

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.

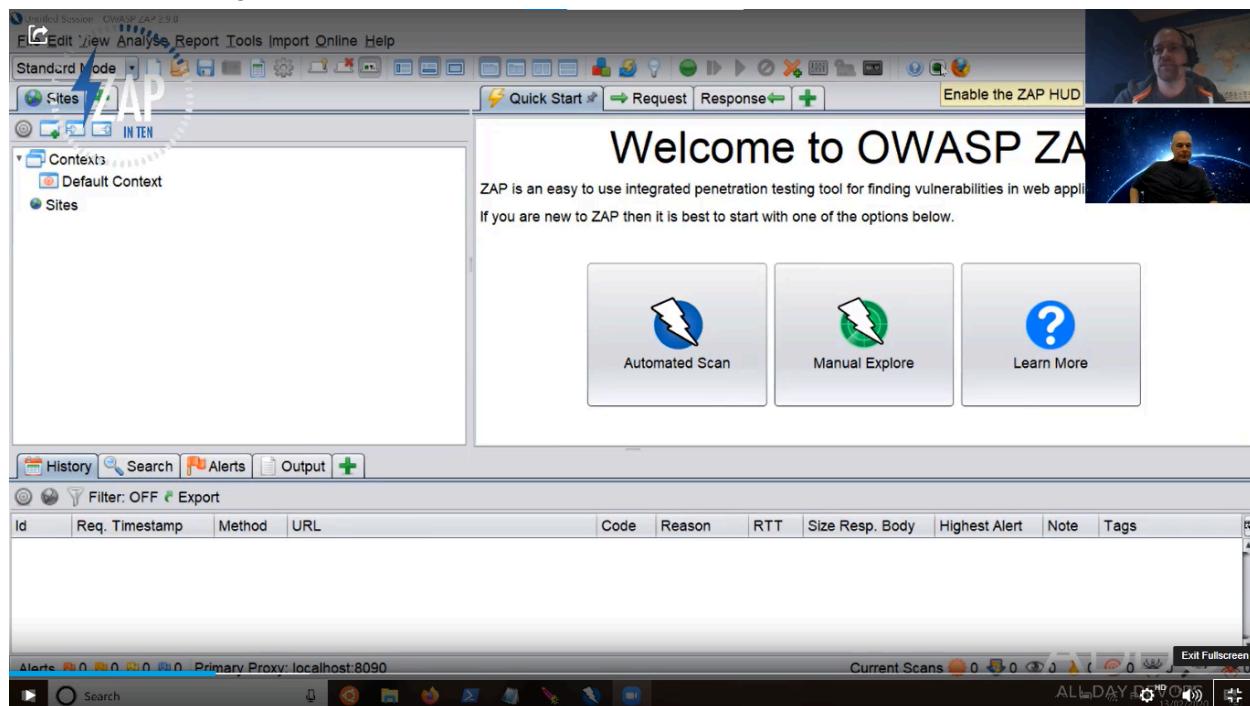
Community Insights from PeerSpot:

https://drive.google.com/file/d/1gMpmOp77HW_ilfF3EZbRtpYpD96tdo2I/view?usp=sharing

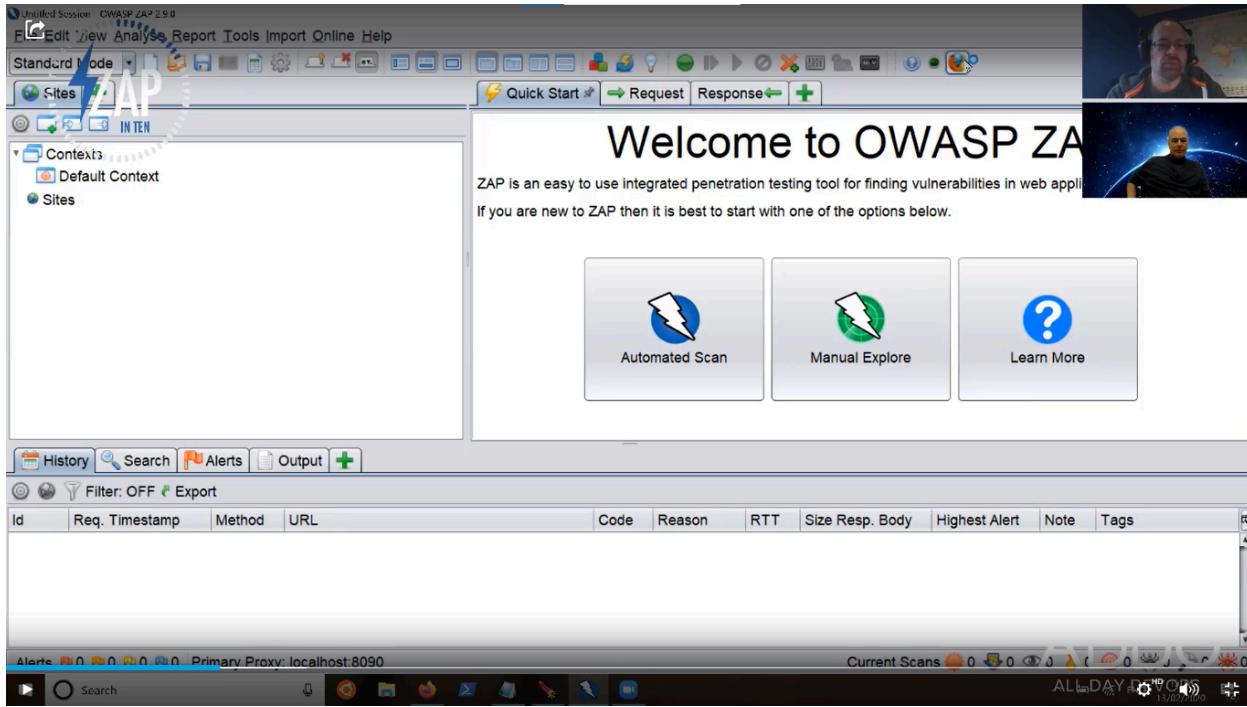
Step by step Procedure:

Initialization:

Method I: Enabling HTTP Automatic Authentication



Step 01: Disable ZAP HUD



Step 02: Launch Firefox

The screenshot shows a Firefox browser window with the URL <https://jigsaw.w3.org/HTTP/>. A login dialog is open, prompting for a user name ('guest') and password ('*****'). A tooltip provides information about the 'Set-Cookie' header. In the background, a sidebar lists various HTTP-related topics such as 'Chunk Encoding', 'TE', 'Content-MD5', 'Retry-After (delay)', 'Retry-After (date)', '300 Multiple Choices', '406 Not Acceptable', '414 Request-URI Too Long', 'Redirect test page', 'Basic Authentication test', 'Digest Authentication test', and 'Content-Location test'. Each topic has a brief description.

Step 03: Log in to the Site

Welcome to OWASP ZAP

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications. If you are new to ZAP then it is best to start with one of the options below.

Automated Scan

Manual Explore

Learn More

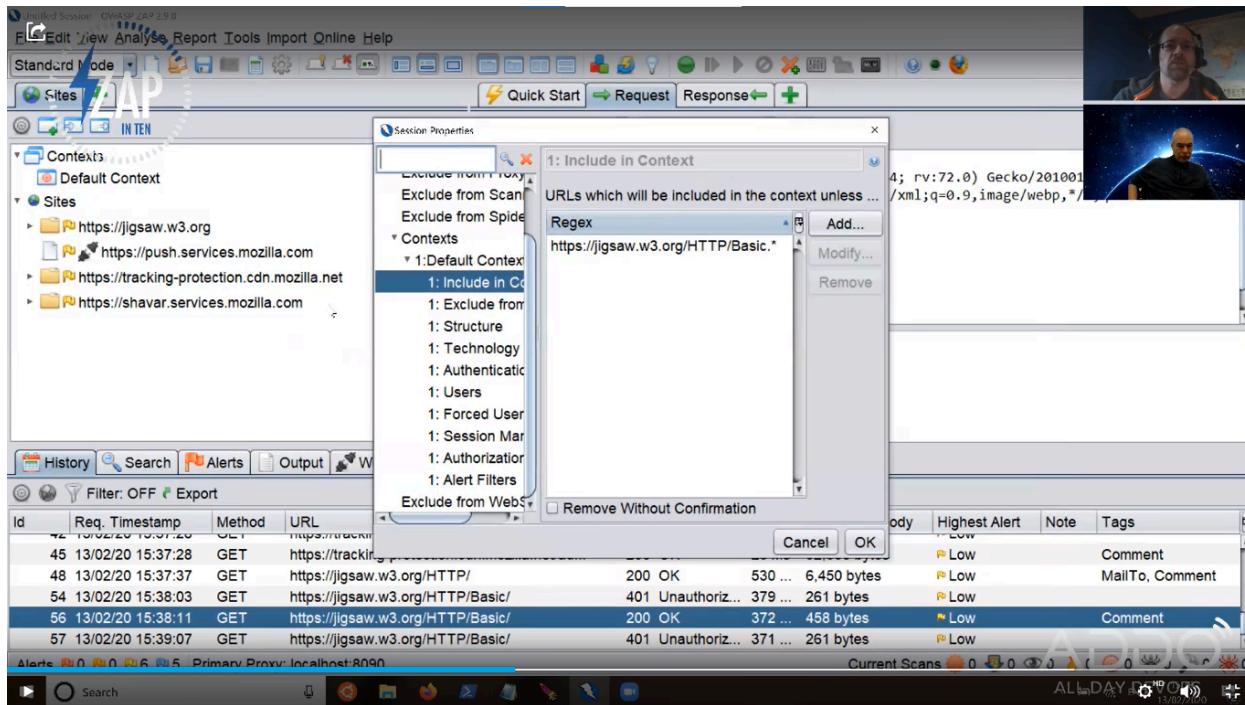
ID	Req. Timestamp	Method	URL	Code	Reason	RTT	Size	Resp. Body	Highest Alert	Note	Tags
40	13/02/20 15:37:20	GET	https://tracking-protection.cdn.mozilla.net/b...	200	OK	21 ms	0,940 bytes		Low		
42	13/02/20 15:37:28	GET	https://tracking-protection.cdn.mozilla.net/ba...	200	OK	24 ms	2,293 bytes		Low		
45	13/02/20 15:37:28	GET	https://tracking-protection.cdn.mozilla.net/ad...	200	OK	20 ms	52,566 bytes		Low		
48	13/02/20 15:37:37	GET	https://jigsaw.w3.org/HTTP/	200	OK	530 ...	6,450 bytes		Low	Comment	
54	13/02/20 15:38:03	GET	https://jigsaw.w3.org/HTTP/Basic/	401	Unauthorized	379 ...	261 bytes		Low	MailTo, Comment	
56	13/02/20 15:38:11	GET	https://jigsaw.w3.org/HTTP/Basic/	200	OK	372 ...	458 bytes		Low	Comment	

Step 04: Go back to ZAP and In History, Find the Auth Request

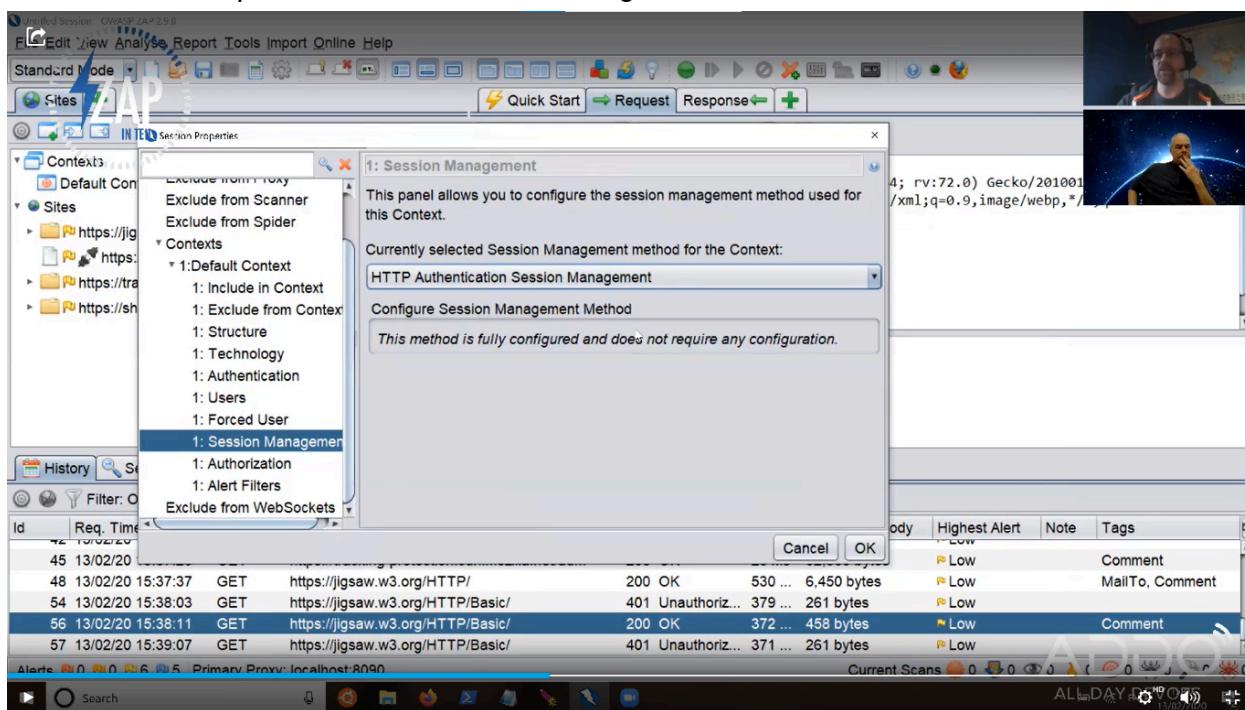
Attack

- Include in Context
- Flag as Context
- Run application
- Accept...
- Exclude from Context
- Open/Rerun with Request Editor...
- Exclude from...
- Open URL in Browser
- Show in Sites Tab
- Open URL in System Browser
- Copy URLs to Clipboard
- Manage Tags...
- Note...
- Delete
- Break...
- New Alert...
- Alerts for This Node
- Generate Anti-CSRF Test FORM
- Invoke with Script...
- Add to Zest Script
- Compare 2 requests
- Compare 2 responses
- Include Channel Url in Context
- Exclude Channel Url from Context
- Save Raw
- Save XML

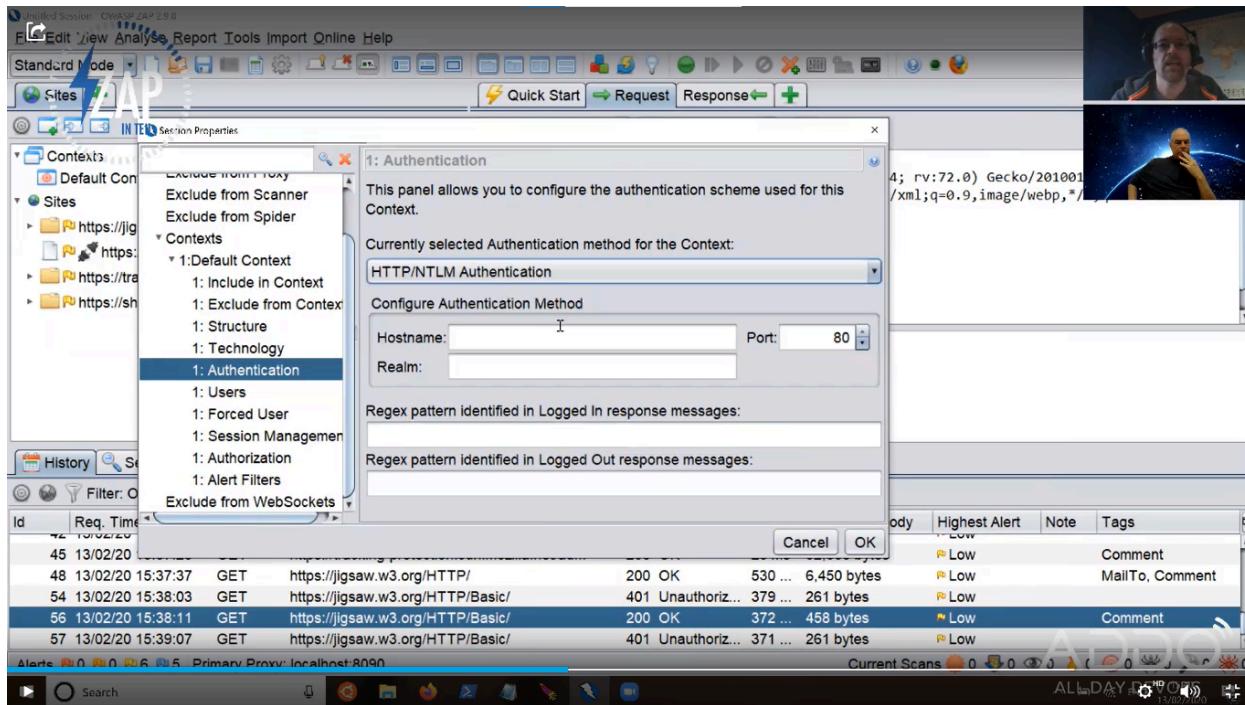
Step 05: Right Click > Include in Context > Default Context



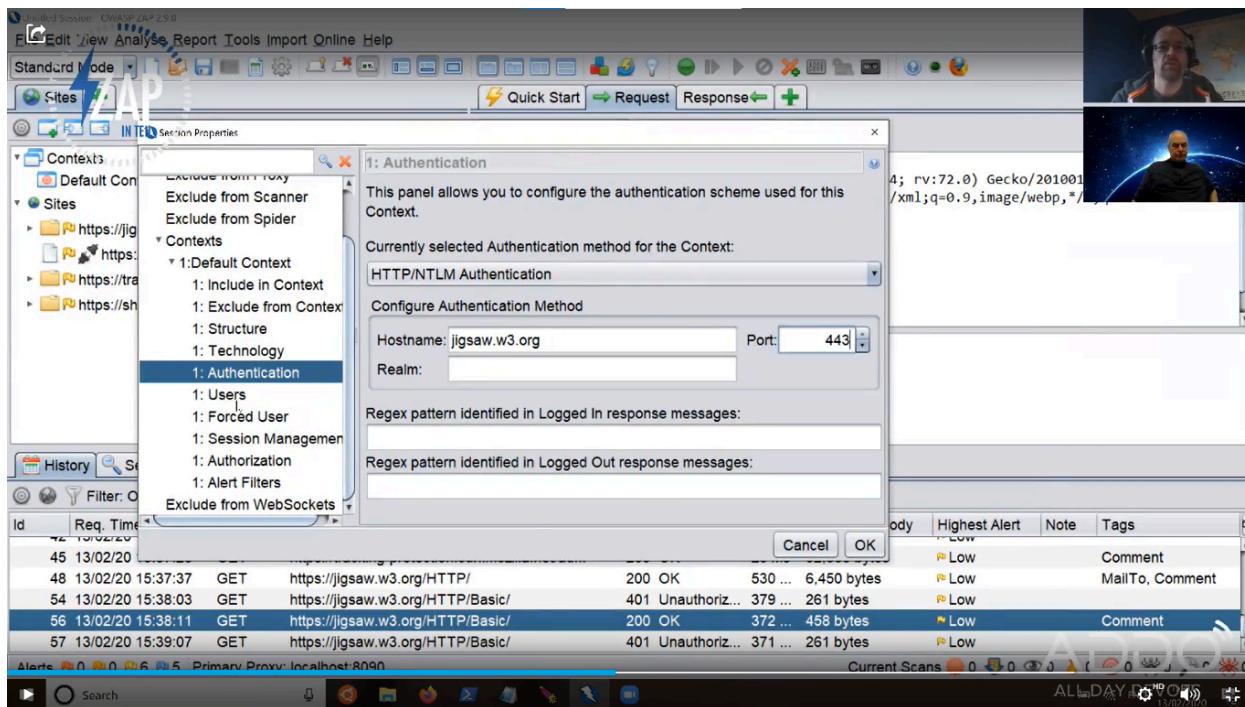
Step 06: Check the URL as a Regex in Include in Context Section



Step 07: Change the Session Mgt as HTTP Auth Session Mgt



Step 08: Choose Authentication Method as HTTP/NTLM Authentication



Step 09: Configure Hostname and Port Number

User Name: guest
Enabled:
Username: guest
Password:

1: Technology
1: Authentication
1: Users
1: Forced User
1: Session Management
1: Authorization
1: Alert Filters

Add... Modify... Remove Enable All Disable All

ID	Name
4	rv:72.0 Gecko/201001/xm...;q=0.9,image/webp,*/*

History Search Alerts 0 0 0 6 Primary Proxy: localhost:8090 Current Scans 0 0 0 0 ALL DAY OFF 13:09:10

Step 10: Add the user in User Section

Header: Text Body: Text

GET https://jigsaw.w3.org/HTTP/Basic/ HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:72.0) Gecko/20100101
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*
Accept-Language: en-GB,en;q=0.5
Connection: keep-alive
Referer: https://jigsaw.w3.org/HTTP/
Upgrade-Insecure-Requests: 1
Authorization: Basic Z3Vlc3Q6Z3Vlc3Q=
Host: jigsaw.w3.org

History Search Alerts 0 0 0 6 Primary Proxy: localhost:8090 Current Scans 0 0 0 0 ALL DAY OFF 13:09:10

Step 11: Enable Forced User Mode

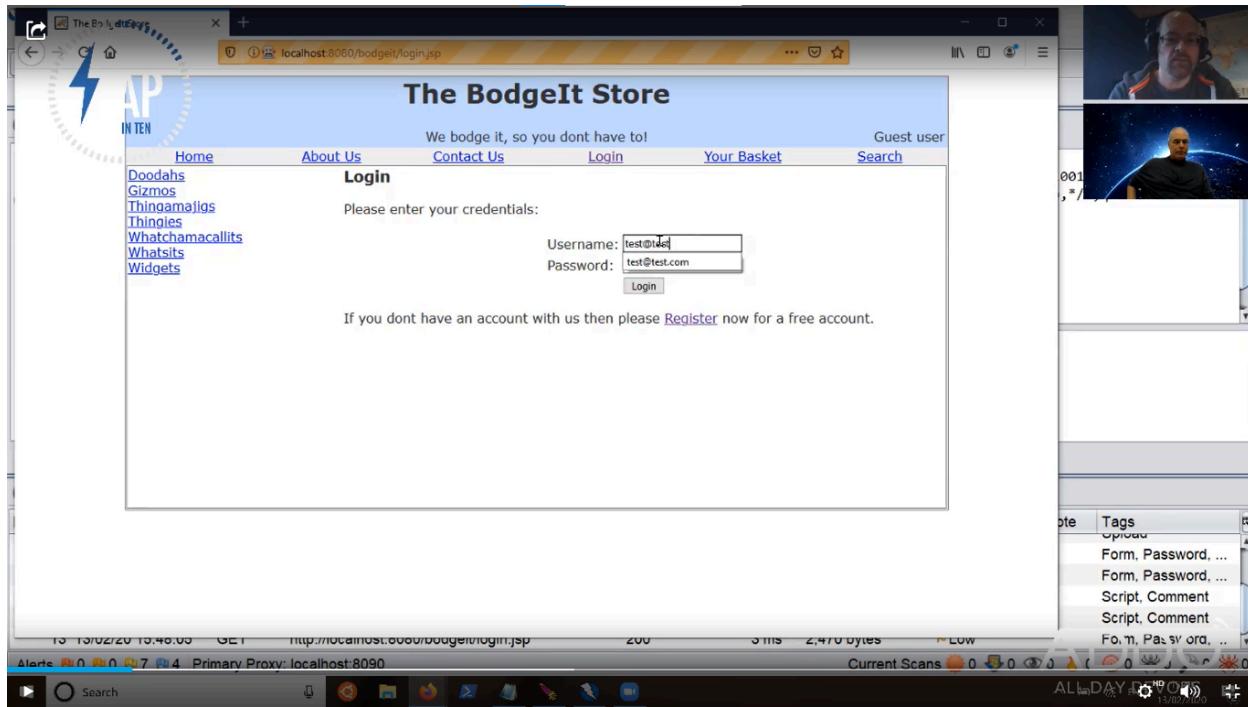
The screenshot shows the OWASP ZAP 2.9.0 interface. In the center, a dialog box titled "Session Properties" is open, specifically the "1: Forced User" tab. It asks, "Select the user that will be used for all the requests made for this context, if the 'Forced User' mode is enabled:" with a dropdown menu showing "guest". On the left, the "Contexts" panel shows "Default Context" selected. On the right, there's a list of alerts and a status bar at the bottom.

Step 12: Choose the Forced User as the User entered

The screenshot shows the OWASP ZAP 2.9.0 interface. A context menu is open over a selected item in the list on the left. The "Open URL in Browser" option is highlighted, with "Firefox" selected from a submenu. The main menu also includes options like "Attack", "Include in Context", and "Exclude from". On the right, there's a list of alerts and a status bar at the bottom.

Step 13: Open the request from the browser and verify automatic authentication

Method II) Enabling Automatic Form based Authentication



Step 01: Access the login using ZAP through Firefox

The screenshot shows the OWASP ZAP 2.9.0 interface. In the 'Sites' panel, there is a sitemap for the 'http://localhost:8080/bodgeit' site, which includes URLs like 'GET:login.jsp', 'POST:login.jsp', 'GET:logout.jsp', 'GET:register.jsp', 'POST:register.jsp', and 'GET:style.css'. The 'Session Properties' dialog is open, specifically the 'Include in Context' tab, where a regex rule 'http://localhost:8080/bodgeit.*' is defined. The 'Alerts' tab at the bottom of the interface lists various security findings, such as 'Form, Password, ...', 'Script, Comment', and 'Form, Password, ...' again, indicating potential vulnerabilities in the login and registration forms.

Step 02: Access site from sitemap and include in context and verify the URL

The screenshot shows the OWASP ZAP 2.9.0 interface. A context named 'bodgeit' is selected in the left sidebar. A context menu is open over the 'bodgeit' folder, with 'Session Management' highlighted. A modal dialog titled '1: Session Management' is displayed, stating: 'This panel allows you to configure the session management method used for this Context.' It shows 'Cookie-based Session Management' as the currently selected method. Below it, a note says: 'This method is fully configured and does not require any configuration.' The bottom right of the dialog has 'Cancel' and 'OK' buttons.

Step 03: Set session mgt as Cookie based session mgt

The screenshot shows the OWASP ZAP 2.9.0 interface. The same context 'bodgeit' is selected. A context menu is open over the 'bodgeit' folder, with 'Authentication' highlighted. A modal dialog titled '1: Authentication' is displayed, stating: 'This panel allows you to configure the authentication scheme used for this Context.' It shows 'Manual Authentication' as the currently selected method. Below it, a note says: 'This method is fully configured and does not require any configuration.' The bottom right of the dialog has 'Cancel' and 'OK' buttons.

Step 04: Choose authentication mode as manual authentication

The screenshot shows the OWASP ZAP interface. In the center, a context menu is open over a POST request from the history tab. The 'Flag as Context' option is highlighted. Other options visible include 'Attack', 'Include in Context', 'Run application', 'Exclude from Context', and 'Open/Resend with Request Editor...'. On the right side of the interface, there is a 'Logs' panel showing various log entries, and at the bottom right, a 'Current Scans' table.

Step 05: Choose the Auth POST request from the history and set it as Default context: Form based Auth Login Request

The screenshot shows the 'Session Properties' dialog box for the 'Default Context' context. The 'Authentication' tab is selected. It displays the configuration for a 'Form-based Authentication' method, including the 'Login Form Target URL' (set to 'http://localhost:8080/bodgeit/login.jsp'), 'URL to GET Login Page' (set to 'http://localhost:8080/bodgeit/login.jsp'), and 'Login Request POST Data (if any)' (set to 'username=test%40test.com&password=test1'). The 'Username Parameter' is 'username' and the 'Password Parameter' is 'password'. Below these fields, there are sections for 'Regex pattern identified in Logged In response messages:' and 'Regex pattern identified in Logged Out response messages:', both currently empty. At the bottom right of the dialog box are 'Cancel' and 'OK' buttons.

Step 06: Verify the auto filled data as required

Step 07: Add User in User Section

Step 08: From login success response, set the logged out indicator

The screenshot shows the OWASP ZAP 2.9.0 interface. At the top, the menu bar includes Standard Mode, File, Edit, View, Analyse, Report, Tools, Import, Online, Help. Below the menu is a toolbar with icons for various functions. The main window has tabs for 'Sites' and 'IN TEN'. The 'Sites' tab is selected, showing a tree view of contexts and sites. Under the 'Default Context' site, there is a folder for 'http://localhost:8080/bodgeit'. Inside this folder, several files are listed: 'index.jsp', 'login.jsp', 'logout.jsp', 'register.jsp', and 'style.css'. To the right of the tree view is a 'Header: Text' and 'Body: Text' editor. A status message at the top right says 'Forced User Mode disabled - click to enable'. Below the editor is a preview pane showing a man's face. At the bottom of the interface is a table of network requests with columns for Id, Req. Timestamp, Method, URL, Code, Reason, RTT, Size Resp. Body, Highest Alert, Note, and Tags. The table lists 10 requests, including the ones listed in the tree view. The bottom status bar shows the URL 'localhost:8080/bodgeit/' and the status code '200'. The bottom right corner of the interface shows a timer 'ALL DAY' and other system status indicators.

Step 09: Enable Forced user mode

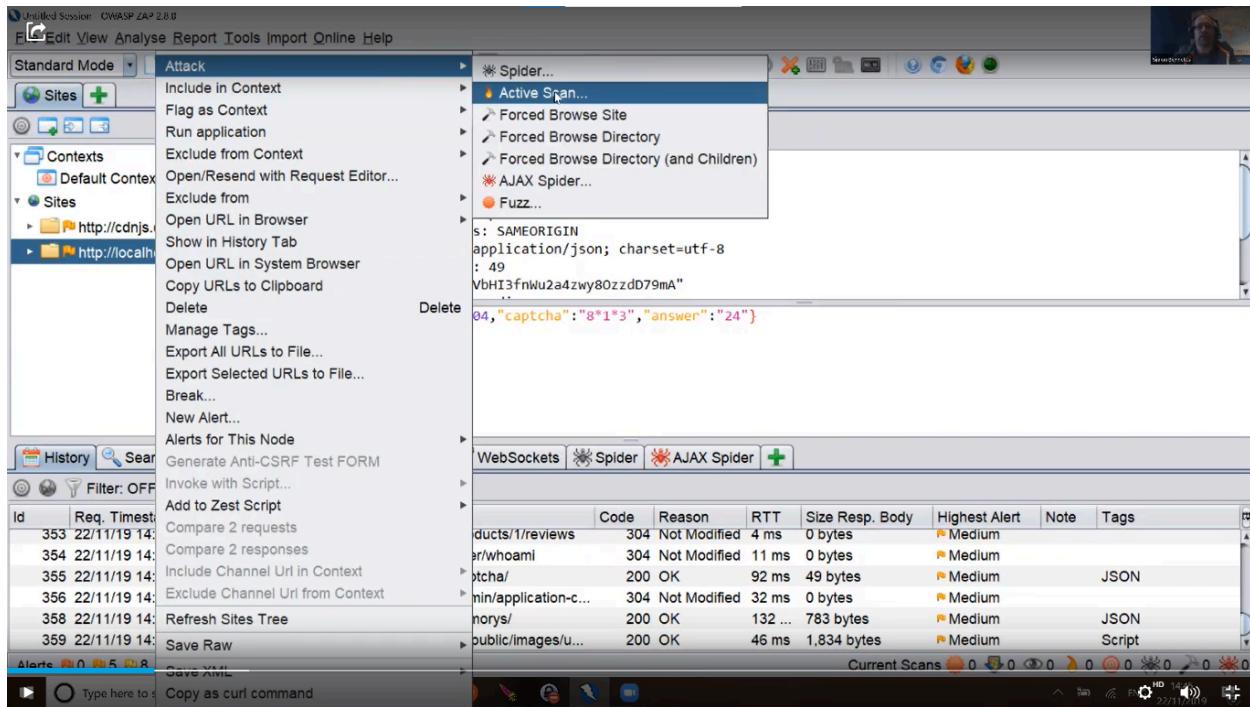
The screenshot shows a web browser displaying the 'The BodgeIt Store' homepage. The page features a logo with a lightning bolt and the text 'The BodgeIt Store'. It includes a navigation menu with links for Home, About Us, Contact Us, Logout, Your Basket, and Search. A 'Our Best Deals!' section displays a table of products:

Product	Type	Price
Doodahs	Doodahs	£6.50
Gizmos	Thingamajigs	£3.50
Thingies	Thingamajigs	£0.90
Whatchamacallits	Widgets	£1.20
Whatsits	Thingamajigs	£1.40
Widgets	Whatchamacallits	£3.74
Widgets	Whatsits	£3.95
Widgets	Thingies	£3.30
Widgets	Thingies	£3.20
TGJ JJJ	Thingamajigs	£0.80

In the status bar at the bottom, it shows the URL 'localhost:8080/bodgeit/login.jsp' and the status code '200'. The bottom right corner of the browser window shows a timer 'ALL DAY' and other system status indicators.

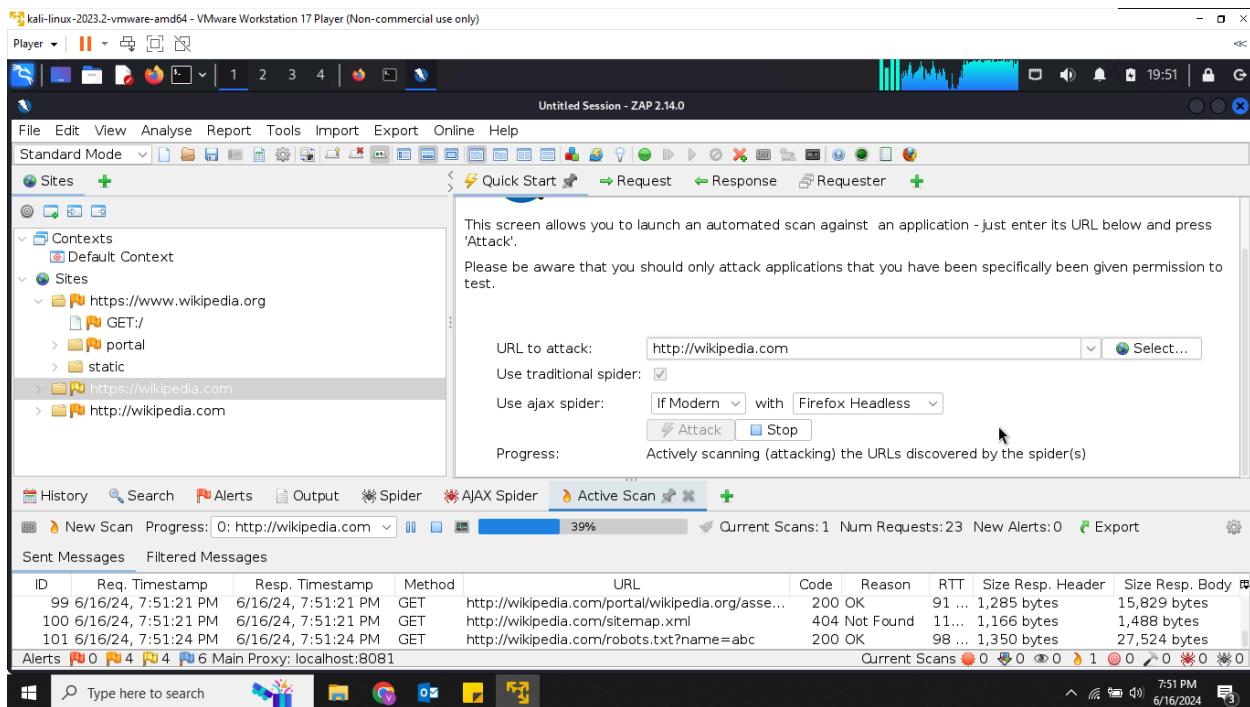
Step 10: Open the login request in the browser and verify automatic login

To Run the scan:

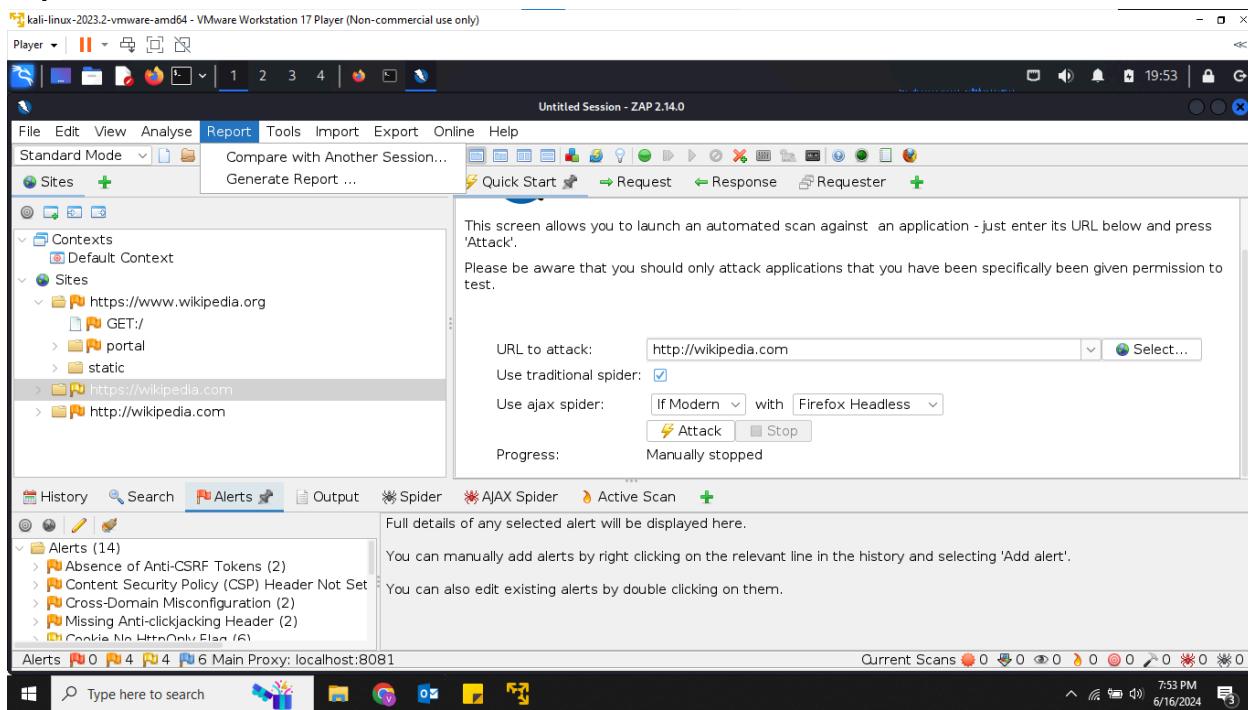


Step 01: Choose Site from the Sites > Attack > Active Scan

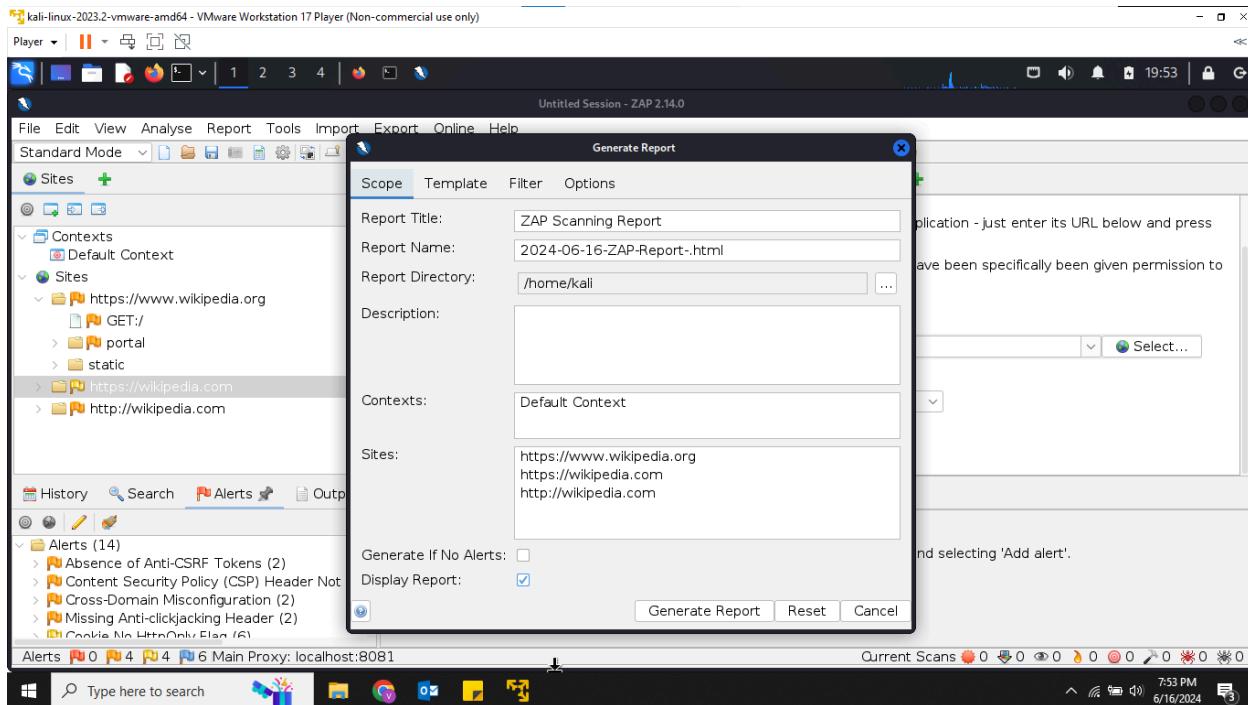
Scan In Progress:



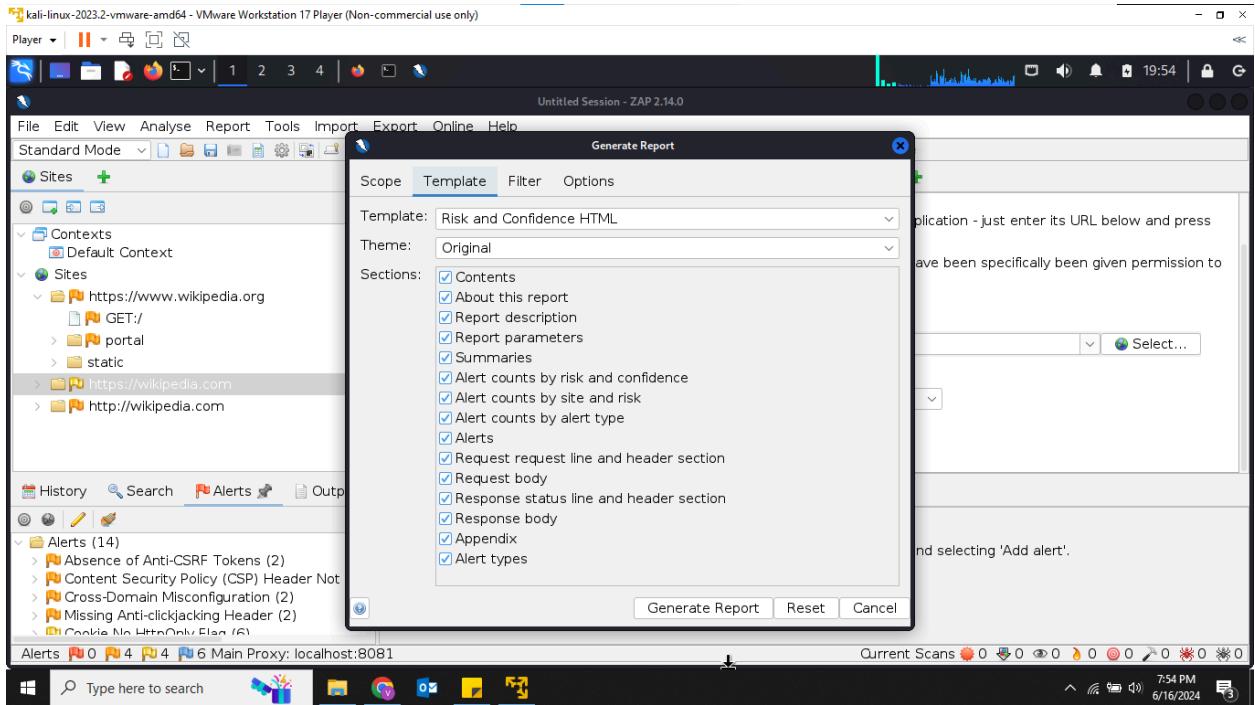
Report Generation:



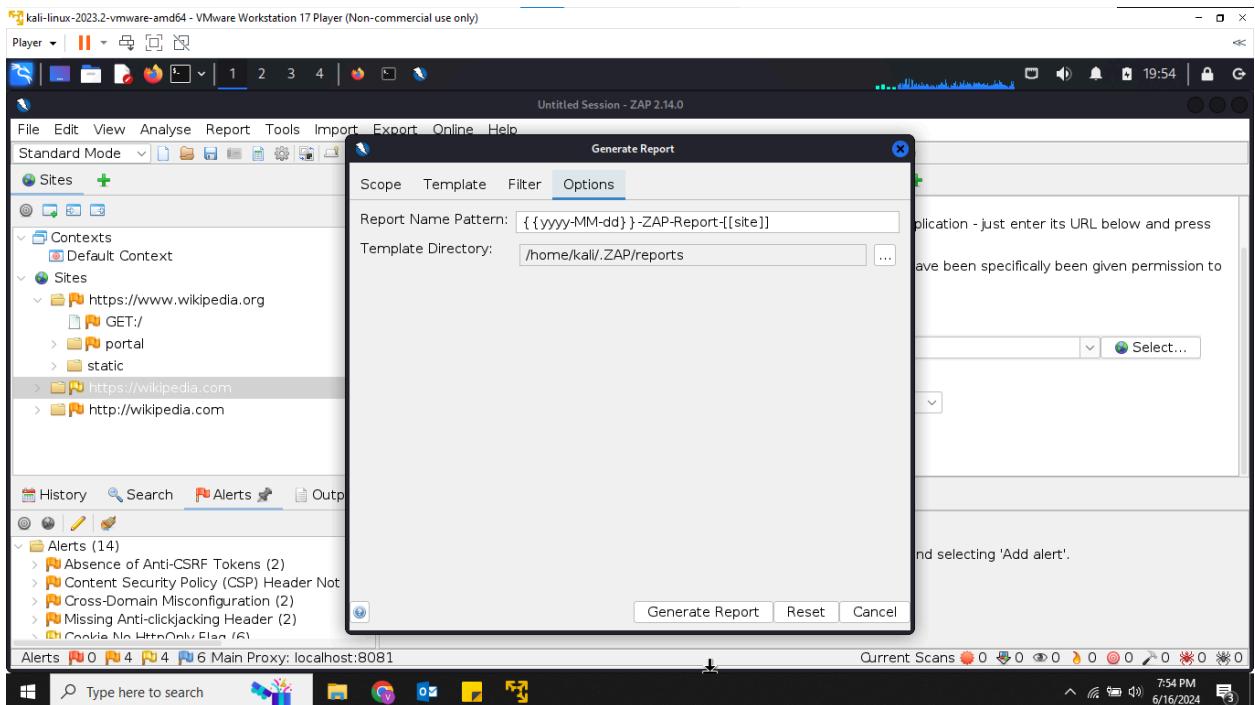
Step 01: Report >> Generate Report



Step 02: Choose the Scope



Step 03: Configure the template



Step 04: Generate the Report