Qualys Web App Scanning Connector for TeamCity

User Guide

Version 1.0.1

April 03, 2020

Qualys, Inc.
919 E Hillsdale Blvd
4th Floor
Foster City, CA 94404
1 (650) 801 6100

Preface

Welcome to Qualys Cloud Platform! In this guide, we'll show you how to install and use the Qualys Web App Scanning Connector to see your Qualys WAS scan data in TeamCity.

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions. The Qualys Cloud Platform and its integrated apps help businesses simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications.

Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Deutsche Telekom, Fujitsu, HCL, HP Enterprise, IBM, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also a founding member of the Cloud Security Alliance (CSA). For more information, please visit www.qualys.com

Qualys Support

Qualys is committed to providing you with the most thorough support. Through online documentation, telephone help, and direct email support, Qualys ensures that your questions will be answered in the fastest time possible. We support you 7 days a week, 24 hours a day. Access support information at www.qualys.com/support/

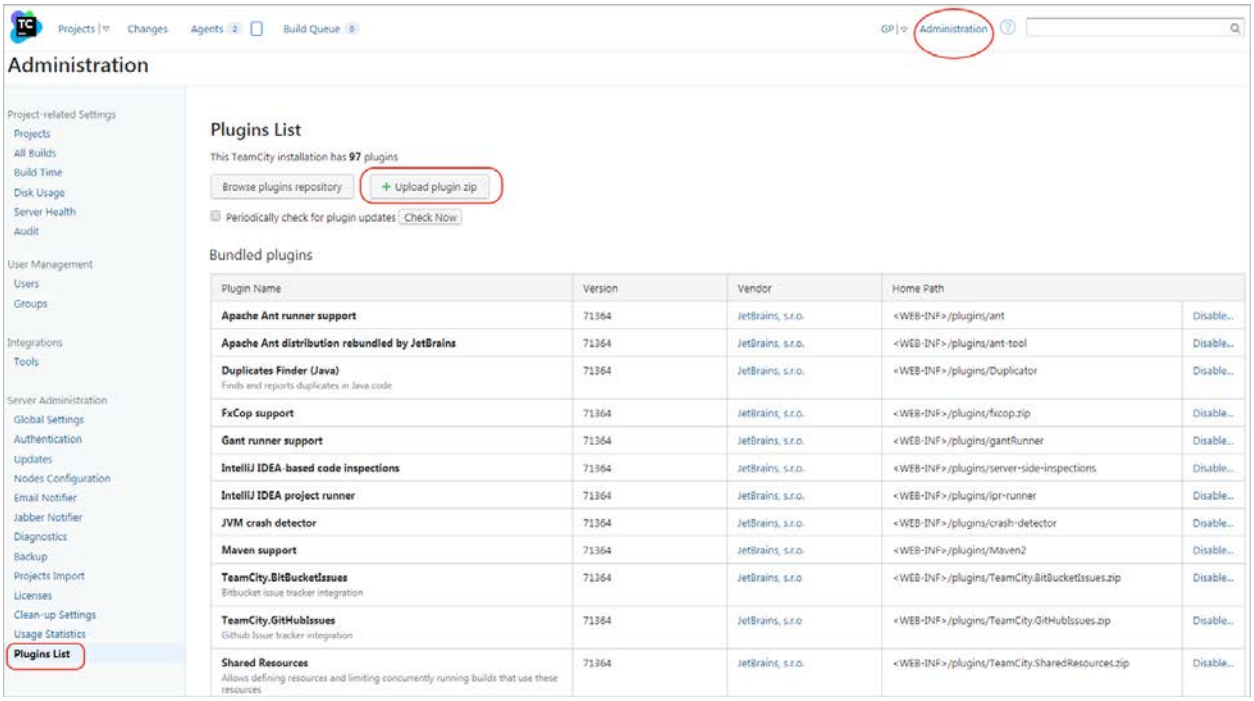
Introduction to Qualys Web App Scanning Connector for TeamCity

The Qualys Web App Scanning Connector empowers DevOps teams to build application vulnerability scans into their existing CI/CD processes. By integrating scans in this manner, application security testing is accomplished earlier in the SDLC to catch and eliminate security flaws.

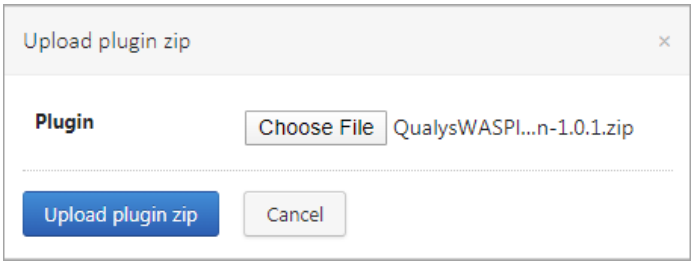
We'll help you: Install the Plugin | Configure the Plugin

Download and Install the Plugin

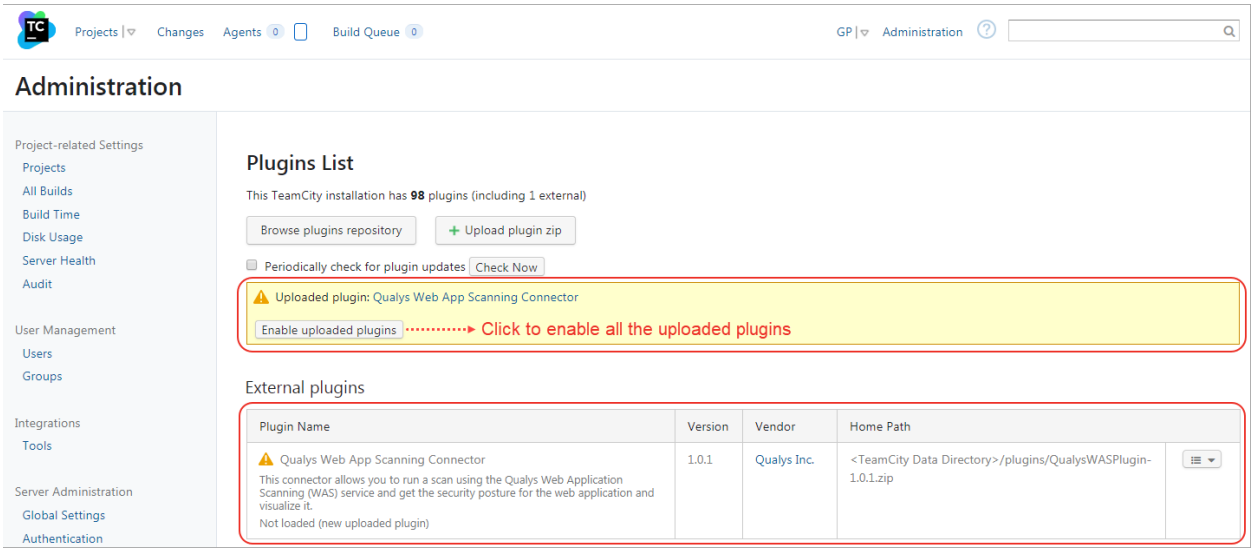
You can download the plugin from Qualys Community page. The plugin comes in the form of a zip file. Once you have the zip file, log into your instance of TeamCity and go to Administration. Under Administration, click Plugins List. On the Plugins List page , click Upload plugin zip.



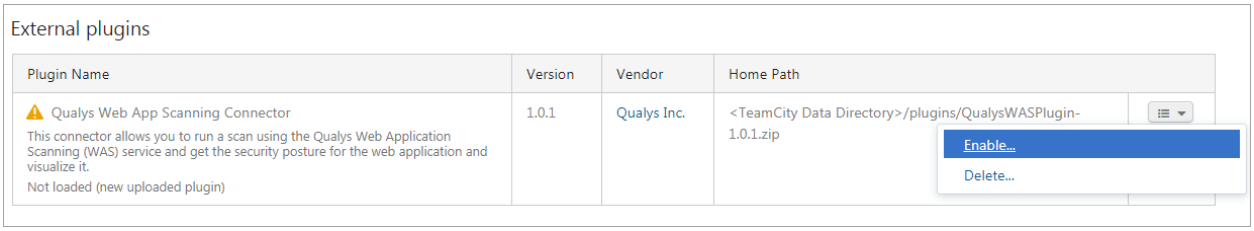
On the Upload plugin zip screen, choose the plugin zip file and click Upload plugin zip.



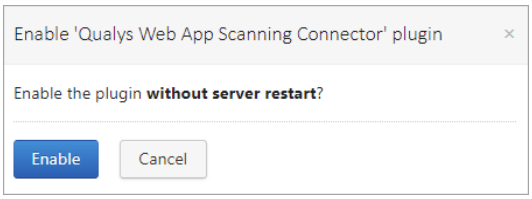
After uploading the plugin installation file, you will see the plugin listed under the External plugins section. A message is shown to enable uploaded plugins. Click Enable uploaded plugins.



Optionally, if you want to enable only Qualys Web App Scanning Connector, then in the table under the External plugins section, go to the row that displays Qualys Web App Scanning Connector and click the drop-down in the last column and select Enable.



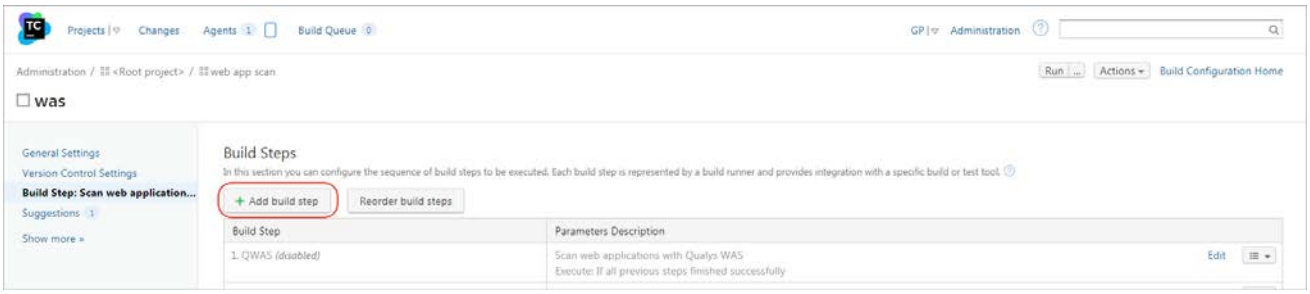
Plugin will be enabled without restarting the server. If you want to restart the server and then enable the plugin, click Cancel.



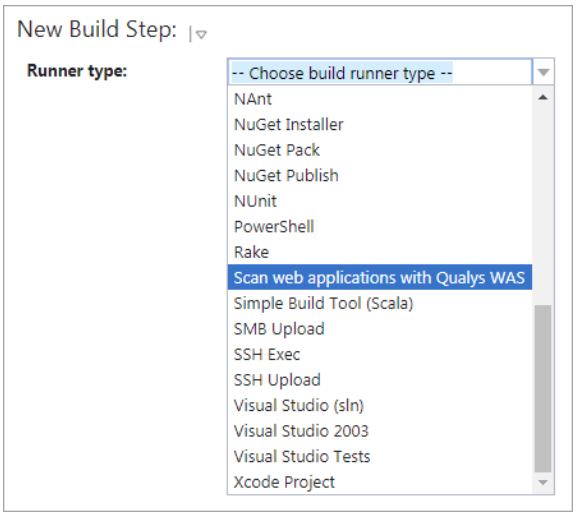
That's it! The installation is now complete. Read on to learn about configuring the plugin.

Configure the Plugin

Go to your project in TeamCity and click Add build step.



Select “Scan web applications with Qualys WAS” from the drop-down menu.



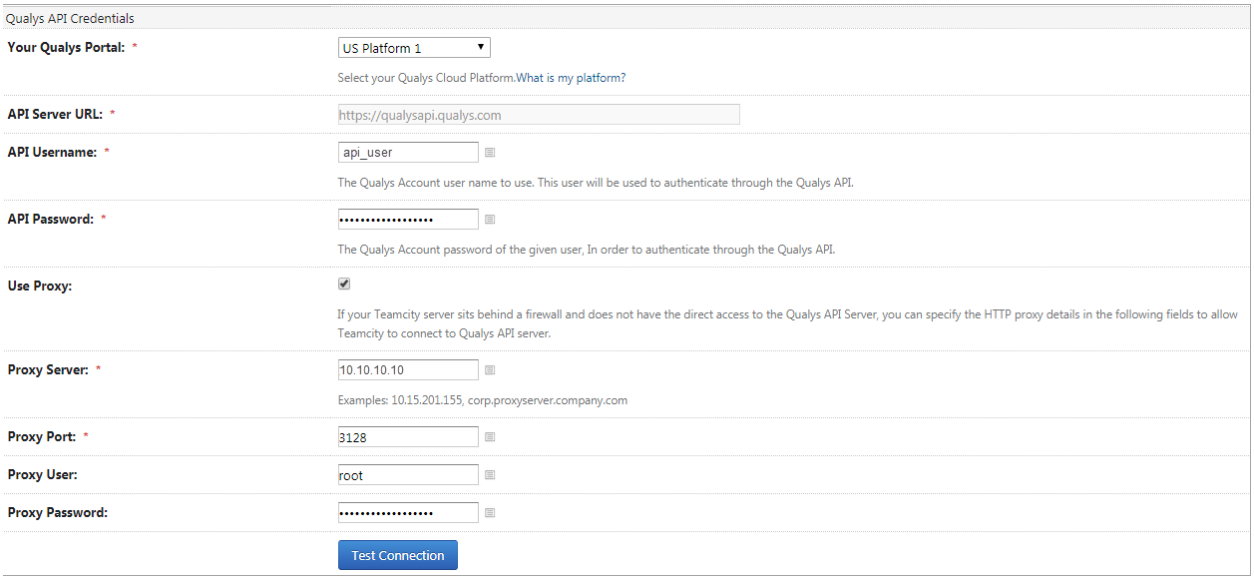
Now you are ready to configure the plugin.

Next, provide a name to the build step and then go to the Qualys API Credentials section.

This step is to confirm that TeamCity can communicate to the Qualys Cloud Platform via the WAS API. You’ll need valid account credentials for an active Qualys WAS subscription. The account must have API access enabled as well as a role assigned with all necessary permissions. Qualys recommends using a service account restricted to API access only (no UI access) and having the least privileges possible.

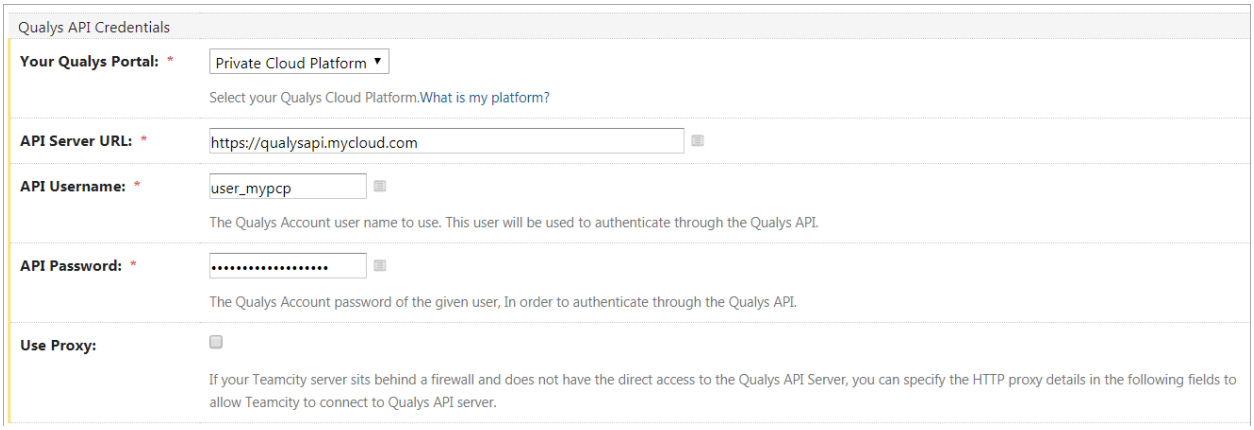
Select the Qualys platform/portal where your Qualys account resides. On selecting the platform, we will show you the API server URL of the selected platform. Enter your account credentials: API username and password for authenticating to the WAS API server. Note that what you select here depends on the Qualys platform your organization is using. Learn more.

If your TeamCity instance does not have direct Internet access and a proxy is required, click the "Use Proxy Settings" checkbox and enter the required information.

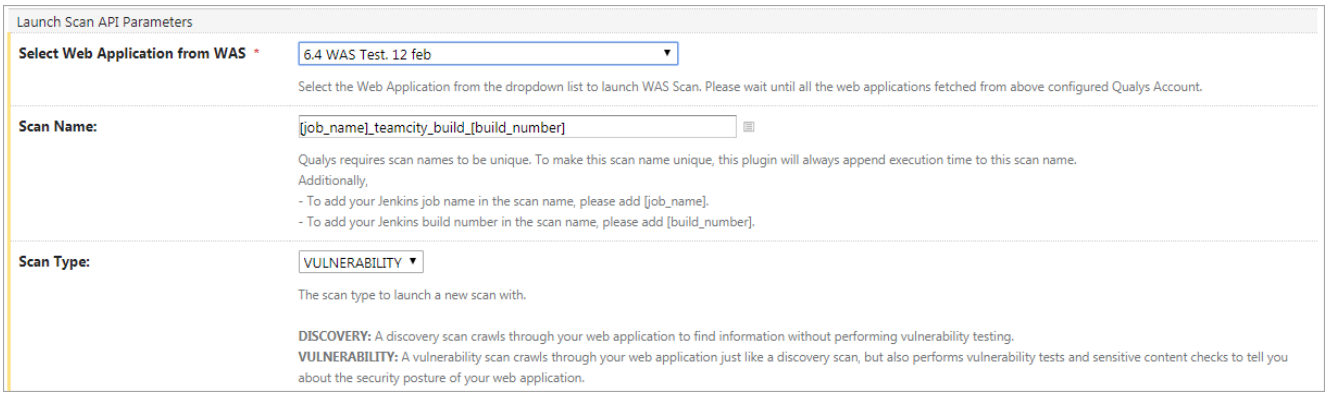


Click the "Test Connection" button. Assuming you have selected the correct platform for your subscription and the credentials are valid, you will see the message "Connection test successful!".

Note that if your Qualys account resides on a private cloud platform, select “Private Cloud Platform” as your Qualys cloud platform, specify the API server URL and your account credentials to access the API.



Next, select the web application in Qualys WAS that you wish to scan.

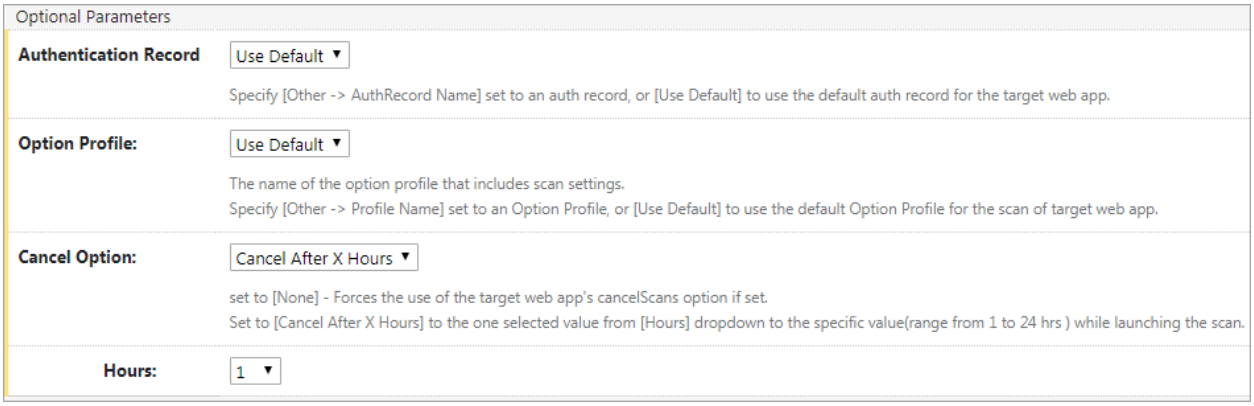


By default, the WAS scan name will be:
`[job_name]_teamcity_build_[build_number] + timestamp`

You can edit the scan name, but a timestamp will automatically be appended regardless.

You can choose to run a Discovery scan or Vulnerability scan. The default is Vulnerability scan.

Next, configure optional scan parameters.

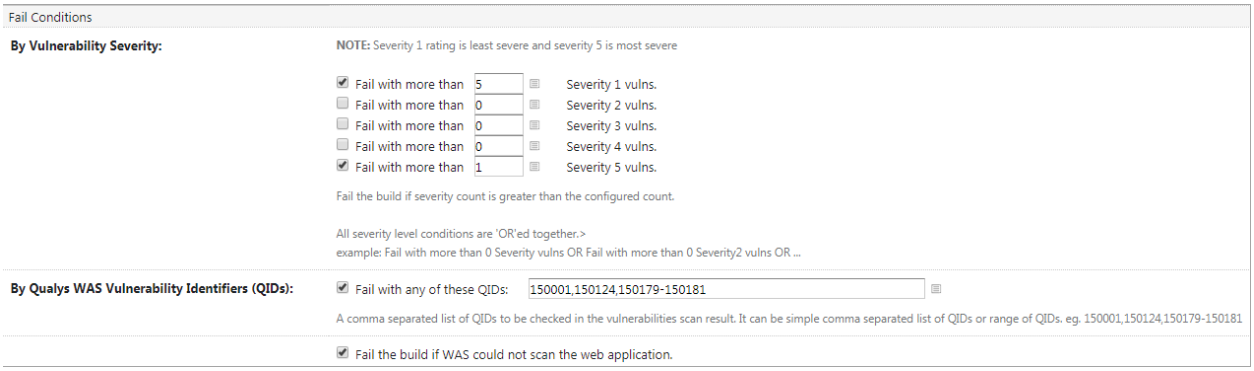


Authentication Record – You can choose to run the scan without authentication (the default) but keep in mind the scanner will not be able to log into the web application and test the authenticated surface area of the application in that case. You may instead want to select "Use Default", in which case the default authentication record for the web app in WAS (if any) will be used. Optionally, you can also select the Other option and choose a specific authentication record ID if desired.

Option Profile – The option profile contains the various scan settings such as the vulnerability types that should be tested (detection scope), scan intensity, error thresholds, etc. Selecting "Use Default" will use the default option profile for the web app in WAS. This is the recommended setting; however, you can also select the “Other” option and choose a specific option profile ID if desired.

Cancel Options – The default is not to cancel the scan, in which case the scan will run to completion. However, you can choose to cancel the scan after a set number of hours. Keep in mind you may not get any results if the scan is canceled before finishing.

Next, configure the pass/fail criteria for a build.



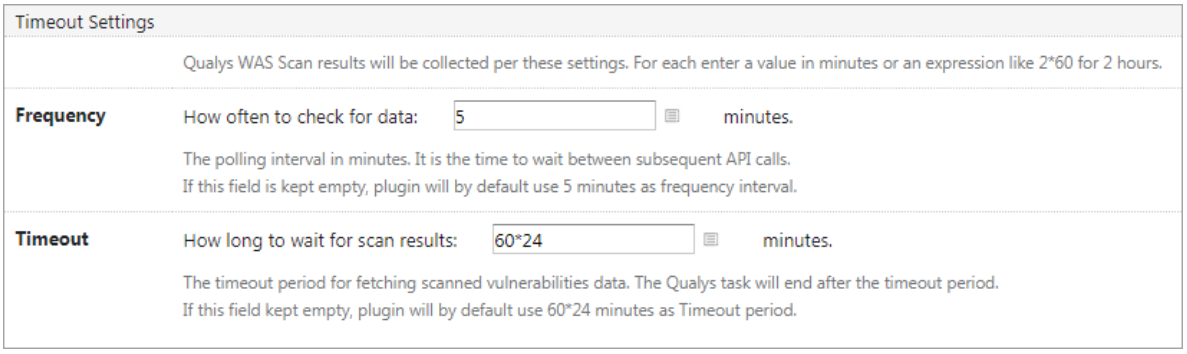
You can set conditions to fail a build by 1) Vulnerability Severity, 2) Qualys WAS Vulnerability Identifiers (QIDs). You may also choose to fail the build in case the Plugin initiates the scan but WAS module could not complete this scan due to some issues such as scanners not found and so on.

To fail the build by vulnerability severity, specify the count of vulnerabilities for one or more severity types. A build will fail if in scan results the number of detections exceeds the number specified for one or more severity types. For example, to fail a build if severity 5 vulnerabilities count is more than 2, select the “Fail with more than severity 5” option and specify 2.

Note that a Qualys severity “5” rating is the most dangerous vulnerability while severity “1” is the least.

Similarly, to fail a build by QIDs, select “Fail with any of these QIDs” check box and specify one or more QIDs.

Next, configure scan status polling frequency and timeout duration for the scan.



In the Timeout settings, specify the polling frequency in minutes for collecting the WAS scan status data and the timeout duration for a running scan.

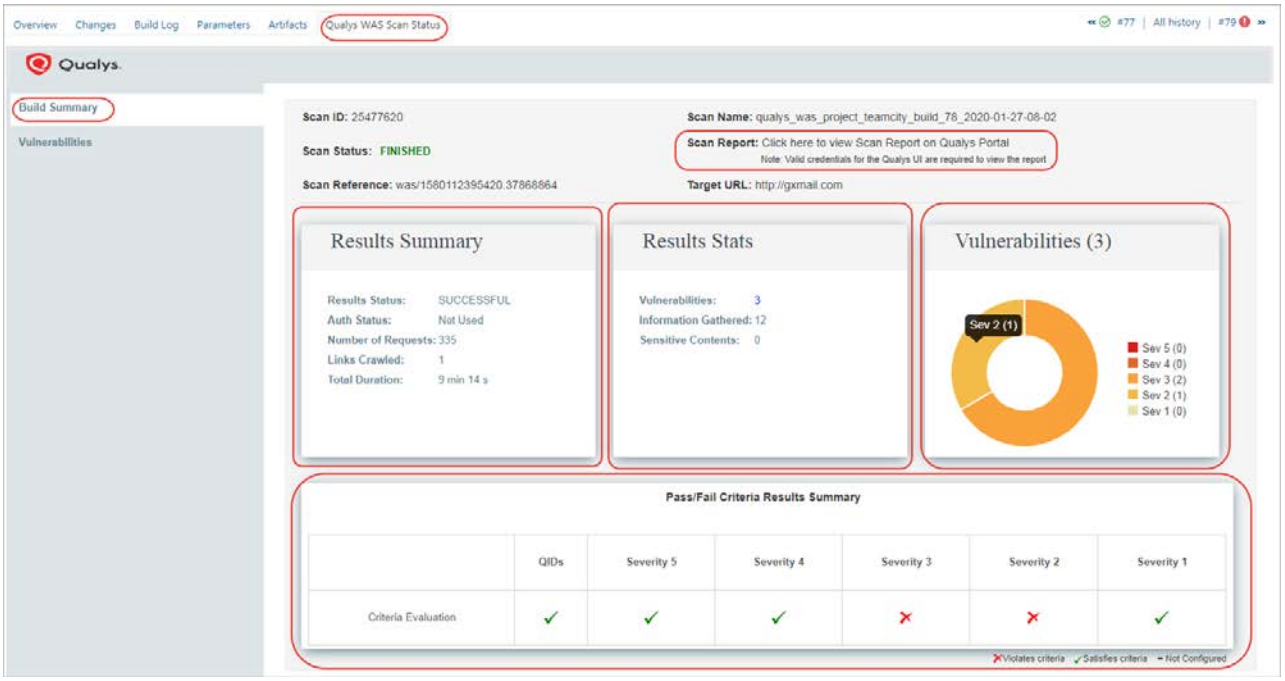
Click Save to save the Web application scanning configurations.

Qualys WAS Scan Status

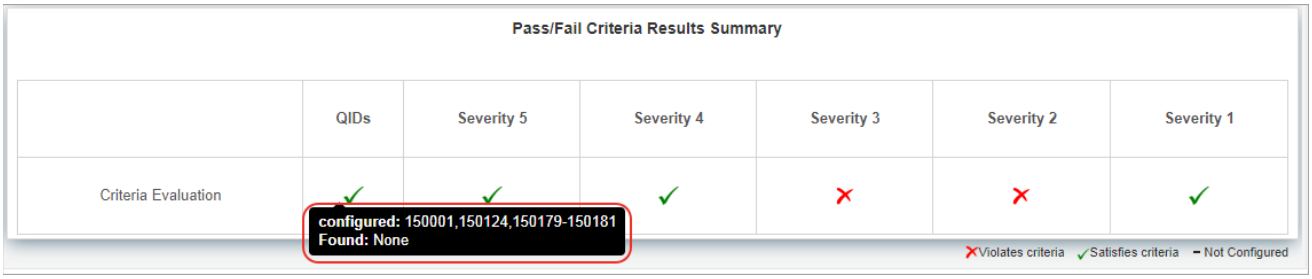
After the scan completes, the Qualys WAS Scan Status tab shows the scan results for the web application in the Build Summary tab. In the header of the scan results, we show you ScanID, scan name and scan status (finished/canceled). You can click the link shown in the Scan Report field to view the detailed WAS scan report on the Qualys portal.

We also have these sections. The Results Summary section shows the success/fail status of web application scanning with other details related to scanning. 2) Results Stats section shows the counts of different types of vulnerabilities found in the scan and 3) Vulnerabilities section shows the total number of vulnerabilities found by severity in a graphical chart view. Move the mouse over the different colored sections of the chart to view the vulnerability counts for various severity types.

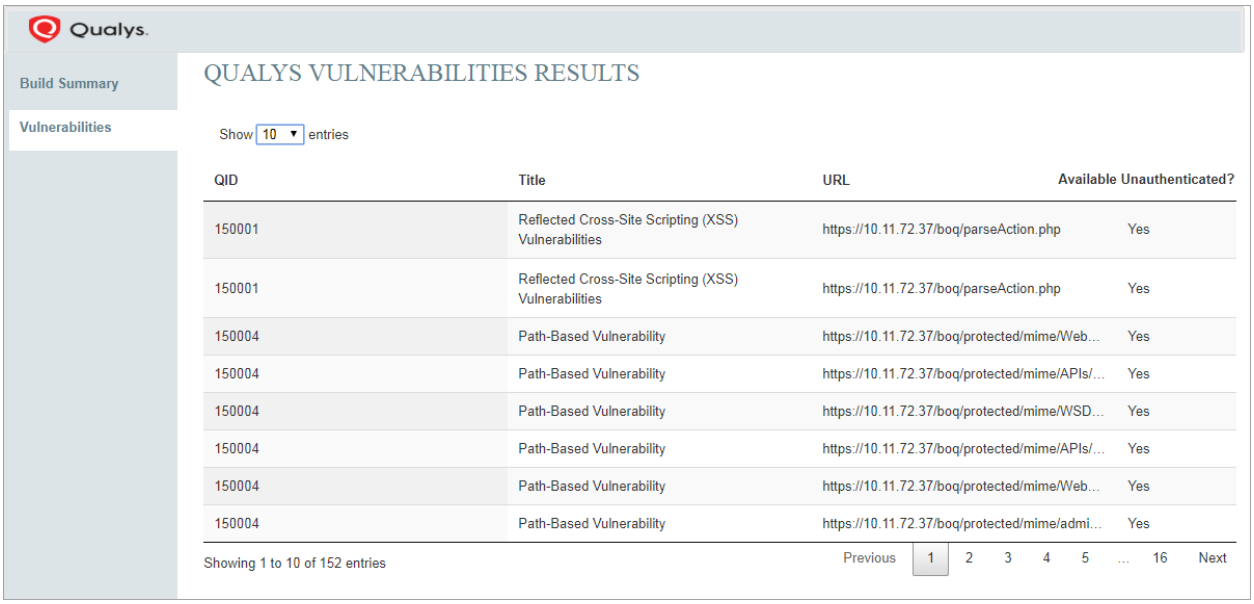
Below these sections is the Pass/Fail Criteria Results Summary section that shows the pass/fail criteria and whether they are violated or satisfied. When the criteria are violated, the ✗ icon is shown while for satisfied criteria, the ✓ icon is shown.



Move the mouse over the ✗ and ✓ icons to view the value that you have configured for the criteria, and the actual value obtained after the scan.



The Vulnerabilities tab is available to provide you the details of vulnerabilities, such as QIDs, vulnerability titles, URLs where the vulnerabilities occur and authentication status.



Troubleshooting

You entered valid Qualys credentials, but the drop-down menu to select a Web application is empty or does not show the desired Web application.

This issue occurs when the Qualys account provided does not have proper role or scope to access the web application you wish to scan. Ensure that the account has been set up with the required roles and scope to access the desired Web application.

You entered valid Qualys credentials, but the drop-down menu for Authentication Record Name or Profile Name is empty or does not show the desired item.

This issue occurs when the Qualys account provided does not have proper role or scope to access the auth record or option profile you wish to use. Ensure that the account has been set up with the required roles and scope to access the desired authentication record or option profile.

URL to the Qualys API Server

The Qualys API URL you should use for API requests depends on the Qualys platform where your account is located.

Click here to identify your Qualys platform and get the API URL.