Web Application Scanning - Qualys WAS

Ben Allen

August 2013
Why Scan Applications?

• Attackers are already trying
• Know what data is at risk
• Understand how flaws impact your ability to protect important data
• Think about how applications are developed in a new way
• Demonstrate the need to fix / re-write / protect / shut down old applications
Approaches to Scanning

Manual
+ full access to details
+ can exploit, pivot
+ business logic testing
+ complex processes
- time consuming
- difficult to repeat exactly

Automated
+ easily repeated
+ scheduled
+ report on differences
- limited configuration
- little insight into details, process
- cannot test business logic
Qualys WAS

• To request access, email abuse@umn.edu

• If you have any questions, please email abuse@umn.edu

• Qualys has offered to come to campus to provide training on WAS … we will gladly arrange if there is demand
Qualys WAS

Workflow Overview

• Configure an “Option Profile” (if needed)
• Define a “Web Application”
• Launch (or schedule) a scan of a Web Application using a specific Option Profile
• Review the results

• Note: Logins to Qualys portal are permitted only from UMN IP addresses
Qualys WAS: Choose WAS
Qualys WAS: Dashboard

Dashboard
Sun 11 Aug 2013
23 total scanned web apps
0 with Malware Monitoring

Most Vulnerable Web Applications

<table>
<thead>
<tr>
<th>Web Application Name</th>
<th>Last Scan Date</th>
<th>Total Vulnerabilities</th>
<th>High</th>
<th>Med</th>
<th>Low</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>UIIS-BALLEN-DojoBasic</td>
<td>26 Jul 2013</td>
<td>58</td>
<td>25</td>
<td>7</td>
<td>27</td>
<td>HIGH</td>
</tr>
<tr>
<td>LT Root Wordpress</td>
<td>04 May 2012</td>
<td>71</td>
<td>9</td>
<td>1</td>
<td>61</td>
<td>HIGH</td>
</tr>
<tr>
<td>UIIS-Workshop-A-DYWA</td>
<td>09 Aug 2013</td>
<td>57</td>
<td>6</td>
<td>11</td>
<td>40</td>
<td>HIGH</td>
</tr>
</tbody>
</table>

Your Last Scans

<table>
<thead>
<tr>
<th>Scan Name</th>
<th>Scan Date</th>
<th>Status</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>BDJA - 2...</td>
<td>06 Aug 2013</td>
<td>Finished</td>
<td>HIGH</td>
</tr>
<tr>
<td>UIIS-Workshop-A-DYWA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BDJA - ...</td>
<td>06 Aug 2013</td>
<td>No Host Alive</td>
<td>-</td>
</tr>
<tr>
<td>UIIS-Workshop-A-DYWA</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Your Upcoming Scans

No upcoming scans.

Catalog

Total 3236
3236 New
0 Rogue
0 Approved
0 Ignored
0 In Subscription

Latest Reports

Scan Report
09 Aug 2013
Configure an Option Profile

• UIS has made a copy of the default option profile for each of your departments
• Option Profiles are GLOBAL to WAS … changing the default profile affects all UMN users
• Please copy the default profile and edit to suit your needs
• Prefix your option profile names with your department name to help navigate
Configure an Option Profile

• Option profiles control how the scan runs
  – What requests are used (GET, POST, both)?
  – How many links should be crawled?
  – How intense should the scanner be?
  – Should brute-forcing be done? How much?
  – Use a custom list of scanner tests (QIDs)?
Qualys WAS: Option Profiles
Qualys WAS: Option Profiles
Qualys WAS: Option Profiles
Qualys WAS: Option Profiles
Qualys WAS: Option Profiles
Define a Web Application

• A Web Application defines the target in WAS
  – Metadata - Name, URL (can include port), Scope, Business Information, Tags
  – Option Profile
  – Crawl Settings
  – Authentication Settings
  – Exclusion Lists
  – Malware Monitoring
  – Comments
Qualys WAS: Define Application
Qualys WAS: Define Application
Qualys WAS: Define Application

Web Application Creation

Step 2 of 8

2. Scan Settings

Please choose a default scan setting for the web application

Default Scan Options

Please choose a default scan setting for the web application. This can be modified for each scan.

Option Profile

- None
- LT Media Lab Scan Profile
- OIT Video Solutions-Initial WAS Options
- OIT-Initial WAS Options
- SPH-EHS-Initial WAS Options
- SUA-Initial WAS Options
- [Other options listed]
Qualys WAS: Define Application
Qualys WAS: Define Application
Configure Authentication

- Authentication is managed per application
- Setup is done when defining an application
- Handles server auth – HTTP Basic, Digest and NTLM
- Handles form-based authentication
- Can use Selenium for advanced needs
Qualys WAS: Authentication
Qualys WAS: Authentication
Qualys WAS: Authentication
Qualys WAS: Authentication
Qualys WAS: Authentication

• Authentication is configured
• Continue with application configuration
Qualys WAS: Define Application
Qualys WAS: Define Application
Qualys WAS: Define Application

Web Application Creation

Step 7 of 8

Review comments associated to this web application

Enter a new comment:

Demonstration web application for WAS Workshop
Qualys WAS: Define Application

Web Application Creation

Step 8 of 8

Review and confirm web application settings

Basic Information
- Name: UIS - Workshop Target 1
- Owner: Ben Allen (umnsa_ba)

Business Function: --
Business Location: --
Business Description: --

Comment:
Demonstration web application for UIS Workshop

Target Information
- Web Application URL:
  http://134.84.85.120:42841
- Crawl Scope:
  Limit to URL hostname (134.84.85.120)
- Explicit URLs to Crawl:
  --
Qualys WAS: Launch Scan

- Scans can be launched from the “Finish And Scan” button on the previous screen.
- Scans can also be launched from the Web Applications list. I find this method more reliable.
- There are 2 scan types – Discovery & Vulnerability.
Qualys WAS: Launch Scan

- Discovery
- No vulnerability checks
- Good to run first; use to understand what will be visited
- Spider + information checks

- Vulnerability
- Discovery plus tests for vulnerabilities
Qualys WAS: Launch Scan
Qualys WAS: Launch Scan

**Launch New WAS Vulnerability Scan**

**Step 1 of 2**

**Target**

Name your scan and configure target to be assessed

**Definition**

**Scan Name**

UIS - Workshop - Web Application Vulnerability Scan - UIS - W

**Target Information**

Select the web application you want to launch a scan against. An optional authentication record can be selected to run the scan in authenticated mode.

**Web Application**

UIS - Workshop Target 1

**Authentication Record**

UIS - Workshop Simple Authn

**Option Profile**

Default [UIS Workshop Copy of Initial WAS Options]

Select also the scanner that will launch the scan against the selected web application.

**Scanner Appliance**

External

[Continue button]
Launch New WAS Vulnerability Scan

Step 2 of 2

Review and confirm scan settings

Definition

Scan Name
UIS - Workshop - Web Application Vulnerability Scan - UIS - Workshop Target 1 - 2013-08-11

Target Information

Web Application
UIS - Workshop Target 1
Authentication Record
UIS - Workshop Simple Authn
Option Profile
Default [UIS Workshop Copy of Initial WAS Options]
Scanner Appliance
External
Constraints
This task will run till completion.

Previous  Find
Qualys WAS: Scan Status
Qualys WAS: Scan List

• The “Scan List” page shows the most recent scans, and their states
• The “Quick Actions” menu gives access to:
  – cancel running scans
  – view the scan details
  – view the report for completed scans
Qualys WAS: Scan List
Qualys WAS: View Scan

• Selecting “View” from the “Quick Actions” menu shows the scan details, including:
  – Status – Finished, Submitted, Running
  – Authentication Status
  – Screen Shot
  – Summary of Results (graph)
  – Details (duration, # requests, etc.)
Qualys WAS: View Scan

WAS Vulnerability Scan View

Scan findings overview

UIS - Workshop - Web Application Vulnerability Scan - UIS - Workshop Target 1 - 2013-08-11

Status
Finished

Authentication Status
Failure

Duration
00:43:07

Crawling Time
00:02:08

Assessment Time
00:39:17

Links Crawled
42

# Requests
9498

Operating System
Ubuntu / Linux 2.6.x

![Graph showing vulnerabilities and log information](image-url)
Qualys WAS: View Report

• Choosing “View Report” from the “Quick Actions” menu opens the report viewer
• Reports can be downloaded in multiple formats
  – PDF, PPT, HTML, CSV
• Reports can be modified interactively to adjust what is included and how items are grouped
Qualys WAS: Save Report

Save report

Please provide the following information about this report.

Report Format

Select a format*

- Web Archive (.HTML)
- Compressed HTML pages (ZIP)
- Web Archive (.HTML)
- Portable Document Format (PDF)
- Encrypted Portable Document Format (PDF)
- Microsoft PowerPoint Document (PPT)
- Extensible Markup Language (XML)
- Comma-Separated Value (CSV)

(*) Required Fields

Cancel

Apply all suggested

Save
Qualys WAS: View Report
Qualys WAS: View Report
Qualys WAS

• Online help is well written, and context aware
• Qualys publishes video tutorials on many features (including Selenium)
• We have access to Qualys support for more in-depth training – can tailor to suit the U's needs
• Email abuse@umn.edu with questions