Fortify Plugin

Plugin Information
View Fortify on the plugin site for more information.

The plugin adds the ability to perform security analysis with Micro Focus Fortify Static Code Analyzer, upload results to Micro Focus Fortify Software Security Center, show analysis results summary, and set build failure criteria based on analysis results.

Summary

Use the Fortify Jenkins Plugin in your continuous integration builds to identify security issues in your source code with Fortify Static Code Analyzer. After the Fortify Static Code Analyzer analysis is complete, you can upload the results to a Fortify Software Security Center server. The Fortify Jenkins Plugin also enables you to view the analysis result details within Jenkins. It provides metrics for each build and an overview of the results, without requiring you to log into Fortify Software Security Center.

This is the official Fortify plugin for working with Fortify on-premises products. Link to the Official Fortify Jenkins Plugin documentation

Features

- Provides a post-build action to analyze the source with Fortify Static Code Analyzer, update Security Content, upload analysis results to Fortify Software Security Center, and fail the build depending on uploaded results processed by Fortify Software Security Center
- Provides pipeline support for source code analysis with Fortify Static Code Analyzer, Security Content update, and uploading to Fortify Fortify Software Security Center
- Displays Fortify security analysis results for each Job (a history trend and latest issues from Fortify Software Security Center), and navigates to individual issues on Fortify Software Security Center for detailed analysis

Video tutorial

http://youtube.com/watch?v=cjEwDmTsxII

Setup

1. Create an authentication token of type JenkinsToken or CIToken

    a. either on the SSC server
    Log in to SSC, click the Administration tab and select Users -> Token Management link on the left side.

    Copy the second (decoded) token at the bottom of the message (the one that says it can be used with fortifyclient).

    b. or using the fortifyclient utility:

    From the *<ssc_install_dir>*/Tools/fortifyclient/bin directory, run the following:

    ```
    fortifyclient token -gettoken CIToken -url <ssc_url> -user <user_name> [-daysToLive <number_of_days>]
    ```

    Note: Find the Tools folder in the directory where the Fortify Software Security Center WAR file was extracted.

    where:

    - *<ssc_url>* includes both the port number and the context path /ssc. For example, http://*<hostname>*:*<port>*/ssc.
    - *<user_name>* is the Fortify Software Security Center username of an account that has the required privileges to read or write information from or to Fortify Software Security Center.
    - *<number_of_days>* is the number of days before the token expires. The default is 365.

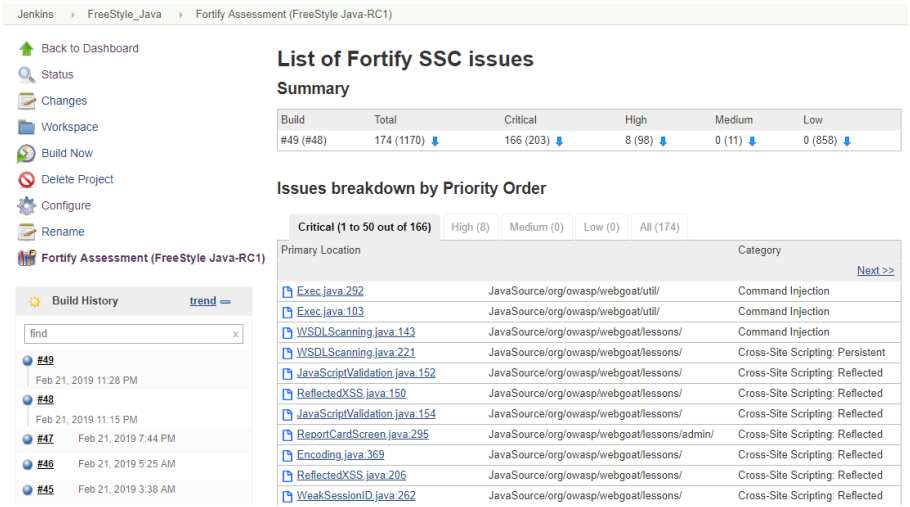
    You are prompted for a password. Type the password for *<user_name>*.

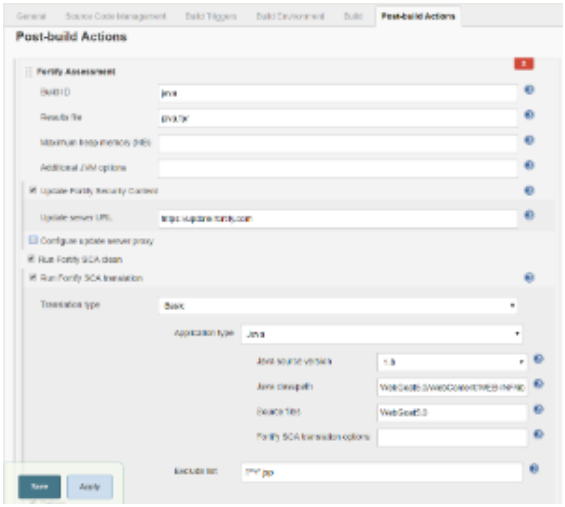
    The fortifyclient utility displays a token of the general form: cb79c492-0a78-44e3-b26c-65c14df52e86.
2. From Jenkins, select **Manage Jenkins > Manage Plugins**, on the **Plugin Manager** page, click the **Available** tab, in the **Filter** box, type Fortify. Select the checkbox for the **Fortify** plugin, and then click either **Install without restart** or **Download and install after restart**.
3. From the Jenkins menu, select **Jenkins > Manage Jenkins > Configure System**. To use fail condition and see security results in Jenkins you need to upload to Fortify Software Security Center, so scroll down to the **Fortify Assessment** section, and then do the following:
    - In the **SSC URL** box, type the Fortify Software Security Center server URL. The correct format for the Fortify Software Security Center URL is: http://*<host_IP>*:*<port>*/ssc.
    - To connect to Fortify Software Security Center with a proxy server, select **Use Proxy for SSC**, and then specify the proxy information. Use the following format for the **Proxy server host:port**: *<address>*:*<port_number>*
    - In the **Authentication token** box, type the authentication token generated for the Fortify Software Security Center server in Step 1.
    - Click **Advanced settings**, and then click **Test Connection**.
4. To analyze your project with Fortify Static Code Analyzer or to update Fortify security content as part of your build, create a Jenkins environment variable to specify the location of the Fortify Static Code Analyzer executables. In **Global properties**, create the following environment variable:
    - **Name:** FORTIFY_HOME

- **Value:** *<sca_install_dir>*

where *<sca_install_dir>* is the path where Fortify Static Code Analyzer is installed. For example, on Windows the default installation location is C:\Program Files\Fortify\Fortify_SCA_and_Apps_*<version>*.

Preview





Version history

Version 19.1 (February, 2019)

The first official open source release
New features and updates
• Pipeline support
• Providing information on artifact processing state on SSC
• Fortify SSC REST API support
• Compatibility with the latest Jenkins server versions

Feedback welcome

This plugin is maintained by the Fortify team. If you have any problems, questions, or enhancement requests or would like to contribute to the code please let us know via GitHub Issues.