Micro Focus
Fortify Security Assistant Plugin for IntelliJ IDEA

Software Version: 22.1

User Guide

Document Release Date: Revision 1: June 1, 2022

Software Release Date: January 2022

Legal Notices

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

https://www.microfocus.com

Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors (“Micro Focus”) are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Except as specifically indicated otherwise, a valid license from Micro Focus is required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

Trademark Notices

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

This document was produced on June 01, 2022. To check for recent updates or to verify that you are using the most recent edition of a document, go to:

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

Contents

Preface

Contacting Micro Focus Fortify Customer Support

Visit the Support website to:

- Manage licenses and entitlements
- Create and manage technical assistance requests
- Browse documentation and knowledge articles
- Download software
- Explore the Community

https://www.microfocus.com/support

For More Information

For more information about Fortify software products:

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

About the Documentation Set

The Fortify Software documentation set contains installation, user, and deployment guides for all Fortify Software products and components. In addition, you will find technical notes and release notes that describe new features, known issues, and last-minute updates. You can access the latest versions of these documents from the following Micro Focus Product Documentation website:

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

To be notified of documentation updates between releases, subscribe to Fortify Product Announcements on the Micro Focus Community:

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

Fortify Product Feature Videos

You can find videos that highlight Fortify products and features on the Fortify Unplugged YouTube channel:

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

Change Log

The following table lists changes made to this document. Revisions to this document are published between software releases only if the changes made affect product functionality.

Software Release / Document Version	Changes
22.1 / Revision 1: June 1, 2022	Updated: • "Fortify Security Assistant Requirements" on page 6 - Supports Android Studio

Chapter 1: Introduction

This section contains the following topics:

Fortify Security Assistant Plugin for IntelliJ IDEA

Fortify Security Assistant Plugin for IntelliJ IDEA (Fortify Security Assistant) works with a portion of the Fortify security content to provide alerts to potential security issues as you write your code. Fortify Security Assistant provides detailed information about security risks and recommendations for how to secure the potential issue. Fortify Security Assistant works with IntelliJ IDEA and Android Studio.

Fortify Security Assistant includes both structural and configuration analyzers to detect:

- Potentially dangerous uses of functions and APIs
- Insecure application configurations in property and XML files

Note: The instructions in this guide describe a third-party product and might not match the specific, supported version you are using. See your product documentation for the instructions for your version.

Fortify Security Content

Fortify Security Assistant uses a knowledge base of rules to enforce secure coding standards applicable to the codebase for static analysis. Micro Focus Fortify Software Security Content consists of Fortify Secure Coding Rulepacks, which describe general secure coding idioms for popular languages and public APIs.

Fortify Security Assistant Requirements

Fortify Security Assistant requires:

- A valid Fortify license file

  For information about how to obtain a Fortify license, contact Micro Focus Fortify Customer Support at https://www.microfocus.com/support.

- Up-to-date Micro Focus Fortify Software Security Content

  You can either:

  - Download the Fortify security content directly from the Fortify Rulepack update server or from a Fortify Software Security Center server.
  - Use a local copy of Fortify security content.

    You might choose this option if you do not have a network connection to a server.

  For instructions, see "Configuring Fortify Security Assistant" on page 8.
- Fortify Security Assistant works with:
  - IntelliJ IDEA versions 2020.x and 2021.x
  - Android Studio version 2021.x

Chapter 2: Installation and Configuration

This section contains the following topics:

Installing Fortify Security Assistant

You can install the Fortify Security Assistant on Windows, Linux, and macOS. The Fortify Security Assistant plugin is available for download from the JetBrains Marketplace.

To install Fortify Security Assistant:

1. Start IntelliJ IDEA.
2. Open the Settings dialog box as follows:
   - On Windows or Linux, select **File > Settings**.
   - On macOS, select ***<IDE_name>*** **> Preferences**.
3. On the left pane, select **Plugins**.
4. Select the **Marketplace** tab, and then in the search box type `Fortify Security Assistant`.
5. Click **Install**.
6. Click **OK**.

If this is the first time you have installed Fortify Security Assistant, you must next specify the Fortify license file and load Fortify security content (see "Configuring Fortify Security Assistant" below).

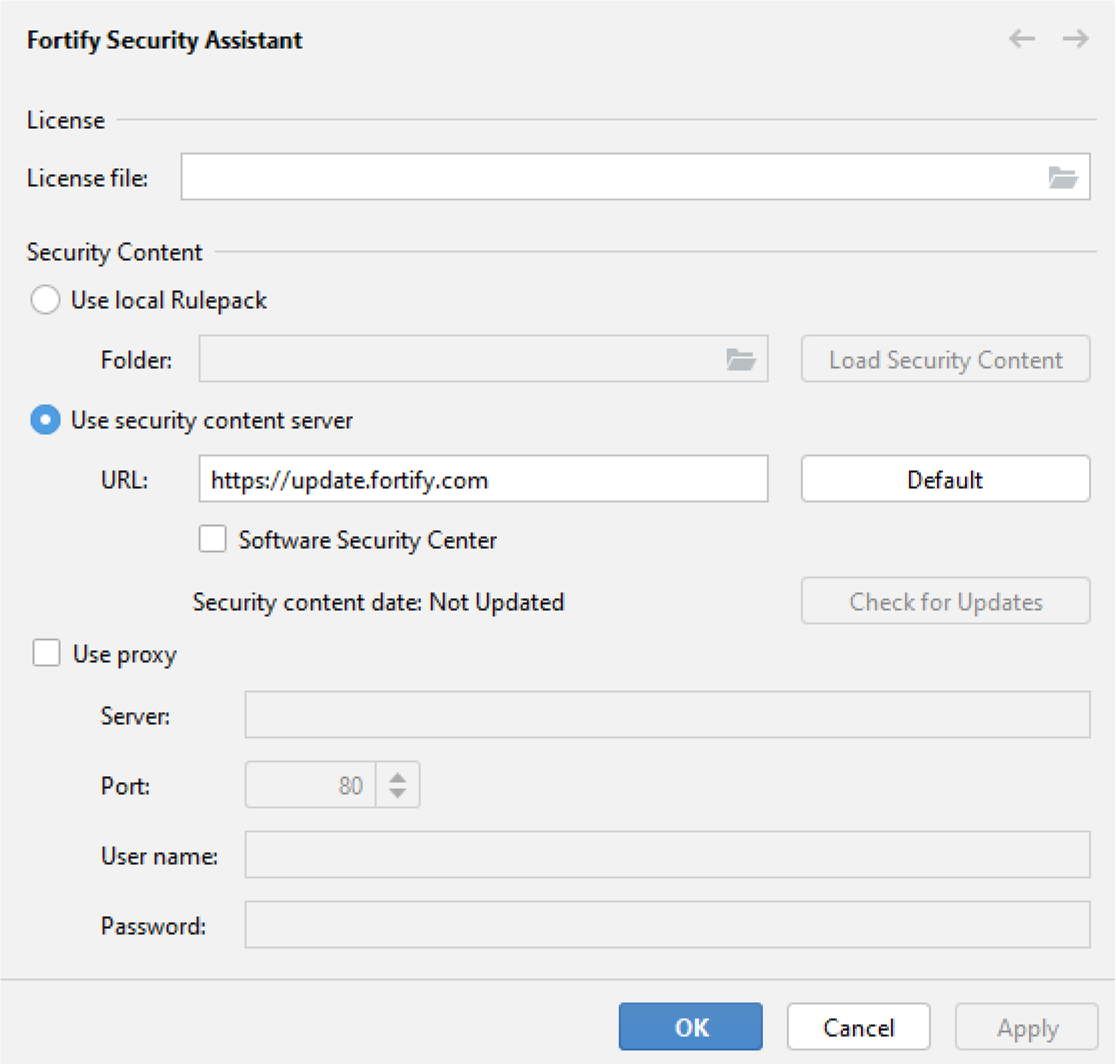
Configuring Fortify Security Assistant

In order for Fortify Security Assistant to detect vulnerabilities in your code, you must have a valid Fortify license file and load up-to-date Micro Focus Fortify Software Security Content. You can download Fortify security content from the Fortify Rulepack update server (https://update.fortify.com), or from a Micro Focus Fortify Software Security Center server.

If you do not have a network connection to the Fortify Rulepack update server or a Fortify Software Security Center server, Fortify Security Assistant can load Fortify security content from a local folder.

To configure Fortify Security Assistant:

1. Select **File > Settings**, and then select **Fortify Security Assistant**.



Fortify Security Assistant

License

License file:

Security Content

○ Use local Rulepack

Folder:

● Use security content server

URL: https://update.fortify.com

□ Software Security Center

Security content date: Not Updated

□ Use proxy

Server:

Port: 80

User name:

Password:

2. To specify the license file, click **Browse** to the right of the **License file** box and navigate to the license file (`fortify.license`) on your system.
3. To load or update Fortify security content stored locally:
   a. Select **Use local Rulepack**.
   b. Click **Browse** next to the **Folder** box and navigate to a folder on your system that contains the Rulepacks.

      The selected folder must contain Rulepacks as ZIP, XML, or BIN files.
   c. Click **Load Security Content**.

4. To download Fortify security content from a Rulepack update server or from Fortify Software Security Center:
   a. Select **Use security content server**.
   b. To download security content from the Fortify Rulepack update server, in the **URL** box, type a Rulepack server URL.

      The default is the Fortify Rulepack update server URL (http://update.fortify.com).

      > **Note:** Click **Default** to set the URL to the default Fortify Rulepack update server.

   c. To download security content from Fortify Software Security Center:
      i. In the **URL** box, type a Fortify Software Security Center URL.
      ii. Select the **Software Security Center** check box.
   d. If a connection to the security content server requires a proxy, select **Use proxy** and provide the proxy server host name (for example, my.proxy.com), port, and proxy authentication credentials if required.
   e. Click **Check for Updates**.

      > **Note:** If you get an error that indicates the downloaded security content is unverified, you might have an invalid license file. Contact Micro Focus Fortify Customer Support for assistance.

5. Click **OK**.

Uninstalling Fortify Security Assistant

To uninstall the Micro Focus Fortify Security Assistant Plugin for IntelliJ IDEA:

1. Start IntelliJ IDEA or Android Studio.
2. Open the Settings dialog box as follows:
   - On Windows or Linux, select **File > Settings**.
   - On macOS, select ***<IDE_name>*** **> Preferences**.
3. On the left, select **Plugins**.
4. From the installed **Plugins** list, select **Fortify Security Assistant**.
5. Select **Uninstall**.

Chapter 3: Using Fortify Security Assistant

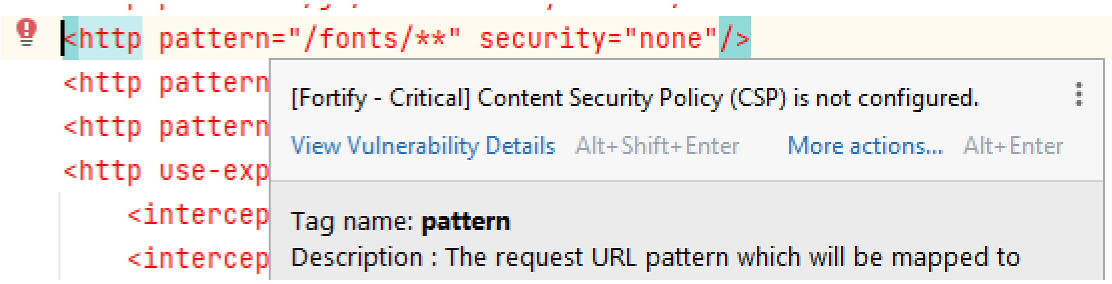
Fortify Security Assistant notifies you of any detected issues as you write your code. You can also use Fortify Security Assistant to examine an entire project and then you can review possible security issues (see "Scanning a Project for Security Issues" on page 13).

This section contains the following topics:

Finding Security Issues as you Write Code

As you write your code, Fortify Security Assistant provides notifications of potential security issues in the **Fortify Security Assistant** window and in the IntelliJ IDEA **Problems** window. Critical issues are shown in red in the code editor.

To see more details about the detected issue from the code editor, place the cursor over the issue, and select **View Vulnerability Details** to open the Fortify **Vulnerability Details** window. This window provides a detailed description of the issue, examples, and recommendations of how to fix the issue.



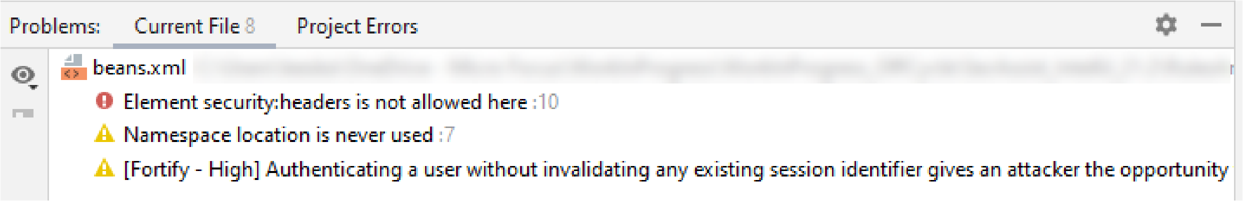
```
<http pattern="/fonts/**" security="none"/>
<http pattern
<http pattern
<http use-exp
    <intercep
    <intercep
```

[Fortify - Critical] Content Security Policy (CSP) is not configured.

View Vulnerability Details Alt+Shift+Enter
More actions... Alt+Enter

Tag name: **pattern**
Description : The request URL pattern which will be mapped to

Issues detected are also shown in the **Problems** window prefixed with `[Fortify - <priority>]` as shown in the following example:



beans.xml

Element security:headers is not allowed here :10

Namespace location is never used :7

[Fortify - High] Authenticating a user without invalidating any existing session identifier gives an attacker the opportunity

See Also

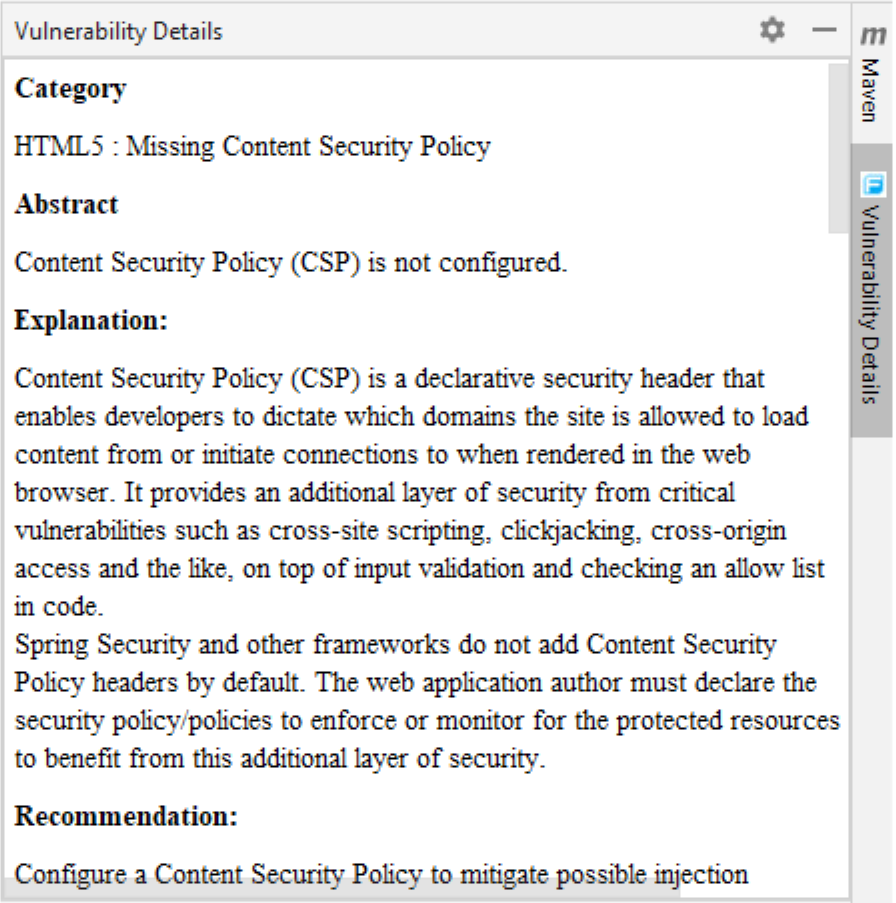
"Viewing Vulnerability Details" below

"Scanning a Project for Security Issues" on the next page

Viewing Vulnerability Details

To see a detailed description of an issue, from the code editor or the **Fortify Security Assistant** window, right-click the issue, and then select **View Vulnerability Details**.

The **Vulnerability Details** window provides a detailed description of the issue, examples, and recommendations of how to fix the issue.



Category

HTML5 : Missing Content Security Policy

Abstract

Content Security Policy (CSP) is not configured.

Explanation:

Content Security Policy (CSP) is a declarative security header that enables developers to dictate which domains the site is allowed to load content from or initiate connections to when rendered in the web browser. It provides an additional layer of security from critical vulnerabilities such as cross-site scripting, clickjacking, cross-origin access and the like, on top of input validation and checking an allow list in code.
Spring Security and other frameworks do not add Content Security Policy headers by default. The web application author must declare the security policy/policies to enforce or monitor for the protected resources to benefit from this additional layer of security.

Recommendation:

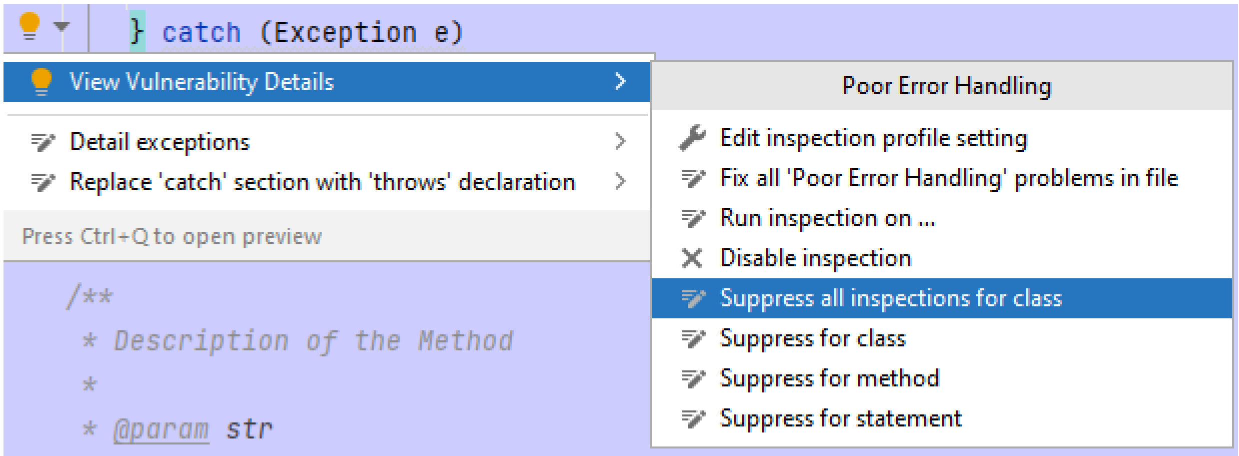
Configure a Content Security Policy to mitigate possible injection

Suppressing Issues

You might want to suppress warnings for specific issues that might not be high priority or of immediate concern.

To suppress issues, use the native IntelliJ IDEA suppress inspections feature in the code editor. You can suppress issues from the code editor and the **Problems** window. To access the suppression options in the code editor, right-click the issue, and then click to open the **View Vulnerability Details** submenu.

The following is an example that shows how to access the inspection suppression options from the code editor:



```
} catch (Exception e)
```

```
/**
 * Description of the Method
 *
 * @param str
```

View Vulnerability Details
Detail exceptions
Replace 'catch' section with 'throws' declaration
Press Ctrl+Q to open preview
Poor Error Handling
Edit inspection profile setting
Fix all 'Poor Error Handling' problems in file
Run inspection on ...
Disable inspection
Suppress all inspections for class
Suppress for class
Suppress for method
Suppress for statement

For more information about re-enabling suppressed inspections, see the IntelliJ IDEA documentation.

The visibility of suppressed issues in the **Fortify Security Assistant** window depends on the setting for the **Suppressed** column). For instructions on how to change the visibility of suppressed issues, see "Working with the Fortify Security Assistant Window" on page 16.

See Also

"Disabling Vulnerability Categories" on the next page

Scanning a Project for Security Issues

You can use Fortify Security Assistant to analyze the whole project (or a specific set of files) and identify security issues. You cannot make any code changes during the analysis.

To scan a project for issues, select **Code > Inspect Code**.

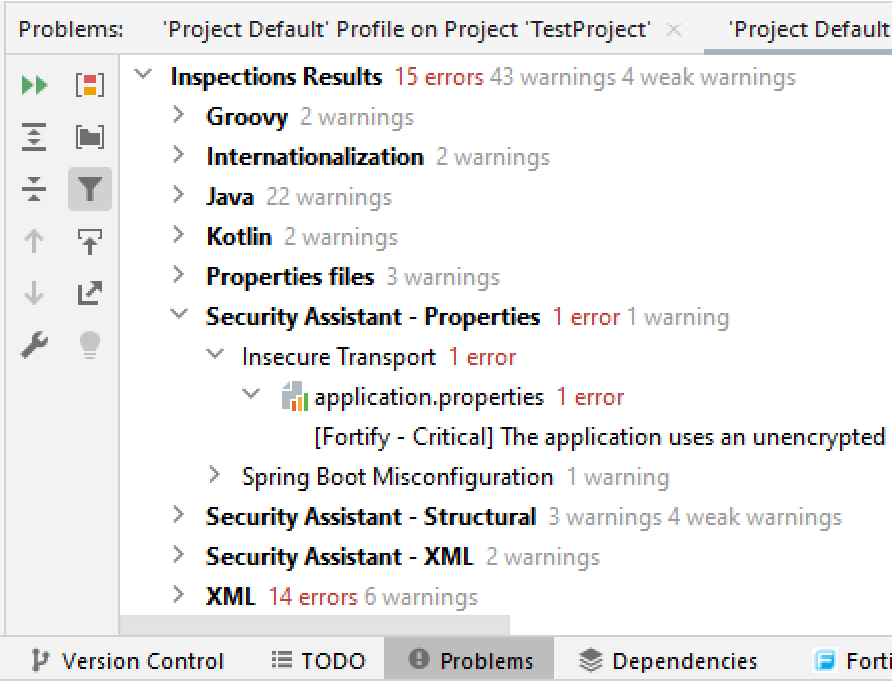
If you see the following message in the Event Log:

```
Please wait for the security content (Rulepack) to be loaded. Security
content is required to detect vulnerabilities.
```

Then wait until the Fortify security content is loaded. Run the code inspection again after you see the following message:

```
Fortify Security Assistant is ready to work
```

Fortify Security Assistant displays any detected issues in the IntelliJ IDEA **Problems** window. The issues are grouped by analyzer as shown in the following example.



- **Inspections Results** 15 errors 43 warnings 4 weak warnings
  - **Groovy** 2 warnings
  - **Internationalization** 2 warnings
  - **Java** 22 warnings
  - **Kotlin** 2 warnings
  - **Properties files** 3 warnings
  - **Security Assistant - Properties** 1 error 1 warning
    - Insecure Transport 1 error
      - application.properties 1 error
        - [Fortify - Critical] The application uses an unencrypted
    - Spring Boot Misconfiguration 1 warning
  - **Security Assistant - Structural** 3 warnings 4 weak warnings
  - **Security Assistant - XML** 2 warnings
  - **XML** 14 errors 6 warnings

The detected security issues are also displayed in the **Fortify Security Assistant** window. For information about reviewing the security issues in the **Fortify Security Assistant** window, see "Working with the Fortify Security Assistant Window" on page 16.

Disabling Vulnerability Categories

As you review Fortify detected issues, you might want to completely disable a category of reported issues. It is useful to disable vulnerability categories if you are sure that the vulnerability category is not, and will never be, an issue of concern.

All issues in the disabled vulnerability categories are not reported again unless you re-enable them (see "Enabling Vulnerability Categories" on the next page).

To disable a vulnerability category, use the native IntelliJ IDEA disable inspection feature (**File > Settings > Editor > Inspections**). There are three groupings of Fortify Security Assistant vulnerability categories:

- Security Assistant - Properties
- Security Assistant - Structural
- Security Assistant - XML

Note: You can also disable a Fortify vulnerability category for a scanned project from the **Problems** window.

After you clear a check box for a vulnerability category, issues that fall into that vulnerability category are no longer highlighted in the code as a Fortify issue.

Enabling Vulnerability Categories

To re-enable a Fortify vulnerability category that you have disabled, use the native IntelliJ IDEA re-enable inspection feature (**File > Settings > Editor > Inspections**). Locate the Fortify Security Assistant vulnerability category you want to re-enable and select the check box.

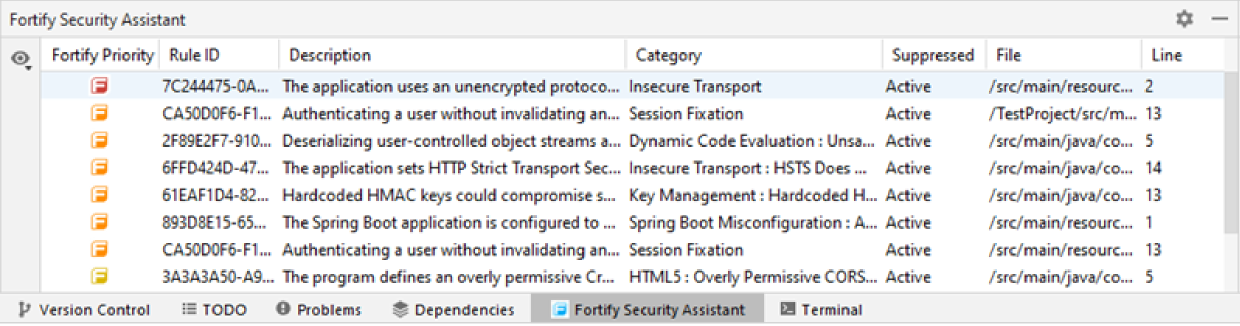
Note: You can also re-enable a vulnerability category for a scanned project from the **Problems** window. To refresh the issues displayed in the Fortify Security Assistant window after re-enabling a vulnerability category, rescan the project (see "Scanning a Project for Security Issues" on page 13).

See Also

"Disabling Vulnerability Categories" on the previous page

Working with the Fortify Security Assistant Window

Fortify Security Assistant displays all the security issues detected as you write code and for open files in the **Fortify Security Assistant** window.



Fortify Priority	Rule ID	Description	Category	Suppressed	File	Line
🟥	7C244475-0A...	The application uses an unencrypted protoco...	Insecure Transport	Active	/src/main/resourc...	2
🟧	CA50D0F6-F1...	Authenticating a user without invalidating an...	Session Fixation	Active	/TestProject/src/m...	13
🟧	2F89E2F7-910...	Deserializing user-controlled object streams a...	Dynamic Code Evaluation : Unsa...	Active	/src/main/java/co...	5
🟧	6FFD424D-47...	The application sets HTTP Strict Transport Sec...	Insecure Transport : HSTS Does ...	Active	/src/main/java/co...	14
🟧	61EAF1D4-82...	Hardcoded HMAC keys could compromise s...	Key Management : Hardcoded H...	Active	/src/main/java/co...	13
🟧	893D8E15-65...	The Spring Boot application is configured to ...	Spring Boot Misconfiguration : A...	Active	/src/main/resourc...	1
🟧	CA50D0F6-F1...	Authenticating a user without invalidating an...	Session Fixation	Active	/src/main/resourc...	13
🟨	3A3A3A50-A9...	The program defines an overly permissive Cr...	HTML5 : Overly Permissive CORS...	Active	/src/main/java/co...	5

The following table describes the Fortify information provided for each issue.

Column	Description
Fortify Priority	Colored icon indicates the Fortify Priority Order used to categorize the severity of a vulnerability - 🟥 Critical - 🟧 High - 🟨 Medium - 🟨 Low
Rule ID	Unique identifier of the rule that triggered the vulnerability detection
Description	Brief description of the issue
Category	Fortify vulnerability category
Suppressed	Indicates whether the issue has been suppressed **Note:** By default, suppressed issues are not visible in this window. To see suppressed issues in this list, select **View Options** (👁) **> Show Suppressed**.
File	The name of the file where the issue occurs. To change whether to show the file path or only the file name, select **View Options** (👁) **> Show Short File Name**.
Line	The line number where the issue occurs in the file.

As you review the detected issues, you can do the following:

- Read more information about the vulnerability by right-clicking an issue, and then selecting **View Vulnerability Details**.

  > **Note:** If the **Vulnerability Details** window is already open, click an issue to see the corresponding details in this window.

- Open the file and locate the line of code where the issue was found by clicking the issue.
- Group the issues by file name, Fortify Priority, Fortify Rule ID, or Fortify category by clicking **View Options** (👁) and then selecting the grouping you want.
- Change whether suppressed issues are visible by selecting **View Options** (👁) **> Show Suppressed**.
- Show issues for the current file only by selecting **View Options** (👁) **> Show only Current File**.

See Also

"Viewing Vulnerability Details" on page 12

"Suppressing Issues" on page 13

Troubleshooting

For help diagnosing a problem, you can open the Fortify Security Assistant log file from IntelliJ. To open the log file, select **Help > Show Fortify Security Assistant Log**. If you contact Micro Focus Fortify Customer Support, provide them with this log file.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email.

Note: If you are experiencing a technical issue with our product, do not email the documentation team. Instead, contact Micro Focus Fortify Customer Support at https://www.microfocus.com/support so they can assist you.

If an email client is configured on this computer, click the link above to contact the documentation team and an email window opens with the following information in the subject line:

Feedback on User Guide (Fortify Security Assistant Plugin for IntelliJ IDEA 22.1)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to fortifydocteam@microfocus.com.

We appreciate your feedback!