Web Application Scanning (Beta)

Getting Started Guide

September 21, 2020

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

Table of Contents

About this Guide

Welcome to Qualys Web Application Scanning (WAS)! We'll help you get acquainted with the Qualys solutions for scanning your web applications for vulnerabilities using the Qualys Cloud Security Platform.

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 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 online support information at www.qualys.com/support/.

WAS Community

To know more about latest features, discussions, documents and videos related to WAS, you can access Qualys WAS Community page.

Welcome to WAS

Qualys Web Application Scanning (WAS) provides organizations with the ease of use, centralized management and integration capabilities they need to keep the attackers at bay and their web applications secure.

Qualys WAS is an automated scanner that uses fault injection tests to find vulnerabilities. It inserts specially crafted character strings into your application form fields. WAS then examines the responses from your web application to determine the existence of vulnerability. You can see what is sent and how your application responded in WAS's reporting capabilities.

Qualys WAS enables organizations to scan their web applications for vulnerabilities. It assess, track and remediate web application vulnerabilities.Qualys WAS enables organizations to assess, track and remediate web application vulnerabilities.

Key Features

- Crawl web applications (Intranet, Internet) and scan them for vulnerabilities
- Fully interactive UI with flexible workflows and reporting
- Identify web applications' handling of sensitive or secret data
- Customize: exclude/allow lists, robots.txt, sitemap.xml and more
- Supports common authentication schemes
- View reports with recommended security coding practice and configuration

Robust Scalable Scanning Capabilities

- Supports scanning HTML web applications with JavaScript and embedded Flash
- Comprehensive detection of custom web application vulnerabilities including OWASP Top 10 Vulnerabilities
- Differentiates exploitable fault-injection problems from simple information disclosure
- Profiles custom web application behaviors
- Configures scanning performance with customizable performance level

Qualys Cloud Platform - Benefits for Users

New technologies implemented in the Java-based backend offer many benefits for users:

- UI with dynamic and interactive interfaces, wizards and new report templates to present scan data with a wide range of presentation options.
- We have integrated Unified Dashboard (UD) with WAS. UD brings information from all Qualys applications into a single place for visualization.
- Customizable template-driven reporting engine outputs reports in a variety of formats (html, pdf, encrypted pdf, ppt, xml, cvs).

- Fast searching of several extensive Qualys data sets related to web applications and detections using search tokens.

- Create and manage tags (static and dynamic) to group and organize web applications.

REST API Scanning, CI/CD Integration, and More

We support Swagger version 2.0, allowing DevOps teams to streamline assessments of REST APIs and get faster visibility of the security posture of mobile application backends and Internet of Things (IoT) services. Additionally, a new native plugin for Jenkins delivers automated vulnerability scanning of web applications for teams using the popular Continuous Integration/Continuous Delivery (CI/CD) tool. In tandem, customers can now leverage the new Qualys Browser Recorder, a free Google Chrome browser extension, to easily review scripts for navigating through complex authentication and business workflows in web applications.

- Scanning of Swagger-based Representational State Transfer (REST) APIs - In addition to scanning Simple Object Access Protocol (SOAP) web services, Qualys WAS leverages the Swagger specification for testing REST APIs. Users need to only ensure the Swagger version 2.0 file (JSON format) is visible to the scanning service, and the APIs will automatically be tested for common application security flaws.

- Enhanced API Scanning with Postman Support - Postman is a widely-used tool for functional testing of REST APIs. A Postman Collection is a file that can be exported from the tool that clubs together related requests (API endpoints) and share them with other users. These collections are exported in JSON format. With the release of Postman Collection support in Qualys WAS, customers have the option to configure their API scans using the Postman Collection for their API.

- Jenkins plugin - The Qualys WAS Jenkins plugin 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 thereby significantly reducing the cost of remediation compared to doing so later in the SDLC. Download the plugin here.

- Qualys Browser Recorder – This new Chrome extension allows users to record web browser activity and save the scripts for repeatable, automated testing. Scripts are played back in Qualys WAS, allowing the scanning engine to successfully navigate through complex authentication and business workflows. The Qualys Browser Recorder extension is free and available to anyone (not just Qualys customers) via the Chrome Web Store.

Adding Users

It's easy to add users to your Qualys subscription and grant them access to WAS. You'll need a Manager role to do this.

How do I add new users?

Use the New User work-flow provided in the Vulnerability Management application. Select VM/VMDR from the app picker and go to the Users section to create a new user. We'll walk you through the steps.

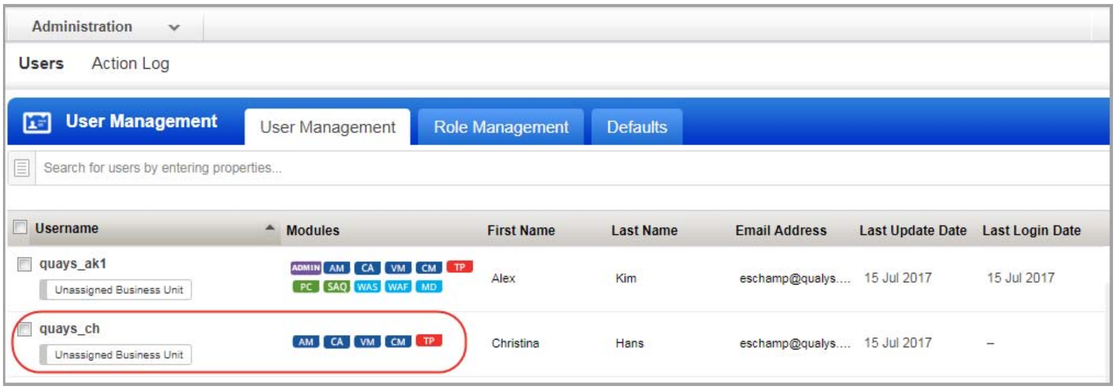
Viewing users, their roles and permissions

The Qualys Cloud Platform UI shows you all the users in your subscription, their assigned roles and permissions to the various applications which are enabled for your account. You'll notice newly added sub-accounts (Scanners, Readers, Unit Managers, etc) are not granted access to WAS automatically.

How to grant a user access to WAS?

Say you created a new user Christina Hans with the Scanner role and you want Christina to be able to scan web application for security risks using WAS.

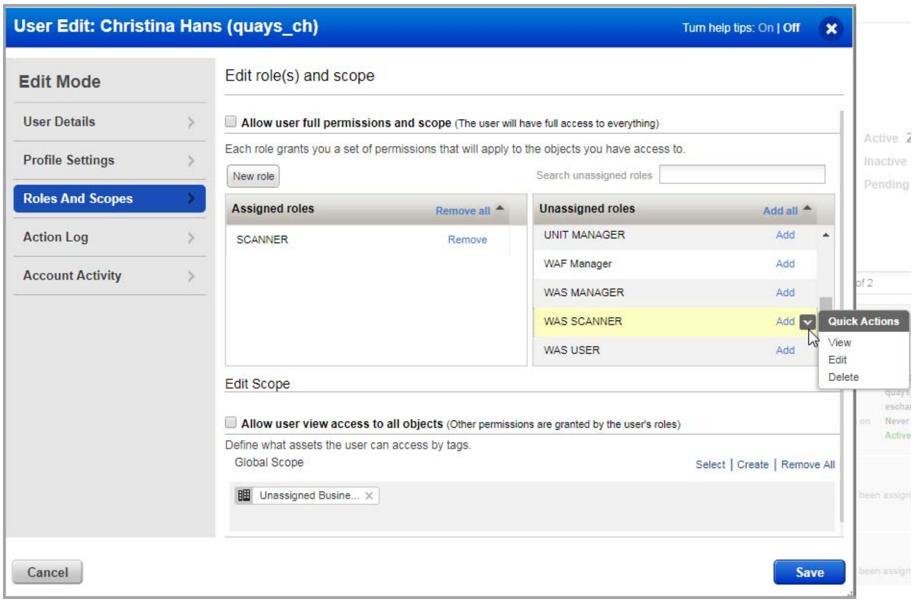
View the new user's permissions for applications with Qualys Cloud Platform. Go to the Administration utility. You'll notice for the new user WAS application is not listed.



Username	Modules	First Name	Last Name	Email Address	Last Update Date	Last Login Date
quays_ak1 Unassigned Business Unit	ADMIN AM CA VM CM TP PC SAQ WAS WAF MD	Alex	Kim	eschamp@qualys....	15 Jul 2017	15 Jul 2017
quays_ch Unassigned Business Unit	AM CA VM CM TP	Christina	Hans	eschamp@qualys....	15 Jul 2017	–

Edit the new user (select the user and pick Edit from the Quick Actions menu). Under Roles and Scopes the user is assigned SCANNER role for VM and/or PC scanning (depending on your subscription settings).

Qualys provides predefined WAS user roles to help you grant users WAS permissions easily. The predefined roles are WAS MANAGER, WAS SCANNER, WAS USER.



User Edit: Christina Hans (quays_ch) Turn help tips: On | Off

Edit Mode

- User Details
- Profile Settings
- Roles And Scopes
- Action Log
- Account Activity

Edit role(s) and scope

□ **Allow user full permissions and scope** (The user will have full access to everything)

Each role grants you a set of permissions that will apply to the objects you have access to.

New role   Search unassigned roles

Assigned roles	Remove all
SCANNER	Remove

Unassigned roles	Add all
UNIT MANAGER	Add
WAF Manager	Add
WAS MANAGER	Add
WAS SCANNER	Add
WAS USER	Add

Edit Scope

□ **Allow user view access to all objects** (Other permissions are granted by the user's roles)

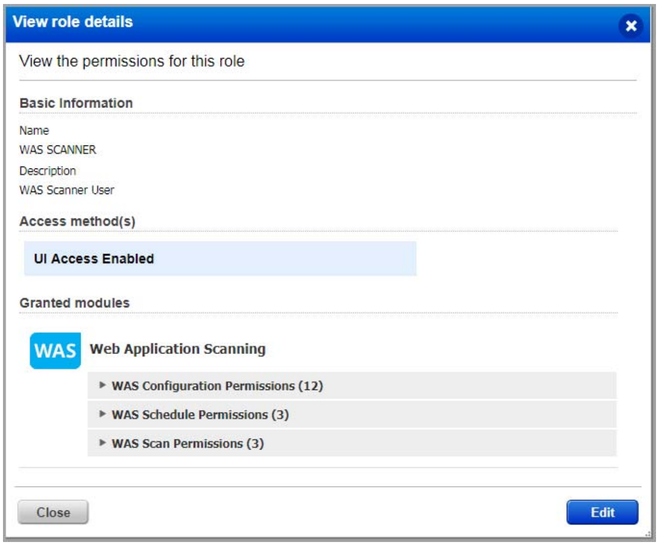
Define what assets the user can access by tags.

Global Scope   Select | Create | Remove All

Unassigned Busine...

Cancel   Save

Our user Christina has SCANNER role (for VM/PC) so we'll add WAS SCANNER role to her account. Select WAS SCANNER then pick View from the Quick Actions menu. You'll see WAS SCANNER permission groups and can drill down to see the role details. This role does not grant permissions to add/update/purge web applications for example.



View role details

View the permissions for this role

Basic Information

Name
WAS SCANNER
Description
WAS Scanner User

Access method(s)

UI Access Enabled

Granted modules

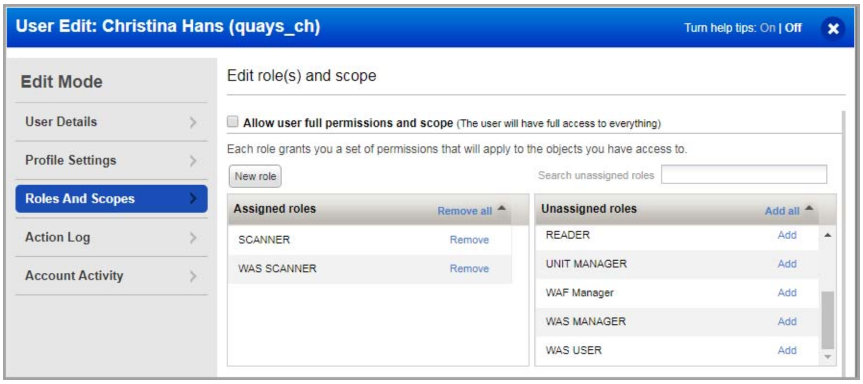
WAS **Web Application Scanning**

- WAS Configuration Permissions (12)
- WAS Schedule Permissions (3)
- WAS Scan Permissions (3)

Close   Edit

Click Close to edit user settings.

Click the Add link next to WAS SCANNER role to add it to the user's assigned roles. Assigned roles will look like this.



User Edit: Christina Hans (quays_ch)

Turn help tips: On | Off

Edit Mode

- User Details
- Profile Settings
- Roles And Scopes
- Action Log
- Account Activity

Edit role(s) and scope

□ **Allow user full permissions and scope** (The user will have full access to everything)

Each role grants you a set of permissions that will apply to the objects you have access to.

New role

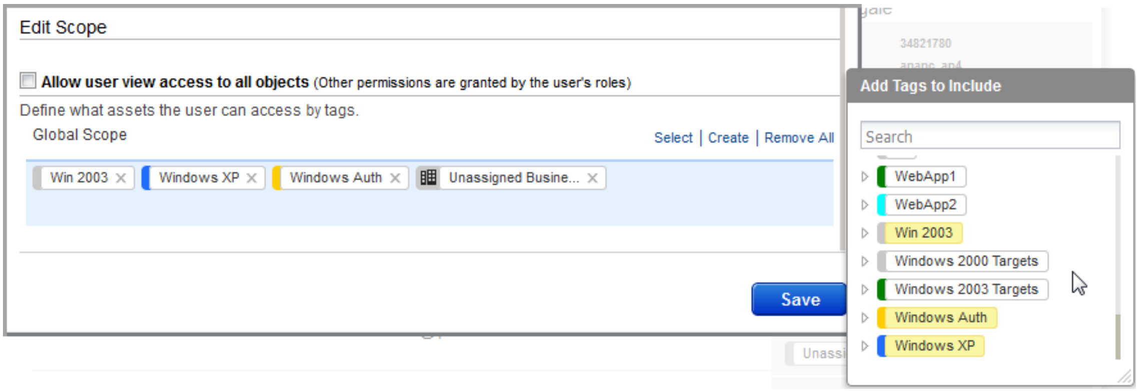
Search unassigned roles

Assigned roles	Remove all
SCANNER	Remove
WAS SCANNER	Remove

Unassigned roles	Add all
READER	Add
UNIT MANAGER	Add
WAF Manager	Add
WAS MANAGER	Add
WAS USER	Add

Update the Edit Scope section to grant the user access to web applications in your subscription. By default the user doesn't have access to any web applications or other WAS configurations. Choose one of the options.

Assign specific tags.



Edit Scope

□ **Allow user view access to all objects** (Other permissions are granted by the user's roles)

Define what assets the user can access by tags.

Global Scope

Select | Create | Remove All

Win 2003 ✕ | Windows XP ✕ | Windows Auth ✕ | Unassigned Busine... ✕

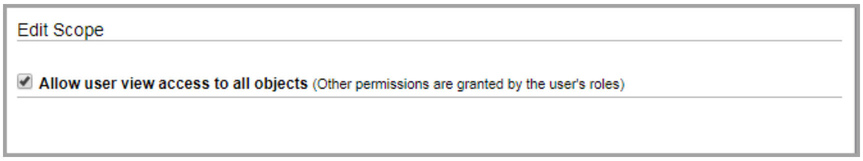
Save

Add Tags to Include

Search

- WebApp1
- WebApp2
- Win 2003
- Windows 2000 Targets
- Windows 2003 Targets
- Windows Auth
- Windows XP

Grant full scope (i.e. all tags)



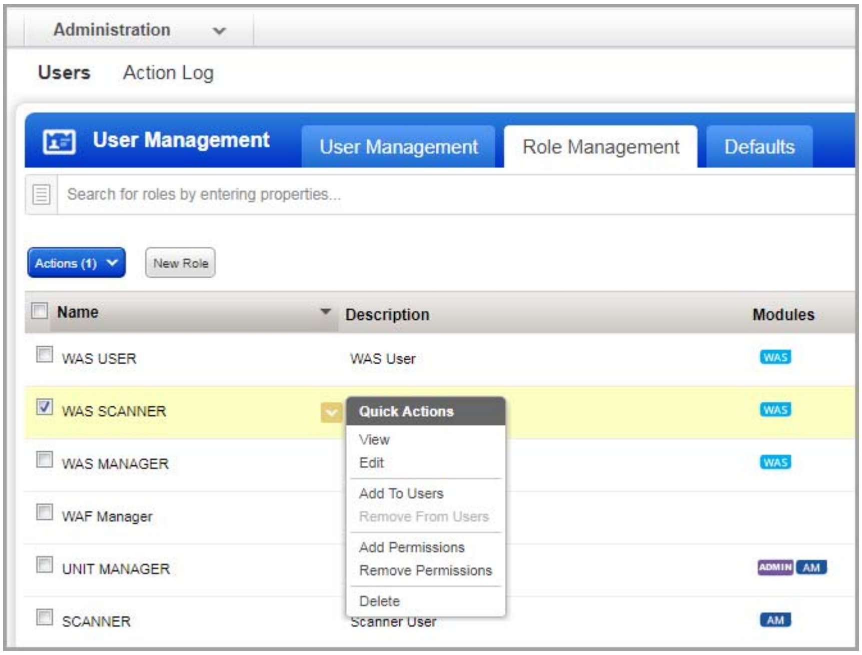
Edit Scope

☑ **Allow user view access to all objects** (Other permissions are granted by the user's roles)

Click Save to save the user settings.

Role Management

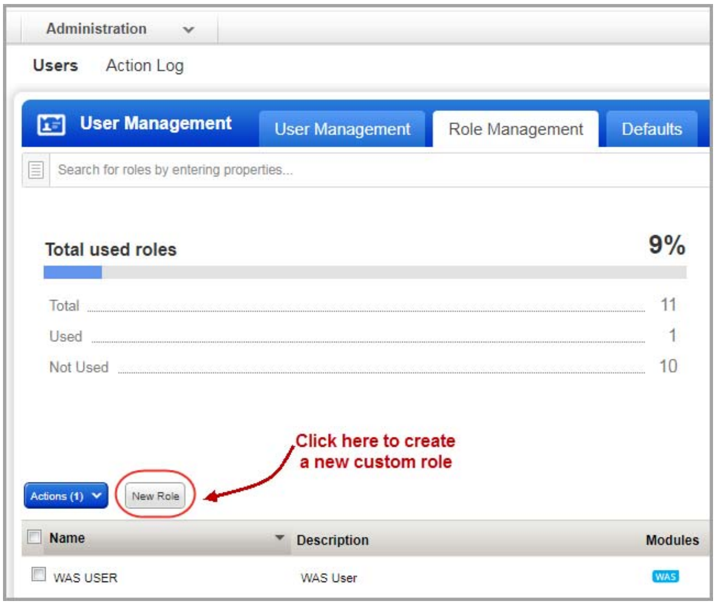
The Role Management section shows you all about the roles in your subscription.



	Name	Description	Modules
□	WAS USER	WAS User	WAS
☑	WAS SCANNER		WAS
□	WAS MANAGER		WAS
□	WAF Manager		
□	UNIT MANAGER		ADMIN AM
□	SCANNER	Scanner User	AM

For each role you can view details and take actions to add to users, add permissions, remove permissions etc.

The New Role option lets you create a custom role with the exact permissions you want.



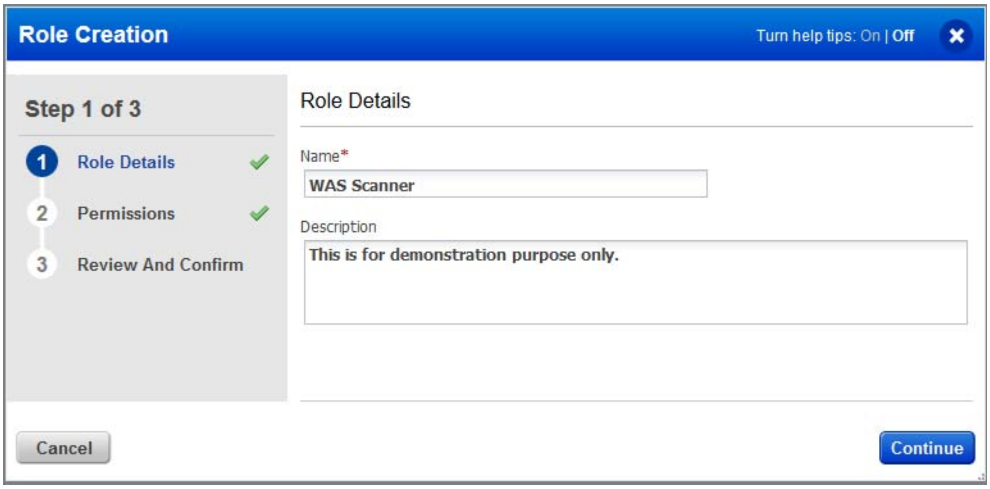
Total used roles 9%

Total	11
Used	1
Not Used	10

Click here to create a new custom role

	Name	Description	Modules
□	WAS USER	WAS User	WAS

For example you can create role WAS Scanner.



Role Creation

Step 1 of 3

1 Role Details ✓
2 Permissions ✓
3 Review And Confirm

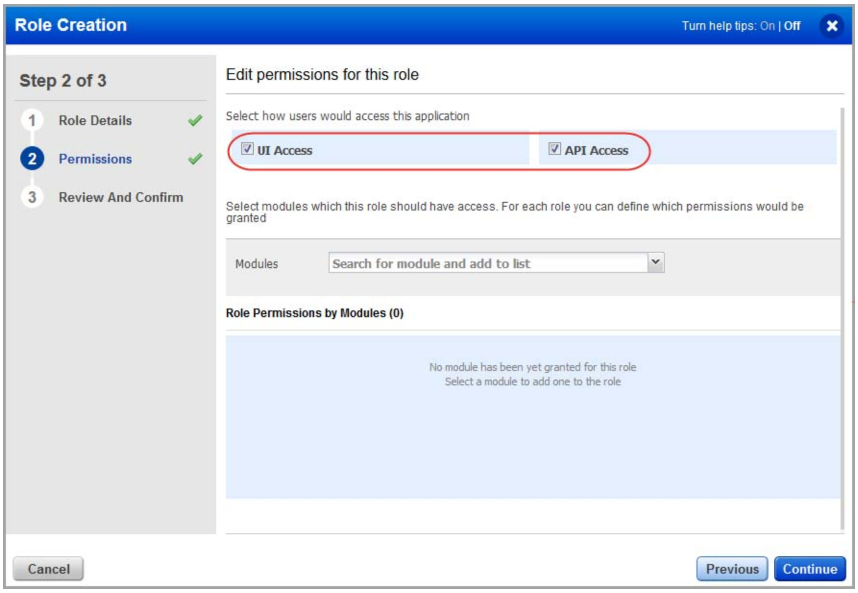
Role Details

Name*: WAS Scanner

Description: This is for demonstration purpose only.

Grant the role access to UI and/or API.

In the role details, choose the access methods for the user.



Role Creation

Step 2 of 3

1 Role Details ✓
2 Permissions ✓
3 Review And Confirm

Edit permissions for this role

Select how users would access this application

☑ UI Access ☑ API Access

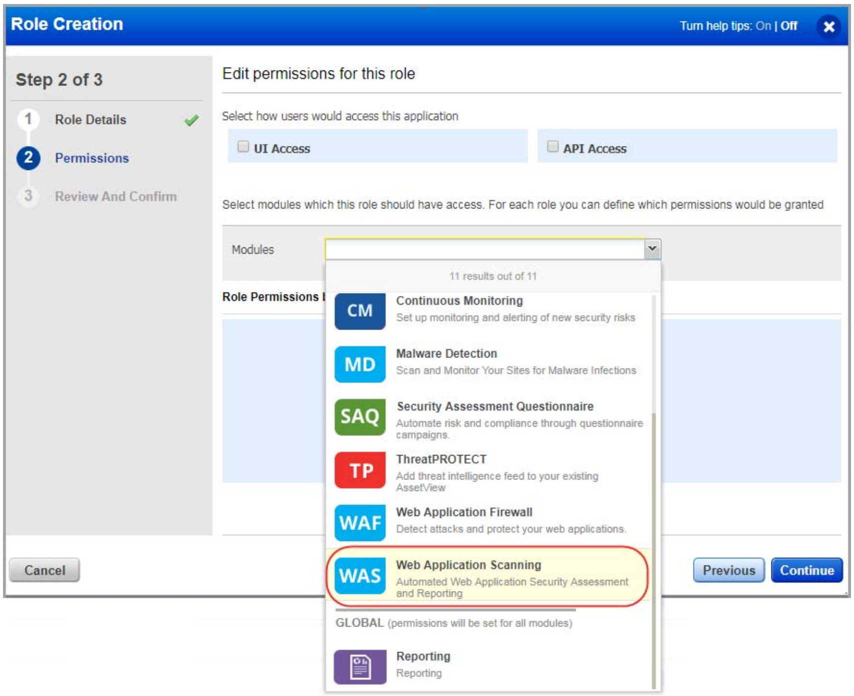
Select modules which this role should have access. For each role you can define which permissions would be granted

Modules: Search for module and add to list

Role Permissions by Modules (0)

No module has been yet granted for this role
Select a module to add one to the role

Grant the role access to the WAS app. In the Permissions section add select the WAS app from the menu provided.



Role Creation

Step 2 of 3

Edit permissions for this role

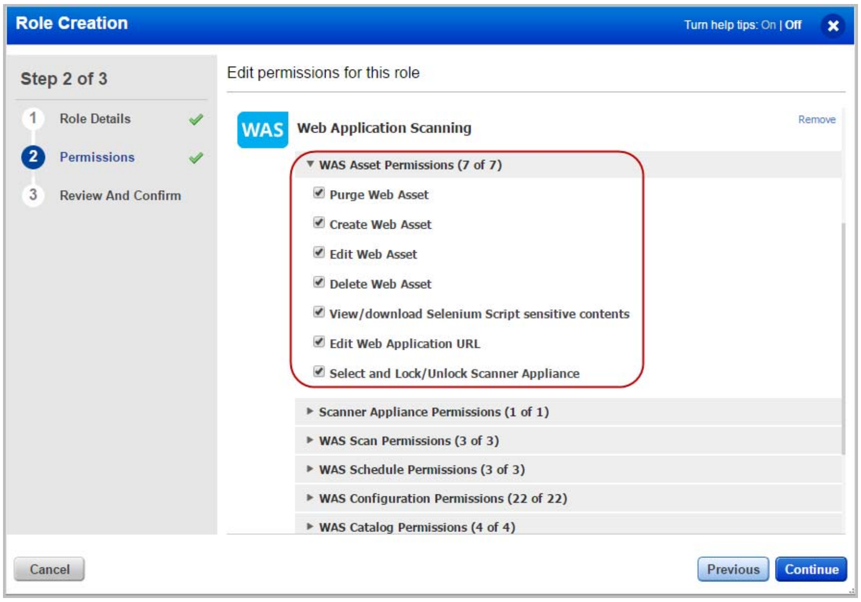
Select how users would access this application

□ UI Access
□ API Access

Select modules which this role should have access. For each role you can define which permissions would be granted

Turn help tips: On | Off
1 Role Details
2 Permissions
3 Review And Confirm
Modules
11 results out of 11
CM Continuous Monitoring
Set up monitoring and alerting of new security risks
MD Malware Detection
Scan and Monitor Your Sites for Malware Infections
SAQ Security Assessment Questionnaire
Automate risk and compliance through questionnaire campaigns.
TP ThreatPROTECT
Add threat intelligence feed to your existing AssetView
WAF Web Application Firewall
Detect attacks and protect your web applications.
WAS Web Application Scanning
Automated Web Application Security Assessment and Reporting
GLOBAL (permissions will be set for all modules)
Reporting
Reporting
Role Permissions
Cancel
Previous
Continue

Grant the role permissions within the WAS app.



Role Creation

Step 2 of 3

Edit permissions for this role

WAS Web Application Scanning

▾ WAS Asset Permissions (7 of 7)

☑ Purge Web Asset
☑ Create Web Asset
☑ Edit Web Asset
☑ Delete Web Asset
☑ View/download Selenium Script sensitive contents
☑ Edit Web Application URL
☑ Select and Lock/Unlock Scanner Appliance

▸ Scanner Appliance Permissions (1 of 1)
▸ WAS Scan Permissions (3 of 3)
▸ WAS Schedule Permissions (3 of 3)
▸ WAS Configuration Permissions (22 of 22)
▸ WAS Catalog Permissions (4 of 4)

Edit the user account and assign role.

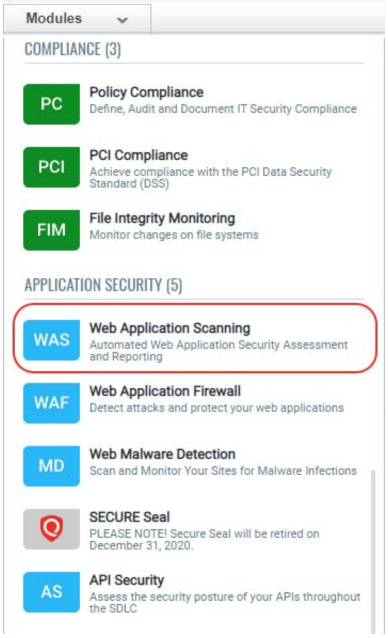
Get Started

Qualys WAS is the most powerful web application scanner available.

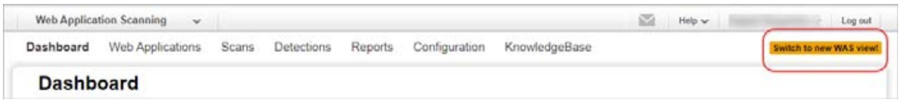
Note: The new WAS UI supports only the Web Applications and Detection features. The guide gives overview of these features. For detailed information on web application and detections functions, see WAS Online Help.We will navigate you to our Classic WAS UI version for the features that are not available in the new WAS UI.

Let’s go!

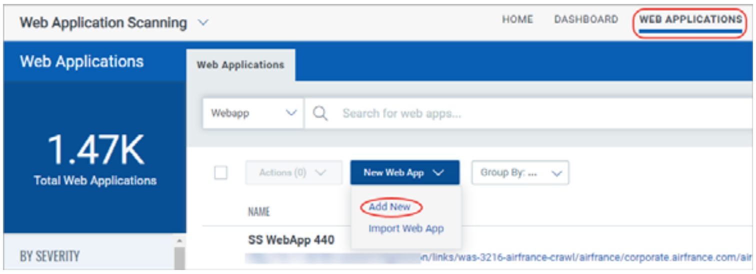
Just log in and select Web Application Scanning from module picker.


Modules
COMPLIANCE (3)
PC
Policy Compliance
Define, Audit and Document IT Security Compliance
PCI
PCI Compliance
Achieve compliance with the PCI Data Security Standard (DSS)
FIM
File Integrity Monitoring
Monitor changes on file systems
APPLICATION SECURITY (5)
WAS
Web Application Scanning
Automated Web Application Security Assessment and Reporting
WAF
Web Application Firewall
Detect attacks and protect your web applications
MD
Web Malware Detection
Scan and Monitor Your Sites for Malware Infections
SECURE Seal
PLEASE NOTE! Secure Seal will be retired on December 31, 2020.
AS
API Security
Assess the security posture of your APIs throughout the SDLC

Click **Switch to new WAS view!**



Start by telling us about the web application you want to scan - just click **Web Applications** > **New Web App**.

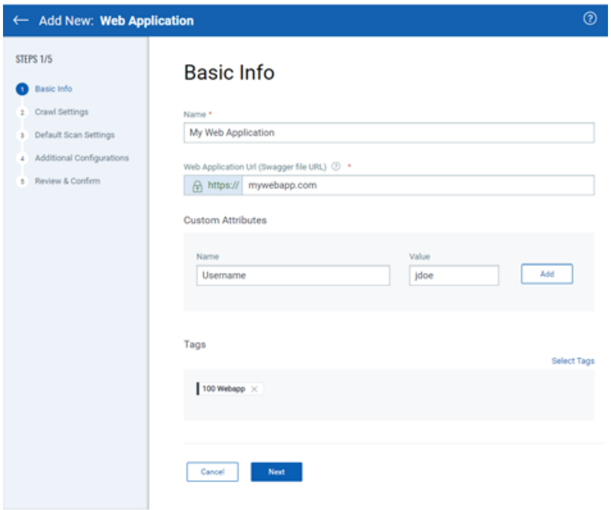


SS WebApp 440
[redacted]n/links/was-3216-airfrance-crawl/airfrance/corporate.airfrance.com/air

Add your web application settings

The web application name and URL are required when adding a web app from scratch..

Want to scan your external site for malware? Just turn on Malware Monitoring and we'll perform automatic daily malware scans.



Basic Info

Name * My Web Application

Web Application Url (Swagger file URL) * https:// mywebapp.com

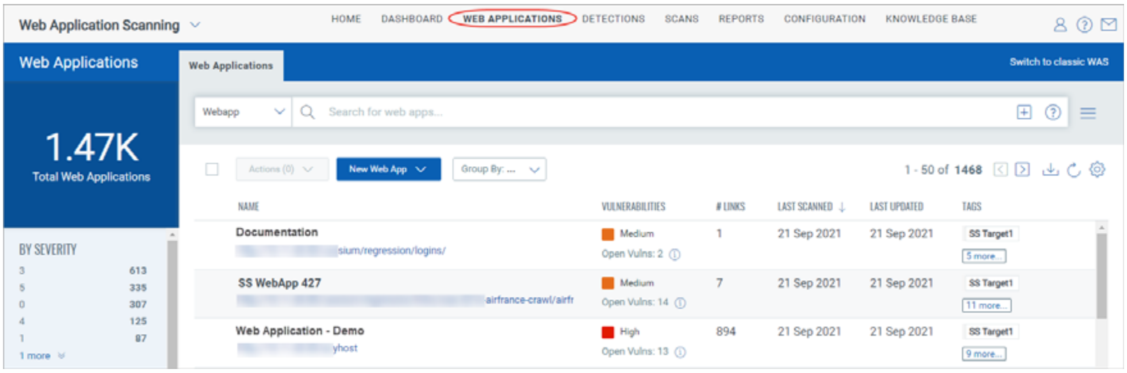
Custom Attributes

Name: Username
Value: jdoe

Tags

100 Webapp

Your web application appears in the Web Applications tab, where you can edit the application settings.



BY SEVERITY

3	613
5	335
0	307
4	125
1	87

NAME	VULNERABILITIES	# LINKS	LAST SCANNED ↓	LAST UPDATED	TAGS
Documentation [redacted]sium/regression/logins/	🟧 Medium Open Vulns: 2	1	21 Sep 2021	21 Sep 2021	SS Target1 5 more...
SS WebApp 427 [redacted]airfrance-crawl/airfr	🟧 Medium Open Vulns: 14	7	21 Sep 2021	21 Sep 2021	SS Target1 11 more...
Web Application - Demo [redacted]yhost	🟥 High Open Vulns: 13	894	21 Sep 2021	21 Sep 2021	SS Target1 9 more...

Why use authentication?

Using authentication allows our service to access to all parts of your web application during the crawling process. This way we can perform more in-depth assessment of your web application. Some web applications require authenticated access to the majority of their functionality. Authenticated scanning can be configured for HTML forms like login pages and server-based authentication (HTTP Basic, Digest, NTLM, or SSL client certificates). Just go to the Authentication tab, select New Record and configure an authentication record with access credentials. Form and server authentication may be combined as needed - we'll monitor the session state to ensure an authenticated scan remains authenticated throughout the crawl.

Do I need to provide authentication details?

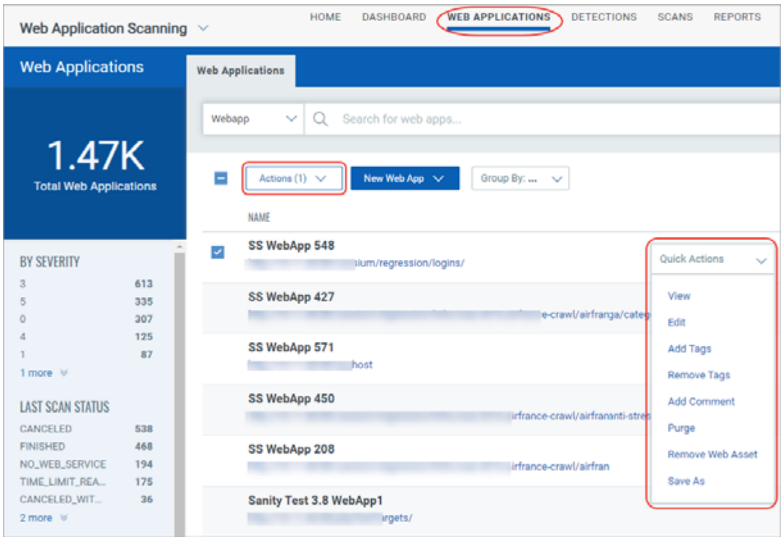
Is authentication needed to access the functionality of this web application? If yes be sure to select an authentication record.

Tell me about the option profile

An option profile is a set of scan configuration options. We recommend "Initial WAS Options" to get started. Editing options in the profile allows you to customize crawling and scan parameters.

Take actions on Web Applications

Take action against individual applications using the **Quick Actions** menu. Select or hover a web application and click the arrow to view the options in the **Quick Actions** menu. Use the Quick Actions menu to view, edit the details of web assets, add tags and remove tags from web assets, purge scan data of web assets. You can also remove web assets from the subscription and other associated modules and create a new web asset with the same configurations using the Save as option. You can take action against multiple web applications using the **Bulk Actions** menu.



1.47K
Total Web Applications

BY SEVERITY	
3	613
5	335
0	307
4	125
1	87
1 more	

LAST SCAN STATUS	
CANCELED	538
FINISHED	468
NO_WEB_SERVICE	194
TIME_LIMIT_REA...	175
CANCELED_WIT...	36
2 more	

NAME

☑ SS WebApp 548
[redacted]ium/regression/logins/

SS WebApp 427
[redacted]e-crawl/airfranga/categ

SS WebApp 571
[redacted]host

SS WebApp 450
[redacted]irfrance-crawl/airfrananti-stre

SS WebApp 208
[redacted]irfrance-crawl/airfran

Sanity Test 3.8 WebApp1
[redacted]rgets/

Good to Know

What vulnerability checks are tested? We'll scan for all vulnerability checks (QIDs) listed in the KnowledgeBase unless you configure your option profile to do limit the scan to certain vulnerabilities (confirmed, potential and/or information gathered). We constantly update the KnowledgeBase as new security information becomes available. Click KnowledgeBase on the top menu.

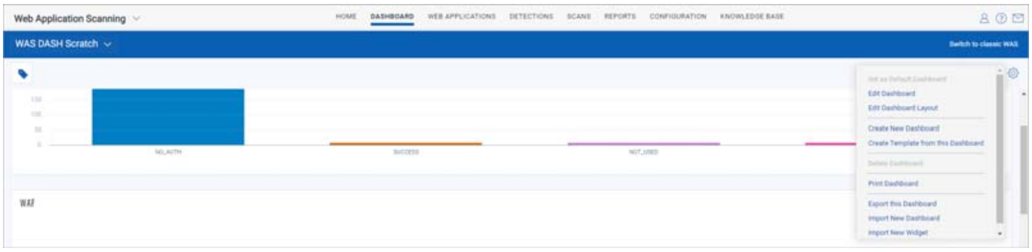
What is Severity? Each QID is assigned a severity level by our service: confirmed vulnerability (red), potential vulnerability (yellow) and information gathered (blue).

Get the latest security status from your dashboard

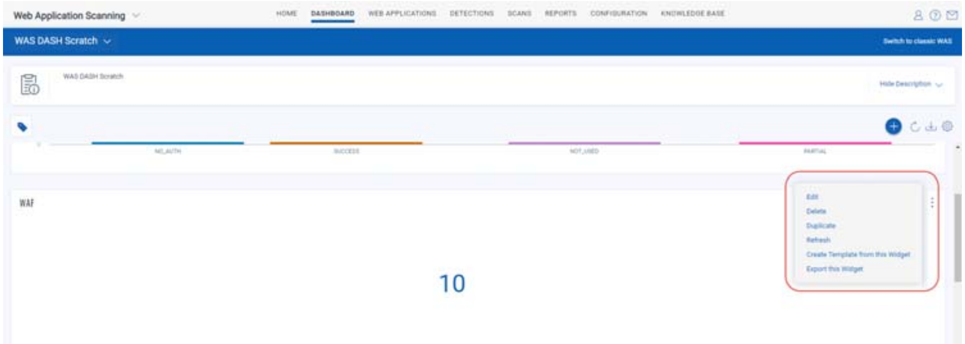
Your dashboard gives you security status at a glance and it's always up to date. Dashboards help you visualize your web applications and their detections. We have integrated Unified Dashboard (UD) with WAS. UD brings information from all Qualys applications into a single place for visualization. UD provides a powerful new dashboarding framework along with platform service that will be consumed and used by all other products to enhance the existing dashboard capabilities.

Click the gear icon at the top right to create, edit, print a Dashboard. You also have an option to add widgets with search queries to see exactly what you're interested in. You can also export and import Dashboard and Widget configurations to a file in a json format allowing you to share them between accounts or within the Qualys community.

Create multiple dashboards and switch between them for different views of your data.



From the Widget menu, you can edit, delete, duplicate, refresh, and export a widget. You also have an option to create a template from a widget.



Adding widgets

1) Start by clicking the Add Widget button on your dashboard.

2) Pick one of our widget templates - or create your own.

4) Click the gear icon at the top right and from the menu you can also import configurations to a file in a json format, allowing you to share the widgets between accounts or within the Qualys community.

Tips:

- Wondering how we created the widgets on the default dashboard? Choose widgets menu> Edit to see the settings.

Manage Detections

Manage all your detections in one place. The detections tab acts as a central area for application security vulnerability detections, management and information. We list all your findings (Qualys, Burp, and Bugcrowd) in the Detections tab.

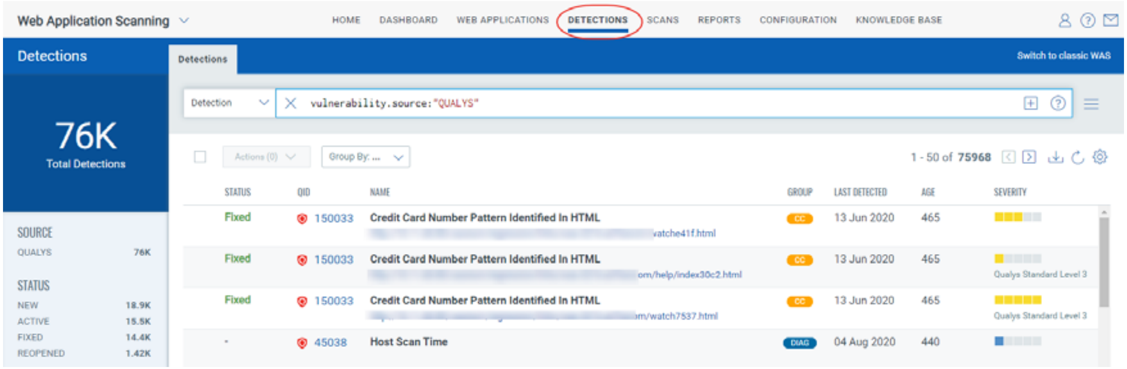
We have filters in the left pane to enhance the search and quickly locate the detection type. In addition to the common filters, use the search tokens to build complex search expression to find detections specific to your requirement. For example, to view BURP findings with age greater than 10 days, enter this search express in the search bar: vulnerability.source:"BURP" and vulnerability.age>10.

You can distinguish the finding type with the icon displayed in the list.

- Qualys detections

- Burp issues

- Bugcrowd submissions



vulnerability.source:"QUALYS"

76K
Total Detections

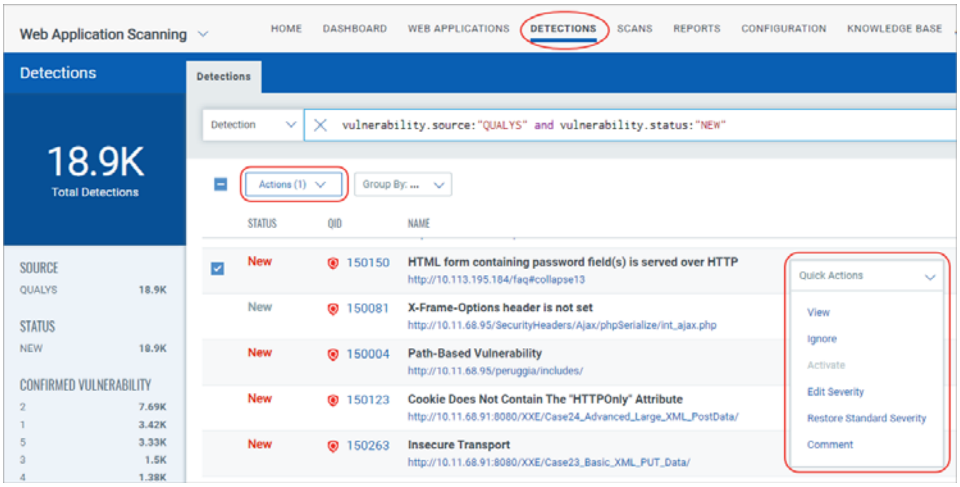
SOURCE	
QUALYS	76K

STATUS	
NEW	18.9K
ACTIVE	15.5K
FIXED	14.4K
REOPENED	1.42K

STATUS	QID	NAME	GROUP	LAST DETECTED	AGE	SEVERITY
Fixed	150033	Credit Card Number Pattern Identified In HTML [redacted]vatche41f.html	CC	13 Jun 2020	465	■■■□□
Fixed	150033	Credit Card Number Pattern Identified In HTML [redacted]om/help/index30c2.html	CC	13 Jun 2020	465	■□□□□ Qualys Standard Level 3
Fixed	150033	Credit Card Number Pattern Identified In HTML [redacted]m/watch7537.html	CC	13 Jun 2020	465	■■■■■ Qualys Standard Level 3
-	45038	Host Scan Time	DIAG	04 Aug 2020	440	■□□□□

Take actions on detections

Take action against individual detections using the **Quick Actions** menu. Select or hover a detection and click the arrow to view the options in the **Quick Actions** menu. Use the Quick Actions menu to edit, ignore, and reactivate ignored detections. You can also edit and restore the severity level of the detections, add comments to the detections. You can take action against multiple detections using the **Bulk Actions** menu.



```
vulnerability.source:"QUALYS" and vulnerability.status:"NEW"
```

18.9K
Total Detections

SOURCE	
QUALYS	18.9K
STATUS	
NEW	18.9K
CONFIRMED VULNERABILITY	
2	7.69K
1	3.42K
5	3.33K
3	1.5K
4	1.38K

	STATUS	QID	NAME
☑	New	150150	HTML form containing password field(s) is served over HTTP http://10.113.195.184/faq#collapse13
	New	150081	X-Frame-Options header is not set http://10.11.68.95/SecurityHeaders/Ajax/phpSerialize/int_ajax.php
	New	150004	Path-Based Vulnerability http://10.11.68.95/peruggia/includes/
	New	150123	Cookie Does Not Contain The "HTTPOnly" Attribute http://10.11.68.91:8080/XXE/Case24_Advanced_Large_XML_PostData/
	New	150263	Insecure Transport http://10.11.68.91:8080/XXE/Case23_Basic_XML_PUT_Data/

Scanning using Selenium scripts

You can use Qualys Browser Recorder (QBR) to create a Selenium script. QBR is a free browser extension (for Google Chrome browser) to record & play back scripts for web application automation testing. QBR allows you to capture web elements and record actions in the browser to let you generate, edit, and play back automated test cases quickly and easily. It also allows you to select a UI element from the browser's currently displayed page and then select from a list of Selenium commands with parameters. You can use these scripts in WAS to help the scanner navigate through the complex authentication and business workflows in a web application.

A common authentication mechanism used by web applications is single sign-on (SSO). This introduces complexity and can cause some confusion when it comes to authenticating and scanning with Qualys WAS. With use of QBR, you could simplify authentication mechanism for the scanner. For detailed steps, refer to our blog article.