II) HCL App Scan Standard

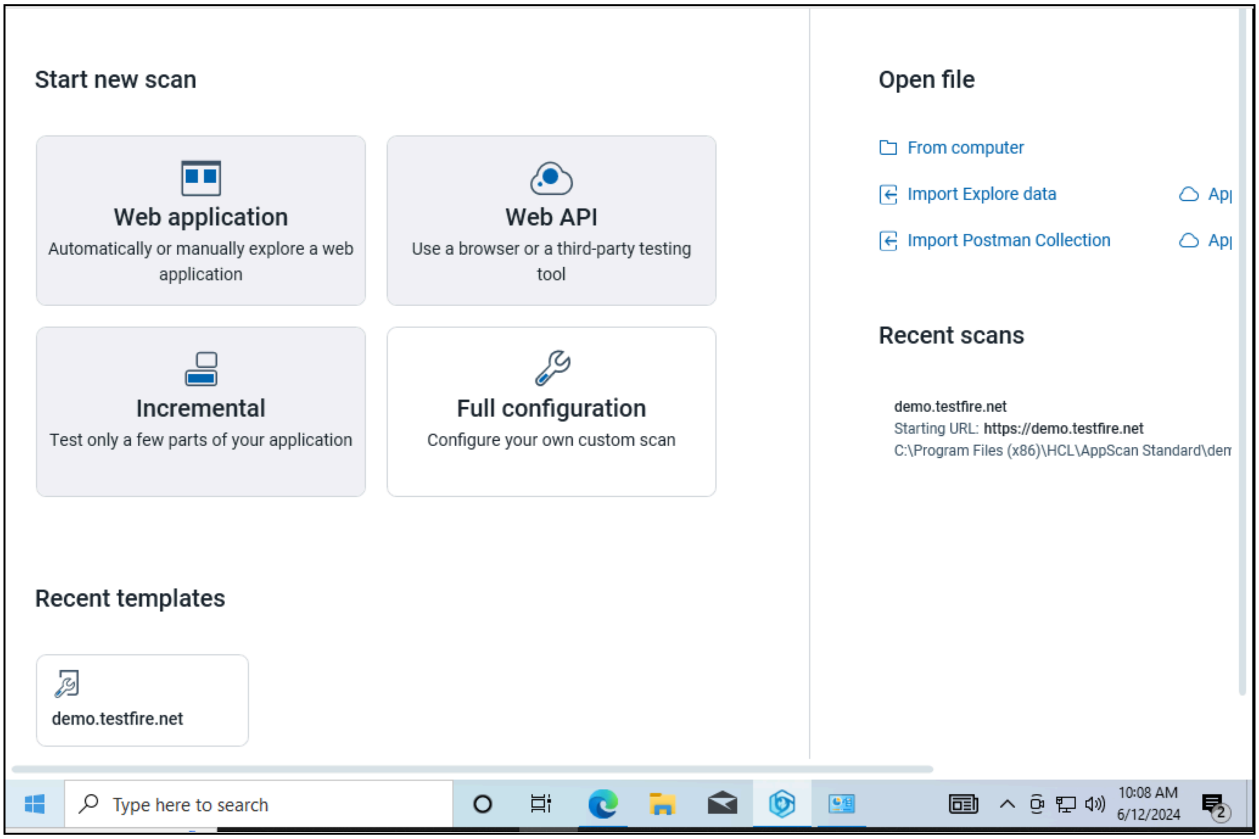
HCL App Scan Standard is primarily designed for security experts and pen testers to use when performing security tests on web applications and web API. It runs automated scans that explore and test web applications based on one of the most powerful scanning engines available.
It allows quickly triage and prioritize issues, using a wealth of information provided including test descriptions and detailed vulnerability descriptions. Advisories provide issue remediation advice and fix recommendations for each detected issue.

Community Insights from Gartner:

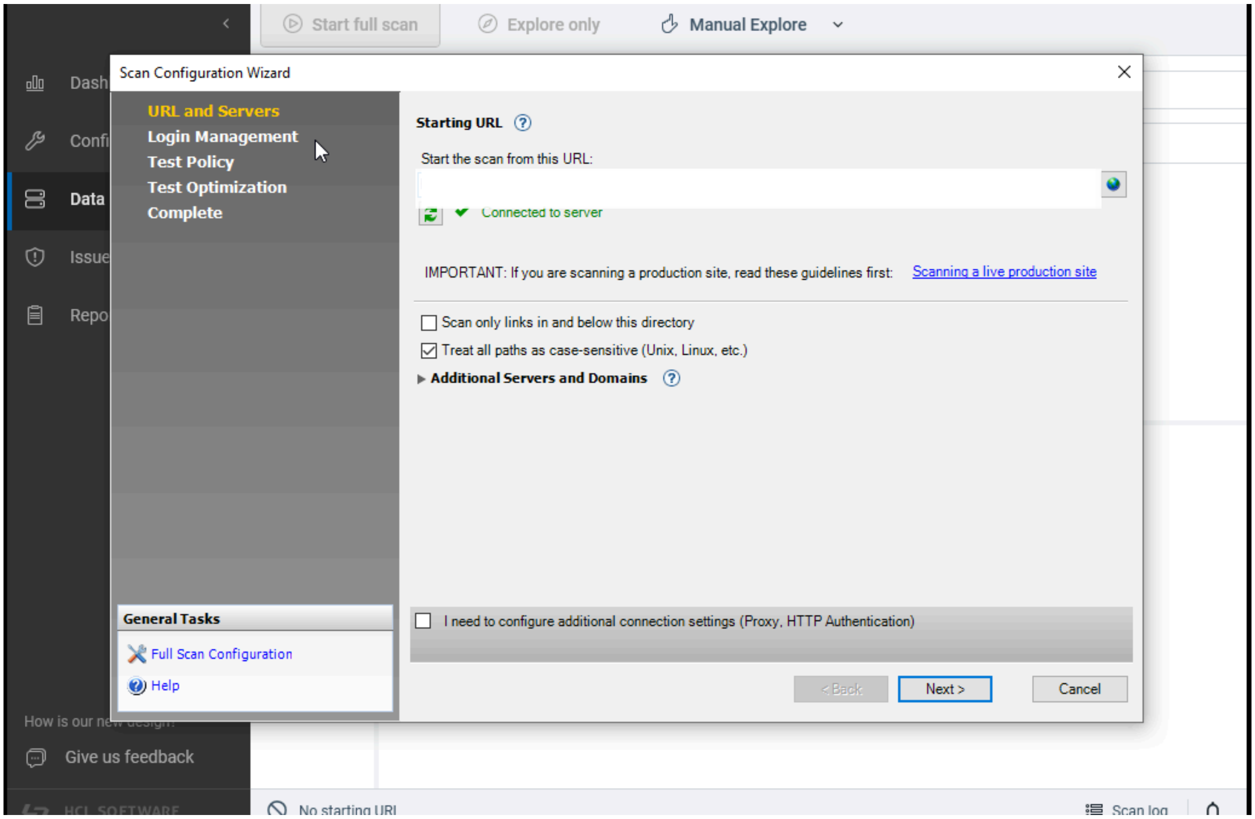
https://drive.google.com/file/d/11AgkaZVaEbERjtmPw0OSVzS2D83fLaRL/view?usp=sharing

Step by Step Procedure:

Initialization:


Start new scan
Web application
Automatically or manually explore a web application
Web API
Use a browser or a third-party testing tool
Incremental
Test only a few parts of your application
Full configuration
Configure your own custom scan
Recent templates
demo.testfire.net
Open file
From computer
Import Explore data
Ap|
Import Postman Collection
Ap|
Recent scans
demo.testfire.net
Starting URL: https://demo.testfire.net
C:\Program Files (x86)\HCL\AppScan Standard\dem
Type here to search
10:08 AM
6/12/2024

Step 01: Open HCL App Scan Standard



Scan Configuration Wizard

- URL and Servers
- Login Management
- Test Policy
- Test Optimization
- Complete

Starting URL

Start the scan from this URL:

✓ Connected to server

IMPORTANT: If you are scanning a production site, read these guidelines first: Scanning a live production site

□ Scan only links in and below this directory

☑ Treat all paths as case-sensitive (Unix, Linux, etc.)

▶ **Additional Servers and Domains**

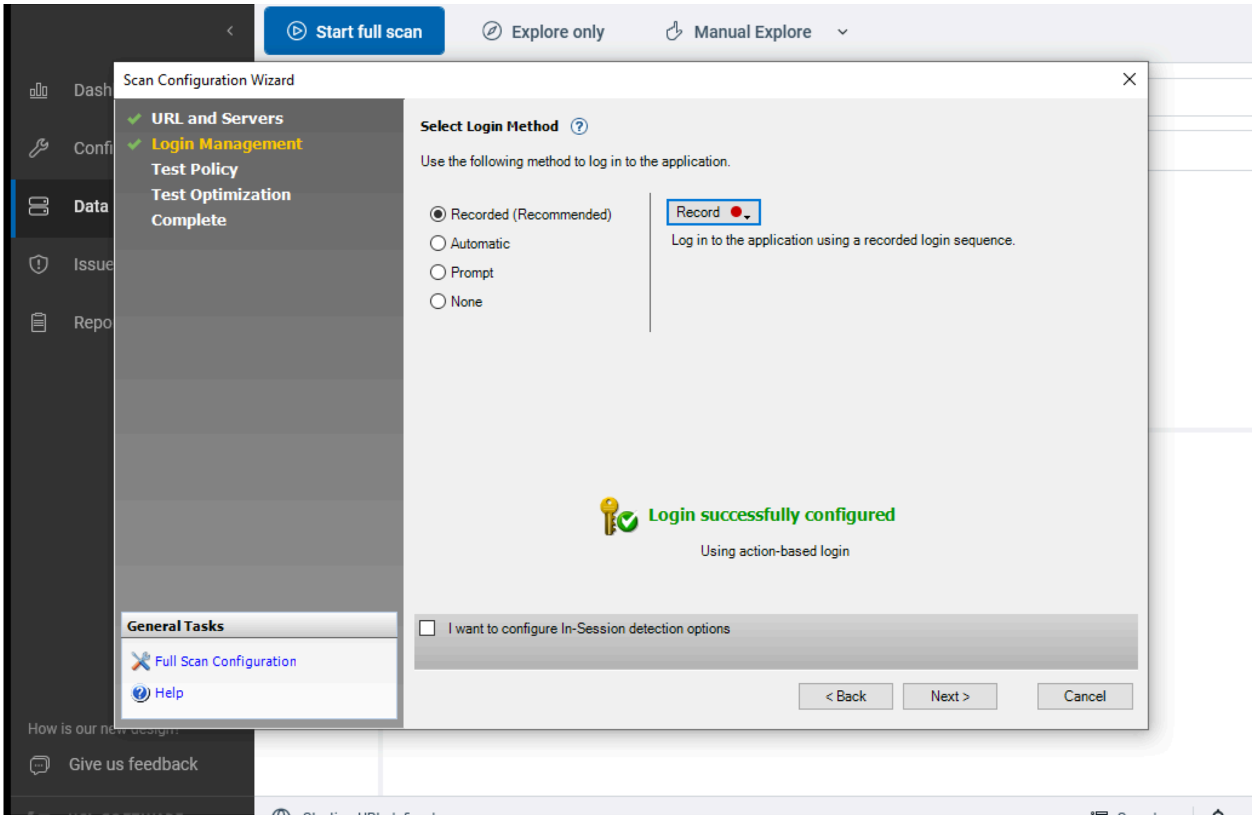
General Tasks

- Full Scan Configuration
- Help

□ I need to configure additional connection settings (Proxy, HTTP Authentication)

< Back | Next > | Cancel

Step 02: Insert the URL to Scan



Scan Configuration Wizard

- ✓ URL and Servers
- ✓ Login Management
- Test Policy
- Test Optimization
- Complete

Select Login Method

Use the following method to log in to the application.

● Recorded (Recommended)
○ Automatic
○ Prompt
○ None

Record ●

Log in to the application using a recorded login sequence.

Login successfully configured

Using action-based login

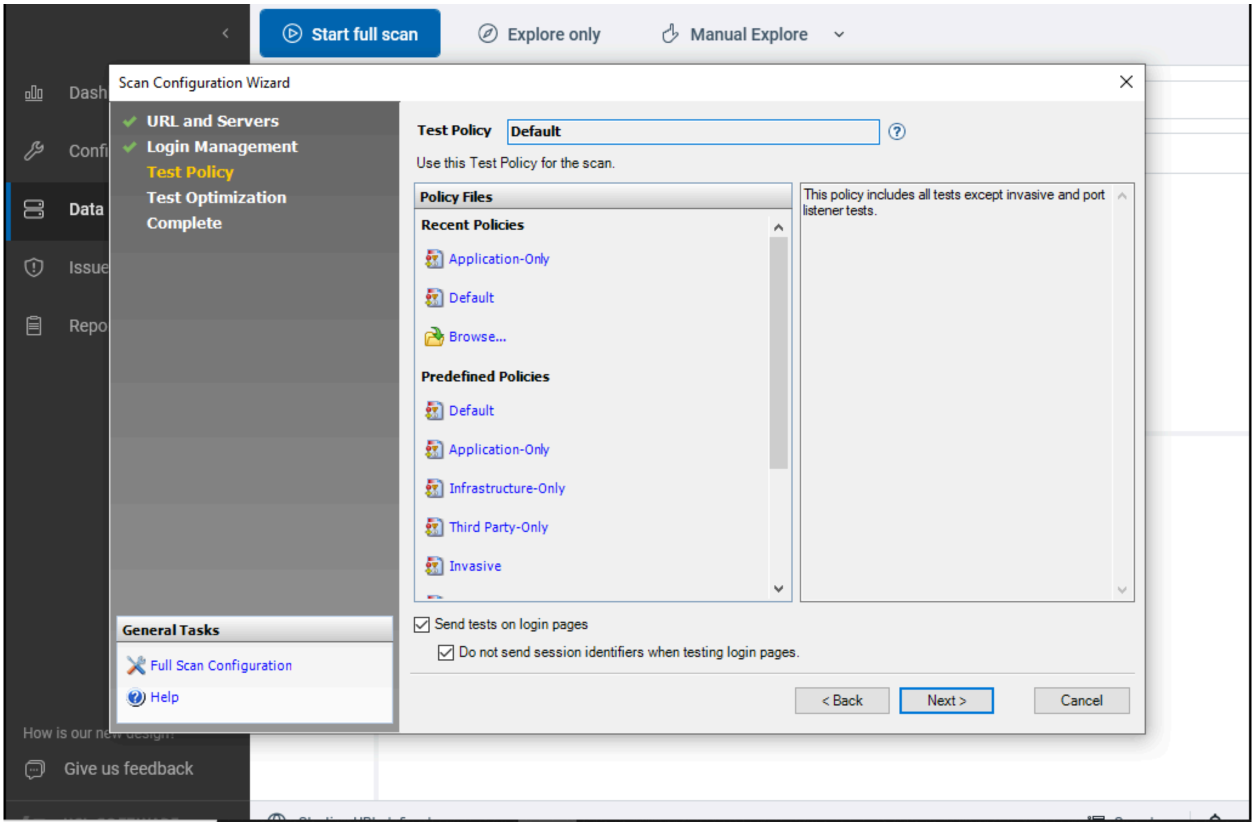
General Tasks

- Full Scan Configuration
- Help

□ I want to configure In-Session detection options

< Back | Next > | Cancel

Step 03: Record the login



Scan Configuration Wizard

- ✓ URL and Servers
- ✓ Login Management
- Test Policy
- Test Optimization
- Complete

Test Policy: Default

Use this Test Policy for the scan.

Policy Files

Recent Policies

- Application-Only
- Default
- Browse...

Predefined Policies

- Default
- Application-Only
- Infrastructure-Only
- Third Party-Only
- Invasive

This policy includes all tests except invasive and port listener tests.

☑ Send tests on login pages

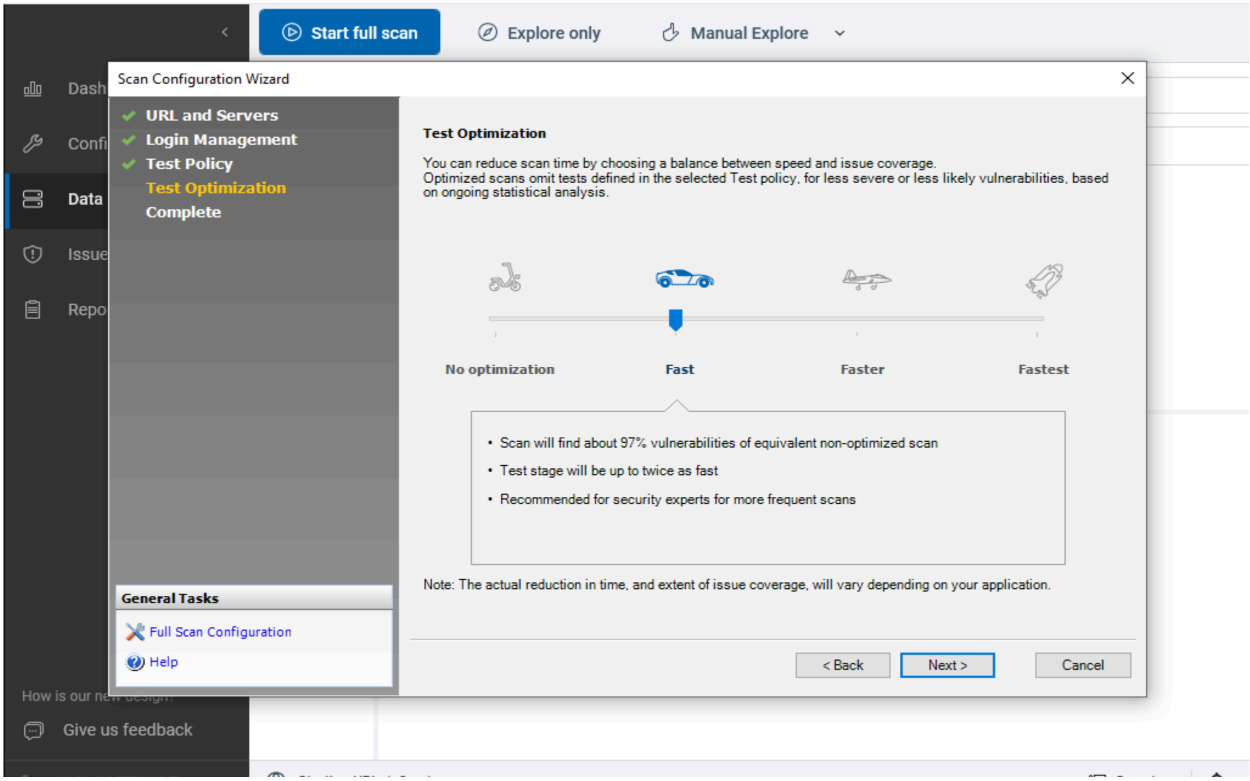
☑ Do not send session identifiers when testing login pages.

General Tasks

- Full Scan Configuration
- Help

< Back | Next > | Cancel

Step 04: Choose the Policy to carry out the scanning



Scan Configuration Wizard

- ✓ URL and Servers
- ✓ Login Management
- ✓ Test Policy
- Test Optimization
- Complete

Test Optimization

You can reduce scan time by choosing a balance between speed and issue coverage. Optimized scans omit tests defined in the selected Test policy, for less severe or less likely vulnerabilities, based on ongoing statistical analysis.

No optimization | **Fast** | Faster | Fastest

- Scan will find about 97% vulnerabilities of equivalent non-optimized scan
- Test stage will be up to twice as fast
- Recommended for security experts for more frequent scans

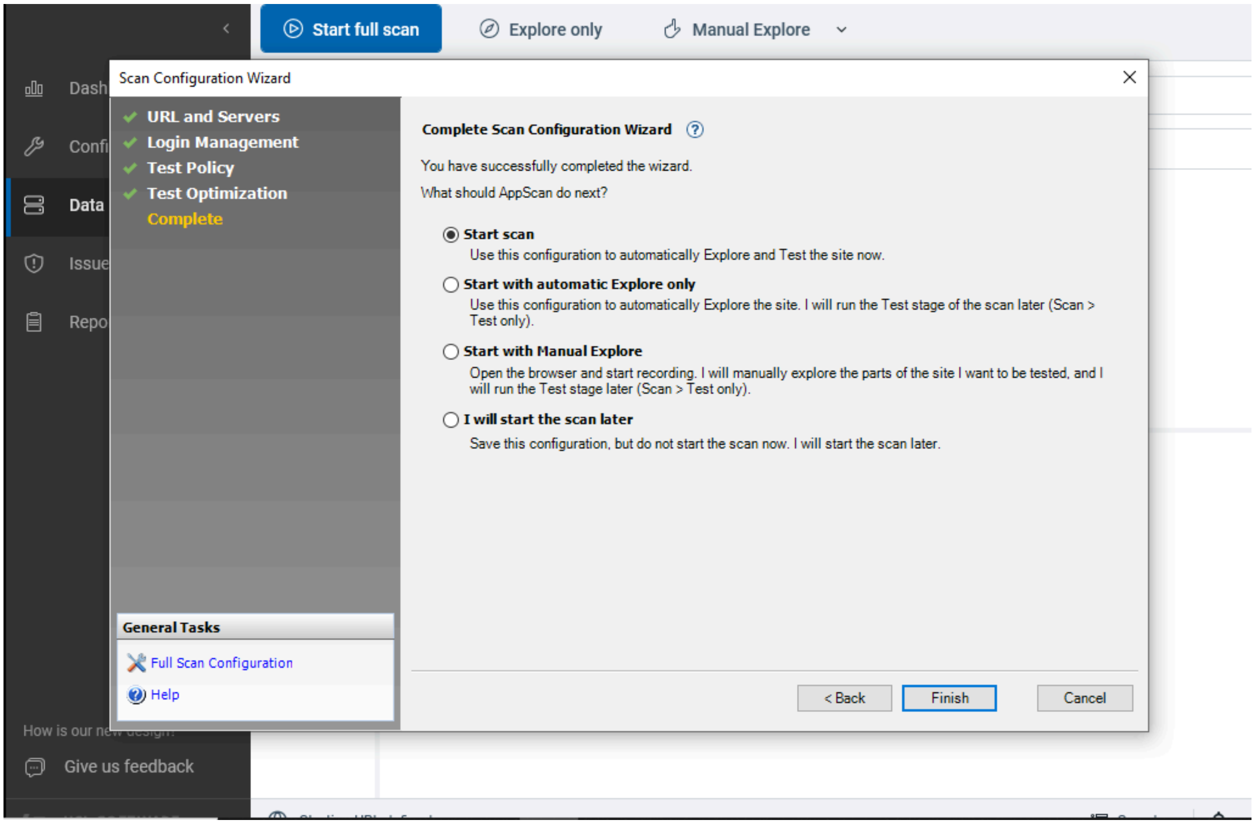
Note: The actual reduction in time, and extent of issue coverage, will vary depending on your application.

General Tasks

- Full Scan Configuration
- Help

< Back | Next > | Cancel

Step 05: Choose the testing Speed level



Scan Configuration Wizard

- ✓ URL and Servers
- ✓ Login Management
- ✓ Test Policy
- ✓ Test Optimization
- Complete

Complete Scan Configuration Wizard

You have successfully completed the wizard.

What should AppScan do next?

● **Start scan**
Use this configuration to automatically Explore and Test the site now.

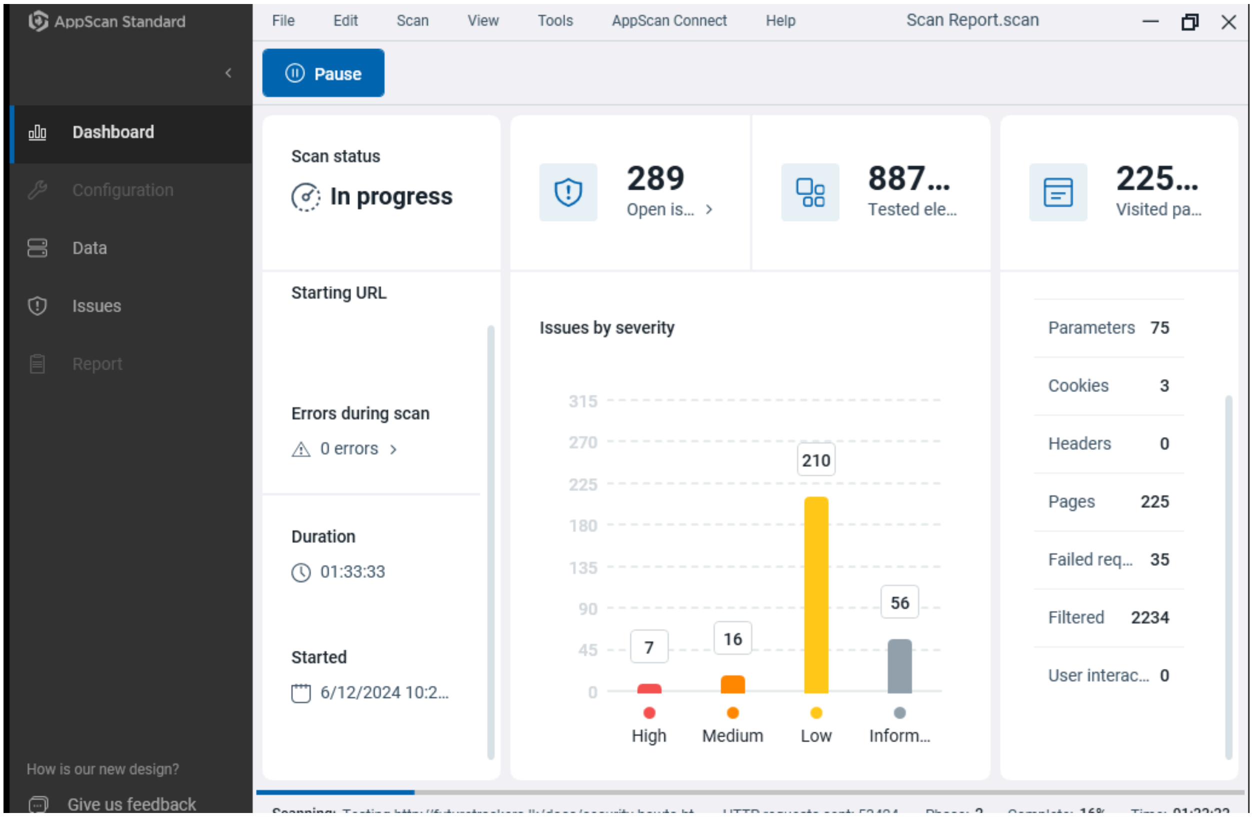
○ **Start with automatic Explore only**
Use this configuration to automatically Explore the site. I will run the Test stage of the scan later (Scan > Test only).

○ **Start with Manual Explore**
Open the browser and start recording. I will manually explore the parts of the site I want to be tested, and I will run the Test stage later (Scan > Test only).

○ **I will start the scan later**
Save this configuration, but do not start the scan now. I will start the scan later.

Step 06: Start the Scan

Scan In Progress:



Scan status: In progress

289 Open is...

887... Tested ele...

225... Visited pa...

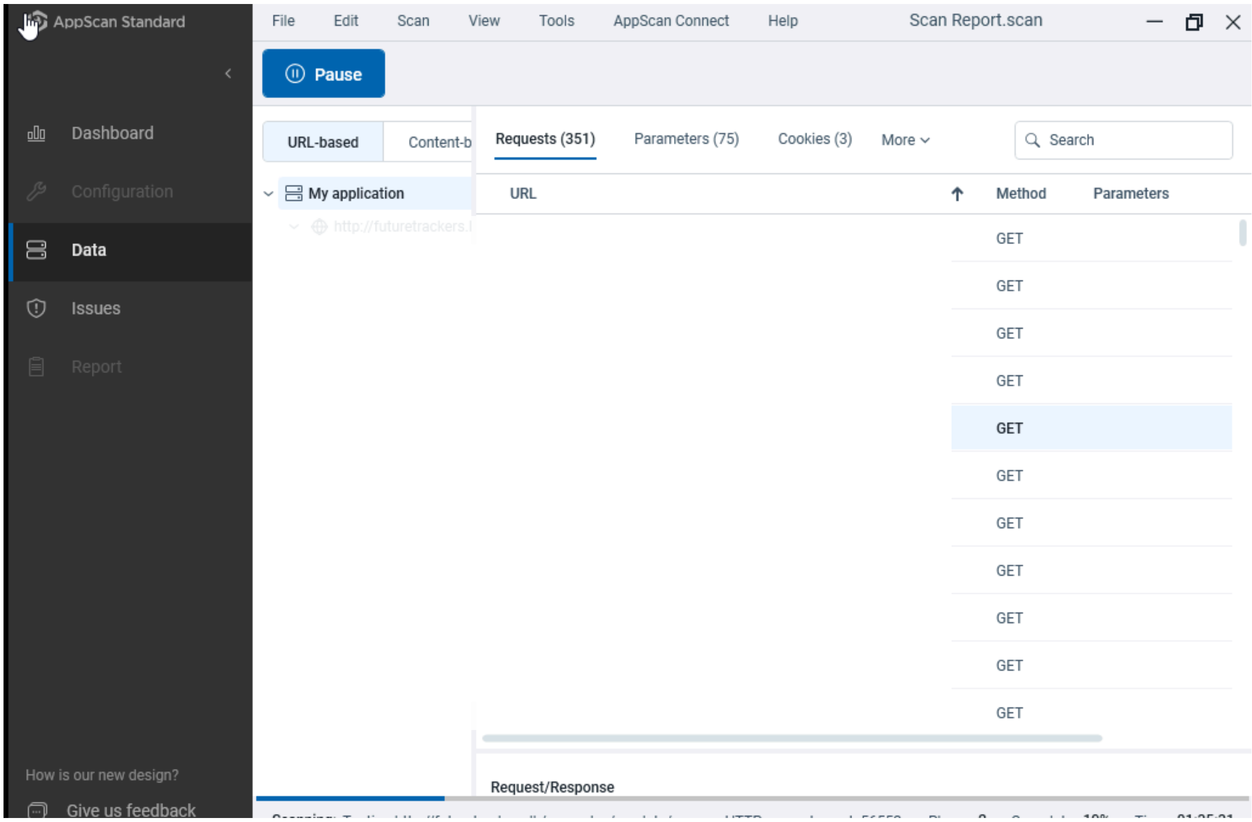
Starting URL

Errors during scan: 0 errors

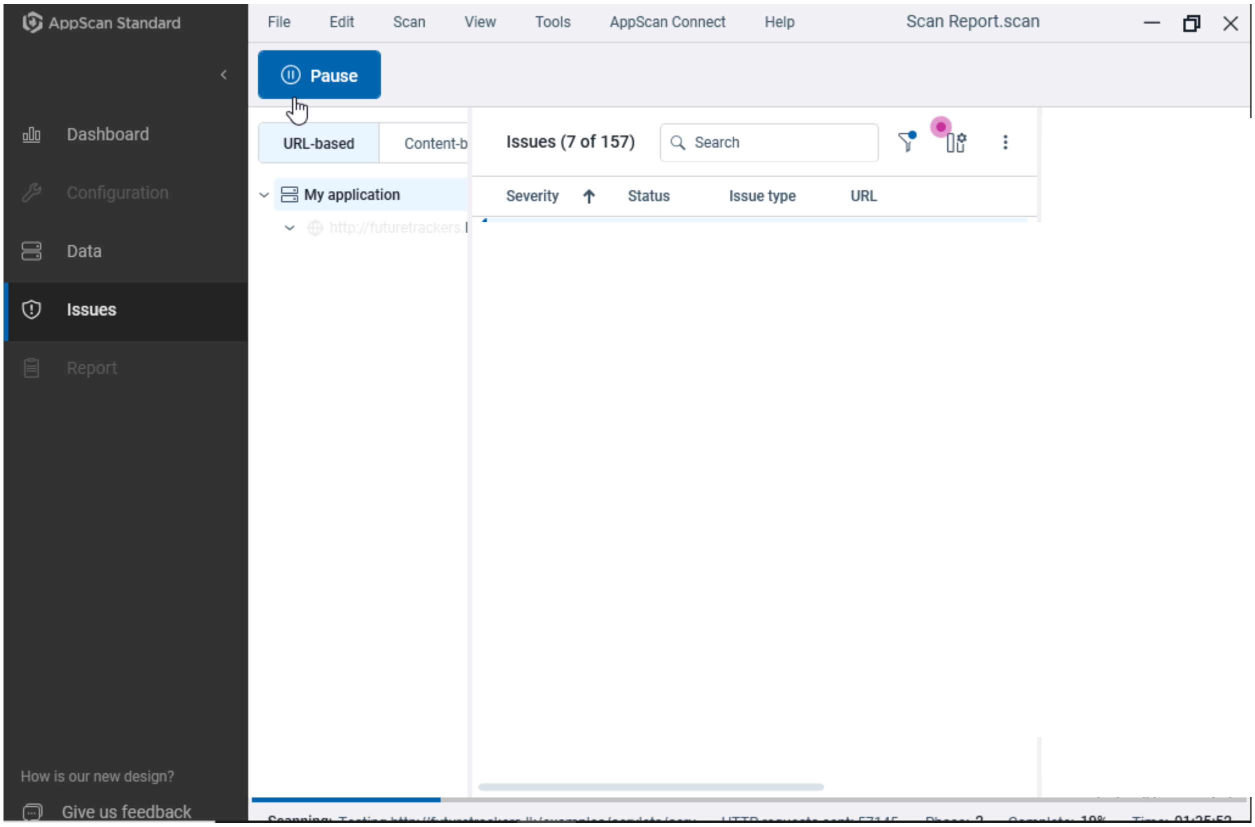
Duration: 01:33:33

Started: 6/12/2024 10:2...

Parameters	75
Cookies	3
Headers	0
Pages	225
Failed req...	35
Filtered	2234
User interac...	0

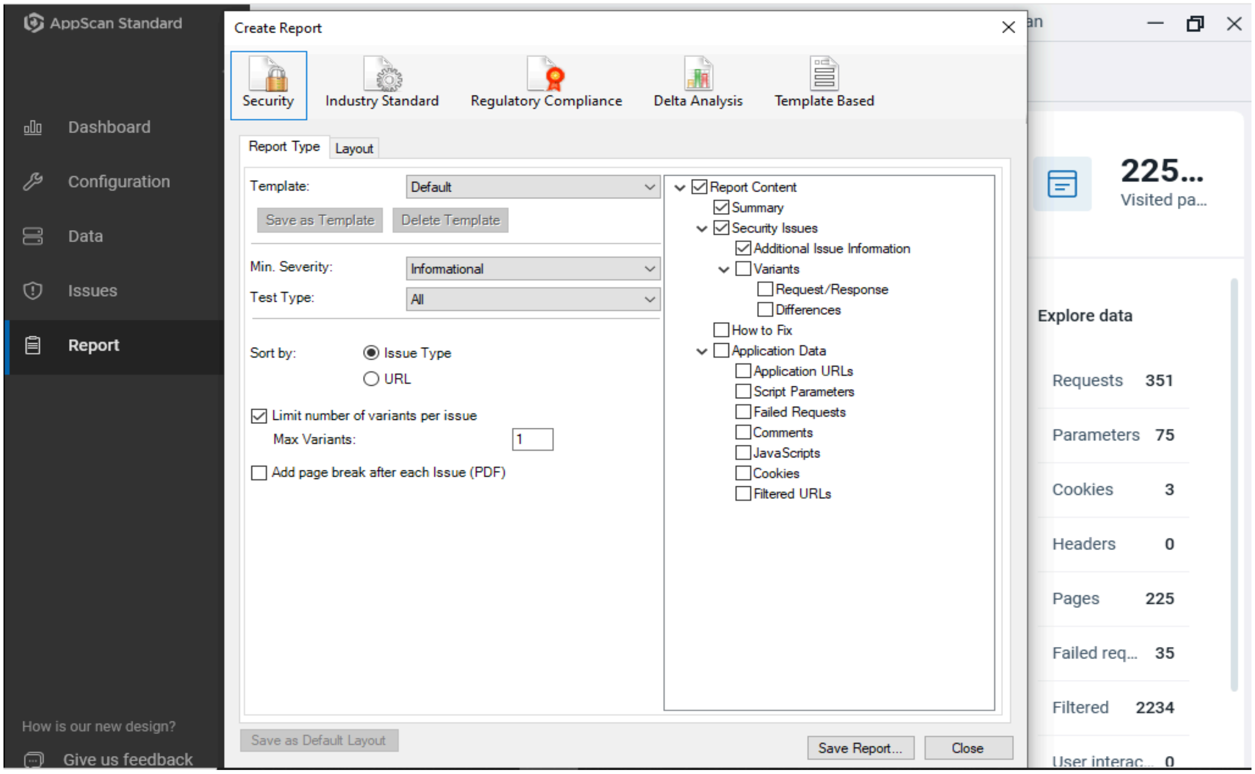


URL	Method	Parameters
	GET	
	GET	
	GET	
	GET	
	GET	
	GET	
	GET	
	GET	
	GET	
	GET	
	GET	



Scanning: Testing http://futuretrackers.lk/examples/servlets/serv... HTTP requests sent: 57145 Phase: 2 Complete: 10% Time: 01:25:52

Report Generation:



Create Report

Report Type | Layout

Template: Default

Min. Severity: Informational

Test Type: All

Sort by: ● Issue Type ○ URL

☑ Limit number of variants per issue

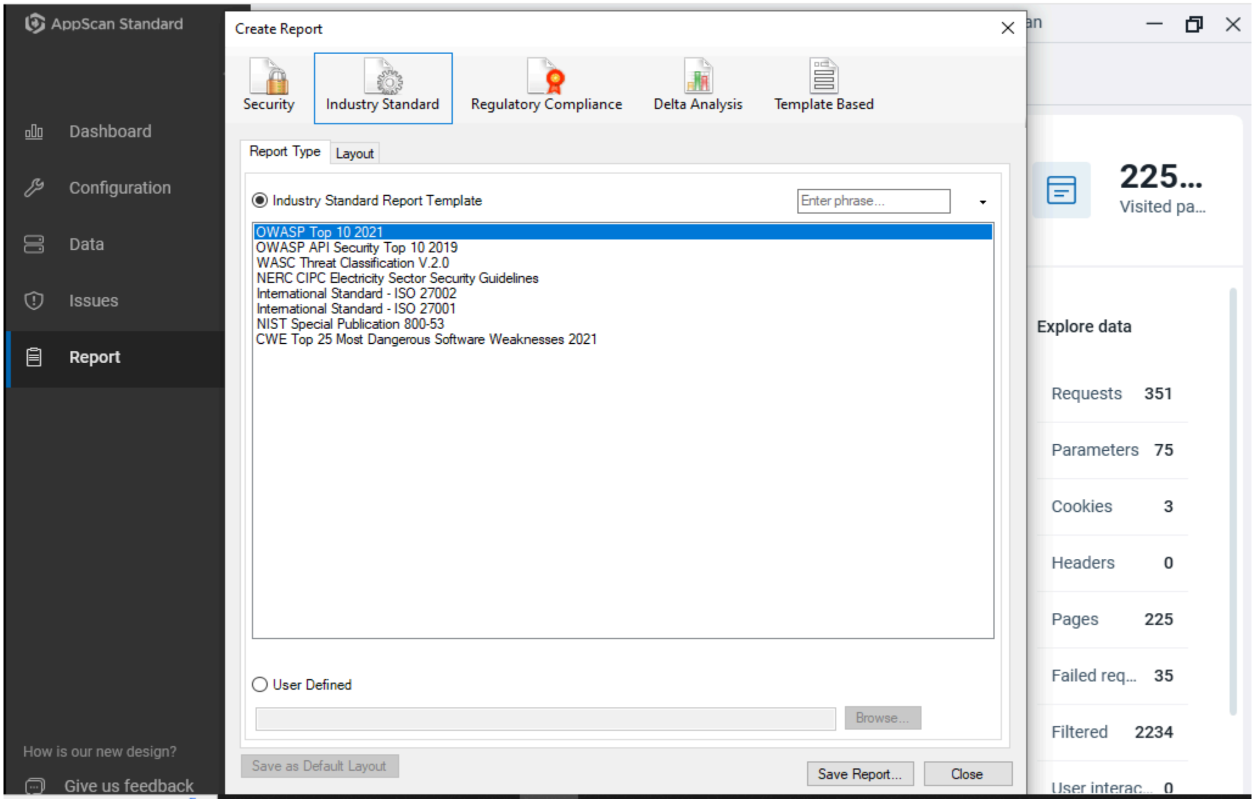
Max Variants: 1

□ Add page break after each Issue (PDF)

- ☑ Report Content
  - ☑ Summary
  - ☑ Security Issues
    - ☑ Additional Issue Information
    - □ Variants
      - □ Request/Response
      - □ Differences
  - □ How to Fix
  - □ Application Data
    - □ Application URLs
    - □ Script Parameters
    - □ Failed Requests
    - □ Comments
    - □ JavaScripts
    - □ Cookies
    - □ Filtered URLs

Requests	351
Parameters	75
Cookies	3
Headers	0
Pages	225
Failed req...	35
Filtered	2234
User interac...	0

Step 01: Select the report and customize the content



Create Report

Report Type | Layout

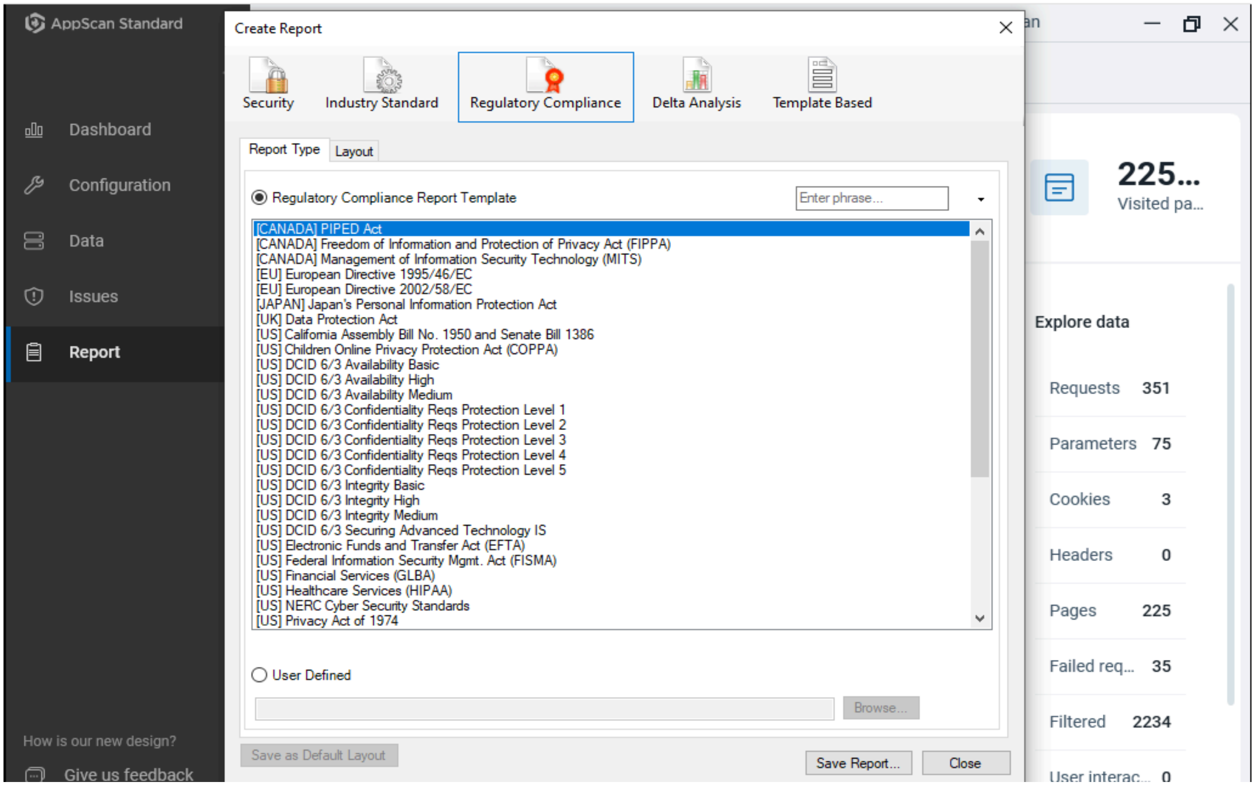
● Industry Standard Report Template

OWASP Top 10 2021
OWASP API Security Top 10 2019
WASC Threat Classification V.2.0
NERC CIPC Electricity Sector Security Guidelines
International Standard - ISO 27002
International Standard - ISO 27001
NIST Special Publication 800-53
CWE Top 25 Most Dangerous Software Weaknesses 2021

○ User Defined

Requests	351
Parameters	75
Cookies	3
Headers	0
Pages	225
Failed req...	35
Filtered	2234
User interac...	0

Step 02: Select the Report type



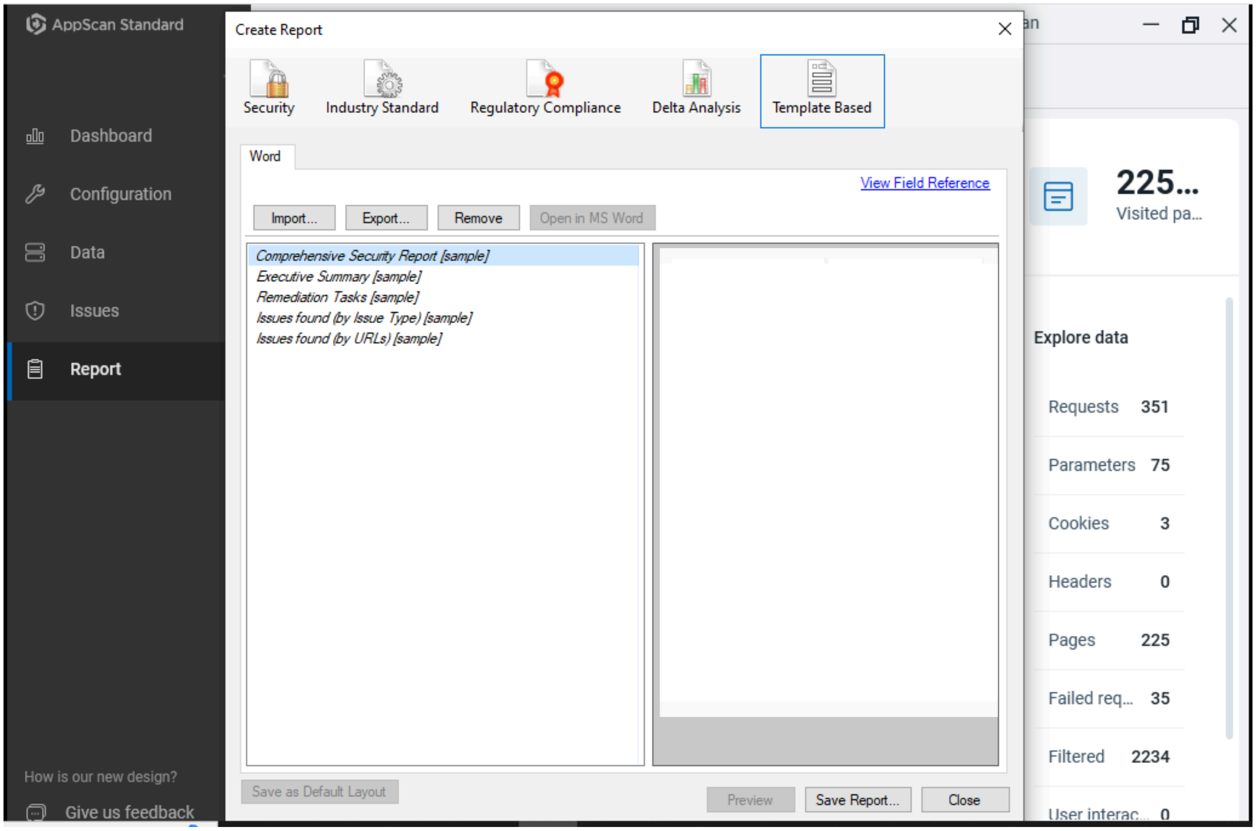
● Regulatory Compliance Report Template

- [CANADA] PIPED Act
- [CANADA] Freedom of Information and Protection of Privacy Act (FIPPA)
- [CANADA] Management of Information Security Technology (MITS)
- [EU] European Directive 1995/46/EC
- [EU] European Directive 2002/58/EC
- [JAPAN] Japan's Personal Information Protection Act
- [UK] Data Protection Act
- [US] California Assembly Bill No. 1950 and Senate Bill 1386
- [US] Children Online Privacy Protection Act (COPPA)
- [US] DCID 6/3 Availability Basic
- [US] DCID 6/3 Availability High
- [US] DCID 6/3 Availability Medium
- [US] DCID 6/3 Confidentiality Reqs Protection Level 1
- [US] DCID 6/3 Confidentiality Reqs Protection Level 2
- [US] DCID 6/3 Confidentiality Reqs Protection Level 3
- [US] DCID 6/3 Confidentiality Reqs Protection Level 4
- [US] DCID 6/3 Confidentiality Reqs Protection Level 5
- [US] DCID 6/3 Integrity Basic
- [US] DCID 6/3 Integrity High
- [US] DCID 6/3 Integrity Medium
- [US] DCID 6/3 Securing Advanced Technology IS
- [US] Electronic Funds and Transfer Act (EFTA)
- [US] Federal Information Security Mgmt. Act (FISMA)
- [US] Financial Services (GLBA)
- [US] Healthcare Services (HIPAA)
- [US] NERC Cyber Security Standards
- [US] Privacy Act of 1974

○ User Defined

Requests	351
Parameters	75
Cookies	3
Headers	0
Pages	225
Failed req...	35
Filtered	2234
User interac...	0

Step 03: Select the Regulatory Compliance



- *Comprehensive Security Report [sample]*
- *Executive Summary [sample]*
- *Remediation Tasks [sample]*
- *Issues found (by Issue Type) [sample]*
- *Issues found (by URLs) [sample]*

Requests	351
Parameters	75
Cookies	3
Headers	0
Pages	225
Failed req...	35
Filtered	2234
User interac...	0

Step 04: Choose the report template and generate the report

III) OWASP ZAP Scanner

ZAP (Zed Attack Proxy) is an open-source security tool maintained by the OWASP (Open Web Application Security Project) community, designed for finding vulnerabilities in web applications. It is widely used for security testing and is recognized for its ease of use, powerful features, and active development community.

Its powerful features include AJAX Spider which is designed to explore web applications that use AJAX and JavaScript, Passive Scanning, Active Scanning and Scripting which allows users to customize and extend the tool's capabilities using scripts etc.

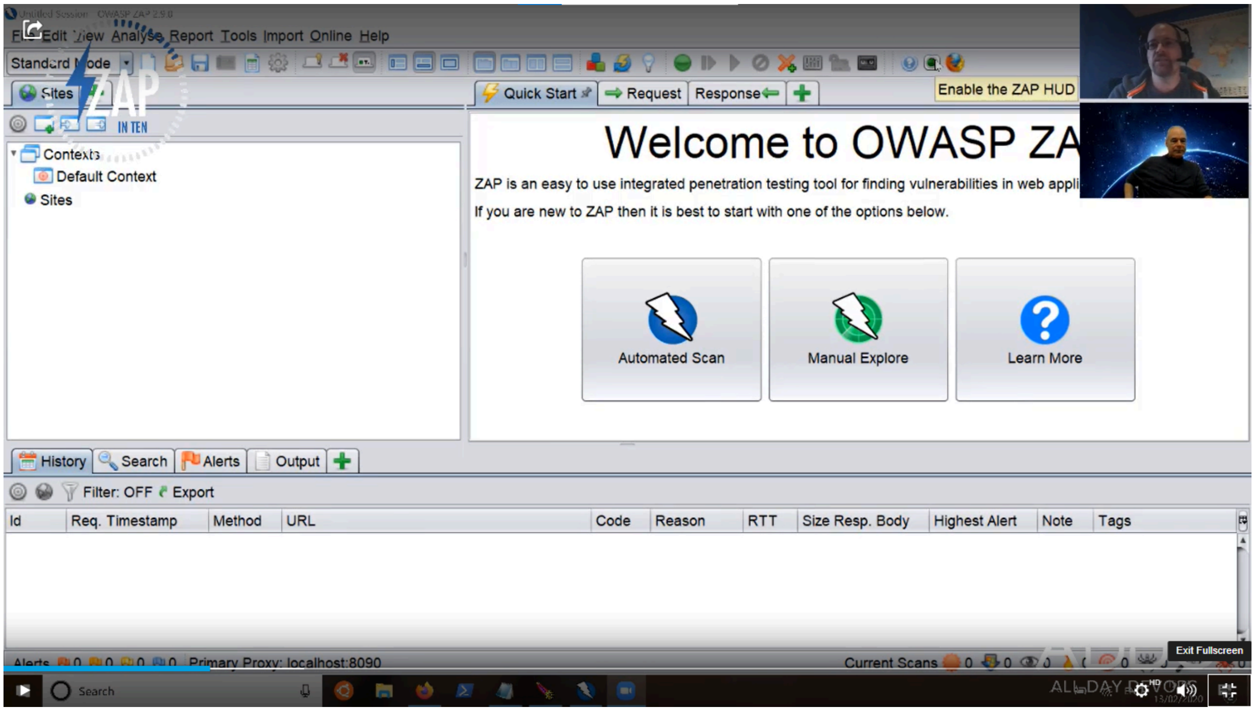
Community Insights from PeerSpot:

https://drive.google.com/file/d/1gMpmOp77HW_iIfF3EZbRtpYpD96tdo2I/view?usp=sharing

Step by step Procedure:

Initialization:

Method I: Enabling HTTP Automatic Authentication



Welcome to OWASP ZA

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web appli

If you are new to ZAP then it is best to start with one of the options below.

Step 01: Disable ZAP HUD