗した要求がないことを確認します。

Selenium WebDriverとの統合

メモ: この機能はテクノロジプレビューです。テクノロジプレビュー機能は現在サポートされていないため、完全に機能しない可能性があります。また、運用環境での展開には適しません。ただし、これらの機能は、将来的には完全なサポートを提供できることを目指すために広く拡大することを主な目的として、便宜的に提供されています。

Fortify WebInspectをSelenium WebDriver (Selenium 2.0とも呼ばれる)と統合して、次の操作を実行できます。

- WI.exeコマンドラインツールを使用してスキャンを実行する
- Fortify WebInspect REST APIを使用してワークフローマクロを作成する

既知の制限事項

Fortify WebInspectをSelenium WebDriverを統合する場合の既知の制限事項は次のとおりです。

- Fortify WebInspectは、Selenium WebDriverのみをサポートしています。
- Fortify WebInspectは、RemoteWebDriverクラスなどのリモートサーバ設定を使用するSelenium WebDriverをサポートしていません。

- Selenium WebDriverマクロは、ワークフローマクロとしてのみ使用できます。ログインマクロまたは起動マクロとして使用することはできません。
- コマンドラインインターフェース(CLI)またはAPIからのみ、Selenium WebDriverマクロを使用してスキャンを開始できます。ユーザインターフェースからスキャンを開始することはできませんが、Selenium WebDriverマクロの再スキャンおよびインポート/エクスポートは可能です。
- Fortify WebInspect Enterpriseのサポートは限定的です。CLIまたはAPIから作成したマクロファイルを使用できますが、それはセンサマシン上でSelenium WebDriver環境のセットアップを完了した場合に限られます。

プロセスの概要

次の表では、Fortify WebInspectとSelenium WebDriverを統合するプロセスについて説明します。

| ステージ | 説明 |
|------|---|
| 1. | <p>Fortify WebInspectは、Fortify WebInspectプロキシを使用してWebブラウザからトラフィックをキャプチャできる必要があります。プロキシキャプチャを有効にするには、次のいずれかを実行します。</p> <ul style="list-style-type: none"> 「"Seleniumスクリプトへのプロキシの追加" 次のページ」の説明に従って、コード内で直接 Seleniumスクリプトにプロキシを追加するか、コマンドラインインターフェースのプレースホルダを使用してプロキシを追加します。 Firefoxを使用する場合は、「"Fortify WebInspect geckodriver.exeの使用" ページ346」の説明に従って、Fortify WebInspect geckodriver.exeを使用してトラフィックをキャプチャします。 |
| 2. | 「 "Selenium WebDriver環境のインストール" ページ346 」の説明に従って、Fortify WebInspectを実行しているマシンにSelenium WebDriver環境をインストールします。 |
| 3. | 「 "コマンドラインからのテスト" ページ346 」の説明に従って、コマンドラインから Selenium WebDriverスクリプトを起動し、許可ホストを定義できることを確認します。 |
| 4. | 必要に応じて、「 "Fortify WebInspectへのファイルのアップロード" ページ350 」の説明に従って、すべてのスクリプトとその依存関係をSelenium APIにアップロードするか、Fortify WebInspectを実行しているマシンに手動でコピーします。 |
| 5. | 「 "Seleniumコマンドの使用" ページ350 」の説明に従って、ステージ3のコマンドを使用し、WI.exeを使用してスキャンを実行するか、WebInspect REST APIを使用してマクロを作成します。 |
| 6. | 発生したエラーを修復します。 |

| ステージ | 説明 |
|------|---|
| | <p>WI.exeでスキャンを実行するか、APIでマクロを作成すると、マクロが検証されます。Seleniumコマンドごとにエラーと警告が返されます。この機能はデフォルトで有効になっています。無効にするには:</p> <ul style="list-style-type: none"> WI.exeで、引数 <code>-selenium_no_validation</code> パラメータを使用します。詳細については、「"WI.exeの使用" ページ303」を参照してください。 APIで、<code>VerifyMacro</code> パラメータを <code>false</code> に設定します。詳細については、「Fortify WebInspect REST API Swagger UI」を参照してください。 <p>問題をトラブルシューティングするには、スキャンログでエラーを確認し、<code>StateRequestor</code> ログで警告を確認します。</p> <p>ヒント: 通常、ログは次のディレクトリパスに書き込まれます。</p> <ul style="list-style-type: none"> デフォルトユーザであるSYSTEM USERでAPIスキャンが実行されている場合、ログは次の場所に書き込まれます。 <code>C:\ProgramData\HP\HP WebInspect\Scan\logs\<scan_guid>\ScanLog</code> <code>C:\ProgramData\HP\HP WebInspect\Scan\logs\<scan_guid>\StateRequestor</code> すべてのCLIおよびUIスキャンのログと、APIスキャンが現在のユーザで実行されている場合のログは、次の場所に書き込まれます。 <code>C:\Users\<user.name>\AppData\Local\HP\HP WebInspect\Logs\<scan_guid>\ScanLog</code> <code>C:\Users\<user.name>\AppData\Local\HP\HP WebInspect\Logs\<scan_guid>\StateRequestor</code> |

Seleniumスクリプトへのプロキシの追加

Webブラウザからのトラフィックをキャプチャするこの方法を使用するには、Selenium初期化にプロキシを適用するFortifyコードを自分のコードの中に直接追加するか、該当する場合はコマンドラインインターフェース(CLI)で引数として渡します。

長所

Seleniumがサポートする任意のブラウザから実行できるため、このアプローチには柔軟性があります。さらに、この方法ではいくらかのアップグレードプロテクションが提供されます。Fortifyコードはスクリプト内に存在するため、コードを少し変更するだけで、今後のバージョンのSeleniumでも引き続き使用することができます。

短所

この方法では、ブラウザを正しく初期化するために、Fortify コードをスクリプトに一度手動で追加する必要があります。

サンプルコード

Fortify_WI_Proxyという名前の環境変数から値を取得し、それをWebブラウザと信頼証明書に対するHTTPおよびHTTPSのプロキシとして保存する必要があります。方法はプログラミング言語ごとに異なります。次のセクションでは、いくつかの言語のサンプルコードを示します。

メモ: これらのコードサンプルは、Selenium WebDriverバージョン3.14に基づいています。ご使用の特定のバージョン用のコードは異なる場合があります。

C#

C#コードでは、ブラウザドライバが初期化されている場所を見つけて、それにブラウザオプションを追加する必要があります。Chromeブラウザの例を次に示します。

```
ChromeOptions chromeOptions = new ChromeOptions(); string proxy = Environment.GetEnvironmentVariable("Fortify_WI_Proxy"); if (!String.IsNullOrEmpty(proxy)) { chromeOptions.AcceptInsecureCertificates = true; chromeOptions.Proxy = new Proxy(); chromeOptions.Proxy.HttpProxy = proxy; chromeOptions.Proxy.SslProxy = proxy; } ... new ChromeDriver(chromeOptions) // オプションはこのクラスに含める
```

Firefoxブラウザの例を次に示します。

```
FirefoxOptions config = new FirefoxOptions(); string proxy = Environment.GetEnvironmentVariable("Fortify_WI_Proxy"); if (!String.IsNullOrEmpty(proxy)) { config.AcceptInsecureCertificates = true; config.Proxy = new Proxy(); config.Proxy.HttpProxy = proxy; config.Proxy.SslProxy = proxy; } ... new FirefoxDriver(config)
```

Java

Javaコードでは、ブラウザドライバが初期化されている場所を見つけて、それにブラウザオプションを追加する必要があります。Chromeブラウザの例を次に示します。

```
ChromeOptions options = new ChromeOptions(); String wi_proxy = System.getenv("Fortify_WI_Proxy"); if (wi_proxy != null) { Proxy proxy = new Proxy(); proxy.setHttpProxy(wi_proxy); proxy.setSslProxy(wi_proxy); options.setProxy(proxy); options.setAcceptInsecureCerts(true); } ChromeDriver driver=new ChromeDriver(options);
```

Firefoxブラウザの例を次に示します。

```
FirefoxOptions options = new FirefoxOptions(); String wi_proxy =
System.getenv("Fortify_WI_Proxy"); if (wi_proxy != null) { Proxy proxy =
new Proxy(); proxy.setHttpProxy(wi_proxy); proxy.setSslProxy(wi_proxy);
options.setProxy(proxy); options.setAcceptInsecureCerts(true); }
FirefoxDriver driver=new FirefoxDriver(options);
```

JavaScript

JavaScriptコードでは、ブラウザドライバが初期化されている場所を見つけて、ブラウザオプションを追加する必要があります。Chromeブラウザの例を次に示します。

```
const selProxy = require('selenium-webdriver/proxy'); ..... (async function
example() { let env = process.env.Fortify_WI_Proxy; if (env) { let caps =
{ acceptInsecureCerts: true }; //すべての証明書の受諾を許可する let proxy = {
http: env, https: env }; // env変数をプロキシとして適用する driver = await new
Builder().withCapabilities(caps).setProxy (selProxy.manual
(proxy)).forBrowser('chrome').build(); // プロキシとacceptInsecureCertsを設定
する }else driver = await new Builder().forBrowser('chrome').build();
```

Firefoxブラウザの例を次に示します。

```
const selProxy = require('selenium-webdriver/proxy'); ..... let env =
process.env.Fortify_WI_Proxy; if (env) { let caps = { acceptInsecureCerts:
true }; //すべての証明書の受諾を許可する let proxy = { http: env, https: env
}; // env変数をプロキシとして適用する driver = await new Builder
().withCapabilities(caps).setProxy (selProxy.manual(proxy)).forBrowser
('firefox').build(); // プロキシとacceptInsecureCertsを設定する }else driver =
await new Builder().forBrowser('firefox').build();
```

Python

Pythonコードでは、ブラウザドライバが初期化されている場所を見つけて、それにブラウザオプションを追加する必要があります。Chromeブラウザの例を次に示します。

```
capabilities1 = DesiredCapabilities.CHROME.copy() Fortify = os.environ.get
('Fortify_WI_Proxy') if Fortify is not None: prox = Proxy() prox.proxy_
type = ProxyType.MANUAL prox.http_proxy = Fortify prox.ssl_proxy = Fortify
prox.add_to_capabilities(capabilities1) cls.driver = webdriver.Chrome
(executable_path='C:/chromedriver.exe', desired_
capabilities=capabilities1)
```

Firefoxブラウザの例を次に示します。

```
import os from selenium.webdriver import DesiredCapabilities from
selenium.webdriver.common.proxy import Proxy, ProxyType ..... capabilities1 =
DesiredCapabilities.FIREFOX.copy() Fortify = os.environ.get('Fortify_WI_
Proxy') if Fortify is not None: capabilities1['acceptInsecureCerts'] =
True prox = Proxy() prox.proxy_type = ProxyType.MANUAL prox.http_proxy =
Fortify prox.ssl_proxy = Fortify prox.add_to_capabilities(capabilities1)
cls.driver = webdriver.Firefox(executable_path='C:/geckodriver.exe',
capabilities=capabilities1)
```

Ruby

Rubyコードでは、ブラウザドライバが初期化されている場所を見つけて、それにブラウザオプションを追加する必要があります。Chromeブラウザの例を次に示します。

```
http_proxy = ENV['Fortify_WI_Proxy'] if http_proxy proxy =
Selenium::WebDriver::Proxy.new(http: http_proxy, ssl: http_proxy)
capabilities = Selenium::WebDriver::Remote::Capabilities.chrome (accept_
insecure_certs: true) capabilities.proxy = proxy; else capabilities =
Selenium::WebDriver::Remote::Capabilities.chrome() end driver =
Selenium::WebDriver.for :chrome, desired_capabilities: capabilities
```

Firefoxブラウザの例を次に示します。

```
http_proxy = ENV['Fortify_WI_Proxy'] if http_proxy proxy =
Selenium::WebDriver::Proxy.new(http: http_proxy, ssl: http_proxy)
capabilities = Selenium::WebDriver::Remote::Capabilities.firefox (accept_
insecure_certs: true) capabilities.proxy = proxy; else capabilities =
Selenium::WebDriver::Remote::Capabilities.firefox() end driver =
Selenium::WebDriver.for :firefox, desired_capabilities: capabilities
```

CLIの使用

スクリプトがプロキシを設定する引数を受け入れる場合は、この方法を使用してFortify WebInspectプロキシをスクリプトに追加できます。たとえば、-proxy "<host:port>"という名前の引数がある場合、次のように、実行時にコマンドでプレースホルダ{Fortify_WI_Proxy}を使用できます。

```
-proxy "{Fortify_WI_Proxy}"
```

ホストとポートを個別に指定する必要がある場合は、次のようにそれぞれに対してプレースホルダを使用できます。

```
-proxy "{Fortify_WI_Proxy_Host}:{Fortify_WI_Proxy_Port}"
```

これらの引数は、実行時にスクリプト内 のプレースホルダをFortify WebInspectプロキシに置き換えます。

Fortify WebInspect geckodriver.exeの使用

GeckoDriverは、W3C WebDriver互換のクライアントがGeckoベースのブラウザと通信できるようにするプロキシです。geckodriver.exeアプリケーションはFirefoxブラウザ用にこのプロキシを提供します。この方法でWebブラウザからのトラフィックをキャプチャするには、既存のgeckodriver.exeを、<InstallationDirectory>\ExtensionsフォルダにあるFortify WebInspect geckodriver.exeに置き換える必要があります。

メモ: デフォルトのインストールディレクトリはC:\Program Files\Fortify\Fortify WebInspect\Extensionsです。

長所

この方法では必要な作業が少なくなります。

短所

最新バージョンのgeckodriver.exeを使用できません。また、Firefoxスクリプトだけを使用する必要があります。

Selenium WebDriver環境のインストール

Fortify WebInspectがインストールされているマシンに、Seleniumスクリプトを実行するために必要なすべてのソフトウェアとツールをインストールする必要があります。これには次のものが含まれますが、これに限定されません。

- ブラウザ
- テストランナ
- Seleniumスクリプトの実行をサポートするために必要なすべての前提条件ソフトウェアたとえば、.NET NUnitフレームワークの場合、.NETと、Seleniumスクリプトを実行する実行可能ファイルとしてnunit3-console.exeをインストールする必要があります。

重要! 必要なソフトウェアとツールは、プログラミング言語によって異なります。

コマンドラインからのテスト

コマンドラインからSelenium Webdriverスクリプトを起動して実行できるようにするには、Seleniumスクリプトを実行するコマンドを作成して使用する必要があります。使用的するコマンドは、Seleniumテストの実行に使用するプログラミング言語およびテストフレームワークによって異なります。

たとえば、.NETで NUnitを実行するには、次のようなコマンドを実行できます。

```
D:\tmp\selenium_wd\bin\net35\nunit3-console.exe "D:\tmp\selenium_wd\selenium_c_sharp-master\Selenium\bin\Debug\Selenium.dll"
```

この例では、nunit3-console.exeはユニットテストランナであり、Selenium.dllはユニットテストが含まれているDLLです。その他の例については、「["Seleniumコマンドの作成" 下](#)」を参照してください。

ヒント: POST /configuration/selenium/folder および GET /configuration/selenium/file/{foldername} APIエンドポイントを使用して、展開したファイルのフルパスを表示できます。この情報を使用して、CLIのコマンドを更新できます。詳細については、「["Fortify WebInspectへのファイルのアップロード" ページ350](#)」を参照してください。

Seleniumコマンドの作成

Seleniumコマンドは、ユニットテストを実行するためにコマンドラインで使用します。ほとんどの場合、このコマンドはビルドサーバでのユニットテストの実行時またはデバッグ時に使用されます。このコマンドは、使用しているユニットテストフレームワークによって異なります。各フレームワークには専用のランナとコマンドライン引数があります。以降のセクションでは、さまざまな言語での各種フレームワークに関するヒントとサンプルコマンドについて説明します。

.NET MSTest

MSTestフレームワークは、vstest.console.exeというツールを次の構文で使用します。

```
<Path_to_Vstest_Executable>\Vstest.console.exe <Path_to_Unit_Test_dlls>\<TestFileNames> <Options>
```

ほとんどの場合、この実行可能ファイルを呼び出すときにはDLL(実行するテストファイル名)のリストを指定する必要があります。次のサンプルコードは、2つのテストファイルを実行します。

```
"C:\Program Files (x86)\Microsoft Visual Studio 14.0\Common7\IDE\Extensions\Microsoft\TestWindow\vstest.console.exe"
"C:\Projects\Tests\bin\TestHomepage_unittest.dll"
"C:\Projects\Tests\bin\AddCart_unittest.dll"
```

.NET NUnit

NUnitフレームワークは、nunit3-console.exeというツール(バージョン3.x)を次の構文で使用します。

```
NUNIT3-CONSOLE <InputFiles> <Options>
```

この実行可能ファイルを呼び出すときにはDLL(実行するテストファイル名)のリストを指定する必要があります。次のサンプルコードは、2つのテストファイルを実行します。

```
C:\nunit\net35\nunit3-console.exe "C:\Projects\Tests\bin\TestHomepage_unittest.dll" "C:\Projects\Tests\bin\AddCart_unittest.dll"
```

xUnit.net

xUnit.netフレームワークには、`xunit.console.exe`および`xunit.console.x86.exe`という2つのコマンドラインランナがあります。次の構文を使用します。

```
xunit.console <assemblyFile> [configFile] [assemblyFile [configFile]...]  
[options] [reporter] [resultFormat filename [...]]
```

xUnit.netでは環境設定ファイル(configFile)のファイル拡張子として.jsonおよび.xmlを使用できます。

該当する実行可能ファイルを呼び出すときには、DLL(実行するテストファイル名)のリストを指定する必要があります。次のサンプルコードは、2つのテストファイルを実行します。

```
C:\xunit\xunit.console.exe "C:\Projects\Tests\bin\TestHomepage_  
unittest.dll" "C:\Projects\Tests\bin\AddCart_unittest.dll"
```

Java TestNG

TestNGフレームワークには、クラスパス(-cp)オプションで指定した`testng.jar`ライブラリと、`java.exe`アプリケーションが必要です。-cpオプションに、プロジェクトを実行するために必要なすべてのライブラリクラスを一覧にする必要があります。次の構文を使用します。

```
java -cp "<Path_to_testngjar>/testng.jar:<Path_to_Test_Classes>"  
org.testng.TestNG <Path_to_Test_xml>
```

次のサンプルコードは、XMLテストファイルを実行します。

```
C:\Program Files\Java\jdk-12.0.1\bin\java.exe -cp ".\libs\:\ C:\Program  
Files\jbdevstudio4\studio\plugins\*" org.testng.TestNG testng.xml
```

Java JUnit

JUnitフレームワークには複数のバージョンがあり、バージョンごとに独自のテスト実行コマンドがあります。-cpオプションに、プロジェクトを実行するために必要なすべてのライブラリクラスを一覧にする必要があります。

JUnitバージョン5.xでは次の構文を使用します。

```
java -jar junit-platform-console-standalone-<version>.jar --class-path <Path_to_Compiled_Test_Classes> --scan-class-path
```

JUnitバージョン4.xでは次の構文を使用します。

```
java -cp .\libs\:<Path_to_Junitjar>\junit.jar org.junit.runner.JUnitCore  
[test class name]
```

JUnitバージョン3.xでは次の構文を使用します。

```
java -cp .\libs\:<Path_to_Junitjar>\junit.jar junit.textui.TestRunner [test  
class name]
```

次のサンプルコードは、テストクラスを実行します。

```
C:\Program Files\Java\jdk-12.0.1\bin\java -cp
  C\java\libs\*:C:\junit\junit.jar org.junit.runner.JUnitCore
  C:\project\test.class
```

Python unittestおよびPyUnit

Pythonには、ご使用のPythonのバージョンに応じてPython unittestまたはPyUnitという組み込みのユニットテストモジュールがあります(-m)。これらのフレームワークは、次の構文を使用します。

```
python -m unittest [options] [tests]
```

この構文の[tests]には、任意の数のテストモジュール、クラス、およびテストメソッドのリストを指定できます。次のコマンドは、Pythonのunittestのヘルプを表示します。

```
python -m unittest -h
```

次のサンプルコードは、unittestモジュールでtests.pyという名前のテストファイルを実行します。

```
C:\Python\Python37-32\python.exe -m unittest
  C:\SampleProjects\POMProjectDemo\Tests\tests.py
```

Ruby RSpec

RSpecフレームワークでは、Rubyコードのユニットテストライブラリが提供されます。このフレームワークは、次の構文を使用します。

```
<Path_to_RSpec>\rspec.bat [options] [files or directories]
```

次のサンプルコードは、テストライブラリを実行します。

```
C:\Ruby26-x64\bin\rspec.bat -I C:\Ruby26-x64\Project\lib\ C:\Ruby26-
  x64\Project\spec\calculator_spec.rb
```

JavaScript Jest

Jestでは、JavaScriptコードでテストを作成および実行するためのJavaScriptライブラリが提供されます。このフレームワークは、次の構文を使用します。

```
<Path_to_Jest>\jest.js [--config=<pathToConfigFile>] [TestPathPattern]
```

次のサンプルコードは、テストライブラリを実行します。

```
C:\Users\admin\AppData\Roaming\npm\jest.cmd" --
  config=C:\Users\admin\AppData\Roaming\npm\jest.config.js
  C:/Users/admin/AppData/Roaming/npm/sum.test.js
```

Fortify WebInspectへのファイルのアップロード

コマンドラインインターフェース(CLI)でスキャンを実行するか、APIを使用してマクロを作成するには、Fortify WebInspectがインストールされているマシンにすべてのスクリプトとその依存関係をアップロードする必要があります。

CLIの使用

CLIからスキャンを実行するには、Fortify WebInspectがインストールされているマシンにファイルを手動でコピーする必要があります。

APIの使用

Fortify WebInspect REST APIでは、これらのファイルを展開するための次のエンドポイントが提供されます。

- POST /configuration/selenium/folder - ZIPファイルをアップロードおよび圧縮解除する
- GET /configuration/selenium/folder - すでにアップロードされているZIPファイルのリストを取得する
- GET /configuration/selenium/file/{filename} - ZIPファイルに含まれているファイルのリストを取得する
- DELETE /configuration/selenium/folder/{filename} - ZIPファイルを削除する

これらのエンドポイントの使用に関する詳細については、Swagger UIの特定のエンドポイントメソッドを参照してください。詳細については、「["Fortify WebInspect REST API Swagger UIへのアクセス" ページ329](#)」を参照してください。

Seleniumコマンドの使用

Seleniumコマンドの作成とテストが完了したら、そのコマンドを使用して、WI.exeを使用してスキャンを実行するか、またはAPIを使用してマクロを作成することができます。

重要! Seleniumコマンドを使用してスキャンを実行すると、次のいずれかの場所にログディレクトリが作成されます。

C:\Users\<UserName>\AppData\Local\Temp\

C:\Windows\Temp (Fortify WebInspect REST APIがシステムユーザにより実行されている場合)

スキャンの実行中にgeckodriver.exeまたはchromedriver.exeプロセスを終了すると、これらの一時ファイルは削除されません。これらのファイルを手動で削除する必要があります。

WI.exeを使用したスキャンの実行

コマンドラインインターフェース(CLI)では、WI.exeに-selenium_workflowパラメータがあります。このパラメータは、ArrayOfSeleniumCommandというXMLオブジェクトをファイルまたは文字列とし

て受け入れます。

重要! コマンドをファイルではなく文字列として実行し、コマンドに二重引用符 ("") が含まれている場合、これを<Command>タグに入れて保存するときに、二重引用符をバックスラッシュ文字 (\) でエスケープする必要があります。たとえば、コマンドでパスに空白が含まれており、Command内で二重引用符を使用してこのパスを受け渡す場合、次のように引用符をエスケープする必要があります。

```
<Command>"C:\Program Files\nunit\nunit3-console.exe"  
C:\Projects\Tests\bin\TestHomepage_unittest.dll "C:\Projects\Tests  
Main\bin\AddCart_unittest.dll"</Command>
```

次の構文に従い、以前に作成したSeleniumコマンドをCommandタグに入れます。詳細については、「["Seleniumコマンドの作成" ページ347](#)」を参照してください。

```
<ArrayOfSeleniumCommand> <SeleniumCommand> <Command>"Commands"</Command>  
<AllowedHosts> <string>http://hostname</string> </AllowedHosts>  
<WorkingDirectory>C:\path to project folder\</WorkingDirectory>  
</SeleniumCommand> <SeleniumCommand> ... </SeleniumCommand> ...  
</ArrayOfSeleniumCommand>
```

コマンドをファイルとして渡す場合は、次の構文を使用します。

```
-selenium_workflow "@PathToFile"
```

次のサンプルコードは、wd_firefox.txtというファイルをコマンドとして渡します。

```
-selenium_workflow "@D:\tmp\selenium_wd\wd_firefox.txt"
```

詳細については、「["WI.exeの使用" ページ303](#)」を参照してください。

APIを使用したマクロの作成

APIを使用してマクロを作成するには、次のエンドポイントを使用します。

POST /configuration/selenium/macro

次のサンプルコードは、cURLを使用してマクロを追加します。

```
curl -X POST --header "Content-Type: application/json" -d "  
{"VerifyMacro":true,"name": "test","command":  
"D:\\tmp\\selenium_wd\\bin\\net35\\nunit3-console.exe",  
"allowedHosts":  
["http://zero.webappsecurity.com"]}  
http://localhost:8083/webinspect/configuration/selenium/macro
```

次のサンプルコードは、cURLを使用してスキャンを開始します。

```
curl.exe -X POST --header "Content-Type: application/json" --header
"Accept: application/json" -d "{\"settingsName\": \"Default\",
\"overrides\": { \"startOption\": \"macro\", \"workflowMacros\":
[\"test \"], \"AllowedHosts\":[\"\\\"*\\\"] , \"crawlAuditMode\":
\"auditOnly\" } }" http://localhost:8083/webinspect/scanner/scans
```

使用法に関する詳細な情報とサンプルコードがSwagger UIに含まれています。オブジェクトは、「["WI.exeを使用したスキャンの実行" ページ350](#)」で説明されているオブジェクトに似ています。詳細については、「["Swagger UIの使用" ページ329](#)」を参照してください。

WorkingDirectoryおよびAllowedHosts引数はオプションです。場合によっては、AllowedHostsが自動的に判別されることがあります。ただし、FortifyではマクロごとにAllowedHostsを設定することをお勧めします。

場合によっては、WorkingDirectory引数に「現在の作業ディレクトリ」である作業ディレクトリパスを設定する必要があります。

Burp API拡張機能について

Burp Suiteは、Webアプリケーションのセキュリティテストを実行するためのツールキットです。Fortify WebInspectには、Burp拡張機能が含まれています。この拡張機能を使用すれば、Burp Suiteユーザは、Fortify WebInspect APIを介してFortify WebInspectをBurpに接続できます。

Burp API拡張機能を使用するメリット

Fortify WebInspectをBurpに接続すると、次のようなメリットが得られます。

- Fortify WebInspectスキャンから脆弱性のBurp問題を作成する
 - 現在実行中のまたは完了したスキャンで検出された脆弱性を要求する
 - 重大度などの指定された基準に基づいて脆弱性を要求する

メモ: Fortify WebInspectのチェックIDと名前は、Burp問題のIDと名前に対応しません。

- Burpでセッションを選択し、Fortify WebInspectに送信する

メモ: セッションを選択する理由は次のとおりです。

- 実行中のスキャンでFortify WebInspectのWeb探索に場所を追加する必要がある
- 実行中のスキャンに新しい脆弱性を追加する必要がある
- 完了したスキャンに新しい脆弱性を追加する必要がある

- Fortify WebInspectからスキャン情報を取得する
 - 特定のスキャンのステータスを取得する
 - 現在接続されているFortify WebInspectデータベースで使用可能なスキャンのリストを取得する
 - スキャンのステータス(実行中/完了)に基づいてスキャンのリストを取得する

サポートされるバージョン

Fortify WebInspect Burp API拡張機能は、新しいBurp拡張機能APIと互換性があります。

次も参照

["Fortify WebInspect REST API" ページ326](#)

["Burp API拡張機能の使用" 下](#)

Burp API拡張機能の使用

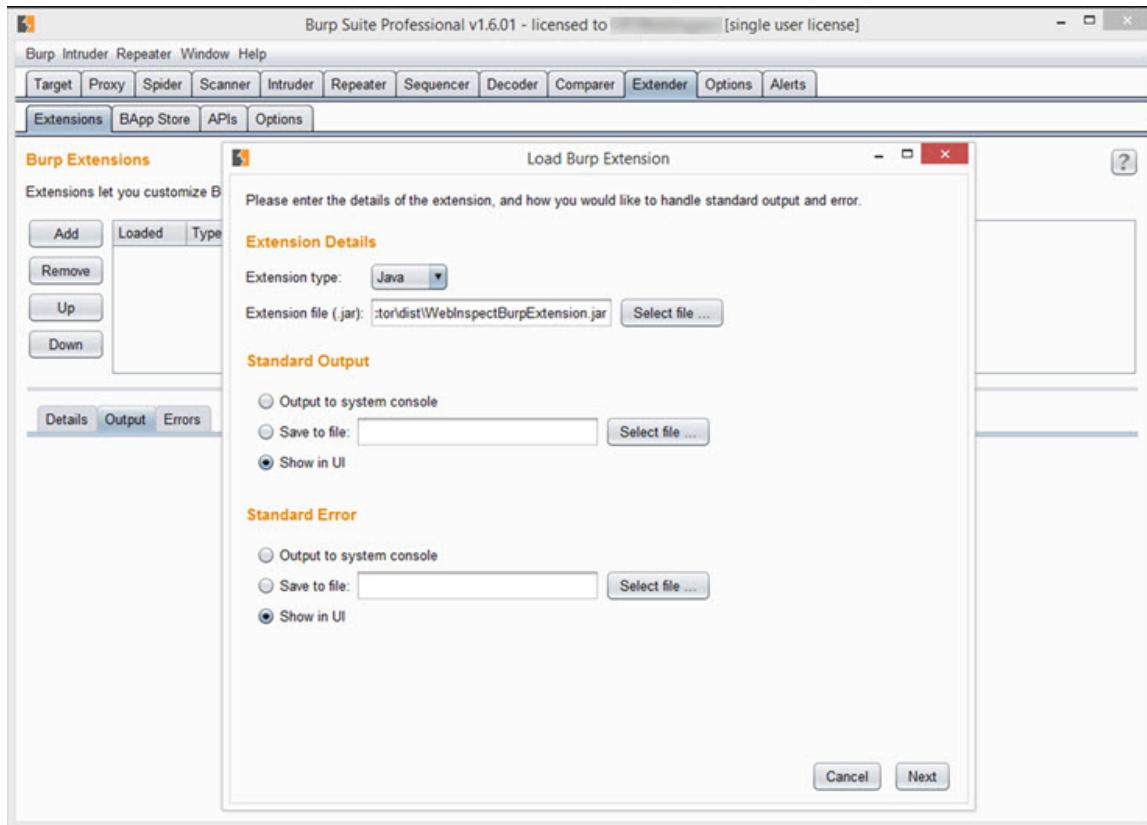
このトピックでは、Fortify WebInspect Burp拡張機能を設定して使用する方法について説明します。

Burp拡張機能のロード

Burpで次のステップを実行して、Fortify WebInspect Burp拡張機能をロードします。

1. [エクステンダ(Extender)]タブで [拡張機能(Extensions)]を選択し、[追加(Add)]をクリックします。

【Burp拡張機能のロード(Load Burp Extension)】ウィンドウが表示されます。



2. **機能拡張ファイル(.jar) (Extension file (.jar))** フィールドで、**ファイルの選択(Select file)** をクリックし、WebInspectBurpExtension.jarファイルに移動します。

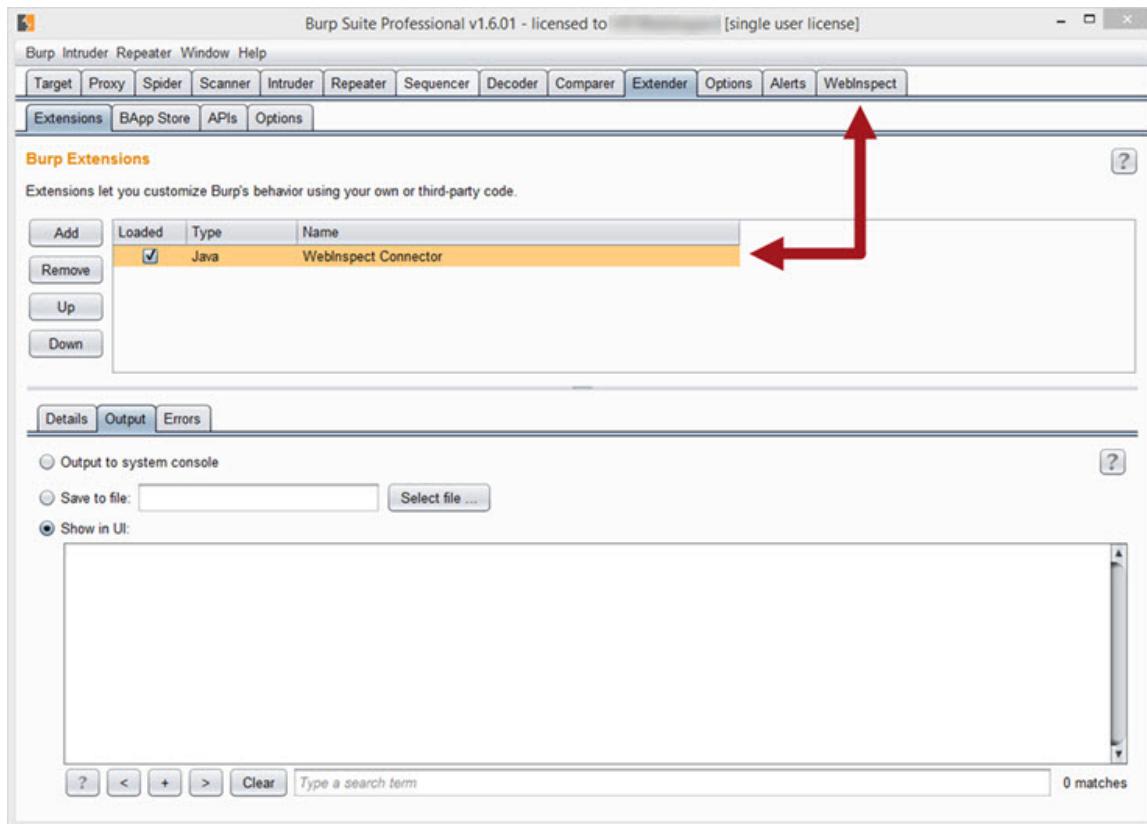
ヒント: WebInspectBurpExtension.jarファイルは、WebInspectがインストールされている場所のExtensionsディレクトリにあります。デフォルトの場所は次のいずれかです。

C:\Program Files\Fortify\Fortify WebInspect\Extensions

C:\Program Files (x86)\Fortify\Fortify WebInspect\Extensions

3. **標準出力(Standard Output)** セクションと **標準エラー(Standard Error)** セクションで、**UIに表示(Show in UI)** オプションが選択されていることを確認します。
4. **次へ(Next)** をクリックします。

WebInspect ConnectorがBurp拡張機能のリストに表示され、「WebInspect」というタブがBurpユーザインターフェースに追加されます。[WebInspect]タブが表示されない場合は、Burp拡張機能が正しくロードされていません。この場合は、[出力(Output)]タブと[エラー(Errors)]タブで、問題のトラブルシューティングに役立つ情報を確認してください。

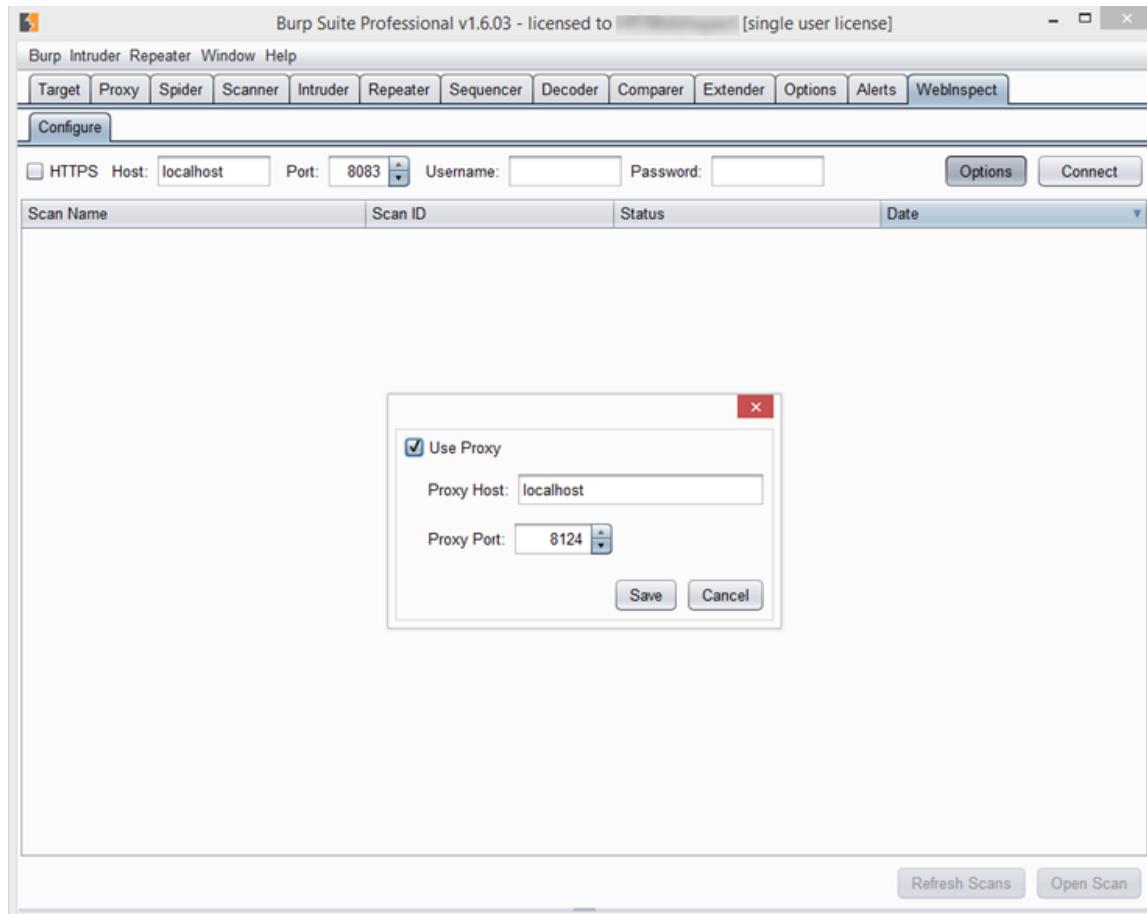


Fortify WebInspectへの接続

Fortify WebInspectに接続するには、Burpで次のステップを実行します。

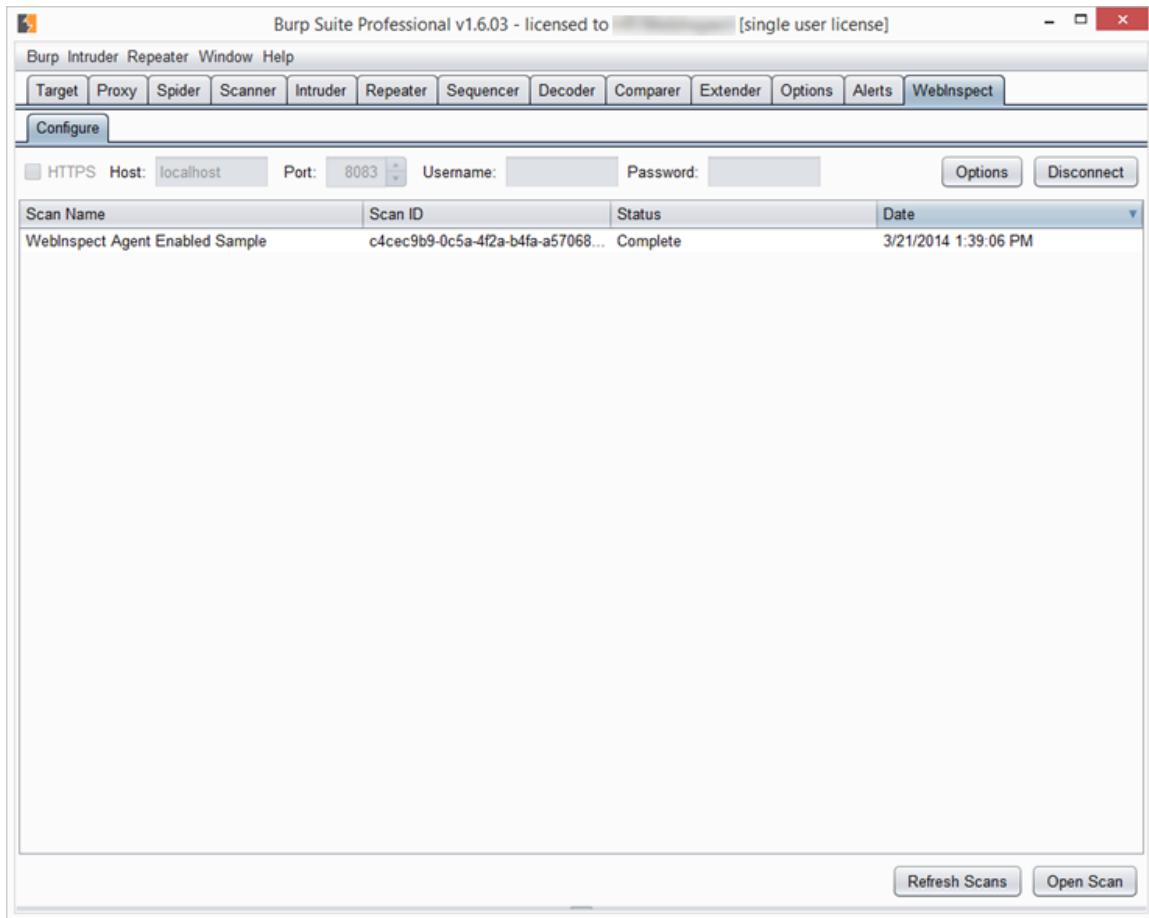
1. WebInspect APIサービスが実行されていることを確認します。詳細については、「["Micro Focus Fortify Monitor" ページ115](#)」を参照してください。
2. [WebInspect] > [設定(Configure)] タブで次の操作を行います。
 - a. APIでHTTPS認証が必要な場合は、[HTTPS] チェックボックスをオンにします。
 - b. Fortify WebInspect APIサービスのホスト名を [ホスト(Host)] に、ポート番号を [ポート(Port)] に入力します。
 - c. APIで認証が必須として設定されている場合は、ユーザ名とパスワードを入力します。
 - d. [オプション(Options)] をクリックして、API HTTP要求のプロキシ設定を行います。

プロキシ設定 ウィンドウが表示されます。



- e. 「プロキシを使用する(Use Proxy)」]チェックボックスをオンにして、「プロキシホスト(Proxy Host)」]に名前を入力し、「プロキシポート(Proxy Port)」]に番号を入力します。
- f. 「保存(Save)」]をクリックします。
3. 「接続(Connect)」]をクリックします。

【WebInspect】タブに、Fortify WebInspectスキャンのリストが表示されます。



スキャンのリストの更新

Fortify WebInspectスキャンのリストを更新するには、【スキャンの更新(Refresh Scans)】をクリックします。

Burpでのスキャンの操作

Fortify WebInspectスキャンを操作するには、Burpで次のステップを実行します。

1. 次のいずれかを実行してスキャンを開きます。
 - リスト内のスキャンをダブルクリックする。
 - リストからスキャンを選択し、【スキャンを開く(Open Scan)】をクリックする。

[WebInspect]タブの下の新しいタブでスキャンが開き、Web探索 セッションと脆弱性 セッションが一覧表示されます。セッションのリストは、タイプに基づいて脆弱性 セッション、Web探索 セッションの順に自動的にソートされます。

| Host | Method | URL | Type | Severity | Name |
|-------------------------------|--------|-----------------------------|---------------|----------|-------------------------------|
| http://zero.webappsecurity... | GET | /banklogin.asp?serviceNa... | Vulnerability | High | Credential Management: I... |
| http://zero.webappsecurity... | GET | /banklogin.asp?serviceNa... | Vulnerability | High | Transport Layer Protection... |
| http://zero.webappsecurity... | GET | /scripts/weblog | Vulnerability | High | Access Control: Administr... |
| http://zero.webappsecurity... | GET | /stats/ | Vulnerability | High | Credential Management: I... |
| http://zero.webappsecurity... | GET | /stats/ | Vulnerability | High | Transport Layer Protection... |
| http://zero.webappsecurity... | GET | /cgi.zip | Vulnerability | High | Access Control: Unprotect... |
| http://zero.webappsecurity... | GET | /cimerror.html | Vulnerability | High | Poor Error Handling: Unha... |
| http://zero.webappsecurity... | GET | /login/login.asp | Vulnerability | High | Credential Management: I... |
| http://zero.webappsecurity... | GET | /login/login.asp | Vulnerability | High | Transport Layer Protection... |
| http://zero.webappsecurity... | GET | /join.asp | Vulnerability | High | Password Management: I... |
| http://zero.webappsecurity... | GET | /join.asp | Vulnerability | High | Cross-Frame Scripting |
| http://zero.webappsecurity... | GET | /forgot.asp | Vulnerability | High | Password Management: I... |
| http://zero.webappsecurity... | GET | /Default.asp.bak | Vulnerability | High | Access Control: Unprotect... |
| http://zero.webappsecurity... | GET | /Default.asp.bak | Vulnerability | High | Access Control: Unprotect... |
| http://zero.webappsecurity... | GET | /adcenter.cgi | Vulnerability | High | Transport Layer Protection... |
| http://zero.webappsecurity... | GET | /login.asp | Vulnerability | High | Credential Management: I... |
| http://zero.webappsecurity... | GET | /login.asp | Vulnerability | High | Password Management: I... |
| http://zero.webappsecurity... | GET | /login.asp | Vulnerability | High | Transport Layer Protection... |
| http://zero.webappsecurity... | GET | /login/login.asp?UserNa... | Vulnerability | High | Password Management: I... |
| http://zero.webappsecurity... | GET | /admin/WS_FTP.LOG | Vulnerability | High | Access Control: Missing ... |
| http://zero.webappsecurity... | GET | /join1.asp?Name=12345&... | Vulnerability | High | Poor Error Handling: Unha... |

2. ソートされた列を逆の順序でソートするには、列ヘッダをクリックします。異なるソート基準を使用してリストをソートするには、ソート基準にする列のヘッダをクリックします。次の表で、いくつかのソートシナリオを説明します。

| 次の場合 ... | ソート基準 ... |
|--|--|
| スキャンに複数のホストが含まれており、セッションをホスト別にグループ化する場合 | ホスト |
| 特定のメソッドを使用しているすべてのセッションを表示する場合 | メソッドでソートし、目的のメソッドまでスクロールする |
| Webサイト内の特定のページに影響するすべてのセッションを表示する場合 | URLでソートし、目的のページまでスクロールする |
| 重大度が [重大(Critical)] および [高(High)] のすべてのセッションを選択して Burpツールに送信する場合 | 重大度でソートし、重大度が [重大(Critical)] および [高(High)] のセッションまでスクロールする |

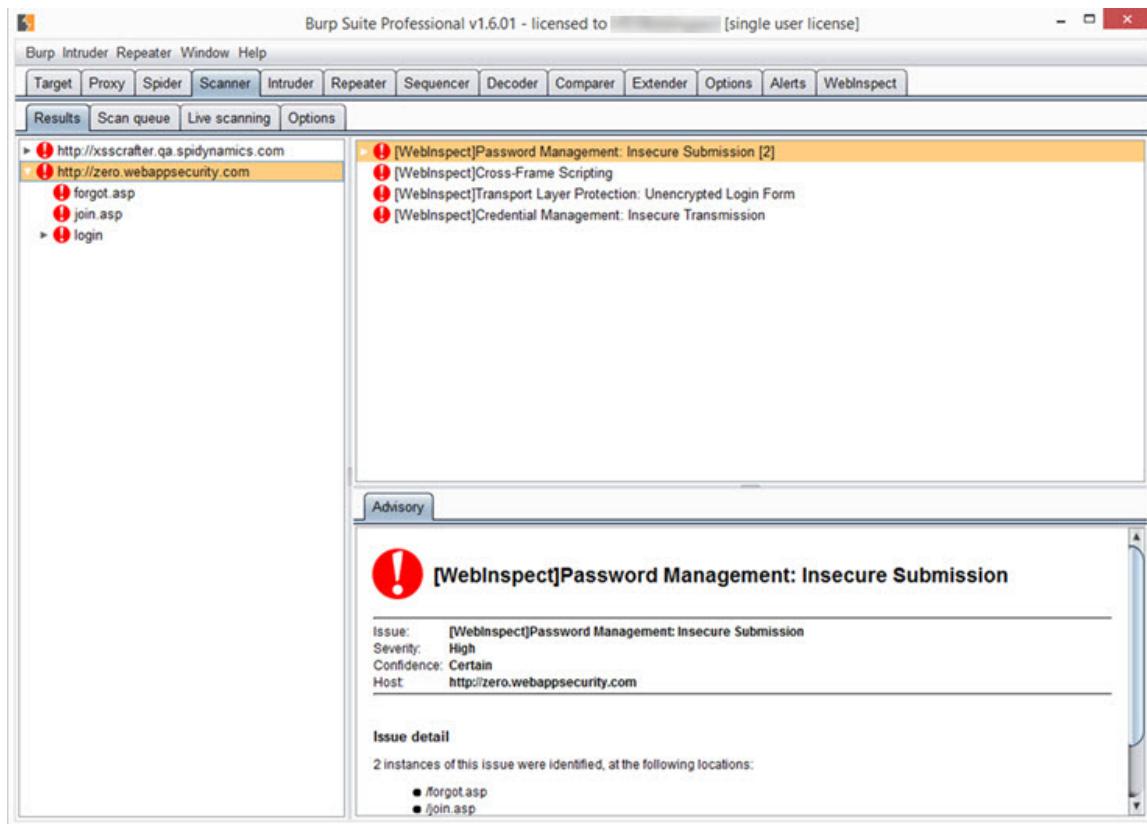
| 次の場合... | ソート基準... |
|----------------------------|---------------------------|
| 同じチェック名を持つすべてのセッションを選択する場合 | 名前でソートし、目的のチェック名までスクロールする |

3. Burpがまだ実行中のスキャンに接続されている場合などにセッションのリストを更新するには、[セッションの更新(Refresh Sessions)]をクリックします。
4. セッションの要求を表示するには、リストでそのセッションをクリックします。セッション要求情報がウィンドウの下部に表示されます。要求をクリックすると、応答が表示されます。
5. 1つ以上のセッションをBurpツールに送信してさらに分析するには、セッションを選択し、右クリックして該当する[送信先(Send To)]オプションを選択します。

メモ: 現在のオプションは、[Spiderに送信(Send To Spider)]、[Intruderに送信(Send To Intruder)]、および[Repeaterに送信(Send To Repeater)]です。Burpツールの詳細については、Burp Suiteのマニュアルを参照してください。

6. 脆弱なセッションの問題を作成し、Burpの[スキャナ(Scanner)]タブに追加するには、セッションを右クリックして[問題の作成(Create Issue)]を選択します。

この問題にはFortify WebInspectのレポートデータが取り込まれ、問題名には[WebInspect]というタグが付いています。これは、外部リソースから問題が追加されたことを示します。



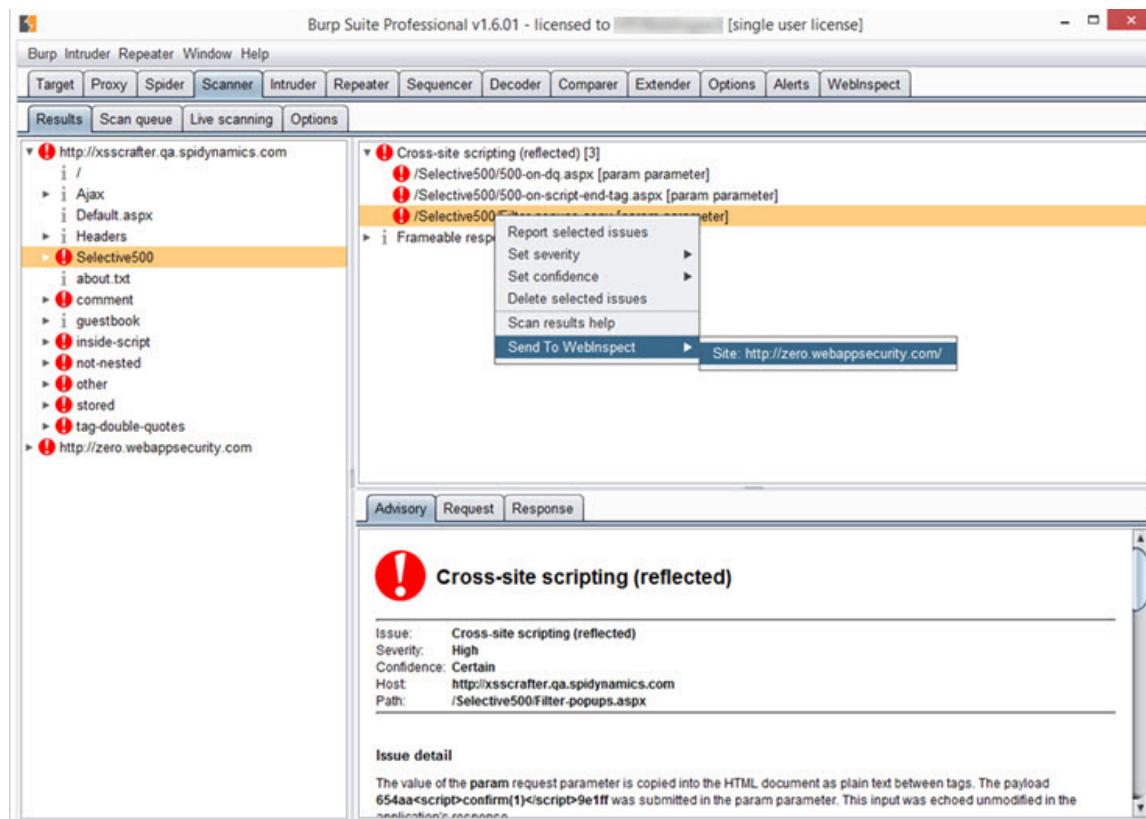
メモ: 問題の作成(Create Issue)】オプションは、Burp Professional Editionでのみ使用可能であり、Web探索セッションでは使用できません。

7. 停止したスキャンを続行するには、[スキャンの再開(Resume Scan)]をクリックします。
8. Fortify WebInspectスキャンを閉じるには、[タブを閉じる(Close Tab)]をクリックします。

BurpからWebInspectへの項目の送信

Web探索対象の要求/応答および問題をFortify WebInspectに送信するには、Burpで次のステップを実行します。

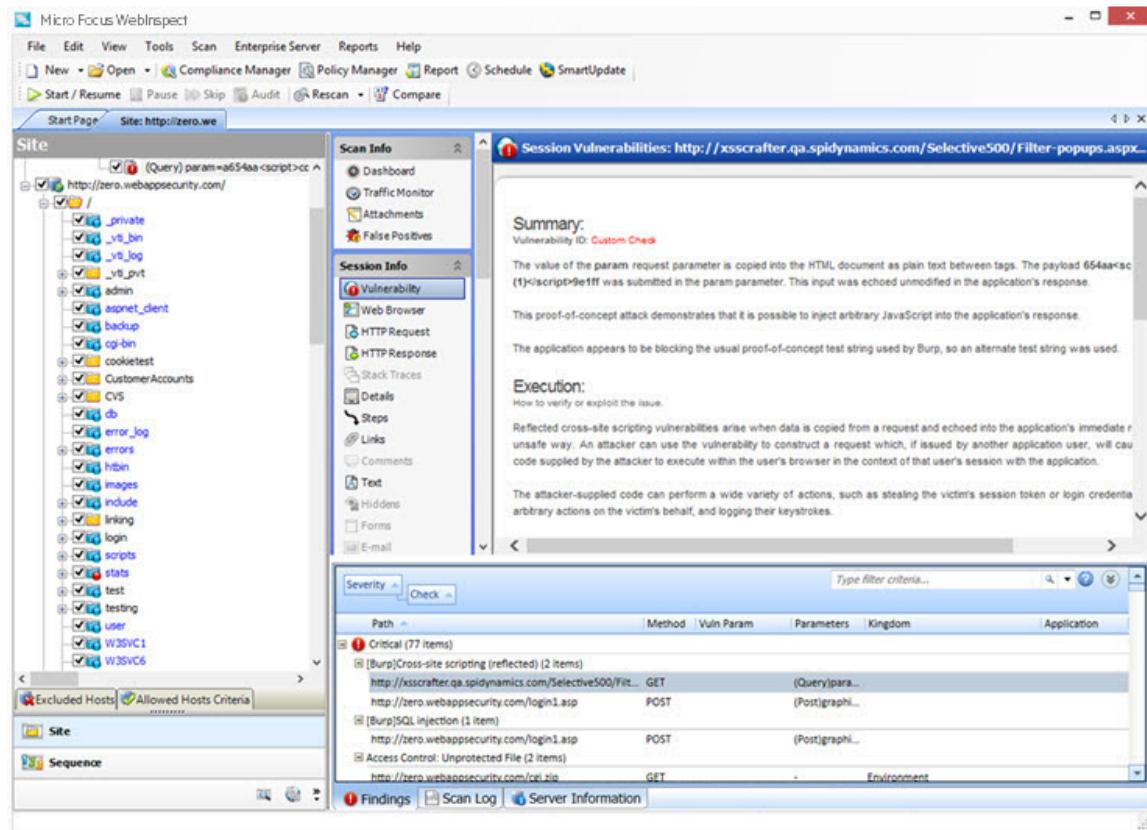
1. 目的のFortify WebInspectスキャンが[WebInspect]タブで開いていることを確認します。
- ヒント:** BurpでFortify WebInspectスキャンが開いていない場合、コンテキストメニューに[WebInspectに送信(Send to WebInspect)]オプションが表示されません。
2. [スキャナ(Scanner)]タブをクリックしてから、[結果(Results)]タブをクリックします。
 3. Web探索対象の要求/応答をFortify WebInspectに送信するには、その要求を右クリックして、[WebInspectに送信(Send To WebInspect)]>[スキャン名]を選択します。



Fortify WebInspectにより、Web探索可能な要求のセッションが作成されます。
[WebInspect]タブでスキャンに戻り、[スキャンの再開(Resume Scan)]をクリックして、セッションをWeb探索します。

メモ: 開いているスキャンのスキャン設定は、送信されるセッションに適用されます。これは、Fortify WebInspectがセッションで実行する内容に影響する場合があります。たとえば、開いているスキャンがホストA用で、ホストBからセッションを送信するが、開いているスキャンの【許可ホスト(Allowed Hosts)】リストにホストBが含まれていない場合、このセッションは除外され、Web探索は行われません。

4. Fortify WebInspectに問題を手動での検出事項として送信するには、問題を右クリックして、【WebInspectに送信(Send To WebInspect)】>【スキャン名】を選択します。



次も参照

["Burp API拡張機能について" ページ352](#)

["Fortify WebInspect REST API" ページ326](#)

["Micro Focus Fortify Monitor" ページ115](#)

WebInspect SDKについて

WebInspect Software Development Kit(SDK)はVisual Studio拡張機能であり、これを使うとソフトウェア開発者はセッション応答で特定の脆弱性をテストする監査拡張機能を作成できます。

きます。

注意! Fortifyでは、Visual Studioを使用したコード開発の専門知識を持つ有資格のソフトウェア開発者のみがWebInspect SDKを使用することを推奨しています。

監査拡張機能/カスタムエージェント

開発者は、WebInspect SDKをFortify WebInspectコードへのエントリポイントとして使用できます。Fortify WebInspectが要求/応答ペアを作成すると、開発者は応答を調べて、脆弱性にフラグを付ける監査拡張機能を作成できます。作成が済むと、開発者は拡張機能をSecureBase(アダプティブエージェントと脆弱性チェックのFortify WebInspectデータベース)のローカルコピーに送信し、そこでカスタムエージェントとして保存します。カスタムエージェントにはGUID(Globally Unique Identifier)が割り当てられ、Fortify WebInspect製品のPolicy Managerでポリシーに使用できるようになります。

メモ: カスタムエージェントは、SecureBaseの更新によって上書きされません。

スキャン結果を検査するときには、カスタムエージェントによって検出された脆弱性に対して、標準チェックによって検出された脆弱性に対するアクションと同じアクション(URLのコピーや脆弱性の確認など)を実行できます。詳細については、「["結果の検査" ページ257](#)」を参照してください。

SDKの機能

SDKは、開発者に次の機能を提供します。

- Fortify WebInspect Web探索プログラムと監査機能により生成されるセッションを検査する
- パラメータに値を挿入する(パラメータおよびサブパラメータのファジング)
- URLをWeb探索のためにキューに登録する(Fortify WebInspect Web探索プログラムがWeb探索できるようにするため)
- 脆弱性にフラグを付ける
- Fortify WebInspectリクエスタから生のHTTP要求を送信する
- ParseLibによる要求と応答の解析
- イベントとエラーをログに記録する

インストールの推奨事項

WebInspect SDKは、Fortify WebInspect製品と同じマシンにインストールする必要はありません。ほとんどの場合、ソフトウェア開発者の開発マシンにインストールされます。ただし、デバッグが必要な新しい拡張機能を開発している場合、Fortifyでは、拡張機能を作成する開発マシンにFortify WebInspectをインストールすることをお勧めします。これにより、拡張機能をローカルでテストできます。デバッグを必要としない既存の拡張機能の場合は、Fortify WebInspectをローカルにインストールする必要はありません。

WebInspect SDKのインストールと使用に関する最小要件については、『*Micro Focus Fortify Software System Requirements*』ドキュメントを参照してください。

WebInspect SDKのインストール

WebInspect SDKを使用するには、開発者がWebInspectSDK.vsixという名前のVisual Studio拡張機能ファイルをインストールする必要があります。

Fortify WebInspectのインストール中に、WebInspectSDK.vsixファイルのコピーがFortify WebInspectのインストール場所のExtensionsディレクトリにインストールされます。デフォルトの場所は次のいずれかです。

- C:\Program Files\Fortify\Fortify WebInspect\Extensions
- C:\Program Files (x86)\Fortify\Fortify WebInspect\Extensions

開発者のマシンでFortify WebInspectがインストールされている場所にローカルコピーをインストールするには:

1. **Extensions**フォルダに移動し、WebInspectSDK.vsixファイルをダブルクリックします。
VSIXインストーラが起動します。
2. プロンプトが表示されたら、拡張機能をインストールするVisual Studio製品を選択し、**[インストール(Install)]**をクリックします。
WebInspect Audit ExtensionプロジェクトテンプレートがVisual Studioで作成されます。
「["インストールの検証" 下](#)」に進みます。

開発者のマシンでFortify WebInspectがインストールされていない場所にローカルコピーをインストールするには:

1. **Extensions**フォルダに移動し、WebInspectSDK.vsixファイルをUSBドライブなどのポータブルメディアにコピーします。
2. Visual Studio 2013や、関連する必須ソフトウェアおよびハードウェアがインストールされている開発マシンにドライブを挿入します。
3. USBドライブに移動し、WebInspectSDK.vsixファイルをダブルクリックします。
VSIXインストーラが起動します。
4. プロンプトが表示されたら、拡張機能をインストールするVisual Studio製品を選択し、**[インストール(Install)]**をクリックします。
WebInspect Audit ExtensionプロジェクトテンプレートがVisual Studioで作成されます。
「["インストールの検証" 下](#)」に進みます。

インストールの検証

拡張機能が正常にインストールされていることを検証するには:

1. Visual Studioで **ツール] > 拡張機能と更新プログラム]**を選択します。
2. 拡張機能のリストを下に向かってスクロールします。

リストに [WebInspect SDK] が表示されていれば、拡張機能は正常にインストールされています。

インストール後の作業

WebInspect SDKをインストールして設定した後、開発者はVisual Studioで新しいWebInspect Audit Extensionプロジェクトを作成できます。このプロジェクトでは、開発者は監査拡張機能を作成し、その拡張機能をデバッグおよびテストし、カスタムエージェントとしてSecureBaseに発行します。WebInspect Audit Extensionプロジェクトテンプレートの使用法については、Visual StudioのWebInspect SDKのドキュメントを参照してください。

開発者がカスタムエージェントをSecureBaseに送信した後、このエージェントをPolicy Managerのポリシーで選択できるようになります。詳細については、Policy Managerのドキュメントを参照してください。

ページまたはディレクトリの追加

Fortify WebInspectでは検出されなかったリソースを検出するために手動検査または他のセキュリティ分析ツールを使用する場合、これらの場所を手動で追加して脆弱性を割り当てることができます。データをFortify WebInspectスキャンに組み込むことで、Fortify WebInspect機能を使用して脆弱性を報告および追跡することができます。

メモ: データ階層に何かを追加する場合は、論理的な順序に従って手動でリソースを追加する必要があります。たとえば、サブディレクトリとページを作成するには、サブディレクトリを作成してからページを作成する必要があります。

1. ページまたはディレクトリのデフォルト名を、追加するリソースの名前に置き換えます。
2. 必要に応じて、HTTP要求と応答を編集します。要求パスは変更しないでください。
3. リソースに要求を送信し、応答をセッションデータに記録できます。これにより、Fortify WebInspectによって検出されなかったリソースの存在も検証されます。
 - a. [HTTP Editor]をクリックして、HTTP Editorを開きます。
 - b. 必要に応じて、要求を変更します。
 - c.  Sendをクリックします。
 - d. HTTP Editorを閉じます。
 - e. 変更した要求と応答の使用を求めるプロンプトが表示されたら、[はい(Yes)]を選択します。
4. (オプション)すべての要求と応答の変更を削除するには、[リセット(Reset)]をクリックします。
5. 終了したら、[OK]をクリックします。

バリエーションの追加

Fortify WebInspectでは検出されなかったリソースを検出するために手動検査またはその他のセキュリティ分析ツールを使用する場合、これらの場所を手動で追加して脆弱性を割り当てることができます。データをFortify WebInspectスキャンに組み込むことで、Fortify WebInspect機能を使用して脆弱性を報告および追跡することができます。

バリエーションとはある場所のサブノードであり、その場所の特定の属性を一覧にしたもので、たとえば、場所 login.aspには次のバリエーションがあるかもしれません。

(Post) uid=12345&Password=foo&Submit=Login

他の場所と同様に、バリエーションには脆弱性とサブノードが付加されている場合もあります。

1. **名前(Name)** ボックスで、デフォルトの「attribute=value」を、送信する実際のパラメータに置き換えます(uid=9999&Password=kungfoo&Submit=Loginなど)。
2. **POST(Post)** または **クエリ(Query)** を選択します。
3. 必要に応じて、HTTP要求と応答を編集します。要求パスは変更しないでください。
4. リソースに要求を送信し、応答をセッションデータに記録できます。これにより、Fortify WebInspectによって検出されなかったリソースの存在も検証されます。
 - a. **HTTP Editor** をクリックして、HTTP Editorを開きます。
 - b. 必要に応じて、要求を変更します。
 - c.  **Send** をクリックします。
 - d. HTTP Editorを閉じます。
 - e. 変更した要求と応答の使用を求めるプロンプトが表示されたら、**はい(Yes)** を選択します。
5. (オプション)すべての要求と応答の変更を削除するには、**リセット(Restet)** をクリックします。
6. 終了したら、**OK** をクリックします。

Fortify Monitor: Enterprise Serverセンサの設定

この設定情報は、Fortify WebInspectをセンサとしてFortify WebInspect Enterpriseに統合するために使用されます。情報を入力してセンササービスを開始したら、Fortify WebInspect グラフィカルユーザインターフェースではなく、Fortify WebInspect Enterprise Webコンソールを使用してスキャンを実行する必要があります。

センサ設定項目の説明を次の表に示します。

| 項目 | 説明 |
|--|---|
| マネージャURL (Manager URL) | Enterprise Server ManagerのURLまたはIPアドレスを入力します。 |
| センサ認証 (Sensor Authentication) | ユーザ名(ドメイン\ユーザ名の形式)とパスワードを入力してから、[テスト(Test)]をクリックしてエントリを検証します。 |
| プロキシの有効化 (Enable Proxy) | Fortify WebInspectがプロキシサーバを経由して、Enterprise Server Managerにアクセスする必要がある場合は、[プロキシの有効化(Enable Proxy)]を選択してから、サーバのIPアドレスとポート番号を入力します。認証が必要な場合は、有効なユーザ名とパスワードを入力します。 |
| データベース設定の上書き (Override Database Settings) | 通常、Fortify WebInspectは、スキヤンデータをFortify WebInspectデータベース用のアプリケーション設定で指定されたデバイスに保存します。ただし、Fortify WebInspectがセンサとしてFortify WebInspect Enterpriseに接続されている場合は、このオプションを選択してから、[設定(Configuration)]をクリックして代替デバイスを指定できます。 |
| サービスアカウント (Service Account) | センササービスには、LocalSystemアカウントまたは指定したアカウントを使用してログオンできます。 |
| センサステータス (Sensor Status) | このエリアにはセンササービスの現在のステータスが表示され、サービスを開始または停止するためのボタンが表示されます。 |

センサとして設定後(After Configuring as a Sensor)

Fortify WebInspectをセンサとして設定したら、[開始(Start)]をクリックします。

ブラックアウト期間

Fortify WebInspectがFortify WebInspect Enterpriseに接続されている場合は、ユーザがブラックアウト期間中にスキャンを試みる可能性があります。これは、スキャンが企業管理者によって許可されない一定の時間です。この問題が発生した場合は、次のエラーメッセージが表示されます。

「開始URLが次のブラックアウト期間に入っているためスキャンを開始できません...(Cannot start Scanner because the start URL is under the following blackout period(s)...)」

スキャンを実行するには、ブラックアウト期間が終了するまで待つ必要があります。

同様に、ブラックアウト期間が始まったときにスキャンが実行されていた場合、企業管理者はスキャンを一時停止して、保留中のジョブキューに登録し、ブラックアウト期間が終了したらスキャンを完了します。複数のIPアドレスに対してブラックアウトが定義されている場合、企業管理者は、指定されたIPアドレスの1つからスキャンが開始された場合にのみスキャンを一時停止します。除外されていないIPアドレスでスキャンが開始されるものの、その後、IPアドレスがブラックアウト設定で指定されたホストへのリンクをたどる場合、スキャンは一時停止されません。

除外の作成

除外/拒否基準を追加するには:

1. **追加(Add)**]([**その他の除外/拒否基準(Other Exclusion/Rejection Criteria)**]リストの右側にある)をクリックします。
除外の作成(Create Exclusion)]ウィンドウが開きます。
2. **ターゲット(Target)**]リストから項目を選択します。
3. ターゲットとして [クエリパラメータ(Query Parameter)]、[ポストパラメータ(Post Parameter)]、または [応答ヘッダ(Response Header)]を選択した場合は、**ターゲット名(Target Name)**]を入力します。
4. **一致タイプ(Match Type)**]リストから、ターゲット内のテキストの一一致に使用される方法を選択します。
 - **正規表現に一致(Matches Regex)**] - **一致文字列(Match String)**]ボックスで指定した正規表現に一致します。
 - **正規表現の拡張に一致(Matches Regex Extension)**] - **一致文字列(Match String)**]ボックスで指定したFortify正規表現の拡張から入手可能な構文に一致します。詳細については、「[正規表現の拡張](#)」ページ324を参照してください。
 - **一致(Matches)**] - **一致文字列(Match String)**]ボックスで指定したテキスト文字列に一致します。
 - **含む(Contains)**] - **一致文字列(Match String)**]ボックスで指定したテキスト文字列を含みます。
5. **一致文字列(Match String)**]ボックスに、ターゲットで検索する文字列または正規表現を入力します。または、**一致タイプ(Match Type)**]で正規表現オプションを選択した場合は、ドロップダウン矢印をクリックして、**正規表現の作成(Create Regex)**]を選択し、Regular Expression Editorを起動します。
6. をクリックします。
7. (オプション)ステップ2-6を繰り返して、条件を追加します。複数の一一致はAND処理されます。
8. **現在の設定(Current Settings)**]で作業している場合は、**テスト(Test)**]をクリックして現在のスキャンの除外を処理できます。基準によって絞り込まれたそのスキャンからのセッションがテスト画面に表示され、必要に応じて設定を変更できます。
9. **OK**]をクリックします。

10. [他の除外/拒否基準(Other Exclusion/Rejection Criteria)]リストに除外が表示されている場合は、[拒否(Reject)]と[除外(Exclude)]のいずれかまたは両方を選択します。

メモ: スキャン中は、応答タイプ、応答ヘッダタイプ、およびステータスコードターゲットタイプを拒否することができません。これらのターゲットタイプは除外することしかできません。

例1

Microsoft.comのリソースに対する要求を無視して送信しないようにするには、次の除外を入力して、[拒否(Reject)]を選択します。

| ターゲット(Target) | ターゲット名(Target Name) | 一致タイプ(Match Type) | 一致文字列(Match String) |
|---------------|---------------------|-------------------|---------------------|
| URL | N/A | 含む(contains) | Microsoft.com |

例2

一致文字列として「logout」と入力します。この文字列がURLの任意の部分で見つかった場合は、そのURLが除外または拒否されます(選択されたオプションによって異なる)。「logout」の例を使用すると、Fortify WebInspectは、logout.aspやapplogout.jspなどのURLを除外または拒否します。

| ターゲット(Target) | ターゲット名(Target Name) | 一致タイプ(Match Type) | 一致文字列(Match String) |
|---------------|---------------------|-------------------|---------------------|
| URL | N/A | 含む(contains) | logout |

例3

次の例では、クエリパラメータ「username」が「John」と等しいクエリを含むセッションを拒否または除外します。

| ターゲット(Target) | ターゲット名(Target Name) | 一致タイプ(Match Type) | 一致文字列(Match String) |
|---------------------------|---------------------|-------------------|---------------------|
| クエリパラメータ(Query parameter) | username | 一致(matches) | John |

例4

次の例では、次のディレクトリを除外または拒否します。

http://www.test.com/W3SVC55/

http://www.test.com/W3SVC5/

http://www.test.com/W3SVC550/

| ターゲット (Target) | ターゲット名 (Target Name) | 一致タイプ (Match Type) | 一致文字列 (Match String) |
|----------------|----------------------|-------------------------|----------------------|
| URL | N/A | 正規表現に一致 (matches regex) | /W3SVC[0-9]*/ |

Internet Protocolバージョン6

Fortify WebInspect (バージョン8.1以降)は、WebサイトとWebサービススキャンで、Internet Protocolバージョン6(IPv6)アドレスをサポートしています。開始URLを指定する場合は、IPv6アドレスを括弧で囲む必要があります。次に例を示します。

- `http://[::1]`
Fortify WebInspectは「localhost」をスキャンします。
- `http://[fe80::20c:29ff:fe32:bae1]??/subfolder/??`
Fortify WebInspectは、指定されたアドレスのホストのスキャンを「subfolder」ディレクトリから開始します。
- `http://[fe80::20c:29ff:fe32:bae1]??:8080/subfolder/??`
Fortify WebInspectは、ポート8080で実行されているサーバの「subfolder」で始まる部分をスキャンします。

第6章: デフォルトのスキャン設定

この章では、デフォルトのスキャン設定について説明します。[デフォルト設定(Default Settings)]を使用して、スキャンアクションのスキャンパラメータを設定します。Fortify WebInspectは、スキャンの開始中に代わりのオプションを指定(スキャンウィザードから、または現在の設定(Current Settings)]にアクセスして使用可能なオプションを使用する)しない限り、これらを使用します。

次も参照

["Web探索設定" ページ418](#)

["監査設定" ページ431](#)

スキャン設定: 方法

この機能にアクセスするには、[編集(Edit)]メニューをクリックし、[デフォルトのスキャン設定(Default Scan Settings)]または[現在のスキャン設定(Current Scan Settings)]を選択します。その後で、[スキャン設定(Scan Settings)]カテゴリで、[方法(Method)]を選択します。

スキャンモード(Scan Mode)

[スキャンモード(Scan Mode)]オプションについて、次の表で説明します。

| オプション | 説明 |
|---------------------------------|--|
| Web探索のみ (Crawl Only) | このオプションは、サイトのツリー構造を完全にマッピングします。Web探索が完了したら、[監査(Audit)]をクリックしてアプリケーションの脆弱性を評価できます。 |
| Web探索および監査 (Crawl and Audit) | Fortify WebInspectは、サイトの階層データ構造をマッピングし、各リソース(ページ)が検出されるたびにそれを監査します(サイト全体をWeb探索してから監査を実行するのではなく)。このオプションは、Web探索が完了する前にコンテンツが変更される可能性がある非常に大規模なサイトで最も有用です。これについては、[デフォルト設定(Default Settings)]の[Web探索および監査モード(Crawl and Audit Mode)]の[同時(Simultaneously)]というオプションで説明しています。詳細については、「 "Web探索および監査モード(Crawl and Audit Mode)" 次のページ 」を参照してください。 |
| 監査のみ(Audit) | Fortify WebInspectは、選択されたポリシーの手法を適用して脆弱 |

| オプション | 説明 |
|--------------------------------|---|
| Only) | セキュリティリスクを判断しますが、WebサイトのWeb探索は行いません。サイト上のリンクをたどることも評価することもありません。 |
| 手動 (ガイド付きスキャン では使用できません) | 手動モードでは、アクセス先として選んだのがアプリケーションのどのセクションであれ、そこに手動で移動できます。サイト全体のWeb探索は実行されず、サイト内を手動で移動中に検出したリソースに関する情報のみを記録します。この機能は、Webフォームのログオンページからサイトに入る場合、または調査するアプリケーションの個別のサブセットまたは部分を定義する場合に最もよく使用されます。サイト内を移動し終わったら、結果を監査して、記録したサイトのその部分に関連するセキュリティ脆弱性を評価できます。 |

Web探索および監査モード(Crawl and Audit Mode)

【Web探索および監査モード(Crawl and Audit Mode)】オプションについて、次の表で説明します。

| オプション | 説明 |
|------------------------|--|
| 同時 (Simultaneously) | Fortify WebInspectは、サイトの階層データ構造をマッピングし、各リソース(ページ)が検出されるたびにそれを監査します(サイト全体をWeb探索してから監査を実行するのではなく)。このオプションは、Web探索が完了する前にコンテンツが変更される可能性がある非常に大規模なサイトで最も有用です。 |
| 順次(Sequentially) | このモードでは、Fortify WebInspectはサイト全体をWeb探索し、サイトの階層データ構造をマッピングして、サイトのルートから順次監査を実行します。 |

Web探索および監査の詳細(Crawl and Audit Details)

【Web探索および監査の詳細(Crawl and Audit Details)】オプションについて、次の表で説明します。

| オプション | 説明 |
|--|--|
| 検索プローブを含める(検索攻撃を送信する)(Include search probes (send search)) | このオプションを選択すると、Fortify WebInspectは、サーバ上に存在する場合も存在しない場合もあるファイルやディレクトリに対する要求を、それらのファイルがサイトのWeb探索で検出されない場合でも送信します。 |

| オプション | 説明 |
|---|--|
| attacks)) | このオプションは、スキャンモードが [Web探索および監査(Crawl & Audit)]に設定されている場合にのみデフォルトで選択されます。スキャンモードが [Web探索のみ(Crawl Only)]または [監査のみ(Audit Only)]に設定されている場合、このオプションはデフォルトでクリア(オフ)されます。 |
| 「ファイルが見つからない」応答でのリンクのWeb探索(Crawl links on File Not Found responses) | このオプションを選択すると、Fortify WebInspectは「ファイルが見つからない」とマークされた応答のリンクを検索し、Web探索を行います。 このオプションは、スキャンモードが [Web探索のみ(Crawl Only)]または [Web探索および監査(Crawl & Audit)]に設定されている場合はデフォルトで選択されます。このオプションは、スキャンモードが [監査のみ(Audit Only)]に設定されている場合は利用できません。 |

ナビゲーション

「ナビゲーション(Navigation)」オプションについて、次の表で説明します。

| オプション | 説明 |
|---|---|
| Web探索時のWebフォームの自動入力(Auto-fill Web forms during crawl) | このオプションを選択すると、Fortify WebInspectは、すべてのフォームで検出された入力コントロールの値を送信します。値は、Web Form Editorを使用して作成したファイルから抽出されます。参照ボタンを使用して、使用する値を含むファイルを指定します。または、[編集(Edit)]ボタン  (現在選択されているファイルを変更する場合)または[作成(Create)]ボタン  (Webフォームファイルを作成する場合)を選択することもできます。 注意! この機能を認証に使用しないでください。Web探索プログラムと監査プログラムが状態を共有するように設定されている場合、およびFortify WebInspectがサイトから誤ってログアウトすることがない場合は、Web Form Editorによって抽出された値をログインフォームに使用できます。ただし、最初のログインの後に監査またはWeb探索によってログアウトがトリガされた場合は、Fortify WebInspectは再ログインできず、監査は認証されなくなります。Fortify WebInspectが誤ってアプリケーションからログアウトした場合に途中で終了するのを防ぐには、「スキャン設定(Scan Settings)-認証(Authentication)」に移動し、 |

| オプション | 説明 |
|--|--|
| | <p>【フォーム認証にログインマクロを使用する(Use a login macro for forms authentication)】を選択します。</p> |
| Webフォーム値の入力を要求する(Prompt for Web form values) | <p>このオプションを選択すると、Fortify WebInspectは、HTTPフォームまたはJavaScriptフォームを検出した際にスキャンを一時停止し、フォーム内の入力コントロールの値を入力できるウィンドウを表示します。しかし、タグ付けされた入力に対してのみプロンプトを表示する(Only prompt for tagged inputs)】も選択した場合、Fortify WebInspectはユーザ入力用に一時停止しません。ただし、(Web Form Editorを使用して)特定の入力コントロールが対話型入力としてマーク(Mark as Interactive Input)】と指定されている場合は例外です。入力するためのこの一時停止は「対話型モード」と呼ばれ、スキャン中にいつでもキャンセルできます。</p> <p>対話型スキャンの設定の詳細については、「"対話型スキャン" ページ200」を参照してください。</p> |
| Webサービス設計を使用する(Use Web Service Design) | <p>このオプションは、Webサービススキャンにのみ適用されます。</p> <p>Webサービススキャンを実行するときに、Fortify WebInspectはWSDLサイトをWeb探索し、操作ごとに各パラメータの値を送信します。これらの値は、Web Service Test Designerツールを使用して作成したファイルに含まれています。次に、Fortify WebInspectは、SQLインジェクションなどの脆弱性を検出するために各パラメータを攻撃して、サイトを監査します。</p> <p>参照ボタンを使用して、使用する値を含むファイルを指定します。または、編集 [ボタン  (現在選択されているファイルを変更する場合)または 作成(Create) [ボタン  (SOAP値ファイルを作成する場合)]を選択することもできます。</p> |

SSL/TLSプロトコル(SSL/TLS Protocols)

SSL (Secure Sockets Layer)およびTLS (Transport Layer Security)プロトコルは、WebブラウザとWebサーバ間のインターネットランザクションに対してセキュアなHTTP (HTTPS)接続を提供します。SSL/TLSプロトコルは、Webアプリケーションのサーバ認証、クライアント認証、データ暗号化、およびデータ整合性を有効にします。

メモ: [アプリケーション設定(Application Settings)]で [OpenSSLエンジンを使用する(Use OpenSSL Engine)]が選択されている場合、[SSL/TLSプロトコル(SSL/TLS Protocols)]オプションは無効化されます。個々のプロトコルを選択することはできません。詳細については、「["アプリケーション設定: 全般" ページ442](#)」を参照してください。

Webサーバが使用するSSL/TLSプロトコルを選択します。次のオプションを指定できます。

- SSL 2.0を使用(Use SSL 2.0)
- SSL 3.0を使用(Use SSL 3.0)
- TLS 1.0を使用(Use TLS 1.0)
- TLS 1.1を使用(Use TLS 1.1)
- TLS 1.2を使用(Use TLS 1.2)

Webサーバに対応するSSL/TLSプロトコルを設定していない場合でも、Fortify WebInspectは引き続きサイトに接続しますが、パフォーマンスへの影響が生じる場合があります。

たとえば、Fortify WebInspectの設定がSSL 3.0のみを使用するように設定されているのに対し、WebサーバがTLS 1.2接続のみを受け入れるように設定されている場合、Fortify WebInspectはまずSSL 3.0との接続を試みますが、失敗します。その後、Fortify WebInspectは、TLS 1.2がサポートされていることを検出するまで、各プロトコルを実装します。接続は成功しますが、この作業にはより多くの時間がかかります。Fortify WebInspectで正しい設定([TLS 1.2を使用(Use TLS 1.2)])を行っていれば、最初の試みで成功したはずです。

スキャン設定: 全般

この機能にアクセスするには、[編集(Edit)]メニューをクリックし、[デフォルトのスキャン設定(Default Scan Settings)]または[現在のスキャン設定(Current Scan Settings)]を選択します。その後で、[スキャン設定(Scan Settings)]カテゴリで、[全般(General)]を選択します。

スキャンの詳細(Scan Details)

[スキャンの詳細(Scan Details)]オプションについて、次の表で説明します。

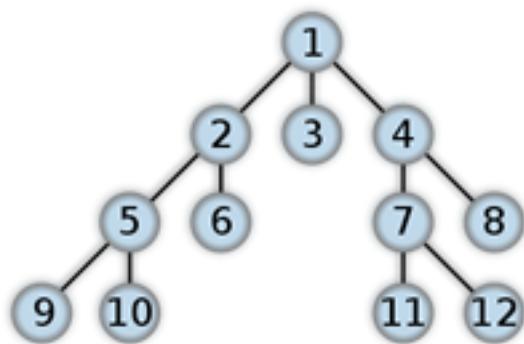
| オプション | 説明 |
|--------------------------------------|--|
| パス切り捨てを有効にする(Enable Path Truncation) | <p>パスの切り捨て攻撃は、ファイル名がない既知のディレクトリを求める要求です。これにより、ディレクトリ一覧が表示される場合があります。Fortify WebInspectはパスの切り捨てを実行し、その際にディレクトリの一覧が表示されたり、異常なエラーが発生したりしないかを確認します。</p> <p>例: リンクがhttp://www.site.com/folder1/folder2/file.aspで構成されている場合、パスを切り捨てて、 http://www.site.com/folder1/folder2/と http://www.site.com/folder1/を探すと、サーバでディレクトリの内容が表示されたり、未処理の例外が発生したりする場合があります。</p> |

| オプション | 説明 |
|--|---|
| 大文字と小文字を区別する要求と応答の処理(Case-sensitive request and response handling) | ターゲットサイトのサーバでURLの大文字と小文字が区別される場合は、このオプションを選択します。 |
| 相関データの再計算(Recalculate correlation data) | このオプションは、スキャンを比較する場合にのみ使用されます。この設定の変更は、Fortifyカスタマサポート担当者からのアドバイスがある場合にのみ行ってください。 |
| 応答データの圧縮(Compress response data) | このオプションを選択すると、Fortify WebInspectでは、各HTTP応答を圧縮形式でデータベースに保存してディスク容量を節約します。 |
| Traffic Monitorのログを有効にする(Enable Traffic Monitor Logging) | 基本スキャンの実行中、Fortify WebInspectでは、Webサイトの階層構造を示すセッションと脆弱性が検出されたセッションのみをナビゲーションペインに表示します。ただし、[Traffic Monitor]オプションを選択した場合、Fortify WebInspectは[Traffic Monitor]ボタンを[スキャン情報(Scan Info)]パネルに追加し、Fortify WebInspectによって送信されたすべての単一のHTTP要求と、サーバから受信した関連するHTTP応答を表示および確認できるようにします。 |
| Traffic Monitorファイルの暗号化(Encrypt Traffic Monitor File) | <p>通常、すべてのセッションは、Traffic Monitorファイルに平文として記録されます。パスワードなどの機密情報をコンピュータに保存するこに不安を感じる場合は、ファイルの暗号化を選択できます。</p> <p>暗号化されたファイルは圧縮できません。このオプションを選択すると、ログファイルの入ったエクスポートされたスキャンのサイズが大幅に増加します。</p> <p>メモ: Traffic Viewerツールは、トラフィックファイルの暗号化をサポートしていません。[Traffic Monitorファイルの暗号化(Encrypt Traffic Monitor File)]オプションは、レガシトラフィックファイルがある特別な状況でのみ使用するために予約されています。</p> |
| Web探索と監査の最大再帰深度(Maximum crawl-audit recursion depth) | 攻撃によって脆弱性が明らかになった場合、Fortify WebInspectは、そのセッションをWeb探索し、表示されるすべてのリンクをたどります。そのWeb探索と監査によってさらに別のリソースへのリンクが示された場合、深さのレベルがインクリメントされ、検出されたリソースがWeb探索および監査されます。このプロセスは、他のリンクが見 |

| オプション | 説明 |
|-------|--|
| | つからなくなるまで繰り返し実行できます。ただし、無限ループに入ることがないように、再帰回数を制限できます。デフォルト値は2です。最大再帰レベルは1,000です。 |

Web探索の詳細

デフォルトでは、Fortify WebInspectは、ルートノードから始まり、すべての隣接ノード(1レベル下)を探索する幅優先(breadth-first)Web探索を使用します。その後、それらの最も近いノードごとに、未探索の隣接ノードが探索され、すべてのリソースが特定されるまで順に探索されます。次の図は、リンクされたページが幅優先Web探索を使用してアクセスされる順序を示しています。ノード1には、ノード2、3、および4へのリンクがあります。ノード2には、ノード5および6へのリンクがあります。



ユーザインターフェースでは、このWeb探索方法を変更できません。ただし、設定可能な [Web探索の詳細(Crawl Details)] オプションについて、次の表で説明します。

| オプション | 説明 |
|--|---|
| キーワード検索監査を有効にする (Enable keyword search audit) | キーワード検索は、その名前が示すように、サーバの応答を調べて、たいていの場合に脆弱性を示す特定のテキスト文字列を検索する攻撃エンジンを使用します。通常、このエンジンは、Web探索のみのスキャンでは使用されませんが、このオプションを選択して有効にできます。 |
| 冗長ページ検出の実行(Perform redundant page detection) | 非常にダイナミックなサイトでは、事実上同一の無限の数のリソース(ページ)が作成される可能性があります。各リソースの追跡を許可されると、Fortify WebInspectはスキャンを完了できなくなります。このオプションはページ構造を比較して類似性のレベルを判断し、Fortify WebInspectが冗長リソースの処理を識別して除外できるようにします。 |

重要! 冗長ページ検出は、スキャンのWeb探索部分で機能し

| オプション | 説明 |
|---|---|
| | <p>ます。監査の対象となるセッションが冗長になる場合、そのセッションがスキャンから除外されることはありません。</p> <p>冗長ページ検出では、次の設定を行えます。</p> <ul style="list-style-type: none"> ページ類似性のしきい値(Page Similarity Threshold) - 2つのページが冗長と見なされるのに必要な類似度を示します。1から100のパーセンテージを入力します。100は完全一致です。デフォルト設定は95%です。 含めるタグ属性(Tag attributes to include) - ページ構造に含めるタグ属性を示します。通常、タグ属性とその値は、構造を決定するときに削除されます。カンマ区切りリストでこのフィールドにタグ属性を指定すると、それらの属性とその値がページ構造に追加されます。デフォルトでは、「<code>id, class</code>」タグ属性が含まれます。 <p>ヒント: いくつかのサイトは、主に1種類のタグで構成されることがあります(例: <code><div></code>)。これらの属性を含めると、より厳密なページの照合が行われます。これらの属性を除外すると、照合の厳密度は低くなります。</p> |
| 1つのURLの最大ヒット数を以下に制限する(Limit maximum single URL hits to) | サイトの設定により、Web探索が同じURLを無限にループする場合があります。このフィールドを使用して、1つのURLがWeb探索される回数を制限します。デフォルト値は5です。 |
| ヒット数にパラメータを含める(Include parameters in hit count) | <p>【1つのURLの最大ヒット数を以下に制限する(maximum single URL hits to)】(上記)を選択すると、同じURLが検出されるたびにカウンタがインクリメントされます。ただし、【ヒット数にパラメータを含める(Include parameters in hit count)】も選択すると、HTTP要求で指定されたURLにパラメータが追加された場合に、Web探索プログラムは、そのリソースを1つのURLの上限までWeb探索します。異なるパラメータのセットは、それぞれ固有のものと見なされ、別のカウントが行われます。</p> <p>たとえば、このオプションを選択すると、「<code>page.aspx?a=1</code>」と「<code>page.aspx?b=1</code>」の両方が固有のリソースとしてカウントされます(つまり、Web探索プログラムが2つのページを検出したことを意味します)。</p> <p>このオプションを選択しない場合、「<code>page1.aspx?a=1</code>」と</p> |

| オプション | 説明 |
|---|---|
| | <p>「page.aspx?b=1」は同じリソースとして扱われます(つまり、Web探索プログラムが同じページを2度検出したことを意味します)。</p> <p>メモ: この設定は、GETとPOSTの両方のパラメータに適用されます。</p> |
| ディレクトリの最大ヒット数を以下に制限する(Limit maximum directory hit count to) | <p>この設定では、Web探索中に各ディレクトリ内で一巡するサブディレクトリおよびページの最大数を定義します。この設定は、Web探索の範囲を縮小し、コンテンツ管理システム(CMS)で構成されるサイトなど、一部のサイトのスキャン時間を短縮するのに役立ちます。デフォルト設定は200です。</p> |
| 最小フォルダ深度 (Minimum folder depth) | <p>【ディレクトリの最大ヒット数を以下に制限する(Limit maximum directory hit count to)】(上記)を選択した場合、この設定は、ディレクトリの最大ヒット数の適用を開始するフォルダの深さを定義します。デフォルト設定は1です。</p> |
| リンクトラバーサルシーケンスの最大数を以下に制限する (Limit maximum link traversal sequence to) | <p>このオプションは、Fortify WebInspectがサイトをWeb探索するときに連続してアクセスできるハイパーテインクの数を制限します。たとえば、5つのリソースが次のようにリンクされている場合、</p> <ul style="list-style-type: none"> ・ページAにページBへのハイパーテインクが含まれている ・ページBにページCへのハイパーテインクが含まれている ・ページCにページDへのハイパーテインクが含まれている ・ページDにページEへのハイパーテインクが含まれている <p>このオプションを「3」に設定すると、ページEはWeb探索されません。デフォルト値は15です。</p> |
| Web探索フォルダの最大深度を以下に制限する(Limit maximum Crawl folder depth to) | <p>このオプションは、1つの要求に含めることができるディレクトリの数を制限します。デフォルト値は15です。</p> <p>たとえば、次のURLの場合、</p> <p>http://www.mysite.com/Dir1/Dir2/Dir3/Dir4/Dir5/Dir6/Dir7</p> <p>このオプションを「4」に設定すると、ディレクトリ5、6、および7の内容はWeb探索されません。</p> |
| Web探索の最大数を以下に制限する (Limit maximum crawl count to) | <p>この機能は、Web探索プログラムによって送信されるHTTP要求の数を制限します。大規模サイトのスキャンの完了に問題が発生した場合にのみ使用する必要があります。</p> |

| オプション | 説明 |
|---|---|
| | <p>メモ: ここで設定した制限は、スキャン中に表示される「Web探索済み(Crawled)」進行状況バーには直接関連していません。ここで設定したWeb探索の最大数は、アプリケーションのWeb探索中にWeb探索プログラムによって検出されたリンクに適用されます。「Web探索済み(Crawled)」進行状況バーには、Web探索中にWeb探索プログラムによって検出されたリンクだけではなく、Web探索と監査中にリンクの解析が行われるすべてのセッション(要求と応答)が含まれます。</p> |
| Webフォームの最大送信数を以下に制限する(Limit maximum Web form submission to) | <p>通常、Fortify WebInspectは、複数のオプションを持つコントロール(リストボックスなど)が含まれているフォームを検出すると、リストから最初のオプション値を抽出してフォームを送信します。次に、2番目のオプション値を抽出してフォームを再送信し、リスト内のすべてのオプション値が送信されるまでこのプロセスを繰り返します。これにより、可能なすべてのリンクを確実にたどることができます。</p> <p>ただし、値の完全なリストを送信すると逆効果になる場合があります。たとえば、「State」という名前のリストボックスに、米国の50州それぞれについて1つの値が含まれている場合、フォームのインスタンスを50件送信する必要はありません。</p> <p>この設定を使用して、Fortify WebInspectが実行する送信の総数を制限します。デフォルト値は3です。</p> |
| 反復パスセグメントの抑止(Suppress Repeated Path Segments) | <p>多くのサイトには、相対パスのようでありながら、Fortify WebInspectによる解析と、Web探索対象のURLへの追加が済むと、使用不能なURLになるテキストがあります。こうしたものの出現は、パスが連続して追加される場合(/foo/bar/foo/bar/など)に、暴走スキャンになるおそれがあります。こうしたものの出現を減らす上でこの設定は役に立ち、デフォルトで有効になっています。</p> <p>この設定が有効な場合、次のオプションがあります。</p> <p>1 - URL内のどこかで繰り返されている単一のサブフォルダを検出し、一致がある場合はそのURLを拒否します。たとえば、/foo/baz/bar/foo/では「/foo/」が繰り返されているので一致します。この繰り返しは隣接している必要はありません。</p> <p>2 -隣接するサブフォルダの2つ以上のペアを検出し、一致がある場合はURLを拒否します。たとえば、/foo/bar/baz/foo/bar/では「/foo/bar/」が繰り返されているので一致します。</p> <p>3 -隣接する3つのサブフォルダの2つ以上のセットを検出し、一致が</p> |

| オプション | 説明 |
|-------|---|
| | <p>ある場合はURLを拒否します。</p> <p>4 -隣接する4つのサブフォルダの2つ以上のセットを検出し、一致がある場合はURLを拒否します。</p> <p>5 -隣接する5つのサブフォルダの2つ以上のセットを検出し、一致がある場合はURLを拒否します。</p> <p>この設定が無効な場合、サブフォルダの繰り返しは検出されず、一致が原因でURLが拒否されることはありません。</p> |

スキャン設定: JavaScript

この機能にアクセスするには、[編集(Edit)]メニューをクリックし、[デフォルトのスキャン設定(Default Scan Settings)]または[現在のスキャン設定(Current Scan Settings)]を選択します。その後で、[スキャン設定(Scan Settings)]カテゴリで、[JavaScript]を選択します。

JavaScriptの設定

JavaScriptアナライザを使用すると、Fortify WebInspectは、JavaScriptによって定義されたリンクをWeb探索し、JavaScriptによってレンダリングされたドキュメントを作成して監査することができます。

ヒント: スクリプトの分析中にFortify WebInspectがWeb探索を実行する速度を上げるには、イメージ/写真が表示されないようにブラウザオプションを変更します。

次の表の説明に従って設定を行います。

| オプション | 説明 |
|---|---|
| スクリプト実行で検出されたリンクをWeb探索する(Crawl links found from script execution) | このオプションを選択した場合は、Web探索プログラムがダイナミックリンク(つまり、JavaScriptの実行中に生成されたリンク)をたどります。 |
| 詳細スクリプトパーサのデバッグルог記録(Verbose script parser debug) | この設定を選択し、かつ[ログレベルのアプリケーション設定(Application setting for logging level)]が[デバッグ(Debug)]に設定されている場合、Fortify WebInspectはDOMオブジェクトで呼び出されたすべてのメソッドをログに記録します。これにより、中規模 |

| オプション | 説明 |
|--|--|
| logging) | サイトや大規模サイト用の数ギガバイトのデータを簡単に作成できます。 |
| JavaScriptエラーのログ記録(Log JavaScript errors) | Fortify WebInspectは、スクリプト解析エンジンからのJavaScript解析エラーをログに記録します。 |
| JS Framework UI除外の有効化(Enable JS Framework UI Exclusions) | このオプションが選択されている場合、Fortify WebInspectのJavaScriptパーサは、カレンダーコントロールやリボンバーなどの一般的なJQueryおよびExt JSユーザインターフェースコンポーネントを無視します。その後、これらの項目はスキャン中にJavaScript実行から除外されます。 |
| 1ページあたりの最大スクリプトイベント数(Max script events per page) | 特定のスクリプトは、同じイベントを無限に実行します。単一のページで許容されるイベントの数を、1-9999の値に制限できます。デフォルト値は1000です。 |
| サイト全体のイベント削減の有効化(Enable Site-Wide Event Reduction) | このオプションが選択されている場合、Web探索プログラムとJavaScriptエンジンは、Webサイトのさまざまな部分に表示される共通の機能エリア(共通メニューやページフッタなど)を認識します。これにより、すでにWeb探索済みのHTMLコンテンツ内のダイナミックリンクやフォームを検索する必要がなくなり、その結果、スキャンが高速化します。このオプションはデフォルトで有効であり、通常、無効にすべきではありません。 |
| SPAサポート(SPA Support) | <p>SPAサポートは、シングルページアプリケーションに適用されます。有効にすると、DOMスクリプトエンジンは、Web探索中に、JavaScriptインクルード、フレームとiframeのインクルード、CSSファイルリンクルード、およびAJAX呼び出しを検索してから、それらのイベントによって生成されたすべてのトラフィックを監査します。</p> <p>SPAサポートのオプションを以下に示します。</p> <ul style="list-style-type: none"> 自動(Automatic) - Fortify WebInspectがSPAフレームワークを検出すると、自動的にSPAサポートモードに切り替わります。 有効(Enabled) - SPAフレームワークがターゲットアプリケーションで使用されていることを示します。 <p>注意! SPAサポートは、シングルページアプリケーションに対してのみ有効にするべきです。SPAサポートを有効にしてSPA以外のWebサイトをスキャンすると、スキャンが遅くなります。</p> |

| オプション | 説明 |
|-------|--|
| | <ul style="list-style-type: none"> 無効(Disabled) - SPAフレームワークがターゲットアプリケーションで使用されていないことを示します。 <p>詳細については、「"シングルページアプリケーションスキャンについて"ページ210」を参照してください。</p> |

スキャン設定: リクエスタ

リクエスタは、HTTP要求と応答を処理するソフトウェアモジュールです。

この機能にアクセスするには、[編集(Edit)]メニューをクリックし、[デフォルトのスキャン設定(Default Scan Settings)]または[現在のスキャン設定(Current Scan Settings)]を選択します。その後で、[スキャン設定(Scan Settings)]カテゴリで、[リクエスタ(Requestor)]を選択します。

リクエスタパフォーマンス(Requestor Performance)

[リクエスタパフォーマンス(Requestor Performance)]オプションについて、次の表で説明します。

| オプション | 説明 |
|--|--|
| 共有リクエスタを使用する(Use a shared requestor) | このオプションを選択すると、Web探索プログラムと監査プログラムは、サイトのスキャン時に共通のリクエスタを使用し、各スレッドは同じ状態を使用します。この状態も両方のモジュールで共有されます。これは以前のバージョンのFortify WebInspectで使用されていた手法を再現するものであり、状態の維持が重要な考慮事項ではない場合に適しています。スレッドの最大数(最大75)も指定します。 |
| 個別のリクエスタを使用する(Use separate requestors) | このオプションを選択した場合、Web探索プログラムと監査プログラムは別々のリクエスタを使用します。また、監査プログラムのリクエスタは、すべてのスレッドで同じ状態を使用するのではなく、各スレッドに状態を関連付けます。この方法により、スキャンが大幅に高速になります。 |

Web探索および監査を実行するとき、リクエスタごとに作成できるスレッドの最大数を指定できます。[Web探索リクエスタスレッド数(Crawl requestor thread count)]オプションでは、最大25の同時HTTP要求を送信してから、最初の要求に対するHTTP応答を待

| オプション | 説明 |
|-------|---|
| | <p>機するように設定できます。デフォルト設定は5です。</p> <p>監査リクエスタスレッド数(Audit requestor thread count)]は、最大50に設定できます。デフォルト設定は10です。スレッド数を増やすと、スキャンの速度を速くすることができますが、スキャンするサーバのリソースだけでなく、システムリソースも消費し尽くされる場合があります。</p> <p>メモ: スキャンするアプリケーションの容量によっては、スレッド数を増やすと、サーバの負荷が増大するために要求の失敗が増加し、一部の応答が要求タイムアウト(Request timeout)]設定を超える場合があります。要求の失敗によってスキャンのカバレッジが縮小する可能性があります。これは、失敗した応答によって、追加の攻撃露呈部分が明らかになったり脆弱性が表面化したりした可能性があるためです。要求の失敗の増加に気付いた場合は、それを縮小するために要求タイムアウト(Request timeout)]を大きくしたり、[Web探索リクエスタスレッド数(Crawl requestor thread count)]と監査リクエスタスレッド数(Audit requestor thread count)]を小さくしたりすることができます。</p> <p>また、スキャンするアプリケーションの性質によっては、Web探索スレッド数の増加により、同じサイトの後続のスキャンどうしの整合性が低下する場合があります。これはWeb探索要求の順序が異なることが原因です。デフォルトの[Web探索リクエスタスレッド数(Crawl requestor thread count)]設定を1に減らすと、整合性が向上する可能性があります。</p> |

リクエスタ設定(Requestor Settings)

[リクエスタ設定(Requestor Settings)]オプションについて、次の表で説明します。

| オプション | 説明 |
|---|--|
| 最大応答サイズを以下に制限する(Limit maximum response size to) | このオプションを選択すると、受け入れるサーバ応答のサイズを制限し、最大サイズ(キロバイト単位)を指定できます。デフォルトは1000キロバイトです。Flashファイル(.swf)およびJavaScriptの「include」ファイルは、この制限を受けないことに注意してください。 |
| 要求の再試行回数(Request retry) | 「failed」応答(ソケットエラーまたは要求タイムアウトとして定義されます)を受信した後に、Fortify WebInspectがHTTP要求を再送信 |

| オプション | 説明 |
|-------------------------------|---|
| count) | する回数を指定します。値はゼロより大きくする必要があります。 |
| 要求タイムアウト (Request timeout) | Fortify WebInspectがサーバからのHTTP応答を待つ時間を指定します。このしきい値を超えると、Fortify WebInspectは、再試行回数に達するまで要求を再送信します。Fortify WebInspectは、応答を受信しない場合、タイムアウトをログに記録し、次の一連の攻撃の最初のHTTP要求を送信します。デフォルト値は20秒です。 メモ: タイムアウトが初めて発生したときに、Fortify WebInspectはタイムアウト期間を延長し、サーバが応答していないことを確認します。延長された要求タイムアウト時間内にサーバが応答した場合、その延長期間が現在のスキャンの新しい要求タイムアウトになります。 |

コネクティビティの喪失が検出された場合にスキャンを停止する(Stop Scan if Loss of Connectivity Detected)

スキャン中に、Webサーバで障害が発生したり、過度にビジーになって、タイミングよく応答できなくなったりする場合があります。タイムアウトの回数にしきい値を指定することで、スキャンを終了するようにFortify WebInspectに指示できます。

次の表で、オプションについて説明します。

| オプション | 説明 |
|---|--|
| スキャンを停止するまでの「単一ホスト」の連続した再試行失敗数 (Consecutive "single host" retry failures to stop scan) | 1つの特定のサーバで許可される連続タイムアウトの数を入力します。デフォルト値は75です。 |
| スキャンを停止するまでの「すべてのホスト」の連続した再試行失敗数 (Consecutive "any host" retry failures to stop scan) | すべてのホストで許可される連続タイムアウトの総数を入力します。デフォルト値は150です。 |

| オプション | 説明 |
|--|--|
| スキャンを停止するまでの「单一ホスト」の非連続の再試行失敗数 (Nonconsecutive "single host" retry failures to stop scan) | 1つのホストで許可される非連続タイムアウトの総数を入力します。デフォルト値は「無制限」です。 |
| スキャンを停止するまでの「すべてのホスト」の非連続の再試行失敗数 (Nonconsecutive "any host" retry failures to stop scan) | すべてのホストで許可される非連続のタイムアウトの総数を入力します。デフォルト値は350です。 |
| 最初の要求が失敗した場合にスキャンを停止する>If first request fails, stop scan) | このオプションを選択すると、ターゲットサーバがFortify WebInspectの最初の要求に応答しない場合に、Fortify WebInspectで強制的にスキャンが終了されます。 |
| 受信した場合にスキャンを停止する応答コード(Response codes to stop scan if received) | 受信した場合に、Fortify WebInspectで強制的にスキャンが終了されるHTTPステータスコードを入力します。カンマを使用してエントリを区切ります。コードの範囲(両端を含む)を指定するにはハイフンを使用します。 |

スキャン設定: セッション除外

この機能にアクセスするには、[編集(Edit)]メニューをクリックし、[デフォルトのスキャン設定(Default Scan Settings)]または[現在のスキャン設定(Current Scan Settings)]を選択します。その後で、[スキャン設定(Scan Settings)]カテゴリで、[セッション除外(Session Exclusions)]を選択します。

これらの設定は、Fortify WebInspect脆弱性スキャンのWeb探索と監査の両方のフェーズに適用されます。Web探索のみまたは監査のみの除外を指定するには、[Web探索設定:

セッション除外 (Crawl Settings: Session Exclusions)] または 駿査設定: セッション除外 (Audit Settings: Session Exclusions)] を使用します。

除外または拒否するファイル拡張子

ファイルのタイプを指定して、そのファイルを除外するか拒否するかを指定できます。

- 拒否 (Reject) - Fortify WebInspectは、指定したタイプのファイルを要求しません。
- 除外 (Exclude) - Fortify WebInspectはファイルを要求しますが、(駿査中に)それらのファイルを攻撃したり、それらのファイルで他のリソースへのリンクを検査したりしません。

デフォルトでは、ほとんどのイメージ、描画、メディア、オーディオ、ビデオ、および圧縮ファイルのタイプは拒否されます。

拒否または除外するファイル拡張子を追加するには:

- 「追加 (Add)」] をクリックします。
除外拡張子 (Exclusion Extension)] ウィンドウが開きます。
- 「ファイル拡張子 (File Extension)」] ボックスに、ファイル拡張子を入力します。
- 「拒否 (Reject)」] と 「除外 (Exclude)」] のどちらかまたは両方を選択します。
- 「OK」] をクリックします。

除外 MIMEタイプ

Fortify WebInspectは、指定したMIMEタイプに関連付けられたファイルを処理しません。デフォルトでは、イメージ、オーディオ、およびビデオのタイプは除外されます。

除外する MIMEタイプを追加するには:

- 「追加 (Add)」] をクリックします。
除外するMimeタイプの指定 (Provide a Mime-type to Exclude)] ウィンドウが開きます。
- 「Mimeタイプの除外 (Exclude Mime-type)」] ボックスに、MIMEタイプを入力します。
- 「OK」] をクリックします。

その他の除外/拒否基準

HTTPメッセージのさまざまなコンポーネントを特定してから、そのコンポーネントを含むセッションを除外するか拒否するかを指定できます。

- 拒否 (Reject) - Fortify WebInspectは、指定されたホストまたはURLにHTTP要求を送信しません。たとえば、通常、サイトからのログオフを処理するURLは拒否する必要があります。これは、スキャンが完了する前にアプリケーションからログアウトしたくないためです。
- 除外 (Exclude) - Web探索中に、Fortify WebInspectは、指定されたURLまたはホストで他のリソースへのリンクを調査しません。スキャンの駿査部分の間は、Fortify WebInspectが指定されたホストまたはURLを攻撃しません。HTTP応答を処理せずにURLまたはホストにアクセスする場合は、「除外 (Exclude)」] オプションを選択しますが、「拒否 (Reject)」] は

選択しません。たとえば、処理しないURL上 の壊れたリンクをチェックするには、**除外(Exclude)**]オプションだけを選択します。

基準の編集

デフォルトの基準を編集するには:

1. 基準を選択して、**編集(Edit)**](**その他の除外/拒否基準(Other Exclusion/Rejection Criteria)**]リストの右側にある)をクリックします。
[ホストまたはURLの拒否 または除外(Reject or Exclude a Host or URL)] ウィンドウが開きます。
2. **ホスト(Host)**]または **URL**]を選択します。
3. **ホスト/URL(Host/URL)**]ボックスに、URLまたは完全修飾ホスト名、またはターゲットのURLまたはホストに一致するように設計された正規表現を入力します。
4. **拒否(Reject)**]と **除外(Exclude)**]のどちらかまたは両方を選択します。
5. **OK**]をクリックします。

基準の追加

除外/拒否基準を追加するには:

1. **追加(Add)**](**その他の除外/拒否基準(Other Exclusion/Rejection Criteria)**]リストの右側にある)をクリックします。
[除外の作成(Create Exclusion)] ウィンドウが開きます。
2. **ターゲット(Target)**]リストから項目を選択します。
3. ターゲットとして **クエリパラメータ(Query Parameter)**]または **ポストパラメータ(Post Parameter)**]を選択した場合は、**ターゲット名(Target Name)**]を入力します。
4. **一致タイプ(Match Type)**]リストから、ターゲット内のテキストの一一致に使用される方法を選択します。
 - **正規表現に一致(Matches Regex)**]- **一致文字列(Match String)**]ボックスで指定した正規表現に一致します。
 - **正規表現の拡張に一致(Matches Regex Extension)**]- **一致文字列(Match String)**]ボックスで指定したFortify正規表現の拡張から入手可能な構文に一致します。
 - **一致(Matches)**]- **一致文字列(Match String)**]ボックスで指定したテキスト文字列に一致します。
 - **含む(Contains)**]- **一致文字列(Match String)**]ボックスで指定したテキスト文字列を含みます。
5. **一致文字列(Match String)**]ボックスに、ターゲットで検索する文字列または正規表現を入力します。または、**一致タイプ(Match Type)**]で正規表現オプションを選択した場合は、ドロップダウン矢印をクリックして、**正規表現の作成(Create Regex)**]を選択し、Regular Expression Editorを起動します。

6.  をクリックします(または<Enter>を押します)。
7. (オプション)ステップ2-6を繰り返して、条件を追加します。複数の一致はAND処理されます。
8. 現在の設定(Current Settings)]で作業している場合は、[テスト(Test)]をクリックして現在のスキャンの除外を処理できます。基準によって絞り込まれたそのスキャンからのセッションがテスト画面に表示され、必要に応じて設定を変更できます。
9. [OK]をクリックします。
10. [その他の除外/拒否基準(Other Exclusion/Rejection Criteria)]リストに除外が表示されている場合は、[拒否(Reject)]と[除外(Exclude)]のいずれかまたは両方を選択します。

メモ: スキャン中は、応答タイプ、応答ヘッダタイプ、およびステータスコードターゲットタイプを拒否することができません。これらのターゲットタイプは除外することしかできません。

例 1

Microsoft.comのリソースに対する要求を無視して送信しないようにするには、次の除外を入力して、[拒否(Reject)]を選択します。

| ターゲット(Target) | ターゲット名(Target Name) | 一致タイプ(Match Type) | 一致文字列(Match String) |
|---------------|---------------------|-------------------|---------------------|
| URL | N/A | 含む(contains) | Microsoft.com |

例 2

一致文字列として「logout」と入力します。この文字列がURLの任意の部分で見つかった場合は、そのURLが除外または拒否されます(選択されたオプションによって異なる)。「logout」の例を使用すると、Fortify WebInspectは、logout.aspやapplogout.jspなどのURLを除外または拒否します。

| ターゲット(Target) | ターゲット名(Target Name) | 一致タイプ(Match Type) | 一致文字列(Match String) |
|---------------|---------------------|-------------------|---------------------|
| URL | N/A | 含む(contains) | logout |

例 3

次の例では、クエリパラメータ「username」が「John」と等しいクエリを含むセッションを拒否または除外します。

| ターゲット(Target) | ターゲット名(Target Name) | 一致タイプ(Match Type) | 一致文字列(Match String) |
|---------------|---------------------|-------------------|---------------------|
| | | | |

| | Name) | (Match Type) | (Match String) |
|---------------------------|----------|--------------|----------------|
| クエリパラメータ(Query parameter) | username | 一致(matches) | John |

例4

次の例では、次のディレクトリを除外または拒否します。

http://www.test.com/W3SVC55/

http://www.test.com/W3SVC5/

http://www.test.com/W3SVC550/

| ターゲット (Target) | ターゲット名 (Target Name) | 一致タイプ (Match Type) | 一致文字列 (Match String) |
|----------------|----------------------|-------------------------|----------------------|
| URL | N/A | 正規表現に一致 (matches regex) | /W3SVC[0-9]*/ |

スキャン設定: 許可ホスト

この機能にアクセスするには、[編集(Edit)]メニューをクリックし、[デフォルトのスキャン設定(Default Scan Settings)]または[現在のスキャン設定(Current Scan Settings)]を選択します。その後で、[スキャン設定(Scan Settings)]カテゴリで、[許可ホスト(Allowed Hosts)]を選択します。

許可ホスト設定の使用

[許可ホスト(Allowed Host)]設定は、Web探索して監査するドメインを追加する場合に使用します。Webプレゼンスで複数のドメインが使用されている場合は、それらのドメインをここに追加します。たとえば、「Wexample.com」をスキャンする場合、「Wexample2.com」と「Wexample3.com」がWebプレゼンスの一部であり、かつそれらをWeb探索と監査に含めたいのであれば、それらのドメインをここに追加する必要があります。

この機能を使用して、指定したテキストが名前に含まれているドメインをスキャンすることができます。たとえば、スキャンターゲットとして「www.myco.com」を指定し、許可ホストとして「myco」と入力したとします。Fortify WebInspectは、ターゲットサイトをスキャンして「myco」を含むURLへのリンクを検出すると、そのリンクをたどってそのサイトのサーバをスキャンします。この処理は、すべてのリンク先のサイトがスキャンされるまで繰り返されます。この仮説例では、Fortify WebInspectによって次のドメインがスキャンされます。

- www.myco.com:80
- contact.myco.com:80
- www1.myco.com
- ethics.myco.com:80
- contact.myco.com:443
- wow.myco.com:80
- mycocorp.com:80
- www.interconnection.myco.com:80

許可されたドメインの追加

許可するドメインを追加するには:

1. **追加 (Add)**]をクリックします。
2. **許可ホストの指定 (Specify Allowed Host)**]ウィンドウで、URL (またはURLを表す正規表現)を入力し、**OK**]をクリックします。

メモ: URLを指定する場合は、プロトコル指定子 (http://やhttps://など)を含めないでください。

ドメインの編集または削除

許可されたドメインを編集または削除するには:

1. **許可ホスト(Allowed Hosts)**]リストからドメインを選択します。
2. **編集 (Edit)**]または **削除 (Remove)**]をクリックします。

スキャン設定: HTTP解析

この機能にアクセスするには、**編集 (Edit)**]メニューをクリックし、**デフォルトのスキャン設定 (Default Scan Settings)**]または**現在のスキャン設定 (Current Scan Settings)**]を選択します。その後で、**スキャン設定 (Scan Settings)**]カテゴリで、**HTTP解析 (HTTP Parsing)**]を選択します。

オプション

[HTTP解析(HTTP Parsing)]オプションについて、次の表で説明します。

| オプション | 説明 |
|---|--|
| 状態に使用されるHTTPパラメータ(HTTP Parameters Used for State) | <p>お使いのアプリケーションでWebサイト内の状態を維持するためにURLの書き換えまたはPOSTデータの手法を使用する場合は、使用するパラメータを指定する必要があります。たとえば、PHPスクリプトでは、セッション内で使用できる、SIDという名前のセッションIDの定数を作成できます。これをURLの末尾に追加すると、そのセッションIDを次のページで使用できるようになります。実際のURLは次のようにになります。</p> <p>.../page7.php?PHPSESSID=4725a759778d1be9bdb668a236f01e01</p> <p>セッションIDは接続ごとに変更されるため、このURLを含むHTTP要求を再生しようとするとエラーが発生します。ただし、パラメータ(この例ではPHPSESSID)を指定すると、Fortify WebInspectは、接続が確立されたたびに、割り当てられた値を、サーバから取得された新しいセッションIDに置き換えます。</p> <p>同様に、一部の状態管理手法では、POSTデータを使用して情報を渡します。たとえば、HTTPメッセージのコンテンツに、<code>userid=slbhkelvbkI73dhj</code>が含まれている場合があります。この場合、「<code>userid</code>」はユーザが指定するパラメータです。</p> <p>メモ: パラメータを指定する必要があるのは、アプリケーションが状態の管理にURLの書き換えまたはPOSTされたデータを使用する場合のみです。クッキーを使用する場合は必要ありません。</p> <p>WebInspectは、潜在的なパラメータがPOSTされたデータとして出現する場合、またはURLのクエリ文字列内に存在する場合に、そのパラメータを特定できます。ただし、アプリケーションでセッションデータが拡張パス情報としてURLに埋め込まれている場合は、それを識別する正規表現を指定する必要があります。次の例では、「1234567」がセッション情報です。</p> <p><code>http://www.onlinestore.com/bikes/(1234567)/index.html</code></p> <p>パラメータを識別するための正規表現は、<code>\w\d+</code>です。</p> |
| CSRFを有効にする(Enable CSRF) | [CSRFを有効にする(Enable CSRF)]オプションは、スキャンしているサイトにクロスサイトリクエストフォージェリ(CSRF)トークンが含まれている場合にのみオンにする必要があります。これをオンにするとプロセスのオーバーヘッドが追加されるためです。詳細については、「 "CSRF" ページ395 」を参照してください。 |

| オプション | 説明 |
|---|---|
| URLパスから状態を判断する(Determine State from URL Path) | アプリケーションがURLパス内の特定のコンポーネントから状態を判断する場合は、このチェックボックスを選択して、それらのコンポーネントを識別する1つ以上の正規表現を追加します。2つのデフォルトの正規表現は、ASP.NETの2つのクッキーレスセッションIDを識別します。3番目の正規表現はjsessionidクッキーに対応します。 |
| 応答状態ルールを有効にする(Enable Response State Rules) | <p>お使いのアプリケーションが、ベアトークンを使用してクライアントの状態を維持している場合は、このオプションを選択して、応答からベアトークンを識別し、次の要求に自動的に追加するルールを作成します。</p> <p>メモ: [自動応答状態ルール(Auto Response State Rules)]オプションはデフォルトで有効に設定され、ベアトークンの自動検出用に事前定義された複数のルールを提供します。次の手順で説明するように、応答状態ルールを有効にして、ルールを追加することにより、ベアトークンの自動検出を強化できます。</p> |

ルールを追加するには:

1. [応答状態ルールを有効にする(Enable Response State Rules)] チェックボックスを選択した後に、[追加(Add)]をクリックします。[ルールの検索と置換(Rule Search and Replace)] ウィンドウが表示されます。
 2. [ルール名(Rule Name)] フィールドに、ルールの固有名を入力します。例: Bearer。
 3. [応答での検索(Search in Response)] フィールドの横の[追加(Add)]をクリックします。[応答での検索(Search in Response)] ダイアログボックスが簡易モードで開きます。
 4. 次のいずれかを実行します。
 - 簡易モードでルールを作成するには、トークンが含まれているテキストを [ルール(Rule)] ボックスに入力します。入力すると、正規表現が [正規表現表示(Regex View)] ボックスに自動的に生成されます。
- ヒント:** *i* をクリックすると、事前定義されたトークンのリストが表示されます。

| オプション | 説明 |
|-------|---|
| | <ul style="list-style-type: none"> 事前定義された正規表現を使用するには、[正規表現モード (Regex Mode)]を選択し、[正規表現 (Regex)]リストから正規表現ステートメントを選択します。これで、選択されたステートメントを編集できます。 <p>5. [OK]をクリックします。</p> <p>正規表現が検証されます。先に進む前に、見つかったエラーをすべて修正する必要があります。</p> <p>6. [要求での置換 (Replace in Request)]フィールドの横の[追加 (Add)]をクリックします。</p> <p>[要求での置換 (Replace in Request)]ダイアログボックスが簡易モードで開きます。</p> <p>メモ: 以前に正規表現モードを選択していた場合は、ダイアログボックスは正規表現モードで開きます。</p> <p>7. 次のいずれかを実行します。</p> <ul style="list-style-type: none"> 簡易モードでルールを作成するには、トークンが含まれているテキストを[ルール (Rule)]ボックスに入力します。入力すると、正規表現が[正規表現表示 (Regex View)]ボックスに自動的に生成されます。 <p>ヒント:  をクリックすると、事前定義されたトークンのリストが表示されます。</p> <ul style="list-style-type: none"> 事前定義された正規表現を使用するには、[正規表現モード (Regex Mode)]を選択し、[正規表現 (Regex)]リストから正規表現ステートメントを選択します。これで、選択されたステートメントを編集できます。 <p>8. [OK]をクリックします。</p> <p>正規表現が検証されます。先に進む前に、見つかったエラーをすべて修正する必要があります。</p> <p>9. [OK]をクリックして、[ルールの検索と置換 (Rule Search and Replace)]ウィンドウを閉じます。</p> <p>重要! システムリソースを消費し、スキャンのパフォーマンスに影響を与える可能性のある正規表現が使用されないようにするために、正規表現の構築時に以下のテキスト文字列は使用しないでください。</p> <ul style="list-style-type: none"> 無限数を表す".*"または".+?"を使用する文字 肯定先読み"(?=...)" |

| オプション | 説明 |
|---|---|
| | <ul style="list-style-type: none"> 否定先読み"(?!...)" 肯定後読み"(?<=...)" 否定後読み"(?<!...)" |
| ナビゲーションに使用されるHTTPパラメータ(HTTP Parameters Used for Navigation) | <p>一部のサイトでは、直接アクセスできるリソースは1つだけであり、要求された情報を提供するためにクエリ文字列を使用します。以下にいくつかの例を示します。</p> <p>例: 1 – http://www.anysite.com?Master.asp?Page=1 例: 2 – http://www.anysite.com?Master.asp?Page=2 例: 3 – http://www.anysite.com?Master.asp?Page=13;Subpage=4</p> <p>通常、Fortify WebInspectでは、これらの3つの要求が同じリソースを参照していると想定し、それらの1つに対してのみ脆弱性スキャンを実行します。そのため、ターゲットのWebサイトでこのタイプのアーキテクチャを採用する場合、使用される特定のリソースパラメータを識別する必要があります。</p> <p>例1と2には、「Page」という1つのリソースパラメータが含まれています。例3には、「Page」と「Subpage」という2つのパラメータが含まれています。</p> <p>リソースパラメータを識別するには:</p> <ol style="list-style-type: none"> 「追加(Add)」をクリックします。 「HTTPパラメータ(HTTP Parameter)」ウィンドウで、パラメータ名を入力して、「OK.」をクリックします。 <p>入力した文字列が「パラメータ(Parameter)」リストに表示されます。</p> <ol style="list-style-type: none"> 追加のパラメータについて上記の手順を繰り返します。 |
| 高度なHTTP解析(Advanced HTTP Parsing) | <p>ほとんどのWebページには、使用する文字セットをブラウザに知らせる情報が含まれています。この指示は、HTMLドキュメントのHEADセクションのContent-Type応答ヘッダ(またはHTTP-EQUIV属性を持つMETAタグ)を使用して行われます。</p> <p>文字セットが示されていないページでは、Fortify WebInspectで使用すべき言語ファミリ(および暗黙の文字セット)を指定できます。</p> |
| 値のみ存在する場合にクエリパラメータ値をパラメータ名として扱 | <p>この設定は、Fortify WebInspectが値のないクエリパラメータを解釈する方法を定義します。次に例を示します。</p> <p><code>http://somehost?param</code></p> <p>このチェックボックスが選択されている場合、Fortify WebInspectは、空の</p> |

| オプション | 説明 |
|---|---|
| う(Treat query parameter value as parameter name when only value is present) | <p>値を持つ「param」という名前のパラメータとして「param」を解釈します。このチェックボックスがオフの場合、Fortify WebInspectは、値「param」を持つ名前のないパラメータとして「param」を解釈します。</p> <p>この設定は、Fortify WebInspectがヒットカウントを計算する方法に影響することがあります(「スキャン設定: 全般」の"1つのURLの最大ヒット数を以下に制限する(Limit maximum single URL hits to)" ページ377の設定を参照してください)。この設定は、URLにアンチキャッシング(anti-caching)パラメータが含まれているシナリオで役に立ちます。多くの場合、これらは数値カウンタまたはタイムスタンプの形式になります。たとえば、以下のパラメータは数値カウンタです。</p> <ul style="list-style-type: none"> • <code>http://somehost?1234567</code> • <code>http://somehost?1234568</code> <p>この場合、値は要求ごとに変わります。値がパラメータ名として処理され、[ヒット数にパラメータを含める(Include parameters in hit count)]設定がオンになっている場合、Web探索のカウントが人為的に引き上げられて、スキャン時間が長くなる可能性があります。このような場合は、値のみ存在する場合にクエリパラメータ値をパラメータ名として扱う(Treat query parameter value as parameter name when only value is present)】チェックボックスをオフにすると、これらのカウンタがヒットカウントに影響しないようになり、スキャン時間がより適切なものとなります。</p> |

CSRF

[CSRFを有効にする(Enable CSRF)]オプションは、スキャンしているサイトにクロスサイトリクエストフォージェリ(CSRF)トークンが含まれている場合にのみオンにする必要があります。これをオンにするとプロセスのオーバーヘッドが追加されるためです。

CSRFについて

クロスサイトリクエストフォージェリ(CSRF)はWebサイトの悪意のあるエクスプロイトであり、Webサイトが信頼するユーザのブラウザから不正なコマンドが送信されます。CSRFエクスプロイトは、サイトがユーザのブラウザで置いている信頼に便乗します。つまり、ユーザがサイトによってすでに認証され、信頼チェーンがまだ開いているという事実を利用します。

例:

ユーザが銀行にアクセスして認証を受け、ユーザのマシンにクッキーが残されます。ユーザは、銀行取引を完了すると、別のブラウザタブに切り替えて、自分の趣味をテーマにし

た、愛好家のWebサイトでやり取りを継続します。サイト上で、誰かがHTMLイメージ要素を含むメッセージを投稿していました。このHTMLイメージ要素には、口座からすべての現金を引き出して別の口座に振り込むという、ユーザの銀行に対する要求が含まれています。ユーザのデバイスにはまだ期限切れではないクッキーがあるため、取引が履行され、口座内のすべての資金が引き出されます。

多くの場合、CSRFエクスプロイトにはユーザの識別情報に対する信頼に依存するサイトが関わっています。多くの場合、その信頼は、クッキーの使用を通して維持されます。次いで、ユーザのブラウザはまだされて、ユーザのブラウザとターゲットサイトとの間にまだ信頼が存在していると思って、ターゲットサイトにHTTP要求を送信します。

CSRFトークンの使用

クロスサイトリクエストフォージェリの発生を阻止する一般的な方法は、「CSRFToken」などの一般名を持つランダムに生成されたパラメータを含む要求を生成するようにサーバをセットアップすることです。トークンはセッションごとに1回ずつ生成することも、要求ごとに新しく生成することもできます。コード内でCSRFトークンを使用し、Fortify WebInspectでCSRFを有効にしている場合は、それを考慮に入れてサイトがWeb探索されます。Fortify WebInspectは、攻撃を仕掛けるたびに、新しいCSRFトークンを取得するためのフォームを要求します。これにより、Fortify WebInspectがスキャンを完了するまでにかかる時間が大幅に増えるため、サイト上でCSRFトークンを使用していない場合はCSRFを有効にしないでください。

Fortify WebInspectでのCSRF認識の有効化

サイトでCSRFトークンを使用している場合は、次のように、Fortify WebInspectでCSRF認識を有効にすることができます。

1. [編集(Edit)]メニューから [デフォルトのスキャン設定(Default Scan Settings)]を選択します。
[スキャン設定(Scan Settings)]ウィンドウが表示されます。
2. [スキャン設定(Scan Settings)]列で、[HTTP解析(HTTP Parsing)]を選択します。
3. [CSRFの有効化(Enable CSRF)]ボックスをオンにします。

スキャン設定: カスタムパラメータ

この機能にアクセスするには、[編集(Edit)]メニューをクリックし、[デフォルトのスキャン設定(Default Scan Settings)]または[現在のスキャン設定(Current Scan Settings)]を選択します。その後で、[スキャン設定(Scan Settings)]カテゴリで、[カスタムパラメータ(Custom Parameters)]を選択します。

カスタムパラメータは、URL書き換え手法およびREST (Representation State Transfer) Webサービステクノロジ(あるいはその一方)を使用するサイトに対応するために使用されます。これらのカスタムパラメータのルールを記述するか、Webアプリケーション記述言語(WADL)で記述された共通の環境設定ファイルからルールをインポートできます。

URLの書き換え

多くのダイナミックサイトではURLの書き換えが使用されます。スタティックURLはユーザが覚えやすく、検索エンジンがサイトにインデックスを付けやすいためです。たとえば、次のようなHTTP要求は、

```
http://www.pets.com>ShowProduct/7
```

サーバの書き換えモジュールに送信され、URLが以下に変換されます。

```
http://www.pets.com>ShowProduct.php?product_id=7
```

この例では、このURLによってサーバはPHPスクリプト「ShowProduct」を実行し、製品番号7の情報を表示します。

Fortify WebInspectは、ページをスキャンする際、どの要素が変数か判断して、攻撃エージェントが脆弱性を完全にチェックできるようにする必要があります。これを有効にするには、これらの要素を識別するルールを定義する必要があります。そのためには、独自のFortify WebInspect構文を使用します。

例:

```
HTML: <a href="someDetails/user1/">User 1 details</a>
```

```
ルール: /someDetails/{username}/
```

```
HTML: <a href="TwoParameters/Details/user1/value2">User 1 details</a>
```

```
ルール: /TwoParameters/Details/{username}/{parameter2}
```

```
HTML: <a href="/Value2/PreFixParameter/Details/user1">User 1 details</a>
```

```
ルール: /{parameter2}/PreFixParameter/Details/{username}
```

RESTfulサービス

RESTful Webサービス(RESTful Web APIとも呼ばれる)は、HTTPおよびRESTの原則を使用して実装されるシンプルなWebサービスです。これは、SOAPおよびWSDL(Web Services Description Language)ベースのWebサービスに代わるシンプルなサービスとして、Web全体で広く普及しています。

以下の要求は、HTTPクエリ文字列を使用してファイルに名前を追加します。

```
GET /adduser?name=Robert HTTP/1.1
```

あるWebサービスでは、これと同じ機能を次の方法で達成できます。パラメータ名と値が要求URIから移動され、要求本文にXMLタグとして現れていることに注意してください。

```
POST /users HTTP/1.1 Host: myserver
Content-Type: application/xml
<?xml version="1.0"?>
<user>
<name>Robert</name>
</user>
```

URLの書き換えとRESTful Webサービスのどちらの場合も、適切な要求の作成方法をFortify WebInspectに指示するルールを作成する必要があります。

ルールの作成

ルールを作成するには:

1. **新規ルール(New Rule)**をクリックします。
2. **式(Expression)**列にルールを入力します。ガイドラインと例については、「["スマートリックスパラメータ"次のページ](#)」を参照してください。

デフォルトでは、**有効(Enabled)**チェックボックスがオンになります。Fortify WebInspectによってルールを調べられ、有効な場合は、赤いXが削除されます。

ルールの削除

ルールを削除するには:

1. **カスタムパラメータルール(Custom Parameters Rules)**リストからルールを選択します。
2. **削除(Delete)**をクリックします。

ルールの無効化

ルールを削除せずに無効にするには:

1. ルールを選択します。
2. **有効(Enabled)**列のチェックマークをオフにします。

ルールのインポート

ルールを含むファイルをインポートするには:

1.  Import...をクリックします。
2. 標準のファイル選択ダイアログボックスを使用して、適用するカスタムルールを含むファイルのタイプ(.wadlまたは.txt)を選択します。
3. ファイルを見つけて、**開く(Open)**をクリックします。

スキャン時に使用されていないルールの自動シードを有効にする(Enable automatic seeding of rules that were not used during scan)

カスタムパラメータの最も信頼できるルールは、WADLファイルから推測されたルール、またはWebサイトの開発者によって作成されたルールです。スキャン中にルールが呼び出されない場合(ルールがどのURLにも一致しないため)、Fortify WebInspectは、サイトの有効な部分が攻撃されていないとプログラム的に想定できます。したがって、このオプションを選択すると、Fortify WebInspectは、攻撃露呈部分を拡大するためにこれらの未使用のルールを実行するセッションを作成します。

URLパラメータのダブルエンコード(Double Encode URL Parameters)

ダブルエンコーディングは、セキュリティ制御をバイパスしたり、アプリケーションから予期しない動作を引き起こしたりするために、ユーザ要求パラメータを16進数形式で2回エンコードする攻撃手法です。たとえば、クロスサイトスクリプティング(XSS)攻撃は通常、次のようにになります。

```
<script>alert('FOO')</script>
```

この悪意のあるコードが脆弱なアプリケーションに挿入され、警告ウィンドウに「FOO」というメッセージが表示される可能性があります。ただし、Webアプリケーションでは、<(より小さい)、>(より大きい)、および/(スラッシュ)などの文字を禁止するフィルタを使用できます。これらの文字がWebアプリケーション攻撃の実行に使用されるためです。攻撃者は、「ダブルエンコーディング」手法を使用してクライアントのセッションを悪用することで、この保護手段を回避しようとする可能性があります。このJavaScriptのエンコーディングプロセスは次のとおりです。

| 文字 | 16進エンコード | エンコードされた%記号 | ダブルエンコードされた結果 |
|----|----------|-------------|---------------|
| < | %3C | %25 | %253C |
| / | %2F | %25 | %252F |
| > | %3E | %25 | %253E |

最後に、ダブルエンコードされた悪意のあるコードは次のようにになります。

```
%253Cscript%253Ealert('XSS')%253C%252Fscript%253E
```

このオプションを選択すると、Fortify WebInspectは、(单一エンコードパラメータではなく)二重エンコードURLパラメータを作成し、攻撃シーケンスの一部として送信します。これは、Webサーバが、たとえば、Apache mod-rewriteとPHPや、Java URL Rewrite Filter 3.2.0などを使用する場合に推奨されます。

パスマトリックスパラメータ

システムでルールを作成するには3つの方法があります。ルールは次の方法で作成できます。

- 手動で入力する
- ユーザが指定した、またはFortify WebInspect Agentを介して受信したWADLファイルから生成する
- ルールのリストを含む扁平ファイルからインポートする

ルールを手動で入力する場合は、パラメータとして扱う必要のあるURLのパスセグメントを指定します。

ルールでは、特殊文字を使用して、パラメータを含む実際のURLの一部が指定されます。URLがルールに一致する場合、パラメータが解析されて攻撃が行われます。ルールの重要なコンポーネントは次のものです。

- パス(gp/c/{book_name}/)
- クエリ(「?」の後に続くもの)
- フラグメント(「#」の後に続くもの)

パスセグメントの定義

パスセグメントは「/」文字で始まり、もう1つの「/」文字または行の末尾のいずれかで終了します。たとえば、パス「/a」には1つのセグメントがあるのに対し、パス「/a/」には2つのセグメントがあります(最初のセグメントは文字列「a」を含み、2つ目のセグメントは空です)。パス「/a」とパス「/a/」は等しくありません。URLがルールに一致するかどうかを判断しようとする際には、空のセグメントが考慮されます。

ルールの特別な要素

次の表で説明する特別な要素をルールに含めることができます。

| 要素 | 説明 |
|-----|---|
| * | アスタリスク。以下で定義する結果に使用できます。パス以外の結果に存在する場合は、URLのこの部分が一致に関与しない(つまり、あらゆるものと一致すること)を意味します。 |
| { } | グループ。ルールのパス内で使用できる名前付きパラメータ。内容に特別な意味はなく、攻撃を受けたパラメータの名前としてレポート作成時に使用されます。グループを指定する区切り括弧{ }内で使用できる文字セットは、RFC 3986で*pchar:と定義されています。 |

```

pchar = unreserved / pct-encoded / sub-delims / ":" / "@"
pct-encoded = "%" HEXDIG HEXDIG
unreserved = ALPHA DIGIT - . _ ~
reserved = gen-delims / sub-delims
gen-delims = : / ? # [ ] @@
sub-delims = ! $ & ' ( ) * + , ;

```

「左括弧」と「右括弧」文字は、パーセントエンコード要素としてエスケープしない限り、グループの内容に含めることはできません。

パスの外に*を配置する場合のルールは次のとおりです。パスセグメントにいくつでも*と{}グループを入れることができますが、間にプレーンテキストを挟むことが必要です。次に例を示します。

有効なルール: /gp/c/*={param}
無効なルール: /gp/c/*{}

セグメント内に**、*{}、{}*または{}{}エントリが含まれているルールは無効です。

URLと照合するルールでは、ルールのすべてのコンポーネントが、Web探索されるURLの対応するコンポーネントと一致している必要があります。パスの比較はセグメント単位で実行されます。*と{}グループは任意の数の文字(ゼロ個の文字を含む)に一致し、プレーンテキスト要素はURLのパスセグメントの対応するプレーンテキスト要素に一致します。次に例を示します。

/gp/c/{book_name}は、次のURLに一致します。

- http://www.amazon.com:8080/gp/c/Moby_Dick
- http://www.amazon.com/gp/c/Singularity_Sky?format=pdf&price=0
- <https://www.amazon.com/gp/c/Hobbit>

一方、次のURLとは一致しません。

- http://www.amazon.com/gp/c/Moby_Dick/ (末尾のスラッシュが原因で一致しない)
- http://www.amazon.com/gp/c/Sex_and_the_City/Horror (セグメント数が異なっているため一致しない)

Fortify WebInspectでは、ルールURL内の{}...{}グループに一致するパスセグメントの要素は、クエリ内で検出されたものと同様にパラメータとして扱われます。さらに、ルールに一致するWeb探索対象のURLのクエリパラメータは、URLのパス内にあるパラメータと一緒に攻撃されます。次に挙げる一致するURLの例では、Fortify WebInspectによって、フォーマットパラメータと価格パラメータ、およびパスの3つ目のセグメント(Singularity_Sky)に対して攻撃が行われます。

http://www.amazon.com/gp/c/Singularity_Sky?format=pdf&:price=0

アスタリスクプレースホルダ

「*」プレースホルダは、次に挙げるURLの結果と副次的な結果で使用できます。

- パス-パス内の*は単一のセグメント、またはそれより小さい部分に一致するため、全体に一致させることはできません。
 - パスセグメント- /gp/*/{param}など。この場合、スキーマHTTP、ホスト名(www.amazon.com)、3つのセグメント(1つ目のセグメントは「gp」そのもの、2つ目は任意のセグメント、3つ目はパラメータとして扱われ、一致に関与しない)を含むパスを持つURLと一致します。
 - パスセグメントの一部- /gp/ref=*など。この場合、2つのセグメント(1つ目は「gp」そのもの、2つ目はプレフィクス「ref=」が付加された任意の文字列を含む)を含むパスを持つURLと一致します。
 - クエリ- /gp/c/{param}?*など。この場合、3つのセグメント(1つ目のセグメントは「gp」、2つ目のセグメントは「c」、3つ目のセグメントはパラメータであるため一致に関与しない)から成るパスを持つURLに一致します。このURLには任意の構造のクエリ文字列が含まれている必要があります。ルール/gp/c/{param}とルール/gp/c/{param}?*の違いに注意してください。1つ目のルールはURL http://www.amazon.com/gp/c/Three_Little_Miceと一致

しますが、2つ目のルールは一致しません。

- クエリのキーと値のペア- /gp/c/{param}?format=*など。この場合、クエリ文字列にキーと値のペアが1つだけあり、キー名が「format」の場合に限り、URLと一致します。
- クエリのキーと値のペア- /gp/c/{param}?*=pdfなど。この場合、クエリ文字列にキーと値のペアが1つだけあり、値が「pdf」の場合に限り、URLと一致します。
- フラグメント- /gp/c/{param}#*など。この場合、フラグメント部分が存在するあらゆるURLと一致します。

プレースホルダを使用する利点

プレースホルダを使用する主な利点は、マトリックスパラメータとURLパスベースのパラメータを組み合わせたルールを1つのルール内で作成できることです。関連する以下のURLを例として考慮します。

`http://www.amazon.com/gp/color;foreground=green;background=black/something?format=dvi`

次のルールを使うと、すべてのパラメータに対する攻撃が許可されます。

`gp/*/{param}`

マトリックスパラメータセグメントはパスの2つ目のセグメント内にある*プレースホルダによって無視されますが、Fortify WebInspectによって認識され、適切に攻撃されます。

複数のルールが1つのURLに一致する場合

複数のルールが特定のURLに一致する場合には、次の2つのオプションがあります:

- 一致が1つ検出されたらルールの反復処理を停止し、最初のルールのみを使用する。
- すべてのルールを反復処理し、一致するすべてのカスタムパラメータを収集する。

たとえば、次のURLの場合、

`http://mySite.com/store/books/Areopagitica/32/1`

次のルールが両方とも一致します。

- `*/books/{booktitle}/32/{paragraph}`
- `store/*/Areopagitica/{page}/{paragraph}`

Fortify WebInspectでは、最大の攻撃力バレッジを確保するために両方のルールからパラメータの収集が試みられます。そのため、3つのセグメント(上記の例では「Areopagitica」、「32」、および「1」)がすべて攻撃されます。

スキャン設定: フィルタ

この機能にアクセスするには、[編集(Edit)]メニューをクリックし、[デフォルトのスキャン設定(Default Scan Settings)]または[現在のスキャン設定(Current Scan Settings)]を選択し

ます。その後で、[スキャン設定(Scan Settings)]カテゴリで、[フィルタ(Filters)]を選択します。

[フィルタ(Filters)]設定を使用して、HTTP要求と応答の検索および置換ルールを追加します。この機能は、クレジットカード番号、従業員名、または社会保障番号などの機密データが開示されるのを防ぐために最もよく使用されます。これは、Fortify WebInspectを使用する人や、生データまたは生成されたレポートにアクセスできる人に見られたくない情報を偽装するための方法です。

オプション

[フィルタ(Filter)]オプションについて、次の表で説明します。

| オプション | 説明 |
|---|-------------------------------------|
| HTTP要求コンテンツのフィルタ(Filter HTTP Request Content) | このエリアを使用して、HTTP要求の検索および置換ルールを指定します。 |
| HTTP応答コンテンツのフィルタ(Filter HTTP Response Content) | このエリアを使用して、HTTP応答の検索および置換ルールを指定します。 |

キーワードの検索および置換のためのルールの追加

次のステップに従って、要求または応答でキーワードを検索または置換するための正規表現ルールを追加します。

1. [要求コンテンツ(Request Content)]または[応答コンテンツ(Response Content)]グループのいずれかで、[追加(Add)]をクリックします。
[要求/応答データのフィルタ基準の追加(Add Request/Response Data Filter Criteria)]ウィンドウが開きます。
2. [テキストの検索(Search for text)]ボックスに、検索する文字列を入力(または貼り付け)します(または、文字列を表す正規表現を入力します)。
正規表現表記を挿入したり、Regular Expression Editor(式の作成とテストを容易にします)を起動したりするには、□をクリックします。
3. [テキストの検索場所(Search for text In)]ボックスで、フィルタパターンを検索する要求または応答のセクションを選択します。オプションは次のとおりです。
 - **すべて(All)** - 要求全体または応答全体を検索します。
 - **ヘッダ(Headers)** - 各ヘッダを個別に検索します。Set-CookieヘッダやHTTP Versionヘッダなど、一部のヘッダは検索されません。

メモ: すべてのヘッダを確実に検索するには、[プレフィクス(Prefix)]を選択します。

- **Postデータ(Post Data)** - 要求の場合のみ、すべてのHTTPメッセージ本文データを検索します。
 - **本文(Body)** - すべてのHTTPメッセージ本文データを検索します。
 - **プレフィクス(Prefix)** - 要求行またはステータス行内のすべての内容、すべてのヘッダ、および本文の前の空の行を同時に検索します。
4. [検索テキストを次で置換(Replace search text with)]ボックスに置換文字列を入力(または貼り付け)します。
□をクリックすると、正規表現についてのヘルプが表示されます。
 5. 大文字と小文字を区別して検索する場合は、[大文字と小文字を区別する(Case sensitive match)]チェックボックスを選択します。
 6. [OK]をクリックします。

スキャン設定: クッキー/ヘッダ

この機能にアクセスするには、[編集(Edit)]メニューをクリックし、[デフォルトのスキャン設定(Default Scan Settings)]または[現在のスキャン設定(Current Scan Settings)]を選択します。その後で、[スキャン設定(Scan Settings)]カテゴリで、[クッキー/ヘッダ(Cookies/Headers)]を選択します。

標準のヘッダパラメータ

このセクションのオプションについて、次の表で説明します。

| オプション | 説明 |
|---|--|
| HTTP要求ヘッダに「リファラ」を含める (Include 'referer' in HTTP request headers) | リファラヘッダをFortify WebInspect HTTP要求に含めるには、このチェックボックスを選択します。クライアントは、Refererのrequest-headerフィールドを使用して、Request-URIの取得元リソースのアドレス(URI)をサーバのために指定できます。 |
| HTTP要求ヘッダに「ホスト」を含める (Include 'host' in HTTP request headers) | ホストヘッダをFortify WebInspect HTTP要求に含めるには、このチェックボックスを選択します。Hostのrequest-headerフィールドは、ユーザまたは参照元リソース(通常はHTTP URL)によって指定された元のURIから取得した、要求されているリソースのインターネットホストとポート番号を指定します。 |

カスタムヘッダの追加

このセクションは、Fortify WebInspectが実行する各監査に含まれるヘッダを追加、編集、または削除する場合に使用します。たとえば、「Alert: You are attacked by Consultant ABC」などのヘッダを追加できます。このヘッダは、Fortify WebInspectがそのサイトを監査しているときに会社のサーバに送信されるすべての要求に含まれます。複数のカスタムヘッダを追加できます。

デフォルトのカスタムヘッダについて、次の表で説明します。

| ヘッダ | 説明 |
|------------------|---|
| Accept: */* | 任意のエンコーディングまたはファイルタイプをWeb探索プログラムで受け入れ可能です。 |
| Pragma: no-cache | これにより、強制的に新しい応答が返されます。キャッシュまたはプロキシされたデータは受け入れられません。 |

カスタムヘッダの追加

カスタムヘッダを追加するには:

1. **追加(Add)**をクリックします。
[カスタムヘッダの指定(Specify Custom Header)]ウィンドウが開きます。
2. [カスタムヘッダ(Custom Header)]ボックスに、<name>: <value>という形式を使用してヘッダを入力します。
3. [OK]をクリックします。

カスタムクッキーの追加

このセクションでは、脆弱性スキャンを実行する際に、Fortify WebInspectによってサーバに送信されるHTTP要求でクッキーと一緒に送信されるデータを指定します。

スキャントラフィックにフラグを付けるために使用されるデフォルトのカスタムクッキーは次のとおりです。

CustomCookie=WebInspect;path=/

カスタムクッキーの追加

カスタムクッキーを追加するには:

1. **追加(Add)**をクリックします。
[カスタムクッキーの指定(Specify Custom Cookie)]ウィンドウが開きます。

2. [カスタムクッキー(Custom Cookie)]ボックスに、<name>=<value>という形式を使用してクッキーを入力します。

たとえば、次のように入力すると、

CustomCookie=ScanEngine

各HTTP-Requestには、次のヘッダが含まれます。

Cookie: CustomCookie=ScanEngine

3. [OK]をクリックします。

スキャン設定: プロキシ

この機能にアクセスするには、[編集(Edit)]メニューをクリックし、[デフォルトのスキャン設定(Default Scan Settings)]または[現在のスキャン設定(Current Scan Settings)]を選択します。その後で、[スキャン設定(Scan Settings)]カテゴリで、[プロキシ(Proxy)]を選択します。

オプション

[プロキシ(Proxy)]オプションについて、次の表で説明します。

| オプション | 説明 |
|--|--|
| 直接接続(プロキシ無効)(Direct Connection (proxy disabled)) | プロキシサーバを使用しない場合は、このオプションを選択します。 |
| プロキシ設定の自動検出(Auto detect proxy settings) | WPAD (Web Proxy Autodiscovery)プロトコルを使用してプロキシ自動設定ファイルを探し、ブラウザのWebプロキシ設定を行います。 |
| システムのプロキシ設定を使用する(Use System proxy settings) | ローカルマシンからプロキシサーバ情報をインポートします。 |
| Firefoxプロキシ設定を使用する(Use Firefox proxy settings) | Firefoxからプロキシサーバ情報をインポートします。 メモ: Firefoxプロキシ設定を使用することにしても、プロキシサーバ経由のインターネットアクセスが保証されるわけではありません。Firefoxブラウザの接続設定が[プロキシーを使用しない]に設定されている場合、プロキシは使用されません。 |

| オプション | 説明 |
|--|--|
| PACファイルURLを使用してプロキシを設定する (Configure proxy using a PAC file URL) | [URL] ボックスで指定した場所にあるPAC (Proxy Automatic Configuration) ファイルからプロキシ設定をロードします。 |
| プロキシを明示的に設定する(Explicitly configure proxy) | <p>要求された情報を入力することによって、プロキシを設定します。</p> <ol style="list-style-type: none"> 1. [サーバ(Server)] ボックスにプロキシサーバのURLまたはIPアドレスを入力し、続いて([ポート(Port)] ボックスに)ポート番号(8080など)を入力します。 2. プロキシサーバ経由でTCPトラフィックを処理するプロトコルの [タイプ(Type)] を、SOCKS4、SOCKS5、または標準から選択します。 3. 認証が必要な場合は、[認証(Authentication)] リストからタイプを選択します。 <ul style="list-style-type: none"> • 自動 <p>メモ: 自動検出を指定すると、スキャンの処理が遅くなります。把握している別の認証メソッドを指定すると、スキャンのパフォーマンスは大幅に向上します。</p> • _digest • HTTP基本(HTTP Basic) • Kerberos • ネゴシエート(Negotiate) • NT LAN Manager (NTLM) 4. プロキシサーバで認証が必要な場合は、適格なユーザ名とパスワードを入力します。 5. 特定のIPアドレス(内部テストサイトなど)にアクセスするためにプロキシサーバを使用する必要がない場合は、[プロキシをバイパスするサイト(Bypass Proxy For)] ボックスにアドレスまたはURLを入力します。エントリはカンマで区切ります。 |
| HTTPS用の代替プロキシを指定する (Specify Alternative Proxy for HTTPS) | HTTPS接続を受け入れるプロキシサーバの場合は、[HTTPS用の代替プロキシを指定する(Specify Alternative Proxy for HTTPS)] を選択し、要求された情報を入力します。 |

スキャン設定: 認証

基本スキャン内でこの機能にアクセスするには、[編集(Edit)]メニューをクリックし、[デフォルトのスキャン設定(Default Scan Settings)]または[現在のスキャン設定(Current Scan Settings)]を選択します。その後で、[スキャン設定(Scan Settings)]カテゴリーで、[認証(Authentication)]を選択します。

認証とは、セキュリティ対策として識別情報を検証することです。パスワードとデジタル署名が認証の形態です。Fortify WebInspectが認証を必要とするサーバまたはフォームに遭遇するたびに、ユーザ名とパスワードが入力されるように自動認証を設定できます。そうしなかつた場合は、ログオン情報がないためにWeb探索が途中で停止する可能性があります。

スキャンにはネットワーク認証が必要(Scan Requires Network Authentication)

ユーザがWebサイトまたはアプリケーションにログオンする必要がある場合は、このチェックボックスをオンにします。

認証メソッド

認証が必要な場合は、次のように認証メソッドを選択します。

- ADFS CBT
- 自動
- 基本(Basic)
- ダイジェスト(Digest)
- Kerberos
- NT LAN Manager (NTLM)

認証資格情報

[ユーザ名(User name)]ボックスにユーザIDを入力し、[パスワード>Password)]ボックスにユーザのパスワードを入力します。タイプミスから保護するため、[パスワードの確認]ボックスに再度パスワードを入力します。

注意! Fortify WebInspectは、このパスワードによるアクセスが許可されたすべてのサーバをWeb探索します(このサイト/サーバが「許可ホスト」設定に含まれている場合)。管理システムに損傷を与える可能性を避けるため、管理権を持っているユーザ名とパスワードは使用しないでください。アクセス権が不明な場合は、システム管理者または社内のセキュリティプロフェッショナルに連絡するか、Fortifyカスタマサポートにお問い合わせください。

クライアント証明書

クライアント証明書認証を使用すると、ユーザはユーザ名とパスワードを入力するのではなく、クライアント証明書を提示することができます。ローカルマシンから証明書を選択することも、現在のユーザに割り当てられた証明書を選択することもできます。コンピュータに接続された共通アクセスカード(CAC)リーダなどのモバイルデバイスからの証明書を選択することもできます。クライアント証明書を使用するには:

1. [クライアント証明書(Client Certificates)]エリアで、**有効化(Enable)**]チェックボックスをオンにします。
2. **選択(Select)**]をクリックします。
[クライアント証明書(Client Certificates)]ウィンドウが開きます。
3. 次のいずれかを実行します。
 - コンピュータにとってローカルで、コンピュータ上のすべてのユーザにとってグローバルな証明書を使用するには、**ローカルマシン(Local Machine)**]を選択します。
 - コンピュータ上のユーザーアカウントにとってローカルな証明書を使用するには、**現在のユーザ(Current User)**]を選択します。
- メモ: 共通アクセスカード(CAC)リーダで使用される証明書はユーザ証明書であり、現在のユーザ(Current User)に保管されます。
4. 次のいずれかを実行します。
 - 「個人」(「マイ」)証明書ストアから証明書を選択するには、ドロップダウンリストから **マイ(My)**]を選択します。
 - 信頼されたルート証明書を選択するには、ドロップダウンリストで **ルート(Root)**]を選択します。
5. WebサイトではCACリーダを使用しますか。
 - 「はい」の場合は、次の手順を実行します。
 - i. **証明書(Certificate)**]リストから、「(SmartCard)」というプレフィックスが付いた証明書を選択します。
選択した証明書に関する情報とPINフィールドが **証明書情報(Certificate Information)**]エリアに表示されます。
 - ii. PINが必要な場合は、**PIN**]フィールドにCACのPINを入力します。
メモ: PINが必要な場合に、この時点でPINを入力しないと、スキャン中にPINの入力を求められるたびに、Windowsの **セキュリティ**]ウィンドウにPINを入力する必要があります。
 - iii. **テスト(Test)**]をクリックします。
正しいPINを入力した場合は、成功メッセージが表示されます。
 - 「いいえ」の場合は、**証明書(Certificate)**]リストから証明書を選択します。

選択した証明書に関する情報が「証明書(Certificate)」リストの下に表示されます。

6. [OK]をクリックします。

WebInspectツール用のプロキシ設定ファイルの編集

プロキシが組み込まれたツール(具体的には、Web Macro Recorder、Web Proxy、およびWeb Form Editor)を使用している場合は、証明書が必要な場合でもクライアント証明書を要求しないサーバに遭遇することがあります。この状況に対応するには、次のタスクを実行してSPI.Net.Proxy.Configファイルを編集する必要があります。

タスク1: 証明書のシリアル番号を探す

1. Microsoft Internet Explorerを開きます。
2. [ツール]メニューで、[インターネットオプション]をクリックします。
3. [インターネットオプション]ウィンドウで、[コンテンツ]タブを選択し、[証明書]をクリックします。
4. [証明書]ウィンドウで、証明書を選択して、[表示]をクリックします。
5. [証明書]ウィンドウで、[詳細]タブをクリックします。
6. [シリアル番号]フィールドをクリックし、下側のペインに表示されるシリアル番号をコピーします(数字を強調表示して、<Ctrl>を押しながら<C>を押します)。
7. すべてのウィンドウを閉じます。

タスク2: SPI.Net.Proxy.Configファイルでエントリを作成する

1. SPI.Net.Proxy.Configをファイル編集用に開きます。デフォルトの場所はC:\Program Files\Fortify\Fortify WebInspectです。

2. ClientCertificateOverridesセクションで、次のエントリを追加します。

```
<ClientCertificateOverride HostRegex="RegularExpression"  
CertificateSerialNumber="Number" />
```

ここで:

RegularExpressionは、ホストURLと一致する正規表現です(例: .*austin\.microfocus\.com)。

Numberは、タスク1で取得したシリアル番号です。

3. 編集したファイルを保存します。

マクロ検証を有効にする(Enable Macro Validation)

ほとんどのダイナミックなアプリケーションスキャンでは、アプリケーションのあらゆる側面を明らかにするためにユーザ認証が必要です。ログインマクロでアプリケーションにログインできなかった場合は、スキャン品質が低下します。スキャンの前にログインマクロの品質を測定すれば、低品質のスキャンを回避できます。

「マクロ検証を有効にする(Enable Macro Validation)」を選択して、Fortify WebInspectがスキャンの開始時点でのマクロ動作の矛盾をテストできるようにします。実行された特定のテストの詳細については、「["ログインマクロのテスト" ページ510](#)」を参照してください。

フォーム認証にログインマクロを使用する(Use a login macro for forms authentication)

この種のマクロは、主にWebフォーム認証に使用されます。誤ってアプリケーションからログアウトした場合に、Fortify WebInspectが途中で終了するのを防ぐロジックが組み込まれています。この種のマクロを記録する場合は、必ずアプリケーションのログアウト署名を指定してください。省略記号ボタン [...] をクリックしてマクロを探します。記録(Record)】をクリックしてマクロを記録します。

メモ: ガイド付きスキャンの場合は、ログインマクロを記録するための別のステージが含まれているため、記録(Record)】ボタンを使用できません。

ログインマクロパラメータ(Login Macro Parameters)

このセクションは、「[フォーム認証にログインマクロを使用する\(Use a login macro for forms authentication\)](#)」を選択し、選択または作成したマクロにユーザ名とパスワードのパラメータが指定されたフィールドが含まれている場合にのみ表示されます。

ユーザ名とパスワードのパラメータを含むマクロを使用してスキャンを開始した場合は、これらのエントリに関連付けられた入力要素を含むページをスキャンすると、Fortify WebInspectがここで指定されたユーザ名とパスワードに置き換えます。これにより、独自のユーザ名とパスワードを使用してマクロを作成することができますが、このマクロを使用して他のユーザがスキャンを実行すると、その人のユーザ名とパスワードが置き換えられる可能性があります。このことは、2要素認証スキャンで使用される電話番号、電子メール、および電子メールパスワードのパラメータにも適用されます。

Web Macro Recorderで値がマスクされたパラメータがマクロで使用されている場合、Fortify WebInspectで基本スキャンまたはガイド付きスキャンを設定するときにも、それらの値はマスクされます。

Web Macro Recorderを使用してパラメータを作成する方法の詳細については、『*Micro Focus Fortify WebInspect Tools Guide*』の「Web Macro Recorder」の章を参照してください。

起動マクロを使用する(Use a startup macro)

この種のマクロは、アプリケーションの特定のサブセクションに焦点を当てるために最もよく使用されます。Fortify WebInspectがそのエリアへのナビゲートに使用するURLを指定します。また、ログイン情報が含まれている場合がありますが、Fortify WebInspectがアプリケーションからログアウトできないようにするロジックは含まれていません。Fortify WebInspectは、マクロ内のすべてのURLにアクセスして、ハイパーキーを収集し、データ階層をマッピングします。その後で、開始URLを呼び出し、通常のWeb探索(およびオプションで監査)を開始します。省

略記号ボタン [...] をクリックしてマクロを探します。[記録(Record)] をクリックしてマクロを記録します。

マルチユーザログイン(Multi-user Login)

[マルチユーザログイン(Multi-user Login)] オプションを使用すると、ログインマクロ内 のユーザ名とパスワードをパラメータ化してから、スキャンで使用する複数のユーザ名とパスワードのペアを定義できます。2要素認証が必要な場合は、電話番号、電子メール、および電子メールパスワードをパラメータ化することもできます。このアプローチを使用すると、複数のスレッドでスキャンを実行できます。スレッドごとにログインセッションが異なるため、スキャン時間が短縮されます。

重要! マルチユーザログインを使用するには、まず、[フォーム認証にログインマクロを使用する(Use a login macro for forms authentication)] を選択し、新しいマクロを記録するか、使用する既存のマクロを選択する必要があります。「"フォーム認証にログインマクロを使用する(Use a login macro for forms authentication)" 前のページ」を参照してください。

複数のユーザログインを使用してスキャンを実行するには:

1. [マルチユーザログイン(Multi-user Login)] チェックボックスをオンにします。

メモ: スキャンを実行する前に [マルチユーザログイン(Multi-user Login)] チェックボックスをオフにすると、スキャン中に追加の資格情報が使用されません。Fortify WebInspectは、ログインマクロに記録されたオリジナルの資格情報のみを使用します。

2. 次の表の説明に従って操作を進めます。

| 目的... | 手順... |
|---------------|---|
| ユーザの資格情報を追加する | <ol style="list-style-type: none">[マルチユーザログイン(Multi-user Login)] で、[追加(Add)] をクリックします。 [マルチユーザ資格情報入力(Multi-user Credential Input)] ダイアログボックスが表示されます。[ユーザ名.Username] フィールドに、ユーザ名を入力します。[パスワード.Password] フィールドに、対応するパスワードを入力します。オプションで、2要素認証が必要な場合は、次の基準を追加します。<ul style="list-style-type: none">電話番号(Phone Number) -ユーザ名に対応する電話番号(SMS応答を受信するため)電子メール>Email) -ユーザ名に対応する電子メールアド |

| 目的... | 手順... |
|---------------|--|
| | <p>レス(電子メール応答を受信するため)</p> <ul style="list-style-type: none"> ◦ 電子メールパスワード(Email Password) -電子メールアドレスのパスワード(電子メール応答を受信するため) <p>e. [OK]をクリックします。</p> <p>f. 追加するユーザログインごとにステップa-eを繰り返します。</p> <p>重要! 共有リクエスタスレッドの数が、設定されたユーザの数を超えないようにする必要があります。有効なユーザを持たないリクエスタスレッドでは、スキャンの実行時間が長くなります。複数のユーザを設定する場合は、最初のユーザとして、パラメータ化されたマクロ内のオリジナルのユーザ名とパスワードをカウントすることを忘れないでください。詳細については、「"スキャン設定: リクエスタ" ページ382」を参照してください。</p> |
| ユーザの資格情報を編集する | <p>a. [マルチユーザログイン(Multi-user Login)]で、テーブル内のエントリを選択し、[編集(Edit)]をクリックします。</p> <p>[マルチユーザ資格情報入力(Multi-user Credential Input)]ダイアログボックスが表示されます。</p> <p>b. 必要に応じて資格情報を編集します。</p> <p>c. [OK]をクリックします。</p> |
| ユーザの資格情報を削除する | <p>a. [マルチユーザログイン(Multi-user Login)]で、削除するテーブル内のエントリを選択します。</p> <p>b. [削除>Delete)]をクリックします。</p> |

詳細については、「["マルチユーザログインスキャン" ページ194](#)」を参照してください。

スキャン設定: ファイルが見つからない

この機能にアクセスするには、[編集(Edit)]メニューをクリックし、[デフォルトのスキャン設定(Default Scan Settings)]または[現在のスキャン設定(Current Scan Settings)]を選択します。その後で、[スキャン設定(Scan Settings)]カテゴリで、[ファイルが見つからない(File Not Found)]を選択します。

オプション

[ファイルが見つからない(File Not Found)]オプションについて、次の表で説明します。

| オプション | 説明 |
|---|--|
| HTTP応答コードを使用してFNF(ファイルが見つからない)を判別する (Determine File Not Found (FNF) using HTTP response codes) | <p>サーバからのfile-not-found応答を検出するためにHTTP応答コードを使用する場合は、このオプションを選択します。続いて、次のカテゴリに当てはまるコードを特定できます。</p> <ul style="list-style-type: none"> 強制有効応答コード(FNFは不可)(Forced Valid Response Codes (Never an FNF)): file-not-found応答として扱ってはならないHTTP応答コードを指定できます。 強制FNF応答コード(常にFNF): 常にfile-not-found応答として扱われるHTTP応答コードを指定します。Fortify WebInspectは応答の内容を処理しません。 <p>1つの応答コードまたは応答コードの範囲を入力します。範囲には、ダッシュまたはハイフンを使用して、リスト内の最初と最後のコードを区切ります(たとえば、400-404)。複数のコードまたは範囲を指定するには、各エントリをカンマで区切ります。</p> |
| カスタム提供の署名からFNFを判別する (Determine FNF from custom supplied signature) | <p>このエリアを使用して、会社が使用するカスタムの404ページ通知に関する情報を追加します。404エラーが発生した場合に別のページを表示するように会社が設定している場合は、その情報をここに追加します。サイト固有の404ページからの誤検出がFortify WebInspectで発生する可能性があります。</p> |
| FNFページの自動検出(Auto detect FNF page) | <p>存在しないリソースをクライアントが要求すると、一部のWebサイトではステータス「404 Not Found」を返しません。代わりに、「200 OK」というステータスが返されることがあります。ファイルが見つからないというメッセージが応答に含まれているか、ホームページやログインページにリダイレクトされる場合があります。Fortify WebInspectでこれらの「カスタム」のfile-not-foundページを検出するには、このチェックボックスを選択します。</p> <p>Fortify WebInspectは、サーバ上に存在できない可能性があるリソースに対する要求を送信することによって、カスタムのfile-not-foundページの検出を試みます。続いて、各応答を比較し、応答間で異なるテキストの量を測定します。たとえば、このタイプのほとんどのメッセージは、要求されたリソースの名前が異なる可能性があることを除けば、同じ内容です(「お探しのページは見つかりませんでした(Sorry, the page you requested was not found)」など)。[FNFページの自動検出(Auto detect FNF page)] チェックボックスを選択した場合、同じでなければならない応答コンテンツの割合を[一致するFNFページ(Match FNF page with)] フィールドに指定できます。デフォルトは90%です。</p> |

スキャン設定: ポリシー

この機能にアクセスするには、[編集(Edit)]メニューをクリックし、[デフォルトのスキャン設定(Default Scan Settings)]または[現在のスキャン設定(Current Scan Settings)]を選択します。その後で、[スキャン設定(Scan Settings)]カテゴリで、[ポリシー(Policy)]を選択します。

スキャンウィザードを使用してスキャンを開始するときに別のポリシーに変更できますが、代わりのものを選択しない場合は、ここで選択したポリシーが使用されます。

ポリシーを作成、インポート、または削除することもできます。

ポリシーの作成

ポリシーを作成するには:

1. [作成(Create)]をクリックします。
Policy Managerツールが開きます。
2. [ファイル(File)]メニューから[新規(New)]を選択します(または[新しいポリシー(New Policy)]アイコンをクリックします)。
3. 新しいポリシーのモデルにするポリシーを選択します。
4. 追加の手順については、Policy Managerのオンラインヘルプを参照してください。

ポリシーの編集

ポリシーを編集するには:

1. カスタムポリシーを選択します。
カスタムポリシーのみを編集できます。
2. [編集(Edit)]をクリックします。
Policy Managerツールが開きます。
3. 追加の手順については、オンラインヘルプを参照してください。

ポリシーのインポート

ポリシーをインポートするには:

1. [インポート(Import)]をクリックします。
2. [カスタムポリシーのインポート(Import Custom Policy)]ウィンドウで、省略記号ボタン [...]をクリックします。
3. 標準のファイル選択ウィンドウの[ファイルの種類]リストを使用して、以下のポリシータイプから選択します。

- ポリシーファイル(*.policy): バージョン7.0以降のFortify WebInspectのバージョン用に設計および作成されたポリシーファイル。
- 古いポリシーファイル(*.apc): バージョン7.0より前のFortify WebInspectのバージョン用に設計および作成されたポリシーファイル。
- すべてのファイル(*.*): ポリシー以外のファイルを含む、任意のタイプのファイル。

4. [OK]をクリックします。

ポリシーのコピーがPoliciesフォルダに作成されます(デフォルトの場所は、C:\ProgramData\HP\HP WebInspect\Policies\)。そのポリシーとその有効化されたチェックはすべて、指定したポリシー名を使用してSecureBaseにインポートされます。カスタムエージェントはインポートされません。

ポリシーの削除

ポリシーを削除するには:

1. カスタムポリシーを選択します。
カスタムポリシーのみを削除できます。
2. [削除(Delete)]をクリックします。

スキャン設定: ユーザエージェント

この機能にアクセスするには、[編集(Edit)]メニューをクリックし、[デフォルトのスキャン設定(Default Scan Settings)]または[現在のスキャン設定(Current Scan Settings)]を選択します。その後で、[スキャン設定(Scan Settings)]カテゴリで、[ユーザエージェント(User Agent)]を選択します。

Fortify WebInspectとWeb Macro Recorderの両方でMacro Engine 6.1と同期するユーザエージェント設定を行えます。

プロファイルおよびユーザエージェント文字列

ブラウザのユーザエージェント文字列を指定する定義済みのプロファイルを選択できます。次の表に、使用可能なプロファイルを示します。

| プロファイル (Profile) | ユーザエージェント文字列 |
|------------------------|---|
| デフォルト | Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0) Gecko/20100101 Firefox/71.0 |
| Internet Explorer 6 | Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322) |

| プロファイル (Profile) | ユーザエージェント文字列 |
|---------------------|--|
| Internet Explorer 7 | Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1) |
| Internet Explorer 8 | Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; GTB5; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022; InfoPath.2; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729) |
| Googlebot 2.1 | Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html) |
| Bingbot | Mozilla/5.0 (compatible; bingbot/2.0; +http://www.bing.com/bingbot.htm) |
| Yahoo! Slurp | Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp) |
| iPhone、iOS 14.3 | Mozilla/5.0 (iPhone; CPU iPhone OS 14_3 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0.2 Mobile/15E148 Safari/604.1 |
| カスタム | ユーザ指定。 重要! Fortifyでは、カスタムプロファイルは上級ユーザのみが使用することを推奨しています。 |

ナビゲータインターフェース設定

ナビゲータインターフェース設定は、レガシWebアプリケーションがブラウザ検出を容易にするために使用する情報を提供します。ブラウザ固有の動作が必要な場合は、これらの設定をカスタマイズできます。設定は次のとおりです。

- **appName** -すべてのブラウザがこのプロパティの値として「Netscape」を返します。
- **appVersion** -ブラウザは、「4.0」またはブラウザに関するバージョン情報を表す文字列を返します。
- **platform** -ブラウザは、空の文字列、またはブラウザが実行されているプラットフォームを表す文字列を返します。

例:

MacIntel, Win32, Win64, iPhone

第7章: Web探索設定

この章では、Fortify WebInspect Web探索プログラムで使用されるWeb探索設定について説明します。Fortify WebInspect Web探索プログラムは、Webサイト全体のハイパーアリンクをたどり、ページを取得してインデックスを付け、サイトの階層構造を文書化するように設計されたソフトウェアプログラムです。Fortify WebInspectがサイトをWeb探索する方法を制御するパラメータは、[Web探索設定(Crawl Settings)]リストから選択できます。

Web探索設定: リンク解析

この機能にアクセスするには、[編集(Edit)]メニューをクリックし、[デフォルトのスキャン設定(Default Scan Settings)]または[現在のスキャン設定(Current Scan Settings)]を選択します。その後で、[Web探索設定(Crawl Settings)]カテゴリで、[リンク解析(Link Parsing)]を選択します。

Fortify WebInspectは、HTMLによって定義されたハイパーアリンク(<a href>タグを使用)とスクリプト(JavaScriptとVBScript)によって定義されたすべてのハイパーアリンクをたどります。ただし、リンクの指定に別の構文を使用する他の通信プロトコルに遭遇する場合があります。このような場合に対応するために、カスタムリンク機能と正規表現を使用して、Fortify WebInspectにたどらせるリンクを識別できます。これらは特殊リンク識別子と呼ばれています。

特殊リンク識別子の追加

特殊リンク識別子を追加するには:

1. [追加(Add)]をクリックします。
特殊リンク入力(Specialized Link Entry)】ウィンドウが開きます。
2. [特殊リンクパターン(Specialized Link Pattern)]ボックスに、リンクを識別するために設計された正規表現を入力します。
3. (オプション) [コメント(Comment)]ボックスにリンクの説明を入力します。
4. [OK]をクリックします。

Web探索設定: リンクソース

この機能にアクセスするには、[編集(Edit)]メニューをクリックし、[デフォルトのスキャン設定(Default Scan Settings)]または[現在のスキャン設定(Current Scan Settings)]を選択します。その後で、[Web探索設定(Crawl Settings)]カテゴリで、[リンクソース(Link Sources)]を選択します。

リンク解析とは

Fortify WebInspect Web探索プログラムは、開始URLに要求を送信し、応答の内容からリンク(URL)を再帰的に解析します。これらのリンクは作業キューに登録され、キューが空になるまでWeb探索プログラムが繰り返し実行されます。HTTP応答からリンク情報を抽出するために使用される技術は、総称して「リンク解析」と呼ばれています。Web探索プログラムでリンク解析を実行する方法には、パターンベースとDOMベースの2つの選択肢があります。

パターンベースの解析

パターンベースのリンク解析では、テキスト検索とパターンマッチングを組み合わせてURLが検索されます。これらのURLには、<A>要素など、ブラウザによってレンダリングされる通常のコンテンツだけでなく、追加のサイト構造を明らかにする可能性がある不可視テキストも含まれます。

このオプションは、Fortify WebInspect 10.40以前のバージョンのデフォルトの動作と一致します。これは、WebサイトをWeb探索するためのより積極的なアプローチであり、スキャンの実行により多くの時間がかかる可能性があります。この積極的な動作のせいで、実際のサイトコンテンツを表すものではない余分なリンクがWeb探索プログラムで多数作成されることがあります。このような状況では、DOMベースの解析によって誤検出を減らしてサイトのURLコンテンツを明らかにできるはずです。

メモ: 「パターンベースの解析 (Pattern-based Parsing)」を選択すると、リンクを検索するためのDOMベースの解析技術がすべて使用されます。ただし、パターンベースの解析では、リンクソースのメタデータを計算することができません。DOMベースの解析では、この情報を計算することができるため、よりインテリジェントな解析が可能になります。また、DOMベースの解析では、使用する解析技術をより細かく制御できます。

DOMベースの解析

ドキュメントオブジェクトモデル(DOM)は、HTMLドキュメントとXMLドキュメントの定義と構築、その構造のナビゲート、およびその要素とコンテンツの編集を行う論理構造を提供するプログラミング概念です。

HTMLページのグラフィカルな表現をDOMで示すと、上下逆さまのツリーのようになります。HTMLノードに端を発するツリー構造の分岐にタグ、サブタグ、およびコンテンツが組み込まれます。この構造をDOMツリーと呼びます。

Fortify WebInspectではDOMベースの解析を使用してHTMLページをDOMツリーとして解析します。解析された詳細な構造を使用することで、ハイパーテリンクのソースを特定する際の忠実性と信頼性を向上させます。DOMベースの解析で誤検出を減らすことができ、「積極的なリンク検出」の度合いも減る可能性があります。

一部のサイトではWeb探索プログラムが不良リンクを繰り返し要求し、応答の内容にこれらのリンクがエコーバックされます。場合によっては、問題を悪化させる余分のテキストが追加されます。このような「不良リンクインと不良リンクアウト」の反復サイクルが原因で、スキャンが長時間実行されたり、まれに、永久に実行されたりする可能性があります。DOMベースの解析

リンクソースの慎重な選択によって、この暴走スキャン動作を制限するメカニズムが提供されます。Webアプリケーションはそれぞれ構造や内容が異なるため、リンクソース設定を最適なものとするには実験が必要です。

DOMベースの解析を改善するには、リンクの検索に使用する技術を選択します。サイトに関係ない技術を取り除くことでスキャンの完了に要する時間が短くなる可能性があります。ただし、より徹底的なスキャンを行う場合は、すべての技術を選択するか、パターンベースの解析を使用します。DOMベースの解析技術の説明を次の表に示します。詳細については、「["リンクソース設定の制限" ページ426](#)」を参照してください。

| 技術 | 説明 |
|--|---|
| コメントリンクを含める(積極的) (Include Comment Links (Aggressive)) | <p>プログラマは、自分のために、リンクを含むメモをHTMLコメント内部に残す場合があります。このリンクはサイト上に表示されませんが、攻撃者によって発見される可能性があります。このオプションは、HTMLコメント内部のリンクを検索する場合に使用します。Fortify WebInspectが見つけるリンクは増えますが、これらのリンクは必ずしも有効なURLとは限らず、Web探索プログラムは存在しないコンテンツへのアクセスを試みる場合があります。同じリンクが各ページに置かれていることや、それらが相対リンクであることもあり、結果としてURLカウントが指数関数的に増加して、スキャン時間が長くなる可能性があります。</p> |
| 条件付きコメントリンクを含める (Include Conditional Comment Links) | <p>条件付きコメントリンクは、要求を行うユーザエージェント(ブラウザのタイプとバージョン)に応じて、ページ上のHTMLが条件付きで包含または除外される場合に発生します。</p> <p>通常のコメントの例: <!--hidden.txt --></p> <p>条件付きコメントの例:</p> <pre><!--[if lt IE9]> <script src="//www.somesite.com/static/v/all/js/html5sh.js"></script> <link rel="stylesheet" type="text/css" href='//www.somesite.com/static/v/fn-hp/css/IE8.css'> <![endif]--></pre> <p>Fortify WebInspectは、HTMLコードを評価する際にブラウザの動作をミュレートし、ユーザエージェントに応じてDOMの処理方法を変えます。あるユーザエージェントにとってコメント内のリンクであるものが、他のユーザエージェントにとって通常のHTMLリンクになります。</p> <p>このオプションは、ブラウザのバージョンに基づいてコメントアウトされるリンクなど、HTMLコマンド内部に存在する条件付きリンクを検索する場合に使用します。これらの条件付きステートメントには、スクリプト解析が有効になっている場合に実行する必要があるスクリプトインクルードも含めることができます。これらのリンクのWeb探索はより徹底的なものになりますが、スキャン</p> |

| 技術 | 説明 |
|---|--|
| | 時間が増える可能性があります。加えて、このようなコメントは最新でなく、Web探索する意味がない場合があります。 |
| プレーンテキストリンクを含める (Include Plain Text Links) | <p>.txtファイル内のプレーンテキストやHTMLコード内部の段落を、http://www.something.com/mypage.htmlのようにURLとして書式設定できます。ただし、これは単なるテキストであって真のリンクではないため、ブラウザはこれをリンクとしてレンダリングせず、そのテキストは機能的にページの一部になりません。たとえば、コンテンツは、ユーザによってクリックされることを想定していない偽の構文を使用してHTMLでコーディングする方法を記述したページの一部である可能性があります。このオプションは、Fortify WebInspectがこれらのテキストリンクを解析して、Web探索用のキューに登録する場合に使用します。</p> <p>また、スマートパターンの一一致を使用して、Fortify WebInspectは、.css、.js、.bmp、.png、.jpg、.htmlなどの一般的なファイル拡張子を識別し、これらのファイルをWeb探索キューに登録できます。プレーンテキストで参照されたこれらのファイルを監査すると、誤検出が発生する可能性があります。</p> |
| スタティックスクリプトブロック内のリンクを含める (Include Links in Static Script blocks) | <p>このオプションは、Fortify WebInspectが開始スクリプトタグと終了スクリプトタグの内側でリンクに見えるテキストを調査する場合に使用します。有効なリンクがこれらのスクリプトブロック内で見つかる場合もありますが、開発者が開始スクリプトタグと終了スクリプトタグの内側にリンクに似たテキストを含むコメントを残すこともあります。次に例を示します。</p> <pre><script type="text/javascript"> // go to http://www.foo.com/blah.html for help var url = "http://www.foo.com/xyz/" + path + "?help" </script></pre> <p>加えて、これらのタグの内側のJavaScriptコードがスキャン中にJavaScript実行エンジンによって処理される可能性があります。ただし、上記の例の「var url」のように変数を設定するコード行内のスタティックリンクを検索すると、それらの部分パスがWeb探索用のキューに登録されたときに問題が発生する可能性があります。変数に「foo.html」などの一般的な拡張子を持つ相対リンクが含まれている場合は、Web探索プログラムによって、そのコード行を含むすべてのページの末尾に拡張子が付加されます。これにより、使用できないURLが生成され、誤検出が発生する可能性があります。</p> |
| URLに埋め込まれたURLを解析 | このオプションは、Fortify WebInspectがhref属性内部に存在するすべてのテキストを解析して、Web探索キューに登録する場合に使用します。URLに埋め込まれたURLの例を次に示します。 |

| 技術 | 説明 |
|---|--|
| する(Parse URLs Embedded in URLs) | <pre></pre> <p>ただし、一部のサイトでは、「ファイルが見つからない」ページでフォームアクションタグに入れてURLが返され、次のようにそのURLがオリジナルのURLに付加されます。</p> <pre><form action="http://www.foo.com/xyz/bar.html?url=http%3A%2F%2Fwww.zzz.com%2Fblah?http://www.foo.com/xyz/bar.html?url=http%3A%2F%2Fwww.zzzz.com%2Fblah" /></pre> <p>その後、Fortify WebInspectは、フォームアクションを要求し、もう一度「ファイルが見つからない」応答を受け取ります。ここでも、次に示すように、URLがフォームアクションに追加されます。</p> <pre><form action="http://www.foo.com/xyz/bar.html?url=http%3A%2F%2Fwww.zzz.com%2Fblah?http://www.foo.com/xyz/bar.html?url=http%3A%2F%2Fwww.zzzz.com%2Fblah?http://www.foo.com/xyz/bar.html?url=http%3A%2F%2Fwww.zzzz.com%2Fblah?http://www.foo.com/xyz/bar.html?url=http%3A%2F%2Fwww.zzzz.com%2Fblah" /></pre> <p>このようなサイトでは、これらのURLによって引き続き「ファイルが見つからない」応答が生成され、さらに多くのURLがWeb探索キューに登録されます。その結果、無限のWeb探索ループが発生します。この種のURLをWeb探索キューに登録しないようにするには、このオプションを使用しないでください。</p> |
| ルート化されていないURLを許可する(Allow Un-rooted URLs) (上記の項目にに対して) | <p>このオプションは、前述の5つのオプションの動作を変更します。URLによっては、httpなどの特定のスキームが含まれておらず、完全修飾ドメイン名でないものがあります。xyz.htmlのようなこれらのURLは、アンカーなしまたは「ルート化なし」と見なされます。これは、ルートされていないURLが要求に対して相対的であることが前提です。</p> <p>たとえば、完全修飾されていないURL <code></code> にはスキームが含まれていません。このURLでは、コンテキストURLのスキームが使用されます。HTTPSページがコンテンツの取得を要求すると、HTTPSがURLの前に付加されます。</p> <p>このオプションは、ルート化されていないURLをリンクとして解析時に扱う場</p> |

| 技術 | 説明 |
|----|---|
| | <p>合に使用します。このオプションを選択すると、スキャンがより徹底的で積極的になりますが、完了にはかなり長い時間がかかる可能性があります。</p> <p>URLのサンプルと解析結果</p> <p>次のサンプルでは、さまざまなURLと、それらがWeb探索中に解析される方法について説明します。</p> <p>通常のURL</p> <p>次の要求内のURLには、前方(またはアンカー)スラッシュが含まれています。</p> <p>要求元: <code>http://www.foo.com/x/y/z/</code> 次の場合: <code></code> 結果のリンク先: <code>http://www.foo.com/bar.html</code></p> <p>ルート化されていないシンプルなURL</p> <p>次の要求内のURLは、前方スラッシュが含まれていないため、ルート化されません。</p> <p>要求元: <code>http://www.foo.com/</code> 次の場合: <code></code> 結果のリンク先: <code>http://www.foo.com/bar.html</code></p> <p>ルート化されていない長いURL</p> <p>次の要求は、ルート化されていない長いURLを示しています。</p> <p>要求元: <code>http://www.foo.com/x/y/z/</code> 次の場合: <code></code> 結果のリンク先: <code>http://www.foo.com/x/y/z/bar.html</code></p> <p>コード内のコメント</p> <p><code><!-- baz_ads.js --></code>などのコメントが、コード内のスクリプトインクルードの前に含まれている場合があります。次の要求は、積極的なWeb探索中にこのコメントがどのように解釈されるかを示しています。</p> <p>要求元: <code>http://www.foo.com/x/y/z/</code> 次の場合: <code><!-- baz_ads.js --></code> 結果のリンク先: <code>http://www.foo.com/x/y/z/baz_ads.js</code></p> <p>マスターページにこのコメントを含めた場合は、積極的なスキャン中に、サイト内のページ応答の多く(すべてではない)でコメントが検出されます。この設定では、暴走スキャンが発生する可能性があります。</p> |

| 技術 | 説明 |
|----|---|
| | <p>マスタページ上 のコメント<!-- baz_ads.js -->によって、次のような複数のリンクが作成されます。</p> <pre>http://www.foo.com/baz_ads.js http://www.foo.com/x/baz_ads.js http://www.foo.com/x/y/baz_ads.js http://www.foo.com/x/y/z/baz_ads.js (サイト内のすべてのページで同様です)。</pre> |

フォームアクション、スクリプトインクルード、およびスタイルシート

フォームアクション、スクリプトインクルード、スタイルシートなどの一部のリンクタイプは、特殊で、他のリンクとは異なる方法で扱われます。サイトによっては、これらのリンクをWeb探索して解析する必要がない場合があります。ただし、あらゆるものWeb探索と解析を試みる積極的なスキャンが必要な場合は、この目的を達成するために次のオプションが役に立ちます。詳細については、「["リンクソース設定の制限" ページ426](#)」を参照してください。

メモ: また、これらのオプションのそれぞれでルート化されていないURLを許可することもできます。このトピックの「ルート化されていないURLを許可する」を参照してください。

| オプション | 説明 |
|--|---|
| フォームアクションリンクをWeb探索する (Crawl Form Action Links) | Fortify WebInspectは、Web探索中にHTMLフォームに遭遇すると、ユーザが得る入力のバリエーションを作成し、より多くのサイトコンテンツを収集するための要求としてフォームを送信します。たとえば、POSTメソッドを使用したフォームの場合は、Fortify WebInspectが代わりにGETを使用して情報を公開することもできます。この種のWeb探索に加えて、このオプションは、Fortify WebInspectがフォームターゲットを通常のリンクとして扱う場合に使用します。 |
| スクリプトインクルードリンクをWeb探索する (Crawl Script Include Links) | スクリプトインクルードは、.jsファイルからJavaScriptをインポートして、現在のページで処理されます。このオプションは、Fortify WebInspectが.jsファイルをリンクとしてWeb探索する場合に使用します。 |
| スタイルシートリンクをWeb探索する (Crawl Stylesheet Links) | スタイルシートリンクは、.cssファイルからスタイル定義をインポートして、現在のページにレンダリングします。このオプションは、Fortify WebInspectが.cssファイルをリンクとしてWeb探索する場合に使用します。 |

その他のオプション

次の追加オプションは、サイトのリンク解析を改善するのに役立つ場合があります。詳細については、「["リンクソース設定の制限"次のページ](#)」を参照してください。

| オプション | 説明 |
|--|---|
| FNFページ上のリンクをWeb探索する(Crawl Links on FNF Pages) | <p>このオプションを選択すると、Fortify WebInspectは「ファイルが見つからない」とマークされた応答のリンクを検索し、Web探索を行います。</p> <p>このオプションは、スキャンモードが [Web探索のみ(Crawl Only)] または [Web探索および監査(Crawl & Audit)] に設定されている場合はデフォルトで選択されます。このオプションは、スキャンモードが [監査のみ(Audit Only)] に設定されている場合は利用できません。</p> |
| 反復パスセグメントを使用してURLを抑止する(Suppress URLs with Repeated Path Segments) | <p>多くのサイトには、相対パスのようでありながら、Fortify WebInspectによる解析と、Web探索対象のURLへの追加が済むと、使用不能なURLになるテキストがあります。こうしたものの出現は、パスが連続して追加される場合 (/foo/bar/foo/bar/など) に、暴走スキャンになるおそれがあります。こうしたものの出現を減らす上でこの設定は役に立ち、デフォルトで有効になっています。</p> <p>この設定が有効な場合、次のオプションがあります。</p> <p>1 - URL内のどこかで繰り返されている単一のサブフォルダを検出し、一致がある場合はそのURLを拒否します。たとえば、/foo/baz/bar/foo/では「/foo/」が繰り返されているので一致します。この繰り返しは隣接している必要はありません。</p> <p>2 - 隣接するサブフォルダの2つ以上のペアを検出し、一致がある場合はURLを拒否します。たとえば、/foo/bar/baz/foo/bar/では「/foo/bar/」が繰り返されているので一致します。</p> <p>3 - 隣接する3つのサブフォルダの2つ以上のセットを検出し、一致がある場合はURLを拒否します。</p> <p>4 - 隣接する4つのサブフォルダの2つ以上のセットを検出し、一致がある場合はURLを拒否します。</p> <p>5 - 隣接する5つのサブフォルダの2つ以上のセットを検出し、一致がある場合はURLを拒否します。</p> <p>この設定が無効な場合、サブフォルダの繰り返しは検出されず、一致が原因でURLが拒否されることはありません。</p> |

リンクソース設定の制限

リンクソースのチェックボックスをオフにすると、スタティック解析を使用してその特定の種類のリンクが見つかったとき、Web探索プログラムで処理されません。ただし、これらのリンクは他の多くの方法で見つかる可能性があります。たとえば、[スタイルシートリンクをWeb探索する(Crawl Stylesheet Links)]オプションをオフにしても、パスの切り捨ては制御されず、スクリプトエンジンから発行される.cssファイル要求は抑止されません。この設定をオフにすると、サーバからの.css応答のスタティックリンク解析が阻止されるに過ぎません。同様に、[スクリプトリンクルードリンクをWeb探索する(Crawl Script Include Links)]オプションをオフにしても、スクリプトエンジンから発行される.js、AJAX、frameIncludes、またはその他のファイル要求は抑止されません。したがって、リンクソースのチェックボックスをオフにしても、その種のリンクソースに対する普遍的なフィルタにはなりません。

チェックボックスをオフにする目的は、Web探索が大量の不良リンクでいっぱいになってスキャン時間が極端に長くなるのを防ぐことです。

Web探索設定: セッション除外

[スキャン設定-セッション除外(Scan Settings - Session Exclusions)]で指定した項目はすべて、[Web探索設定(Crawl Settings)]と[監査設定(Audit Settings)]の両方の[セッション除外(Session Exclusions)]に自動的に複製されます。これらの項目は、灰色(黒色ではない)テキストで表示されます。これらのオブジェクトをWeb探索から除外しない場合は、[スキャン設定-セッション除外(Scan Settings - Session Exclusions)]パネルからそれらを削除する必要があります。

このパネル([Web探索設定-セッション除外(Crawl Settings - Session Exclusions)])では、Web探索から除外する追加のオブジェクトを指定することができます。

除外または拒否するファイル拡張子

[拒否(Reject)]を選択した場合は、指定された拡張子を持つファイルが要求されません。

[除外(Exclude)]を選択した場合は、指定された拡張子を持つファイルが要求されますが、監査されません。

除外/拒否するファイル拡張子の追加

ファイル拡張子を追加するには:

1. [追加(Add)]をクリックします。
[除外拡張子(Exclusion Extension)]ウィンドウが開きます。
2. [ファイル拡張子(File Extension)]ボックスに、ファイル拡張子を入力します。
3. [拒否(Reject)]と[除外(Exclude)]のどちらかまたは両方を選択します。
4. [OK]をクリックします。

除外MIMEタイプ

指定されたMIMEタイプに関連付けられたファイルが監査されません。

除外するMIMEタイプの追加

MIMEタイプを追加するには:

1. **追加(Add)**]をクリックします。
除外するMimeタイプの指定(Provide a Mime-type to Exclude)]ウィンドウが開きます。
2. **[Mimeタイプの除外(Exclude Mime-type)]**ボックスに、MIMEタイプを入力します。
3. **OK**]をクリックします。

その他の除外/拒否基準

HTTPメッセージのさまざまなコンポーネントを特定してから、そのコンポーネントを含むセッションを除外するか拒否するかを指定できます。

- **拒否(Reject)** - Fortify WebInspectは、指定されたホストまたはURLにHTTP要求を送信しません。たとえば、通常、サイトからのログオフを処理するURLは拒否する必要があります。これは、スキャンが完了する前にアプリケーションからログアウトしたくないためです。
- **除外(Exclude)** - Web探索中に、Fortify WebInspectは、指定されたURLまたはホストで他のリースへのリンクを調査しません。スキャンの監査部分の間は、Fortify WebInspectが指定されたホストまたはURLを攻撃しません。HTTP応答を処理せずにURLまたはホストにアクセスする場合は、**除外(Exclude)**]オプションを選択しますが、**拒否(Reject)**]は選択しません。たとえば、処理しないURL上に壊れたリンクをチェックするには、**除外(Exclude)**]オプションだけを選択します。

デフォルトの基準の編集

デフォルトの基準を編集するには:

1. 基準を選択して、**編集(Edit)**]([**その他の除外/拒否基準(Other Exclusion/Rejection Criteria)**])リストの右側にある)をクリックします。
ホストまたはURLの拒否または除外(Reject or Exclude a Host or URL)]ウィンドウが開きます。
2. **ホスト(Host)**]または**URL**]を選択します。
3. **ホスト/URL(Host/URL)**]ボックスに、URLまたは完全修飾ホスト名、またはターゲットのURLまたはホストに一致するように設計された正規表現を入力します。
4. **拒否(Reject)**]と**除外(Exclude)**]のどちらかまたは両方を選択します。
5. **OK**]をクリックします。

除外/拒否基準の追加

除外/拒否基準を追加するには:

1. **追加(Add)**](**その他の除外/拒否基準(Other Exclusion/Rejection Criteria)**]リストの右側にある)をクリックします。
除外の作成(Create Exclusion)]ウィンドウが開きます。
2. **ターゲット(Target)**]リストから項目を選択します。
3. ターゲットとして [クエリパラメータ(Query Parameter)]または [ポストパラメータ(Post Parameter)]を選択した場合は、**ターゲット名(Target Name)**]を入力します。
4. **一致タイプ(Match Type)**]リストから、ターゲット内のテキストの一一致に使用される方法を選択します。
 - **正規表現に一致(Matches Regex)**]- **一致文字列(Match String)**]ボックスで指定した正規表現に一致します。
 - **正規表現の拡張に一致(Matches Regex Extension)**]- **一致文字列(Match String)**]ボックスで指定したFortify正規表現の拡張から入手可能な構文に一致します。
 - **一致(Matches)**]- **一致文字列(Match String)**]ボックスで指定したテキスト文字列に一致します。
 - **含む(Contains)**]- **一致文字列(Match String)**]ボックスで指定したテキスト文字列を含みます。
5. **一致文字列(Match String)**]ボックスに、ターゲットで検索する文字列または正規表現を入力します。または、**一致タイプ(Match Type)**]で正規表現オプションを選択した場合は、ドロップダウン矢印をクリックして、**正規表現の作成(Create Regex)**]を選択し、Regular Expression Editorを起動します。
6. をクリックします(または<Enter>を押します)。
7. (オプション)ステップ2-6を繰り返して、条件を追加します。複数の一一致はAND処理されます。
8. **現在の設定(Current Settings)**]で作業している場合は、**テスト(Test)**]をクリックして現在のスキャンの除外を処理できます。基準によって絞り込まれたそのスキャンからのセッションがテスト画面に表示され、必要に応じて設定を変更できます。
9. **OK**]をクリックします。
10. **その他の除外/拒否基準(Other Exclusion/Rejection Criteria)**]リストに除外が表示されている場合は、**拒否(Reject)**]と **除外(Exclude)**]のいずれかまたは両方を選択します。

メモ: スキャン中は、応答タイプ、応答ヘッダタイプ、およびステータスコードターゲットタイプを拒否することができません。これらのターゲットタイプは除外することしかできません。

例 1

Microsoft.comのリソースに対する要求を無視して送信しないようにするには、次の除外を入力して、**拒否(Reject)**]を選択します。

| ターゲット (Target) | ターゲット名 (Target Name) | 一致タイプ (Match Type) | 一致文字列 (Match String) |
|-------------------|-------------------------|-----------------------|-------------------------|
| URL | N/A | 含む(contains) | Microsoft.com |

例 2

一致文字列として「logout」と入力します。この文字列がURLの任意の部分で見つかった場合は、そのURLが除外または拒否されます(選択されたオプションによって異なる)。「logout」の例を使用すると、Fortify WebInspectは、logout.aspやapplogout.jspなどのURLを除外または拒否します。

| ターゲット (Target) | ターゲット名 (Target Name) | 一致タイプ (Match Type) | 一致文字列 (Match String) |
|-------------------|-------------------------|-----------------------|-------------------------|
| URL | N/A | 含む(contains) | logout |

例 3

次の例では、クエリパラメータ「username」が「John」と等しいクエリを含むセッションを拒否または除外します。

| ターゲット (Target) | ターゲット名 (Target Name) | 一致タイプ (Match Type) | 一致文字列 (Match String) |
|-------------------------------|-------------------------|-----------------------|-------------------------|
| クエリパラメータ (Query parameter) | username | 一致 (matches) | John |

例 4

次の例では、次のディレクトリを除外または拒否します。

http://www.test.com/W3SVC55/

http://www.test.com/W3SVC5/

http://www.test.com/W3SVC550/

| ターゲット (Target) | ターゲット名 (Target Name) | 一致タイプ (Match Type) | 一致文字列 (Match String) |
|-------------------|-------------------------|--------------------|-------------------------|
| | | | |

| | | | |
|-----|-----|----------------------------|---------------|
| URL | N/A | 正規表現に一致 (matches regex) | /W3SVC[0-9]*/ |
|-----|-----|----------------------------|---------------|

第8章：監査設定

この章では、監査スキャン中にFortify WebInspectによって使用される監査設定について説明します。監査とは、脆弱性を検出するように設計された、Fortify WebInspectによって実行されるプローブまたは攻撃のことです。Fortify WebInspectによるプローブの実行方法を制御するパラメータは、監査設定(Audit Settings)】リストから選択できます。

監査設定：セッション除外

この機能にアクセスするには、[編集(Edit)]メニューをクリックし、[デフォルトのスキャン設定(Default Scan Settings)]または[現在のスキャン設定(Current Scan Settings)]を選択します。その後で、[監査設定(Audit Settings)]カテゴリで、[セッション除外(Session Exclusions)]を選択します。

[スキャン設定-セッション除外(Scan Settings - Session Exclusions)]で指定した項目はすべて、[Web探索設定(Crawl Settings)]と[監査設定(Audit Settings)]の両方の[セッション除外(Session Exclusions)]に自動的に複製されます。これらの項目は、灰色(黒色ではない)テキストで表示されます。これらのオブジェクトを監査から除外しない場合は、[スキャン設定-セッション除外(Scan Settings - Session Exclusions)]パネルからそれらを削除する必要があります。

このパネル([監査設定-セッション除外(Audit Settings - Session Exclusions)])では、監査から除外する追加のオブジェクトを指定することができます。

除外または拒否するファイル拡張子

[拒否(Reject)]を選択した場合は、Fortify WebInspectが指定された拡張子を持つファイルを要求しません。

[除外(Exclude)]を選択した場合は、Fortify WebInspectが指定された拡張子を持つファイルを要求しますが、監査はしません。

除外/拒否するファイル拡張子の追加

ファイル拡張子を追加するには:

1. [追加(Add)]をクリックします。
除外拡張子(Exclusion Extension)】ウィンドウが開きます。
2. [ファイル拡張子(File Extension)]ボックスに、ファイル拡張子を入力します。
3. [拒否(Reject)]と[除外(Exclude)]のどちらかまたは両方を選択します。
4. [OK]をクリックします。

除外MIMEタイプ

Fortify WebInspectは、指定されたMIMEタイプに関連付けられたファイルを監査しません。

除外するMIMEタイプの追加

MIMEタイプを追加するには:

1. **追加(Add)**]をクリックします。
除外するMimeタイプの指定(Provide a Mime-type to Exclude)]ウィンドウが開きます。
2. **[Mimeタイプの除外(Exclude Mime-type)]**ボックスに、MIMEタイプを入力します。
3. **OK**]をクリックします。

その他の除外/拒否基準

HTTPメッセージのさまざまなコンポーネントを特定してから、そのコンポーネントを含むセッションを除外するか拒否するかを指定できます。

- **拒否(Reject)** - Fortify WebInspectは、指定されたホストまたはURLにHTTP要求を送信しません。たとえば、通常、サイトからのログオフを処理するURLは拒否する必要があります。これは、スキャンが完了する前にアプリケーションからログアウトしたくないためです。
- **除外(Exclude)** - Web探索中に、Fortify WebInspectは、指定されたURLまたはホストで他のリースへのリンクを調査しません。スキャンの監査部分の間は、Fortify WebInspectが指定されたホストまたはURLを攻撃しません。HTTP応答を処理せずにURLまたはホストにアクセスする場合は、**除外(Exclude)**]オプションを選択しますが、**拒否(Reject)**]は選択しません。たとえば、処理しないURL上に壊れたリンクをチェックするには、**除外(Exclude)**]オプションだけを選択します。

デフォルトの基準の編集

デフォルトの基準を編集するには:

1. 基準を選択して、**編集(Edit)**]([**その他の除外/拒否基準(Other Exclusion/Rejection Criteria)**])リストの右側にある)をクリックします。
ホストまたはURLの拒否または除外(Reject or Exclude a Host or URL)]ウィンドウが開きます。
2. **ホスト(Host)**]または**URL**]を選択します。
3. **ホスト/URL(Host/URL)**]ボックスに、URLまたは完全修飾ホスト名、またはターゲットのURLまたはホストに一致するように設計された正規表現を入力します。
4. **拒否(Reject)**]と**除外(Exclude)**]のどちらかまたは両方を選択します。
5. **OK**]をクリックします。

除外/拒否基準の追加

除外/拒否基準を追加するには:

1. **追加(Add)**](**その他の除外/拒否基準(Other Exclusion/Rejection Criteria)**]リストの右側にある)をクリックします。
除外の作成(Create Exclusion)]ウィンドウが開きます。
2. **ターゲット(Target)**]リストから項目を選択します。
3. ターゲットとして [クエリパラメータ(Query Parameter)]または [ポストパラメータ(Post Parameter)]を選択した場合は、**ターゲット名(Target Name)**]を入力します。
4. **一致タイプ(Match Type)**]リストから、ターゲット内のテキストの一一致に使用される方法を選択します。
 - **正規表現に一致(Matches Regex)**]- **一致文字列(Match String)**]ボックスで指定した正規表現に一致します。
 - **正規表現の拡張に一致(Matches Regex Extension)**]- **一致文字列(Match String)**]ボックスで指定したFortify正規表現の拡張から入手可能な構文に一致します。
 - **一致(Matches)**]- **一致文字列(Match String)**]ボックスで指定したテキスト文字列に一致します。
 - **含む(Contains)**]- **一致文字列(Match String)**]ボックスで指定したテキスト文字列を含みます。
5. **一致文字列(Match String)**]ボックスに、ターゲットで検索する文字列または正規表現を入力します。または、**一致タイプ(Match Type)**]で正規表現オプションを選択した場合は、ドロップダウン矢印をクリックして、**正規表現の作成(Create Regex)**]を選択し、Regular Expression Editorを起動します。
6. をクリックします(または<Enter>を押します)。
7. (オプション)ステップ2-6を繰り返して、条件を追加します。複数の一一致はAND処理されます。
8. **現在の設定(Current Settings)**]で作業している場合は、**テスト(Test)**]をクリックして現在のスキャンの除外を処理できます。基準によって絞り込まれたそのスキャンからのセッションがテスト画面に表示され、必要に応じて設定を変更できます。
9. **OK**]をクリックします。
10. **その他の除外/拒否基準(Other Exclusion/Rejection Criteria)**]リストに除外が表示されている場合は、**拒否(Reject)**]と **除外(Exclude)**]のいずれかまたは両方を選択します。

メモ: スキャン中は、応答タイプ、応答ヘッダタイプ、およびステータスコードターゲットタイプを拒否することができません。これらのターゲットタイプは除外することしかできません。

例 1

Microsoft.comのリソースに対する要求を無視して送信しないようにするには、次の除外を入力して、**拒否(Reject)**]を選択します。

| ターゲット (Target) | ターゲット名 (Target Name) | 一致タイプ(Match Type) | 一致文字列 (Match String) |
|-------------------|-------------------------|----------------------|-------------------------|
| URL | N/A | 含む(contains) | Microsoft.com |

例 2

一致文字列として「logout」と入力します。この文字列がURLの任意の部分で見つかった場合は、そのURLが除外または拒否されます(選択されたオプションによって異なる)。「logout」の例を使用すると、Fortify WebInspectは、logout.aspやapplogout.jspなどのURLを除外または拒否します。

| ターゲット (Target) | ターゲット名 (Target Name) | 一致タイプ(Match Type) | 一致文字列 (Match String) |
|-------------------|-------------------------|----------------------|-------------------------|
| URL | N/A | 含む(contains) | logout |

例 3

次の例では、クエリパラメータ「username」が「John」と等しいクエリを含むセッションを拒否または除外します。

| ターゲット (Target) | ターゲット名 (Target Name) | 一致タイプ (Match Type) | 一致文字列 (Match String) |
|------------------------------|-------------------------|-----------------------|-------------------------|
| クエリパラメータ(Query parameter) | username | 一致(matches) | John |

例 4

次の例では、次のディレクトリを除外または拒否します。

http://www.test.com/W3SVC55/

http://www.test.com/W3SVC5/

http://www.test.com/W3SVC550/

| ターゲット (Target) | ターゲット名 (Target Name) | 一致タイプ(Match Type) | 一致文字列 (Match String) |
|-------------------|-------------------------|-------------------|-------------------------|
| | | | |

| | | | |
|-----|-----|----------------------------|---------------|
| URL | N/A | 正規表現に一致 (matches regex) | /W3SVC[0-9]*/ |
|-----|-----|----------------------------|---------------|

監査設定: 攻撃除外

この機能にアクセスするには、[編集(Edit)]メニューをクリックし、[デフォルトのスキャン設定(Default Scan Settings)]または[現在のスキャン設定(Current Scan Settings)]を選択します。その後で、[監査設定(Audit Settings)]カテゴリで、[攻撃除外(Attack Exclusions)]を選択します。

除外パラメータ

この機能を使用して、Fortify WebInspectがHTTP要求で特定のパラメータを使用してWebサイトを攻撃するのを防ぎます。この機能は、ほとんどの場合、クエリとPOSTDATAパラメータの破損を避けるために使用されます。

除外するパラメータの追加

特定のパラメータが変更されるのを防ぐには:

1. [除外パラメータ(Excluded Parameters)]グループで、[追加(Add)]をクリックします。[HTTP除外の指定(Specify HTTP Exclusions)]ウィンドウが開きます。
2. [HTTPパラメータ(HTTP Parameter)]ボックスに、除外するパラメータの名前を入力します。をクリックして、正規表現表記を挿入します。
3. パラメータが見つかる可能性のあるエリア(HTTPクエリデータまたはHTTP POSTデータ)を選択します。必要に応じて、両方のエリアを選択できます。
4. [OK]をクリックします。

除外クッキー(Excluded Cookies)

この機能を使用して、Fortify WebInspectがHTTP要求で特定のクッキーを使用してWebサイトを攻撃するのを防ぎます。この機能は、クッキー値の破損を回避するために使用されます。

この設定では、クッキーの名前を入力する必要があります。

次のHTTP応答の例では、クッキーの名前が「FirstCookie」になっています。

```
Set-Cookie: FirstCookie=Chocolate+Chip; path=/
```

特定のクッキーの除外

特定のクッキーを除外するには:

1. **除外ヘッダ(Excluded Headers)**]グループで、**追加(Add)**]クリックします。
Regular Expression Editorが表示されます。
メモ: クッキーは、テキスト文字列または正規表現を使用して指定できます。
2. テキスト文字列を入力するには:
 - a. **式(Expression)**]ボックスに、クッキー名を入力します。
 - b. **OK**]をクリックします。
3. 正規表現を入力するには:
 - a. **式(Expression)**]ボックスに、検索するテキストと一致すると思われる正規表現を入力または貼り付けます。
□をクリックして、正規表現表記を挿入します。
 - b. **比較テキスト(Comparison Text)**]ボックスに、検索する文字列(**式(Expression)**]ボックスで指定)が含まれていることが分かっているテキストを入力または貼り付けます。
 - c. 式の大文字と小文字と一致する出現箇所のみを検索するには、**大文字/小文字を区別する(Match Case)**]チェックボックスをオンにします。
 - d. 正規表現によって識別された文字列を置き換える場合は、**置換(Replace)**]チェックボックスをオンにしてから、**置換(Replace)**]ボックスから文字列を入力または選択します。
 - e. **テスト(Test)**]をクリックして、正規表現に一致する文字列を比較テキストで検索します。一致は赤色で強調表示されます。
 - f. 正規表現で文字列が識別されましたか?
 - 識別された場合は、**OK**]をクリックします。
 - 識別されなかった場合は、識別したい文字列が **比較テキスト(Comparison Text)**]に含まれているかどうかを確認するか、正規表現を変更します。

除外ヘッダ(Excluded Headers)

この機能を使用して、Fortify WebInspectがHTTP要求で特定のヘッダを使用してWebサイトを攻撃するのを防ぎます。この機能は、ヘッダ値の破損を回避するために使用されます。

特定のヘッダの除外

特定のヘッダが変更されるのを防ぐには、次に説明する手順を使用して正規表現を作成します。

1. **除外ヘッダ(Excluded Headers)**]グループで、**追加(Add)**]クリックします。
Regular Expression Editorが表示されます。

メモ: ヘッダは、テキスト文字列または正規表現を使用して指定できます。

2. テキスト文字列を入力するには:
 - a. **式(Expression)**]ボックスに、ヘッダ名を入力します。
 - b. **OK**]をクリックします。
3. 正規表現を入力するには:
 - a. **式(Expression)**]ボックスに、検索するテキストと一致すると思われる正規表現を入力または貼り付けます。
□をクリックして、正規表現表記を挿入します。
 - b. **比較テキスト(Comparison Text)**]ボックスに、検索する文字列(**式(Expression)**]ボックスで指定)が含まれていることが分かっているテキストを入力または貼り付けます。
 - c. 式の大文字と小文字と一致する出現箇所のみを検索するには、**大文字/小文字を区別する(Match Case)**]チェックボックスをオンにします。
 - d. 正規表現によって識別された文字列を置き換える場合は、**置換(Replace)**]チェックボックスをオンにしてから、**置換(Replace)**]ボックスから文字列を入力または選択します。
 - e. **テスト(Test)**]をクリックして、正規表現に一致する文字列を比較テキストで検索します。一致は赤色で強調表示されます。
 - f. 正規表現で文字列が識別されましたか?
 - 識別された場合は、**OK**]をクリックします。
 - 識別されなかった場合は、識別したい文字列が**比較テキスト(Comparison Text)**]に含まれているかどうかを確認するか、正規表現を変更します。

Audit Inputs Editor

Audit Inputs Editorを使用して、入力を必要とする監査エンジンとチェック用のパラメータを作成または変更します。

- このツールを起動するには、**Audit Inputs Editor**]をクリックします。
- エディタを使用して過去に作成した入力をロードするには、**監査入力のインポート(Import Audit Inputs)**]をクリックします。

監査設定: 攻撃式

この機能にアクセスするには、**編集(Edit)**]メニューをクリックし、**デフォルトのスキャン設定(Default Scan Settings)**]または**現在のスキャン設定(Current Scan Settings)**]を選択します。その後で、**監査設定(Audit Settings)**]カテゴリで、**攻撃式(Attack Expressions)**]を選択します。

追加の正規表現言語

次のいずれかの言語コードと国コードの組み合わせを選択できます(.NET Frameworkクラスライブラリ内のCultureInfoクラスで使用されるのと同様)。

- zh-cn: 中國語-中国
- zh-tw: 中國語-台灣
- ja-jp: 日本語-日本
- ko-kr: 韓国語-韓国
- pt-br: ポルトガル語-ブラジル
- es-es: スペイン語-スペイン

CultureInfoクラスは、関連する言語、サブ言語、国/地域、暦、および文化的慣習などの文化固有の情報を保持します。また、このクラスは、DateTimeFormatInfo、NumberFormatInfo、CompareInfo、およびTextInfoの文化固有のインスタンスへのアクセスも提供します。これらのオブジェクトには、大文字/小文字の指定、日付と数値の書式設定、文字列の比較など、文化固有の操作に必要な情報が含まれています。

監査設定: 脆弱性フィルタリング

この機能にアクセスするには、[編集(Edit)]メニューをクリックして [デフォルト設定(Default Settings)]または [現在の設定(Current Settings)]を選択します。その後で、[監査の設定(Audit Settings)]カテゴリで、[脆弱性フィルタリング(Vulnerability Filtering)]を選択します。

特定のフィルタを適用することで、スキャン中に報告された特定の脆弱性の表示を制限できます。オプションは次のとおりです。

- **標準の脆弱性定義(Standard Vulnerability Definition)** -このフィルタは、類似する要求の同等性を判断できるようにパラメータ名をソートします。たとえば、`http://x.y?a=x;b=y` および`http://x.y;b=y;a=x`の両方のパラメータ「a」でSQLインジェクションの脆弱性が検出された場合、この脆弱性は同等と見なされます。
- **パラメータ脆弱性ロールアップ(Parameter Vulnerability Roll-Up)** -このフィルタは、1つのセッションで検出された複数のパラメータ操作およびパラメータインジェクションの脆弱性を1つの脆弱性に統合します。
- **403ブロッカー(403 Blocker)** -このフィルタは、脆弱なセッションのステータスコードが403(禁止)の場合に脆弱性を取り消します。
- **応答検査DOMイベントの親子(Response Inspection DOM Event Parent-Child)** -このフィルタは、JavaScriptで検出されたキーワード検索の脆弱性と同じ脆弱性が親セッションすでに検出されている場合に、この脆弱性を無視します。

脆弱性フィルタの追加

フィルタをデフォルト設定に追加するには:

1. **編集(Edit)**]メニューをクリックして、**デフォルトのスキャン設定(Default Scan Settings)**]を選択します。
2. **監査設定(Audit Settings)**]パネルの左側の列で、**脆弱性フィルタリング(Vulnerability Filtering)**]を選択します。
使用可能なすべてのフィルタは、**無効なフィルタ(Disabled Filters)**]リストまたは**有効なフィルタ(Enabled Filters)**]リストのいずれかに一覧表示されます。
3. フィルタを有効にするには、**無効なフィルタ(Disabled Filters)**]リストでフィルタを選択し、**追加(Add)**]をクリックします。
そのフィルタが**無効なフィルタ(Disabled Filters)**]リストから削除され、**有効なフィルタ(Enabled Filters)**]リストに追加されます。
4. フィルタを無効にするには、**有効なフィルタ(Enabled Filters)**]リストでフィルタを選択し、**削除(Remove)**]をクリックします。
そのフィルタが**有効なフィルタ(Enabled Filters)**]リストから削除され、**無効なフィルタ(Disabled Filters)**]リストに追加されます。

特定のスキャンの設定を変更することもできます。このためには、スキャンウィザードまたはWebサービススキャンウィザードの下部にある**設定(Settings)**]ボタンをクリックします。

サイト外の脆弱性の抑止

許可ホスト(Allowed Hosts)]リストにないホストへのリンクがWebアプリケーションに含まれている場合、Fortify WebInspectはこれらのホストで受動的な脆弱性を検出することができます。**許可ホスト(Allowed Hosts)**]リストにないサイト外ホストのセッションに対してすべての脆弱性を抑止するには、**サイト外の脆弱性を抑止する(Suppress Offsite Vulnerabilities)**]チェックボックスをオンにします。

許可ホスト(Allowed Hosts)]の詳細については、「["スキャン設定: 許可ホスト" ページ389](#)」を参照してください。

監査設定: スマートスキャン

この機能にアクセスするには、**編集(Edit)**]メニューをクリックし、**デフォルトのスキャン設定(Default Scan Settings)**]または**現在のスキャン設定(Current Scan Settings)**]を選択します。その後で、**監査設定(Audit Settings)**]カテゴリで、**スマートスキャン(Smart Scan)**]を選択します。

スマートスキャンの有効化

スマートスキャンは、Webサイトをホストしているサーバのタイプを検出し、その特定のサーバタイプに対する既知の脆弱性をチェックする「インテリジェント」機能です。たとえば、IISサーバでホストされているサイトをスキャンする場合、Fortify WebInspectはIISが影響を受けやすい脆弱性のみを検索します。ApacheやiPlanetなどの他のサーバに影響を及ぼす脆弱性はチェックしません。

このオプションを選択すると、次に説明する1つ以上の識別方法を選択できます。

HTTP応答で正規表現を使用する(Use regular expressions on HTTP responses)

以前のリリースのFortify WebInspectで採用されたこの方法は、特定のサーバを識別するために設計された定義済みの正規表現に一致する文字列をサーバ応答で検索します。

サーバアナライザのフィンガープリント法を使用し、サンプリングを要求する(Use server analyzer fingerprinting and request sampling)

この高度な方法は、一連のHTTP要求を送信してから、応答を分析してサーバ/アプリケーションタイプを判断します。

カスタムサーバ/アプリケーションタイプの定義(Custom server/application type definitions)

ターゲットドメインのサーバタイプが分かっている場合は、[カスタムサーバ/アプリケーションタイプの定義(Custom server/application type definitions)]セクションを使用してそれを選択できます。この識別方法は、指定されたサーバ用に選択された他の方法を無効にします。

カスタム定義を指定するには:

1. [追加(Add)]をクリックします。
[サーバ/アプリケーションタイプ入力(Server/Application Type Entry)]ウィンドウが開きます。
2. [ホスト(Host)]ボックスに、ドメイン名またはホスト、またはサーバのIPアドレスを入力します。
3. (オプション) [識別(Identify)]をクリックします。

Fortify WebInspectは、サーバに接続し、サーバアナライザのフィンガープリント法を使用してサーバタイプを判断します。成功すると、[サーバ/アプリケーションタイプ(Server/Application Type)]リストで対応するチェックボックスがオンにされます。

メモ: または、[正規表現を使用する(Use Regular Expressions)]オプションを選択した場合は、サーバを識別するために設計された正規表現を入力します。正規表現表記を挿入したり、Regular Expression Editor(式の作成とテストを容易にします)を起動したりするには、□をクリックします。

4. [サーバ&アプリケーションタイプ(Server/Application Type)]リストから、1つ以上のエントリを選択します。
5. [OK]をクリックします。

第9章: アプリケーション設定

この章では、Fortify WebInspectがスキャンデータとログファイルを保存する場所を定義する設定と、ライセンス供与、テレメトリ、およびSmartUpdateに関する設定について説明します。これらの設定により、Fortify WebInspectがMicro Focus Application Lifecycle Management (ALM)などの他のアプリケーションと対話するための設定も行われます。

アプリケーション設定: 全般

この機能にアクセスするには、[編集(Edit)] > [アプリケーション設定(Application Settings)] をクリックしてから、[全般(General)]を選択します。

全般(General)

[全般(General)]のオプションの説明を次の表に示します。

| オプション | 説明 |
|--|---|
| ブラウザビューでアクティブコンテンツを有効にする(Enable Active Content in Browser Views) | <p>このオプションは、Fortify WebInspect内のすべてのブラウザウィンドウでJavaScriptとその他のダイナミックコンテンツの実行を可能にする場合に選択します。</p> <p>たとえば、あるFortify WebInspect攻撃は、ダイナミックに生成されたWebページにスクリプトを埋め込もうとすることによって、クロスサイトスクリプティングをテストします。このスクリプトは、番号「76712」を含むアラートを表示するようにサーバに指示します。アクティブコンテンツが有効で、攻撃が成功した場合(つまり、クロスサイトスクリプティングが可能な場合)は、脆弱なセッションを選択して、[セッション情報(Session Info)]パネルで [Webブラウザ(Web Browser)]をクリックすると、スクリプトが実行され、次の画面が表示されます。</p>  <p>メモ: このオプションが無効な状態でスキャンを開始するか開いてからこのオプションを有効にすると、スキャンを閉じて再度開く</p> |

| オプション | 説明 |
|--|--|
| | までブラウザはアクティブコンテンツを実行しません。 |
| 診断ファイルの作成を有効にする (Enable Diagnostic File Creation) | <p>Fortify WebInspectアプリケーションで障害が発生した場合、このオプションが選択されていると、Fortify WebInspectは、障害発生時にメインメモリに保存されていたデータを含むファイルを作成するよう強制されます。後で、Fortifyサポート担当者にそのファイルを提供できます。</p> <p>このオプションを選択する場合は保持すべき診断ファイルの数も指定できます。ファイルの数がこの制限を超えると、最も古いファイルが削除されます。</p> |
| 「次回から表示しない」メッセージをリセットする(Reset "Don't Show Me Again" messages) | <p>デフォルトで、Fortify WebInspectには、さまざまなプロンプトとダイアログボックスが表示され、実行するアクションの結果として発生する可能性がある特定の結果が知られます。これらのダイアログボックスには、「次回から表示しない(Don't show me again)」というラベルのチェックボックスが表示されます。このオプションを選択すると、Fortify WebInspectは、それらのメッセージの表示を中止します。</p> <p>「次回から表示しない」メッセージをリセットする(Reset "Don't Show Me Again" messages)をクリックすると、それらのメッセージの表示を再開するようにFortify WebInspectに強制できます。</p> |
| 7つの有害な界(7PK)分類を使用する(Use Seven Pernicious Kingdom (7PK) Taxonomy) | <p>このオプションを選択すると、報告された脆弱性を順序付けおよび整理するために、7つの有害な界分類を選択できます。</p> <p>7つの有害な界(7PK)は、Fortify Software Security Research GroupとGary McGraw博士が共同で策定したソフトウェアセキュリティエラーの分類です。各脆弱性カテゴリには、問題の詳細な説明と、オリジナルのソースとコード抜粋への参照が付随している(該当する場合)ため、問題をより適切に把握できます。</p> <p>分類スキームの編成は、生物学から借用した用語を使って記述されます。脆弱性のカテゴリは門と呼ばれ、同じテーマを共有する脆弱性カテゴリのコレクションは界と呼ばれます。脆弱性の門は、ソフトウェアセキュリティにとっての重要度順で提示される有害な界に分類されます。</p> <p>7つの界は次のとおりです。</p> <ol style="list-style-type: none">1. 入力の検証と表現2. APIの誤用3. セキュリティ機能 |

| オプション | 説明 |
|------------------------------------|--|
| | <p>4. 時間と状態 5. エラー 6. コードの品質 7. カプセル化 *環境</p> <p>最初の7つの界は、ソースコードのセキュリティ欠陥に関連するもので、最後の1つは、実際のコード以外のセキュリティ問題を表します。</p> <p>この分類を定義する主な目的は、セキュリティルールのセットを整理して、セキュリティに影響を及ぼすエラーの種類をソフトウェア開発者が理解しやすくすることです。システム障害の発生方法の理解を深めると、開発者は自分が作成するシステムを分析する能力が高まり、セキュリティ問題の特定と、それが見つかった場合の対応がより迅速になって、その後は同じミスを繰り返さなくなるのが普通です。詳細については、https://vulncat.fortify.com/を参照してください。</p> <p>Fortify WebInspectを他のMicro Focus Fortify 製品と統合する場合は7つの有害な界の分類を使用できます。これは統一された分類に対応しているためです。</p> |
| OpenSSLエンジンの使用(Use OpenSSL Engine) | <p>デフォルトで、Fortify WebInspectはこのオプションを使用します。OpenSSLエンジンは、TLS 1.3セキュリティプロトコルを使用する必要があるWebサイトをサポートします。OpenSSLは、以前のバージョンのTLSプロトコルと後方互換性があります。</p> <p>このオプションを有効にすると、[スキャン設定: 方法(Scan Settings: Method)]で [SSL/TLSプロトコル(SSL/TLS Protocols)]オプションが無効になります。スキャン用の個別のプロトコルを選択することはできません。</p> <div style="background-color: #f0f0f0; padding: 10px;"><p>メモ: この機能はテクノロジプレビューです。テクノロジプレビュー機能は現在サポートされていないため、完全に機能しない可能性があります。また、運用環境での展開には適しません。ただし、これらの機能は、将来的には完全なサポートを提供できることを目指すために広く拡大することを主な目的として、便宜的に提供されています。</p></div> |
| HTTP/2サポートを有効にする(Enable | WebサイトがHTTP/2プロトコルのみをサポートしており、HTTP/1プロトコルを使用すると問題が発生する場合に、このオプションを使用 |

| オプション | 説明 |
|-----------------|---|
| HTTP/2 Support) | <p>します。</p> <p>メモ: この機能はテクノロジプレビューです。テクノロジプレビュー機能は現在サポートされていないため、完全に機能しない可能性があります。また、運用環境での展開には適しません。ただし、これらの機能は、将来的には完全なサポートを提供できることを目指すために広く拡大することを主な目的として、便宜的に提供されています。</p> |

WebInspect Agent

Fortify WebInspect Agentオプションの説明を次の表に示します。

| オプション | 説明 |
|---|--|
| ターゲットサイトで検出されたWebInspect Agent情報を使用する (Use WebInspect Agent information when encountered on target site) | <p>このオプションが選択されている状態で、Fortify WebInspectが、Fortify WebInspect Agentがターゲットサーバにインストールされていることを検出すると、Fortify WebInspect Agent情報が取り込まれ、全体的なスキャン効率が高まります。</p> <p>Fortify WebInspectダッシュボード上にFortify WebInspect Agentが検出されたかどうかを示す注が表示されます。</p> |
| 脆弱性ウィンドウで重複する脆弱性別に自動的にグループ化する (Automatically group by duplicate vulnerabilities in vulnerability window) | <p>このオプションが選択され、Fortify WebInspect Agent情報が使用される場合(上記の設定)は、サマリペインの 検出事項 (Findings) タブに一覧表示された脆弱性が、チェック別にグループ化されてから、相当する脆弱性別にグループ化されます。</p> |
| WebInspect Agentに攻撃戦略の提案を許可する(Allow WebInspect Agent to suggest attack strategy) | <p>このオプションが選択され、Fortify WebInspect情報が使用される場合(上記の「ターゲットサイトで検出されたWebInspect Agent情報を使用する」を参照)、エージェントはアクティブモードで動作し、Fortify WebInspectに攻撃戦略を提案して、精度とパフォーマンスを上げることができます。この機能にはバージョン4.1以降のFortify WebInspect Agentが必要です。また、7つの有害な界分類を使用する必要があります。</p> |

アプリケーション設定: データベース

この機能にアクセスするには、[編集(Edit)] > [アプリケーション設定(Application Settings)] をクリックしてから、[データベース(Database)] を選択します。

ヒント: Fortify WebInspectがセンサとしてFortify WebInspect Enterpriseに接続されている場合は、SQLデータベースの設定を上書きできます。詳細については、「["アプリケーション設定: SQLデータベース設定の上書き" ページ469](#)」を参照してください。

スキャン/レポートストレージの接続設定

Fortify WebInspectスキャンとレポートのデータを保存するデバイスを選択します。次の選択肢があります。

- **SQL Server Expressを使用する(Use SQL Server Express)** (SQL Server Express Editionの場合)。各スキャンのデータは、別々のデータベースに保存されます。
- **SQL Serverを使用する(Use SQL Server)** (SQL Server Standard Editionの場合)。複数のスキャンのデータは、1つのデータベースに保存されます。複数のデータベース設定を行い、設定のコレクションのそれぞれに「プロファイル名」を割り当てれば、設定を簡単に切り替えることができます。

SQL Serverデータベース特権

データベース接続に対して指定するアカウントは、指定したデータベースのデータベース所有者(DBO)である必要があります。ただし、このアカウントには、データベースサーバに対する sysadmin (SA)特権は必要ありません。指定されたユーザのためにデータベース管理者(DBA)がデータベースを生成しなかった場合、そのアカウントはデータベースの作成と、セキュリティ許可の操作を行う許可も持っている必要があります。DBAは、Fortify WebInspectがデータベースをセットアップした後にこれらの許可を取り消すことができますが、アカウントはそのデータベースのDBOであり続ける必要があります。

SQL Server Standard Editionの設定

SQL Server Standard Editionのプロファイルを設定するには:

1. **設定(Configure)**](ドロップダウンリスト右側にある)をクリックします。
[データベース設定の管理(Manage Database Settings)]ダイアログボックスが表示されます。
2. **追加(Add)**]をクリックします。
[データベースの追加(Add Database)]ダイアログボックスが表示されます。
3. このデータベースプロファイルの名前を入力します。
4. [サーバ名(Server Name)]リストからサーバを選択します。

重要! SQL Server Browserが有効になっていない場合、データベースサーバはリストに表示されません。この場合は、接続情報を手動で入力する必要があります。接続文字列は次のように書式設定されます。

SERVER\INSTANCE,PORT

コロンまたはセミコロンではなく、カンマを使用してポート定義が追加されることに注意してください。

5. [サーバにログオンする(Log on to the server)]グループで、選択したサーバに使用される認証のタイプを指定します。
 - Windows認証を使用する(Use Windows Authentication) - ユーザのWindowsアカウント名とパスワードを送信することによってログオンします。
 - SQL Server認証を使用する(Use SQL Server Authentication) - SQL Server認証を使用します。この認証は、SQL Serverコンピュータによって維持されている内部ユーザーリストに依存します。ユーザー名とパスワードを入力します。
6. 特定のデータベースを入力または選択するか、[新規(New)]をクリックしてデータベースを作成します。
7. [OK]をクリックして、[データベースの追加(Add Database)]ダイアログボックスを閉じます。
8. [OK]をクリックして、[データベース設定の管理(Manage Database Settings)]ダイアログボックスを閉じます。

スキャン表示の接続設定

スキャンのリストを表示する([スキャンの管理(Manage Scans)]ビューまたはReport Generatorウィザードを使用して)と、Fortify WebInspectはSQL Server Standard Editionおよび/またはSQL Server Express Editionに保存されたスキャンデータにアクセスできます。どちらかまたは両方のオプションを選択できます。

- SQL Server Expressに保存されたスキャンの表示(Show Scans Stored in SQL Server Express): ローカルのSQL Server Express Editionに保存されたスキャンデータにアクセスする場合に、このオプションを選択します。
- SQL Server Standardに保存されたスキャンの表示(Show Scans Stored in SQL Server Standard): SQL Server Standard Edition内のデータにアクセスする場合に、このオプションを選択します。手順については、「["SQL Server Standard Editionの設定"前のページ](#)」を参照してください。

Site Explorer用のスキャンデータの作成

スキャン中に、Fortify WebInspectは、SQL Expressデータベース(.mdf)ファイルを作成するか、既存のSQL Serverデータベース(.mdf)ファイルにスキャンを追加します。ただし、Site Explorerでは、トライックセッションファイル(.tsf)形式のバリエーションを使用します。スキャン中に.tsfファイルを作成するようにFortify WebInspectを設定できます。

メモ: Site Explorer用に作成された.tsfファイルには、標準スキャンファイルにある脆弱性やその他の詳細が組み込まれていません。

Site Explorerで表示可能なトラフィックファイルをFortify WebInspectで作成するには、[Site Explorer用のスキャンデータを作成する(Create Scan Data for Site Explorer)]チェックボックスをオンにします。

このオプションがオンになっている場合は、Fortify WebInspectが、<ScanID>.tsfという形式のファイルをユーザのFortify WebInspectディレクトリ内のscandataフォルダ(以下を参照)に作成します。

c:\users\<username>\appdata\local\hp\hp_webinspect\scandata

スキャンの実行中にこのチェックボックスをオンにしても、現在進行中のスキャンには影響しません。このチェックボックスをオンにした後に開始されたスキャンでのみ、Site Explorer用の.tsfファイルが生成されます。

アプリケーション設定: ディレクトリ

この機能にアクセスするには、[編集(Edit)]>[アプリケーション設定(Application Settings)]をクリックしてから、[ディレクトリ(Directories)]を選択します。

Fortify WebInspectファイルの保存場所の変更

Fortify WebInspectファイルが保存される場所を変更できます。場所を変更するには:

- 情報のカテゴリの横にある省略記号ボタン [...]をクリックします。
- [「フォルダの参照(Browse For Folder)」]ダイアログボックスを使用して、ディレクトリを選択または作成します。
- [OK]をクリックします。

アプリケーション設定: ライセンス

この機能にアクセスするには、[編集(Edit)]>[アプリケーション設定(Application Settings)]をクリックしてから、[ライセンス(License)]を選択します。

ライセンスの詳細

このセクションでは、Fortify WebInspectライセンスに関する情報を提供します。ライセンスの特定の条項を変更する場合は、[ライセンス供与の設定(Configure Licensing)]をクリックしてライセンスウィザードを起動します。

ウィンドウの下側のセクションの内容は、現在採用されているライセンス管理のタイプによって異なります。

- Micro Focusライセンスサーバに直接接続されている。「["Micro Focusへの直接接続" 下](#)」を参照してください。
- ローカルのAutoPass License Server (APLS)に接続されている。「["APLSへの接続" 下](#)」を参照してください。
- ローカルのLicense and Infrastructure Manager (LIM)に接続されている。「["LIMへの接続" 次のページ](#)」を参照してください。

Micro Focusへの直接接続

オプションの説明を次の表に示します。

| オプション | 説明 |
|---------------------|--|
| アップデート(Update) | <p>評価版からアップグレードする場合 やそれ以外の方法でライセンスの条件を変更する場合は、[アップデート(Update)]をクリックします。アプリケーションは、ライセンスサーバに接続して、マシンにローカルに保存されている情報を更新します。</p> <p>メモ: このオプションは、AutoPassライセンスを使用するインストールでは使用できません。</p> |
| 非アクティブ化(Deactivate) | <p>Fortify WebInspectライセンスは、特定のコンピュータに割り当てられます。このライセンスを別のコンピュータに転送する場合：</p> <ol style="list-style-type: none">アクティベーショントークンをコピーします。 この番号を紛失したり、保存場所を忘れたりしないように注意してください。書き留めるか印刷して、安全な場所に保管してください。[非アクティブ化(Deactivate)]をクリックします。 アプリケーションは、ライセンスサーバに接続してライセンスを解放し、別のコンピュータにFortify WebInspectをインストールできるようにします。新しいコンピュータで、ライセンス供与用のFortify WebInspectアプリケーション設定にアクセスし、アクティベーショントークンを入力します。 |

APLSへの接続

APLSによって管理される同時使用(フローティング)ライセンスを使用している間は、Fortify WebInspectを常にAPLSに接続しておく必要があります。[ステータス(Status)]に「**切断**」

(Disconnected)]と表示されている場合は、[再接続(Reconnect)]をクリックして、APLSの接続を再確立します。

LIMへの接続

このコンピュータに割り当てられたFortify WebInspectライセンスをLicense and Infrastructure Managerで処理する方法を選択します。オプションの説明を次の表に示します。

| オプション | 説明 |
|--------------------------------|---|
| 接続ライセンス (Connected License) | LIMに接続できる場合にのみ、コンピュータはFortifyソフトウェアを実行できます。ソフトウェアを起動するたびに、LIMがライセンスプールからこのインストールにシートを割り当てます。ソフトウェアを閉じると、コンピュータからシートが解放されて再びプールに割り当てられるため、別のユーザがそのライセンスを使用できるようになります。 |
| 分離ライセンス | コンピュータはどこでも、企業インターネット(LIMが通常存在する場所)から切断されている場合でさえ、Fortifyソフトウェアを実行できます。しかし、これは指定された有効期限までです。そのため、ラップトップをリモートサイトに持ち込んでソフトウェアを実行することができます。企業インターネットに再接続すると、アプリケーションライセンスの設定にアクセスして、[分離(Detached)]から[接続(Connected)]に再設定できます。 |

アプリケーション設定: Server Profiler

この機能にアクセスするには、[編集(Edit)] > [アプリケーション設定(Application Settings)] をクリックしてから、[Server Profiler]を選択します。

スキャンを開始する前に、Fortify WebInspectは、Server Profilerを呼び出して、ターゲットWebサイトの事前テストを実行し、特定のスキャン設定を変更すべきかどうかを判断できます。変更が必要だと思われる場合、Server Profilerは提案のリストを返します。これらの提案は、受け入れることも拒否することもできます。

この事前テストを有効にするには、ステップ4で[プロファイル(Profile)]をクリックします(または[Profilerを自動的に実行する(Run Profiler Automatically)]を選択します)。

デフォルトで、10個の特定のモジュールが有効になります。モジュールを除外するには、関連付けられたチェックボックスをオフにします。

モジュール

Server Profilerモジュールの説明を次の表に示します。

| モジュール | 説明 |
|--------------------------|--|
| 大文字と小文字を区別するサーバのチェック | このモジュールでは、ホストサーバがURLを識別する際に大文字と小文字を区別するかどうかを判別します。たとえば、一部のサーバ(IISなど)は、www.mycompany.com/samplepage.htmとwww.mycompany.com/TabPage.htmを区別しません。プロファイルにより、サーバが大文字と小文字を区別しないと判別された場合は、Fortify WebInspectの大文字と小文字を区別する機能を無効にできます。そうすることによって、Web探索の速度と精度が向上します。 |
| 「最大フォルダ深さ」設定のチェック | 最大フォルダ深さ設定は主に、プログラムによってURLにサブフォルダを追加するサイトを対象とします。このような制限がない場合、Fortify WebInspectはそれらのダイナミックフォルダを無制限にWeb探索します。このモジュールでは、その制限を超える有効なURLがサイトに含まれているかどうかを判別します。含まれている場合は、設定を大きくすることができます。 |
| クライアント認証プロトコルの検証 | このモジュールでは、必要な認証(サインイン)プロトコル(ある場合)を判別します。Fortify WebInspectは、ADFS CBT、自動、ダイジェスト、HTTP基本、Kerberos、およびNTLMをサポートしています。 |
| 追加のホストのチェック | このモジュールは、ターゲットサイトで追加のホストサーバへの参照を検索し、それらを許可ホストとして含めることができます。 |
| ナビゲーションパラメータの表示 | このモジュールは、ターゲットサイトでページのコンテンツを指定するためにURL内のクエリパラメータが使用されているかどうかを判断します。使用されている場合は、分析中に検出されたパラメータと値のリストを表示します。Fortify WebInspectがスキャン中に使用する1つ以上のパラメータを選択できます。 |
| 非標準の「ファイルが見つからない」応答のチェック | このモジュールは、存在しないリソースをクライアントから要求された場合に、サイトが404以外の応答コードを返すかどうかを判断します。これを認識すると、Fortify WebInspectは不必要的応答を監査しなくなります。 |
| URLに埋め込まれたセッション状態のチェック | 一部のサーバは、クッキーを使用する代わりにセッション状態をURLに埋め込みます。Fortify WebInspectは、正規表現を使用してURLを分析することによって、このプラクティスを検出します。このモ |

| モジュール | 説明 |
|------------------------|---|
| | モジュールは、正規表現に対する変更が必要かどうかを判断します。 |
| スレッド数の分析 | このモジュールは、スレッド数を小さくすべきかどうかを判断します。高速スキャンが有効な場合、スレッド数が比較的に大きくなると、サーバリソースが使い果たされる可能性があります。 |
| 無効な監査除外のチェック | Fortify WebInspect設定では、特定のファイル拡張子を持つページを監査から除外します(「 "監査設定:セッション除外" ページ431 」を参照)。指定された拡張子は、通常、要求のURLにクエリパラメータが含まれていないページ用です。設定が間違っていると、監査が不完全になります。監査除外される拡張子を持つページに実際にはクエリパラメータがある場合、プロファイラはそれを検出でき、それらの除外を削除するよう推奨します。 |
| 最大応答サイズの検証 | Fortify WebInspectスキャン設定では、許容される最大応答サイズを指定します。デフォルトは1,000キロバイトです。このモジュールは最大値より大きい応答の検出を試みて、それが見つかった場合に制限の引き上げを推奨します。 |
| 特定のアプリケーションの設定の最適化 | このモジュールは、スキャンしているのがよく知られたテストサイト(WebGoat、Hacme Bankなど)であるかどうかを判断し、Fortify WebInspectにそのサイト専用に設計された事前入力設定ファイル(テンプレート)があるかどうかを判断します。これらのテンプレートは、スキャンのWeb探索、監査、およびパフォーマンスを最適化するよう設定されています。 |
| 末尾のスラッシュの追加/削除 | このモジュールは、ターゲットサイトで開始URLの末尾のスラッシュが必須か禁止かを判断します。 |
| クロスサイトリクエストフォージェリのチェック | クロスサイトリクエストフォージェリは、ワンクリック攻撃やセッションライディングとも呼ばれます、多くの場合、CSRFと省略されます。CSRFは、Webサイトが信頼するユーザから不正なコマンドが送信されるWebサイトエクスプロイトの一 種です。特定のサイトに対するユーザの信頼を悪用するクロスサイトスクリプティングとは異なり、CSRFは、サイトがユーザのブラウザ内で持っている信頼を悪用します。CSRFの詳細については、「 "CSRF" ページ395 」を参照してください。 |
| WebSphereサーバのチェック | WebSphereサーバには、追加の設定変更が必要です。このProfilerでは、これらの変更が必須かどうかを検出します。 |

アプリケーション設定: ステップモード

この機能にアクセスするには、[編集(Edit)] > [アプリケーション設定(Application Settings)] をクリックしてから、[ステップモード(Step Mode)] を選択します。

ステップモードのオプションの説明を次の表に示します。

| オプション | 説明 |
|------------------------------------|---|
| デフォルト監査モード (Default Audit Mode) | <p>次のいずれかを選択します。</p> <ul style="list-style-type: none">ブラウズ時の監査(Audit as you browse): ターゲットWebサイトを移動している間に、Fortify WebInspectがアクセス先のページを同時に監査します。手動監査(Manual Audit): このオプションを使用すると、ステップモードスキャンを一時停止してFortify WebInspectに戻り、特定のセッションを選択して監査することができます。 |
| プロキシリスナ(Proxy Listener) | <p>次のオプションを選択します。</p> <ul style="list-style-type: none">ローカルIPアドレス(Local IP Address): ステップモードではプロキシが必要です。プロキシで使用するIPアドレスを指定します。ポート(Port): プロキシで使用すべきポートを指定するか、ポートを自動的に割り当てる(Automatically Assign Port) を選択します。 |

アプリケーション設定: 2要素認証

この機能にアクセスするには、[編集(Edit)] > [アプリケーション設定(Application Settings)] をクリックしてから、[2要素認証(Two-Factor Authentication)] を選択します。

テクノロジプレビュー

この機能はテクノロジプレビューとして提供されます。

テクノロジプレビュー機能は現在サポートされていないため、完全に機能しない可能性があります。また、運用環境での展開には適しません。ただし、これらの機能は、将来的には完全なサポートを提供できることを目指すために広く拡大することを主な目的として、便宜的に提供されています。

2要素認証コントロールセンター

「ユーザが持っているもの」としての2要素認証には、WebアプリケーションにログインするユーザにSMS応答または電子メール応答を送信するアプリケーションサーバが関与します。スキヤンで2要素認証を使用するには、Node.jsサーバをコントロールセンターとして設定し、アプリケーションサーバから受信したSMS応答と電子メール応答を処理する必要があります。詳細については、「["2要素認証の使用" ページ198](#)」を参照してください。

コントロールセンターを設定するには:

1. [ローカルIPアドレス(Local IP Address)]ドロップダウンリストで、IPアドレスを選択します。

メモ: これらのIPアドレスは、Fortify WebInspectがインストールされているマシンで使用できます。

2. 次のいずれかを実行します。

- 特定のポートを使用するには、[ポート(Port)]リストからポートを選択します。
- Fortify WebInspectにポートを選択させるには、[ポートを自動的に割り当てる(Automatically Assign Port)]チェックボックスをオンにします。

重要! モバイルアプリケーションからサーバにアクセスするには、コントロールセンターのポートをファイアウォールで公開する必要があります。

3. [初期化(Initialize)]をクリックします。

コントロールセンターが開始されます。

モバイルアプリケーション

アプリケーションサーバがSMS応答を送信する場合は、Fortify2FAモバイルアプリケーションをインストールし、それに2要素認証設定をダウンロードする必要があります。設定後は、モバイルアプリケーションがSMS応答を受信し、それをコントロールセンターに転送します。

メモ: 現時点で、モバイルアプリケーションはAndroidオペレーティングシステムでのみ使用できます。

モバイルアプリケーションを設定するには:

1. [携帯電話番号(Mobile Phone Number)]ボックスに、SMS応答を受信する電話番号を入力します。
2. [QRコードの生成(Generate QR Code)]をクリックします。
コントロールセンターにより、2要素認証設定とモバイルアプリケーションをダウンロードするためのリンクを含むクイックレスポンス(QR)コードが生成されます。
3. モバイルアプリケーションをインストールして設定します。詳細については、「["Fortify2FAモバイルアプリのインストールと設定" 次のページ](#)」を参照してください。

ヒント: スキャンで複数のスレッドを使用する場合は、複数の電話機を使用できます。マルチユーザスキャンに同じ電話番号を使用すると、スキャン時間に影響します。

4. (オプション)別の電話機用にモバイルアプリケーションを設定するには、ステップ1-3を繰り返します。

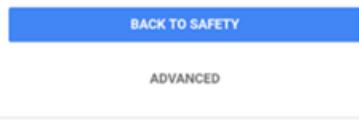
Fortify2FAモバイルアプリのインストールと設定

SMS応答を受信する携帯電話にモバイルアプリケーションをインストールして設定するには:

1. 携帯電話のカメラを使用して、[2要素認証モバイルアプリケーション(Two-factor Authentication Mobile Application)]の設定内のQRコードをスキャンします。
リンクが表示されます。
2. リンク(または[開く(Open)]ボタン)をクリックして、アプリをダウンロードするためのサイトにアクセスします。
自己署名証明書に関する警告が表示されます。

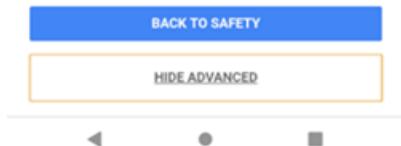


Your connection is not private
Attackers might be trying to steal your information from
[REDACTED] (for example, passwords, messages, or
credit cards). Learn more
NET::ERR_CERT_AUTHORITY_INVALID

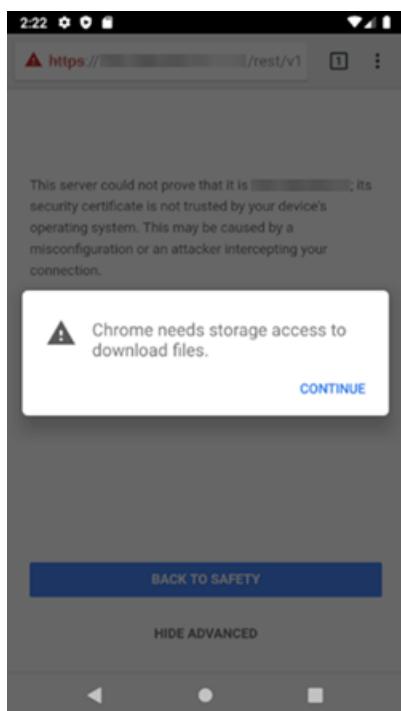


3. 詳細(ADVANCED)をクリックします。

続行するためのリンクと共に追加情報が表示されます。

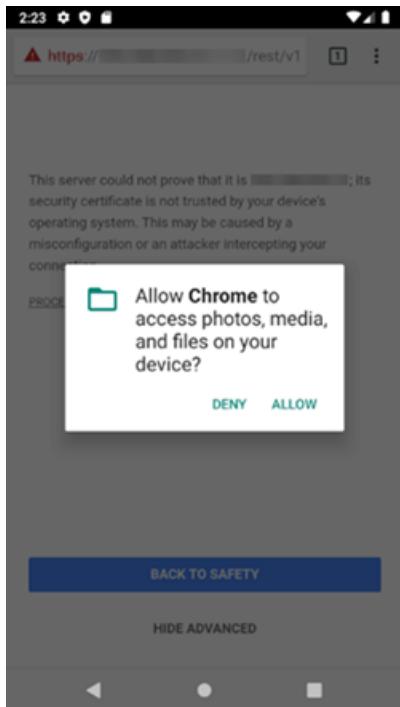


4. **<ip_address>に進む(危険) (PROCEED TO <ip_address> (UNSAFE))**]をクリックします。
ダウンロードファイルへのストレージアクセスを要求するプロンプトが表示されます。

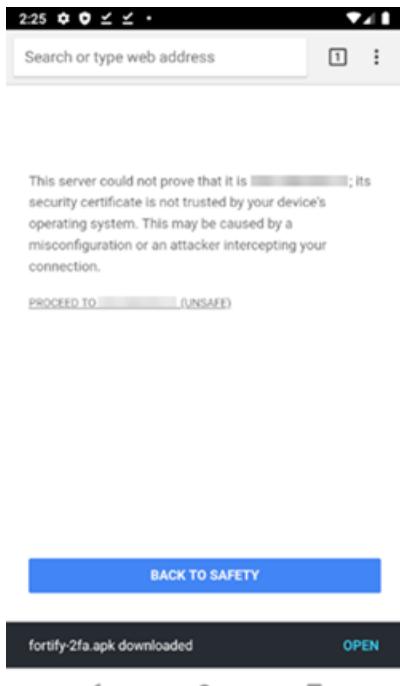


5. **続行(CONTINUE)**]をクリックします。

デバイス上の写真、メディア、およびファイルへのアクセスを要求するプロンプトが表示されます。

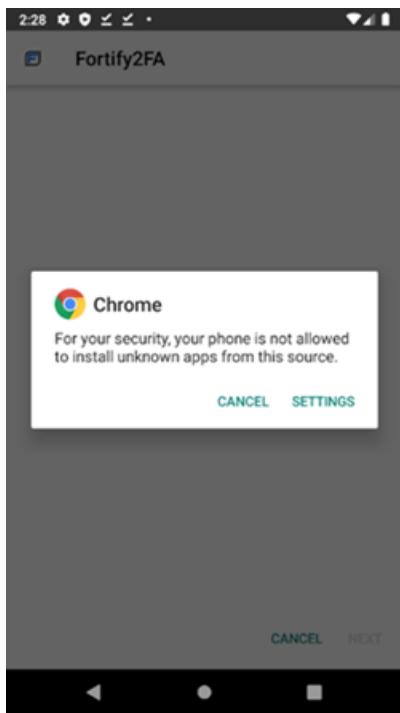


6. [許可(ALLOW)]をクリックします。
fortify-2fa.apkファイルがダウンロードされます。



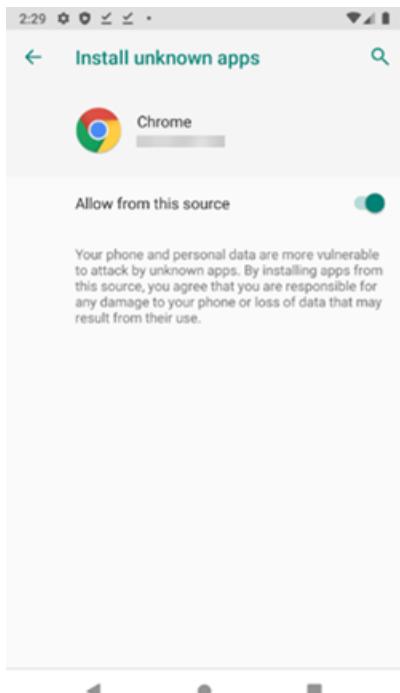
7. [開く(OPEN)]をクリックします。

不明なアプリのインストールに関するプロンプトが表示されます。



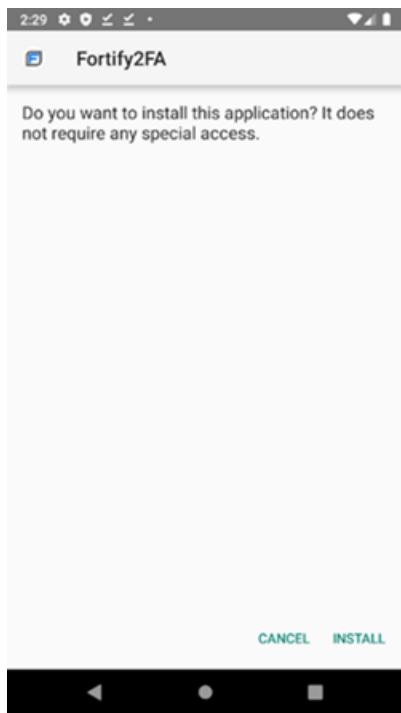
8. [設定(SETTINGS)]をクリックします。

【不明なアプリのインストール(Install unknown apps)】設定が表示されます。

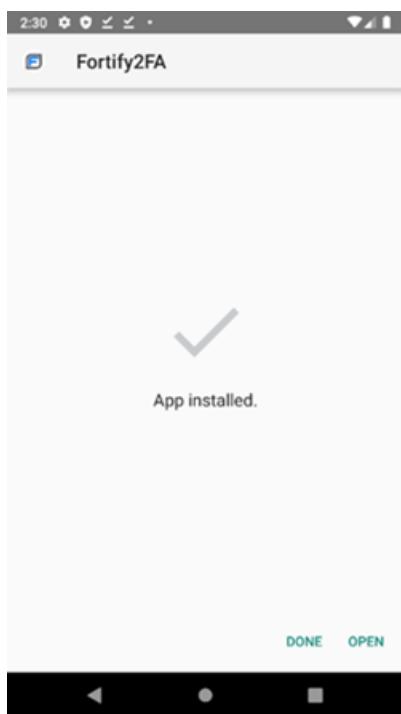


9. 【このソースからの受信を許可する(Allow from this source)】を有効にします。

アプリケーションをインストールするかどうかを尋ねるプロンプトが表示されます。

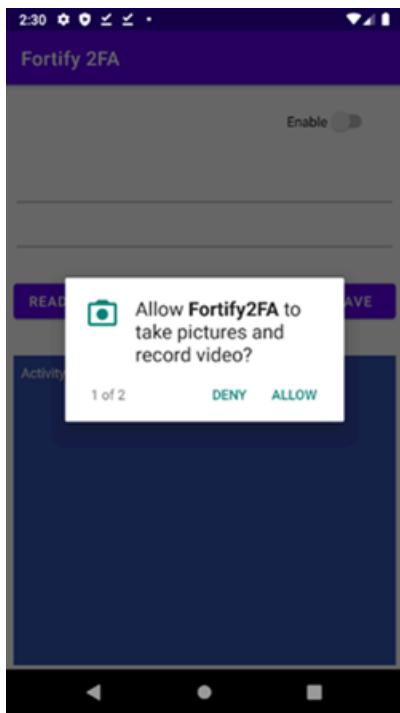


10. [インストール(INSTALL)]をクリックします。
アプリがインストールされていることを示すメッセージが表示されます。



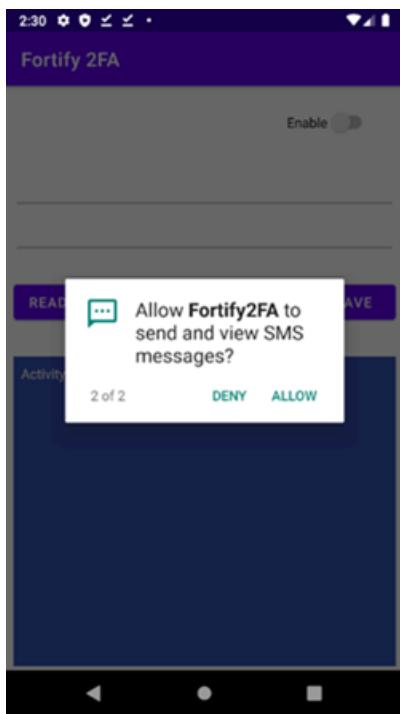
11. [開く(OPEN)]をクリックします。

写真を撮り、ビデオを録画する許可を要求するプロンプトが表示されます。



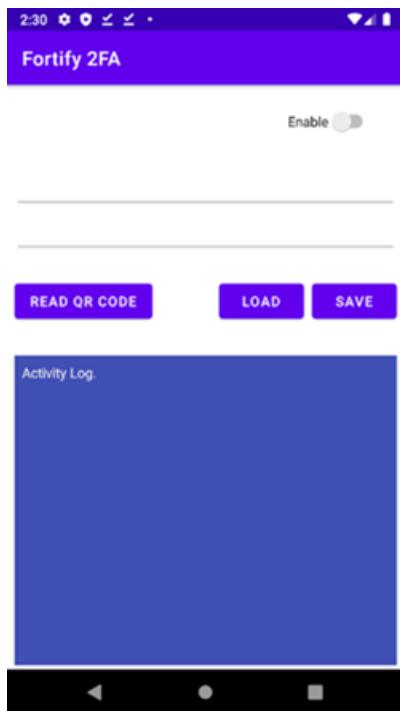
12. 許可(ALLOW)をクリックします。

SMSメッセージを送信して表示する許可を要求するプロンプトが表示されます。



13. 許可(ALLOW)をクリックします。

アプリを設定する準備が整いました。



14. 「QRコードの読み取り(READ QR CODE)」をクリックして、[2要素認証モバイルアプリケーション(Two-factor Authentication Mobile Application)]の設定内のQRコードをスキャンします。
2要素認証の設定は、Fortify2FAモバイルアプリケーションで行われます。

アプリケーション設定: ログ記録

この機能にアクセスするには、[編集(Edit)] > [アプリケーション設定(Application Settings)]をクリックしてから、[ログ記録(Logging)]を選択します。

[ログ記録(Logging)]のオプションの説明を次の表に示します。

| オプション | 説明 |
|--------------------------------|---|
| ログのクリア(Clear Logs) | このボタンをクリックすると、すべてのログがクリアされます。 |
| 最小ログレベル(Minimum Logging Level) | Fortify WebInspectがアプリケーション内で発生するさまざまな機能とイベントをログに記録する方法を指定します。選択肢は、[デバッグ(Debug)]、[情報(Info)]、[警告(Warn)]、[エラー(Error)]、および[重大(Fatal)](詳細度の高いものから低いものの順)です。 |
| ログページのしきい | [ページしない(Never Purge)]を選択しないと、すべてのログによつ |

| オプション | 説明 |
|--|--|
| 値(Threshold for Log Purging) | て使用されているディスク容量の合計が指定のサイズを超えた場合、またはログの数が指定の数を超えた場合に、Fortify WebInspectによってすべてのログが削除されます。または、ログファイルを「ページしない(Never Purge)」を選択することもできます。 |
| ローリングログファイルの最大サイズ(Rolling Log File Maximum Size) | 個々のログファイルに割り当てる最大サイズをキロバイト単位で指定します。ファイルがこの制限に達すると、Fortify WebInspectは単純にそのファイルへの書き込みを停止します。 |

アプリケーション設定: プロキシ

この機能にアクセスするには、[編集(Edit)] > [アプリケーション設定(Application Settings)] をクリックしてから、[プロキシ設定(Proxy Settings)] を選択します。

Fortify WebInspect Webサービスは、アップデートとサポートのコミュニケーションに使用されます。[プロキシ設定(Proxy Settings)] でこれらのサービスへのアクセス方法を設定します。

プロキシサーバを使用しない

これらのサービスへのアクセスにプロキシサーバを使用しない場合は、[直接接続(プロキシ無効)(Direct Connection (proxy disabled))] を選択します。

プロキシサーバを使用する

プロキシサーバを使用してこれらのサービスにアクセスする必要がある場合は、次の表に示すオプションを選択します。

| オプション | 説明 |
|---|--|
| プロキシ設定の自動検出(Auto detect proxy settings) | WPAD (Web Proxy Autodiscovery)プロトコルを使用してプロキシ自動設定ファイルを探し、ブラウザのWebプロキシ設定を行います。 |
| システムのプロキシ設定を使用する(Use System Proxy settings) | ローカルマシンからプロキシサーバ情報をインポートします。 メモ: システムのプロキシ設定を使用することにしても、プロキシサーバ経由のインターネットアクセスが保証されるわけではありません。Internet Explorerの[LANにプロキシサーバを使用する]設定が選択されていない場合、プロキシは使用されません。 |

| オプション | 説明 |
|---|---|
| Firefoxプロキシ設定を使用する(Use Firefox proxy settings) | Firefoxからプロキシサーバ情報をインポートします。 メモ: Firefoxプロキシ設定を使用することにしても、プロキシサーバ経由のインターネットアクセスが保証されるわけではありません。Firefoxブラウザの接続設定が「プロキシーを使用しない」に設定されている場合、プロキシは使用されません。 |
| PACファイルを使用してプロキシを設定する(Configure a proxy using a PAC file) | [URL]ボックスで指定した場所にあるPAC (Proxy Automatic Configuration)ファイルからプロキシ設定をロードします。 |
| プロキシを明示的に設定する(Explicitly configure proxy) | 要求された情報を入力することによって、プロキシを設定します。このトピックの「 "プロキシの設定" 下 」を参照してください。 |

プロキシの設定

プロキシを設定するには:

1. [サーバ(Server)]ボックスにプロキシサーバのURLまたはIPアドレスを入力し、続いて(ポート(Port)]ボックスに)ポート番号(8080など)を入力します。
2. [タイプ(Type)]リストから、プロキシサーバ経由のTCPトラフィックを処理するプロトコル(SOCKS4、SOCKS5、または標準)を選択します。

重要! SOCKS4またはSOCKS5プロキシサーバ設定を使用する場合は、スマートアップデートが使用できません。スマートアップデートは、標準プロキシサーバを使用する場合にのみ使用できます。

3. 認証が必要な場合は、[認証(Authentication)]リストからタイプを選択します。オプションを次に示します。

- **自動**

メモ: 自動検出を指定すると、スキャンの処理が遅くなります。把握している別の認証メソッドを指定すると、スキャンのパフォーマンスは大幅に向上します。

- **_digest(Digest)**
- **HTTP基本(HTTP Basic)**
- **NT LAN Manager (NTLM)**
- **Kerberos**

- ネゴシエート(Negotiate)

4. プロキシサーバで認証が必要な場合は、適格なユーザ名とパスワードを入力します。

アプリケーション設定: レポート

この機能にアクセスするには、[編集(Edit)] > [アプリケーション設定(Application Settings)] をクリックしてから、[レポート(Reports)] を選択します。

オプション

レポートオプションの説明を次の表に示します。

| オプション | 説明 |
|--|--|
| 常にお気に入りを保存するように要求する(Always prompt to save favorites) | 「お気に入り」は、1つ以上のレポートとその関連パラメータの単なる名前付きコレクションです。Report Generatorを使用する場合は、レポートとパラメータを選択してから、[お気に入り(Favorites)] > [お気に入りに追加(Add to favorites)] を選択して組み合わせを作成できます。このオプションを選択すると、レポートを追加または削除してお気に入りが変更されたときに、それを保存するようFortify WebInspectから要求されます。 |
| 脆弱性テキストのスマート切り捨て(Smart truncate vulnerability text) | 生成されたレポートに、非常に長いHTTP要求メッセージと応答メッセージが含まれている場合があります。スペースを節約し、脆弱性に関する適切なデータに焦点を当てるために、脆弱性を識別または確認するデータ(赤い強調表示で識別)の前後のメッセージコンテンツを除外できます。 次の例では、「スマート」切り捨てと20文字のパディングサイズを使用したクロスサイトスクリプティング脆弱性のレポートを示します。ヘッダは常に全体が報告されます。残りのメッセージテキストは、脆弱性、その前の20文字、およびその後の20文字を除き、削除されます。保持されたテキストは、「...TRUNCATED...」という表記で囲まれます。これによって、切り捨てが発生したことを示します。オリジナルのメッセージの長さは、2,377文字(Content-Length: 2377)だったことに注意してください。 |

| オプション | 説明 |
|-------|---|
| | <p>Response:</p> <pre>HTTP/1.1 200 OK Date: Tue, 04 Aug 2009 17:35:10 GMT Server: Microsoft-IIS/6.0 X-Powered-By: ASP.NET Content-Length: 2377 Content-Type: text/html Cache-control: private ...TRUNCATED...1>Household Checking<script>alert(53316)</script></td> </tr> <tr>...TRUNCATED...</pre> <p>レポートでスマート切り捨てを使用するには、脆弱性テキストのスマート切り捨て(Smart truncate vulnerability text)]を選択してから、脆弱性を識別または確認するデータの前後に保持する文字数を指定します。1つの要求または応答で最大10件の脆弱性を報告できます。</p> <p>メモ: この機能が説明どおりに機能するのは、RequestTextデータフィールドとResponseTextデータフィールドを含むレポートコントロールのTruncateVulnerabilityプロパティがTrueに設定され、MaxLengthプロパティが0に設定されている場合のみです。TruncateVulnerabilityがTrueに設定され、MaxLengthプロパティが0以外の場合は、パディングサイズのアプリケーション設定がMaxLength値によって上書きされます。</p> |

ヘッダとフッタ

すべてのレポートでデフォルトで使用されるヘッダとフッタを含むテンプレートを選択します。また、必要に応じて、要求されたパラメータを入力します。

Fortify WebInspect Master Reportは、3つのイメージを使用してレポートを作成します。

- カバーページのイメージはカバーページの中央に表示されます。イメージの上辺が一番上から約3.5インチの位置に表示されます。
- ヘッダロゴのイメージは、各ページのヘッダの左側に表示されます。

アプリケーション設定: テレメトリ

この機能にアクセスするには、**編集(Edit)]> [アプリケーション設定(Application Settings)]**をクリックしてから、**テレメトリ(Telemetry)**]を選択します。

テレメトリについて

テレメトリは、Fortify WebInspectの使用状況情報を収集して送信するための自動化プロセスをFortifyに提供します。Fortifyソフトウェア開発者は、この情報を製品の改善に役立てます。

メモ: 収集される情報には、個人を特定できるデータは含まれません。

「**アプリケーション設定: テレメトリ**」ページを使用して、Fortifyに送信する情報の種類とその他のテレメトリ設定を行います。

テレメトリの有効化

「**テレメトリ**」チェックボックスをオンにして、Fortify WebInspectが使用状況情報を収集してFortifyに送信できるようにします。

テレメトリ経由のスキャンのアップロード

テレメトリ経由で送信されるデータの一部としてスキャンファイルをアップロードするように選択できます。スキャンが一時停止または完了した場合にスキャンファイルのアップロードを要求するには、「**スキャンの停止時にスキャンアップロードを要求する(Prompt for scan upload when a scan stops)**」を選択します。

このプロンプトでは、ログファイルと一緒にスキャンをアップロードすることも、スキャンログファイルのみをアップロードすることもできます。

アップロード間隔の設定

「**アップロード間隔(分単位) (Upload interval (in minutes))**」ボックスでは、収集した情報をFortifyに送信する頻度を定義します。値の範囲は5-45分です。デフォルト設定は10分です。間隔を変更するには:

- 間隔を長くして、Fortifyに情報を送信する頻度を下げるには、「**アップロード間隔(分単位) (Upload interval (in minutes))**」ボックスで必要な設定が表示されるまで上矢印をクリックします。
- 間隔を短くして、Fortifyに情報を送信する頻度を上げるには、「**アップロード間隔(分単位) (Upload interval (in minutes))**」ボックスで必要な設定が表示されるまで下矢印をクリックします。
- 特定の時間間隔を設定するには、「**アップロード間隔(分単位) (Upload interval (in minutes))**」ボックスに数値を入力します。

オンディスクキャッシュサイズの設定

最大オンディスクキャッシュサイズ(MB単位) (Maximum on-disk cache size (in MB))]ボックスでは、テlemetry用に収集された情報に割り当て可能なディスクキャッシュの量を指定します。値の範囲は250-1024MBです。デフォルト設定は500MBです。間隔を変更するには:

- 割り当てられたディスクキャッシュを増減するには、**最大オンディスクキャッシュサイズ(MB単位) (Maximum on-disk cache size (in MB))**]ボックスで必要な設定が表示されるまで上矢印または下矢印をクリックします。
- 特定のキャッシュサイズを設定するには、**最大オンディスクキャッシュサイズ(MB単位) (Maximum on-disk cache size (in MB))**]ボックスに数値を入力します。

送信する情報のカテゴリの特定

分類されたテlemetryオプトイン(Categorized Telemetry Opt-in)]オプションでは、収集して送信する情報のタイプを指定します。すべてのオプションがデフォルトで選択され、Fortifyに送信されるデータに含まれられます。オプションには、さまざまなFortify WebInspect機能、ツール、およびユーザインターフェースなどのカテゴリが含まれます。

カテゴリからオプトアウトするには:

- カテゴリチェックボックスをオフにします。

アプリケーション設定: センサとしての実行

この機能にアクセスするには、**編集(Edit)**] > **アプリケーション設定(Application Settings)**]をクリックしてから、**センサとしての実行(Run as a Sensor)**]を選択します。

センサ

この設定情報は、Fortify WebInspectをセンサとしてFortify WebInspect Enterpriseに統合するために使用されます。情報を入力してセンササービスを開始したら、Fortify WebInspect グラフィカルユーザインターフェースではなく、Fortify WebInspect Enterpriseコンソールを使用してスキャンを実行する必要があります。

次の表に、オプションの説明を示します。

| オプション | 説明 |
|------------------------------|---|
| マネージャURL (Manager URL) | Fortify WebInspect Enterprise ManagerのURLまたはIPアドレスを入力します。 |
| センサ認証(Sensor Authentication) | ユーザ名(ドメイン\ユーザ名の形式)とパスワードを入力してから、 テスト(Test)]をクリックしてエントリを検証します。 |

| オプション | 説明 |
|--|---|
| プロキシの有効化 (Enable Proxy) | Fortify WebInspectがプロキシサーバを経由して、Fortify WebInspect Enterprise Managerにアクセスする必要がある場合は、[プロキシの有効化(Enable Proxy)]を選択してから、サーバのIPアドレスとポート番号を入力します。認証が必要な場合は、有効なユーザ名とパスワードを入力します。 |
| データベース設定の上書き(Override Database Settings) | 通常、Fortify WebInspectは、スキャンデータをデータベースコネクティビティ用のアプリケーション設定で指定されたデバイスに保存します。詳細については、「 "アプリケーション設定: データベース" ページ 446 」を参照してください。 ただし、Fortify WebInspectがセンサとしてFortify WebInspect Enterpriseに接続されている場合は、このオプションを選択してから、[設定(Configure)]をクリックして代替デバイスを指定できます。詳細については、「 "アプリケーション設定: SQLデータベース設定の上書き" 次のページ 」を参照してください。 |
| サービスアカウント (Service Account) | 次のいずれかのオプションを選択して、サービスを実行するアカウントを指定します。 <ul style="list-style-type: none"> ローカルシステムアカウント(Local system account): LocalSystemアカウントは、サービスコントロールマネージャによって使用される定義済みのローカルアカウントです。このサービスは、ローカルリソースに無制限にアクセスできます。 このアカウント(This account): アカウントを特定し、パスワードを提供します。 |
| センサステータス (Sensor Status) | このエリアにはセンササービスの現在のステータスが表示され、サービスを開始または停止するためのボタンが表示されます。 Fortify WebInspectをセンサとして設定したら、[開始(Start)]をクリックします。 <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <p>メモ: 通常、Fortify WebInspectがセンサとして設定されている場合は、Fortify WebInspectをスタンドアロンアプリケーションとして起動すると、センササービスが停止します。その後、Fortify WebInspectを閉じると、サービスが再起動して、再び、Fortify WebInspect Enterprise Managerの制御下に置かれます。ただし、Fortify WebInspectをスタンドアロンアプリケーションとして実行している間にスマートアップデートを実行した場合、サービスは自動的に再起動されません。[開始(Start)]ボタンをクリックする(または、タスクバーの通知エリアにあるFortifyアイコンを右クリックして[センサの開始(Start Sensor)]を選択する)必要が</p> </div> |

| オプション | 説明 |
|-------|-------|
| | あります。 |

アプリケーション設定: SQLデータベース設定の上書き

この機能にアクセスするには、[編集(Edit)] > [アプリケーション設定(Application Settings)] > [センサとして実行(Run as a Sensor)] > [設定(Configure)] をクリックします。

データベース設定の上書き(Override Database Settings)

通常、Fortify WebInspectは、スキャンデータをデータベースコネクティビティ用のアプリケーション設定で指定されたデバイスに保存します。詳細については、「["アプリケーション設定: データベース" ページ446](#)」を参照してください。

ただし、Fortify WebInspectがセンサとしてFortify WebInspect Enterpriseに接続されている場合は、このオプションを選択してから、[設定(Configure)] をクリックして代替デバイスを指定できます。詳細については、「["アプリケーション設定: センサとしての実行" ページ467](#)」を参照してください。

SQLデータベースの設定

センサとしてのFortify WebInspectのSQLデータベース設定を行うには:

1. [アプリケーション設定(Application Settings)] ウィンドウで、[データベース設定の上書き(Override Database Settings)] を選択し、[設定(Configure)] をクリックします。[SQL設定(Configure SQL Settings)] ダイアログボックスが表示されます。
2. 次のいずれかのオプションを選択します。
 - SQL Server Expressを使用する(Use SQL Server Express)
 - SQL Serverを使用する(Use SQL Server)
3. [SQL Server Expressを使用する(Use SQL Server Express)] を選択した場合は、[OK] をクリックしてタスクを完了し、[アプリケーション設定(Application Settings)] ウィンドウに戻ります。
4. [SQL Serverを使用する(Use SQL Server)] を選択した場合は、[サーバ名(Server Name)] を入力するか、リストからサーバ名を選択します。
5. サーバ名を更新するには、[更新(Refresh)] をクリックします。

6. 「サーバにログオンする(Log on to the server)」エリアで、次のいずれかの認証オプションを選択します。
 - Windows認証を使用する(Use Windows Authentication)
 - SQL Server認証を使用する(Use SQL Server Authentication)
7. 「ユーザー名(User name)」と「パスワード(Password)」を入力して、サーバにログオンします。「データベースに接続する(Connect to a Database)」エリアで、リストからデータベース名を選択または入力するか、「新規(New)」をクリックしてデータベースを参照します。
8. 「OK」をクリックします。

アプリケーション設定: スマートアップデート

この機能にアクセスするには、[編集(Edit)] > [アプリケーション設定(Application Settings)] をクリックしてから、「スマートアップデート(Smart Update)」を選択します。

オプション

スマートアップデートオプションの説明を次の表に示します。

| オプション | 説明 |
|--|--|
| サービス(Service) | スマートアップデートサービスのURLを入力します。デフォルト値は: https://smartupdate.fortify.microfocus.com/ |
| 起動時にスマートアップデートを有効にする(Enable Smart Update on Startup) | このオプションを選択すると、Fortify WebInspectの起動時にアップデートが自動的にチェックされます。 |

オフラインのWebInspectの更新手順を含む詳細については、「["SmartUpdate" ページ297](#)」を参照してください。

アプリケーション設定: サポートチャネル

この機能にアクセスするには、[編集(Edit)] > [アプリケーション設定(Application Settings)] をクリックしてから、「サポートチャネル(Support Channel)」を選択します。

Fortify WebInspectサポートチャネルを使用すると、Fortify WebInspectがMicro Focusに対してデータを送信したり、メッセージをダウンロードしたりできるようになります。これは、主に、ログと「誤検出」レポートの送信や「新機能」通知の受信に使用されます。

サポートチャネルを開く

【Micro Focusへの接続を許可する(Allow connection to Micro Focus)】オプションを選択して、Fortify WebInspectサポートチャネルを開きます。その後で、次の項目を指定できます。

- サポートチャネルURL (Support Channel URL) -デフォルトは次のとおりです。
https://supportchannel.fortify.microfocus.com/service.asmx
- アップロードディレクトリ(Upload Directory) -デフォルトは次のとおりです。
C:\ProgramData\HP\HP WebInspect\SupportChannel\Upload\
- ダウンロードディレクトリ(Download Directory) -デフォルトは次のとおりです。
C:\ProgramData\HP\HP WebInspect\SupportChannel\Download\

アプリケーション設定: Micro Focus ALM

この機能にアクセスするには、【編集(Edit)】>【アプリケーション設定(Application Settings)】をクリックしてから、【Micro Focus ALM】を選択します。

Fortify WebInspectとMicro Focus Application Lifecycle Management (ALM)を統合するには、ALMサーバ、プロジェクト、欠陥の優先度、およびその他の属性を記述した1つ以上のプロファイルを作成する必要があります。次いで、Fortify WebInspectの脆弱性をALM欠陥に変換して、ALMデータベースに追加できます。

ALMライセンスの使用

プロファイルの作成や編集では、ALMに発行されたライセンスが使用されます。ただし、ALMアプリケーション設定を閉じると、ライセンスは解放されます。同様に、脆弱性をALMに送信すると、ライセンスが使用されますが、脆弱性の送信後には解放されます。

作業を開始する前に

プロファイルを作成する前に、ALMクライアント登録アドインがFortify WebInspectと同じマシンにインストールされていることを確認してください。詳細については、ALMのマニュアルを参照してください。

プロファイルの作成

プロファイルを作成するには:

- 【追加(Add)】をクリックしてから、【プロファイルの追加(Add Profile)】ダイアログボックスにプロファイル名を入力します。
- ALMサーバのURLを入力または選択します。前にALMサイトを訪問したことがなければ、リストは空です。URLを入力するには、「http://<qc-server>/qcbin/」という形式を使用し

ます。URLに「start_a.htm」(またはその他のファイル名)を追加しないでください。

3. サーバにアクセス可能なユーザ名とパスワードを入力し、**認証(Authenticate)**をクリックします。

認証資格情報が受け入れられると、サーバによって**ドメイン(Domain)**リストと**プロジェクト(Project)**リストが設定されます。

4. **接続(Connect)**をクリックしてから、**欠陥報告(Defect Reporting)**グループで件名を選択します。
5. **欠陥の優先度(Defect priority)**リストから、このプロファイルを使用してALMに報告されるすべてのFortify WebInspect脆弱性に割り当てる優先度を選択します。
6. **欠陥の割り当て先(Assign defects to)**リストを使用して欠陥を割り当てるユーザを選択してから、**プロジェクトの発見場所(Project found in)**リストでエントリを選択します。
7. 残りのリストを使用して、Fortify WebInspect脆弱性評価をALM欠陥評価にマップします。**発行しない(Do Not Publish)**を選択した場合は、脆弱性がエクスポートされません。少なくとも1つのファイルマッピングを選択する必要があります。
8. Fortify WebInspect脆弱性に関連付けられたメモとスクリーンショットをエクスポートするには、**欠陥に対する脆弱性添付ファイルをアップロードする(Upload vulnerability attachments to defect)**を選択します。
9. **必須/任意フィールド(Required/Optional Fields)**グループでエントリをダブルクリックして、要求された情報を入力または選択します。必須フィールドを入力せずに作業を保存しようとすると、Fortify WebInspectが入力を要求します。

第10章: 参照リスト

この章では、Fortify WebInspectのポリシー、スキャンログのメッセージ、およびHTTPステータスコードの一覧を示します。

Fortify WebInspectのポリシー

ポリシーとは、Fortify WebInspectがWebアプリケーションに対して展開する脆弱性チェックと攻撃手法のコレクションです。各ポリシーはSmartUpdate機能によって最新の状態に保たれます。こうして、スキャンの精度が確保されて、ごく最近発見された脅威も検出できるようになります。

Fortify WebInspectには、パッケージ化された次のポリシーが含まれています。これらを使用して、Webアプリケーションの脆弱性を判断できます。

メモ: このリストは、製品に表示されるポリシーと一致しないことがあります。このドキュメントの執筆後にSmartUpdateによって追加または非推奨にされたポリシーが存在する場合があります。

ベストプラクティス

ベストプラクティスグループには、Webアプリケーションに最も広く見られる厄介なセキュリティ上の脆弱性についてアプリケーションをテストするためのポリシーが含まれています。

- API:** このポリシーには、APIセキュリティ評価に関するさまざまな問題を対象としたチェックが含まれています。これには、各種のインジェクション攻撃、トランスポート層セキュリティ、およびプライバシー侵害が含まれますが、クライアントサイドの問題の検出のチェックや攻撃露呈部分の検出(ディレクトリ列举やバックアップファイル検索のチェックなど)は含まれません。このポリシーによって検出される脆弱性はすべて、攻撃者から直接攻撃の的とされる可能性があります。このポリシーは、Web APIを使用するアプリケーションをスキャンするためのものではありません。
- CWE Top 25 <バージョン>:** Common Weakness Enumeration (CWE) Top 25 Most Dangerous Software Errors (CWE Top 25)は、MITREが作成したリストです。このリストは、ソフトウェアの脆弱性につながるおそれのある、まん延の度合いと重大性が最も高いソフトウェアの弱点を示しています。
- DISA STIG <バージョン>:** Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG)には、アプリケーションの開発過程全体に関するセキュリティガイダンスがあります。このポリシーには、DISA STIG <バージョン>の安全なコーディングの要件をアプリケーションが満たすために役立つ選定されたチェックが含まれます。ベストプラクティスグループ内には、DISA STIGポリシーの複数のバージョンが存在する場合があります。

- **General Data Protection Regulation (GDPR):** EU一般データ保護規則(GDPR、General Data Protection Regulation)は、データ保護指令95/46/ECに代わるものとして、組織が個人データを取り扱うための枠組みを提供しています。以下に挙げるGDPR条項は、アプリケーションセキュリティに関連しており、製品およびサービスの設計および開発中に個人データを保護することを企業に義務付けています。
 - 第25条「データ保護バイデザインおよびデータ保護バイデフォルト」。この条項により、企業は、各特定の処理の目的に必要な個人データのみを取り扱うことをデフォルトで保証するために、適切な技術的および組織的な手段を講じる必要があります。
 - 第32条「取り扱いの安全性」。この条項により、企業は、個人データの偶発的または不法な破壊、損失、改変、不正開示、または不正アクセスからシステムおよびアプリケーションを保護する必要があります。
- このポリシーには、特にGDPRのアプリケーションセキュリティに関連して個人データを特定および保護する上で役立つチェックが精選されています。
- **NIST-SP800-53R5:** NIST Special Publication 800-53 Revision 5 (NIST SP 800-53 Rev.5)には、米国連邦政府の機関および情報システムをセキュリティ上の脅威から保護することを目的とするセキュリティ制御およびプライバシー制御のリストが指定されています。このポリシーには、NIST SP 800-53 Rev.5のガイドラインと規格を満たすために監査に含める必要がある選定されたチェックが含まれています。
- **OWASP Application Security Verification Standard (ASVS):** Application Security Verification Standard (ASVS)は、設計者、開発者、テスト担当者、セキュリティ専門家、ツールベンダー、およびコンシューマが安全なアプリケーションを定義、作成、テスト、および検証するために使用できる、アプリケーションのセキュリティ要件またはセキュリティテストのリストです。
このポリシーは、組み込むSecureBaseチェックの各カテゴリに、OWASP ASVSが提示するCWEマッピングを使用しています。CWEは階層的な分類であるため、このポリシーには、「ParentOf」関係を使用してOWASP ASVSが提示するCWEから暗黙的に指定される追加のCWEにマップするチェックも含まれています。
- **OWASP Top 10 <年>:** このポリシーは、Webアプリケーションセキュリティの最低限の基準を提供します。OWASP Top 10は、Webアプリケーションの最も重大なセキュリティ上の欠陥についての幅広いコンセンサスを表します。OWASP Top 10の採用は、おそらく、組織内のソフトウェア開発文化を安全なコードを生み出す文化へと変化させるための最も効果的な最初のステップと言えます。OWASP Top 10のポリシーには、複数のリリースが存在する場合があります。詳細については、「[OWASP Top Ten Project](#)」を参照してください。
- **SANS Top 25 <年>:** SANS Top 25 Most Dangerous Software Errorsでは、ソフトウェアの深刻な脆弱性を引き起こす最も広く見られる重大なエラーを[CWE \(Common Weakness Enumeration\)](#) ID別に分類して列挙しています。多くの場合、これらのソフトウェアエラーは見つけるのも悪用するのも簡単です。これらのエラーにつきものの危険としては、攻撃者がソフトウェアを完全に乗っ取ったり、データを盗んだり、ソフトウェアを完全に停止させたりできることがあります。
- **標準:** 標準スキャンは、サーバの自動Web探索を含んでおり、SQLインジェクションやクロスサイトスクリプトなどの既知と未知の脆弱性のチェックの他、Webサーバ層、Webアプリケーションサーバ層、およびWebアプリケーション層での不適切なエラー処理や脆弱なSSL設定についてのチェックを実行します。

タイプ別

タイプ別 グループには、特定のアプリケーション層、脆弱性の種類、または汎用機能に焦点を絞って設計されたポリシーが含まれます。たとえば、アプリケーションポリシーには、オペレーティングシステムではなくアプリケーションをテストする目的で設計されたすべてのチェックが含まれます。

- 積極的なSQLインジェクション:** このポリシーは、SQLインジェクションの脆弱性に対するWebアプリケーションのセキュリティを総合的に評価します。SQLインジェクションとは、入力が検証されないという脆弱性を利用してWebアプリケーションから任意のSQLクエリやコマンドを渡し、バックエンドのデータベースで実行させるという攻撃手法です。このポリシーを使用すると、より正確で確実になりますが、スキャン時間は長くなります。
- Apache Struts:** このポリシーは、Apache Strutsフレームワークに対する、サポートされている既知のアドバイザリを検出します。
- ブランク:** このポリシーは、ユーザが独自のポリシーを作成するために使用できるテンプレートです。これにはサーバの自動Web探索が含まれていますが、脆弱性チェックは含まれていません。このポリシーを編集して、特定の脆弱性のみをスキャンするカスタムポリシーを作成できます。
- クライアント側:** このポリシーは、攻撃者が攻撃を仕掛けるためにフィッシングを行うことが必要となるすべての問題を検出することを目的としています。それらの問題は通常はクライアント側に現れるので、フィッシングが必要となります。これには、反射型クロスサイトスクリプティングのチェックと、さまざまなHTML5のチェックが含まれます。このポリシーをサーバ側ポリシーと組み合わせて使用することで、クライアントとサーバの両方をカバーすることができます。
- 重大および高:** 重大および高のポリシーは、運用サーバを危険にさらすことなく、差し迫った緊急の脆弱性を検出するためにWebアプリケーションを迅速にスキャンする場合に使用します。このポリシーは、SQLインジェクションやクロスサイトスクリプティングなど、重大度が「重大」および「高」の脆弱性をチェックします。これは、データベースにデータを書き込んだり、サービス拒否状態を生じさせたりする可能性があるチェックは含んでいないため、運用サーバに対して安全に実行できます。
- クロスサイトスクリプティング:** このポリシーは、XSS(クロスサイトスクリプティング)の脆弱性について、Webアプリケーションのセキュリティスキャンを実行します。XSSとは、攻撃者が提供した実行可能コード(HTMLコードやクライアント側スクリプトなど)をWebサイトにエコーさせて、ユーザのブラウザにそのコードをロードする攻撃手法です。このような攻撃を使用して、アクセス制御をバイパスしたりフィッシング攻撃を実行したりすることができます。
- DISA STIG <バージョン>:** Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG)には、アプリケーションの開発過程全体に関するセキュリティガイダンスがあります。このポリシーには、DISA STIG <バージョン>の安全なコーディングの要件をアプリケーションが満たすために役立つ選定されたチェックが含まれます。タイプ別 グループには、DISA STIGポリシーの複数のバージョンが存在する場合があります。
- モバイル:** モバイルスキャンは、モバイルアプリケーションとそれをサポートするバックエンドサービスの間で観察された通信に基づいて、セキュリティ上の欠陥を検出します。

- **NoSQLおよびNode.js:** このポリシーは、サーバの自動Web探索を含んでおり、NoSQLベースのデータベース(MongoDBなど)や、JavaScriptベースのサーバ側インフラストラクチャ(Node.jsなど)を対象にした既知と未知の脆弱性のチェックを実行します。
- **パッシブスキャン:** パッシブスキャンポリシーは、積極的なエクスプロイトを発生させなくても検出可能なアプリケーションの脆弱性をスキャンします。したがって、運用サーバに对しても安全に実行できます。このポリシーによって検出される脆弱性には、パスの開示の問題、エラーメッセージの問題、および類似した性質を持つその他の問題が含まれます。
- **PCI Software Security Framework <バージョン> (PCI SSF <バージョン>):** PCI SSFは、安全な支払いシステムと支払いトランザクション処理ソフトウェアを作成するための要件とガイダンスのベースラインを提供します。このポリシーには、PCI SSFの安全なコーディングの要件を満たすために監査に含める必要があるチェックが含まれています。
- **権限のエスカレーション:** 権限のエスカレーションのポリシーは、攻撃者がデータやアプリケーションへの昇格されたアクセス権を獲得することを許してしまうプログラミングエラーや設計上の欠陥を検出するために、Webアプリケーションをスキャンします。このポリシーは、同一の要求をさまざまな特権レベルで実行してその応答を比較するチェックを実行します。
- **サーバ側:** このポリシーには、サーバ側アプリケーションのさまざまな問題を対象とするチェックが含まれています。これには、さまざまなインジェクション攻撃、トランスポート層のセキュリティ、およびプライバシー侵害が含まれますが、ディレクトリ列举やバックアップファイルの検索などのアタックサーフェスの検出は含まれません。このポリシーによって検出される脆弱性はすべて、攻撃者から直接攻撃的とされる可能性があります。このポリシーをクライアント側ポリシーと組み合わせて使用することで、クライアントとサーバの両方をカバーすることができます。
- **SQLインジェクション:** SQLインジェクションポリシーは、SQLインジェクションの脆弱性について、Webアプリケーションのセキュリティスキャンを実行します。SQLインジェクションとは、入力が検証されないという脆弱性を利用してWebアプリケーションから任意のSQLクエリやコマンドを渡し、バックエンドのデータベースで実行させるという攻撃手法です。
- **トランスポート層セキュリティ:** このポリシーは、安全でないSSL/TLS設定や、トランスポート層の重大なセキュリティ脆弱性(Heartbleed攻撃、Poodle攻撃、SSL再ネゴシエーション攻撃など)について、Webアプリケーションのセキュリティ評価を実行します。
- **WebSocket:** このポリシーは、アプリケーション内のWebSocket実装に関する脆弱性を検出します。

カスタム

カスタムグループには、ユーザが作成したすべてのポリシーと、ユーザが変更したカスタムポリシーが含まれます。

危険

危険グループには、運用サーバの障害を引き起こす可能性があるサービス拒否攻撃などの危険をはらんだチェックを含んでいるポリシーが含まれます。このポリシーは、運用以外のサーバおよびシステムのみに使用してください。

- **全チェック:** 全チェックスキャンには、サーバの自動Web探索が含まれており、データベースであるSecureBaseのアクティブなすべてのチェックを実行します。このスキャンには、Fortifyの

WebアプリケーションとWebサービスの脆弱性のスキャンのための製品で利用可能なコンプロイアンスレポートにリストされるすべてのチェックが含まれます。これには、Webサーバ層、Webアプリケーションサーバ層、およびWebアプリケーション層での既知と未知の脆弱性のチェックが含まれます。

注意! 全チェックスキャンには、データベースにデータを書き込んだり、フォームを送信したり、サービス拒否状態を発生させたりする可能性のあるチェックが含まれています。Fortifyは、全チェックポリシーはテスト環境でのみ使用することを強くお勧めします。

非推奨になったチェックおよびポリシー

以下のポリシーとチェックは非推奨となっており、保守されていません。

- アプリケーション(非推奨):** アプリケーションポリシーは、既知および未知のWebアプリケーション攻撃を送信することで、Webアプリケーションのセキュリティスキャンを実行し、アプリケーション層を評価する特定の攻撃のみを送信します。エンタープライズレベルのWebアプリケーションのスキャンを実行する場合は、アプリケーションのみのポリシーをプラットフォームのみのポリシーと組み合わせて使用することで、スキャンの速度とメモリ使用量を最適化してください。
- 攻撃(非推奨):** 攻撃スキャンには、サーバの自動Web探索が含まれており、Webサーバ層、Webアプリケーションサーバ層、およびWebアプリケーション層で既知および未知の脆弱性のチェックを実行します。攻撃スキャンには、サービス拒否状態を引き起こす可能性があるチェックが含まれます。攻撃スキャンはテスト環境でのみ使用することを強くお勧めします。
- 非推奨のチェック:** テクノロジのライフサイクルが終わりに向かい、技術動向から姿を消していくのに従い、実質的に不要になったチェックをポリシーから削除する必要があります。非推奨のチェックポリシーには、現在の技術的状況に基づいて役目を終えたと見なされたチェックや、コアWebInspectフレームワークの最近の拡張機能を活用するスマートで効率的な監査アルゴリズムを使用して再実装されたチェックが含まれます。
- 開発者(非推奨):** 開発者スキャンには、サーバの自動Web探索が含まれており、Webアプリケーション層に限定した既知および未知の脆弱性のチェックを実行します。このポリシーは、サービス拒否状態を引き起こす可能性のあるチェックは実行しないので、運用システムで安全に実行できます。
- OpenSSL Heartbleed(非推奨):** このポリシーは、重大なTLSハートビート読み取りオーバーランの脆弱性について、Webアプリケーションのセキュリティ評価を実行します。この脆弱性により、悪意のあるユーザが、サイトをホストしているサーバに不正な形式のハートビート要求を送信した場合に、サーバメモリ内の重要なサーバおよびWebアプリケーションのデータが漏えいする可能性があります。
- OWASP Top 10 Application Security Risks - 2010(非推奨):** このポリシーは、Webアプリケーションセキュリティの最低限の基準を提供します。OWASP Top 10は、Webアプリケーションの最も重大なセキュリティ上の欠陥についての幅広いコンセンサスを表します。OWASP Top 10の採用は、おそらく、組織内のソフトウェア開発文化を安全なコードを生み出す文化へと変化させるための最も効果的な最初のステップと言えます。このポリシーには、2010 Top 10リストに固有の要素が含まれています。詳細については、「[OWASP Top Ten Project](#)」を参照してください。

- プラットフォーム(非推奨):** このポリシーは、特にWebサーバおよび既知のWebアプリケーションに対して攻撃を送信することで、Webアプリケーションプラットフォームのセキュリティスキャンを実行します。エンタープライズレベルのWebアプリケーションのスキャンを実行する場合は、プラットフォームのみのポリシーをアプリケーションのみのポリシーと組み合わせて使用することで、スキャンの速度とメモリ使用量を最適化してください。
- QA(非推奨):** このポリシーは、QA担当者がWebアプリケーションセキュリティの観点からプロジェクトリリースの決定を下すのに役立ちます。これは、Webアプリケーションの既知および未知の脆弱性のチェックを実行します。ただし、危険性をはらんだチェックは実行しないため、運用システムで安全に実行できます。
- クイック(非推奨):** このスキャンには、サーバの自動Web探索が含まれており、Webサーバ層、Webアプリケーションサーバ層、およびWebアプリケーション層で、メジャー/パッケージの既知の脆弱性と未知の脆弱性のチェックを実行します。クイックスキャンは、サービス拒否状態を生じさせる可能性のあるチェックは実行しないため、運用システムで安全に実行できます。
- セーフ(非推奨):** セーフスキャンには、サーバの自動Web探索が含まれており、Webサーバ層、Webアプリケーションサーバ層、およびWebアプリケーション層で、メジャー/パッケージの既知の脆弱性のほとんどと、未知の脆弱性のいくつかについてのチェックを実行します。セーフスキャンは、機密性の高いシステムでも、サービス拒否状態を引き起こす可能性のあるチェックは実行しません。
- 標準(非推奨):** 標準(非推奨)ポリシーは、R1 2015リリースで改訂される前のものとの標準ポリシーと同じものです。標準スキャンには、サーバの自動Web探索が含まれており、Webサーバ層、Webアプリケーションサーバ層、およびWebアプリケーション層で既知および未知の脆弱性のチェックを実行します。標準スキャンは、サービス拒否状態を生じさせる可能性のあるチェックは実行しないため、運用システムで安全に実行できます。

スキャンログのメッセージ

このトピックでは、スキャンログに表示されるメッセージについて説明します。メッセージはアルファベット順に並んでいます。

メモ: スキャンログのアラートレベルのメッセージについては、「["アラートのトラブルシューティング" ページ508](#)」を参照してください。

監査エンジン初期化のエラー

メッセージ全体

Audit Engine initialization error, engine:%engine%, error:%error% (監査エンジン初期化のエラー、エンジン:%engine%、エラー:%error%")

説明

監査エンジンの初期化中に回復不可能なエラーが発生しました。Fortifyカスタマサポートにお問い合わせください。

引数の説明

Engine: 初期化を試行したエンジン。

Error: 実際に発生したエラー。

考えられる解決策

該当なし

外部リンク

該当なし

監査エラー

メッセージ全体

Error: Auditor error, session: <session ID> engine:<engine>, error:<error> (エラー: 監査エラー、セッション: <session ID> エンジン:<engine>、エラー:<error>)

説明

監査中にエラーが発生しました。

引数の説明

Session: エラーが発生した際に監査中だったセッション。

Engine: エラーが発生した際に実行されていたエンジン。

Error: 実際に発生したエラー。

考えられる解決策

該当なし

外部リンク

該当なし

自動応答状態の失敗

メッセージ全体

Auto Response State Fail detected. (自動応答状態の失敗が検出されました。)
Please add response state rule. (応答状態ルールを追加してください。)

説明

状態の自動検出は失敗しましたが、要求でAuthorization: Bearerが識別されました。

考えられる解決策

トークンが staticトークン値である場合は、このアラートを無視します。

トークンがダイナミックである場合は、応答状態ルールを作成します。詳細については、「[スキャン設定: HTTP 解析](#) ページ390」を参照してください。

外部リンク

該当なし

チェックエラー

メッセージ全体

Error: Check error, session:8BE3AFEC5051507168B66AEC59C8915B,
Check:10346, engine: SPI.Scanners.Web.Audit.Engines.RequestModify (エラー:
チェックエラー、セッション:8BE3AFEC5051507168B66AEC59C8915B、チェック:10346、
エンジン: SPI.Scanners.Web.Audit.Engines.RequestModify)

説明

チェックの処理中にエラーが発生しました。

引数の説明

Session: チェックエラーが発生したセッション。

Check: 問題が発生したチェック。

Engine: エラーが発生した際に実行されていたエンジン。

Error: エラー。

考えられる解決策

SmartUpdateの最新バージョンをインストールします。

外部リンク

該当なし

完了したスキャン後分析モジュール

メッセージ全体

Completed Post-Scan Analysis Module: %module% (完了したスキャン後分析モ
ジュール: %module%)

説明

スキャン後分析モジュールの1つが終了しました。

引数の説明

module: スキャン後分析モジュールの名前。

考えられる解決策

該当なし

外部リンク

該当なし

Web探索と監査の同時実行の開始

メッセージ全体

Info:Concurrent Crawl and Audit Start (情報:Web探索と監査の同時実行の開始)

説明

このメッセージは、Web探索と監査の同時実行が開始したことを示しています。

引数の説明

該当なし

考えられる解決策

該当なし

外部リンク

該当なし

Web探索と監査の同時実行の停止

メッセージ全体

Info:Concurrent Crawl and Audit Stop (情報:Web探索と監査の同時実行の停止)

説明

このメッセージは、Web探索と監査の同時実行が停止したことを示しています。

引数の説明

該当なし

考えられる解決策

該当なし

外部リンク

該当なし

Web探索の同時実行の開始

メッセージ全体

Info:Concurrent Crawl Start: (情報:Web探索の同時実行の開始)

説明

このメッセージは、Web探索の同時実行が開始したことを示しています。

引数の説明

該当なし

考えられる解決策

該当なし

外部リンク

該当なし

Web探索の同時実行の停止

メッセージ全体

Info:Concurrent Crawl Stop (情報: Web探索の同時実行の停止)

説明

このメッセージは、Web探索の同時実行が停止したことを示しています。

引数の説明

該当なし

考えられる解決策

該当なし

外部リンク

該当なし

コネクティビティの問題、理由

メッセージ全体

Connectivity issue, Reason: FirstRequestFailed, HTTP Status:404, (コネクティビティの問題、理由: FirstRequestFailed、HTTPステータス:404)

説明 このメッセージは、ネットワークのコネクティビティの問題を示しています。Fortify WebInspectがリモートホストと通信できませんでした。

引数の説明

Reason: FirstRequestFailed - 要求が失敗しました。

HTTP Status: 404 - 失敗した要求に対して返されたステータス。

考えられる解決策

- ネットワークハードウェアの電源サイクル

問題が解決しない場合は、モデムとルータの電源を抜いてから数秒待ち、もう一度差し込みます。場合によっては、これらのデバイスの更新が必要なことがあります。ネットワークの障害、またはネットワーク設定が間違っていることが原因である場合があります。

- Microsoftのネットワーク診断ツールを使用する

通知エリアのネットワークアイコンを右クリックして [ネットワーク診断]を開き、[診断と修復]をクリックします。

- **ケーブルの確認**
すべてのケーブルが正しく接続されていることを確認します。
- **ホストの電源の確認**
別のコンピュータに接続しようとしている場合は、そのコンピュータの電源が入っていることを確認します。
- **接続設定の確認**
新しいソフトウェアをインストールした後に問題が発生した場合は、接続設定が変更されていないか確認してください。[スタート]ボタン、[コントロールパネル]、[ネットワークとインターネット]、[ネットワークと共有センター]、[ネットワーク接続の管理]の順にクリックして、[ネットワーク接続]を開きます。接続を右クリックして、[プロパティ]をクリックします。管理者のパスワードまたは確認を求めるプロンプトが表示された場合は、パスワードを入力するか、確認します。
- **すべてのファイアウォールのトラブルシューティング**

外部リンク

[ネットワーク接続に関する問題のトラブルシューティング](#)

[インターネットコネクティビティ評価ツール](#)

コネクティビティの問題、理由、エラー

メッセージ全体

Connectivity issue, Reason:FirstRequestFailed,
Error:Server:zero.webappsecurity.com:80, Error:(11001)Unable to connect to remote host : No such host is known: (コネクティビティの問題、理由:FirstRequestFailed、エラー:Server:zero.webappsecurity.com:80、エラー:(11001)リモートホストに接続できません: ホストが不明です:)

説明

このメッセージは、ネットワークのコネクティビティの問題を示しています。Fortify WebInspectがリモートホストと通信できませんでした。

引数の説明

Reason: FirstRequestFailed - 要求が失敗しました。

Server: 要求が送信されたサーバ。

Error: (11001)Unable to connect to remote host : No such host is known: -コネクティビティの問題が原因で、リモートホストへの通信が失敗しました。

考えられる解決策

- **ネットワークハードウェアの電源サイクル**

問題が解決しない場合は、モdemとルータの電源を抜いてから数秒待ち、もう一度差し込みます。場合によっては、これらのデバイスの更新が必要なことがあります。ネット

ワークの障害、またはネットワーク設定が間違っていることが原因である場合があります。

- Microsoftのネットワーク診断ツールを使用する

通知エリアのネットワークアイコンを右クリックして [ネットワーク診断]を開き、[診断と修復]をクリックします。

- ケーブルの確認

すべてのケーブルが正しく接続されていることを確認します。

- ホストの電源の確認

別のコンピュータに接続しようとしている場合は、そのコンピュータの電源が入っていることを確認します。

- 接続設定の確認

新しいソフトウェアをインストールした後に問題が発生した場合は、接続設定が変更されていないか確認してください。[スタート]ボタン、[ドントロールペネル]、[ネットワークとインターネット]、[ネットワークと共有センター]、[ネットワーク接続の管理]の順にクリックして、[ネットワーク接続]を開きます。接続を右クリックして、[プロパティ]をクリックします。管理者のパスワードまたは確認を求めるプロンプトが表示された場合は、パスワードを入力するか、確認します。

- すべてのファイアウォールのトラブルシューティング

外部リンク

[ネットワーク接続に関する問題のトラブルシューティング](#)

[インターネットコネクティビティ評価ツール](#)

Web探索プログラムエラー

メッセージ全体

Error: Crawler error, session: <session ID> error:<error>(エラー: Web探索プログラムエラー、セッション: <session ID> エラー:<error>)

説明

Web探索プログラムがセッションの処理に失敗しました。ユーザは修正できません。Fortifyカスタマサポートにお問い合わせください。

引数の説明

Session: エラーが発生したセッション。

Error: 実際のエラー。

考えられる解決策

該当なし

外部リンク

該当なし

データベースコネクティビティの問題

メッセージ全体

Error: SPI.Scanners.Web.Framework.Session in updateExisting,retries failed, giving up calling IDbConnnetivityHandler.OnConnectivityIssueDetected (エラー: updateExistingのSPI.Scanners.Web.Framework.Session、再試行が失敗しました。iDbConnnetivityHandler.OnConnectivityIssueDetectedの呼び出しをキャンセルします)

説明

このメッセージは、データベースが応答を停止したことを示しています。

引数の説明

Errorテキスト: メッセージをトリガしたエラーの説明が含まれます。

考えられる解決策

データベースサーバが実行中で、応答していることを確認します。

外部リンク

該当なし

エンジン駆動型監査の開始

メッセージ全体

Info:Engine Driven Audit Start (情報:エンジン駆動型監査の開始)

説明

このメッセージは、エンジン駆動型監査が開始したことを示しています。

引数の説明

該当なし

考えられる解決策

該当なし

外部リンク

該当なし

エンジン駆動型監査の停止

メッセージ全体

Info:Engine Driven Audit Stop (情報:エンジン駆動型監査の停止)

説明

このメッセージは、エンジン駆動型監査が停止したことを示しています。

引数の説明

該当なし

考えられる解決策

該当なし

外部リンク

該当なし

エンジン駆動型エンジンの起動

メッセージ全体

Info: Engine Driven Engine Start, Engine: LFI Agent (情報: エンジン駆動型エンジンの起動、エンジン: LFIエージェント)

説明

このメッセージは、示されているエンジンが実行を開始したことを示しています。

引数の説明

Engine: 起動中のエンジン。

考えられる解決策

該当なし

外部リンク

該当なし

エンジン駆動型エンジンの停止

メッセージ全体

Info: Engine Driven Engine Stop, Engine: LFI Agent Sessions Processed:406 (情報: エンジン駆動型エンジンの停止、エンジン: LFI Agent、処理済みセッション:406)

説明

指定されたエンジンに対するエンジン駆動型監査が完了しました。

引数の説明

Engine: 停止されたエンジン。

Sessions processed: エンジンによって処理されたセッションの数。

考えられる解決策

該当なし

外部リンク

該当なし

外部の相関関係が有効

メッセージ全体

External Correlation Enabled, Origin:<product_name> OriginID:<numeric_value> OriginDateTime:<date_time> File:<filename>.json (外部の相関関係が有効、オリジン:<product_name> OriginID:<numeric_value> OriginDateTime:<date_time> ファイル:<filename>.json モード:CompatibleTypesOnly)

説明

外部の相関関係がスキャンに対して自動的に有効になっています。

引数の説明

Origin: Fortify_SASTなど、相関関係のある外部製品。

OriginID: 検出事項を含む外部スキャンのID。

OriginDateTime: 外部スキャンがいつ作成されたか。

File: 外部の検出事項を含むJSONファイル。

考えられる解決策

該当なし

外部リンク

該当なし

外部の検出事項

メッセージ全体

External Finding, Origin:<product_name> OriginID:<numeric_value> OriginDateTime:<date_time> OriginFindingID:<guid> FindingType:<type> (外部の検出事項、オリジン:<product_name> OriginID:<numeric_value> OriginDateTime:<date_time> OriginFindingID:<guid> FindingType:<type>)

説明

外部スキャンでの検出事項に関する情報を提供します。

引数の説明

Origin: Fortify_SASTなど、相関関係のある外部製品。

OriginID: 検出事項を含む外部スキャンのID。

OriginDateTime: 外部スキャンがいつ作成されたか。

OriginFindingID: 外部スキャンファイル内の検出事項の固有のID。

FindingType: 外部スキャンファイル内の検出事項の種類(XSSなど)。

考えられる解決策

該当なし

外部リンク

該当なし

相関関係のある検出事項

メッセージ全体

Finding Correlated, Check:<check_id><check_name> Param:<parameter_name> Request:<http_method><resource_url> (相関関係のある検出事項、チェック:<check_id><check_name> パラメータ:<parameter_name> 要求:<http_method><resource_url>)

説明

この検出事項は、外部スキャンの検出事項と相関関係があります。

引数の説明

Check: SecureBaseからのチェックIDとチェック名。

Param: 攻撃で使用されたパラメータ名。

Request: HTTP要求メソッド(POST、PUT、GETなど)と攻撃されたリソースのURL。

考えられる解決策

該当なし

外部リンク

該当なし

ライセンスの問題

メッセージ全体

Error: License issue: License Deactivated (エラー: ライセンスの問題: ライセンスが無効です)

説明

ライセンスで問題が発生しました。

引数の説明

Issue: 発生した問題。

考えられる解決策

Fortify WebInspectが適切にライセンスされていることを確認します。

外部リンク

該当なし

ログメッセージの発生

メッセージ全体:

<Level>: <ScanID> , <Logger>: <Exception>

説明:

例外に関する一般的なメッセージ

引数の説明

ScanID: スキャンID。

Logger: ロガーの名前。

Exception: スローされた例外。

考えられる解決策

該当なし

外部リンク

該当なし

メモリ制限に到達

メッセージ全体

警告: メモリ制限に到達しました: レベル:1、制限:1073610752、割り当て済み:1076625408。

エラー: メモリ制限に到達しました: レベル:0、制限:1073610752、割り当て済み:1076625408。

説明

WIプロセスのメモリ制限に到達しました。

引数の説明

Level: 問題の重大度。

Limit: プロセスのメモリ制限。

Actual: プロセスに実際に割り当てられたメモリ。

考えられる解決策

実行されていない他のスキャンを終了します。

1つのFortify WebInspectインスタンスでは、一度に1つのスキャンだけを実行してください。

外部リンク

該当なし

脆弱性のセッションが見つからない

メッセージ全体

Info: Missing Session for Vulnerability (情報: 脆弱性のセッションが見つかりません)

説明

脆弱性に関連付けられているセッションが見つかりません。

引数の説明

該当なし

考えられる解決策

該当なし

外部リンク

該当なし

新しいブラインドSQLチェックが有効になっていない

メッセージ全体

New Blind SQL check (checkid newcheckid%) is not enabled. (新しいブラインドSQLチェック(checkid newcheckid%)が有効になっていません。) A policy with both check %newcheckid% and check %oldcheckid% enabled is recommended. (チェック%newcheckid%とチェック%oldcheckid%が有効なポリシーを推奨します。)

説明

ブラインドSQLインジェクションの新しいチェックが、スキャンポリシーに含まれていません。

引数の説明

newcheckid: 新しいSQLインジェクションチェックの識別子(10962)

oldcheckid: 古いSQLインジェクションチェックの識別子(5659)

考えられる解決策

新しいチェック(10962)を、スキャンポリシーに追加します。

外部リンク

該当なし

永続的クロスサイトスクリピティング監査の開始

メッセージ全体

Info: Persistent Cross-Site Scripting Audit Start (情報: 永続的クロスサイトスクリピティング監査の開始)

説明

永続的クロスサイトスクリピティング監査が開始しました。

引数の説明

該当なし

考えられる解決策

該当なし

外部リンク

該当なし

永続的クロスサイトスクリピティング監査の停止

メッセージ全体

Info:Persistent Cross-Site Scripting Audit Stop (情報:永続的クロスサイトスクリピティング監査の停止)

説明

永続的クロスサイトスクリピティング監査が停止しました。

引数の説明

該当なし

考えられる解決策

該当なし

外部リンク

該当なし

スキャン後分析の開始

メッセージ全体

Post-Scan Analysis started. (スキャン後分析が開始しました。)

説明

スキャン後分析が開始しました。使用されているモジュールごとに追加のメッセージが表示されます(認証、マクロ、ファイルが見つからない、など)。

引数の説明

該当なし

考えられる解決策

該当なし

外部リンク

該当なし

スキャン後分析の完了

メッセージ全体

Post-Scan Analysis completed. (スキャン後分析が完了しました。)

説明

スキャン後分析が終了しました。使用されているモジュールごとに追加のメッセージが表示されます(認証、マクロ、ファイルが見つからない、など)。

引数の説明

該当なし

考えられる解決策

該当なし

外部リンク

該当なし

監査反映の開始

メッセージ全体

Info:Reflect Audit Start (情報:監査反映の開始)

説明

反映フェーズが開始しました。

引数の説明

該当なし

考えられる解決策

該当なし

外部リンク

該当なし

監査反映の停止

メッセージ全体

Info:Reflect Audit Stop (情報:監査反映の停止)

説明

反映フェーズが完了しました。

引数の説明

該当なし

考えられる解決策

該当なし

外部リンク

該当なし

応答状態ルールの失敗

メッセージ全体

Response State Rules Fail detected for %count% rule(s). (%count%ルールに対して、応答状態ルールの失敗が検出されました。) Name of rule(s): %ruleslist%. (ルールの名前: %ruleslist%.)

説明

応答状態ルールは設定されていますが、スキャン中にトリガされませんでした。

引数の説明

count: 失敗したルールの数

ruleslist: 失敗したルールの名前

考えられる解決策

ルール内の正規表現を修正するか、ルールを削除します。詳細については、「["スキャン設定: HTTP解析" ページ390](#)」を参照してください。

外部リンク

該当なし

スキャン完了

メッセージ全体

Info:Scan Complete, ScanID:<id-number> (情報:スキャン完了、ScanID:<id-number>)

説明

このメッセージは、スキャンが正常に完了したことを示しています。

引数の説明

ScanID: スキャンの固有のID

考えられる解決策

該当なし

外部リンク

該当なし

スキャン失敗

メッセージ全体

Info:Scan Failed, ScanID::<id-number> (情報:スキャンが失敗しました、ScanID::<id-number>)

説明

このメッセージは、スキャンが失敗したことを示しています。

引数の説明

ScanID: スキャンの固有のID

考えられる解決策

スキャンが失敗した理由によって異なります(別のメッセージによって示されます)。

外部リンク

該当なし

スキャン開始

メッセージ全体

Info:Scan Start, ScanID:<id-number> Version:X.X.X.X, Location:C:\Program Files\Fortify\Fortify WebInspect\WebInspect.exe (情報:スキャン開始、ScanID:<id-number> バージョン:X.X.X.X、場所:C:\Program Files\Fortify\Fortify WebInspect\WebInspect.exe)

説明

このメッセージは、スキャンの開始を示しています。

引数の説明

ScanID: スキャンの固有のID。

Version: スキャンを実行しているFortify WebInspectのバージョン。

Location: Fortify WebInspect実行可能なファイルの物理的な場所です。

考えられる解決策

該当なし

外部リンク

該当なし

スキャン開始エラー

メッセージ全体

Scan start error: %error% (スキャン開始エラー: %error%)

説明

スキャンの開始中に回復不可能なエラーが発生しました。Fortifyカスタマサポートにお問い合わせください。

引数の説明

error: 問題の説明。

考えられる解決策

該当なし

外部リンク

該当なし

スキャン停止

メッセージ全体

Info:Scan Stop, ScanID:<id-number> (情報:スキャン停止、ScanID:<id-number>)

説明

このメッセージは、スキャンが停止されたことを示しています。

引数の説明

ScanID: スキャンの固有のID。

考えられる解決策

該当なし

外部リンク

該当なし

スキャナ再試行の開始

メッセージ全体

Info:Scanner Retry Start (情報:スキャナ再試行の開始)

説明

再試行フェーズが開始しました。

引数の説明

該当なし

考えられる解決策

該当なし

外部リンク

該当なし

スキャナ再試行の停止

メッセージ全体

Info:Scanner Retry Stop (情報:スキャナ再試行の停止)

説明

再試行フェーズが停止しました。

引数の説明

該当なし

考えられる解決策

該当なし

外部リンク

該当なし

順次監査の開始

メッセージ全体

Info:Sequential Audit Start (情報:順次監査の開始)

説明

このメッセージは、順次監査が開始したことを示しています。

引数の説明

該当なし

考えられる解決策

該当なし

外部リンク

該当なし

順次監査の停止

メッセージ全体

Info:Sequential Audit Stop (情報:順次監査の停止)

説明

このメッセージは、順次監査が停止したことを示しています。

引数の説明

該当なし

考えられる解決策

該当なし

外部リンク

該当なし

順次Web探索の開始

メッセージ全体

Info:Sequential Crawl Start (情報:順次Web探索の開始)

説明

このメッセージは、順次Web探索が開始したことを示しています。

引数の説明

該当なし

考えられる解決策

該当なし

外部リンク

該当なし

順次Web探索の停止

メッセージ全体

Info:Sequential Crawl Stop (情報:順次Web探索の停止)

説明

このメッセージは、順次Web探索が停止したことを示しています。

引数の説明

該当なし

考えられる解決策

該当なし

外部リンク

該当なし

設定の上書き

メッセージ全体

Settings Override, Setting:<setting>, Original Value:<original>, New Value:<newValue>, Reason:<reason> (設定の上書き、設定:<setting>、元の値:<original>、新しい値:<newValue>、理由:<reason>)

説明

設定が製品によって変更されました。これは、設定のアップグレードの問題を示している可能性があります。

引数の説明

Setting: 上書きされる設定。

Original Value: 設定の元の値。

New Value: 設定の変更後の値。

Reason: 上書きの理由。

考えられる解決策

工場出荷時のデフォルト値を復元して、カスタム設定値を再適用します。

外部リンク

該当なし

SPAフレームワークの検出

メッセージ全体

The crawl identified the following Single Page Application frameworks: %frameworks%. (Web探索で、次のシングルページアプリケーションフレームワークが特定されました。%frameworks%.) SPA support enabled. (SPAサポートが有効になっています。)

説明

Web探索プログラムにより1つ以上のSPA (シングルページアプリケーション)フレームワークが検出され、スキャンに対してSPAサポートが有効化されました。

引数の説明

frameworks: 検出されたフレームワークのリスト。

考えられる解決策

該当なし

外部リンク

該当なし

起動URLのエラー

メッセージ全体

Start Url Error:%url%, error:%error% (起動 Urlのエラー:%url%、エラー:%error%)

説明

起動URLの処理中に回復不可能なエラーが発生しました。URL構文を確認し、間違いなかった場合は、Fortifyカスタマサポートにお問い合わせください。

引数の説明

url: エラーの原因となったURL。

error: エラーの説明。

考えられる解決策

該当なし

外部リンク

該当なし

開始URLの拒否

メッセージ全体

Start Url Rejected:%url%, reason:%reasons%, session:%session% (開始 Urlが拒否されました:%url%、理由:%reasons%、セッション:%session%)

説明

要求拒否設定によりURLが拒否されました。設定を変更するか、別の開始URLを使用する必要があります。

引数の説明

url: 開始 URL

reason: 拒否の理由。

session: エラーが発生したセッション。

考えられる解決策

該当なし

外部リンク

該当なし

スキャン後 分析 モジュールの開始

メッセージ全体

Starting Post-Scan Analysis Module: %module% (スキャン後 分析 モジュールを開始しています: %module%)

説明

スキャン後 分析 モジュールの1つが開始しました。

引数の説明

module: スキャン後 分析 モジュールの名前。

考えられる解決策

該当なし

外部リンク

該当なし

停止の要求

メッセージ全体

Info:Stop Requested, reason=Pause button pushed (情報:停止が要求されました、理由=一時停止ボタンが押されました)

説明

スキャンが一時停止状態になります。

引数の説明

Reason: 停止の理由。

考えられる解決策

該当なし

外部リンク

該当なし

監査検証の開始

メッセージ全体

Info:Verify Audit Start (情報:監査検証の開始)

説明

検証フェーズが開始しました。

引数の説明

該当なし

考えられる解決策

該当なし

外部リンク

該当なし

監査検証の停止

メッセージ全体

Info: Verify Audit Stop (情報: 監査検証の停止)

説明

検証フェーズが完了しました。

引数の説明

該当なし

考えられる解決策

該当なし

外部リンク

該当なし

Webマクロエラー

メッセージ全体

Error: Web Macro Error, Name: Login webmacro Error: RequestAborted (エラー: Webマクロエラー、名前: Login webmacro エラー: RequestAborted)

説明

Webマクロの再生中にエラーが発生しました。

引数の説明

Name: エラーが発生した際に再生されていたマクロの名前。

Error: 発生したエラー。

考えられる解決策

検出されたエラーによって異なります。RequestAbortedエラーの場合、マクロ再生中はサーバは応答しません。この問題が頻繁に発生する場合は、[要求タイムアウト (Request timeout)]の値を大きくする必要があります。その他の解決策については、コネクティビティに関する問題を参照してください。

外部リンク

該当なし

Webマクロステータス

メッセージ全体

Error: Web Macro Status, Name: login.webmacro Expected:302, Actual:200, Url:<URL> (エラー: Webマクロステータス、名前: login.webmacro 想定:302、実際:200、Url:<URL>)

説明

Fortify WebInspectは、マクロの再生中に、マクロを記録した際に取得した応答と一致しない応答を受信しました。

引数の説明

Name: Webマクロの名前。

Expected: 返されることが想定されたステータスコード。

Actual: 実際に返されたステータスコード。

URL: 要求のターゲットURL。

考えられる解決策

これは、Fortify WebInspectがすでにログインしている状態でログインを試行したか、Fortify WebInspectがログインに失敗したことを示している可能性があります。スキャン中にFortify WebInspectがログインに成功したかどうかを確認してください。そうでない場合は、ログインマクロを再度記録します。

外部リンク

該当なし

HTTPステータスコード

次のステータスコードのリストは、Hypertext Transfer Protocolバージョン1.1規格(RFC 2616)からの引用です。詳細については、<http://www.w3.org/Protocols/>を参照してください。

| コード | 定義 |
|--------|------------|
| 100 | 続行 |
| 101 | プロトコルの切り替え |
| 200 OK | 要求が成功しました |

| コード | 定義 |
|-----------------------------------|---|
| 201 Created | 要求が完了し、新しいリソースが作成されました |
| 202 Accepted | 要求が処理のために受理されました。処理は完了していません。 |
| 203 Non-Authoritative Information | エンティティヘッダに返されるメタ情報は、元のサーバから取得可能な確定的なセットではなく、ローカルまたはサードパーティのコピーから収集されたものです。 |
| 204 No Content | サーバは要求を完了しましたが、エンティティ本体を返す必要はなく、更新されたメタ情報を返すことができます。 |
| 205 Reset Content | サーバが要求を完了しました。ユーザエージェントは、要求の送信の原因となったドキュメントビューをリセットする必要があります。 |
| 206 Partial Content | サーバがリソースに対する部分的なGET要求を完了しました。 |
| 300 Multiple Choices | 要求されたリソースは一連の表現のいずれか1つに対応し、それらはそれぞれ独自の場所を持ちます。エージェント駆動型のネゴシエーション情報(セクション12)が提供されるので、ユーザ(またはユーザエージェント)は希望の表現を選択し、その要求を該当する場所にリダイレクトできます。 |
| 301 Moved Permanently | 要求されたリソースに新しい永続URIが割り当てされました。今後、このリソースを参照するときには、返されたURIのいずれかを使用する必要があります。 |
| 302 Found | 要求されたリソースは、一時的に別のURIに存在します。 |
| 303 See Other | 要求に対する応答は別のURIにあり、そのリソースに対するGETメソッドを使用して取得する必要があります。 |
| 304 Not Modified | クライアントが条件付きGET要求を実行して、アクセスは許可されたものの文書が未変更だった場合、サーバはこのステータスコードで応答します。 |
| 305 Use Proxy | 要求されたリソースへのアクセスは、Locationフィールドで指定されたプロキシを介して行う必要があります。 |
| 306 Unused | 未使用。 |
| 307 Temporary Redirect | 要求されたリソースは、一時的に別のURIに存在します。 |

| コード | 定義 |
|-----------------------------------|--|
| 400 Bad Request | 構文の形式が正しくないため、サーバはこの要求を理解できませんでした。 |
| 401 Unauthorized | この要求にはユーザ認証が必要です。応答には、要求されたリソースに適用可能なチャレンジを含むWWW-Authenticateヘッダフィールド(セクション14.47)が含まれている必要があります。 |
| 402 Payment Required | このコードは将来の使用のために予約されています。 |
| 403 Forbidden | サーバは要求を理解しましたが、要求の実行を拒否しています。 |
| 404 Not Found | サーバはRequest-URIに一致する内容を検出できませんでした。 |
| 405 Method Not Allowed | Request-URIで示されたリソースでは、Request-Lineに指定されたメソッドが許可されていません。 |
| 406 Not Acceptable | 要求で指定されたリソースで生成可能なのは、要求で送信されたAcceptヘッダによれば受け入れ不能なコンテンツ特性を持つ応答エンティティだけです。 |
| 407 Proxy Authentication Required | このコードは401 (Unauthorized)と似ていますが、クライアントが最初にプロキシに対して自身を認証する必要があることを示しています。 |
| 408 Request Timeout | サーバの待機時間内に、クライアントが要求を生成しませんでした。 |
| 409 Conflict | リソースの現在の状態との競合のため、要求を完了できませんでした。 |
| 410 Gone | 要求されたリソースはすでにサーバ上になく、転送アドレスも不明です。 |
| 411 Length Required | サーバは、定義されたContent-Lengthがない要求の受け入れを拒否します。 |
| 412 Precondition Failed | 1つ以上のrequest-headerフィールドに指定された事前条件が、サーバ上でテストされた際にfalseと評価されました。 |
| 413 Request Entity Too Large | 要求エンティティの大きさがサーバの処理能力を超えていたため、サーバは要求の処理を拒否しています。 |
| 414 Request-URI Too Long | Request-URIが長すぎてサーバが解釈できないため、サーバは要求の処理を拒否しています。 |

| コード | 定義 |
|-------------------------------------|--|
| 415 Unsupported Media Type | 要求のエンティティの形式が、要求されたメソッドの要求されたリソースでサポートされていないため、サーバは要求の処理を拒否しています。 |
| 416 Requested Range Not Satisfiable | 要求にRange request-headerフィールド(セクション14.35)が含まれているものの、このフィールド内のrange-specifier値がどれも選択されたリソースの現在の範囲と重ならず、かつ要求にIf-Range request-headerフィールドが含まれていない場合、サーバはこのステータスコードを含む応答を返します。 |
| 417 Expectation Failed | このサーバは、Expect request-headerフィールド(セクション14.20を参照)に指定された条件を満たすことができません。または、サーバがプロキシである場合、このサーバはネクストホップサーバでは要求が満たせないという明白な証拠を持っています。 |
| 500 Internal Server Error | サーバが予期しない条件を検出したため、要求を完了できませんでした。 |
| 501 Not Implemented | サーバは、要求を実行するために必要な機能をサポートしていません。これは、サーバが要求メソッドを認識せず、どのリソースについてもこれをサポートできない場合の妥当な応答です。 |
| 502 Bad Gateway | サーバがゲートウェイまたはプロキシとして機能しているときに、要求を完了しようとしてアクセスした上流サーバから無効な応答を受け取りました。 |
| 503 Service Unavailable | サーバの一時的な過負荷または保守のため、サーバは現在要求を処理できません。 |
| 504 Gateway Timeout | サーバがゲートウェイまたはプロキシとして機能しているとき、要求を完了するためにはURIで指定された上流サーバ(HTTP、FTP、LDAPなど)かその他の補助サーバ(DNSなど)にアクセスする必要がありました。所定の時間内にそこから応答を受け取れませんでした。 |
| 505 HTTP Version Not Supported | サーバは、要求メッセージで使用されたHTTPプロトコルバージョンをサポートしていないか、サポートを拒否しています。 |

第11章:トラブルシューティング

この章には、トラブルシューティングの表、ログインマクロのテストに関する情報、およびFortify WebInspectのアンインストールオプションの説明が記載されています。

WebInspectのトラブルシューティング

以降の段落では、Fortify WebInspectおよびWebInspectツールのトラブルシューティング情報について説明します。

コネクティビティに関する問題

次の表に、コネクティビティに関する問題の説明を示します。

| 症状またはエラーメッセージ | 考えられる原因 | 考えられる解決方法 |
|---|--|---|
| HTTPではなくHTTPSを使用するサイトのテスト中に、マクロレコードまたはガイド付きスキャンウィザードを使用するとき、サイトへのコネクティビティがありません。 | Fortify WebInspectを実行しているユーザーに、Windows MachineKeysフォルダに対する必要なアクセス許可がありません。 | 許可の変更を、C:\ProgramData\Microsoft\Crypto\RSA\MachineKeysに関して行います。 フォルダのプロパティの[セキュリティ]タブで、[詳細設定]ボタンを使用して、[このフォルダー、サブフォルダーおよびファイル]に関してユーザーにフルコントロールを許可するようにアクセス許可を設定します。 |
| [OpenSSLエンジンを使用する(Use OpenSSL Engine)]アプリケーション設定が選択されており、ガイド付きスキャンブラウザ、Profilerの結果、またはスキャンログに次のテキストを含むエラーが表示されます。 | OpenSSLの不具合が原因で、ターゲットWebアプリケーションでコネクティビティの問題が発生しました。 | ターゲットWebアプリケーションへの接続に使用する証明書が、エクスポート可能としてマークされていることを確認します。詳細については、Windowsのマニュアルを参照してください。 |

| 症状またはエラーメッセージ | 考えられる原因 | 考えられる解決方法 |
|---|---------|-----------|
| 「このクライアント証明書キーを証明書ストレージへエクスポートできるようにしてください。(Make this client Certificate key exportable in Certificate storage.)」 | | |

スキャン初期化の失敗

次の表に、スキャン初期化に関する問題の説明を示します。

| 症状またはエラーメッセージ | 考えられる原因 | 考えられる解決方法 |
|--|--|---|
| SQL Expressをスキャンデータベースとして使用しているときに、スキャンの初期化が失敗します。 | SQL Expressサービスが実行されていません。 | サービスが実行されていることを確認します。このサービスの名前は「SQL Server (SQLEXPRESS)」などです。 |
| | SQL Expressキャッシュが破損している可能性があります。 | <p>キャッシュをクリアするには:</p> <ol style="list-style-type: none"> すべてのSQL関連のサービスとプロセスを停止します。 SQL Expressキャッシュフォルダを削除します。 <p>通常は次のような場所にあります。</p> <pre>C:\Users\<username>\AppData\Local\Microsoft\Microsoft SQL Server Data\SQLEXPRESS</pre> <ol style="list-style-type: none"> マシンを再起動します。 |
| SPI.Parsers.Scriptのロードに関連するエラーが原因でスキャン初期化が失敗します | Windowsで、Visual Studio 2015、2017、または2019用の | 続行する前に、C++再頒布可能パッケージを手動でインストールします。 |

| 症状またはエラーメッセージ | 考えられる原因 | 考えられる解決方法 |
|---------------|--|-----------|
| す。 | Microsoft Visual C++再頒布可能パッケージを適用できなかった可能性があります。 | |

スキャン設定の問題

次の表に、スキャンの設定中に発生する可能性がある問題の説明を示します。

| 症状またはエラーメッセージ | 考えられる原因 | 考えられる解決方法 |
|--|--|------------------------------------|
| ガイド付きスキャンで、欠落している.dllファイルに関するtruchlientbrowser.exeシステムエラーが発生します。 | Windowsで、Visual Studio 2015、2017、または2019用のMicrosoft Visual C++再頒布可能パッケージを適用できなかった可能性があります。 | 続行する前に、C++再頒布可能パッケージを手動でインストールします。 |

アラートのトラブルシューティング

アラートは、必ずしもスキャン品質の問題が発生していることを示しているわけではありません。一部のアラートは誤検出の可能性があります。ただし、アラートから、スキャンに悪影響を及ぼす可能性がある問題を把握できる可能性があります。

重要! アラート機能はテクノロジプレビューとして提供されています。

テクノロジプレビュー

テクノロジプレビュー機能は現在サポートされていないため、完全に機能しない可能性があります。また、運用環境での展開には適しません。ただし、これらの機能は、将来的には完全なサポートを提供できることを目指すために広く拡大することを主な目的として、便宜的に提供されています。

アラートの無効化

アラート機能には、サンプル間隔およびアクティブ間隔が含まれます。サンプル間隔アラートは、最大で1分に1回の頻度でスキャンログに記録されます。サンプル間隔アラートはスキャンの機能的な問題を示していない可能性がありますが、受信するアラートの数が問題になる

場合は、Fortifyカスタマサポートに連絡して、個々のアラートまたはアラート機能の無効化の支援を依頼してください。詳細については、「[序文](#)」を参照してください。

アラートのトラブルシューティングの表

重要!スキャン設定を変更する解決策はすべて、将来のスキャンを対象として実行される必要があります。現在のスキャンのスキャン設定を変更することはできません。

次の表に、アラートの考えられる原因と解決方法の説明を示します。

| アラート | 考えられる原因 | 考えられる解決方法 |
|------------------|--|--|
| 過剰なログインが検出されます | ログインマクロの再生回数が、実行された要求の数に対して多すぎます。ログイン資格情報が正しくないか、またはログアウト署名が無効である可能性があります。 | 次のいずれかを実行します。 <ul style="list-style-type: none">マクロのトラブルシューティング手順を実行します。新しいログインマクロを記録します。 詳細については、『 <i>Micro Focus Fortify WebInspect Tools Guide</i> 』を参照してください。 |
| 冗長なコンテンツが検出されました | 冗長なコンテンツが検出されました。 | 冗長ページ検出を有効にすることで、パフォーマンスを向上できる可能性があります。詳細については、「 "スキャン設定:全般" ページ374 」を参照してください。 |
| 応答時間が長すぎます | Webサーバからの応答に、平均よりも長い時間がかかっています。応答時間が長くなると、スキャンにかかる時間が長くなる可能性があります。 | ネットワークのコネクティビティ、またはAUT(テスト中のアプリケーション)のパフォーマンスを確認します。 |
| WAFが検出されました | WAF(Webアプリケーションファイアウォール)署名が検出されました。 | AUTを保護しているWAFを無効にします。 |

ログインマクロのテスト

Fortify WebInspectは、次の場合にログインマクロに対してテストを実行します。

- 自動生成されたマクロ、新しく記録されたマクロ、または既存のマクロがスキャン設定中にテストされる場合
- ログインマクロのスキャン開始時([スキャン設定:認証(Scan Settings: Authentication)]で「マクロ検証を有効にする(Enable macro validation)」が選択されている場合)

実行される検証テスト

次の表で、Fortify WebInspectが実行するテストについて説明しています。

| テスト | 失敗した場合の結果 |
|------------------------------------|--------------------------------|
| 検証ステップが欠落しているかどうかを判断する。 | スキャンは続行しますが、警告がスキャンログに書き込まれます。 |
| 自動生成されたマクロがアプリケーションにログインすることを検証する。 | スキャンは停止し、エラーがスキャンログに書き込まれます。 |
| マクロの再生でアプリケーションにログインすることを検証する。 | スキャンは停止し、エラーがスキャンログに書き込まれます。 |

テストに失敗した後にスキャンが停止した場合、スキャンログで特定のエラーメッセージを調べて、問題を特定して解決できることがあります。エラーメッセージとこのトピックのトラブルシューティングのヒントを使用すると、問題の解決に役立ちます。

トラブルシューティングのヒント

マクロが失敗した場合はいつも、無効なマクロが記録されている可能性があります。ただし、以前は良好だったマクロが失敗した場合は、たいていサイトの変更または資格情報が原因です。

次の表に、各エラーメッセージの考えられる原因と解決方法を示します。

メモ: この表には、各エラーメッセージのすべての考えられる原因と解決方法が含まれているわけではありません。追加のトラブルシューティングが必要となることがあります。

| エラーメッセージ | 考えられる原因 | 考えられる解決方法 |
|---|--------------------------------------|--|
| 自動ログインの生成に失敗しました(Automatic login generation failed) | 指定されたユーザ資格情報が無効であるために、ログインマクロを作成できませ | 有効であると判明している資格情報を使用して、ログインマクロの自動生成(Auto- |

| エラーメッセージ | 考えられる原因 | 考えられる解決方法 |
|---|--|---|
| | んでした。 | gen Login Macro)]オプションを再試行してください。 |
| 実行に失敗しました (Execution Failed) | 検証要素、ユーザ名、パスワードなどのHTML要素が見つかりませんでした。 | ログイン入力要素を識別するため、Web Macro Recorderで新しいマクロを記録します。 |
| | ユーザ名が無効になっている(データベースから削除された)か、パスワードが変更されています。 | 有効であると判明している資格情報を使用して、Web Macro Recorderで新しいマクロを記録します。 |
| ログイン検証ステップが見つかりません(Logged in verification step not found) | ログインマクロに検証ステップが含まれていません。 | Web Macro Recorderでマクロを編集して、ログインが成功したかどうかを示す検証ステップを追加します。 |
| 無効なログイン後に検証ステップが失敗しませんでした (Verification step did not fail after invalid login) | 無効なログイン試行の後に検証ステップが成功しました。有効な検証ステップは、ログインが成功した場合にのみ成功します。これは、誤ったログイン検証オブジェクトが選択されたことを示しています。 | Web Macro Recorderでマクロを編集して、検証ステップに別のオブジェクトを選択します。 |

Web Macro Recorderの使用法の詳細については、『*Micro Focus Fortify WebInspect Tools Guide*』を参照してください。

Fortify WebInspectのアンインストール

アンインストール時に、Fortify WebInspectの修復またはコンピュータからの削除を選択できます。

削除のオプション

削除(Remove)]を選択する場合は、次のオプションの1つまたは両方を選択できます。

- 製品を完全に削除(Remove product completely) - WebInspectアプリケーションとすべての関連ファイル(ローカル(非共有)SQLサーバに保存されているスキャンデータ、設定ファイル、およびログなど)を削除します。

- ライセンスの無効化(Deactivate license) - Fortify WebInspectライセンスを解放します。これにより、別のコンピュータにFortify WebInspectをインストールできるようになります。アプリケーションデータとファイルは削除されません。

マニュアルのフィードバックの送信

このマニュアルに関するご意見をお待ちしています。電子メールで**弊社ドキュメントチーム**にお送りください。

メモ: 弊社 製品に関する技術的な問題が発生した場合は、ドキュメントチームに電子メールを送信するのではなく、Micro Focus Fortifyカスタマサポート (<https://www.microfocus.com/support>)にお問い合わせください。

このコンピュータに電子メールクライアントが設定されている場合は、ドキュメントチームに連絡するために上記のリンクをクリックすると、件名の欄に次の情報が記載された電子メールウインドウが開きます。

ユーザガイド (Fortify WebInspect 21.2.0)に関するフィードバック

その電子メールにフィードバックを記載して、[送信(send)]をクリックしてください。

電子メールクライアントが使用できない場合は、上記の情報をWebメールクライアントの新しいメッセージにコピーして、フィードバックをfortifydocteam@microfocus.comにお送りください。

ご意見をお寄せください。