Qualys Web Application Scanning

Qualys.

Starting the Lab Tutorial

Navigate to the URL provided in the lab tutorial supplement to start the tutorial for a topic:

PLAY **Lab 1**: WAS KnowledgeBase
https://ior.ad/7Aty

1

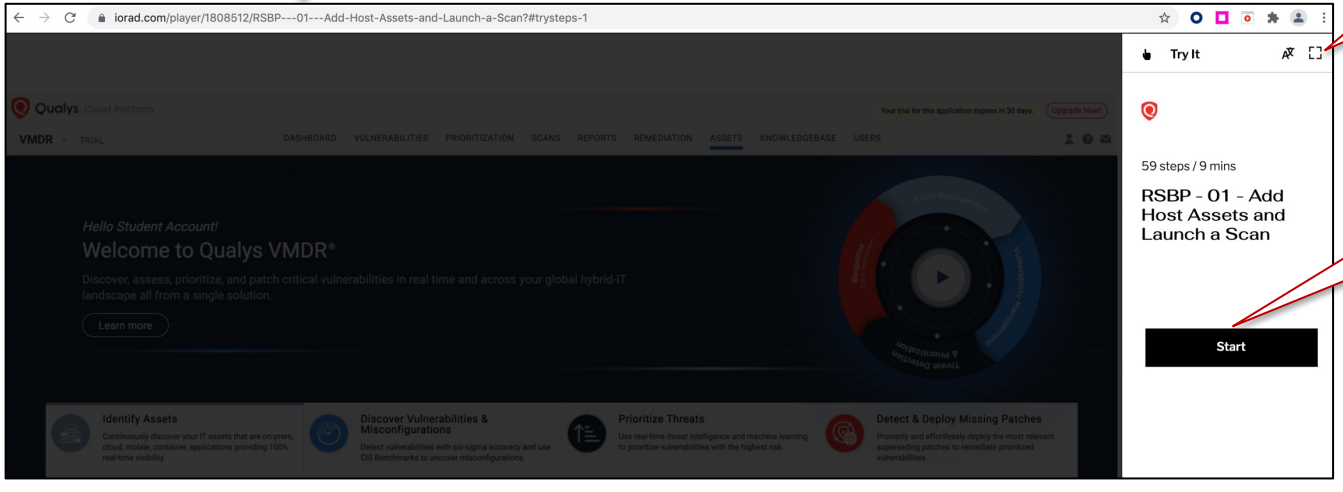
Open this link or copy/paste the link in a separate browser window/tab

2

Maximize the screen

3

Start the tutorial



Qualys.

Agenda

Qualys Web Application Scanning

Session One:

- WAS Overview
- Basic Web Application Setup
  - Basic Info
  - Crawl Settings
  - Default Scan Settings
- Discovery Scan (Crawling)
- Advanced Web App Setup

Session Two:

- Additional Configurations
- Web App Testing (Vulnerability Scan)
- WAS Reporting
- Tags and Users
- WAS Integrations

Qualys.

Web Application Scanning Overview

Qualys.

WAS Overview

Automated Testing (Fault Injection)

- Submit “specially crafted” characters
- Observe the server’s response
- This represents 80 – 85% of Web app vulnerabilities

Manual Testing (BURP Integration)

- Automated tools effectively detect Web application bugs (SQL execution inside user input)
- Human beings are much better at discovering program design flaws

Qualys.

What Do Automated Tools Miss?

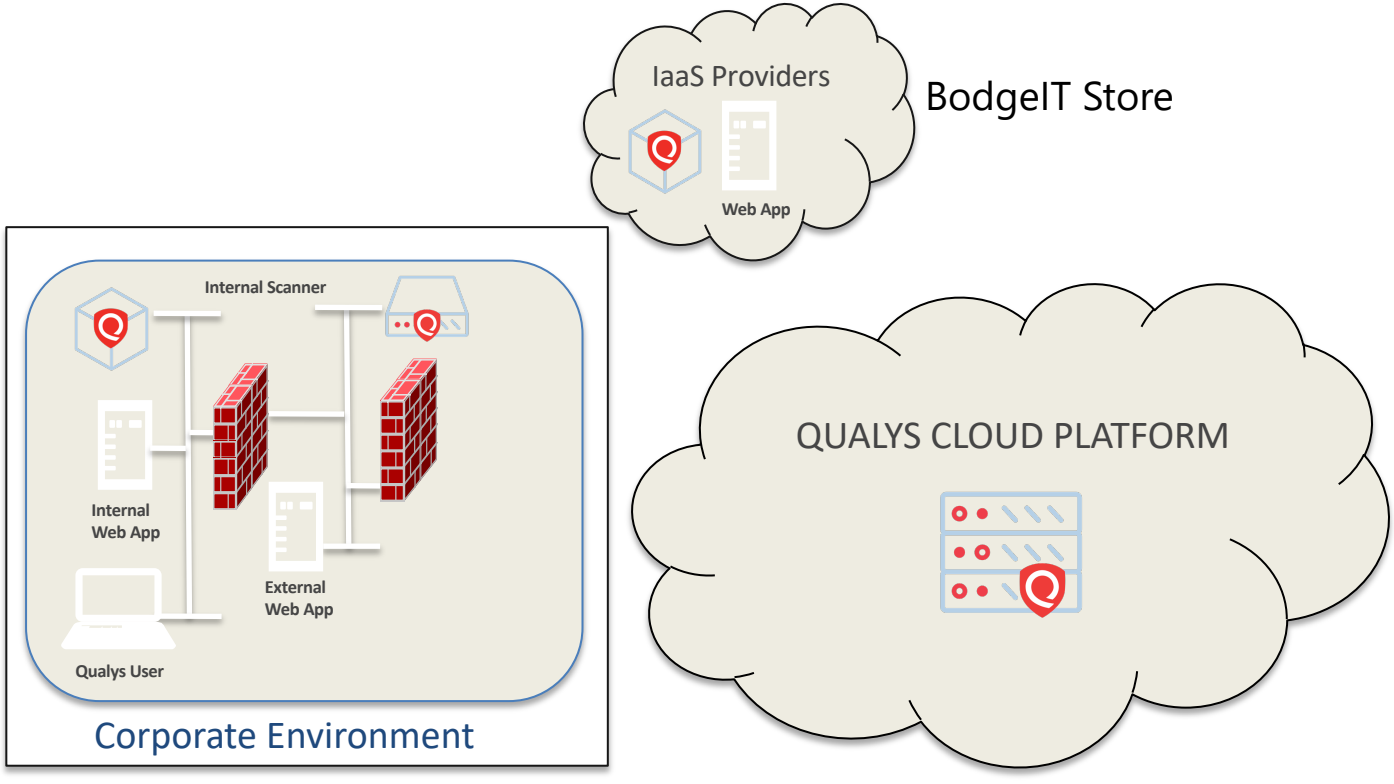
These typically require manual testing and detection:

- **Design Flaws & Logic Errors**: Manually enter URL into browser's address field to force access to an unauthorized page (i.e., point of authentication vs. point of authorization attack).

- **Permission Errors**: Public file share that has employee payroll or medical records.

Qualys.

Qualys Cloud Platform

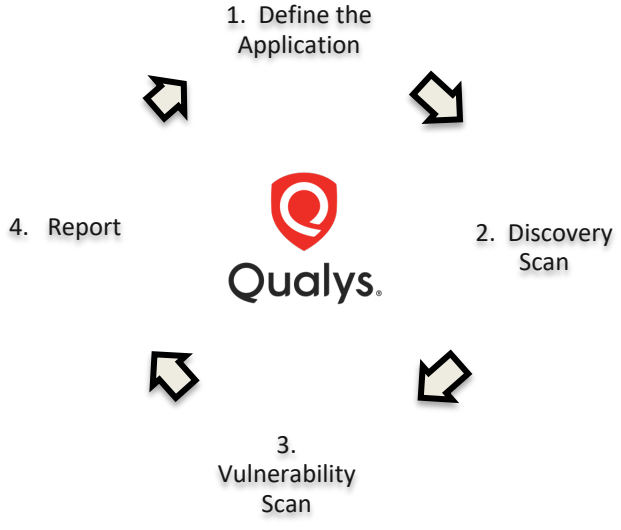


Qualys.

WAS Workflow

The workflow for analyzing a Web application involves five steps:

1. Define Web Application
2. Perform Discovery Scan (i.e., Crawl)
3. Perform Vulnerability Scan
4. Create Vulnerability Report
5. Fix Vulnerabilities

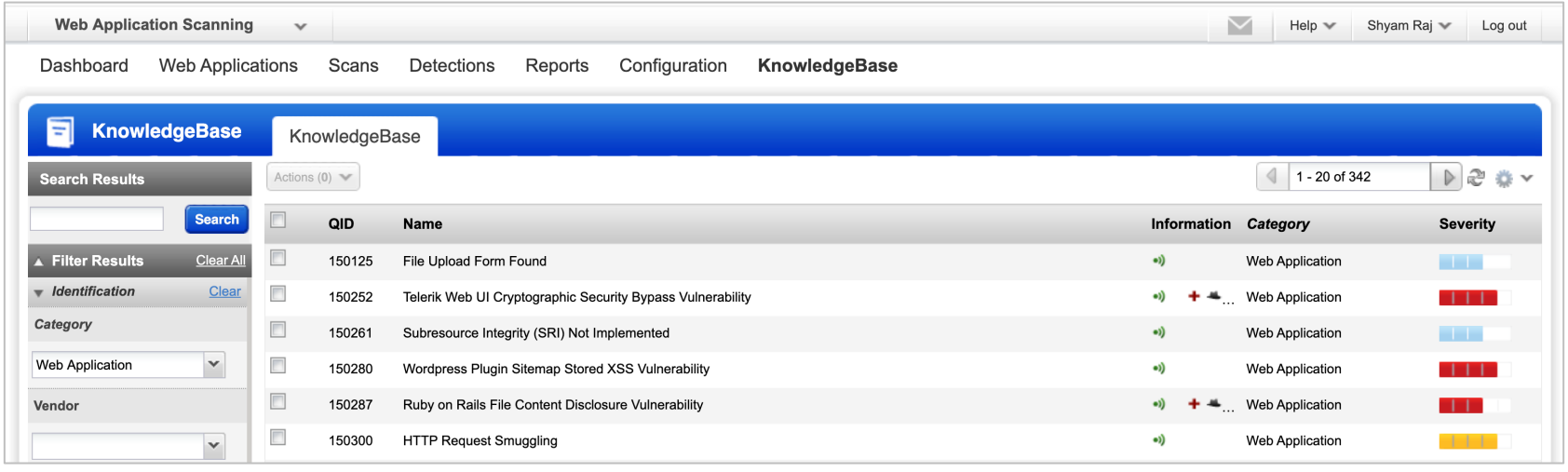


Qualys.

KnowledgeBase & Search Lists

Qualys.

What does Qualys WAS check?



- WAS QIDs fall under the “Web Application” category in the KnowledgeBase.
- WAS QIDs begin with 150xxx.

Qualys.

Lab Tutorials

Please follow **pages 3 – 5** from the Lab Tutorial Supplement

- Lab 1 – KnowledgeBase, p. 4

Qualys.

Web App QIDs

Confirmed Vulnerabilities

Severity	Level	Description
	Minimal	Basic information disclosure (e.g. web server type, programming language) might enable intruders to discover other vulnerabilities, but lack of this information does not make the vulnerability harder to find.
	Medium	Intruders may be able to collect sensitive information about the application platform, such as the precise version of software used. With this information, intruders can easily exploit known vulnerabilities specific to software versions. Other types of sensitive information might disclose a few lines of source code or hidden directories.

Potential Vulnerabilities

Severity	Level	Description
	Minimal	Presence of this vulnerability is indicative of basic information disclosure (e.g. web server type, programming language) and might enable intruders to discover other vulnerabilities. For example in this scenario, information such as web server type, programming language, passwords or file path references can be disclosed.
	Medium	Presence of this vulnerability is indicative of basic information disclosure (e.g. web server type, programming language) and might enable intruders to discover other vulnerabilities. For example version of software or session data can be disclosed, which could be used to exploit.

Sensitive Content

Severity	Level	Description
	Minimal	Sensitive content was found in the web server response. During our scan of the site form(s) were found with field(s) for credit card number or social security number. This information disclosure could result in a confidentiality breach and could be a target for intruders. For this reason we recommend caution.
	Medium	Sensitive content was found in the web server response. Specifically our service found a certain sensitive content pattern (defined in the option profile). This information disclosure could result in a confidentiality breach and could be a target for intruders. For this reason we recommend caution.

Information Gathered

Severity	Level	Description
	Minimal	Intruders may be able to retrieve sensitive information related to the web application platform.
	Medium	Intruders may be able to retrieve sensitive information related to internal functionality or business logic of the web application.
	Serious	Intruders may be able to detect highly sensitive data, such as personally identifiable information (PII) about other users of the web application.

Qualys.

Search List

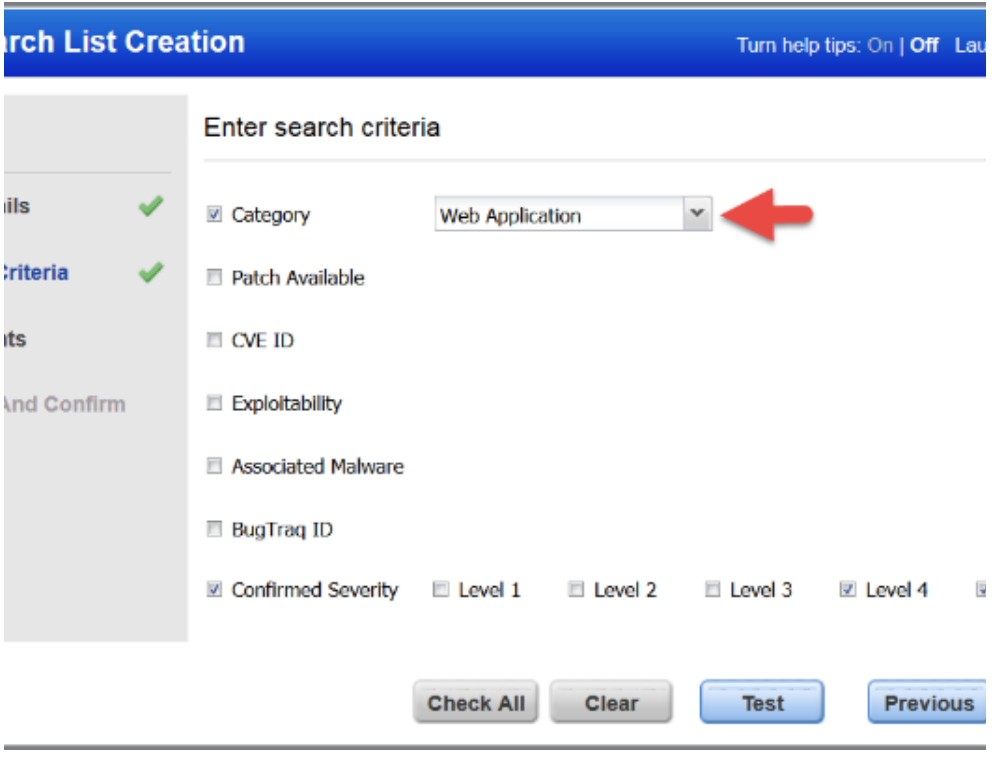
User-defined list of QIDs:

- **Dynamic** - Automatically updated based on list criteria.
- **Static** - Must be updated manually.

Scan and report exclusively on the vulnerabilities in a Search List.

Examples:

- Run a scan just for SQLi.
- Build a report for only XSS.



Qualys.

Lab Tutorials

Please follow **pages 3 – 5** from the Lab Tutorial Supplement

- Lab 2 – Search List, p. 4

Qualys.

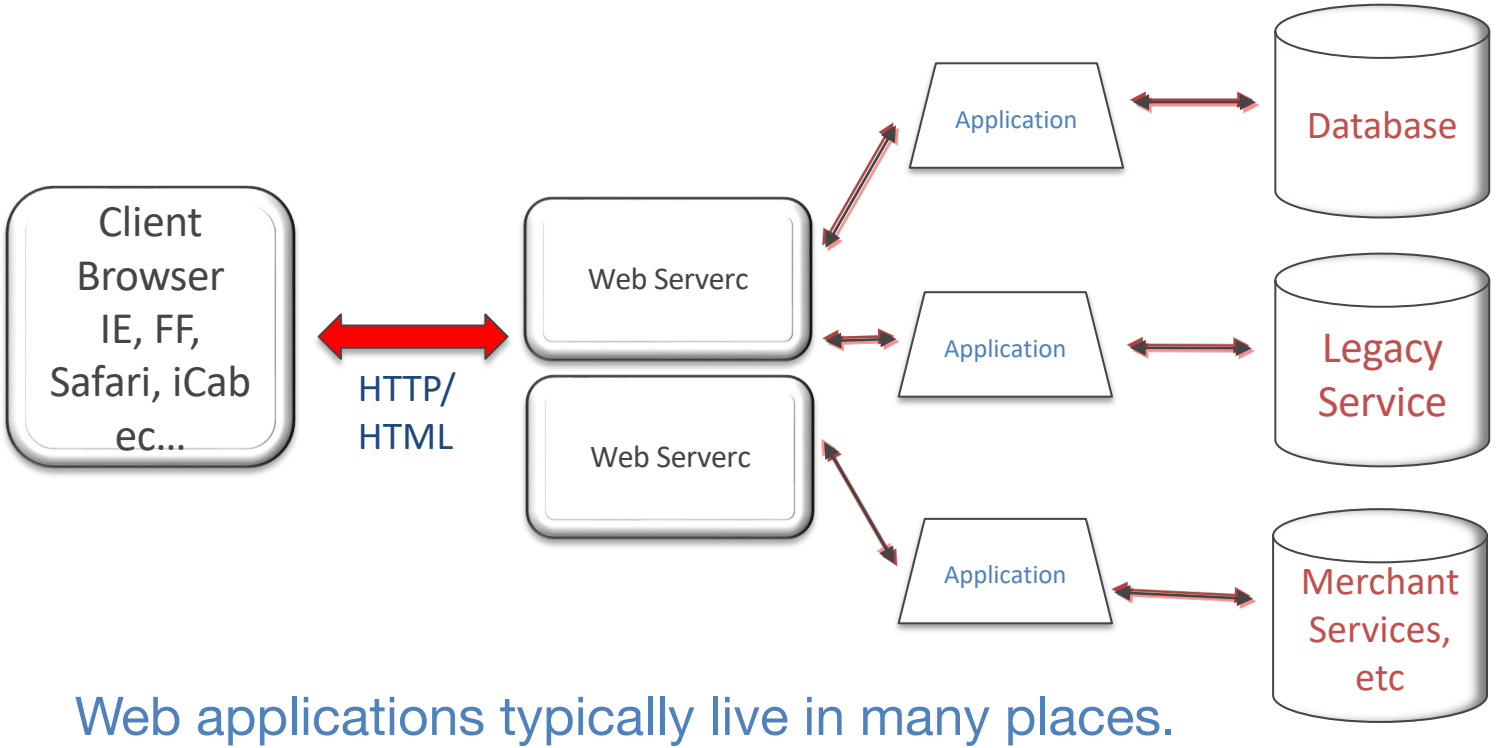
Basic Web Application Setup

Qualys.

Qualys WAS Lifecycle

Qualys.

Multi-tier Web App Architecture



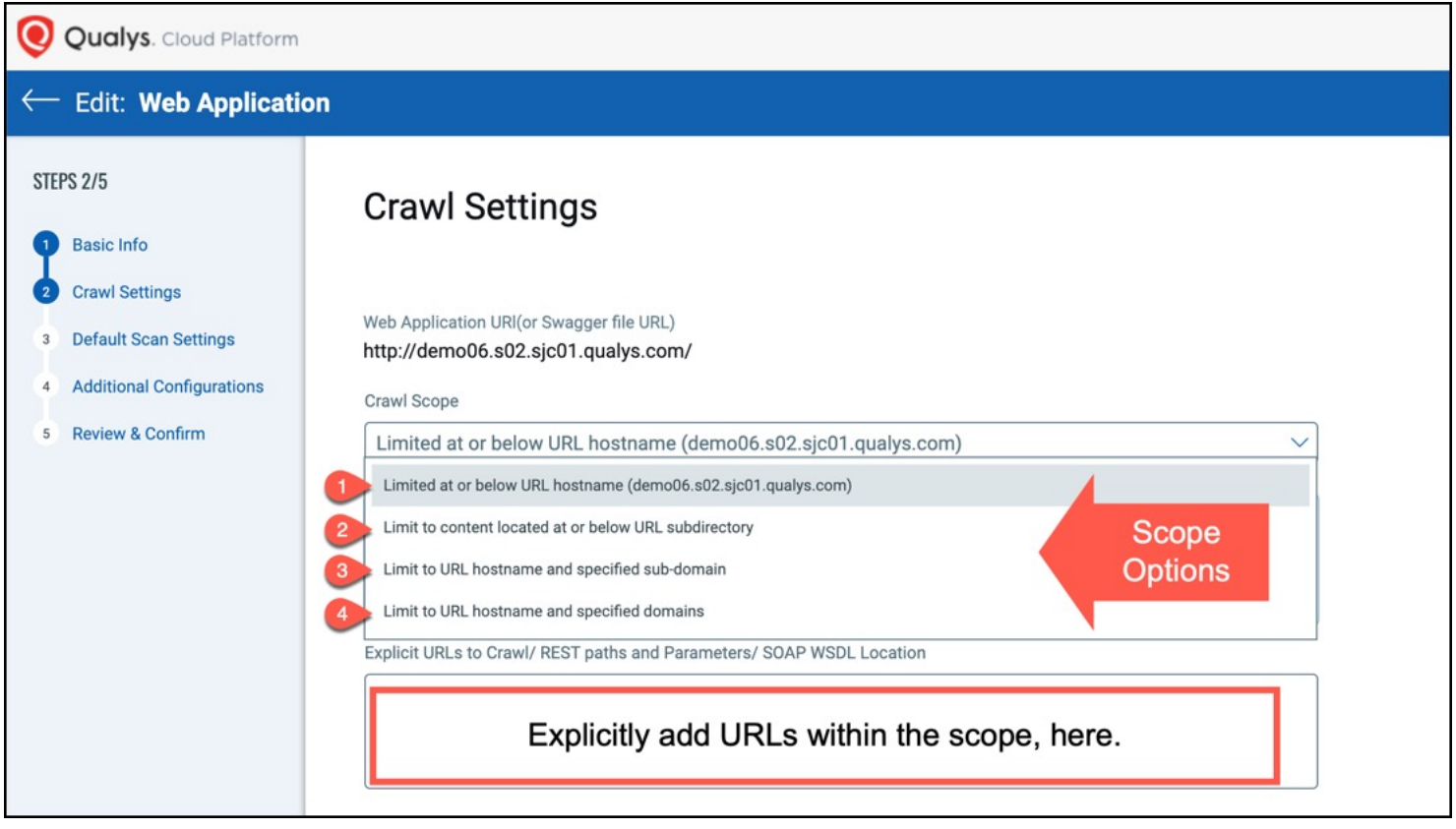
Web applications typically live in many places.

Qualys.

Defining a Web Application

- Uniquely identifiable entry point (URL):
  `protocol://hostname[:port]/[path/]file`
  - BODGEIT STORE: http://54.173.177.208:8080/bodgeit/
  - BANK of QUALYS: http://demo06.s02.sjc01.qualys.com
- Uniquely distinguishable application code
- Supports a specific business function.
- Associated with a specific development team.
- APPLICATION SCOPE (Crawl Scope)
  - Covers presentation, application logic and database layers.
  - May span multiple hosts, domains, or subdomains.
  - Often designed to meet failover and scalability objectives.

Crawl Scope Options



Any URLs explicitly added must fall within the selected Crawl Scope.

Qualys.

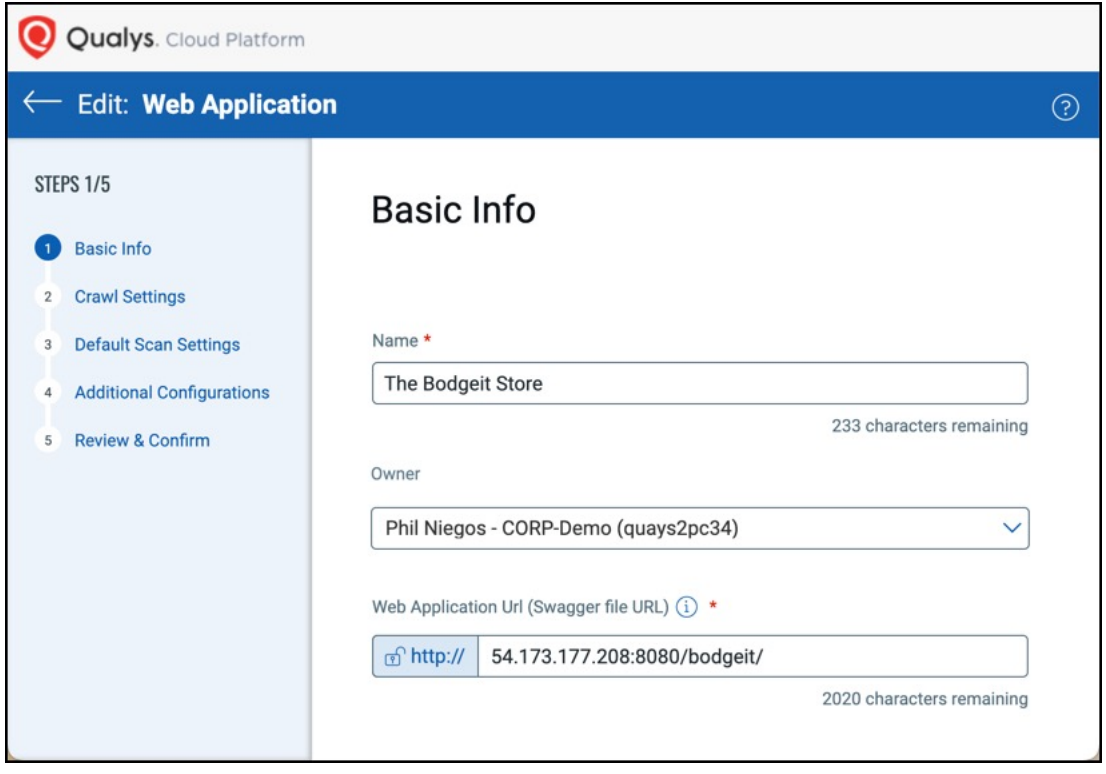
Lab Tutorials

Please follow **pages 6 – 8** in the Lab Tutorial Supplement

- Lab 3 – Bodgeit Store Web App,
- Lab 4 – Standard Login Authentication, p. 6

Qualys.

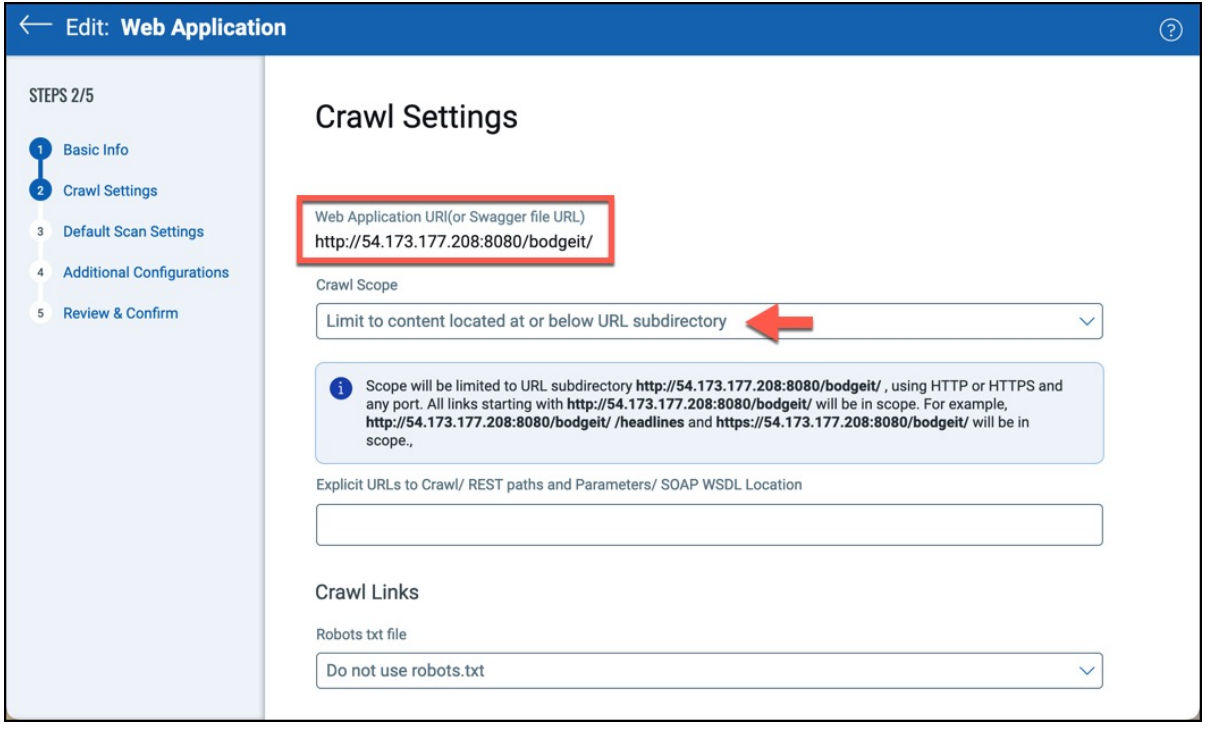
Basic Info



The Web Application URL specifies the starting point of Web app scans and contains an IP address or fully qualified domain name (FQDN).

Qualys.

Crawl Settings

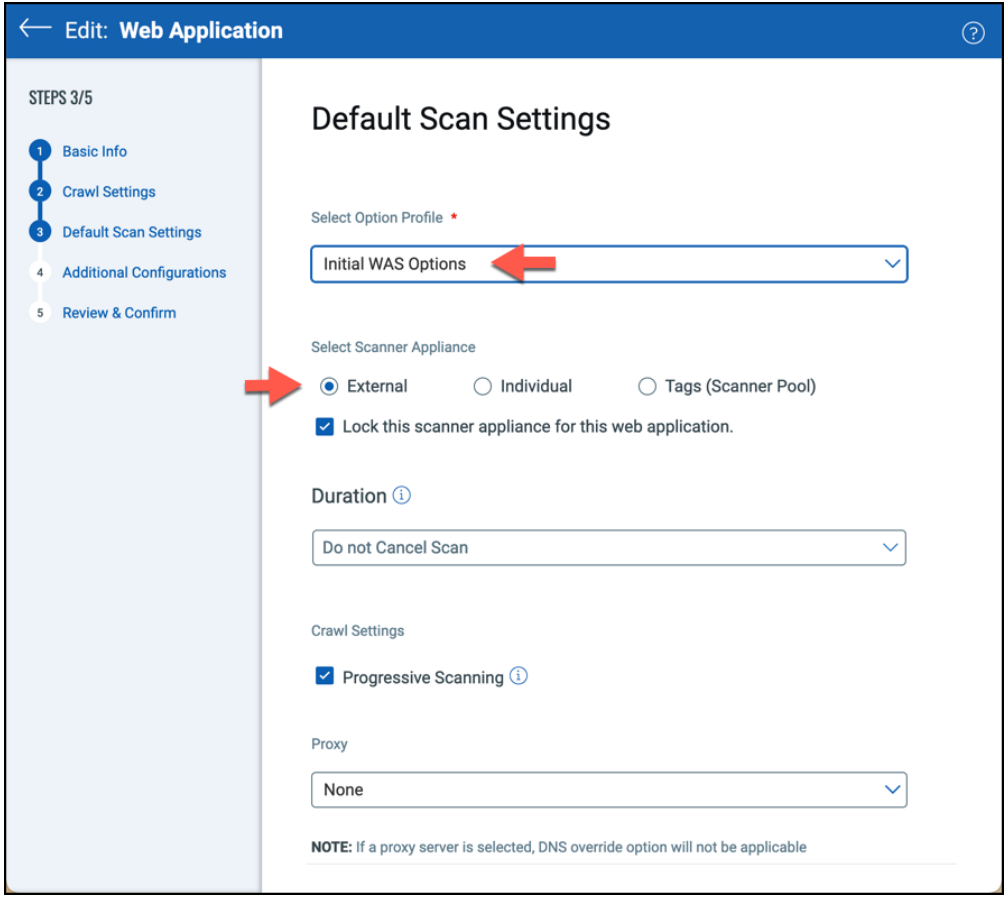


Bodgeit Store Scope: Limit to content located at or below URL subdirectory.

`http://54.173.177.208:8080/bodgeit/`

Qualys.

Default Scan Settings



Many of the options specified here in the Default Scan Settings (including the Option Profile) can be adjusted or changed at scan time.

Qualys.

Option Profile

Qualys.

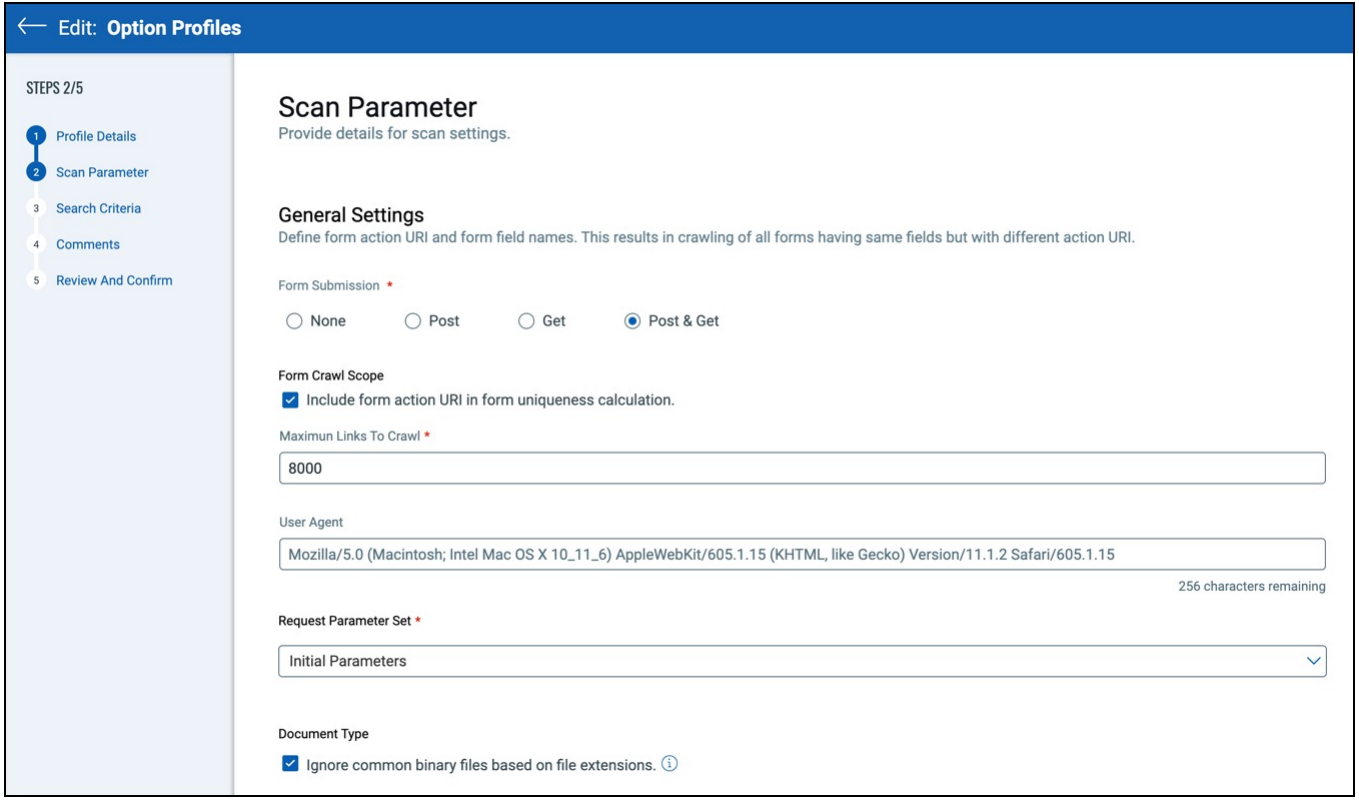
Lab Tutorial

Please follow **pages 9 – 11** from the Lab Tutorial Supplement

- Lab 5 – Option Profile, p. 9

Qualys.

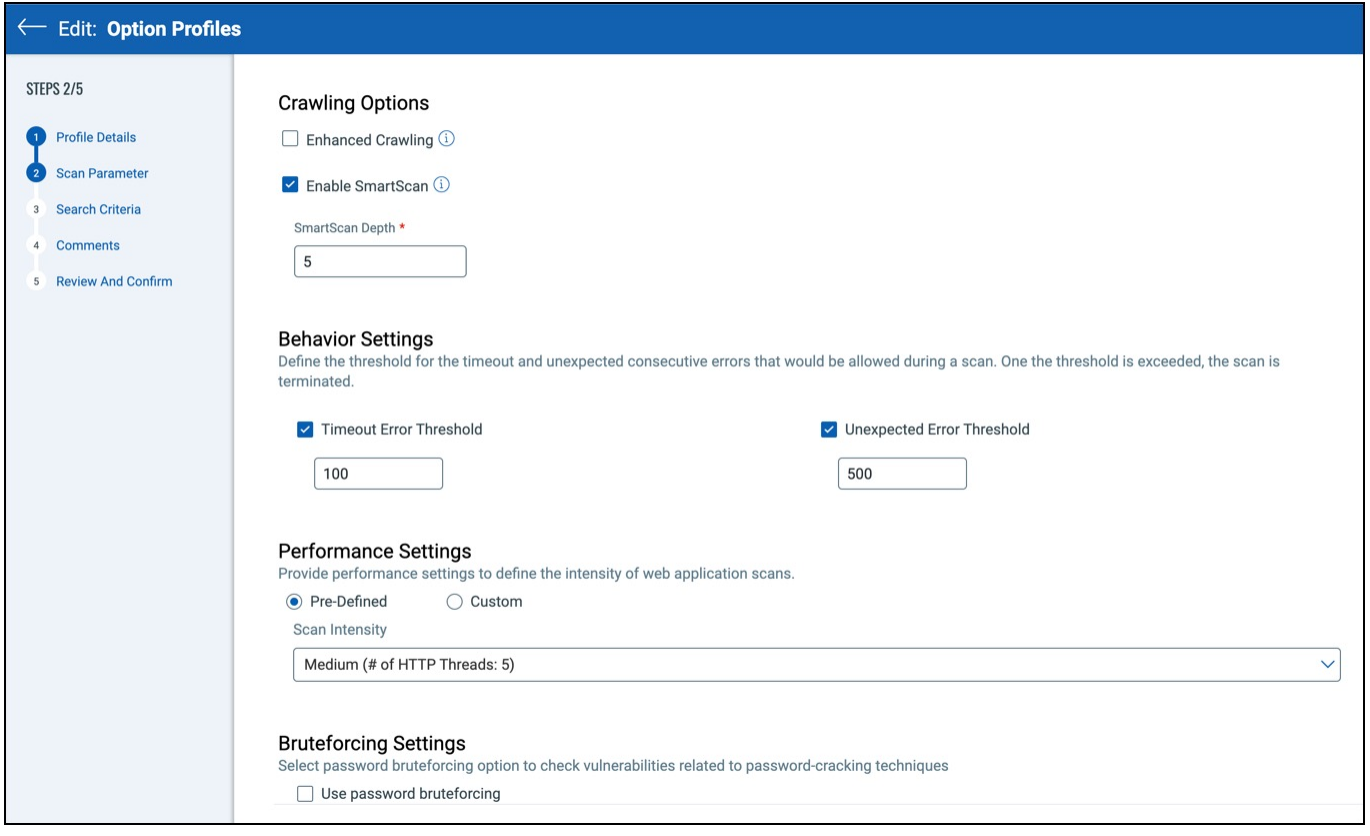
Option Profile Scan Parameters



General Settings

Qualys.

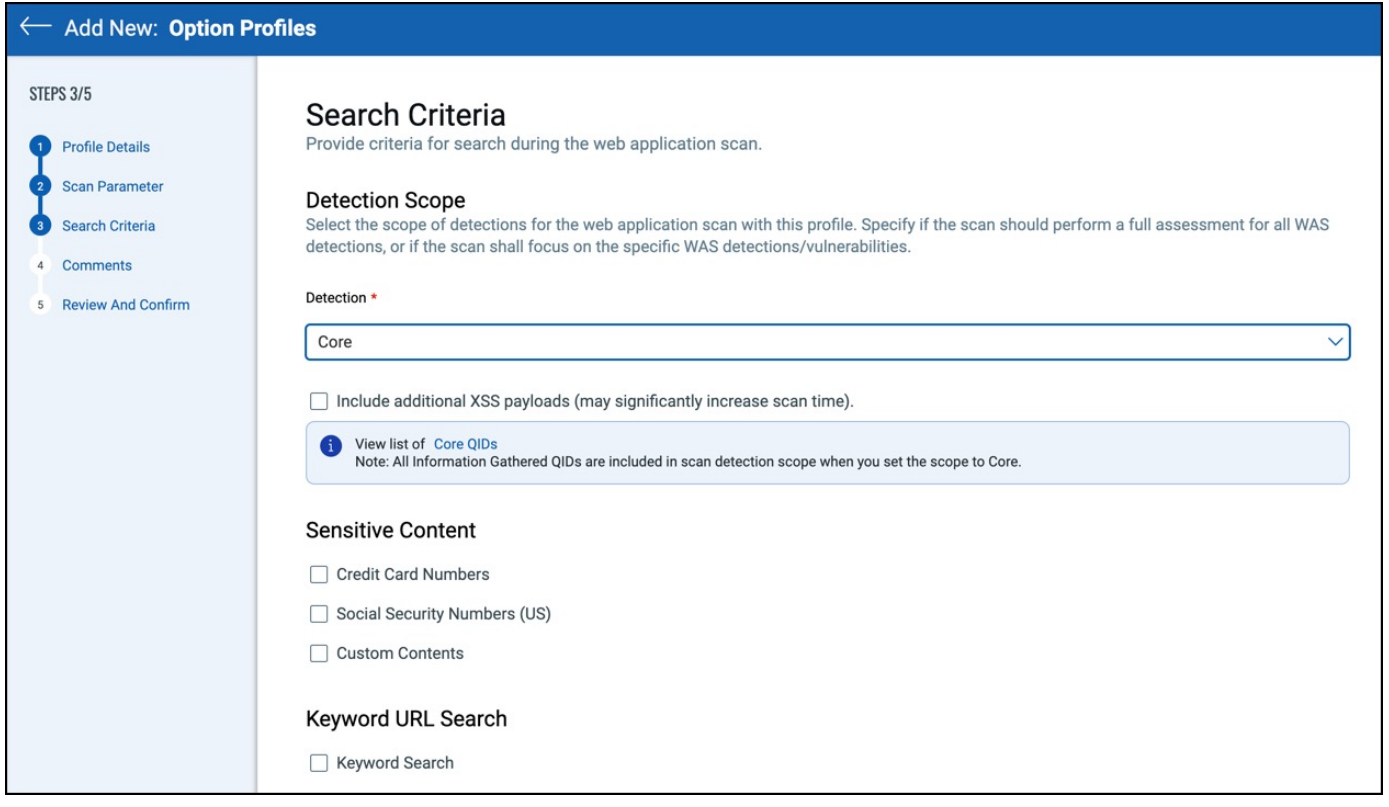
Option Profile Scan Parameters (cont.)



Crawling, Behavior, Performance, and Bruteforcing

Qualys.

Option Profile Search Criteria



Detection Scope, Sensitive Content, and Keyword URL Search

Qualys.

Session Break

Qualys.

Discovery Scan (Crawling)

Qualys.

Qualys WAS Lifecycle

Qualys.

Discovery

1. Scan begins at starting URL identified in the application definition.
2. Using the Scope Options identified in the Web app's Crawl Settings, the scan follows links to discover pages and content.
3. Configuration data is collected from the target app and its host.
4. Vulnerability testing is not performed.

Qualys.

The Crawl

HTML-based links

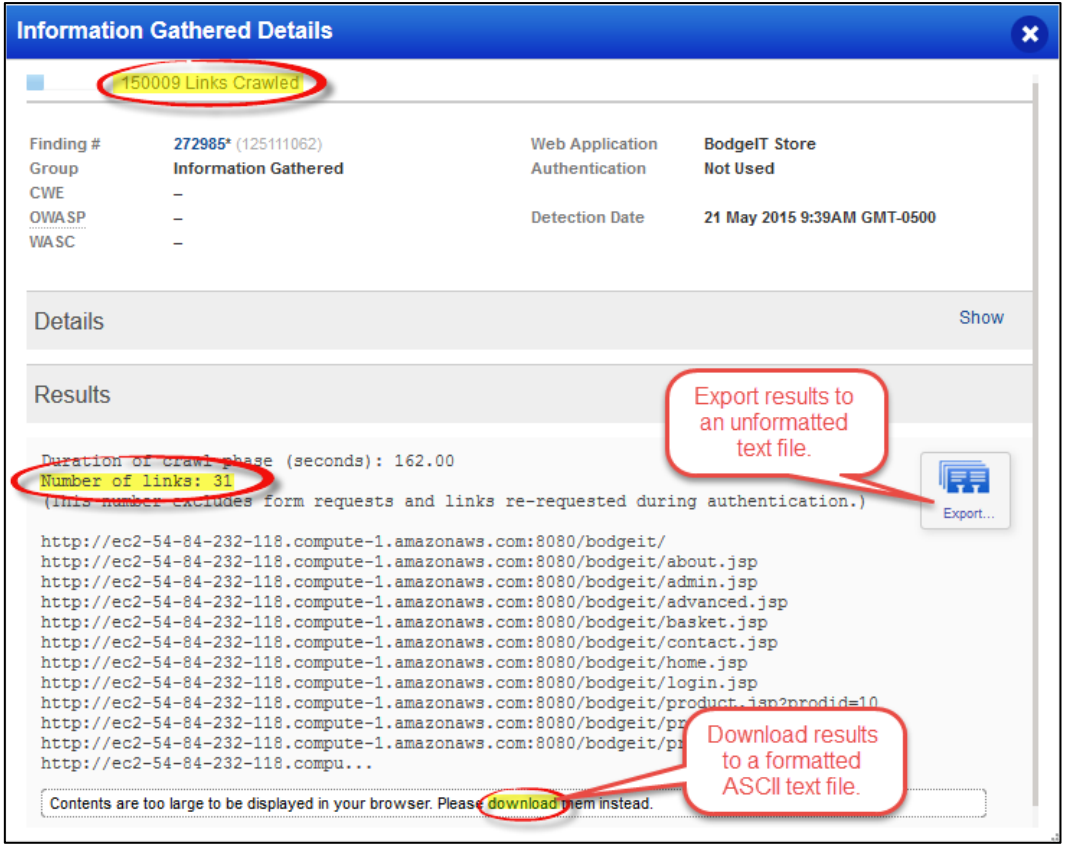
```
<li class="heading underline"><a href="/company/newsroom/news-releases/">Newsroom</a></li>
<li><a href="/company/newsroom/news-releases/">News Releases</a></li>
<li><a href="https://community.qualys.com/blogs" target="_blank">Qualys Blogs</a></li>
<li><a href="/company/newsroom/media-coverage/">Media Coverage</a></li>
<li><a href="/research/security-alerts/">Security Alerts</a></li>
```

Links via JavaScript

```
<script src="/asset/vendor/modernizr/border-image.js"></script>
<script src="//ajax.aspnetcdn.com/ajax/jQuery/jquery-1.7.2.min.js"></script>
<script src="//d1dejaj6dcgv24.cloudfront.net/vendors/jquery.tools-1.2.7.min.gz.js"></script>
<script src="//d1dejaj6dcgv24.cloudfront.net/vendors/jquery.easing-1.3.min.gz.js"></script>
<script src="/asset/script/main.js"></script>
<script type="text/javascript" src="/asset/script/homepage.js"></script>
```


Qualys.

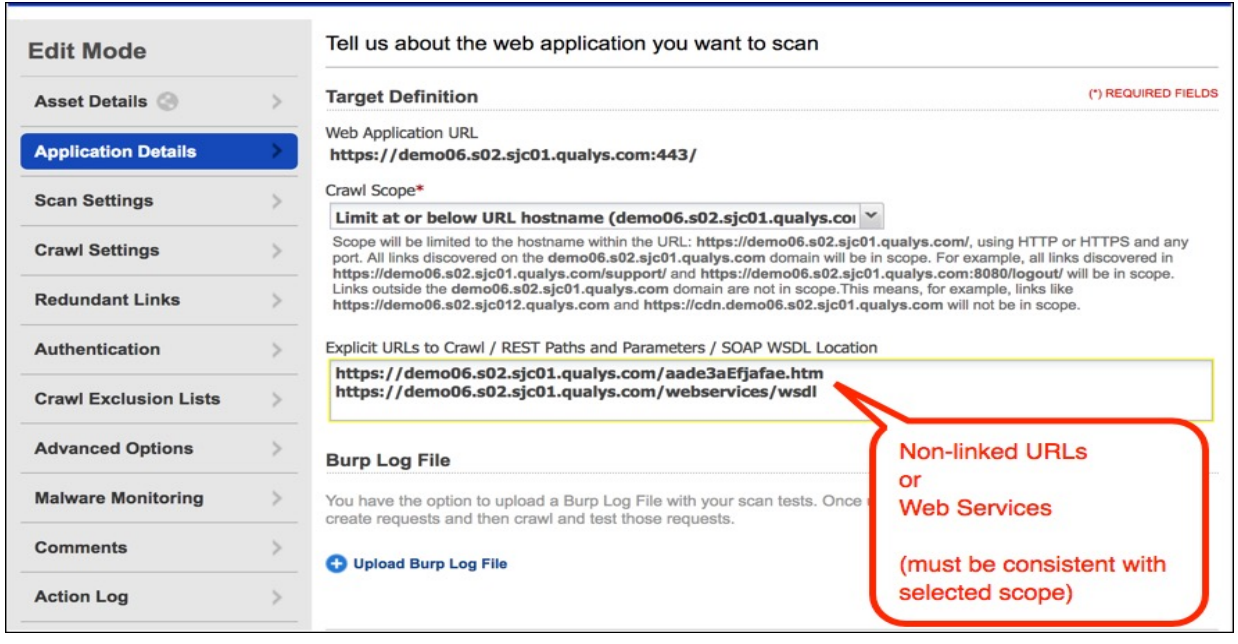
QID 150009 - Links Crawled



Qualys.

Explicit URLs to Crawl

- Specify URLs you want the service to crawl
- Useful for pages not linked to other pages in the application



Qualys.

QID 150115 - Authentication Form Found

```
Authentication form found at: http://demo06.s02.sjc01.qualys.com/
Action uri: http://demo06.s02.sjc01.qualys.com/
Fields: login, password, action, submit
```

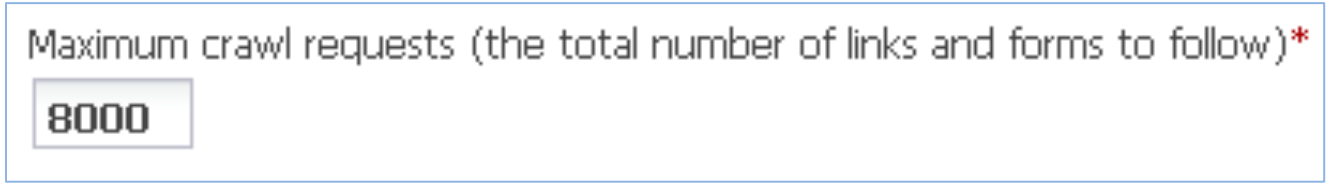
Standard HTTP Login Form

Qualys.

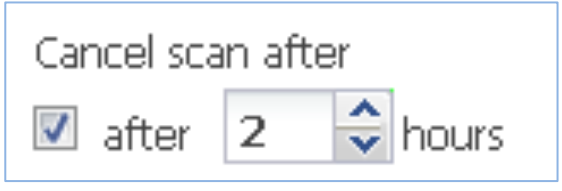
When does a Discovery Scan End?

Crawl stops when:

- Max number of links threshold is met



- No new links are discovered
- Scan time-out is reached



**Default max. scan time = 24 hrs.*

Qualys.

“No Web Service”

Scan will return “No Web Service” status if the scanner:

- Cannot get a DNS lookup on the site
- Cannot reach the target because of routing
- Cannot get a web service to respond to a GET request

Lab Tutorials

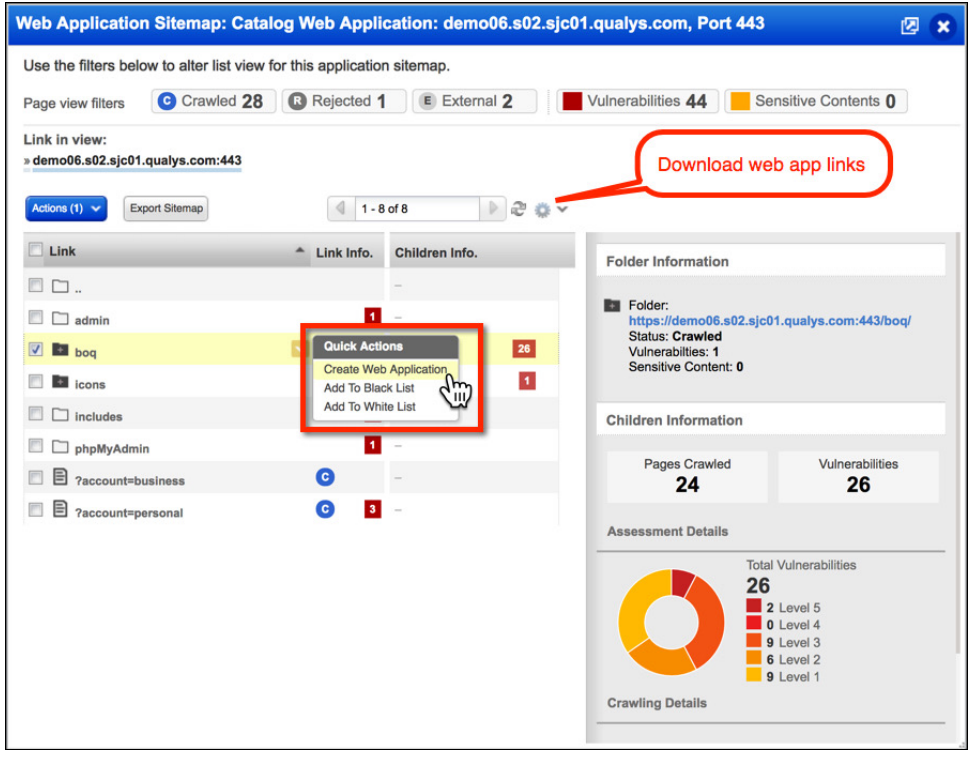
Please follow **pages 12 - 14 in** the Lab Tutorial Supplement

- Lab 6 – Web App Scanning, p. 12

Qualys.

Web Application Sitemap

- View pages crawled
- Create new Web apps
- Add URLs to Black List
- Add URLs to White List



Lab Tutorials

Please follow **page 15 in** the Lab Tutorial Supplement

- Lab 7 – Sitemap, p. 15

Qualys.

Basic Web App Setup Review

1. Basic Info

- Web application name and URL
- Custom attributes and Asset Tags

2. Crawl Settings

- Crawl Scope
- Crawl Links (Selenium scripts)

3. Default Scan Settings

- Option Profile (Form Uniqueness, Enhanced Crawling, SmartScan)
- Progressive Scanning

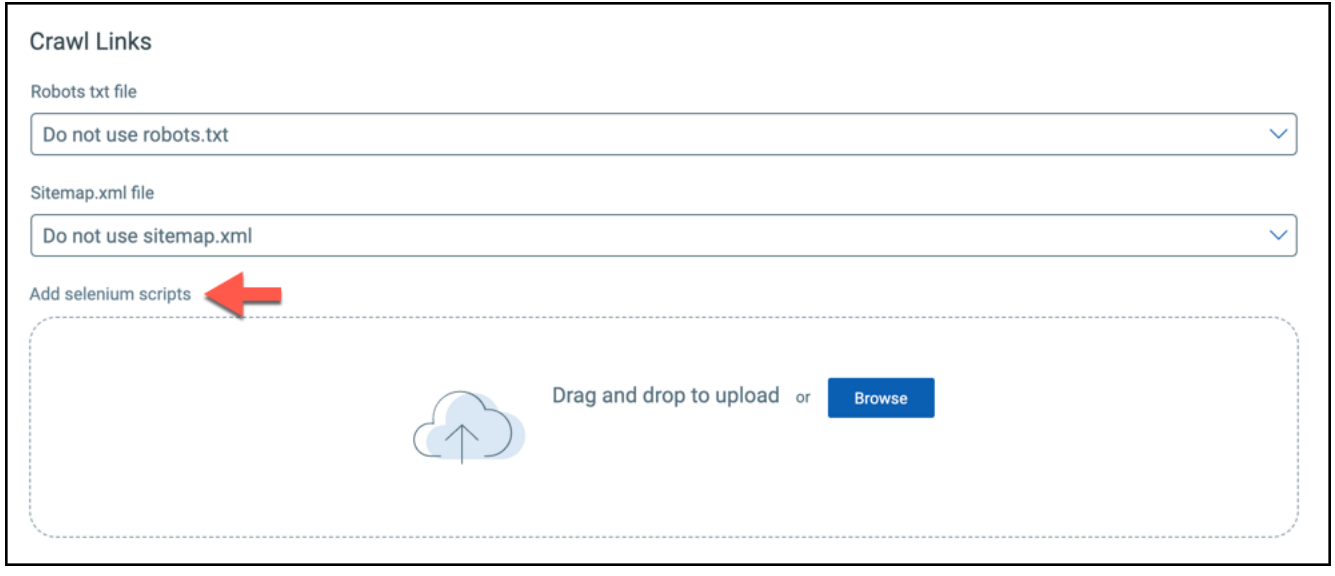
4. Additional Configurations

Qualys.

Advanced Web App Setup

Qualys.

Crawl Settings: Selenium Scripts



Add a script created with Qualys Browser Recorder.

Qualys.

Lab Tutorials

Please follow **pages 18 – 19** from the Lab Tutorial Supplement

- Lab 8 – QBR Crawl Script, p. 18

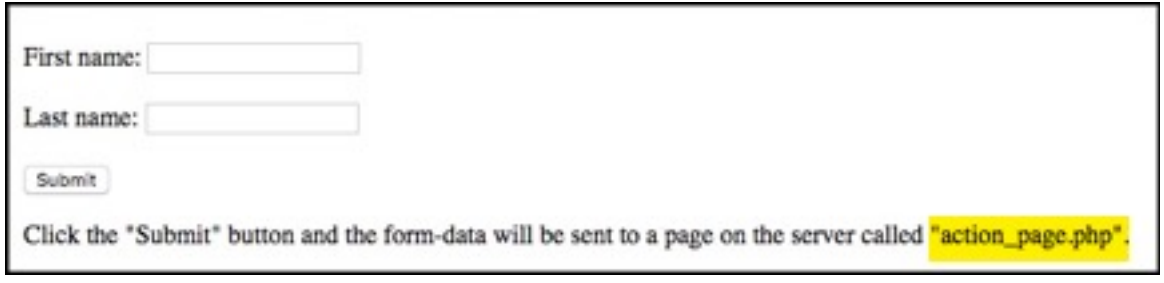
Qualys.

Option Profile: Form Crawl Scope

Form Crawl Scope

☑ Include form action URI in form uniqueness calculation.

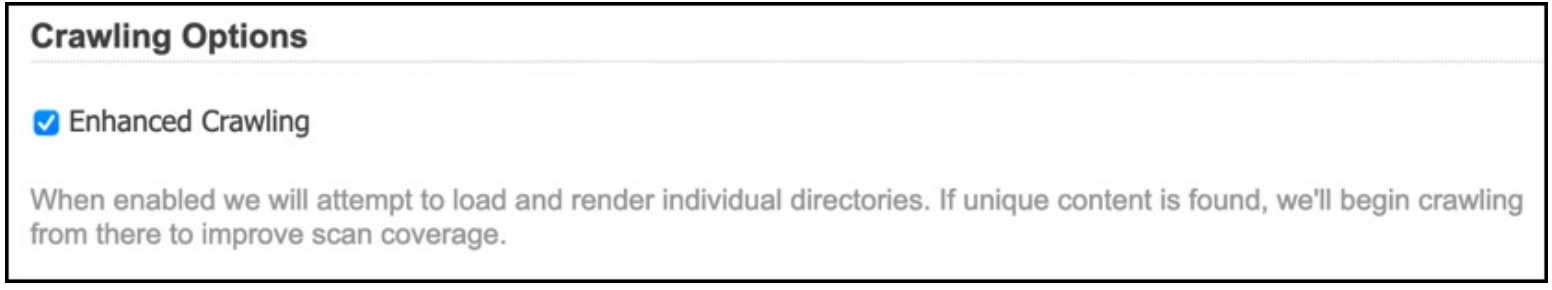
When enabled, form uniqueness is calculated using the form action URI in addition to form field names.




```
<form action="/action_page.php" method="get">
  <label for="fname">First name:</label>
  <input type="text" id="fname" name="fname"><br><br>
  <label for="lname">Last name:</label>
  <input type="text" id="lname" name="lname"><br><br>
  <input type="submit" value="Submit">
</form>
```

Qualys.

Option Profile: Enhanced Crawling



If the following link is found during crawling: https://www.example.com/foo/abc/xyz/register.php

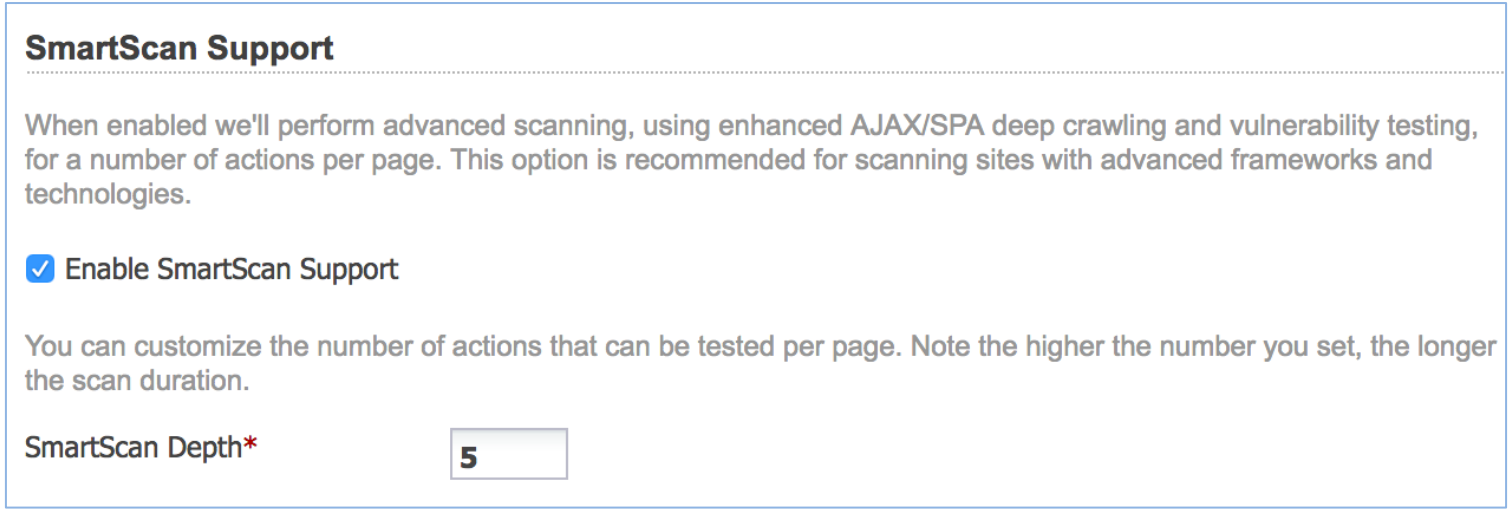
Step 1 : We make a request https://www.example.com/foo/abc/xyz/
Step 2 : Remove the directory "xyz/" from the URL and crawl https://www.example.com/foo/abc/
Step 3 : Further remove the directory ”abc/" from the URL and crawl, https://www.example.com/foo/

Objects found during this process will get added to the crawl queue thus improving the scan coverage.

Qualys.

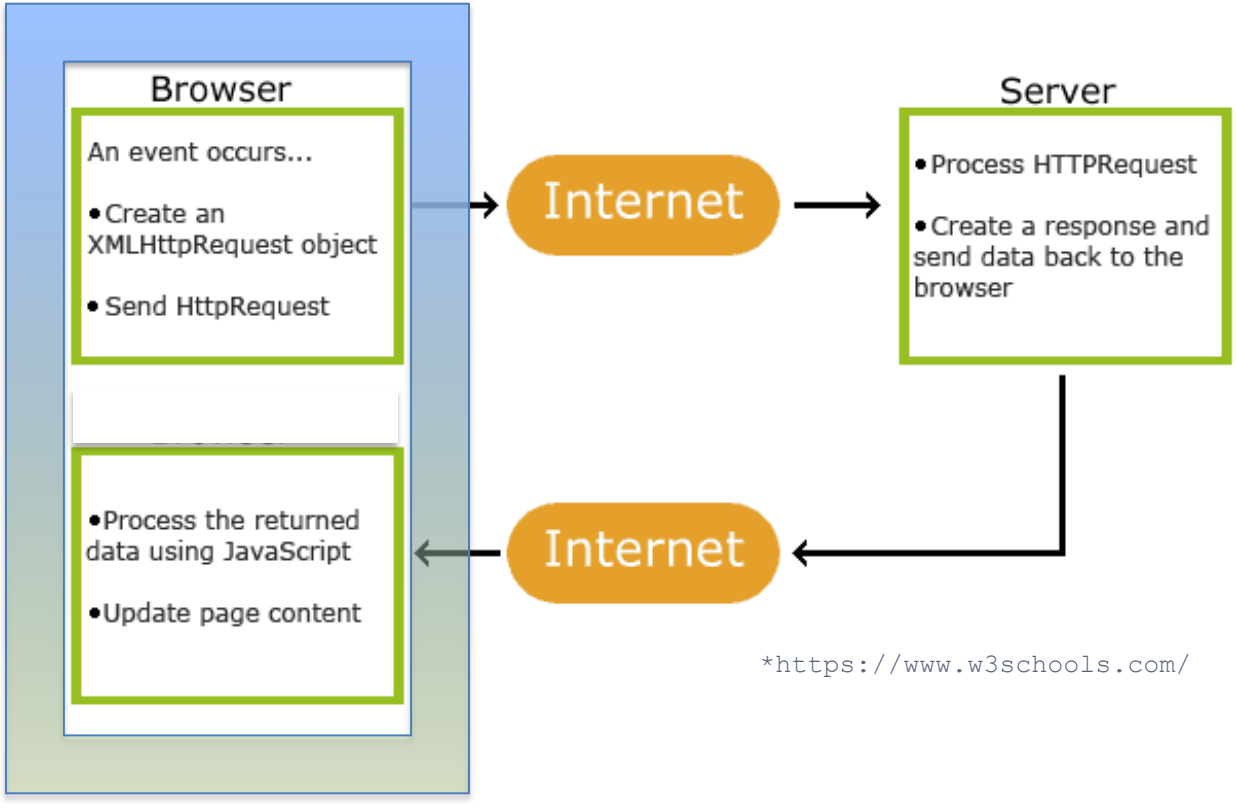
Option Profile: SmartScan

- Used for enhanced AJAX or Single Page Applications (SPA)
- Supports sites using AngularJS and bootstrap
- View QID 150148 “AJAX links crawled” to verify SmartScan is working



Qualys.

How AJAX Works



*https://www.w3schools.com/

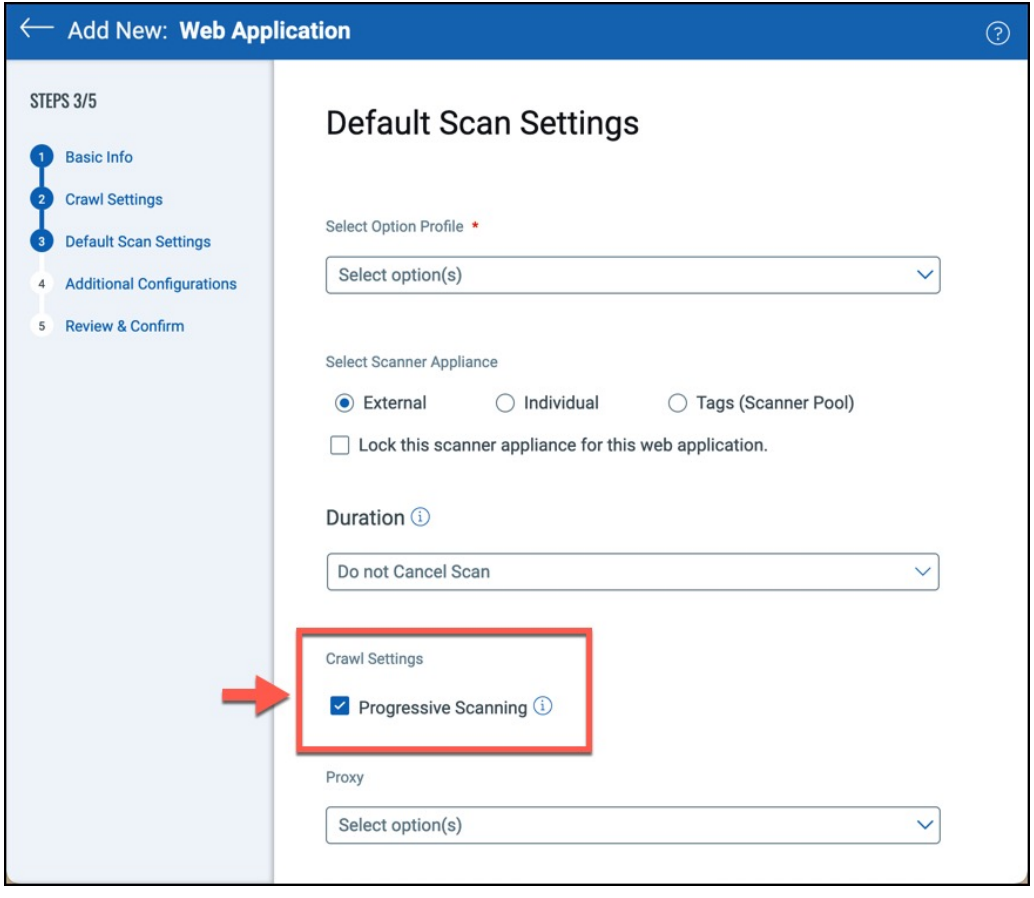
- Read data from a Web server - after the page has loaded
- Update a Web page without reloading the page
- Send data to a Web server - in the background

Qualys.

Progressive Scanning

Qualys.

Progressive Scanning



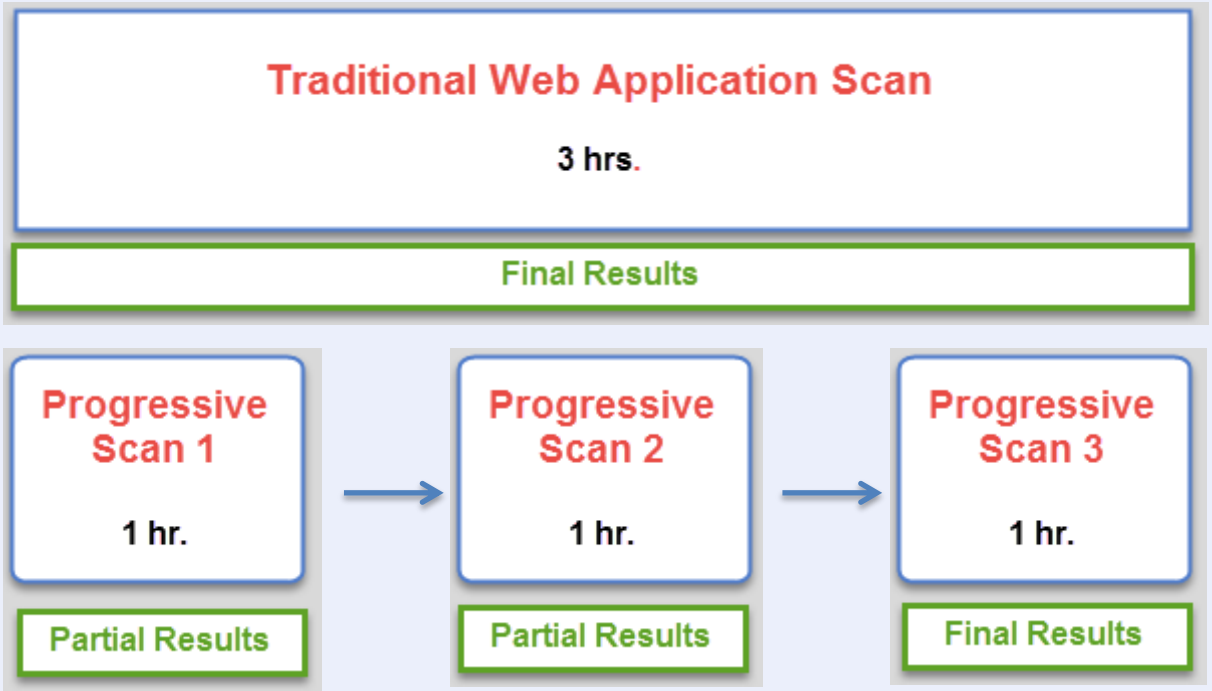
Qualys.

Progressive Scanning Behavior

- Remedies small or insufficient scanning windows, by expanding testing coverage, over time (scans are performed in multiple, progressive stages).
- Each successive scan builds upon the information obtained from the previous scan.
- Web app's history or findings are updated in stages, with each scan.
- Prioritizes pages not previously crawled and new functionality.

Qualys.

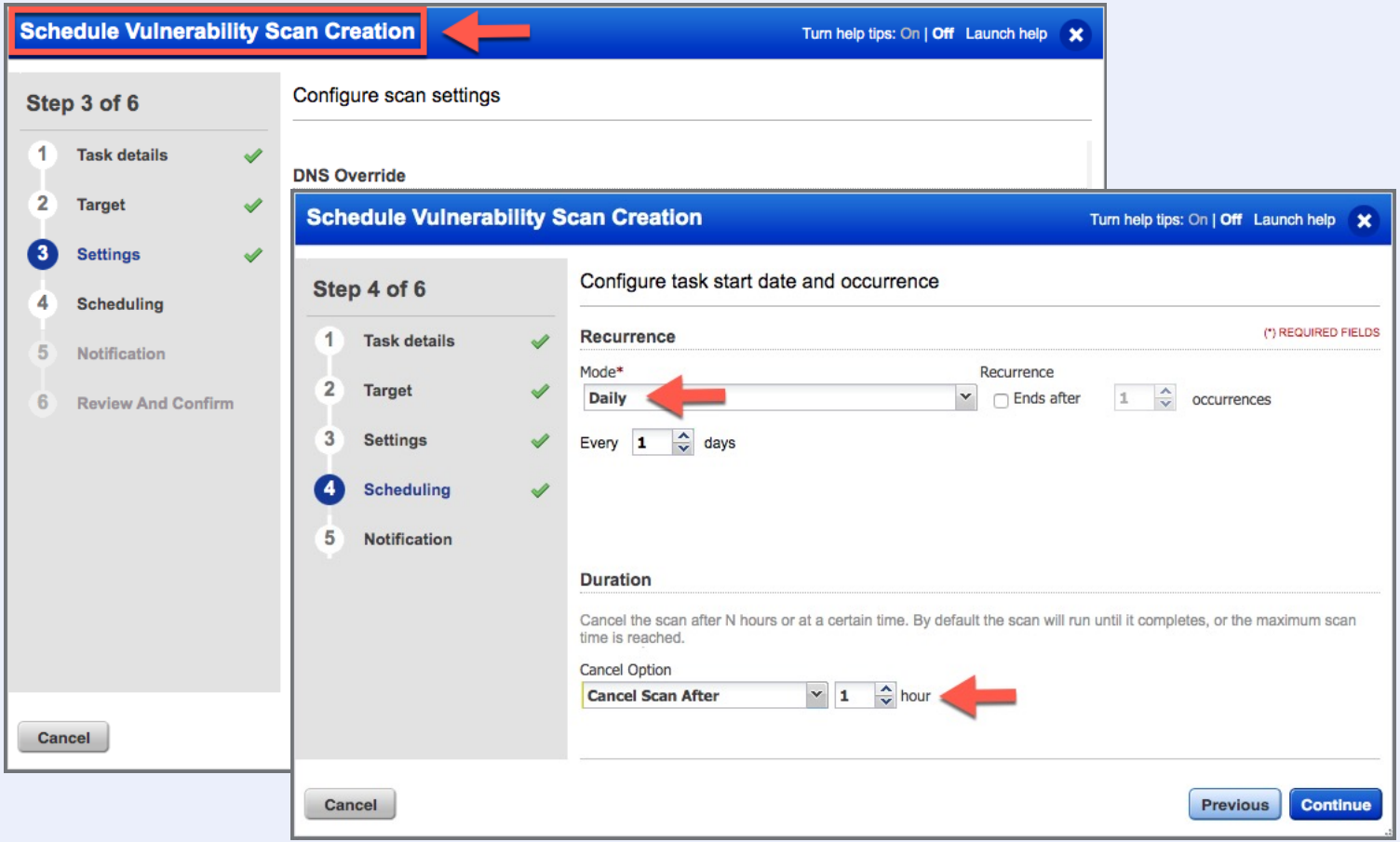
Progressive Scan Example



Works best with Frequently Scheduled Scans

Qualys.

Schedule a Progressive Scan



Qualys.

Agenda

Qualys Web Application Scanning

Session Two:

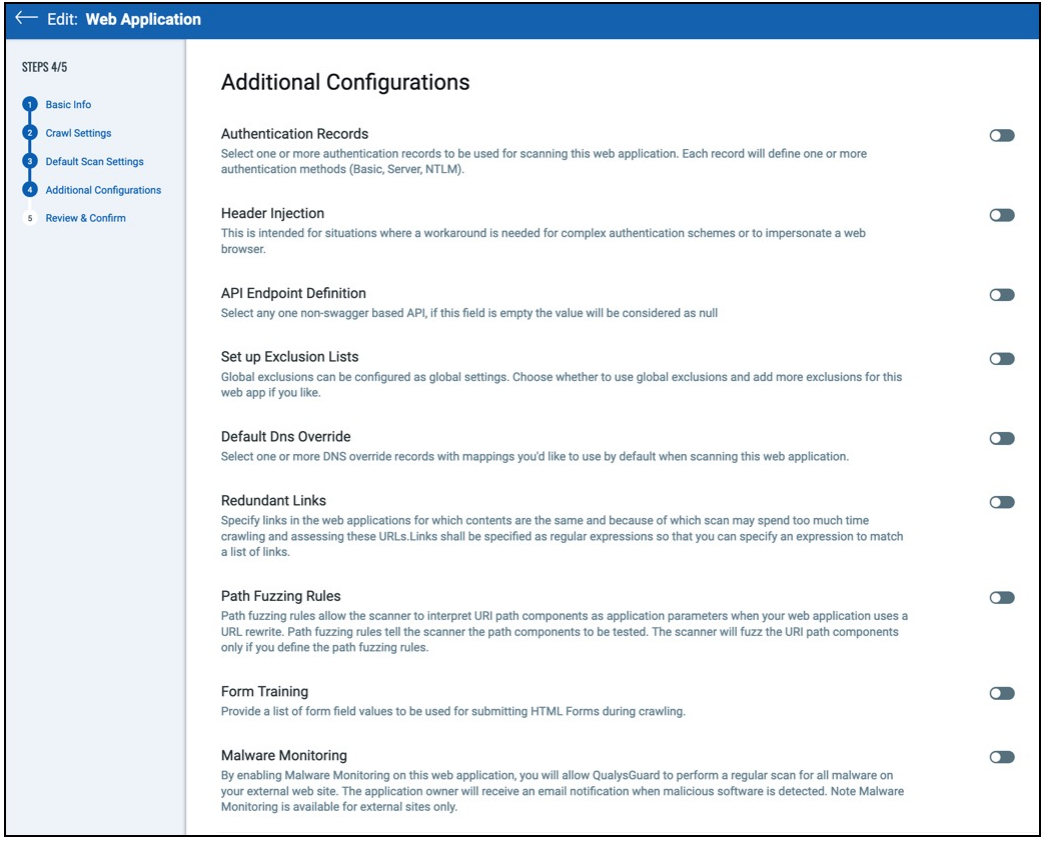
- Additional Configurations
- Web App Testing
- WAS Reporting
- Tags and Users
- WAS Integrations

Qualys.

Additional Configurations

Qualys.

Additional Configurations



- Authentication Records
- Header Injection
- API Endpoint Definition
- Set up Exclusion Lists
- Default DNS Override
- Redundant Links
- Path Fuzzing Rules
- Form Training
- Malware Monitoring

Authentication

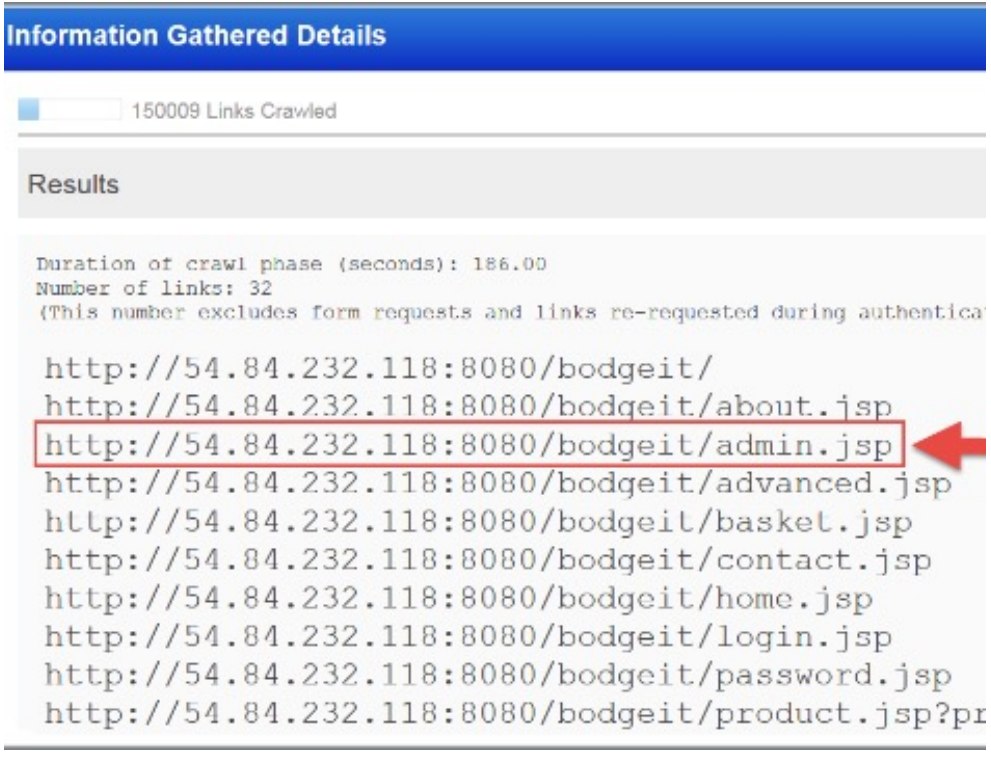
Best Practice: perform authenticated scans using non-privilege accounts.

Form Records

- Standard Login
- Custom
- Selenium Script - Qualys Browser Recorder

Server Records

- Basic
- Digest
- NTLM



Qualys.

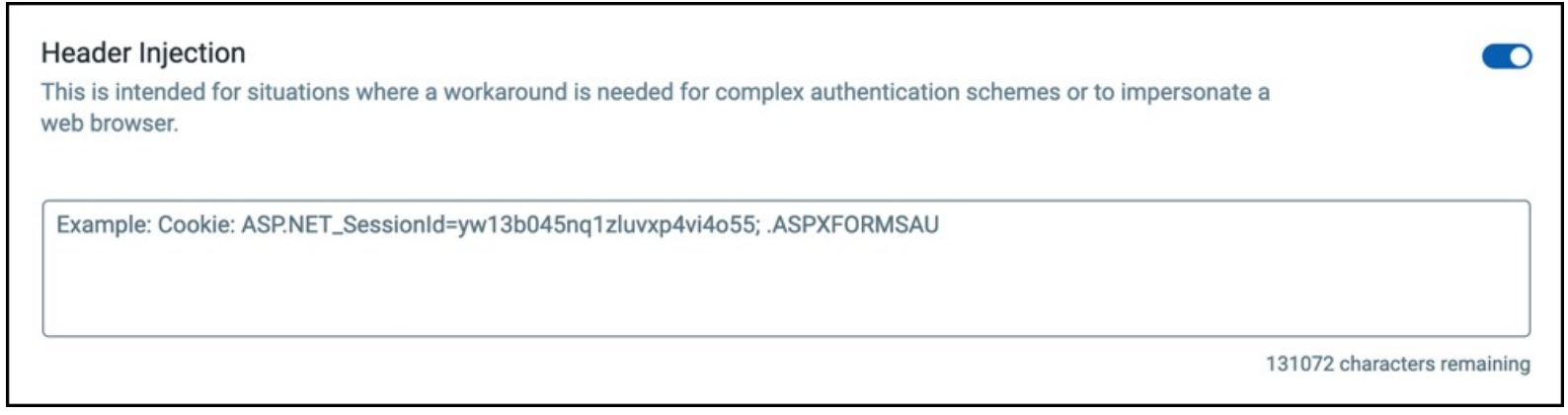
Lab Tutorials

Please follow **pages 18 – 19** from the Lab Tutorial Supplement

- Lab 9 – QBR Authentication Script, p. 19

Qualys.

Header Injection



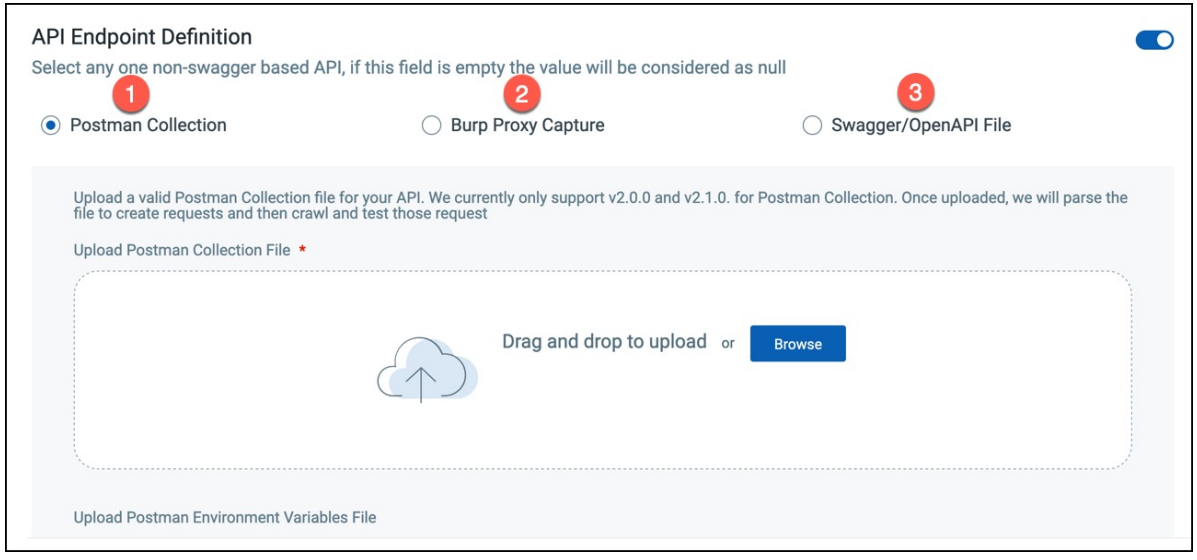
Header injection – HTTP headers injected by our scanning service to facilitate the web application scan. This option is commonly used to provide a workaround for complex authentication schemes.

Qualys.

API Endpoint Testing

Qualys.

API Testing

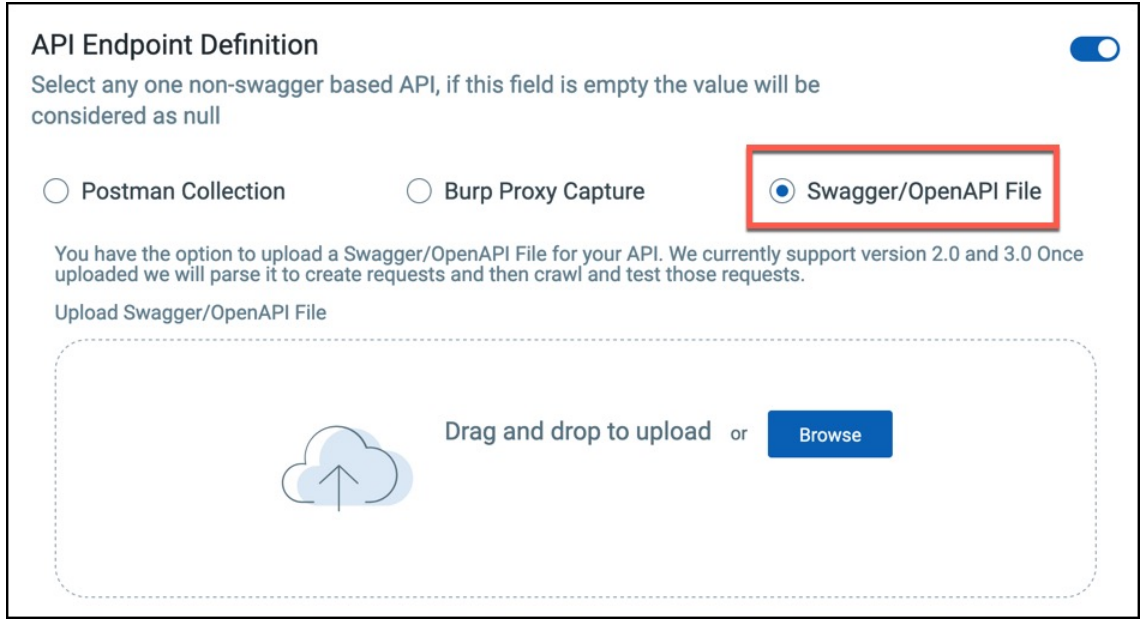


- APIs are vulnerable to many of the same attacks used against Web applications.
- You can specify API endpoints using:
  1. Swagger file
  2. Postman Collection
  3. Burp Proxy Capture

Qualys.

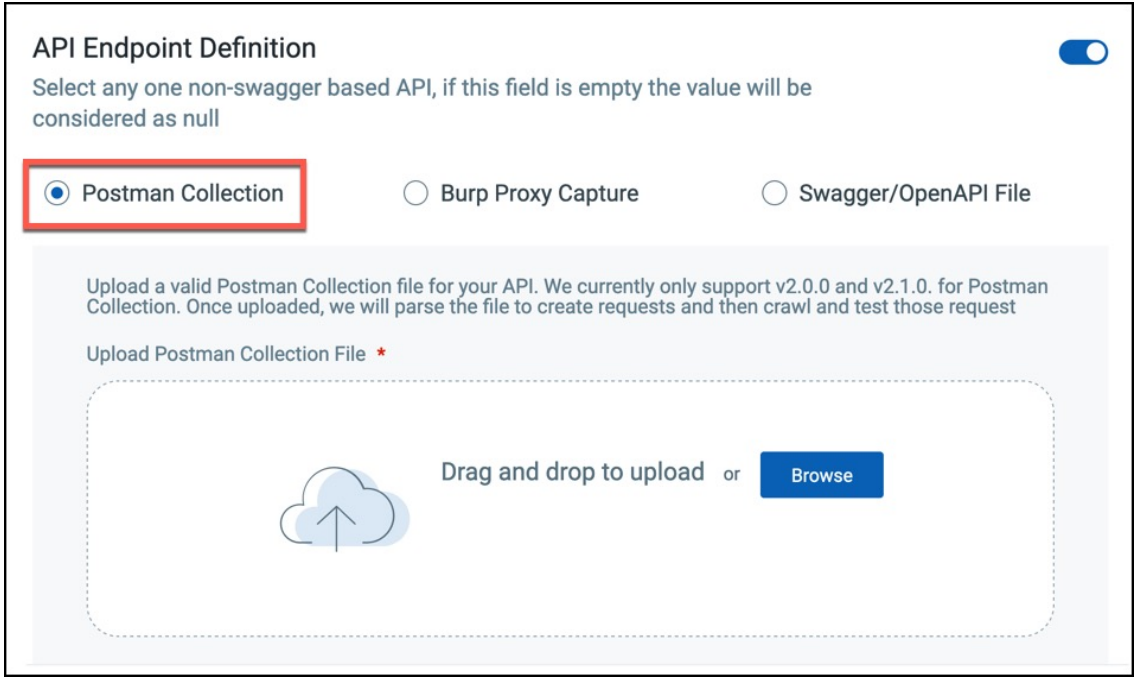
Swagger-Based REST APIs

- Qualys WAS can identify ”Swagger-based” REST API endpoints using a Swagger file.
- The Swagger file provides all the details about the APIs and how to invoke them. (Supported format: JSON)



Qualys.

API Endpoint Definition Using Postman



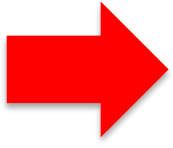
- If you are using Postman to create and document APIs, Postman collections can be uploaded to pass API endpoint definitions to the WAS scanning engine.

Qualys.

API Endpoint Definition Using Burp

- Qualys WAS can also discover REST API endpoints using a Burp proxy capture.
- Burp proxy can be configured to capture all requests to the REST API services.
- The captured request can be saved and exported in the form of XML file.

Burp Suite



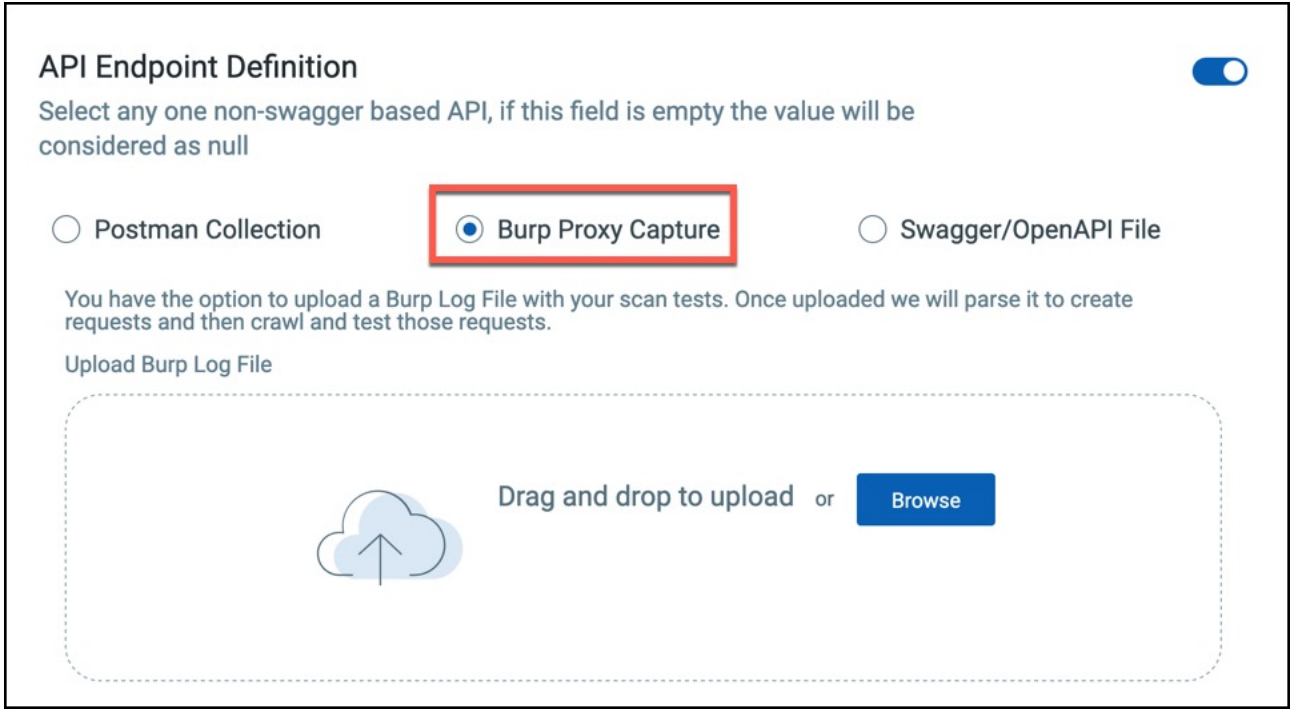
Web Application Scanning

- Documentation and resources
  - https://www.qualys.com/docs/qualys-was-crawling-rest-services.pdf

Qualys.

API Endpoint Definition Using Burp

- XML file will contain all the information about the endpoints which should be tested in Qualys WAS.



Qualys.

Explicit URLs for REST & SOAP

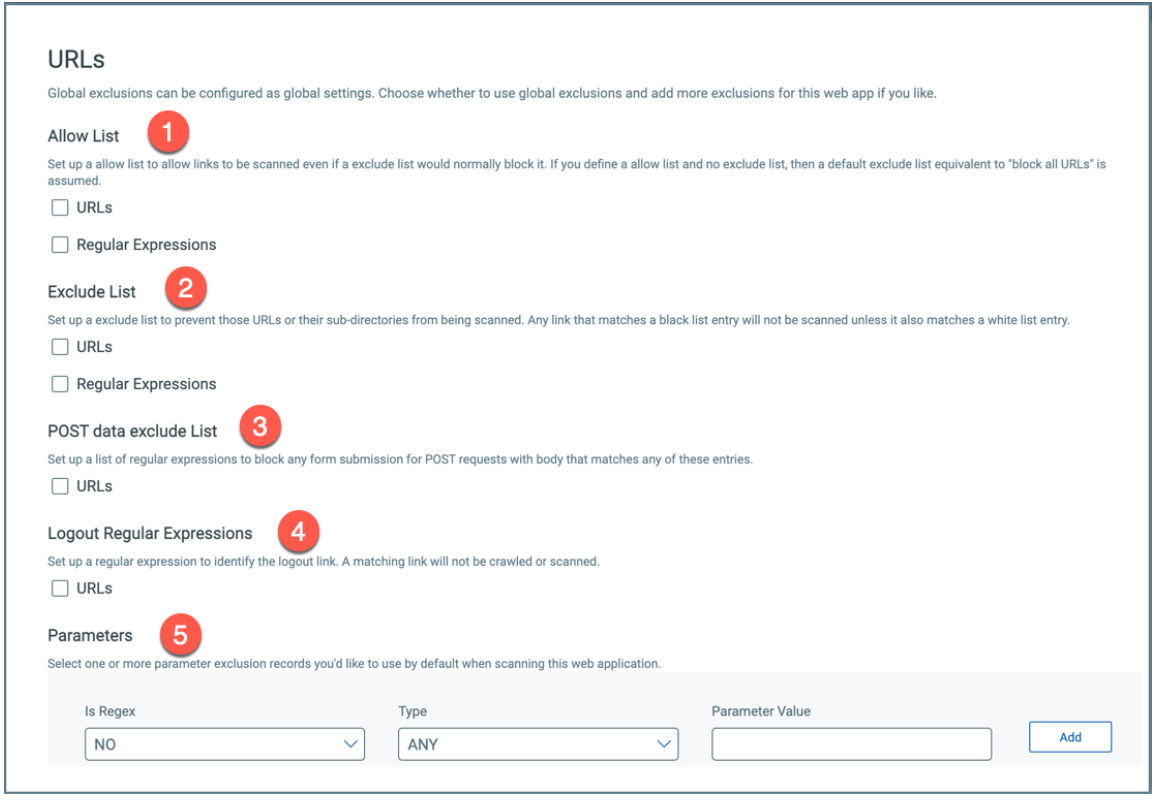
- You can manually add the REST Paths and Parameters, to the “Explicit URLs to Crawl” field.
- Qualys WAS also supports basic security testing of SOAP based web services that have a Web Service Description Language (WSDL) file added to the “Explicit URLs to Crawl” field.
- Both “REST Paths and Parameters” and “SOAP WSDL files” should fall within the crawl scope.

Qualys.

Setup Exclusion Lists

Qualys.

Setup Exclusion Lists

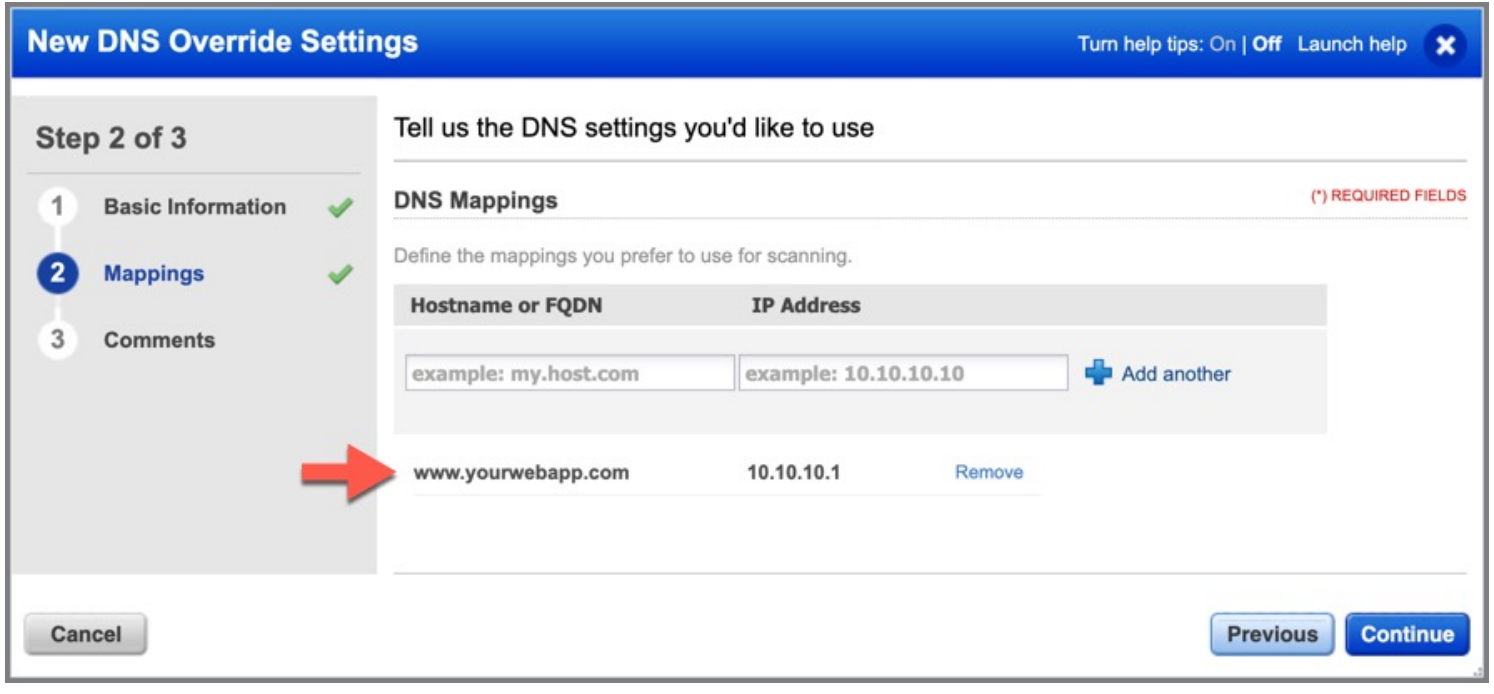


Qualys.

Default DNS Override

Qualys.

Default DNS Override



Quickly override the current DNS entry for any WAS Web app, without the hassle of modifying DNS records or HOSTS files.

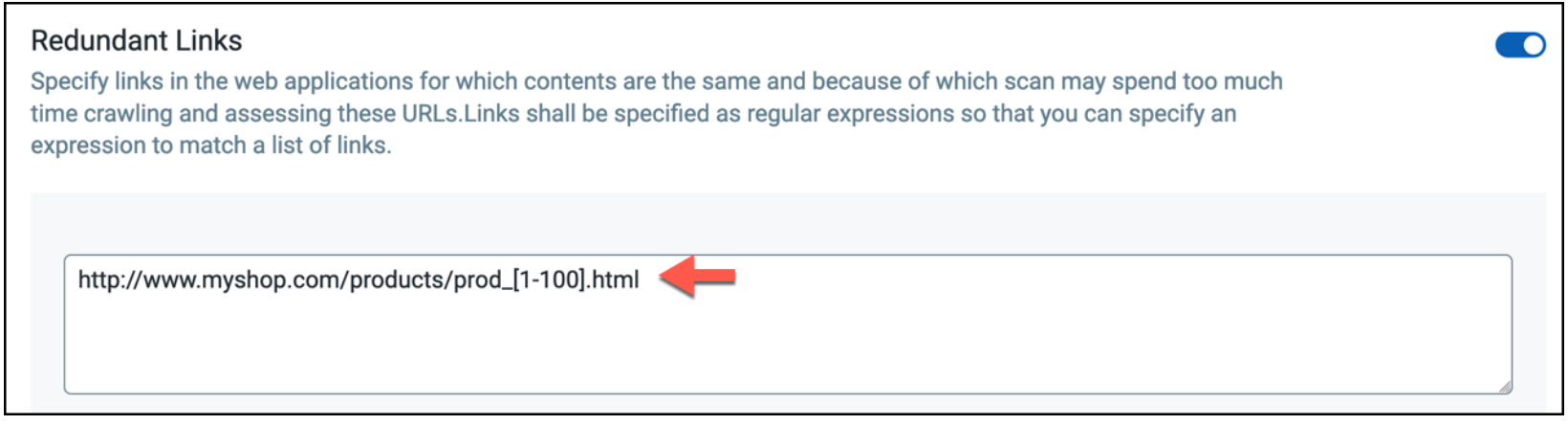
Qualys.

Redundant Links

Qualys.

Redundant Links

- What if different “dynamically” generated links all go the the same Web page?



- Specify redundant link patterns to avoid crawling and scanning the same pages (multiple times).

Qualys.

Path Fuzzing Rules

Qualys.

Path Fuzzing Rules

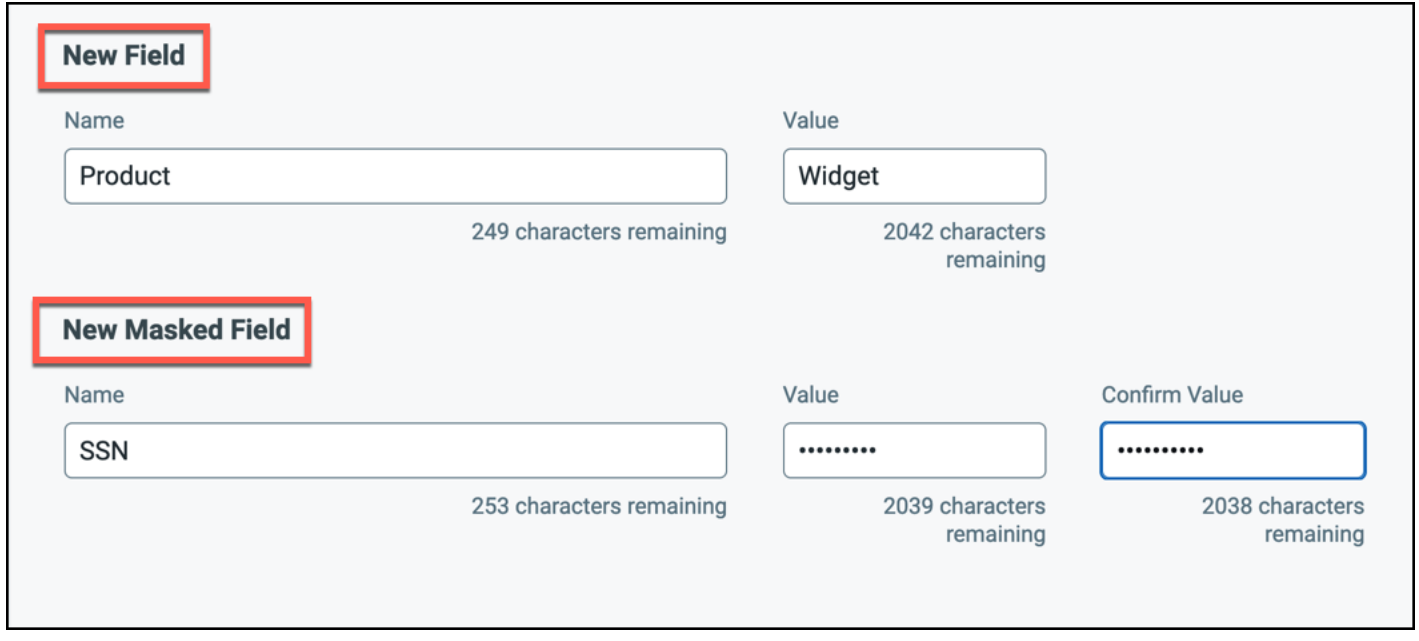
- For testing Web app technologies that support URL Rewriting, such as ASP and .Net MVC.
- Example: Let us consider news web site:
  - http://www.abc.com/issue/17/section/sports/article/28
  - http://www.abc.com/search.php?issue=17&section=sports&article=28
- The Path Fuzzing Rule is:
  - http://www.abc.com/issue/{issue}/section/{section}/article/{article}
  - Qualys Scanner Appliance will perform fault injection tests (SQLi, XSS, etc...) within the curly braces.

Form Training

Qualys.

Form Training

- Configure preset values for common form fields.
- Similar outcome as Qualys Browser Recorder or Initial Parameters.

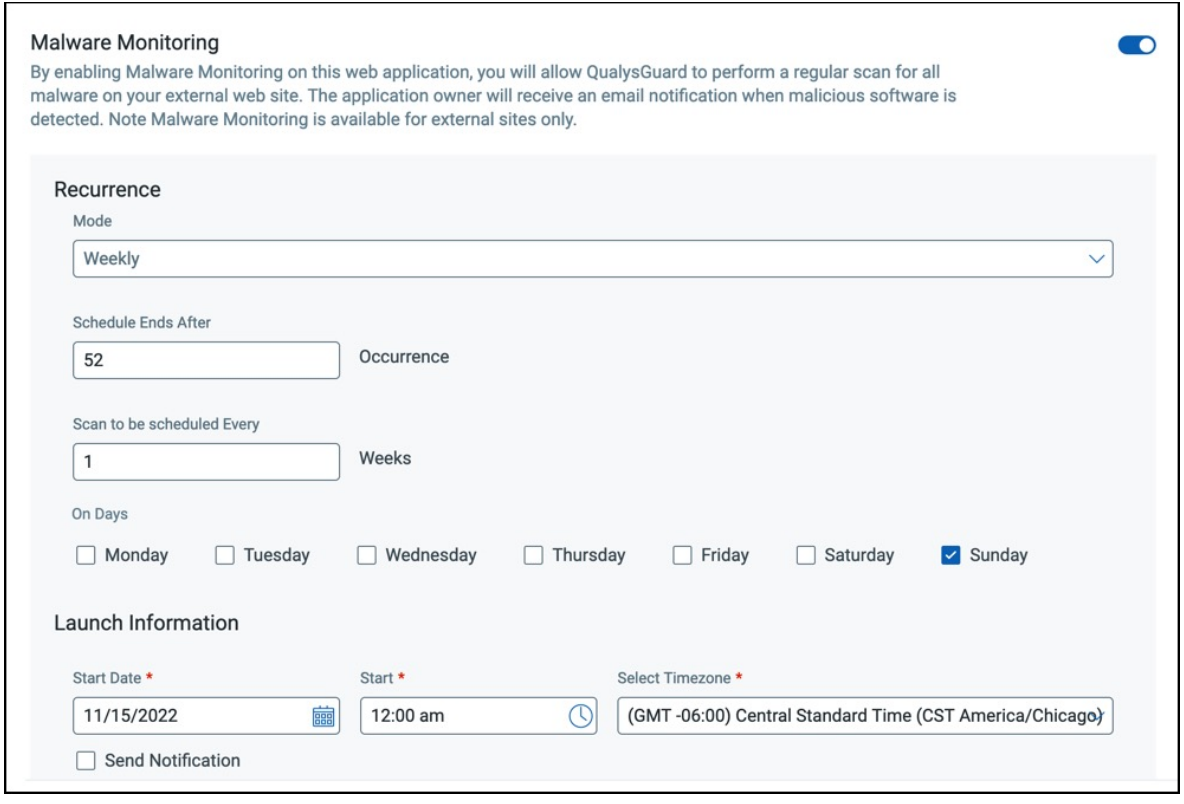


Qualys.

Malware Monitoring

Qualys.

Malware Monitoring



Enable Qualys Malware Scans for external facing Web apps.

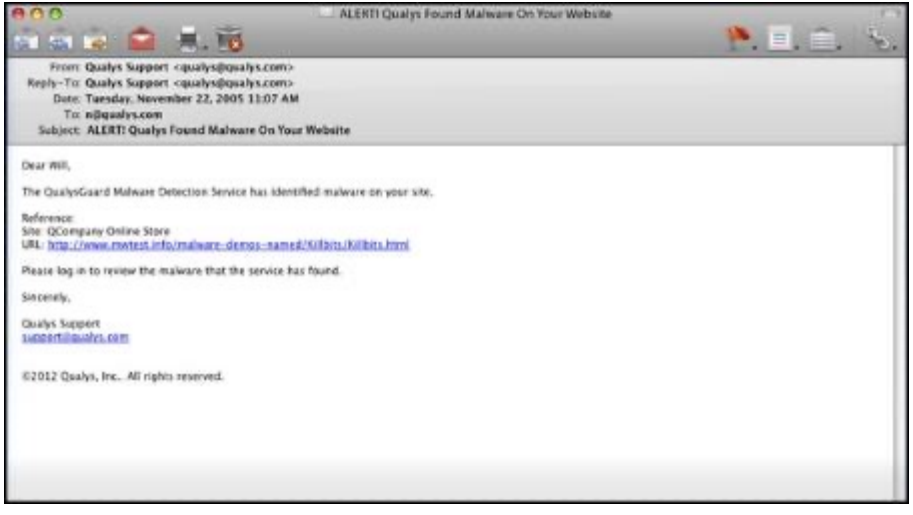
Qualys.

Malware Detection

Web Application URL

Qualys MDS Virtual Machine Farm

- ✓ MDS scans targeted Web app (staying within its defined scope).
- ✓ MDS provides both signature-based and behavioral analysis (i.e., “zero-day” detections) .
- ✓ Alerts are sent via email if/when Malware is found.



Qualys.

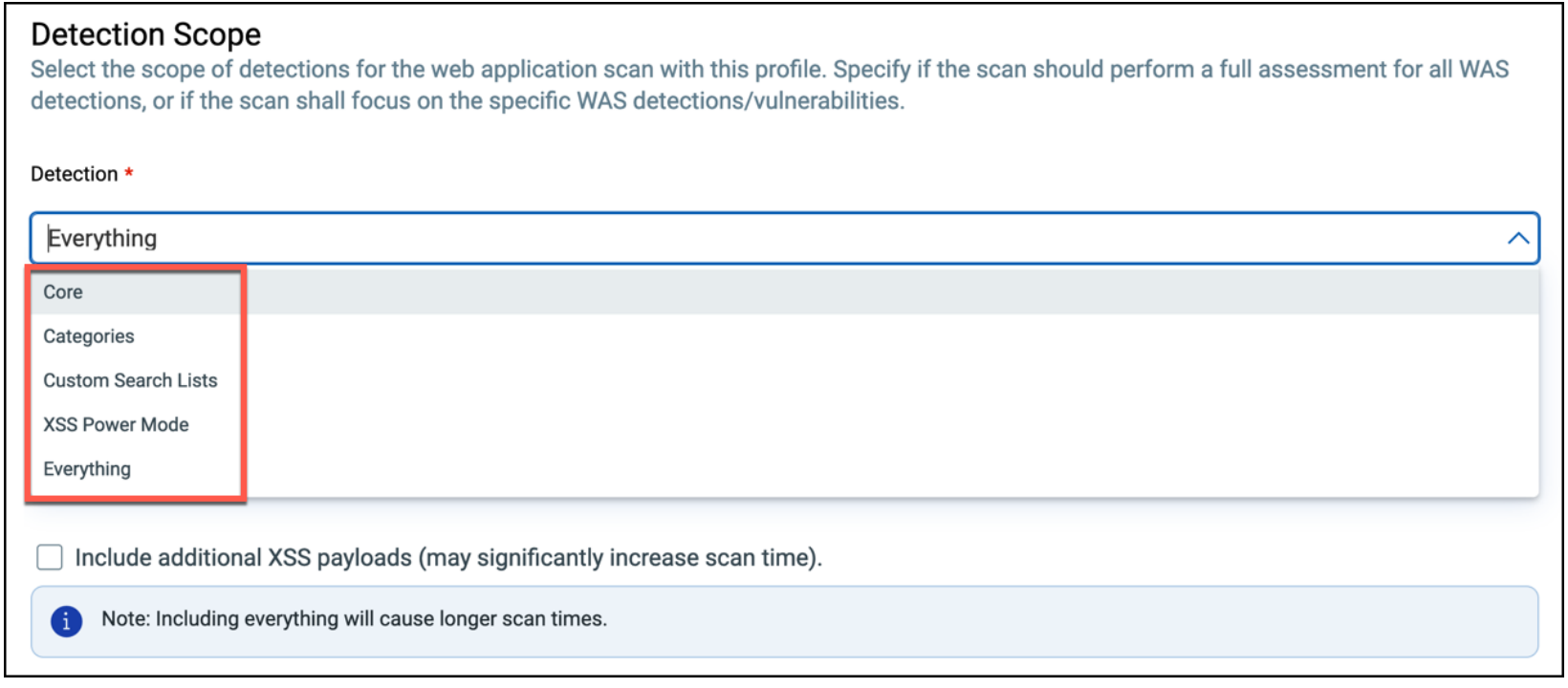
Web Application Testing

Qualys.

Qualys WAS Lifecycle

Qualys.

Detection Scope



Assessment test are performed according to the “Detection Scope” settings configured in the Web app’s Option Profile.

Qualys.

WASC

WASC www.webappsec.org divides Web vulnerabilities into six categories

Authentication

Authorization

Client-side Attacks

Command Execution

Information Disclosure

Logical Attacks

Attacks
Abuse of Functionality
Brute Force
Buffer Overflow
Content Spoofing
Credential/Session Prediction
Cross-Site Scripting
Cross-Site Request Forgery
Denial of Service
Fingerprinting
Format String
HTTP Response Smuggling
HTTP Response Splitting
HTTP Request Smuggling
HTTP Request Splitting
Integer Overflows
LDAP Injection
Mail Command Injection

Null Byte Injection
OS Commanding
Path Traversal
Predictable Resource Location
Remote File Inclusion (RFI)
Routing Detour
Session Fixation
SOAP Array Abuse
SSI Injection
SQL Injection
URL Redirector Abuse
XPath Injection
XML Attribute Blowup
XML External Entities
XML Entity Expansion
XML Injection
XQuery Injection

Qualys.

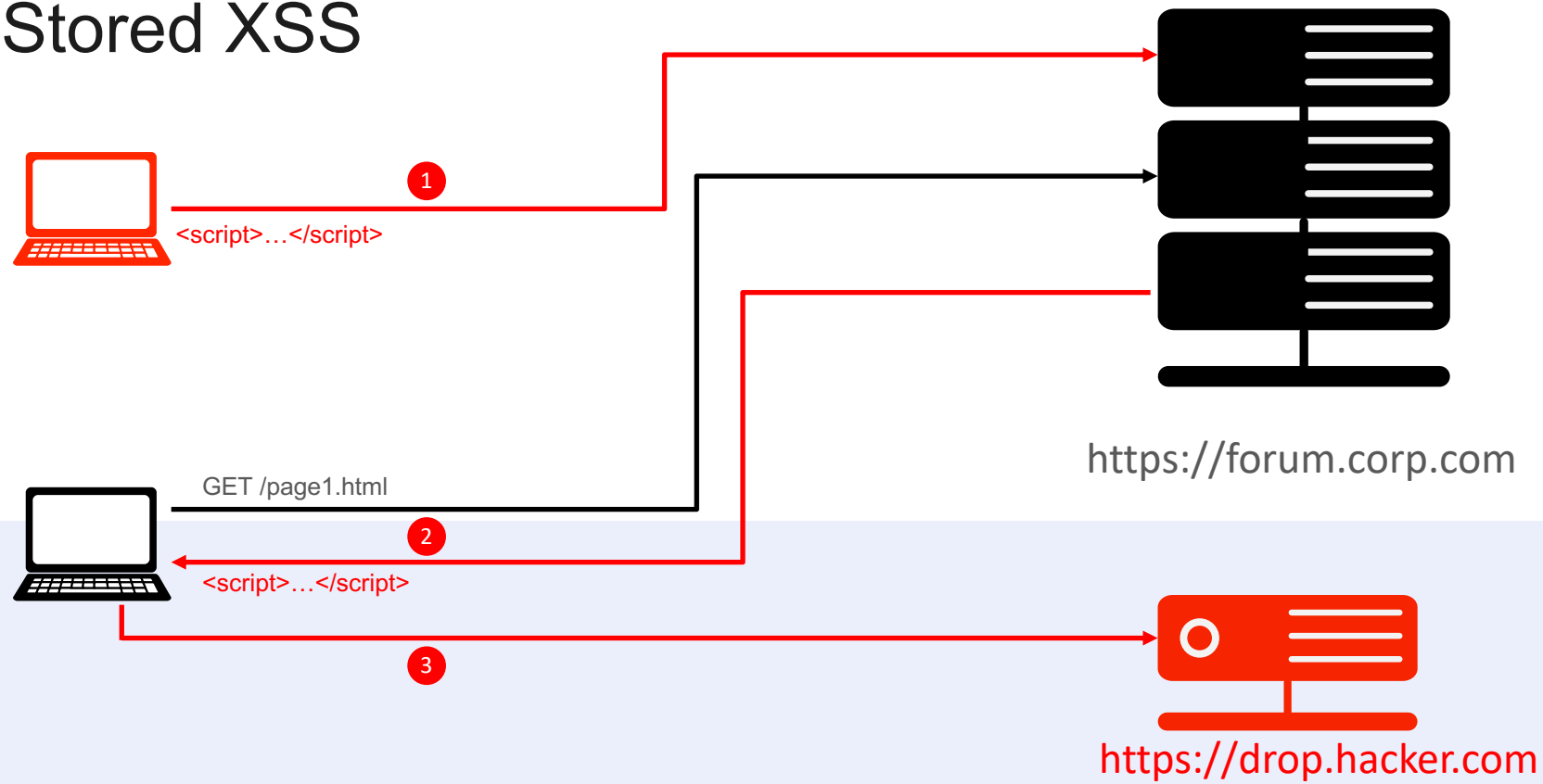
Rank	ID	Name	Score
[1]	CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	75.56
[2]	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	45.69
[3]	CWE-20	Improper Input Validation	43.61
[4]	CWE-200	Information Exposure	32.12
[5]	CWE-125	Out-of-bounds Read	26.53
[6]	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	24.54
[7]	CWE-416	Use After Free	17.94
[8]	CWE-190	Integer Overflow or Wraparound	17.35
[9]	CWE-352	Cross-Site Request Forgery (CSRF)	15.54
[10]	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14.10
[11]	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11.47
[12]	CWE-787	Out-of-bounds Write	11.08
[13]	CWE-287	Improper Authentication	10.78
[14]	CWE-476	NULL Pointer Dereference	9.74
[15]	CWE-732	Incorrect Permission Assignment for Critical Resource	6.33
[16]	CWE-434	Unrestricted Upload of File with Dangerous Type	5.50
[17]	CWE-611	Improper Restriction of XML External Entity Reference	5.48
[18]	CWE-94	Improper Control of Generation of Code ('Code Injection')	5.36
[19]	CWE-798	Use of Hard-coded Credentials	5.12
[20]	CWE-400	Uncontrolled Resource Consumption	5.04
[21]	CWE-772	Missing Release of Resource after Effective Lifetime	5.04
[22]	CWE-426	Untrusted Search Path	4.40
[23]	CWE-502	Deserialization of Untrusted Data	4.30
[24]	CWE-269	Improper Privilege Management	4.23
[25]	CWE-295	Improper Certificate Validation	4.06

Qualys.

OWASP

Qualys.

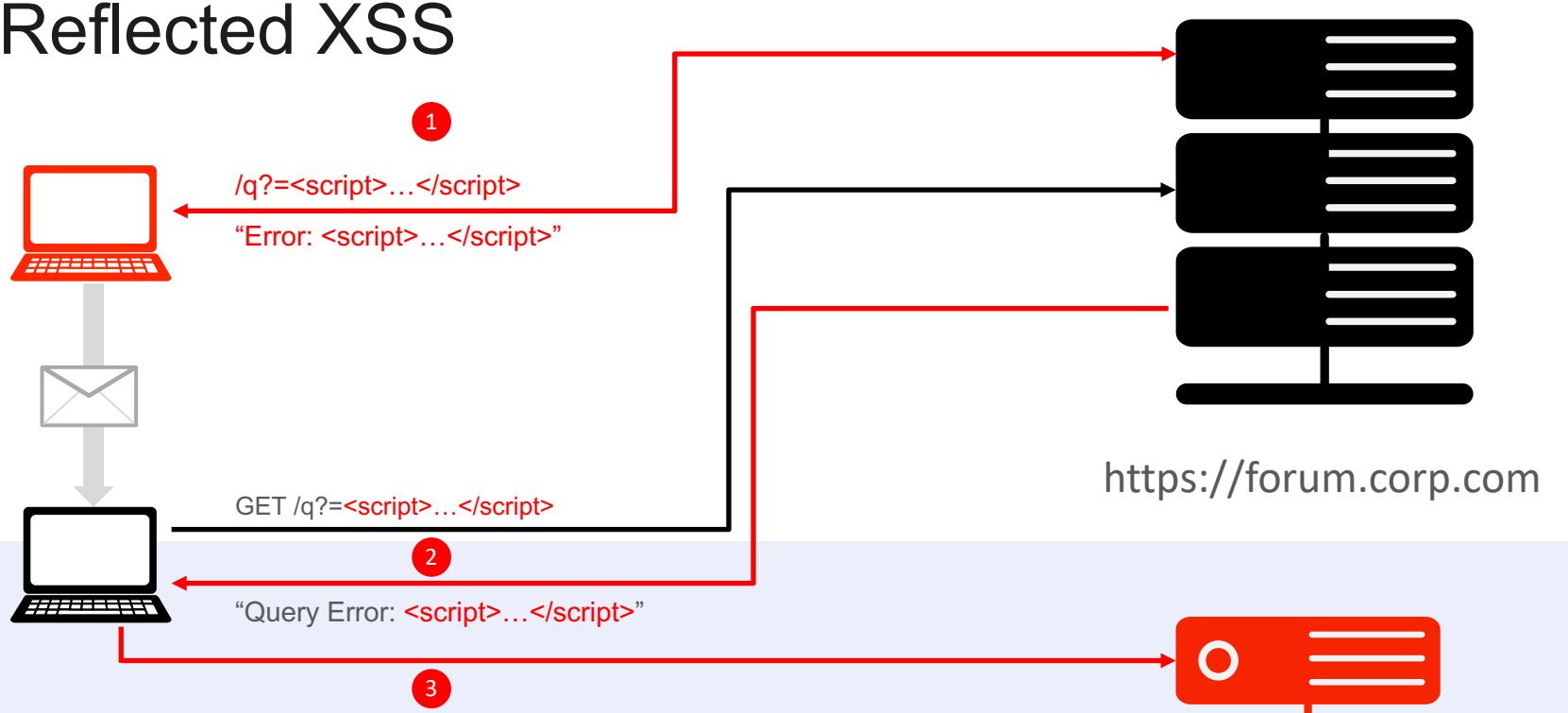
Stored XSS



1. Hacker uploads malicious script into Web app's repository or database
2. User requests page, stored hacker script sent
3. Client executes code

Qualys.

Reflected XSS



1. Hacker find vulnerable parameter.
2. User requests page, hacker code reflected back.
3. Client executes code.

Qualys.

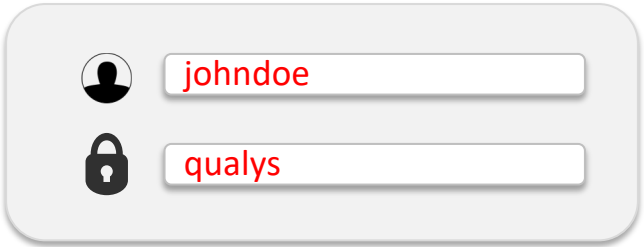
BodgeIT XSS Vulnerability

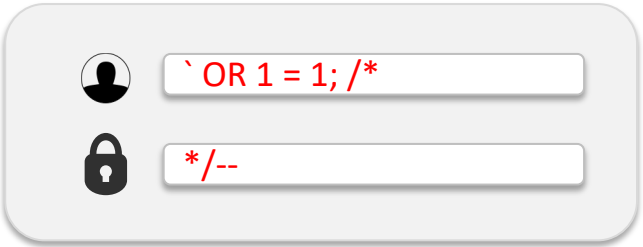
`http://54.173.177.208:8080/bodgeit/search.jsp`

- BodgeIT Store “Search” field does not sanitize input.
- Injected scripts are rendered or reflected within the client browser.

Qualys.

SQL injection





select * from users where username='johndoe' and password = 'qualys'

select * from users where username='` OR 1 = 1; /* 'and password = ' */--'

Qualys.

Blind SQLi

True

False

GET /article.php?id=1 and 1 = 1

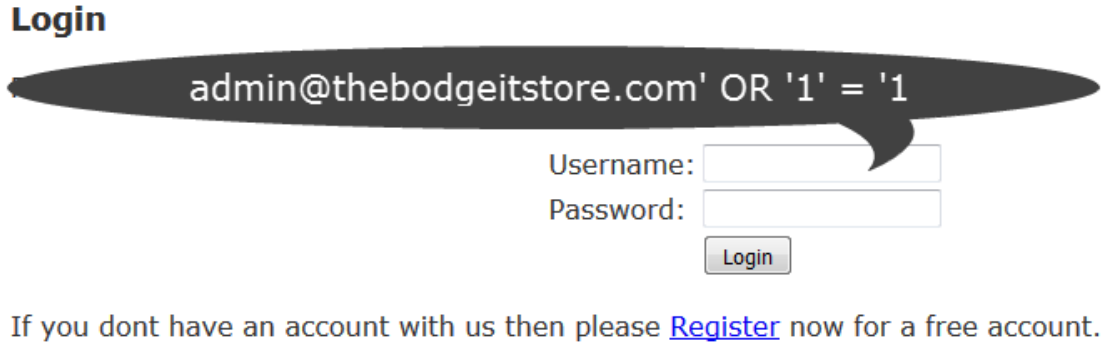
GET /article.php?id=1 and 1 = 2

- By asking the server true and false questions and getting different results we are able to determine if vulnerability.

Qualys.

BodgeIT SQLi Vulnerability

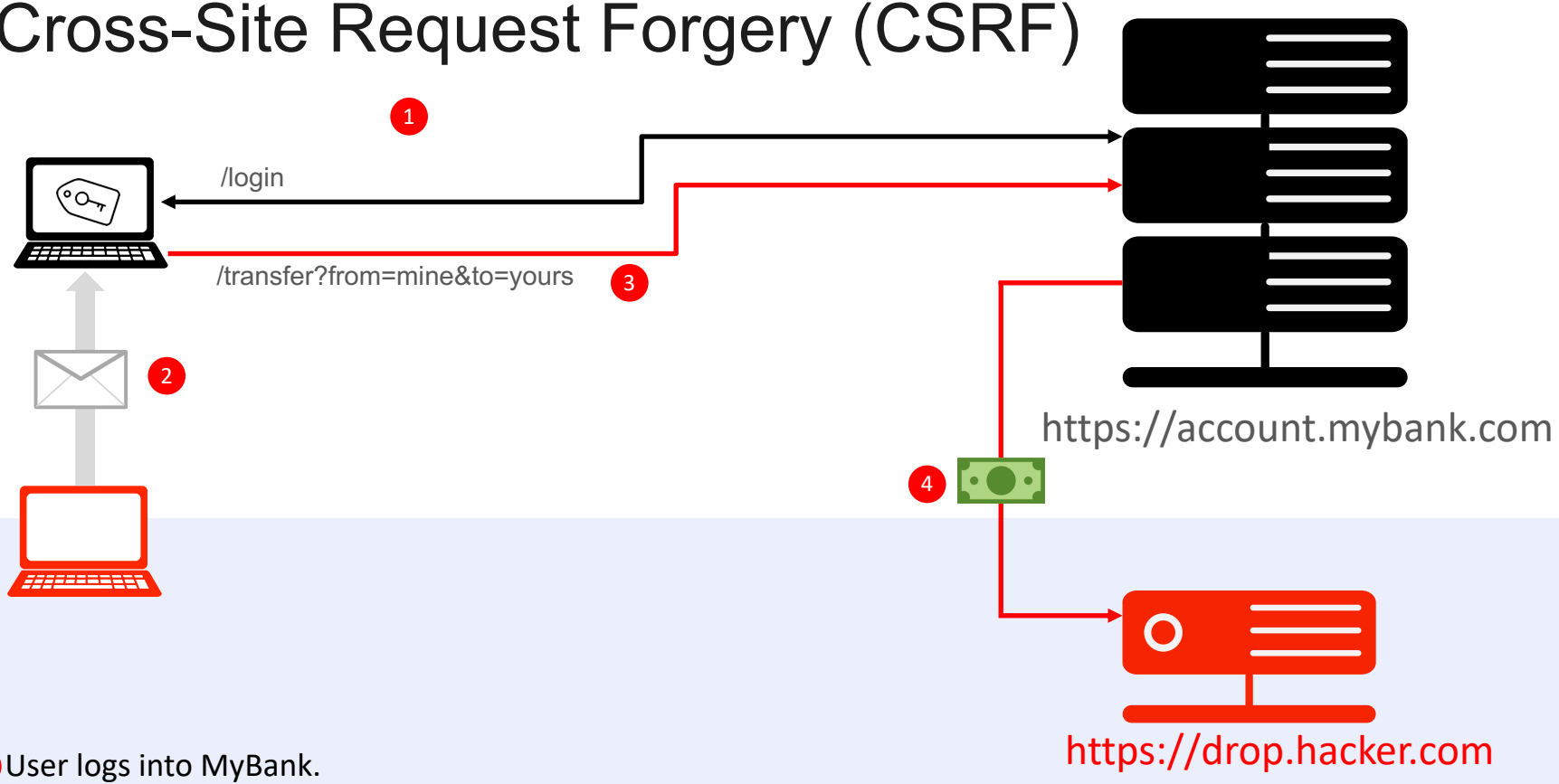
`http://54.173.177.208:8080/bodgeit/login.jsp`



The BodgeIT Store ”Login” page uses string concatenation to build a SQL request, making it easy to inject a malicious SQL command into the “Username” field.

Qualys.

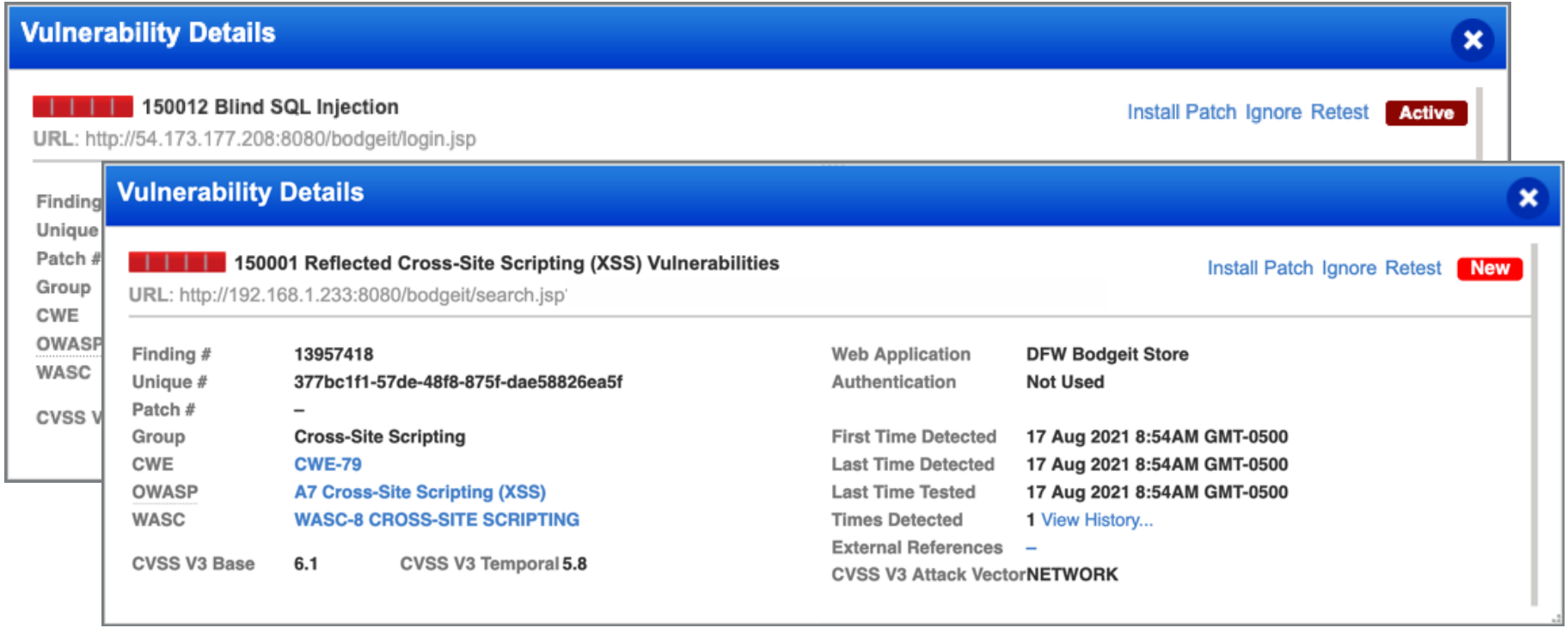
Cross-Site Request Forgery (CSRF)



1. User logs into MyBank.
2. User is sent a phishing email with false link.
3. Clinking on the link a request is sent to the banks website using the users authentication token.
4. User money is transferred to the hackers account.

Qualys.

Web App Report Details



When viewing Web App reports, click the “CWE,” “OWASP,” or “WASC” links for more details.

Qualys.

Session Break

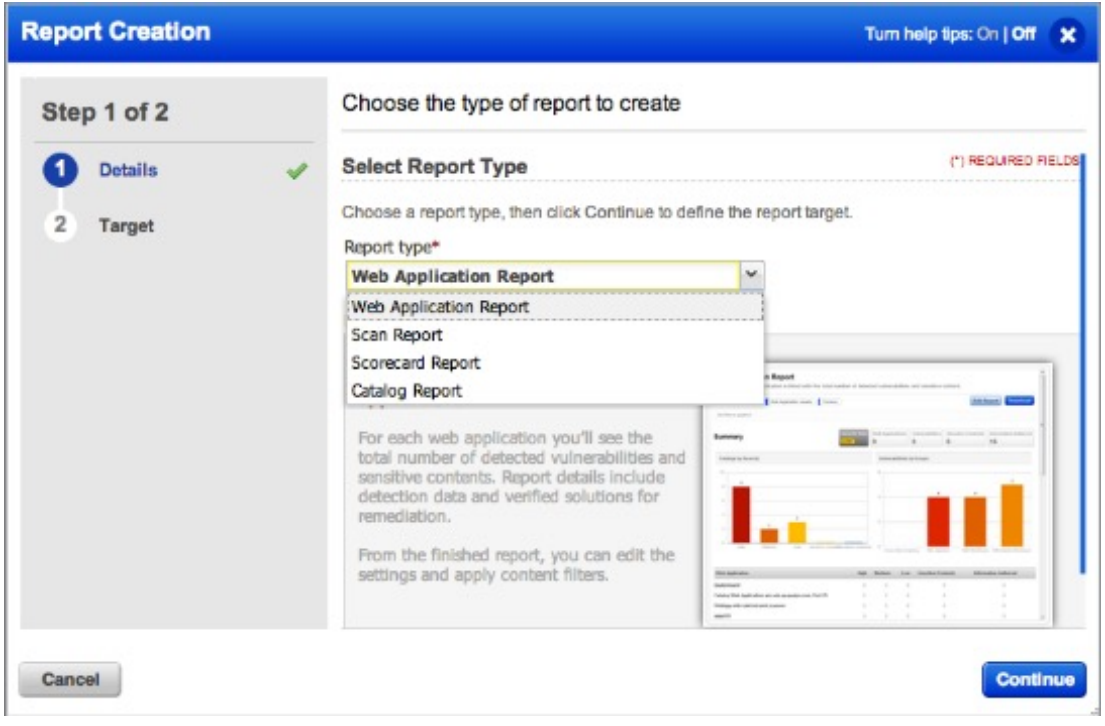
Qualys.

Reporting

Qualys.

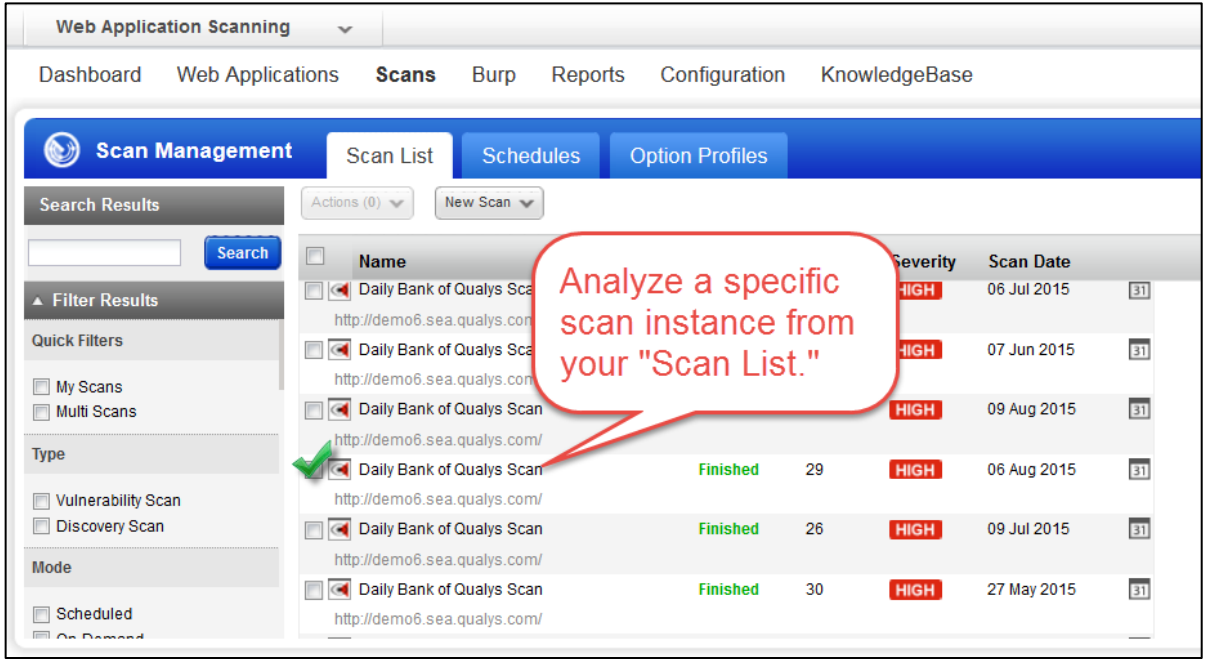
WAS Reporting

- Scan Report
- Web Application Report
- Scorecard Report
- Catalog Report



Qualys.

Scan Report



Focus on single scan instance (date + time), therefore NO vulnerability history data.

Qualys.

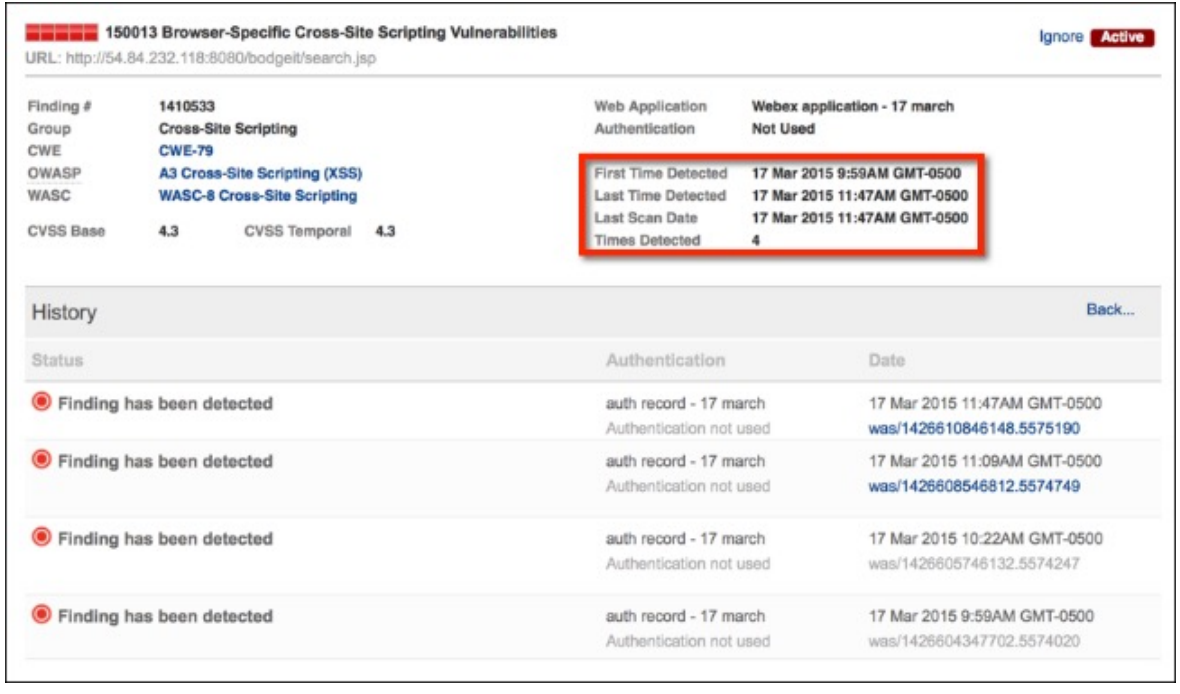
Lab Tutorials

Please follow **pages 20 – 21** in the Lab Tutorial Supplement

- Lab 10 – Scan Report, p. 20

Qualys.

Web Application Report



- Combines all scans performed on a single Web application.
- Vulnerability History and Status included (New, Active, Re-opened, Fixed).

Qualys.

Lab Tutorials

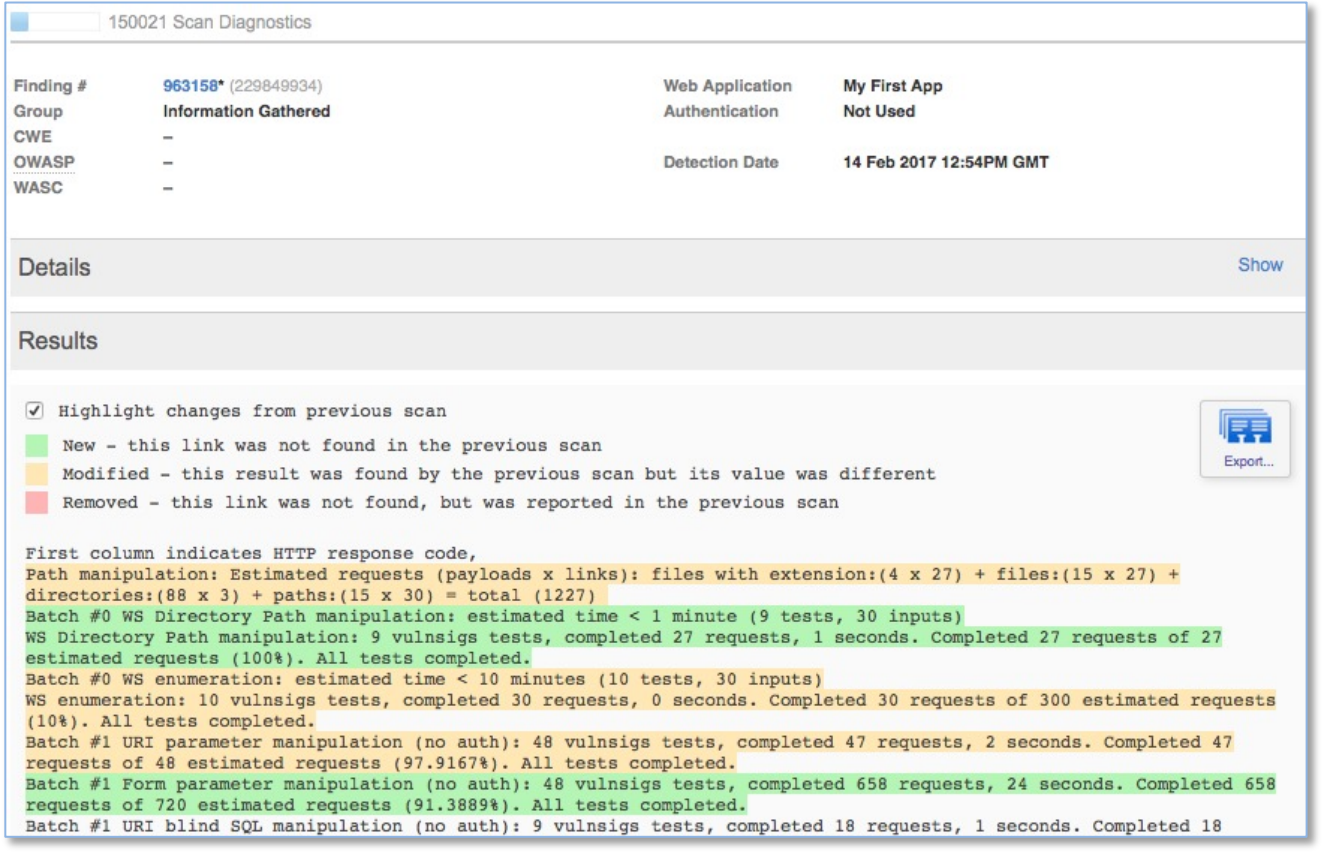
Please follow **pages 20 - 21** in the Lab Tutorial Supplement

- Lab 11 – Web App Report, p. 21

Qualys.

QID 150021 – Scan Diagnostics

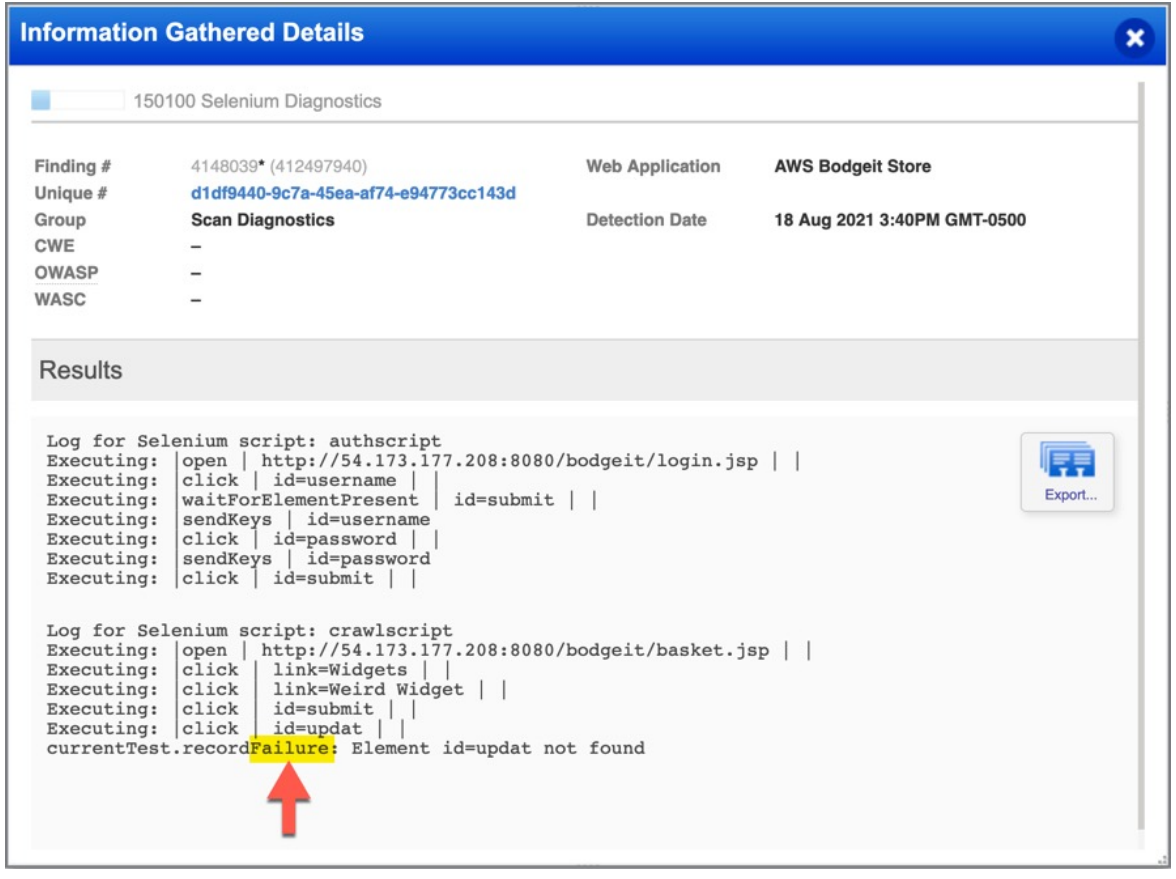
The scan diagnostics data provides technical details about the scanner appliance performance and behavior.



Qualys.

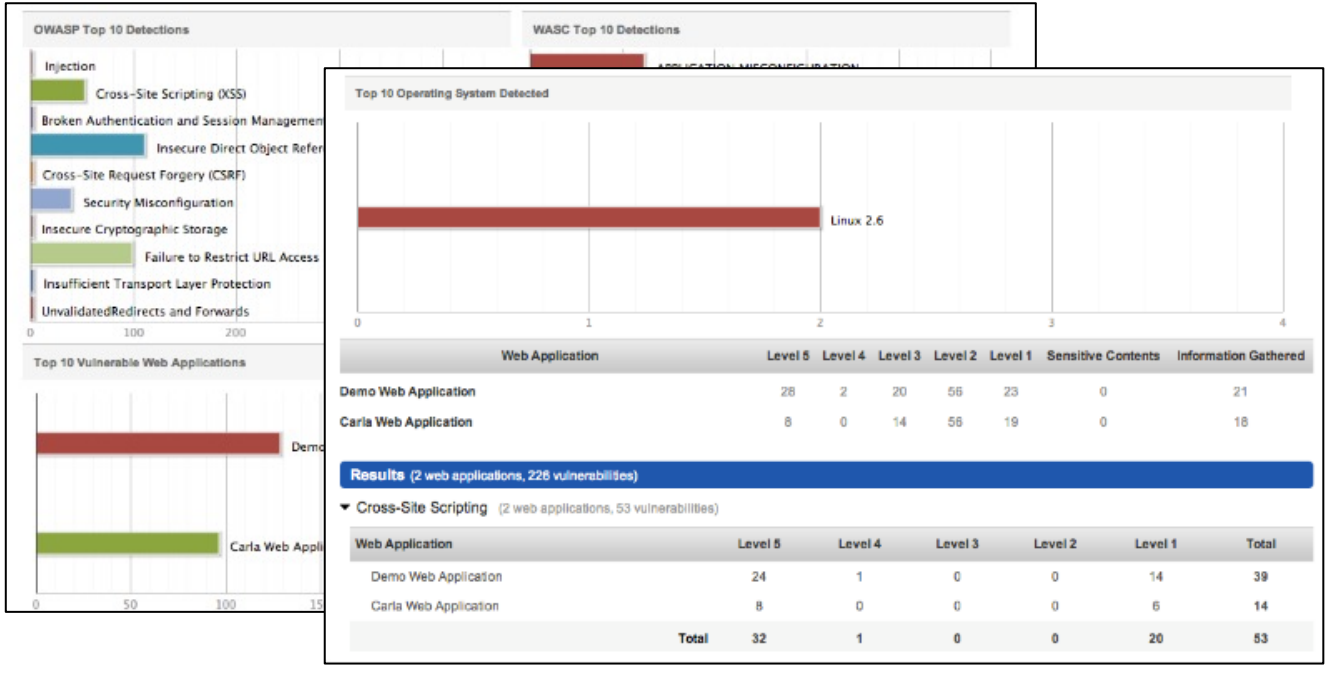
QID 150100 – Selenium Diagnostics

- Troubleshoot Selenium script
- Search for keyword: “Failure”



Qualys.

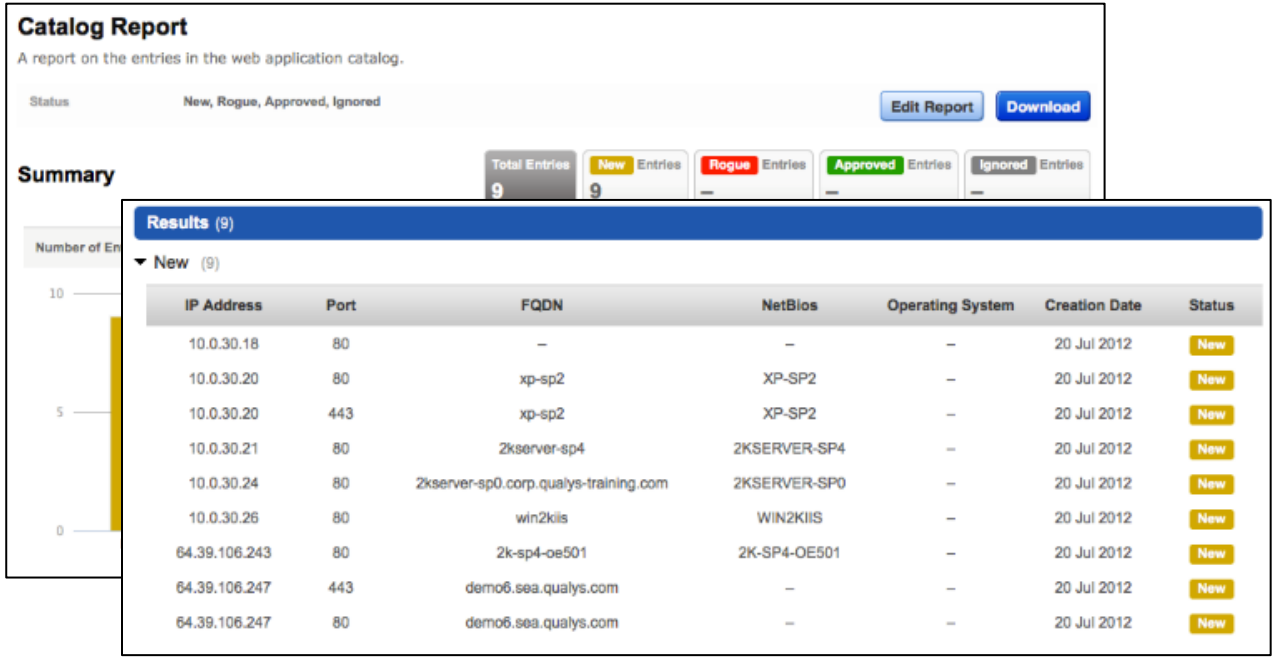
WAS Scorecard Report



Easily Analyze the status of multiple Web application projects.

Qualys.

WAS Catalog



Manage and track Web applications throughout your entire enterprise architecture.

Qualys.

Tags and Users

Qualys.

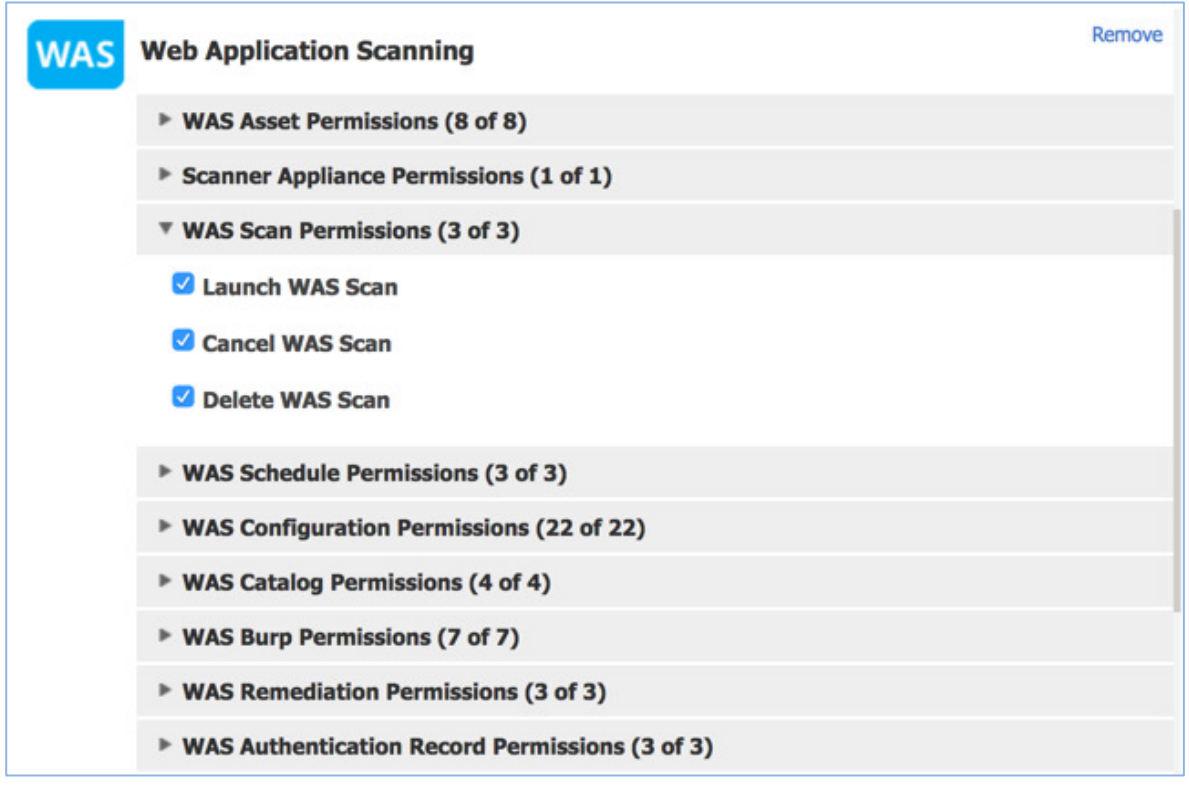
Asset Tags

Asset Tags can be added or removed from most WAS objects:

- Users
- Web Applications
- Templates
- Option Profiles
- Brute Force Lists
- Search Lists
- Scanners
- Parameter Sets
- Authentication Records
- and more...

Qualys.

User Roles



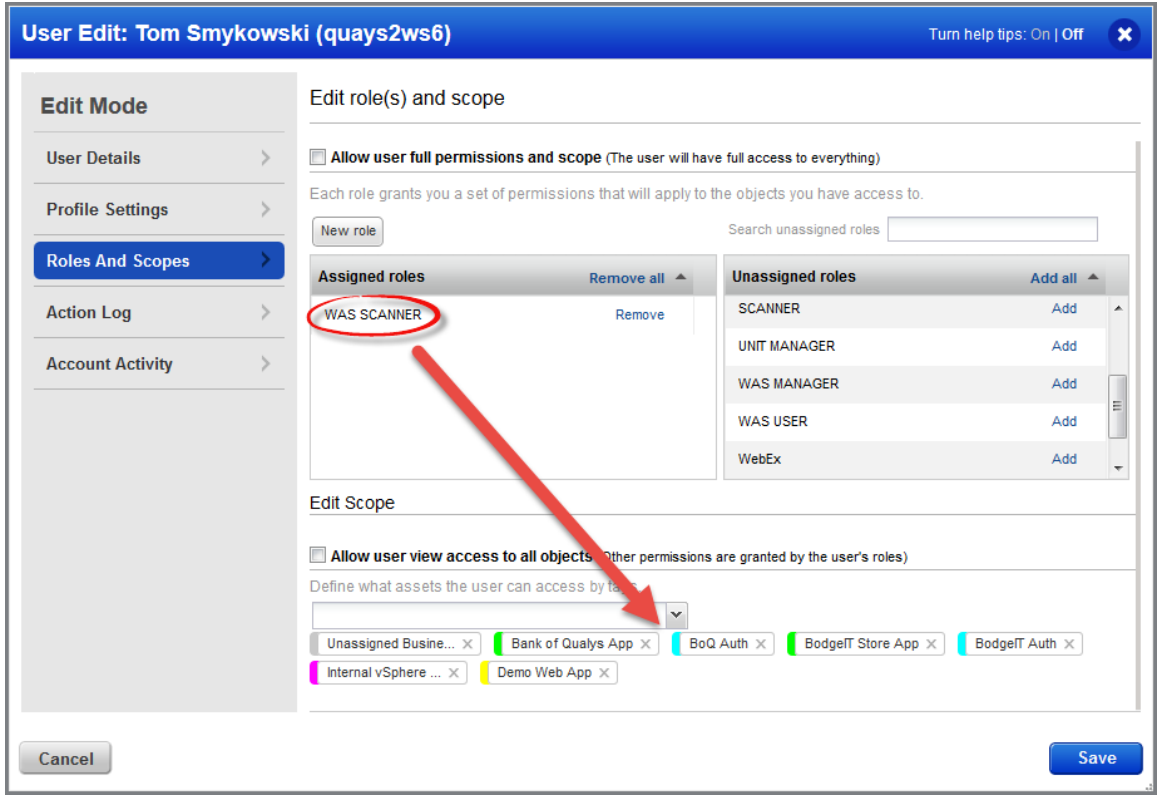
Set granular permissions to build custom roles.

Qualys.

Combine Roles & Tags

Administration
Control user access permissions and activity in your subscription.

- Combine user roles with Asset Tags to provide access privileges.
- Ensure that user role privileges meet or exceed those required for all tags in the user's scope.



Qualys.

Lab Tutorials

Please follow **pages 22 – 25** in the Lab Tutorial Supplement

- Lab 12 – Tagging, p. 22
- Lab 13 – User Management, p. 24

Qualys.

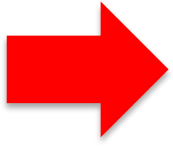
WAS Integrations

Qualys.

Burp Suite Professional

- Import Burp findings into Qualys WAS.
- View detections lists.
- Create Web Application reports to display both Burp and WAS findings.

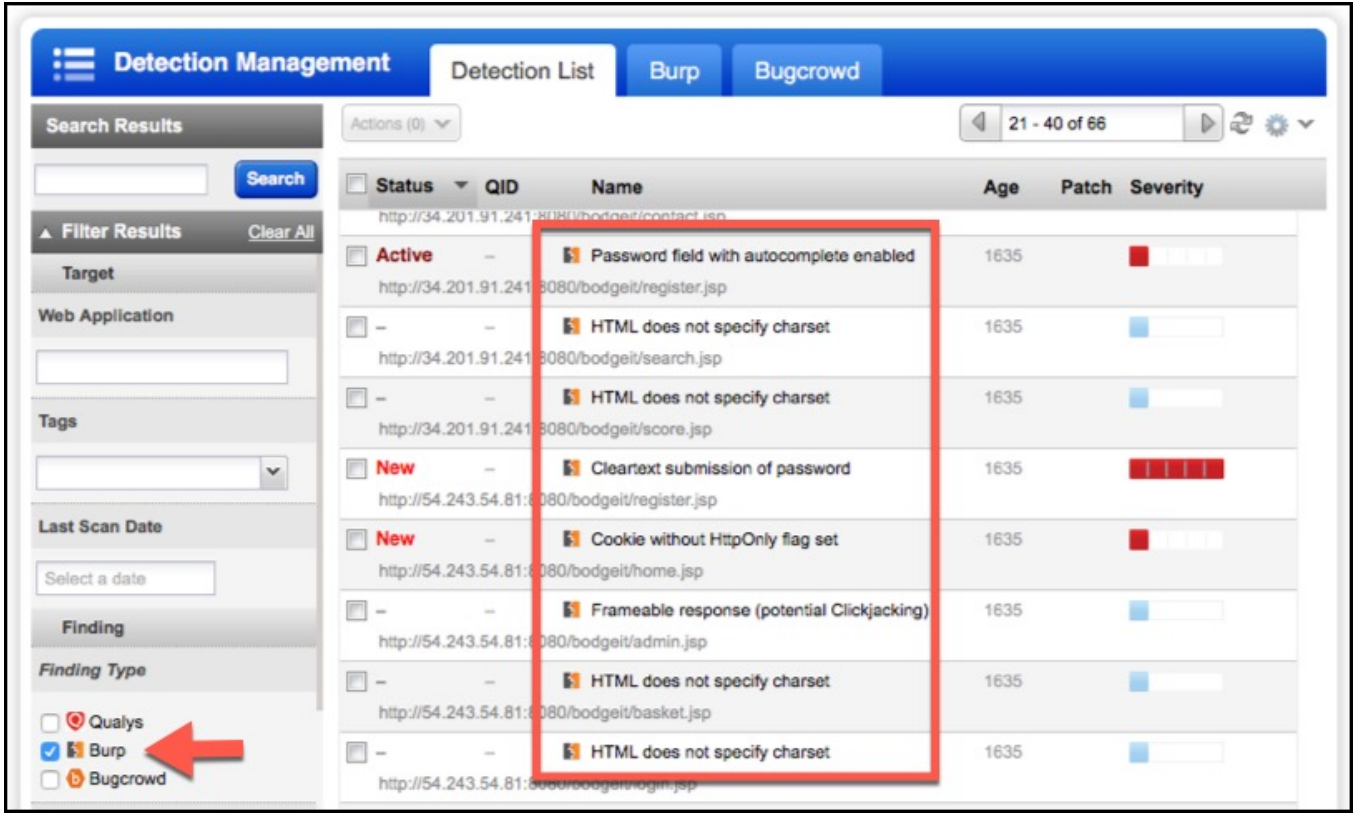
Burp Suite



Web Application Scanning

Qualys.

Burp Suite Professional Integration



Qualys.

Lab Tutorial

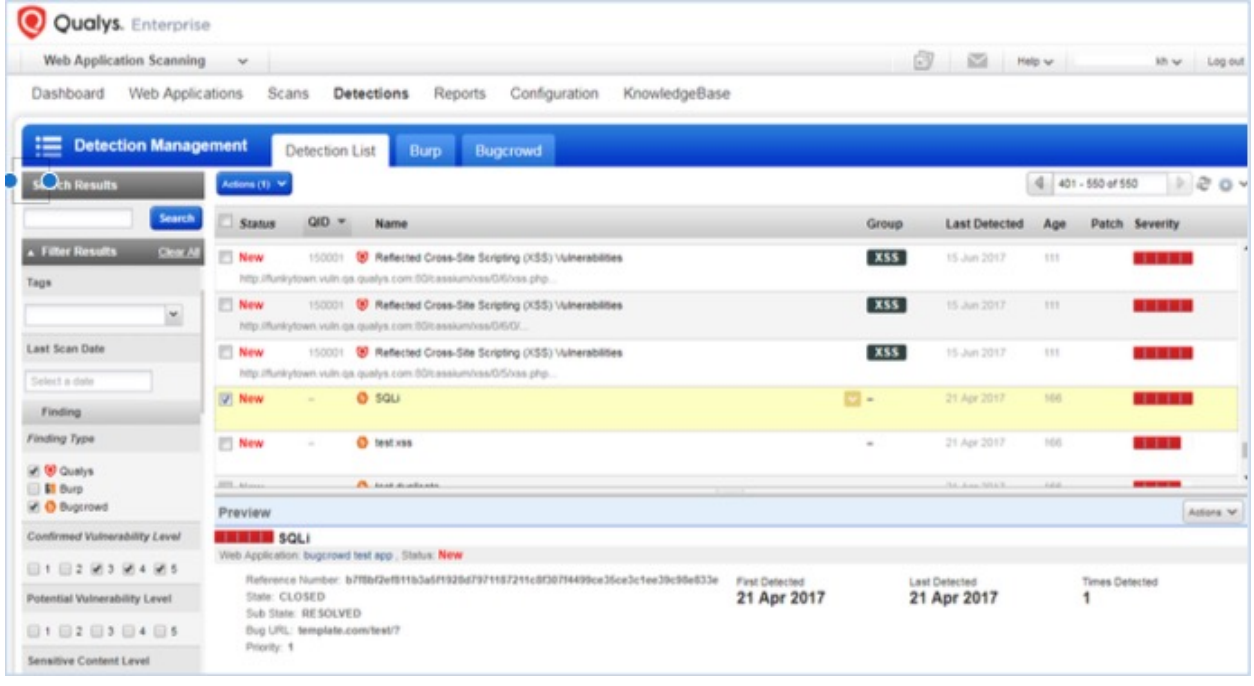
Please follow **page 26** from the Lab Tutorial Supplement

- Lab 14 – Burp Integration, p. 26

Qualys.

Bugcrowd Integration

- Import approved Bugcrowd submissions into Qualys WAS.
- View and report on vulnerabilities identified by WAS, as well as those found via Bugcrowd bug bounty programs.



Qualys.

Qualys®

Thank You

training@qualys.com