CyberRes

Article

Fortify's Latest and Greatest

New Features of Fortify 21.2 Release

Fortify 21.2: Build Software Resilience Seamlessly

General Availability—Fortify 21.2.0 Release

At Fortify, our goal is to assist organizations in building software resilience for modern development from a partner they can trust. Fortify continues to cover a wide range of AppSec use cases common to today's landscape. From DevSecOps, Cloud Transformation, Securing the Software Supply Chain, and Maturity at Scale, Fortify delivers a holistic, inclusive and extensible platform that supports the breadth of your software portfolio.

We are excited to announce the general availability of our CyberRes Fortify 21.2.0 release! With enhanced offerings to increase speed, accuracy, scalability, and ease of use, this marks an important chapter in Fortify's elevation of application security. This release contains updates to Fortify Static Code Analyzer, Fortify WebInspect, Fortify Software Security Center, and Fortify Software Composition Analysis.

There are lots of core upgrades, new features, and fine tuning in this release, with full details found in the release documentation. Here, we wanted to highlight a few key features:

Time vs Depth
Choose the level of depth in your testing efforts for a faster scan speed for time sensitive moments during development.

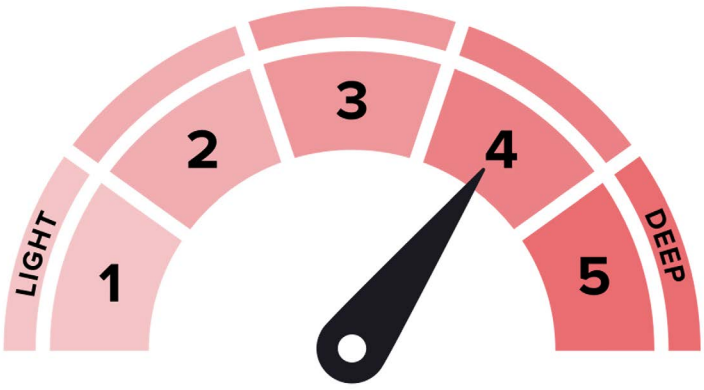

Figure 1. Speed dial for Static Code Analyzer

SAST + DAST Correlation
ScanCentral DAST can now uncover correlations between DAST and SAST results and forward the information to Fortify Software Security Center. Learn More

API Discovery
You aren't aware of all your APIs – you don't always know there is an API in your application. Now WebInspect can detect APIs automatically. Learn more

Infrastructure-as-Code Support
Secure your cloud and virtual environments through scanning the technology used to create them. Learn more

Modern App Support
Engine updates ensure WebInspect keeps up to date with current trends and is always able to scan your applications

2FA Support
More and more organizations are requiring two-factor authentication (2FA). Many organizations had to work around this, but WebInpect now supports this automatically so scans can avoid getting paused. Learn more

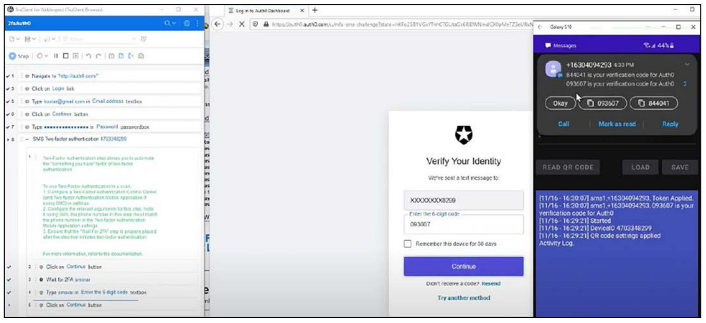

Figure 2. 2FA support with WebInspect

Fortify Platform

Static/Dynamic Issue Correlation Indicator

In this release, we introduce the static/dynamic issue correlation indicator. After static and dynamic scans are run on an application version and the results have been uploaded to Fortify Software Security Center, issues that were uncovered by both static and dynamic scans are tagged with the correlation indicator on the AUDIT page.

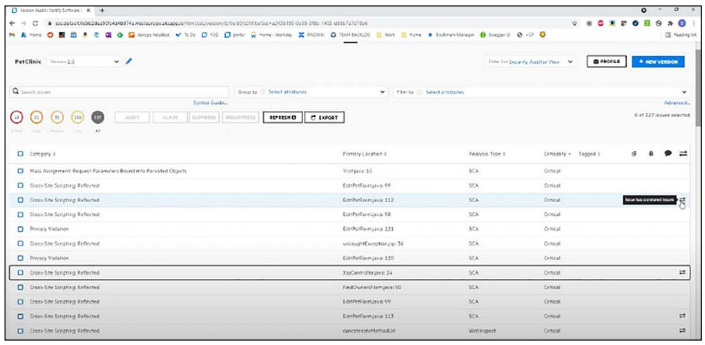

Figure 3. SAST + DAST Correlation

ScanCentral SAST Controller Updates

- You can now place the ScanCentral SAST Controller into maintenance mode which prevents scans that are running on the sensor from losing data.
- You can shutdown ScanCentral SAST Controller sensors individually or in a batch. ScanCentral DAST Scans Support
- The Scans feature now includes both static and dynamic scan results

New Premium Quarterly Reports

- PCISSF (Software Security Framework) 1.2 report
- CWE Top 25 report

LDAP Update

- You can now configure Fortify Software Security Center to invalidate tokens created by users who have been disabled in LDAP

Java 11 Deployment

- Software Security Center can be deployed in a Java 11 (or higher) environment Kubernetes Updates
- Added support for Kubernetes 1.21
- Added support for Helm 3.6 and 3.7

Fortify SAST

ScanCentral SAST

ScanCentral enables scaling with a static analysis farm that can meet the changing demands of the CI/CD pipeline. The following features have been added to ScanCentral SAST:

- Support for the Fortify License and Infrastructure Manager
- MSBuild Integration Update
- Go Language Support
- Graceful Shutdown and Timer Support
- Sensor Pool Assignment Improvement

Fortify License and Infrastructure Manager

For customers that use Fortify under the Concurrent Scanning license model, Fortify Static Code Analyzer can now use the Fortify License and Infrastructure Manager to obtain a license key rather than the traditional fortify.license file. This enables the correct sharing of the Fortify Scan Machine license metric between Fortify Static Code Analyzer and WebInspect instances. The option to use the traditional fortify.license file is still available.

Regular Expression (RegEx) Analysis

The Fortify Static Code Analyzer Configuration analyzer can now detect vulnerabilities in file names and content using RegEx-based rules.

Operating System Updates

Fortify added support for the following operating systems and versions:

- IBM AIX 7.1
- Oracle Solaris SPARC 11.3
- Oracle Solaris x64 11.4
- Windows Server 2022

Compiler Updates

Fortify added support for the following compiler versions:

- gcc 10.2.1
- g++ 10.2.1
- Swiftc 5.4.2

Build Tool Updates

Fortify added support for the following build tool versions:

- Gradle 7.2
- Maven 3.8.2
- MSBuild 16.11
- Xcodebuild 12.5.1

C++ Updates
- Added support for gcc on Macintosh
- Added support for gcc version 10.2.1
- Added support for C++ 14 and 17

JavaScript Improvements
- Added support for ECMAScript 2021
- Added support for TypeScript 4.2 - 4.3
- Made Type inference improvements
- Added support for SAPUI5/OpenUI5
- Minified JS excluded from scan by default

Go Language Update
- Added support for Go 1.17

YAML Support
- Added support for translating YAML code

Kotlin Update
- Added support for Kotlin 1.5

PHP
- Completed support for PHP 8

Scala
Eliminated the need for a separate license from Lightbend for Scala translations. A license key is still required to run the plugin. The key is now included in the Fortify distribution.

Configuration Scanning
- JSON scanning enabled by default
- Added YAML scanning

New PCI SSF Report
Generate new PCI SSF Report (version 1.2) from the following tools:
- Fortify Audit Workbench
- Fortify Visual Studio Extension
- Fortify Eclipse Plugins (Complete and Remediation)
- BIRT Report Generator

Fortify DAST

Fortify ScanCentral DAST
With our next generation dynamic application security testing capabilities, you can enable, scale and automate DAST in your CI/CD process using ScanCentral with the existing Fortify Jenkins and Fortify Azure plugins, creating a more holistic AppSec approach. The following features have been added to ScanCentral DAST:

- **Correlated Issues**
  - ScanCentral DAST can now uncover correlations between DAST and SAST results and forward the information to Fortify Software Security Center. Correlated results are displayed in the Fortify Software Security Center AUDIT View.
- **Scan Visualization Update**
  - Selected scan visualizations can be opened in a new browser tab rather than using Site Explorer.
- **Client-Side Certificate Support**
  - Upload a certificate and password for use when running a scan. If a scan requires the certificate, ScanCentral DAST will download and install it.
  - Enable Redundant Page Detection and use it when running a scan.
- **Scan Priority Level**
  - All scans can be assigned a priority level.
  - When a scan is queued because there isn't a free sensor and a scan with a lower priority is running, the lower-priority scan will be shut down so the scan with the higher priority can run. The scan with the lower priority will restart when a sensor becomes available.
- **Azure SQL Support**
  - The ScanCentral DAST Configuration Tool now supports Azure SQL and Azure Managed SQL.
  - The ScanCentral DAST container now supports Azure SQL and Azure Managed SQL.

API Discovery
With the new API Discovery, any Swagger or OpenAPI schema detected during a scan will have its endpoints added to the existing scan and authentication will be applied to the endpoints with our automatic state detection. In addition, probes will be sent to default locations of popular API frameworks to discover schemas.

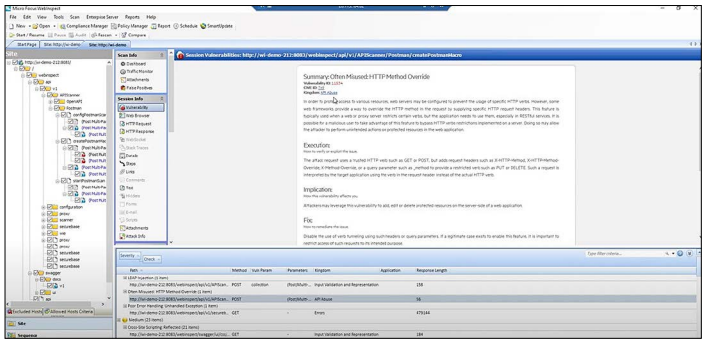

Figure 4. API Discovery in WebInspect

Two-Factor Authentication

Two-factor Authentication is a common requirement in enterprises and can be a burden to the security tester to get a bypass or to manually scan. WebInspect now offers the ability to automate Two-factor Authentication scans. This is accomplished by installing a lightweight Android app onto a phone or emulator that can capture SMS and Email tokens and pass them back to the scanner for authentication. Once configured, there is no need for user interaction.

Watch the Fortify 21.2 Playlist on our Fortify Unplugged YouTube Channel to see demos of the latest features in this release.

Automatic State Detection

WebInspect now automatically detects and configures state for Oauth, JWT, and Bearer Tokens during a scan.

Engine 6.1 Updates

Fortify continues to enhance its engines to improve scan coverage and performance. WebInspect 21.2.0 provides a faster crawl and audit, and better application support from the Web Macro Recorder with Macro Engine 6.1.

Improved DOM XSS Detection

WebInspect 21.2.0 has new DOM XSS detection capabilities for analyzing client-side code for XSS. This will allow for improved XSS attack performance and the ability to detect client-side only attacks, such as XSS in DOM fragments.

Web Fuzzer Tool

The Web Fuzzer Tool lets you run Fuzzing tests that submit random or sequential data to various areas of an application to uncover security vulnerabilities. For example, when searching for buffer overflows, a tester can generate data of various sizes and send it to one of the application entry points to observe how the application handles it.

Learn more here

Contact us at **CyberRes.com**

Like what you read? Share it.

CyberRes
A Micro Focus line of business