Qualys Cloud Platform v2.x

Release Notes

Version 2.41
September 18, 2019

Here's what's new in Qualys Cloud Suite 2.41!

AV AssetView

Tag assets from Global IT Asset Inventory

WAF Web Application Firewall

Configure to keep the Accept-Encoding Header in Request

WAS Web Application Scanning

Support for Postman Collection File Upload

Full Path of Detections in Reports (PDF and HTML)

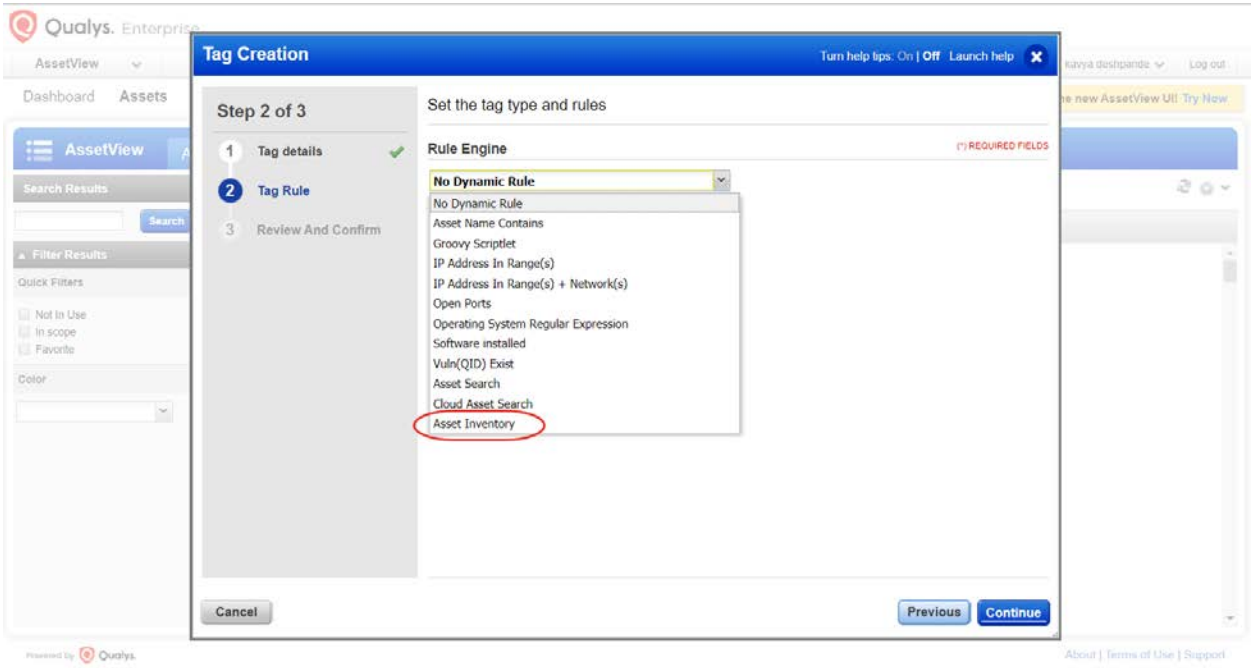
Qualys Cloud Platform 2.41 brings you many more Improvements and updates! Learn more

AV **AssetView**

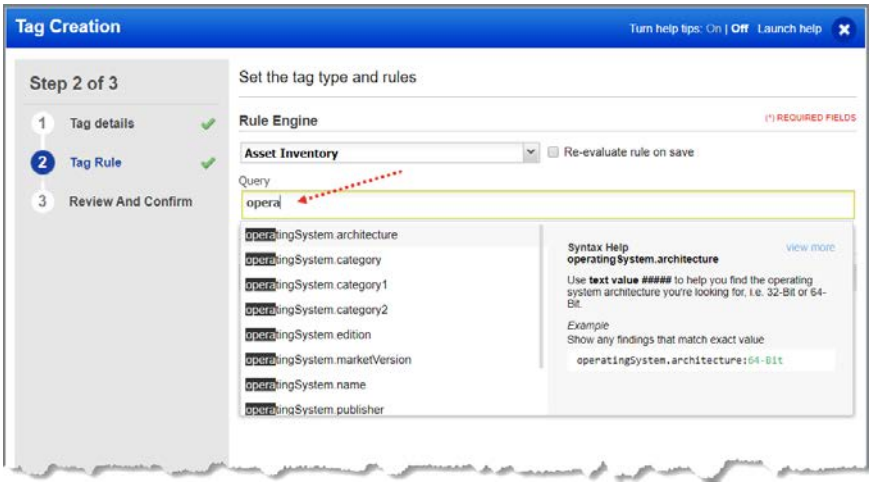
Tag assets from Global IT Asset Inventory

You can now apply tags to organize assets from Global IT Asset Inventory. Tagging assets provides a flexible and scalable way to automatically discover and organize the assets.

1) Click New Tag, 2) choose the Asset Inventory rule, and 3) enter your query.



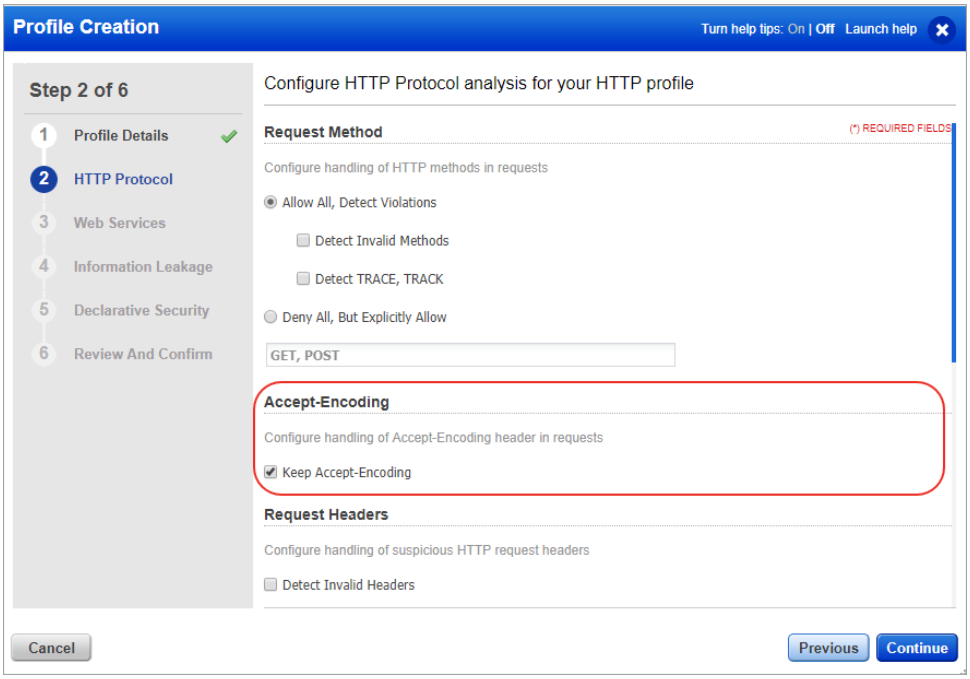
Just start typing in the Query field and we'll show you the Asset Inventory attributes you can search.



WAF **Web Application Firewall**

Configure to keep the Accept-Encoding Header in Request

You can now create an HTTP profile for your web application to specify the WAF application to either retain or remove the Accept-Encoding header field in requests. If you choose to retain the header field then WAF will keep the header field in requests that contain this header field while forwarding the requests to your web application. By default, WAF will remove this header field.



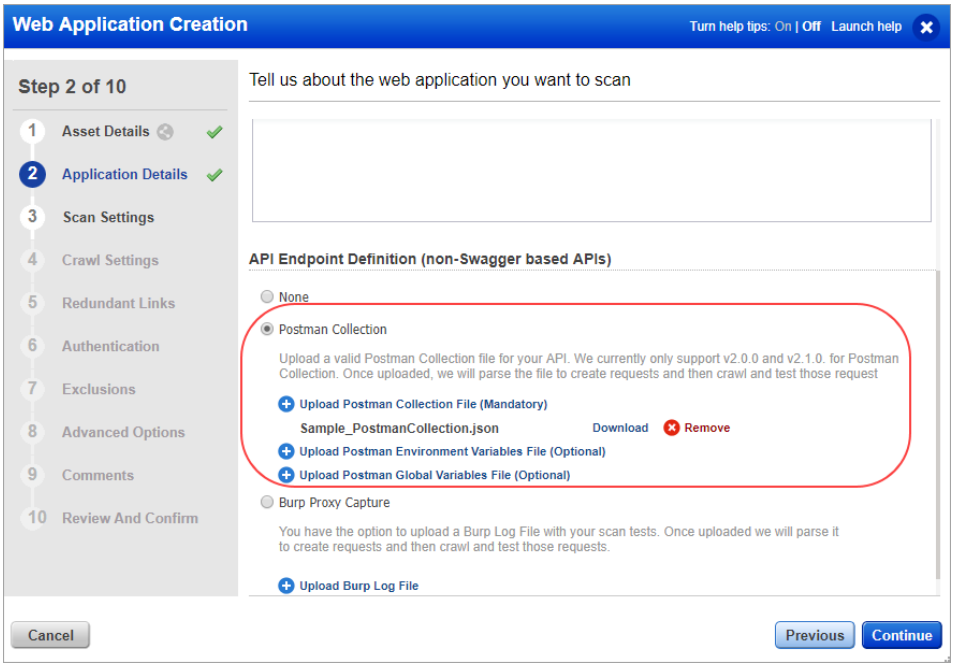
To configure accept encoding, go to Security > HTTP Profiles > Create or Edit an HTTP Profile.

WAS **Web Application Scanning**

Support for Postman Collection File Upload

We now support security test of REST APIs exported using Postman tool.

Postman tool, used to test the REST APIs, has the facility to export and share the REST APIs. Postman Collection file is the group of REST APIs. Just upload the Postman Collection exported file in JSON format and we will then scan for vulnerabilities.



Go to Web Applications > New Web Application. After you define the mandatory parameters in Asset Details, go to Application Details and select Postman Collection in API Endpoint Definition (non-Swagger based APIs).

Upload the Postman Collection File (mandatory) and click Continue. We also support upload of Postman Environmental Variables and Postman Global Variables file.

Note: We currently only support v2.0.0 and v2.1.0. for Postman Collection. The size of the file you upload should not exceed 5 MB.

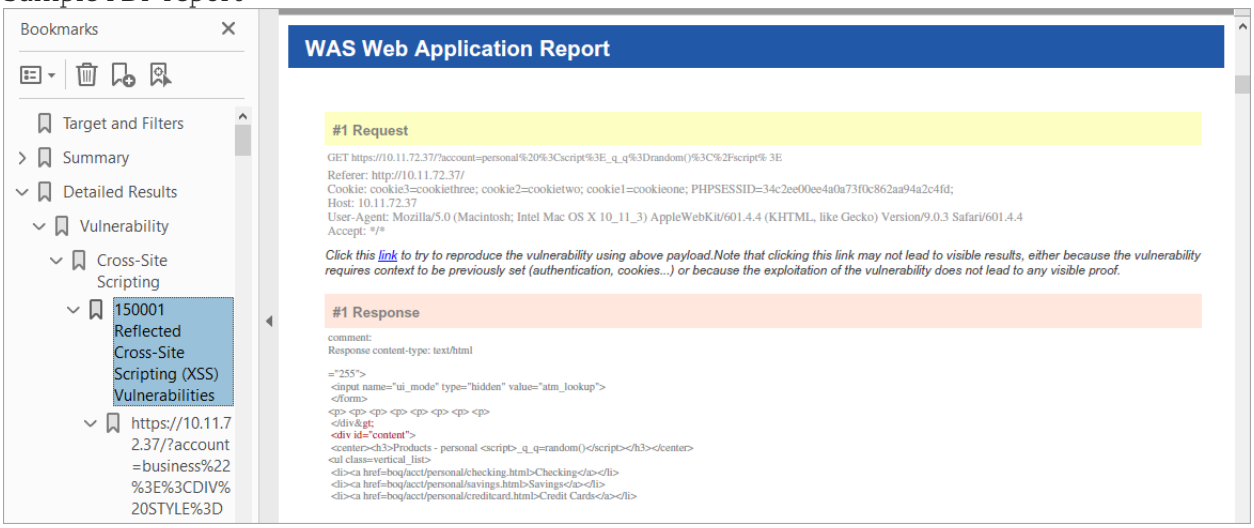
Full Path of Detections in Reports (PDF and HTML)

We provided you with complete and raw HTTP request for detections. Now, the reports downloaded in PDF and HTML format also display complete and raw HTTP request for detections (except for Information Gathered (IG) vulnerabilities).

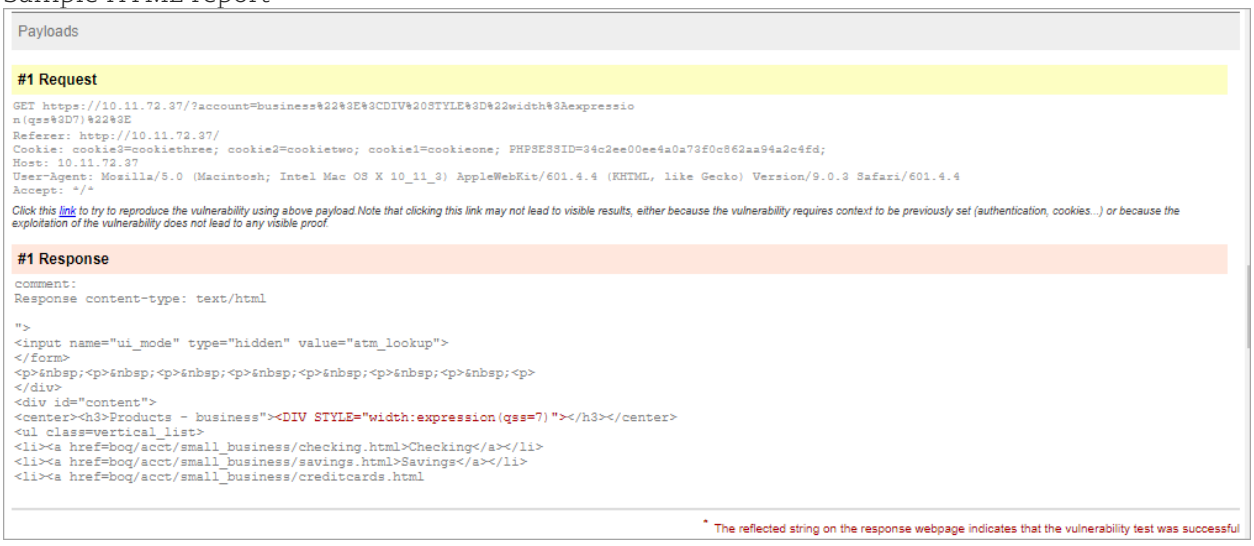
Earlier, WAS reports in PDF or HTML format displayed link, method, POST data, headers and snippets of the response body. Now, the downloaded reports (PDF and HTML) display full request headers and full request body for vulnerabilities. The complete requests and responses will help you to reproduce or validate the issue.

Examples:

Sample PDF report



Sample HTML report



Issues addressed in this release

Qualys Cloud Platform 2.41 brings you many more improvements and updates.

AV AssetView

- Fixed an issue in AssetView where incorrect OS icon was shown for Cisco assets.

CA Cloud Agent

- Fixed an issue in Cloud Agent where incorrect messages were shown while activating agents for modules when module licenses are expired.
- You can now assign the UDC manifest to all agents at once.
- Cloud Agent action logs will now show actions performed on Activation Keys.
- Fixed an issue in Cloud Agent where the MAC VERSION DISTRIBUTION widget on the dashboard was not showing any data.

VM VM Dashboard

- Fixed an issue in VM Dashboard where upon applying the tag filter, trending data was getting displayed with vulnerability count instead of displaying only the vulnerability count.

SAQ Security Assessment Questionnaire

- Fixed the error message shown while updating a campaign for which the template is deleted or is in draft mode.
- Security Assessment Questionnaire now supports sending email to email addresses with top level domain length up to 8 characters.

WAS Web Application Scanning

- We have now fixed an issue so that the downloaded reports in PDF and HTML format now display correct data and the data is in sync with the online report.
- Creating schedules and reports using API with ALL option for tags reflected ANY on UI. This is now fixed to correctly reflect ALL option in tags during schedule and report creation from API.
- We have now fixed the broken link in Vulnerability details for QID 150085 so that the link now opens the correct web page.
- We have updated the WAS online help to reflect correct information related to scan results storage settings.

- We have now fixed an issue so that error is not displayed during retest of a finding due to long scanner name. We have resolved the issue as we are able to retest findings on scanners with long size name.
- Clicking Save during update of Global Settings temporarily disables all the options to avoid duplicate entries caused by multiple clicks in single attempt. Once the update is complete, all options are available for editing again.
- The error message during catalog and maps update was displayed inconsistently. We have now fixed the issue by increasing the character length for error message to 1000 characters. The error message if displayed is consistent across various users.
- We have now resolved an exception so that the finding could be retested correctly without the exception 'Vulnerable URL cannot be found anymore'. For example, QID 150001.
- The cookie related vulnerability details for QIDs 150103, 150120, 150121, 150122, 150123, 150159, 150160, and 150161 for existing scans and web applications is now shown correctly.
- The preview of schedules with authentication records now display correct details. Earlier, the preview displayed "None" despite the schedule having authentication records.
- We have now extended our support so that the Detection Datalist report download successfully works for up to 10000 records.
- We have now fixed data inconsistency for "Function" and "AJAX request" column in downloaded reports with CSV format.
- We have fixed the font anomalies for Web Application Details section of the appendix in the scan report (both PDF and HTML format).
- We have fixed an issue where updating web applications that contain attributes is done successfully. Earlier, web applications with attributes were not updated correctly.

Qualys Cloud Platform

- Fixed an issue is Asset Details > Asset Summary where Last System Boot was showing incorrect date-time.
- Fixed an issue where the Host Asset update API (/qps/rest/2.0/update/am/hostasset) was throwing an error if the POST request contained a large number of Asset IDs.
- Users will now be able to run Azure connectors successfully through the Run Connector API (/qps/rest/2.0/run/am/assetdataconnector).
- Fixed an issue where AWS connectors were getting stuck in the "Synchronizing" state and as a result stale assets were seen in the Assets list.