Qualys Web App Scanning Connector for Bamboo

User Guide

Version 1.0.2

July 3, 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 Bamboo.

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/

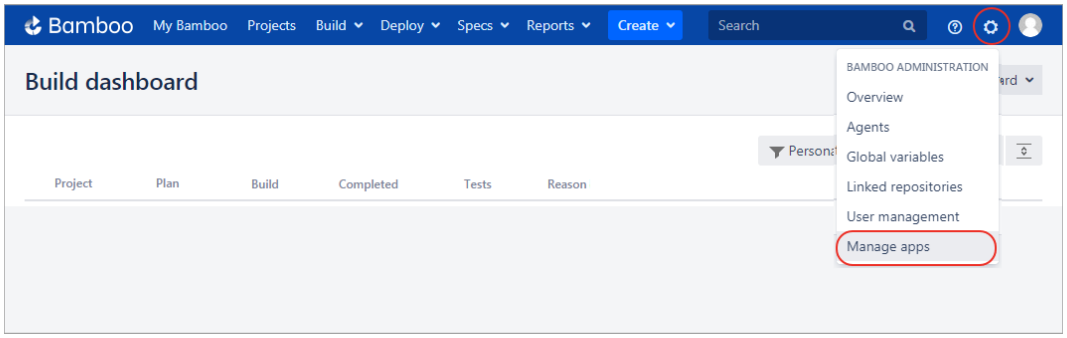
Introduction to Qualys Web App Scanning Connector for Bamboo

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.

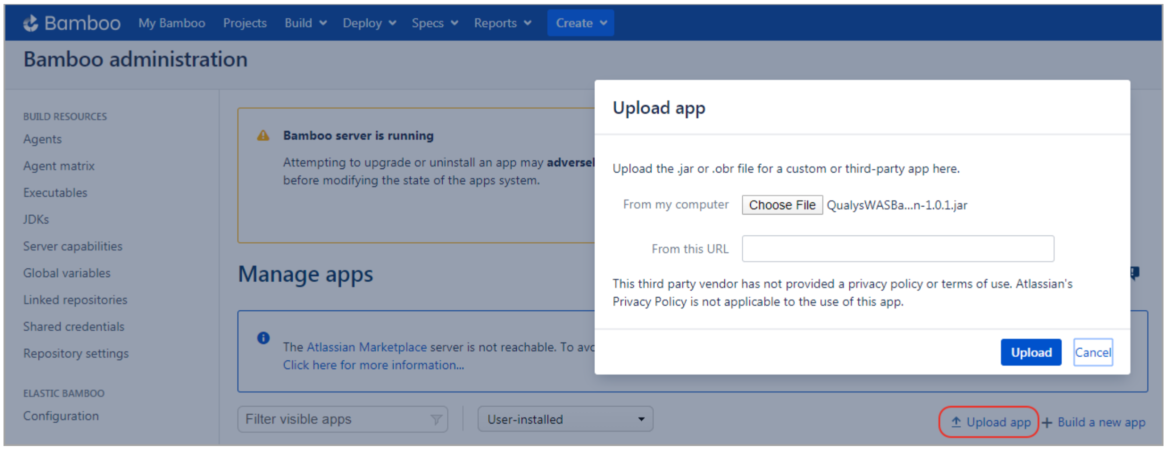
We'll help you: Install the Plugin | Configure the Plugin

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 Bamboo and on the application menu bar, click the Administration settings ⚙ icon and then choose Manage apps.



On the Manage apps page, click the Upload app link. On the Upload app screen, choose the plugin JAR file and click Upload.



Bamboo server is running

Attempting to upgrade or uninstall an app may adversel before modifying the state of the apps system.

The Atlassian Marketplace server is not reachable. To avc Click here for more information...

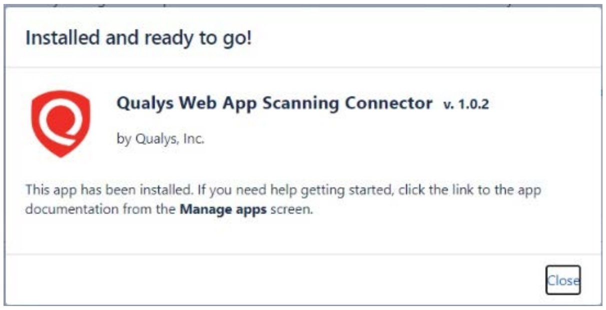
Upload the .jar or .obr file for a custom or third-party app here.

From my computer: QualysWASBa...n-1.0.1.jar

From this URL:

This third party vendor has not provided a privacy policy or terms of use. Atlassian's Privacy Policy is not applicable to the use of this app.

A confirmation message is shown after plugin installation is complete.



Installed and ready to go!

Qualys Web App Scanning Connector v. 1.0.2

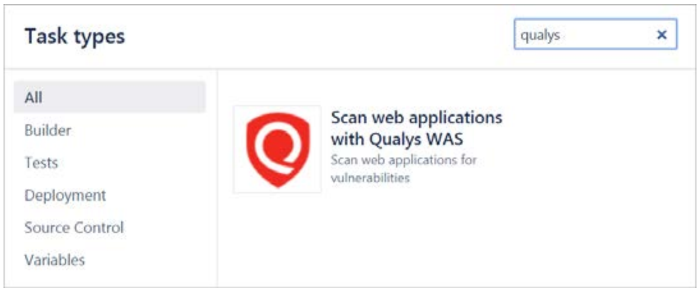
by Qualys, Inc.

This app has been installed. If you need help getting started, click the link to the app documentation from the **Manage apps** screen.

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

Configure the Plugin

Navigate to the Actions menu > Configure plan and select "Scan web applications with Qualys WAS" task type.



Task types

qualys

Scan web applications with Qualys WAS

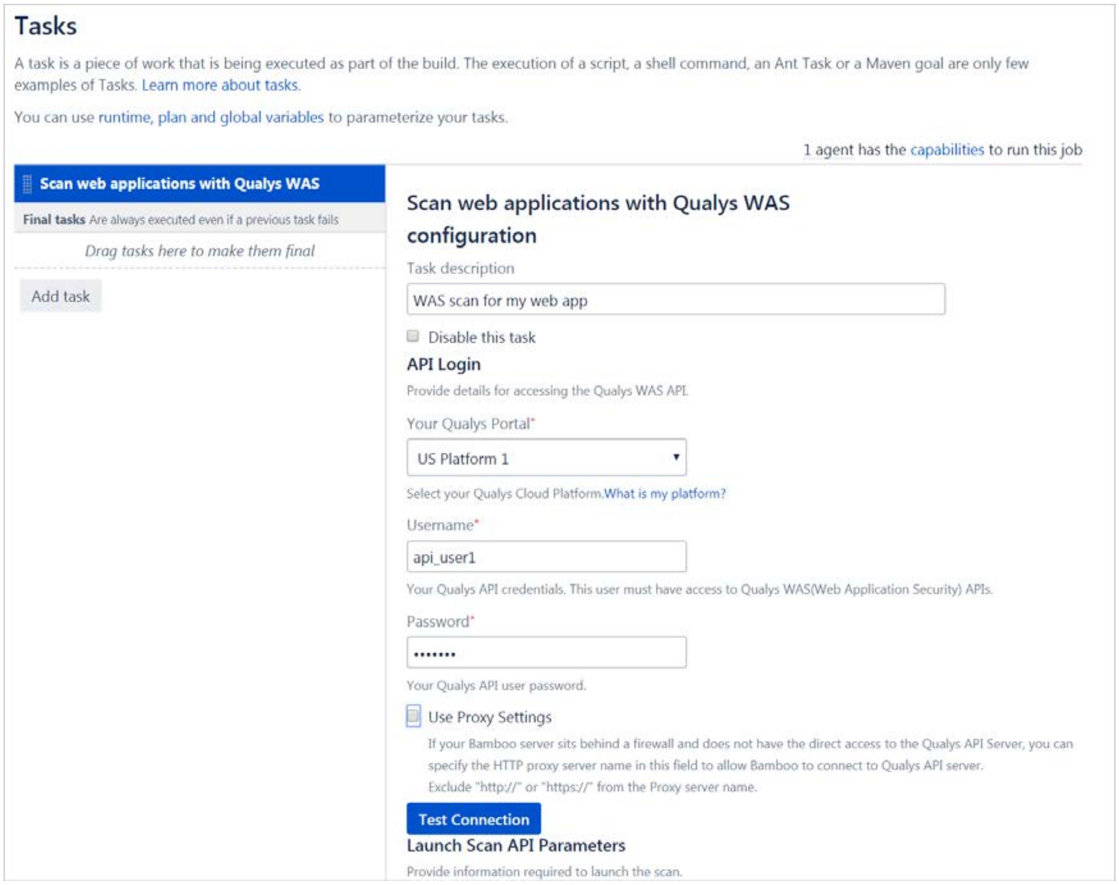
Scan web applications for vulnerabilities

In the configuration form, provide a description for the task. Next, go to the Qualys API Credentials section.

This step is to confirm that Bamboo 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 Bamboo instance does not have direct Internet access and a proxy is required, click the "Use Proxy Settings" checkbox and enter the required information.



Tasks

A task is a piece of work that is being executed as part of the build. The execution of a script, a shell command, an Ant Task or a Maven goal are only few examples of Tasks. Learn more about tasks.

You can use runtime, plan and global variables to parameterize your tasks.

1 agent has the capabilities to run this job

Scan web applications with Qualys WAS
Final tasks Are always executed even if a previous task fails
Drag tasks here to make them final
Add task

Scan web applications with Qualys WAS configuration

Task description: WAS scan for my web app

□ Disable this task

API Login

Provide details for accessing the Qualys WAS API.

Your Qualys Portal*: US Platform 1

Select your Qualys Cloud Platform.What is my platform?

Username*: api_user1

Your Qualys API credentials. This user must have access to Qualys WAS(Web Application Security) APIs.

Password*: •••••••

Your Qualys API user password.

□ Use Proxy Settings

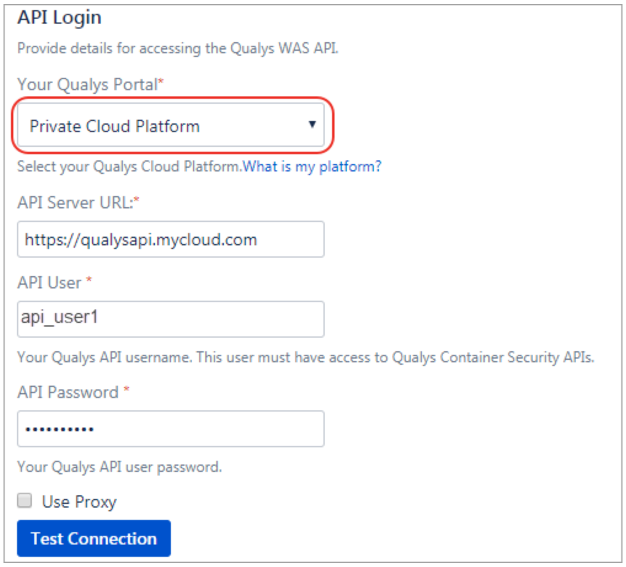
If your Bamboo server sits behind a firewall and does not have the direct access to the Qualys API Server, you can specify the HTTP proxy server name in this field to allow Bamboo to connect to Qualys API server.
Exclude "http://" or "https://" from the Proxy server name.

Launch Scan API Parameters

Provide information required to launch the scan.

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.



API Login

Provide details for accessing the Qualys WAS API.

Your Qualys Portal*: Private Cloud Platform

Select your Qualys Cloud Platform.What is my platform?

API Server URL:*: https://qualysapi.mycloud.com

API User *: api_user1

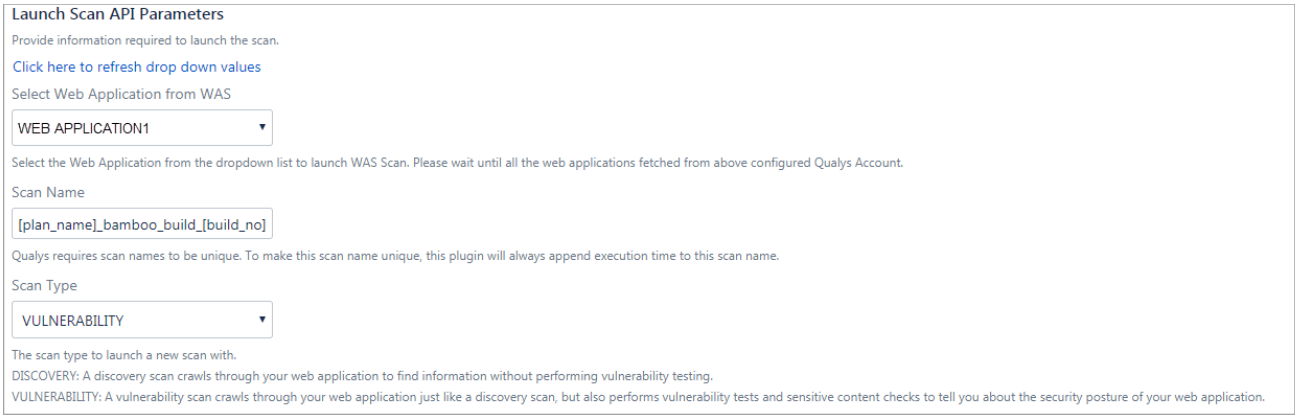
Your Qualys API username. This user must have access to Qualys Container Security APIs.

API Password *: ••••••••••

Your Qualys API user password.

□ Use Proxy

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



Launch Scan API Parameters

Provide information required to launch the scan.

Click here to refresh drop down values

Select Web Application from WAS

WEB APPLICATION1 ▾

Select the Web Application from the dropdown list to launch WAS Scan. Please wait until all the web applications fetched from above configured Qualys Account.

Scan Name

[plan_name]_bamboo_build_[build_no]

Qualys requires scan names to be unique. To make this scan name unique, this plugin will always append execution time to this scan name.

Scan Type

VULNERABILITY ▾

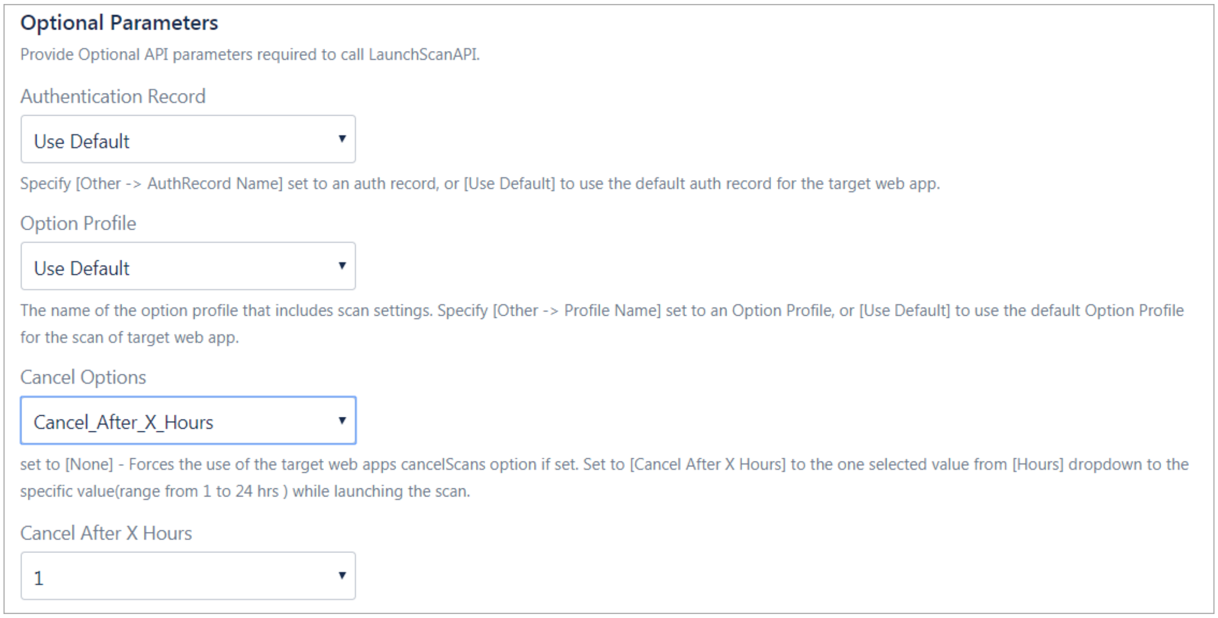
The scan type to launch a new scan with.
DISCOVERY: A discovery scan crawls through your web application to find information without performing vulnerability testing.
VULNERABILITY: A vulnerability scan crawls through your web application just like a discovery scan, but also performs vulnerability tests and sensitive content checks to tell you about the security posture of your web application.

By default, the WAS scan name will be:
`[plan_name]_bamboo_build_[build_no] + 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.



Optional Parameters

Provide Optional API parameters required to call LaunchScanAPI.

Authentication Record

Use Default ▾

Specify [Other -> AuthRecord Name] set to an auth record, or [Use Default] to use the default auth record for the target web app.

Option Profile

Use Default ▾

The name of the option profile that includes scan settings. Specify [Other -> Profile Name] set to an Option Profile, or [Use Default] to use the default Option Profile for the scan of target web app.

Cancel Options

Cancel_After_X_Hours ▾

set to [None] - Forces the use of the target web apps cancelScans option if set. Set to [Cancel After X Hours] to the one selected value from [Hours] dropdown to the specific value(range from 1 to 24 hrs) while launching the scan.

Cancel After X Hours

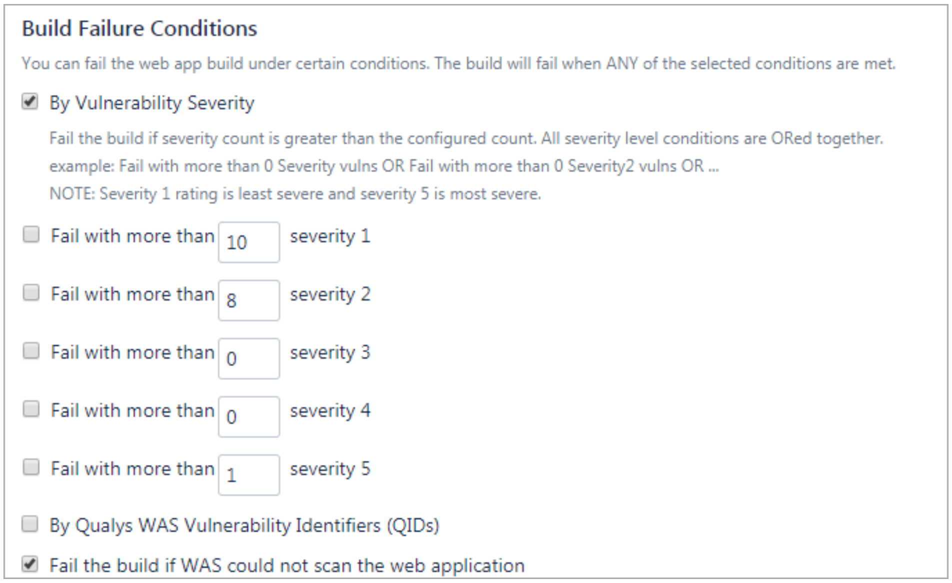
1 ▾

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.



Build Failure Conditions

You can fail the web app build under certain conditions. The build will fail when ANY of the selected conditions are met.

☑ By Vulnerability Severity

Fail the build if severity count is greater than the configured count. All severity level conditions are ORed together.
example: Fail with more than 0 Severity vulns OR Fail with more than 0 Severity2 vulns OR ...
NOTE: Severity 1 rating is least severe and severity 5 is most severe.

☐ Fail with more than 10 severity 1

☐ Fail with more than 8 severity 2

☐ Fail with more than 0 severity 3

☐ Fail with more than 0 severity 4

☐ Fail with more than 1 severity 5

☐ By Qualys WAS Vulnerability Identifiers (QIDs)

☑ Fail the build if WAS could not scan the web application

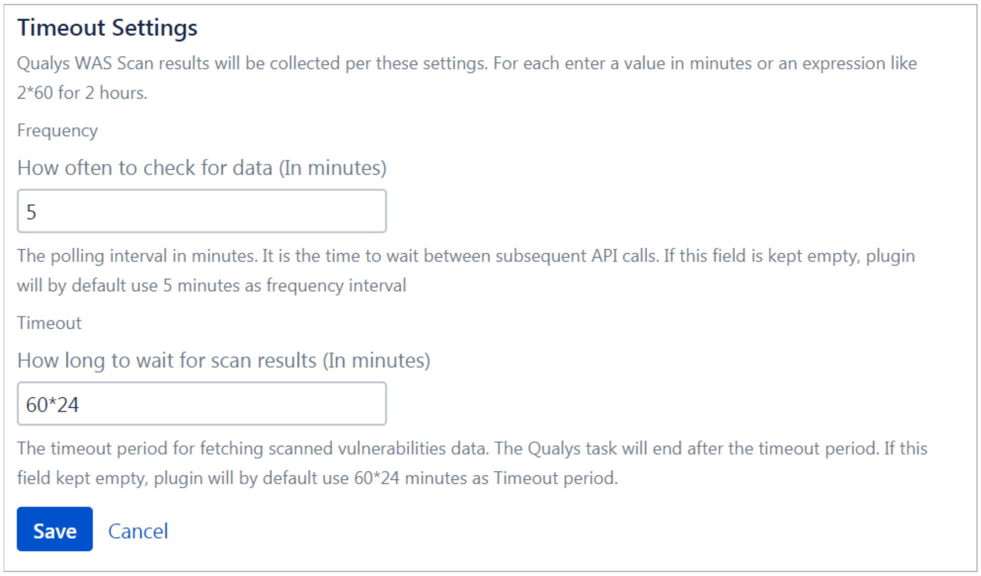
You can set conditions to fail a build by 1) Vulnerability Severity, 2) Qualys WAS Vulnerability Identifiers (QIDs). You may also choose to fail the build in case the Plugin initiates the scan but WAS module could not complete this scan due to some issues such as scanners not found and so on. If any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

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 “By Qualys WAS Vulnerability Identifiers (QIDs)” option and specify one or more QIDs.

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



Timeout Settings

Qualys WAS Scan results will be collected per these settings. For each enter a value in minutes or an expression like 2*60 for 2 hours.

Frequency

How often to check for data (In minutes)

5

The polling interval in minutes. It is the time to wait between subsequent API calls. If this field is kept empty, plugin will by default use 5 minutes as frequency interval

Timeout

How long to wait for scan results (In minutes)

60*24

The timeout period for fetching scanned vulnerabilities data. The Qualys task will end after the timeout period. If this field kept empty, plugin will by default use 60*24 minutes as Timeout period.

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.

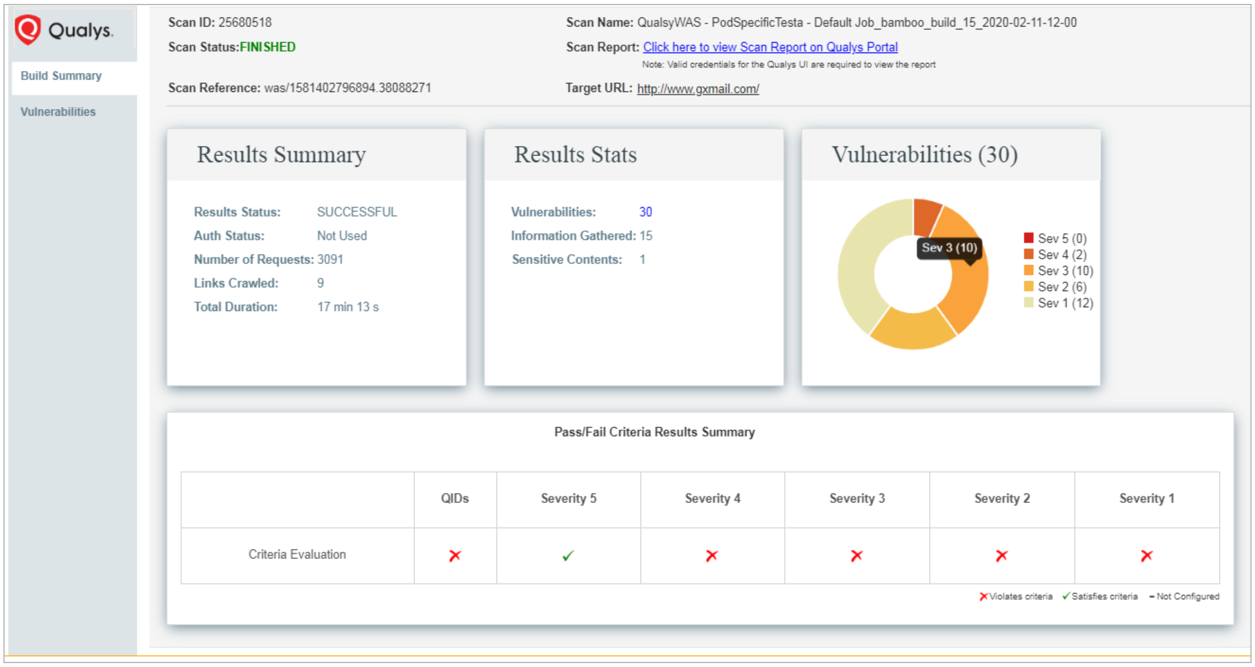
Click Save to save the Web application scanning configurations.

WAS Scan Status Summary Report

After the scan completes, the Qualys WAS Result tab will show the scan result 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.

The report also has other sections. 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 different colored sections of the graph to view the vulnerability counts for different 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.



Scan ID: 25680518

Scan Status: FINISHED

Scan Reference: was/1581402796894.38088271

Scan Name: QualsyWAS - PodSpecificTesta - Default Job_bamboo_build_15_2020-02-11-12-00

Scan Report: Click here to view Scan Report on Qualys Portal

Note: Valid credentials for the Qualys UI are required to view the report

Target URL: http://www.gxmail.com/

Results Summary

Results Status:	SUCCESSFUL
Auth Status:	Not Used
Number of Requests:	3091
Links Crawled:	9
Total Duration:	17 min 13 s

Results Stats

Vulnerabilities:	30
Information Gathered:	15
Sensitive Contents:	1

Vulnerabilities (30)

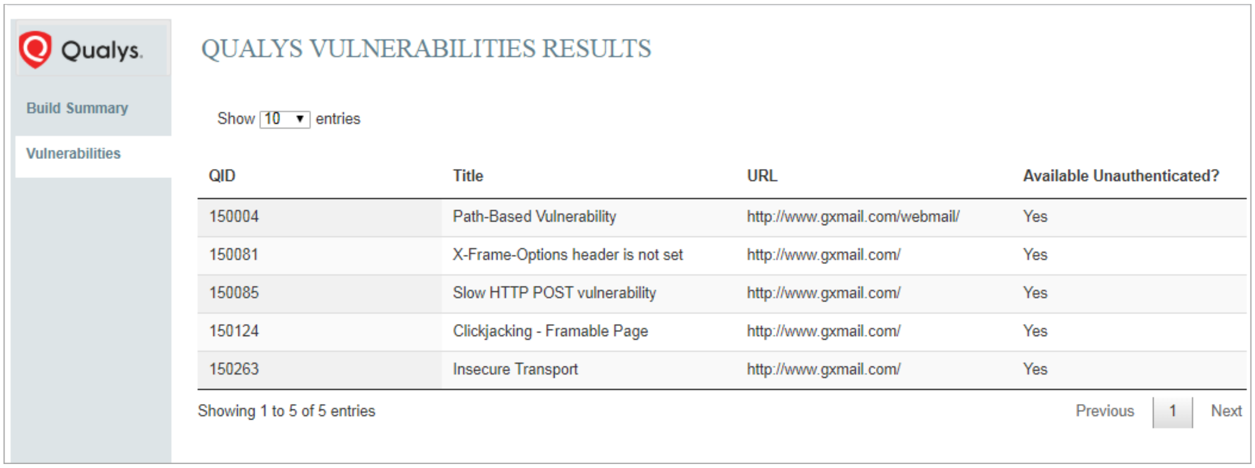
Pass/Fail Criteria Results Summary

	QIDs	Severity 5	Severity 4	Severity 3	Severity 2	Severity 1
Criteria Evaluation	✗	✓	✗	✗	✗	✗

✗ Violates criteria ✓ Satisfies criteria – Not Configured

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.



QUALYS VULNERABILITIES RESULTS

Show 10 entries

QID	Title	URL	Available Unauthenticated?
150004	Path-Based Vulnerability	http://www.gxmail.com/webmail/	Yes
150081	X-Frame-Options header is not set	http://www.gxmail.com/	Yes
150085	Slow HTTP POST vulnerability	http://www.gxmail.com/	Yes
150124	Clickjacking - Framable Page	http://www.gxmail.com/	Yes
150263	Insecure Transport	http://www.gxmail.com/	Yes

Showing 1 to 5 of 5 entries

Known Issues

'Run' and 'Action' drop-downs and these tabs: Summary, Tests, Commits, Artifacts, Logs and Metadata on 'Qualys WAS Scan Result' page may disappear upon refreshing/reloading the page.

The workaround is:

- To get the drop-downs, click on the bamboo plan name at the top of the page. You will see the drop-downs on the plan page.

- To get the tabs, click on the build number.

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.

What's New

Improvements in 1.0.2

- With this release, Qualys Web App Scanning Connector now supports Bamboo server versions up to v7.0.4.