

OpenText™ Fortify Security Assistant Plugin for Eclipse

Software Version: 23.2.0

User Guide

Document Release Date: December 2023

Software Release Date: December 2023

Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2015 - 2023 Open Text.

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

Trademark Notices

“OpenText” and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

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 November 27, 2023. 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	5
Contacting Fortify Customer Support	5
For More Information	5
About the Documentation Set	5
Fortify Product Feature Videos	5
Change Log	6
Getting Started	7
Fortify Security Assistant Plugin for Eclipse	7
Software Requirements	7
Installing Fortify Security Assistant for Eclipse	8
Configuring Fortify Security Assistant for Eclipse	9
Configuring Where to Obtain Security Content	9
Loading Fortify Security Content from a Local System	11
Specifying Categories of Issues to Detect	11
Updating Security Content	13
Finding Security Issues as you Write Java Code	13
Working with Issues in the Code Editor	15
Scanning Projects for Issues	15
Working with the Security Assistant Issues View	16
Showing Suppressed Issues	18
Unsuppressing Issues	18
Hiding Security Issues	18

Revealing Previously Hidden Security Issues	19
Troubleshooting	19
Send Documentation Feedback	20

Preface

Contacting 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 OpenText Product Documentation website:

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

To be notified of documentation updates between releases, subscribe to Fortify Product Announcements on the OpenText 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
23.2.0	Updated: <ul style="list-style-type: none">• Requirements for obtaining Fortify Software Security Content and the supported versions of Eclipse (see "Software Requirements" on the next page)
23.1.0	Updated: <ul style="list-style-type: none">• Supported versions of Eclipse (see "Software Requirements" on the next page)
22.2.0	Added: <ul style="list-style-type: none">• "Troubleshooting" on page 19 Updated: <ul style="list-style-type: none">• Support added for the latest versions of the Eclipse IDE (see "Software Requirements" on the next page)
22.1.0	Updated: <ul style="list-style-type: none">• Support added for the latest versions of the Eclipse IDE (see "Software Requirements" on the next page)• New option to initially import security content from the local system (see "Configuring Fortify Security Assistant for Eclipse" on page 9 and "Updating Security Content" on page 13)

Getting Started

This guide provides information about how to install and use the Fortify Security Assistant Plugin for Eclipse.

Fortify Security Assistant Plugin for Eclipse

Fortify Security Assistant Plugin for Eclipse (Fortify Security Assistant for Eclipse) is a plugin that integrates with the Eclipse Java development environment. Fortify Security Assistant for Eclipse works with a portion of the Fortify security content to provide alerts to potential security issues as you write your Java code. Fortify Security Assistant for Eclipse provides detailed information about security risks and recommendations for how to secure the potential issue.

Fortify Security Assistant includes the semantic and intra-class data flow analyzers to detect:

- Potentially dangerous uses of functions and APIs
- Issues caused by tainted data reaching vulnerable functions and APIs at the intra-class level

Software Requirements

Fortify Security Assistant for Eclipse requires:

- A valid Fortify license
You are prompted to provide a license file the first time you make edits to source code, request to analyze a project, or load Fortify Software Security Content. For information about how to obtain a Fortify license file, contact Customer Support.
- Up-to-date Fortify Software Security Content

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

To update Fortify Software Security Content, do one of the following:

- Download the Fortify security content directly from the Fortify Rulepack update server or from an OpenText™ Fortify Software Security Center server.

Important! To download security content from a Fortify Software Security Center URL or the Fortify Rulepack update server that uses HTTPS, you must import a self- or locally-signed certificate into the Java Runtime Environment (JRE) certificate store.

- Load Fortify security content from a copy on your local system.

For instructions on these options, see ["Configuring Where to Obtain Security Content" on page 9](#).

Fortify Security Assistant supports Eclipse versions 2021-x, 2022-x, and 2023-03-09.

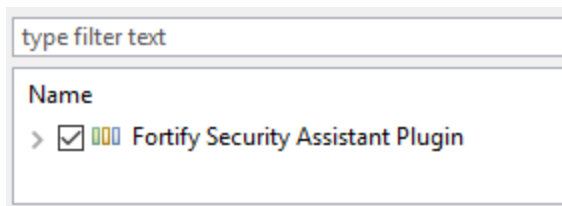
Installing Fortify Security Assistant for Eclipse

You can install the Fortify Security Assistant Plugin for Eclipse on Windows, Linux, and macOS operating systems. To update from an earlier version of Fortify Security Assistant Plugin for Eclipse, you must first remove the existing version.

Note: These instructions 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.

To install Fortify Security Assistant for Eclipse:

1. Start Eclipse.
2. Select **Help > Install New Software**.
The Install wizard starts and displays the **Available Software** step.
3. Click **Add**.
4. Click **Archive**, and then locate and select `Fortify_SecurityAssistant_Eclipse_Plugin_<version>.zip`.
5. Click **Add**.
6. Select the **Fortify Security Assistant Plugin** check box.



Any required third-party dependencies are automatically installed if they do not already exist on your system.

7. Click **Next**.
The **Install Details** step lists **Fortify Security Assistant Plugin For Eclipse**.
To view version and copyright information about the plugin in the **Details** area, click the plugin name.
8. Click **Next**.
9. On the **Review Licenses** step, review and accept the license agreement.
10. Click **Finish**.
11. To complete the installation and restart Eclipse, click **Restart Now** when prompted.
The menu bar now includes the **Fortify** menu.
12. In the Locate Fortify License File dialog box, click **Browse**.

Note: The prompt for the Fortify license file occurs one time after the plugin installation when you have a project open in Eclipse.

13. Navigate to the `fortify.license` file, and then click **OK**.

Fortify Security Assistant for Eclipse verifies the license file and then attempts to download the Fortify Software Security Content from the Fortify Customer Portal. To import Fortify Software Security Content from a Fortify Software Security Center server or the local system, see "[Configuring Where to Obtain Security Content](#)" below or "[Loading Fortify Security Content from a Local System](#)" on page 11.

Configuring Fortify Security Assistant for Eclipse

Fortify Security Assistant for Eclipse requires Fortify Software Security Content to detect issues. You can configure how Fortify Security Assistant for Eclipse obtains security content and which vulnerability categories you want detected.

Configuring Where to Obtain Security Content

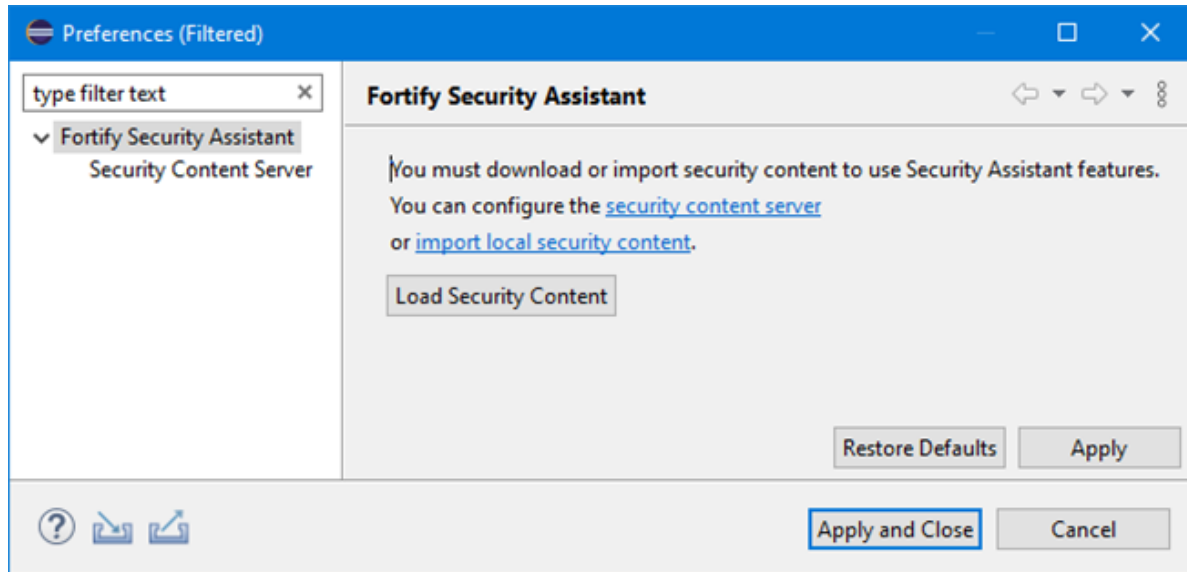
By default, Fortify Security Assistant for Eclipse attempts to download the Fortify Software Security Content from the Fortify Rulepack update server. There are three ways to obtain Fortify security content:

- From the Fortify Rulepack update server
- From a Fortify Software Security Center server
- From your local system if you do not have an internet connection or a Fortify Software Security Center server (see "[Loading Fortify Security Content from a Local System](#)" on page 11)

To configure where to download Fortify security content:

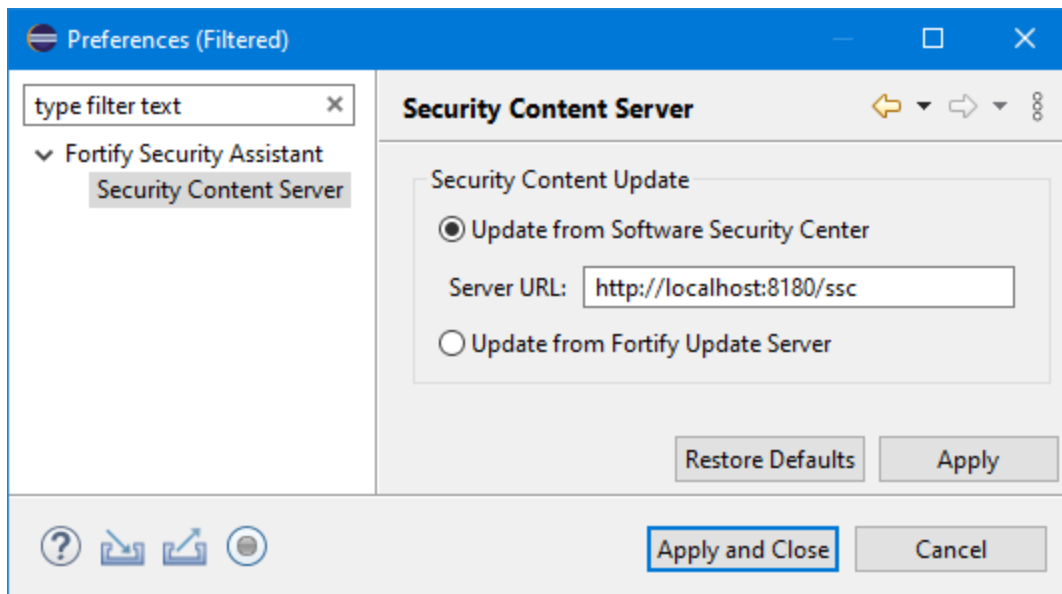
1. Select **Fortify > Configure Security Assistant**.

The following Fortify Security Assistant dialog box shows that no security content is loaded yet.



2. To download the security content from a Fortify Software Security Center server, do the following:

- a. Select **Security Content Server** in the left pane.



- b. Select **Update from Software Security Center**, and then type the URL for your Fortify Software Security Center server in the **Server URL** box.

3. To download and load the security content from the Fortify Rulepack update server, do the following:
 - a. Select **Security Content Server** in the left pane.
 - b. Select **Update from Fortify Update Server**.
4. Click **Apply and Close** to save these settings.
5. Select **Fortify > Update Security Content** to load the security content.

See Also

["Updating Security Content" on page 13](#)

["Loading Fortify Security Content from a Local System" below](#)

Loading Fortify Security Content from a Local System

To import and load security content from your local system:

1. Select **Fortify > Configure Security Assistant**.
2. Click **import local security content**.
3. In the Import Security Content dialog box, select the file type for the Fortify security content.
You can import ZIP, XML, or BIN files.
4. Navigate to and select your Fortify security content.
5. Click **Open**.
6. Click **Apply and Close**.


See Also

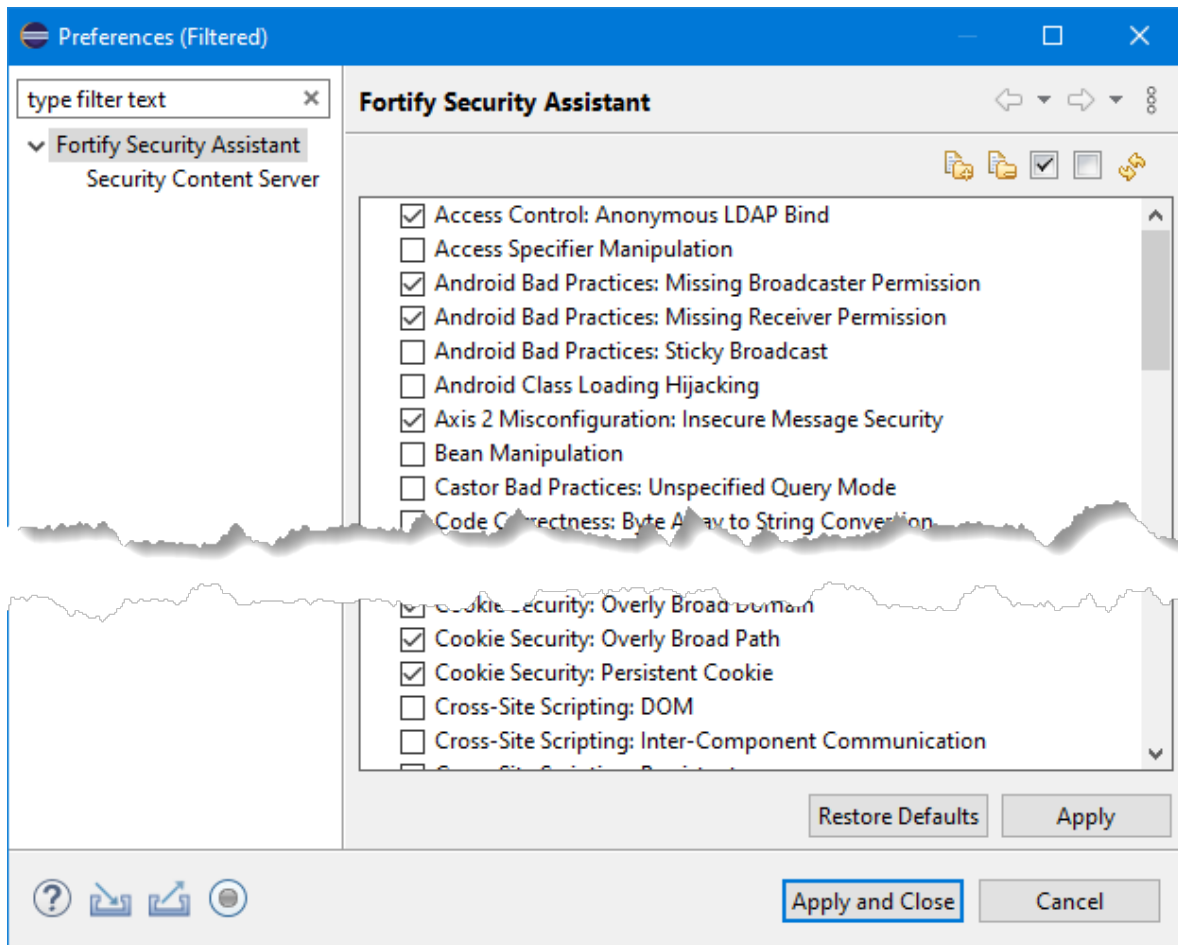
["Updating Security Content" on page 13](#)


Specifying Categories of Issues to Detect


To specify the categories of issues to detect for the workspace or for a project:

1. Do one of the following to select where you want the changes applied:
 - To configure settings for the workspace, select **Fortify > Configure Security Assistant**.
 - To configure settings for a project:
 - i. Right-click a project, and then select **Properties**.
 - ii. In the left pane, select **Fortify Security Assistant**.
 - iii. Select **Enable project specific settings**.

Note: You can also specify the category of issues from a Fortify Security Assistant for Eclipse tooltip in the Code editor. Click **Configure Security Assistant** , and then click **Configure Workspace** or **Configure Project**.



2. Select the categories of issues you want to detect.
You can right-click in the list of categories, and then select **Select All** or select **Clear All (but one)**.
3. To import custom rules:
 - a. Click **Import Security Content** .
 - b. Navigate to where your custom file is located, select the XML, and then click **Open**.

Note: To remove any previously imported custom rules, click **Clear All Imported Security Content** . You cannot undo this action.

4. Click **Apply and Close**.

Fortify Security Assistant for Eclipse re-inspects the project to refresh any issues reported so that it matches your configuration settings.

Updating Security Content


To optimize Fortify Security Assistant for Eclipse functionality, you must have complete and up-to-date Fortify Software Security Content.

To obtain the latest security content from the configured server:

1. Select **Fortify > Update Security Content**.
2. If prompted to accept a key, click **Yes**.

Note: This is only required when you load security content from a Fortify Software Security Center server. After you accept the key the first time, it is saved for the current plugin installation.

To import security content from the local system:

1. Select **Fortify > Configure Security Assistant**.
2. Click **Import Security Content** ().
3. You can import ZIP, XML, or BIN files.
3. Navigate to and select your Fortify security content.
4. Click **Open**.

See Also

["Configuring Where to Obtain Security Content" on page 9](#)


Finding Security Issues as you Write Java Code

Fortify Security Assistant for Eclipse notifies you of any detected issues as you write your code. You can also have Fortify Security Assistant for Eclipse examine an entire project and then review detected security issues (see ["Scanning Projects for Issues" on page 15](#)).

To review the security issues:

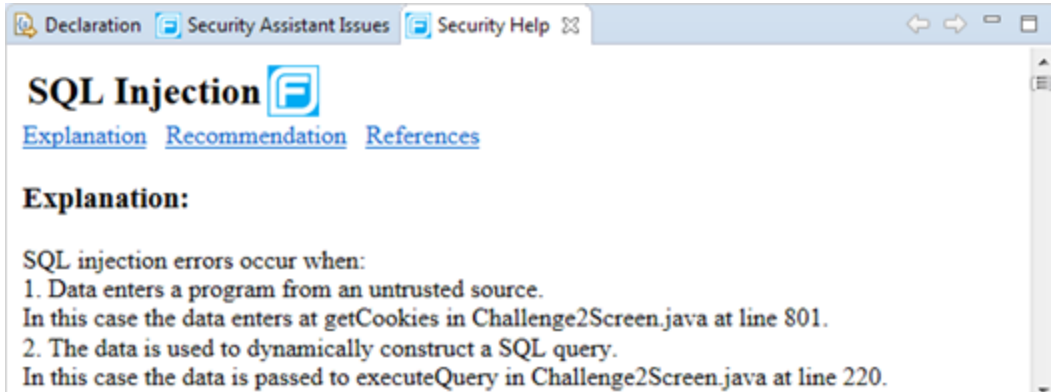
- Fortify Security Assistant for Eclipse highlights detected security issues in the code. It also tags the issue with an icon in the left border of the editor area. Pause your cursor over the highlighted code to open a tooltip that briefly describes the issue as shown in the following example:


```
218     try
219     {
220         ResultSet results = statement3.executeQuery(query);
221
222         while (results.next())
223         {
224             String type = results.getString("cc_type");
225             String num = results.getString("cc_number");
```

[Critical] Security issue: (SQL Injection) 
Vulnerable Code: Click the item to see more details

Fortify Security Assistant for Eclipse sorts issues based on Fortify Priority Order (Critical, High, Medium, and Low).

- Click the issue to see a detailed description of it in the **Security Help** view.



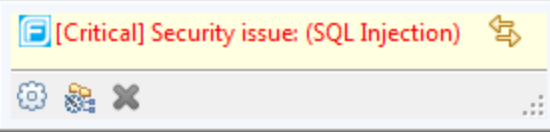
Note: You can page through the visited descriptions in the **Security Help** view with the **Go Back** and **Go Forward**  buttons.

- Select **Fortify > Open Security Issue List** to open the **Security Assistant Issues** view, which displays all the issues detected in the file.
See "[Working with the Security Assistant Issues View](#)" on page 16 for more information.





Working with Issues in the Code Editor

Pause your cursor over the highlighted code to open a tooltip that displays one or more issues. Move your cursor into the Fortify Security Assistant for Eclipse tooltip or press **F2** to access additional options.

```
try
{
    ResultSet results = statement3.executeQuery(query);
    while (results.next())
    {
        String type = results.getStrin
        String num = results.getString( cc_number );
        v.addElement(type + "-" + num);
    }
}
```



The Fortify Security Assistant for Eclipse tooltip displays the icons described in the following table.

Icon	Description
	Specify the categories of issues to show. You can configure settings for the current project or the workspace. Note: Settings configured for a project override the settings for the workspace.
	Configure Fortify Security Assistant for Eclipse annotation preferences.
	Suppress this issue for the function. This indicates that the issue is not a problem. The issue is not reported again for this function unless you unsuppress it.
	For dataflow issues, go to the origin of the tainted data that reached this function.

Scanning Projects for Issues

You can use Fortify Security Assistant for Eclipse to examine a project and identify any security issues.

To scan a project for issues:

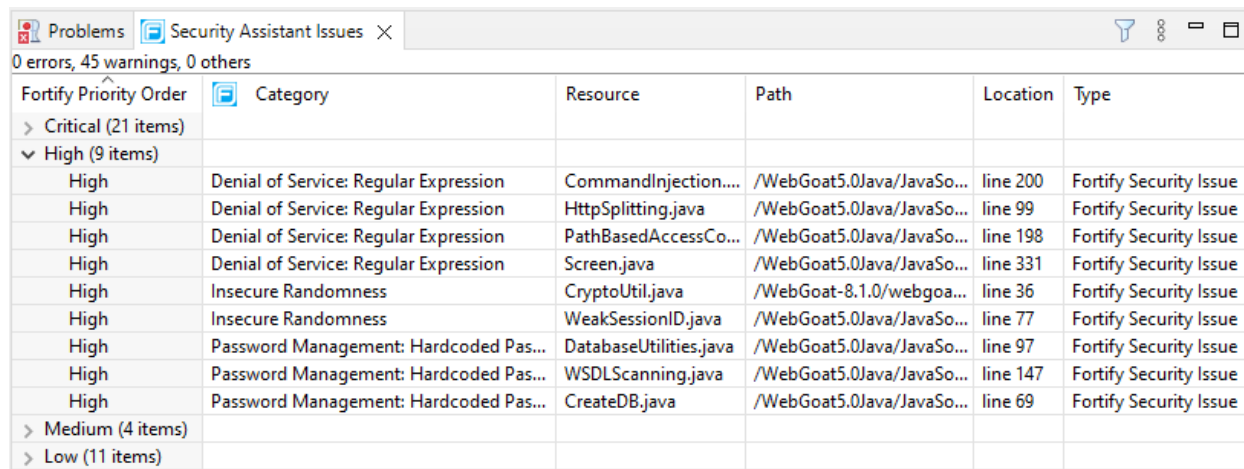
- Right-click the project name, and then select **Inspect the Project**.

Fortify Security Assistant for Eclipse displays any detected issues in the **Security Assistant Issues** view. For information on how to use this view, see ["Working with the Security Assistant Issues View" on the next page](#).

Working with the Security Assistant Issues View

The **Security Assistant Issues** view shows all detected security issues for code that has been inspected with Fortify Security Assistant for Eclipse.

Note: These instructions 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 Priority Order	Category	Resource	Path	Location	Type
> Critical (21 items)					
< High (9 items)					
High	Denial of Service: Regular Expression	CommandInjection...	/WebGoat5.0Java/JavaSo...	line 200	Fortify Security Issue
High	Denial of Service: Regular Expression	HttpSplitting.java	/WebGoat5.0Java/JavaSo...	line 99	Fortify Security Issue
High	Denial of Service: Regular Expression	PathBasedAccessCo...	/WebGoat5.0Java/JavaSo...	line 198	Fortify Security Issue
High	Denial of Service: Regular Expression	Screen.java	/WebGoat5.0Java/JavaSo...	line 331	Fortify Security Issue
High	Insecure Randomness	CryptoUtil.java	/WebGoat-8.1.0/webgoa...	line 36	Fortify Security Issue
High	Insecure Randomness	WeakSessionID.java	/WebGoat5.0Java/JavaSo...	line 77	Fortify Security Issue
High	Password Management: Hardcoded Pas...	DatabaseUtilities.java	/WebGoat5.0Java/JavaSo...	line 97	Fortify Security Issue
High	Password Management: Hardcoded Pas...	WSDLScanning.java	/WebGoat5.0Java/JavaSo...	line 147	Fortify Security Issue
High	Password Management: Hardcoded Pas...	CreateDB.java	/WebGoat5.0Java/JavaSo...	line 69	Fortify Security Issue
> Medium (4 items)					
> Low (11 items)					

Note: If the **Security Assistant Issues** view is not open, select **Fortify > Open Security Issue List**.

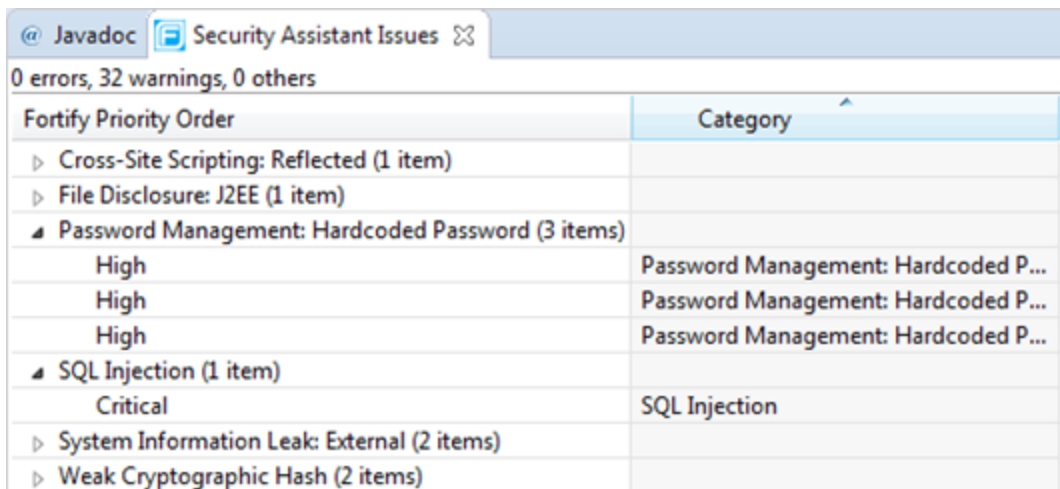
- To see a detailed description of an issue, right-click the issue, and then select **Description**.
The **Security Help** view opens and provides an explanation of the issue, recommendations for fixing the issue, and references related to the issue.
- To go to the location of the issue in the file editor, double-click the issue in the **Security Assistant Issues** view.
- To go to the source location of the tainted data for dataflow issues, right-click the dataflow issue, and then select **Go to Source**.
- To change which issues are shown, click **View Menu**, select **Show**, and then select one or more of the options listed in the following table.

Option	Description
All Critical Security Issues	Shows all critical, non-suppressed issues for Fortify

Option	Description
in Workspace	Security Assistant for Eclipse-inspected code in your workspace
All Security Issues in Workspace	Shows all non-suppressed issues for Fortify Security Assistant for Eclipse-inspected code in your workspace
Security Issues on Selection	Shows all non-suppressed issues based on the current selection
All Suppressed Security Issues	Shows all suppressed issues in your workspace
Show All	Shows all issues (including suppressed) for Fortify Security Assistant for Eclipse-inspected code (selecting this option clears the other options in the Show menu)
	<div style="background-color: #f0f0f0; padding: 5px;"> <p>Note: If you clear all the other show options, the Show All option is automatically selected.</p> </div>

- To change how the issues are grouped, click the **View Menu**, select **Group By**, and then select **Fortify Priority Order** (the default view), **Category**, or **None**.

The following example shows issues grouped by **Category**.



- By default, the maximum number of issues shown in one group is 100. To change the maximum number of issues shown, click **View Menu**, select **Filters**, and type a different value in the **Items per group** box.

To display all issues, select **View Menu > Filters**, and then clear the **Use Limits** check box.

- To change the columns that are displayed, click **View Menu**, and then select **Configure Columns**.

Showing Suppressed Issues

Issues that you have suppressed are not highlighted in the source code (even after you restart Eclipse). By default, Fortify Security Assistant for Eclipse does not display suppressed issues in the **Security Assistant Issues** view.

To show the suppressed issues:

- In the **Security Assistant Issues** view, select **View Menu > Show > All Suppressed Security Issues**.

Suppressed issues are indicated in the **Type** column as a **Suppressed Security Issue**.

Unsuppressing Issues

To unsuppress an issue:

1. If the **Security Assistant Issues** view is not open, select **Fortify > Open Security Issue List**.
2. To show the suppressed issues in the **Security Assistant Issues** view, do one of the following:
 - Select **View Menu > Show > All Suppressed Security Issues**.
 - Select **View Menu > Show > Show All**.
3. Right-click the suppressed issue, and then select **Delete**.
4. Right-click the project, and then select **Inspect the Project** to have the issue display in the **Security Assistant Issues** view.

Hiding Security Issues

You can hide security issues in specified files for the current Eclipse session. Fortify Security Assistant for Eclipse ignores the files during any re-inspection until you either restore (reveal) the security issues for the files or restart Eclipse.

To hide the security issues, do one of the following:

- For a folder, right-click the folder in the Project Explorer or Package Explorer, and then select **Clear Security Issues**.
- For a file, right-click in the file editor, and then select **Clear Security Issues**.

Revealing Previously Hidden Security Issues

You can reveal security issues that you previously hid (cleared) for the current Eclipse session.

To show previously hidden security issues, do one of the following:

- For a folder, right-click the folder, and then select **Restore Cleared Security Issues**.
- For a file, right-click in the file editor, and then select **Restore Cleared Security Issues**.

Troubleshooting

Fortify Security Assistant for Eclipse writes any warnings or errors to the Eclipse Error Log. Include this log file if you contact Customer Support about an issue with Fortify Security Assistant for Eclipse.

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 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 Eclipse 23.2.0)

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@opentext.com.

We appreciate your feedback!