Qualys WAS Lab Tutorial Supplement

Table of Contents

Qualys Web Application Scanning (WAS) enables organizations to assess, track, and remediate Web application vulnerabilities.

The Open Web Application Security Project (OWASP) Top 10 list has become the industry standard for categorizing the most critical risks faced by Web apps. Qualys WAS allows you to accurately find these vulnerabilities – including SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF) and URL redirection – and learn how to mitigate them.

WAS Workflow

The workflow for analyzing a Web application involves five simple steps: 1) Define Web Application, 2) Perform Discovery Scan—Crawl, 3) Perform Vulnerability Scan, 4) Create Reports, and 5) Fix Vulnerabilities

Here is a detailed view of this workflow:

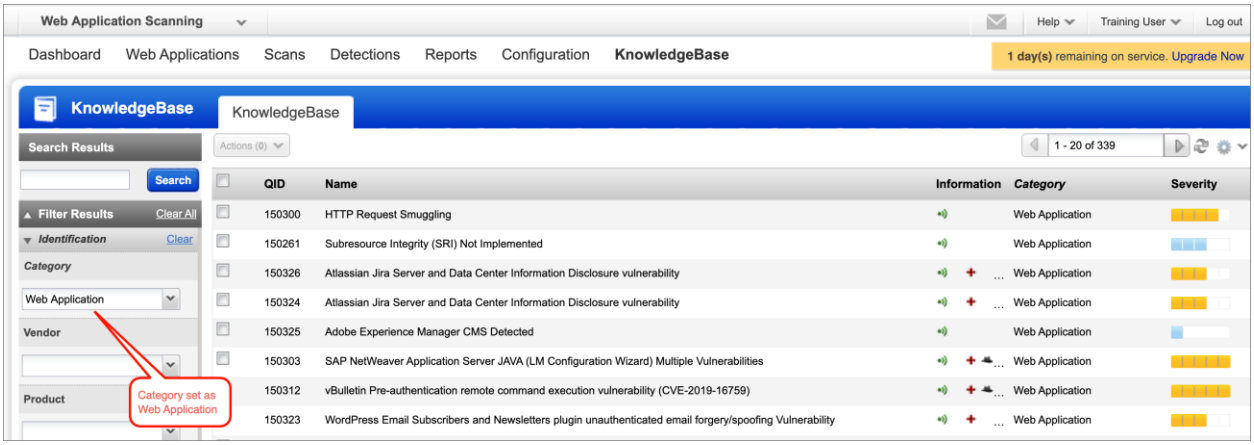
1. Define Web Application
    - Identify the location (URL) of the Web App
    - Define the “scope” of the Web App Crawl
    - Choose from various scanning options—Option Profile:
    - Select a scanner appliance
    - Include “crawling hints” and/or header injection
    - Use optional DNS Override
    - Provide authentication credentials
        - Form records
        - Server records
    - Identify areas to “white list” or “black list”
    - Enable malware monitoring
2. Perform Discovery Scan (Crawl)
3. Perform Vulnerability Scan
4. Create reports to identify links crawled and vulnerabilities detected
5. Fix vulnerabilities

WAS KnowledgeBase

All detectable vulnerabilities (including Web app vulnerabilities) are viewable from within the Qualys KnowledgeBase. This first tutorial uses the "Search & Filter" pane, to focus on Web application vulnerabilities.

Click the following link to view the "WAS KnowledgeBase" tutorial.

PLAY Lab 1 - http://ior.ad/7fLC



The Search and Filtering pane (left) will allow you to locate Web application vulnerabilities.

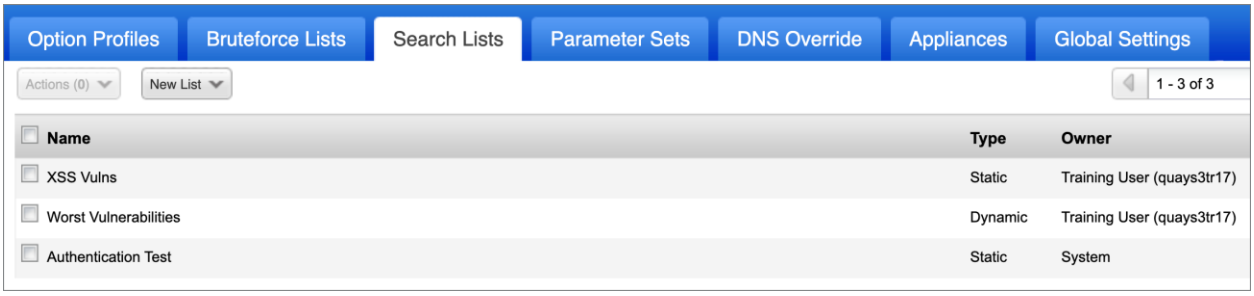
WAS Search List

A "Search List" is an extension of the Qualys KnowledgeBase and is a powerful customization tool within Qualys Web Application Scanning. The name "Search List" is derived from the KnowledgeBase "Search" tool that is used to create a list of vulnerabilities. A Search List is a grouping of QIDs that can be used in various capacities in Qualys WAS.

Click the following link to view the "WAS Search List" tutorial.

PLAY Lab 2 - http://ior.ad/7fmc

You can add a Search List to an Option Profile to customize your scan. For instance, you can run a scan for just a specific vulnerability. Or, you can use a Search List to omit vulnerabilities from a scan.



You can also add a Search List to a Report Template to help prioritize which vulnerabilities will be addressed first. For example, you can build a report containing only XSS vulnerabilities or only your most severe vulnerabilities.

Basic Application Setup

Before a Web Application can be scanned, it must first be added to your WAS subscription. Although Qualys WAS provides many advanced Web app scanning features (e.g., SmartScan, Progressive Scanning, Header Injection, Path Fuzzing, etc…), the basic application setup requirements can be completed in a handful of simple steps.

Bodgeit Store Web App

The Bodgeit Store is a vulnerable Web app, that provides students and security practitioners with a better understanding of Web application vulnerabilities.

Click the following link to view the basic setup steps for the "Bodgeit Store" Web app.

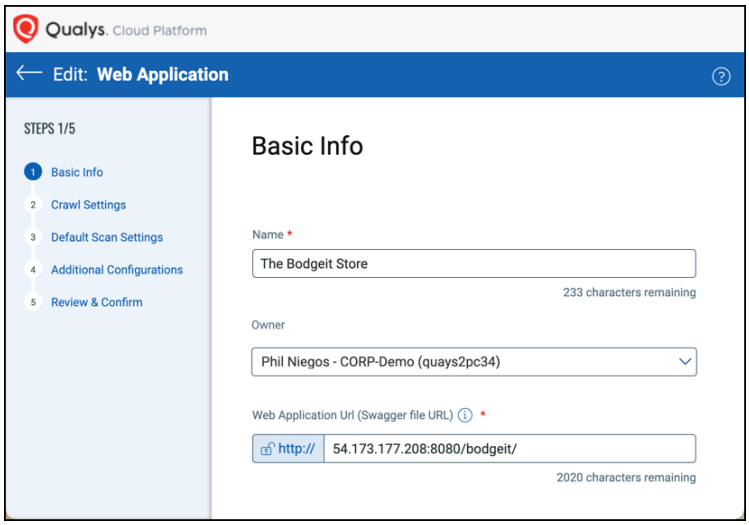
PLAY Lab 3 - https://ior.ad/8CNc

Click the following link to view the "Standard Login Authentication".

Lab 4 - https://ior.ad/98vE

Basic Info

Target definition – Name and URL of the application you're scanning

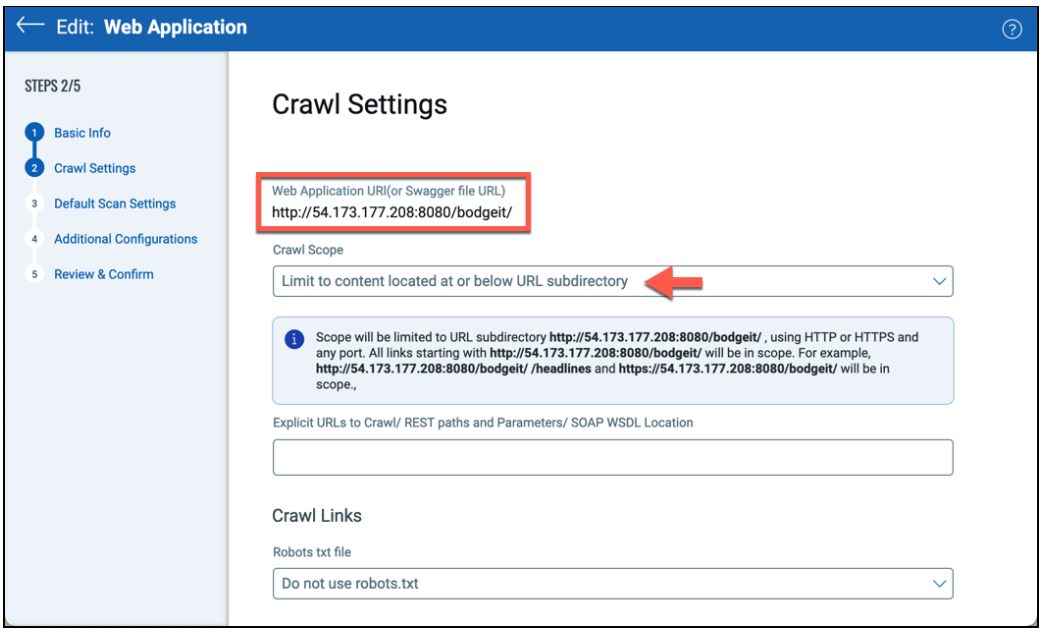


Custom Attributes – Name/Value pairs that can be used for categorizing and filtering the application

Tags – Labels that can be applied to applications for filtering, scanning, and reporting purposes

Crawl Settings

Crawl Scope – a single web application can span multiple domains, IP addresses, and port numbers (including sub-domains and subdirectories). The scope of an application defines its boundaries.



The "Crawl Scope" field provides a few options:

- **Limit at or below URL hostname** - Select to limit crawling to the hostname within the URL, using HTTP or HTTPS and any port.
- **Limit to content located at or below URL subdirectory** - Select to crawl all links starting with a URL subdirectory using HTTP or HTTPS and any port.
- **Limit to URL hostname and specified sub-domain** - Select this option to crawl only the URL hostname and one specified sub-domain, using HTTP or HTTPS and any port.
- **Limit to URL hostname and specified domains** - Select this option to crawl only the URL hostname and specified domains, using http or https and any port.

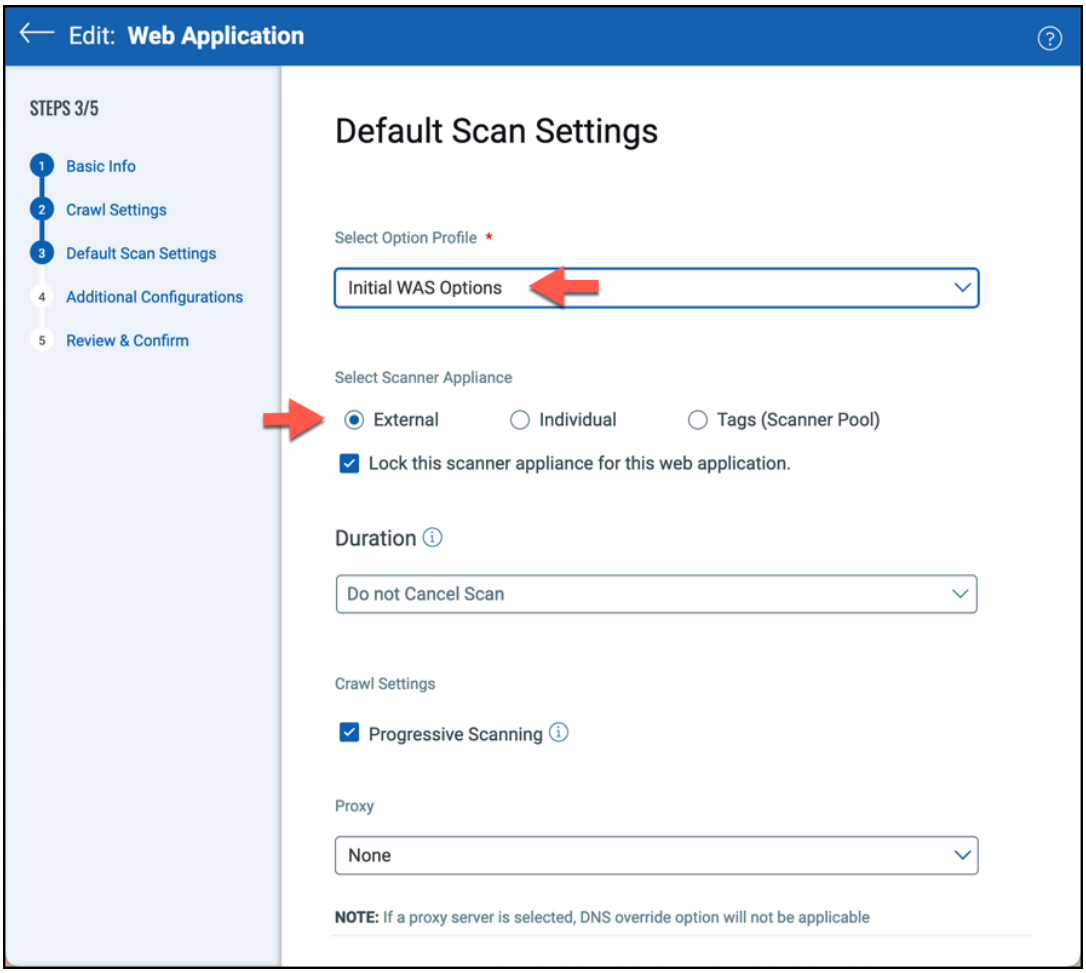
Explicit URLs to Crawl - this is useful for pages not directly linked to other pages within the application. For example, a registration link sent to the user via email. You can also include WSDL URLs for web services you want the service to crawl. Enter each URL on a separate line. Each entry must be a valid http or https URL. You can enter a maximum of 2048 characters for each URL. The URLs you enter must be consistent with the selected scope.

Crawl Links - Instruct the scan to adhere to existing configurations when scanning the web application using a robots.txt or sitemap.xml file

Selenium Script – Upload Selenium scripts recorded using Qualys Browser Recorder to play back functions in web applications during scanning

Default Scan Settings

Many of the defaults configured in this step can be changed or adjusted at scan time.



Option Profile – A collection of scan settings to be used while crawling or scanning the application.

Scanner Appliance – The appliance to be used for crawling or scanning the application. Be sure the Scanner Appliance you are using has access to the application you are scanning.

Duration – How long should the scan run before being automatically cancelled.

Option Profile

PLAY Lab 5 - https://ior.ad/8CW9

The following options are available under the **Scan Parameters** section of an Option Profile:

Form Submission - When forms are submitted, http(s) uses GET or POST methods. The crawl can be limited to either type of form submission, both, and none. It is considered best practice to select "Post & Get" for the most thorough vulnerability analysis. If "none" is chosen, the only forms WAS will submit will be for authentication

Form Crawl Scope – By default, the scanner uses form names to determine the uniqueness of a form. When "Include form action URI in form uniqueness calculation" is enabled, the scanner uses the form action URI and the form field name to determine its uniqueness

Form Crawl Scope	☑ Include form action URI in form uniqueness calculation.

Maximum links to test in scope – Specify the maximum links and forms to crawl during the scan. The maximum is 8000.

User Agent - If your web application requires specific user-agent string to access it, you need to specify the same. The default user agent setting that is used is user-agent: ***Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_3) AppleWebKit/601.4.4 (KHTML, like Gecko) Version/9.0.3 Safari/601.4.4***

Request Parameter Set – Specify the default parameters that need to be injected into your web application, such as first name, last name, email address, phone number etc.

Document Type – Enable the "Ignore common binary files" option to not scan files with extensions pdf, zip, and doc.

Document Type	☑ Ignore common binary files based on file extensions.

Enhanced Crawling – When enabled, the scanner will attempt to load and render individual directories.

For example, if this link is found during crawling:
https://www.example.com/foo/abc/xyz/register.php

The scanner will make the first request to https://www.example.com/foo/abc/xyz and will then remove the directory "xyz" from the URL and crawl, https://www.example.com/foo/abc/ and later it will further remove "abc/" and will crawl https://www.example.com/foo/ .

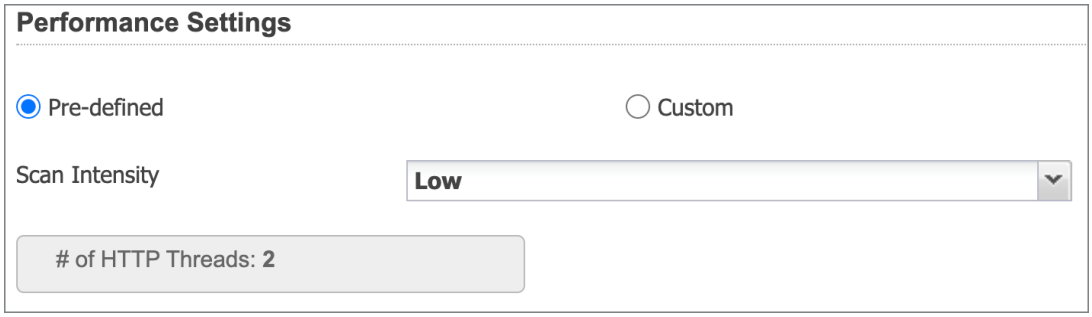
All links found during this process of removal and re-crawling will get added to the crawl queue, thus improving the scan coverage.

Enable SmartScan – When enabled, the scanner will perform advanced scanning, using enhanced AJAX/SPA deep crawling and vulnerability testing. This option is recommended for scanning applications with advanced frameworks and technologies.

Timeout Error Threshold – Maximum number of timeout errors encountered during the scan that will result in the scan being terminated.

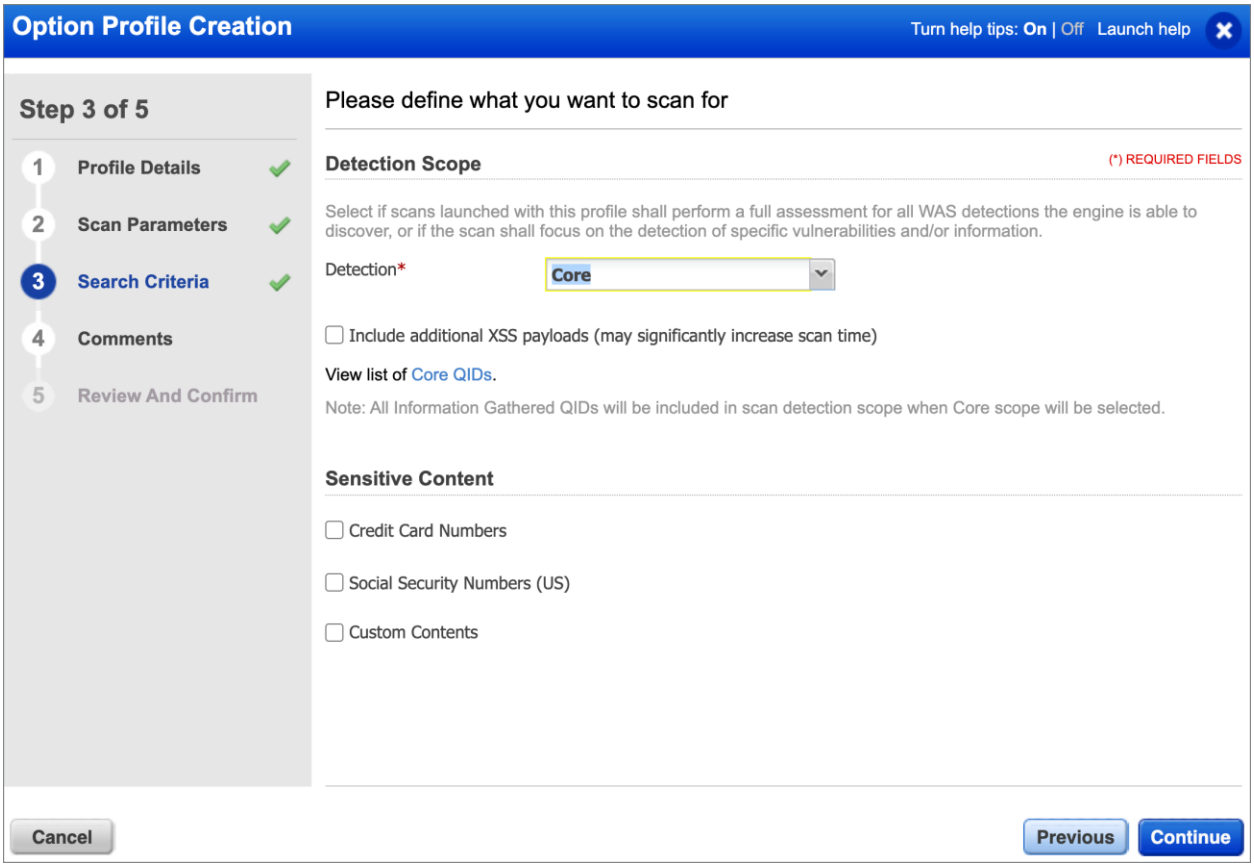
Unexpected Error Threshold - Maximum number of unexpected errors encountered during the scan that will result in the scan being terminated.

Performance Settings – select from Pre-defined (lowest, low, medium, high, and maximum) and Custom to set the scan intensity



Password bruteforcing – enable this to find out how vulnerable your web applications are to password-cracking techniques

The following options are available under the **Search Criteria** section of an Option Profile:



Detection Scope – This determines the vulnerabilities that will be checked during the scan:

- Core – Default for new WAS Option Profiles. Core scope includes vulnerabilities that Qualys considers most common in today's web applications. It does not include all the vulnerabilities that WAS can detect.
- Categories - Specific vulnerabilities defined in the categories. Select a category to check for associated vulnerabilities in the scan.
- Custom Search Lists - Specific vulnerabilities defined in Search Lists. This provides the most granular control over detection scope. You can select search lists to include and Search Lists to exclude.
- XSS Power Mode - Comprehensive tests for cross-site scripting vulnerabilities. The XSS Power Mode detection scope performs tests using the standard XSS payloads, which detect the most common instances of XSS, but also with additional payloads that can identify XSS in certain, less-common situations.
- Everything – All the vulnerabilities that WAS can detect.

Sensitive Content - Check for sensitive content in the web application pages it crawls based on known patterns (such as credit card numbers, social security numbers) or based on custom patterns you enter.

Web App Scanning

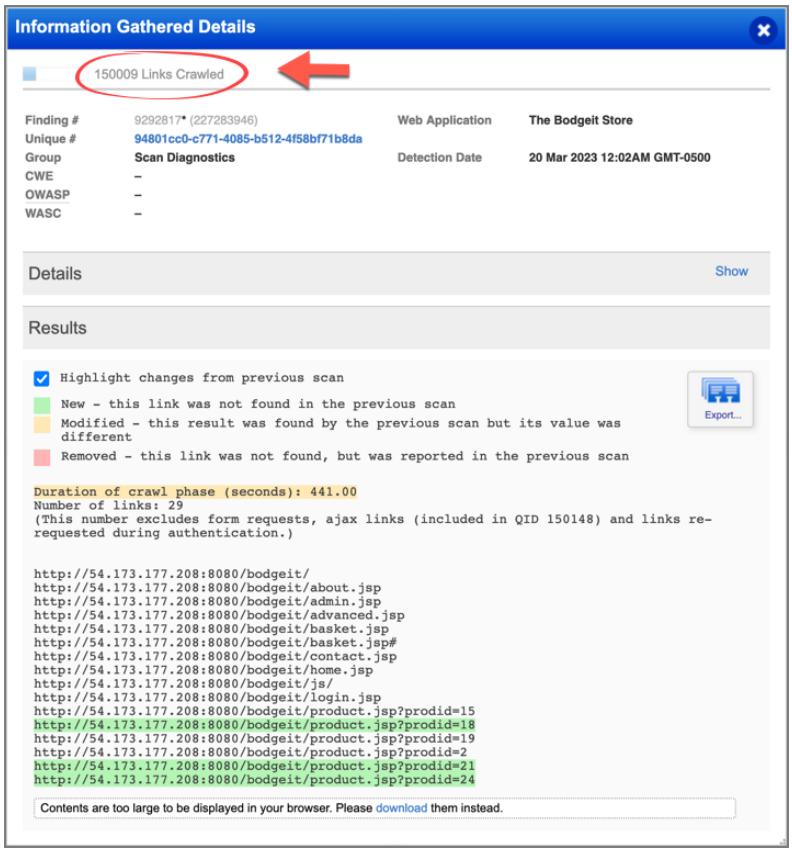
After providing **Basic Info**, **Crawl Settings**, and **Default Scan Settings**, you are ready to perform a Web app scan. Qualys WAS provides a discovery scan for crawling targeted Web apps, and a vulnerability scan for performing assessment tests to identify and reveal specific types of Web app vulnerabilities. While the discovery scan option can be performed exclusively, a vulnerability scan always begins with a crawl, by default.

Click the following link to view the "Web App Scanning" tutorial for the "Bodgeit Store" app.

PLAY Lab 6 - http://ior.ad/7f1T

Discovery Scan

A Discovery Scan begins at the starting URL specified in a Web app's Basic Info settings. Using the Scope Options identified in the Crawl Settings the scan follows links to discover pages and content. While configuration data is collected from the target Web app and its host, vulnerability testing is not performed.



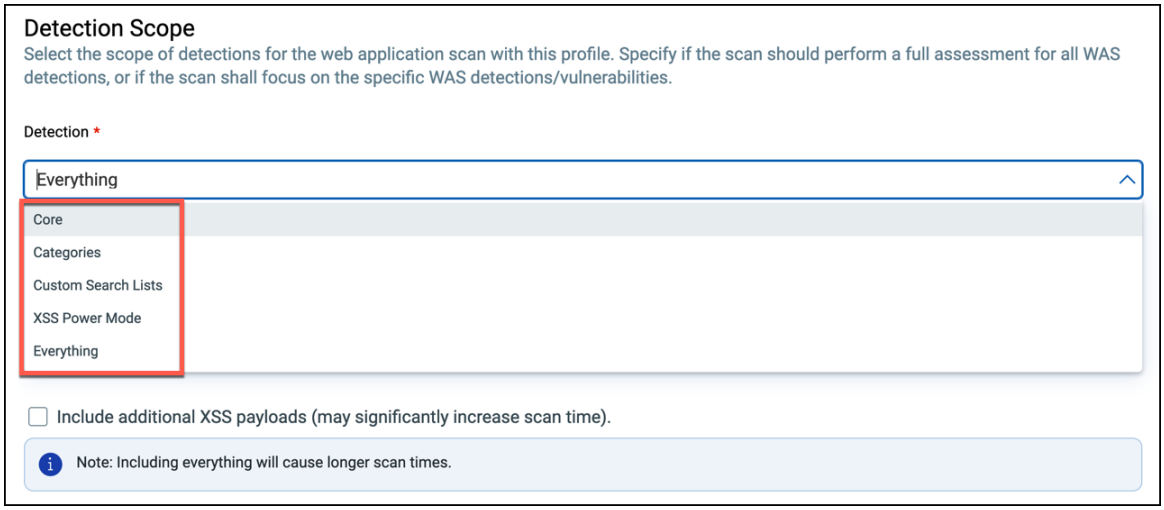
The list of unique links crawled by the WAS scanner appear in QID 150009. The total links crawled includes requests made via HTML forms, and requests for the same link made as an anonymous and authenticated user.

All discovery scans eventually end when one of the following conditions is met:

1. There are no new links to be discovered (i.e., all links have been successfully crawled).
2. The "Maximum Links to Crawl" specified in the scan's Option Profile is met. Presently, the WAS system threshold for "Maximum Links to Crawl" is 8000 links.
3. A Scan Duration has been specified in the Web app's Default Scan Settings or at scan time. Presently, the WAS system Scan Duration is 24 hours. Any Error Thresholds specified in the scan's Option Profile will also impact the duration of any scan.

Vulnerability Scan

WAS performs vulnerability assessment tests according to the Detection Scope specified in the Web app's Option Profile:



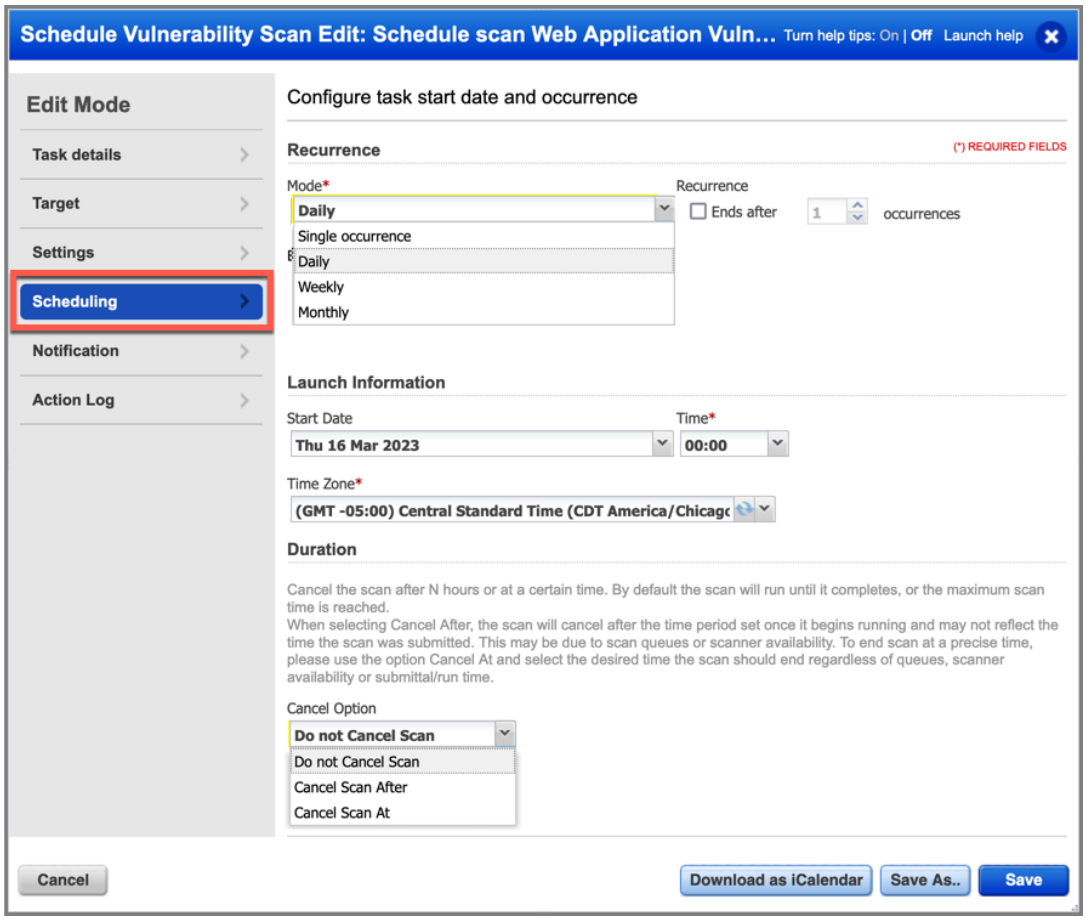
- **Core** – QIDs focus on the most common Web app vulnerabilities (i.e., fringe elements have been removed).
- **Categories** – Select QIDs from multiple Web app vulnerability categories, such as SQLi, XSS, Denial of Service, Clickjacking and more.
- **Custom Search Lists** – Build and scan for your own custom list of QIDs.
- **XSS Power Mode** – A comprehensive list of XSS QIDs.
- **Everything** – all Web app vulnerability QIDs in the Qualys KnowledgeBase.

Fault injection tests are constructed according to Web app vulnerability data and information provided by the Open Web Application Security Project (OWASP), Web Application Security Consortium (WASC), and Common Weakness Enumeration (CWE).

Scheduled Scan

A Scheduled Web app scan includes all of the details typically provided in a Discovery or Vulnerability scan that is launched manually. You are still required to select a scanning target, adjust any Scan Settings (if required), and select Notification options.

The noticeable exception; of course, are the Scheduling options.



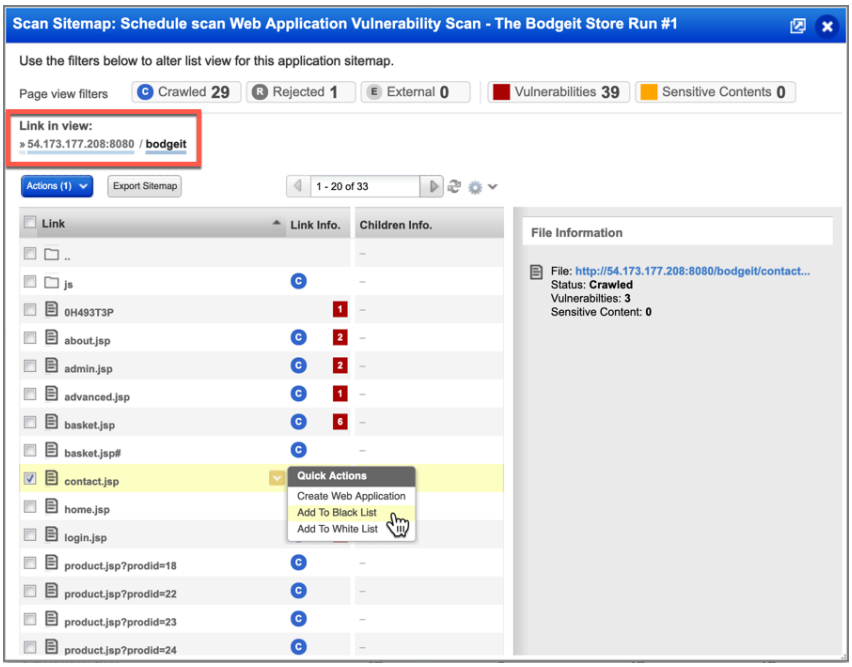
Schedule Web app scans to run daily, weekly, or monthly; including single occurrences if needed.

To accommodate restrictive scanning windows, scheduled scans may be cancelled AFTER a specified amount of time, or AT a specific time of day. When combined with the Progress Scanning feature, the results from multiple scans are combined to produce a final outcome.

Qualys recommends scheduling scans to run daily, when using WAS Progressive Scanning.

WAS Sitemap

A sitemap is automatically generated after Qualys WAS completes a Web application crawl (i.e., discovery or vulnerability scan).



The Web Application Sitemap provides a convenient way to view a list of all pages/links discovered. Leverage the "Quick Actions" menu to quickly apply "whitelist" or "blacklist" exclusion rules to specific pages and links.

Click the following link to view the "Sitemap" tutorial for the "Bodgeit Store" app.

PLAY Lab 7 - http://ior.ad/7f2e

The following filters are available when viewing a sitemap:

- **Crawled** – Show pages that have been crawled during the scan
- **Rejected** – Show pages that have been rejected (this could be due scan permissions or configured blacklists)
- **External** – Show pages that contain external links (not in scope)
- **Vulnerabilities** – Show pages on which vulnerabilities have been detected
- **Sensitive content** – Show pages on which sensitive content has been detected (for example credit card numbers and social security numbers)

Additional Configurations

While the previous lab exercises focused on the basic requirements to successfully launch a Web app scan, many more scanning options and features are provided under Additional Configurations.

Authentication Records

You may define an authentication record to be used for authenticating into the web application.

Header injection

Headers that need to be injected by our scanning service to scan the web application. This option is intended to be used when a workaround is needed for complex authentication schemes or to impersonate a web browser

Examples of header injection:

https://qualysguard.qg2.apps.qualys.com/portal-help/en/was/web_applications/scan_settings.htm

API Endpoint Definition

Qualys WAS supports basic security testing of REST and SOAP APIs. Identify API endpoints by attaching Postman Collections, BURP logs, or Swagger files to a Web app.

Set up Exclusion Lists

- **White List** – add URLs to white list to allow them to be scanned even if a black list would block it.
- **Black List** – Add URLs to blacklist to prevent them and their sub-directories from being scanned
- **POST Data Black List** - Define POST data lists to ensure blocking of form submission for POST requests in your web application as this could have unwanted side effects like mass emailing
- **Logout Regular Expression** - Define logout regular expression to ensure that the logout links of your web application will not be scanned
- **Parameters** – Define parameters to ensure these will be excluded from testing to improve scan efficiency

Default DNS Override

By default the scanner uses the DNS for the web application URL to crawl the web app and perform scanning. Select a DNS override record, to use the mappings in your record

Redundant Links

Links in the application that have the same content and may result in the scanner spending too much time crawling and assessing these URLs

Path Fuzzing Rules

If your application uses URL rewrite, use path fuzzing rules to specify the path components that need to be tested. More information can be found here:
https://qualysguard.qg3.apps.qualys.com/portal-help/en/was/web_applications/path_fuzzing_rules.htm

Form Training

Define an action URI, specific form field and its value to be substituted during crawling and fuzzing. This feature allows you to override a specific field's value in any given form

Malware Monitoring

Configure a malware scan to scan your web application for malwares. Read more here:
https://qualysguard.qg3.apps.qualys.com/portal-help/en/was/web_applications/malware_monitoring.htm

Qualys Browser Recorder

The QBR allows you to record your input decisions (e.g., keystrokes and mouse clicks) while you navigate the pages of any Web application. The script that is generated by QBR can then be replayed during your WAS scans, to perform your navigation steps and input decisions.

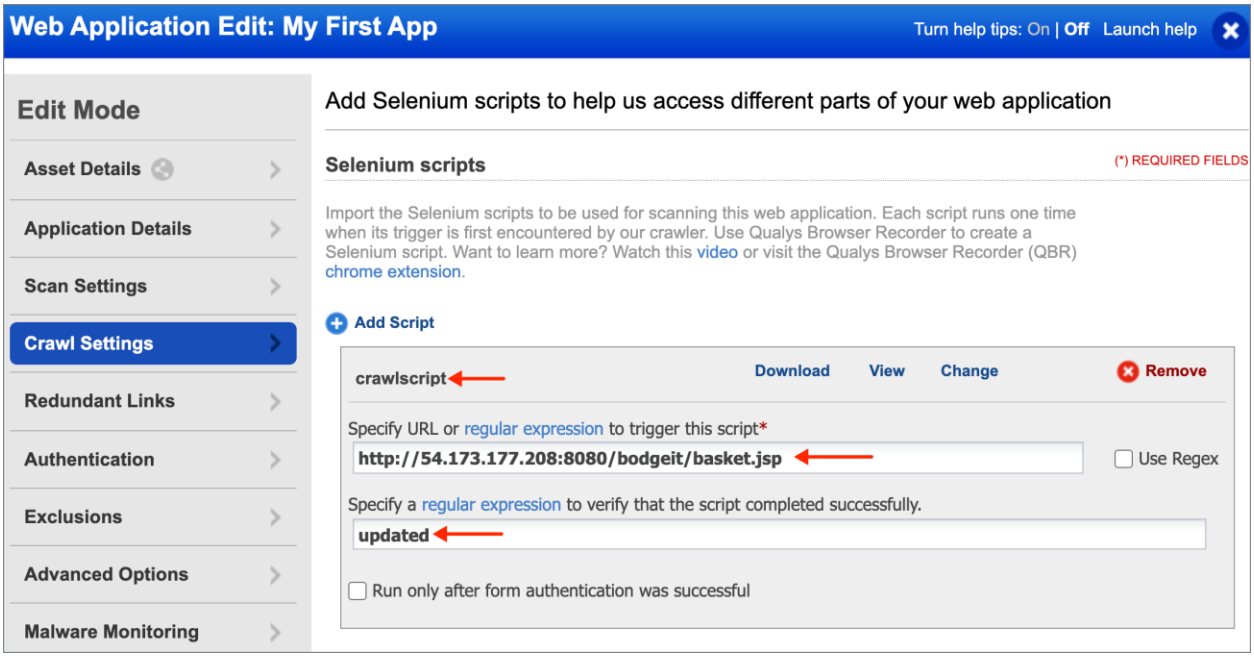
Crawl Script

Web applications often contain pages that require input from a knowledgeable application user, like the "Shopping Basket" page found in the BodgeIT Store.

Click the following link to view the "Crawl Script" tutorial for the "Bodgeit Store" shopping cart.

PLAY Lab 8 - http://ior.ad/7f7S

The crawl script can be uploaded to a Web application. This will cause the application to be crawled using the script.



When the scan is complete, look for QID 150100 to check for Selenium Diagnostics:

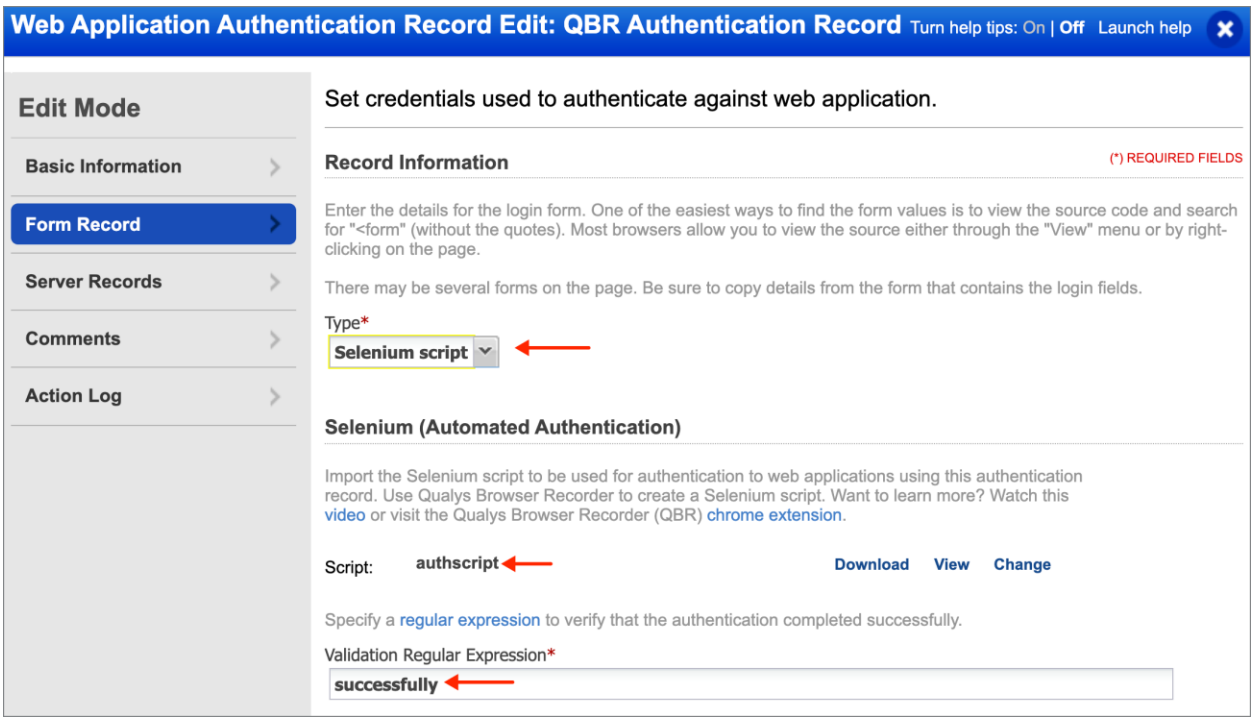
Authentication Script

The authentication script can be used to create an authentication record.

Click the following link to view the "Authentication Script" tutorial for the "Bodgeit Store" login page.

PLAY Lab 9 - http://ior.ad/7f8a

Detailed usage instructions for QBR can be found here - https://www.qualys.com/docs/qualys-browser-recorder-user-guide.pdf



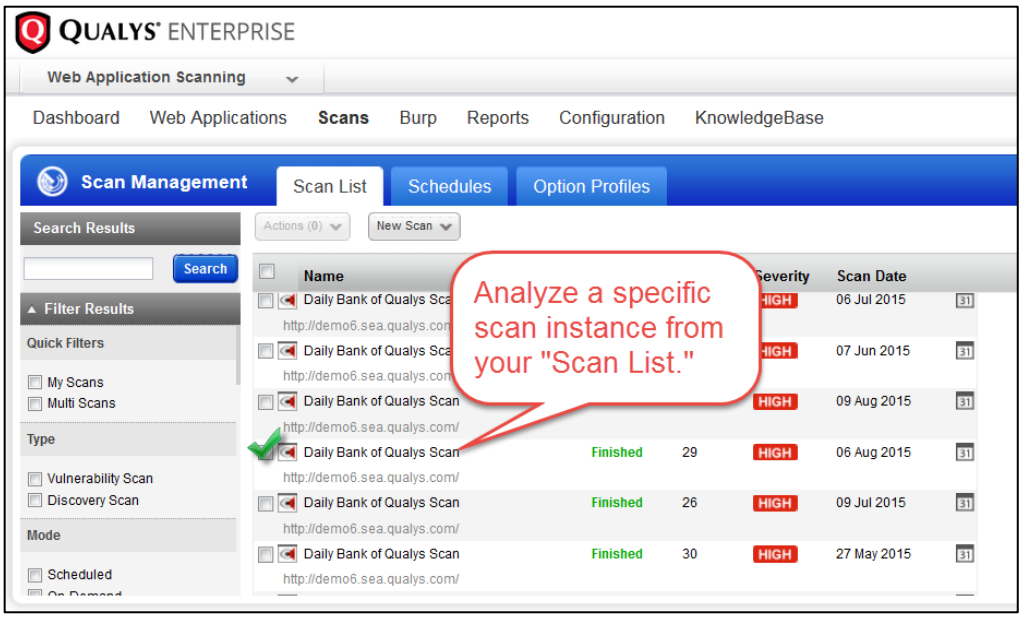
WAS Reporting

Currently, the Qualys Web Application Scanning service offers 4 types of reports: Web Application Report, Scorecard Report, Scan Report, and a Catalog Report.

- **Scan Report** – Reports on findings from specific scans.
- **Web Application Report** – Reports on aggregated findings from all scans.
- **Scorecard Report** – Provides an overall scorecard with high-level numbers and graphs.
- **Catalog Report** – Provides a catalog of web services processed from completed maps, vulnerability scans and WAS scans.

Scan Report

The Scan Report, focus on single scan instance and does not provide vulnerability history data.

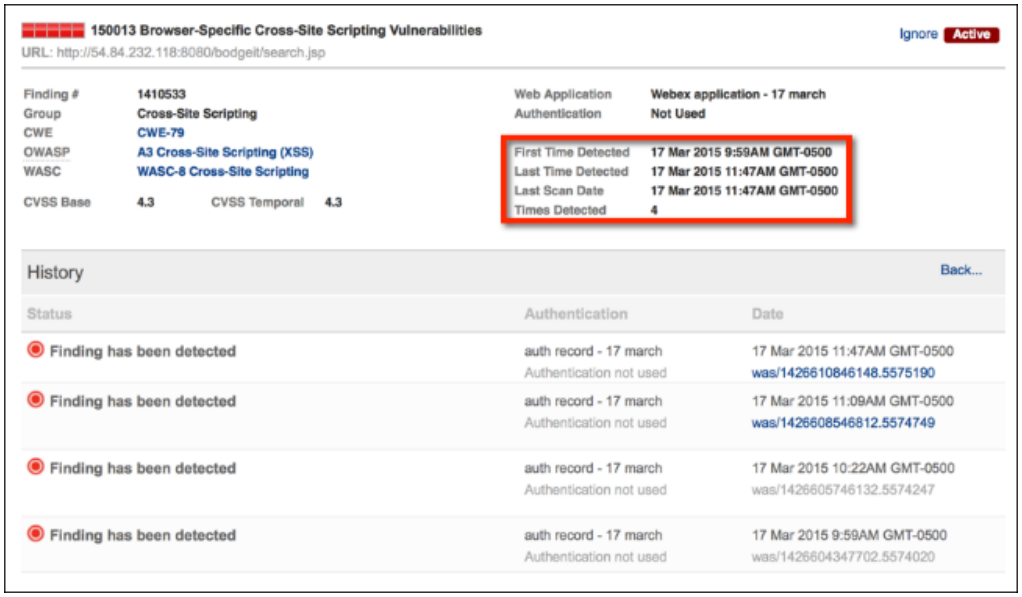


Click the following link to view the "Scan Report" tutorial.

PLAY Lab 10 - http://ior.ad/7ff3

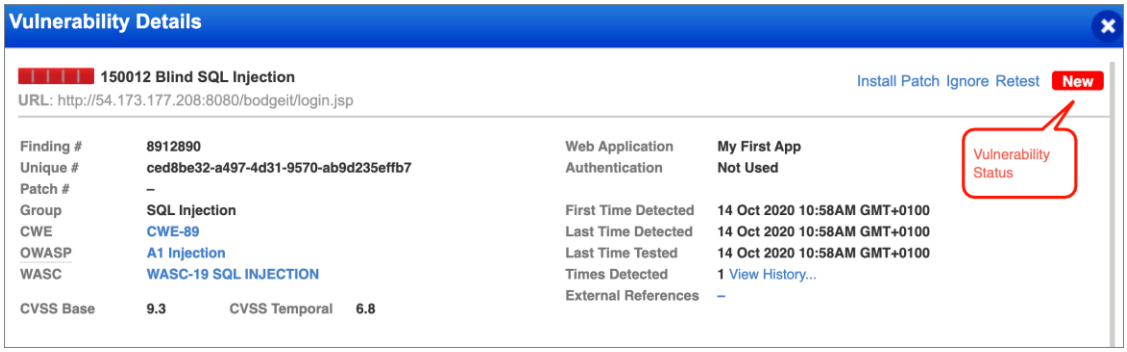
Web Application Report

The Web Application Report, combines all scans performed on a single Web application and therefore, vulnerability history and status (New, Active, Re-opened, Fixed) are included.



Click the following link to view the "Web App Report" tutorial.

PLAY Lab 11 - https://ior.ad/97AK



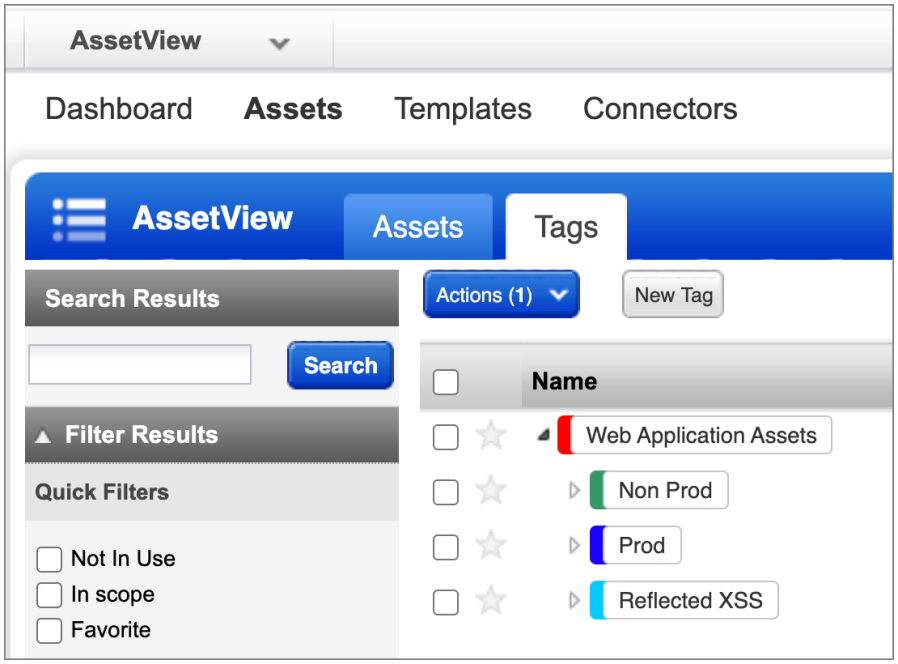
Vulnerability status – Web application reports show the status of vulnerabilities, it may be one of the following:

- New – vulnerabilities discovered for the first time in the latest scan
- Active – open vulnerabilities that have discovered more than once
- Fixed – vulnerabilities that have not been found in the latest scan
- Re-opened – vulnerabilities marked as fixed but detected again on the latest scan
- Ignored – vulnerabilities marked as ignored

Tagging

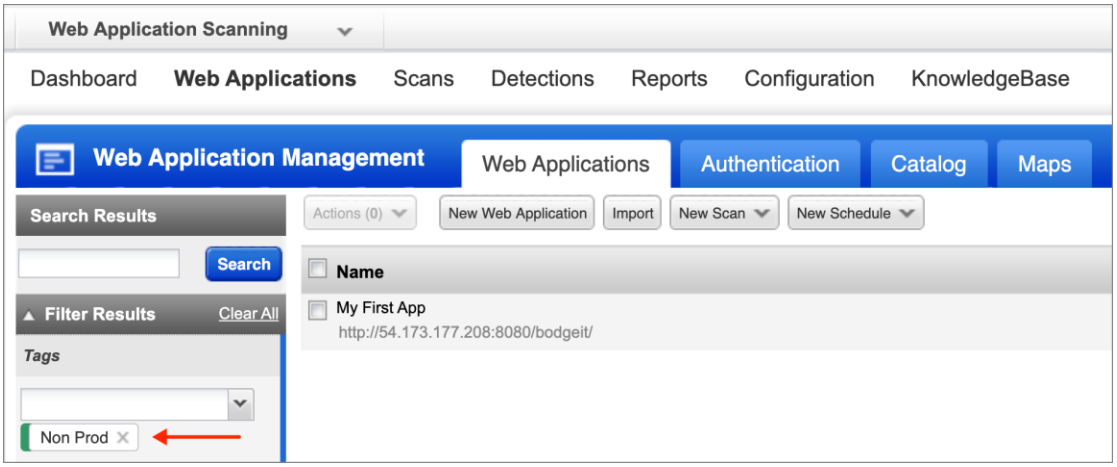
Tags are labels that can be applied to web applications. Tags can be used for filtering, scanning, and reporting purposes.

PLAY Lab 12 - https://ior.ad/7T5W

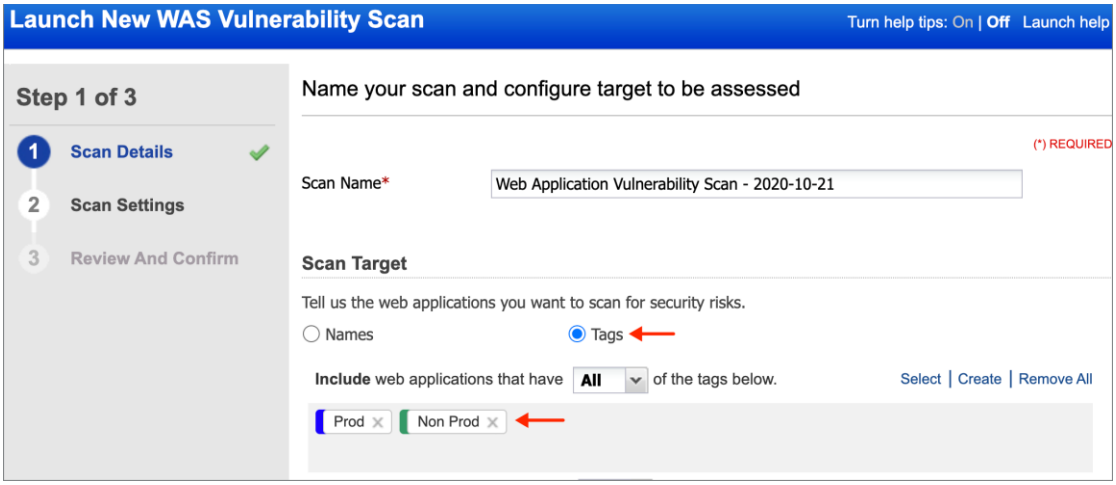


Tags are created from the Global AssetView (GAV) and CyberSecurity Asset Management (CSAM) applications.

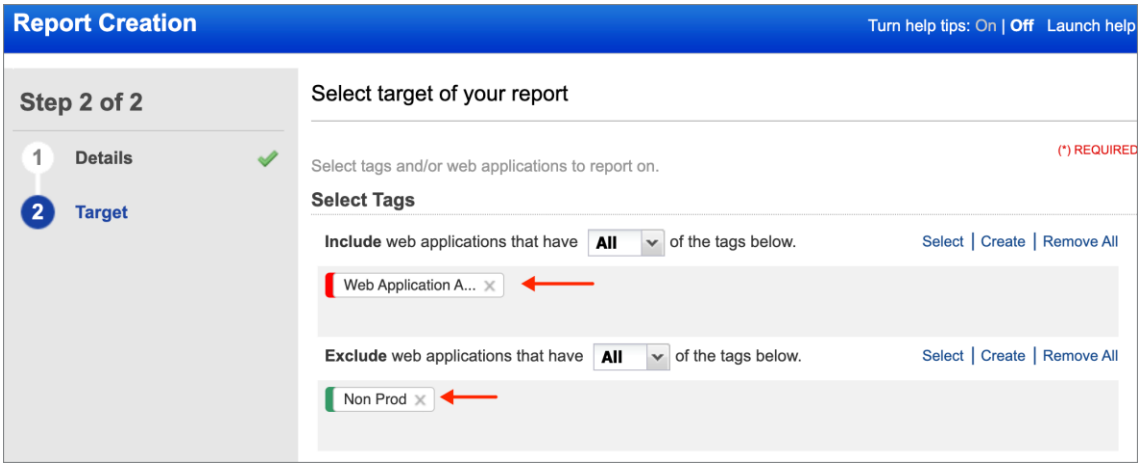
Use Tags for Filtering:



Use Tags for Scanning:



Use Tags for Reporting:



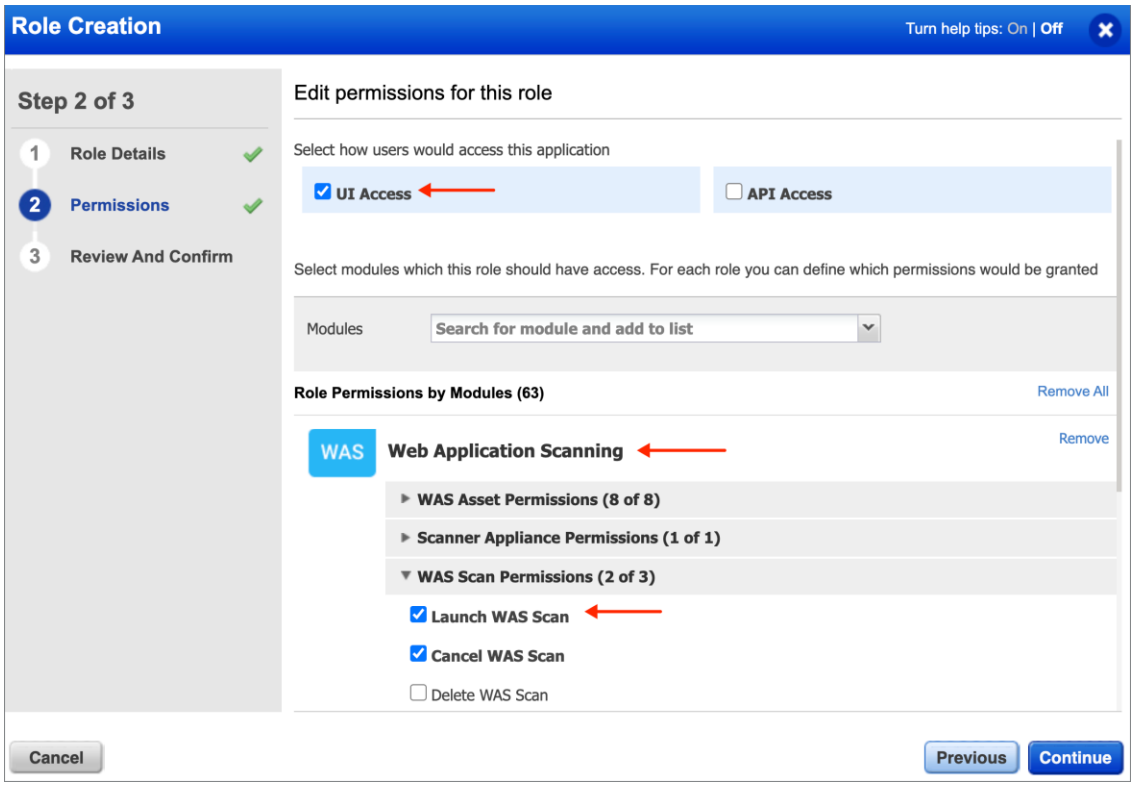
User Management

PLAY Lab 13 - https://ior.ad/97Lz

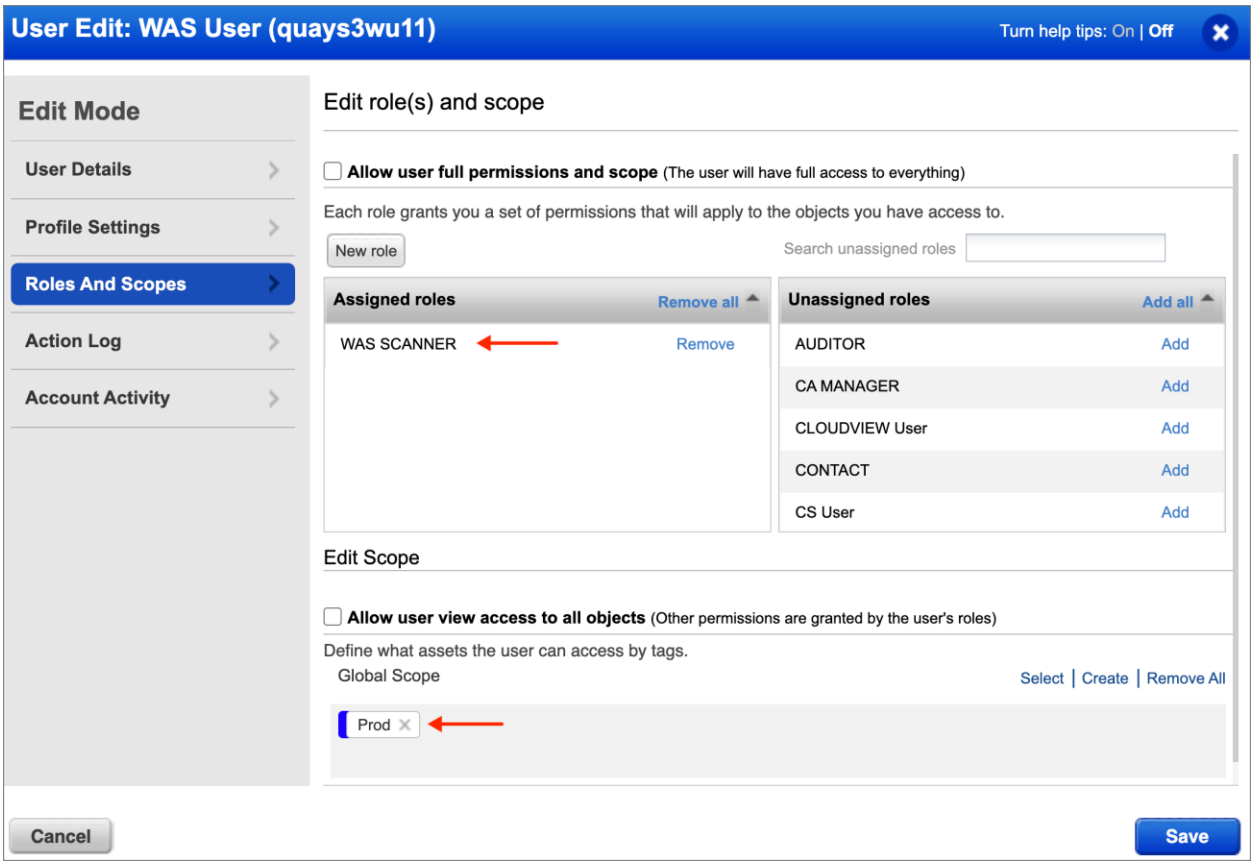
Users can be created from the Administration module. Once the user is created and activated, they will need to be given a scope and set of permissions from the interface.

Role Creation

To assign permissions to a user, first create a role from the Administration module. The role allows you to define the applications the user will have access to, how the user is allowed to access (UI or API), and permissions the user will have on the allowed applications.



By assigning the role to the user's profile, you can define the permissions available to the user. The scope of the user can be limited by attaching tags to the user's profile.

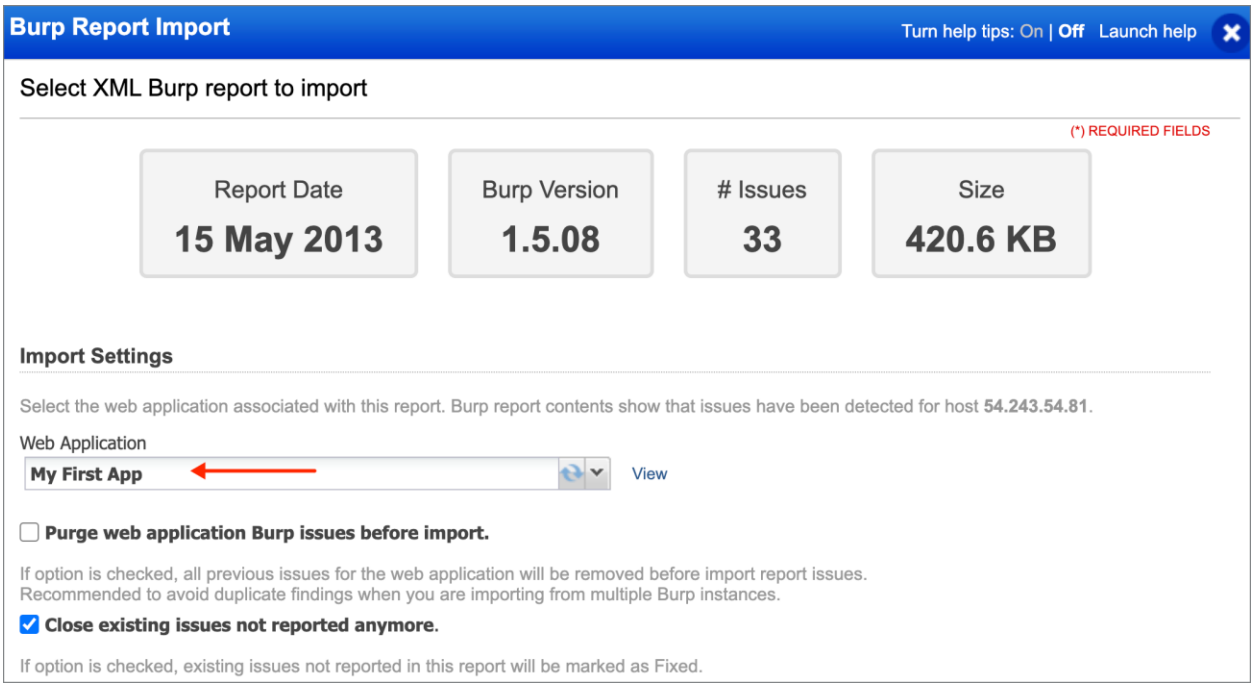

User Edit: WAS User (quays3wu11)
Turn help tips: On | Off
Edit Mode
User Details
Profile Settings
Roles And Scopes
Action Log
Account Activity
Edit role(s) and scope
Allow user full permissions and scope (The user will have full access to everything)
Each role grants you a set of permissions that will apply to the objects you have access to.
New role
Search unassigned roles
Assigned roles
Remove all
WAS SCANNER
Remove
Unassigned roles
Add all
AUDITOR
Add
CA MANAGER
Add
CLOUDVIEW User
Add
CONTACT
Add
CS 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
Prod
Cancel
Save

Burp Integration

PLAY Lab 14 -
https://ior.ad/97Nj

Qualys offers integration with Burp. Burp is an attack proxy used for automated and manual penetration testing. This can be used in tandem with Qualys for sensitive applications that need thorough testing.

With this integration, Burp Suite Professional (BSP) results can be uploaded to Qualys. This allows Qualys to act as a centralized storage location for scan results from Burp, to go along with the results already obtained by the Qualys WAS service.



When importing BURP results into WAS, the BURP results must be associated with a specific Web Application.

Appendix A: Web App Examples

The examples provided in this appendix, demonstrate the different ways a Web Application can be defined. This will impact the total number of Web apps added to your WAS subscription.

EXAMPLE SITE 1

`http://e-commerce:80/browse.cgi`
`http://e-commerce:443/login.cgi`

Scenario:

- WAS users only need to define the *starting* port.
- The scanner will discover all ports in other links.
- (1 app total)

It is common for Web sites to provide open access (i.e., HTTP, port 80) to public pages and then require authentication (i.e., HTTP, port 443) to access secure or restricted pages within the site. **WAS scans use HTTP or HTTPS and ANY port**. Therefore, sites that provide links with different port numbers do not need to define separate WAS Web apps (as long as all links fall within the application scope). Keep in mind that WAS will require an appropriate authentication record to reach pages that require authentication credentials.

EXAMPLE SITE 2

`http://intranet:80/index.cgi`
`http://intranet:8080/index.cgi`

Scenario 1:

- If the app on port 80 has links to app on port 8080
- Links are same business function (1 app total)

Scenario 2:

- If Link on port 80 serves a separate, unrelated business functions than the link on port 8080.
- (2 apps total)

Here's another example where WAS will automatically adjust to different port numbers used on the same site. As long as the two links support the same business function, a single WAS Web app is appropriate.

However; If the link on port 80 serves a separate business function than the link on port 8080, two WAS Web apps are required.

EXAMPLE SITE 3

```
http://intranet/admin/
http://intranet/hr/
http://intranet/finance
```

Scenario 1:

- Each directory is part of a single app if they are part of an Intranet Portal
- (1 app total)

Scenario 2:

- Authentication credentials are different for each, with different business functions
- (3 apps total)

If a single login page provides access to all three URLs (i.e., they encompass a single business function where users require the ability to navigate between them) then a single WAS Web app is appropriate.

However, if these URLs serve three separate business functions (i.e., separate logins for each URL), create three distinct WAS Web apps.