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.

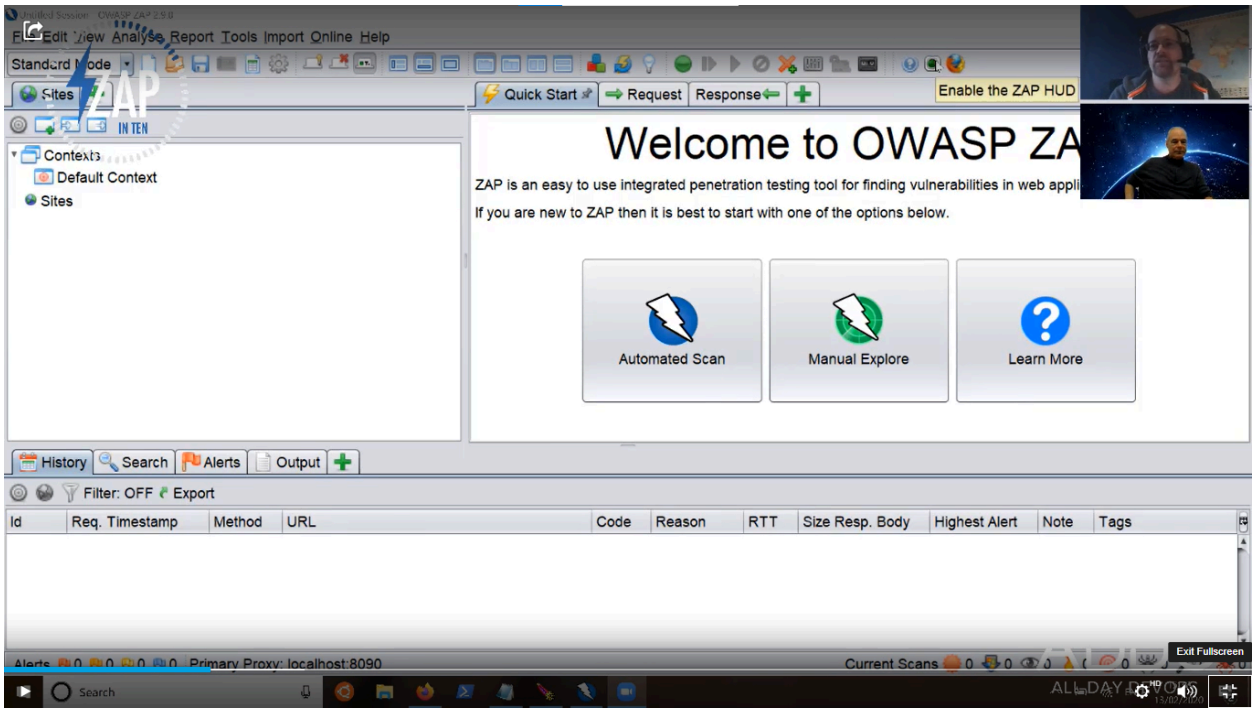
Community Insights from PeerSpot:

https://drive.google.com/file/d/1gMpmOp77HW_iIfF3EZbRtpYpD96tdo2l/view?usp=sharing

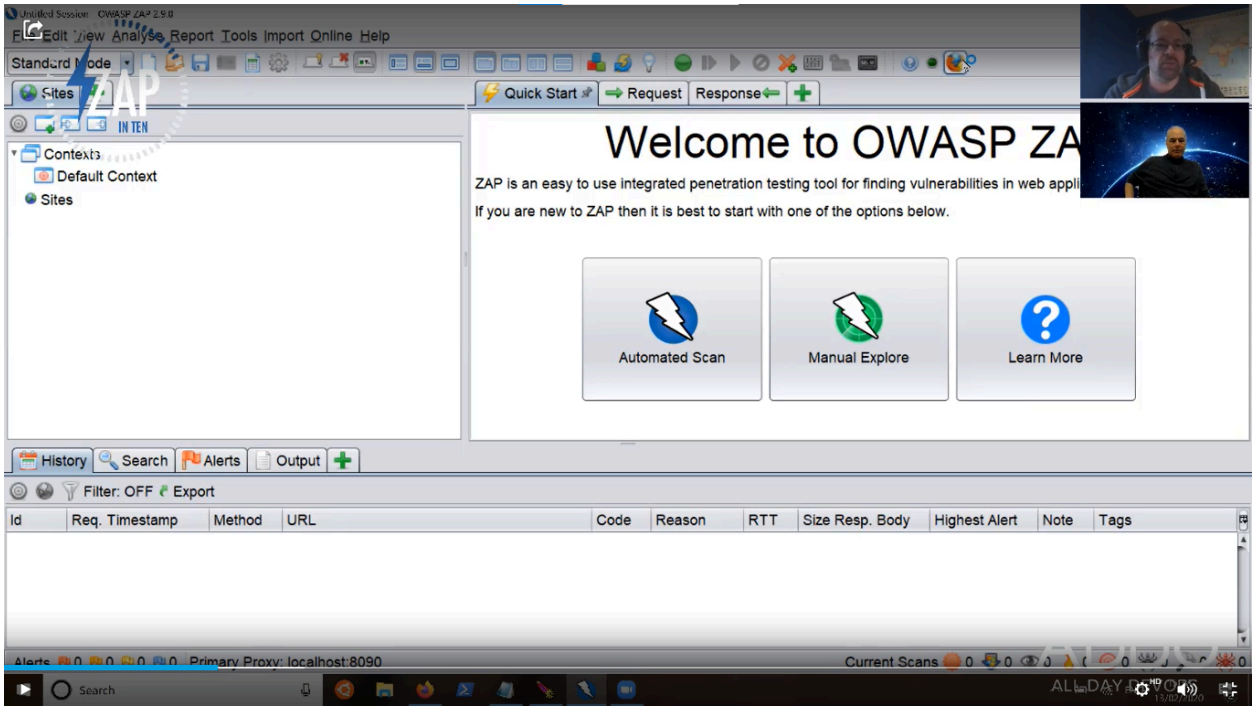
Step by step Procedure:

Initialization:

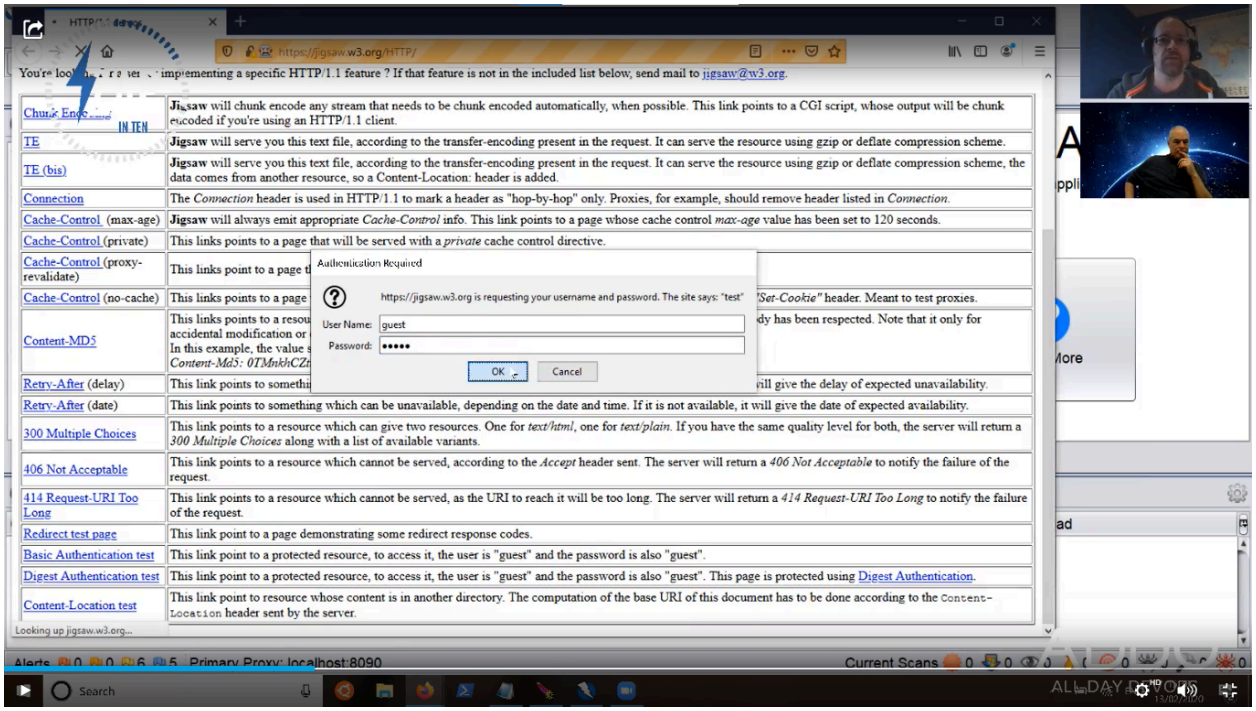
Method I: Enabling HTTP Automatic Authentication



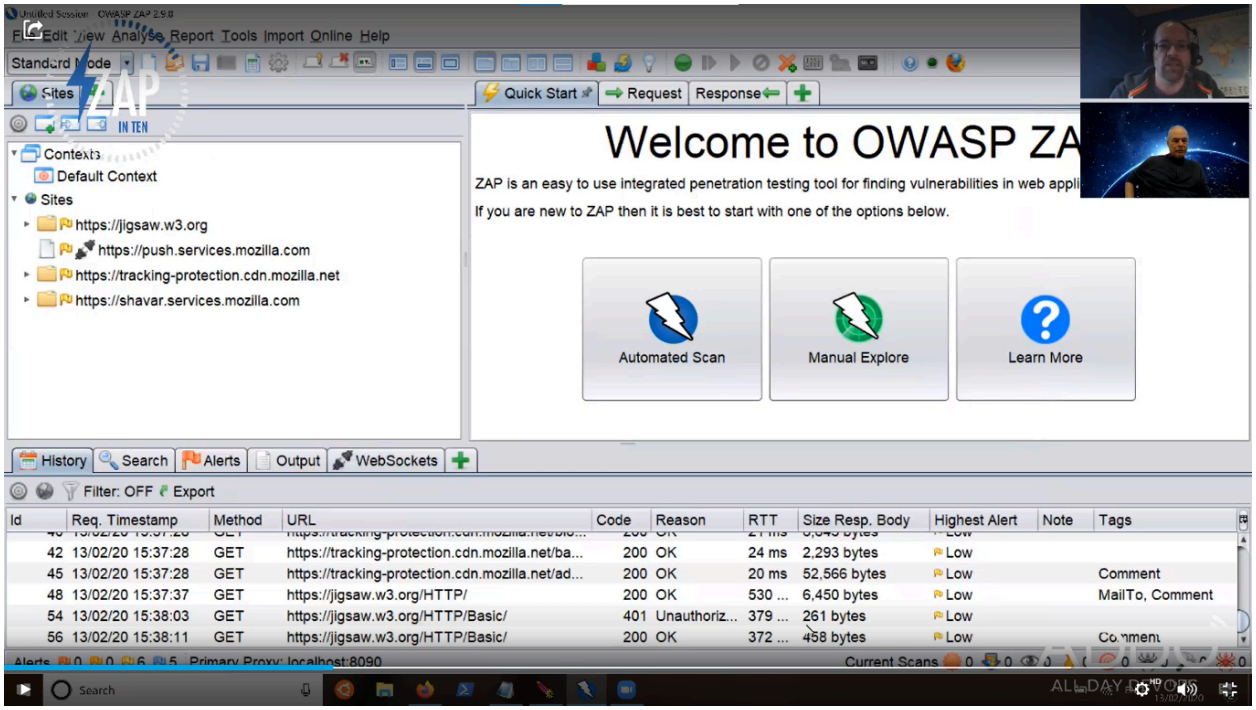
Step 01: Disable ZAP HUD



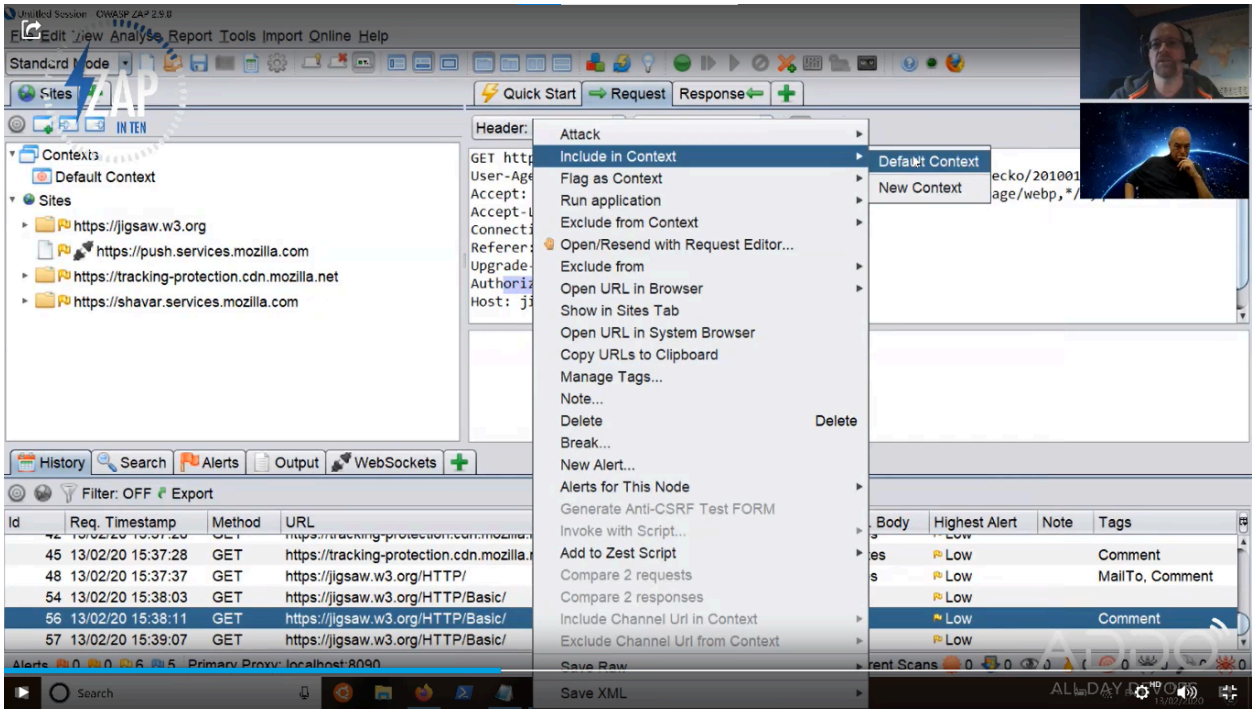
Step 02: Launch Firefox



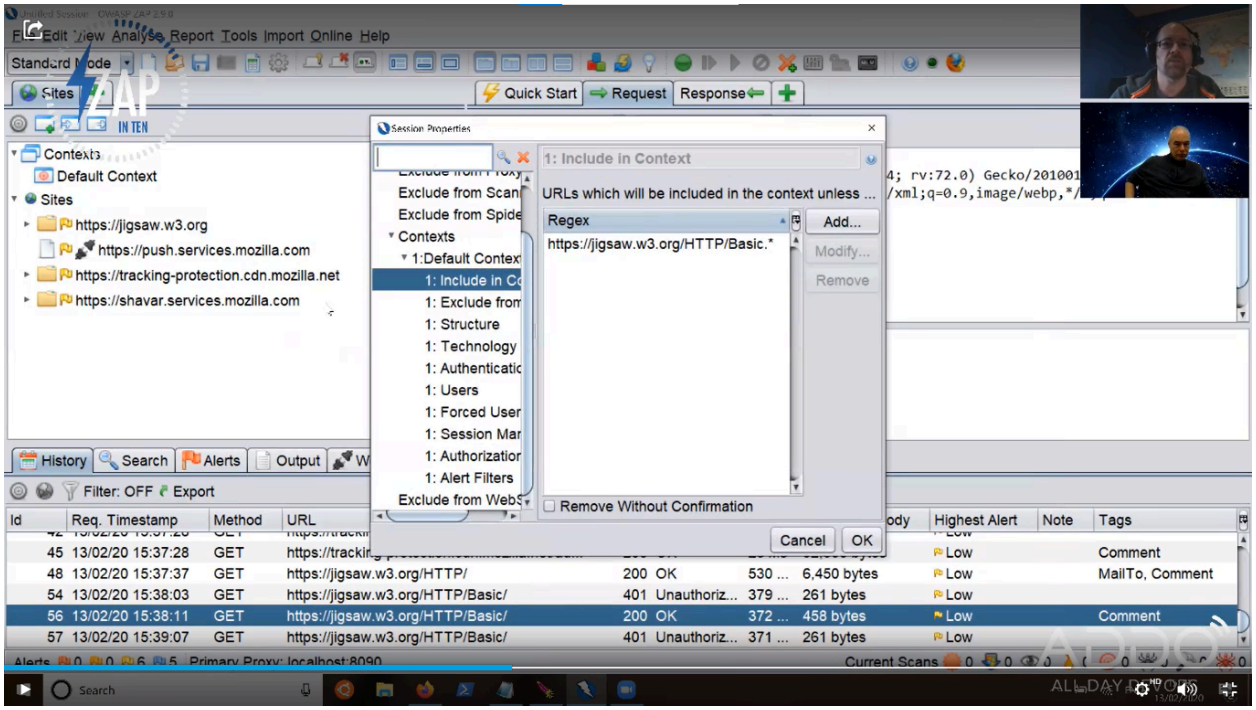
Step 03: Log in to the Site



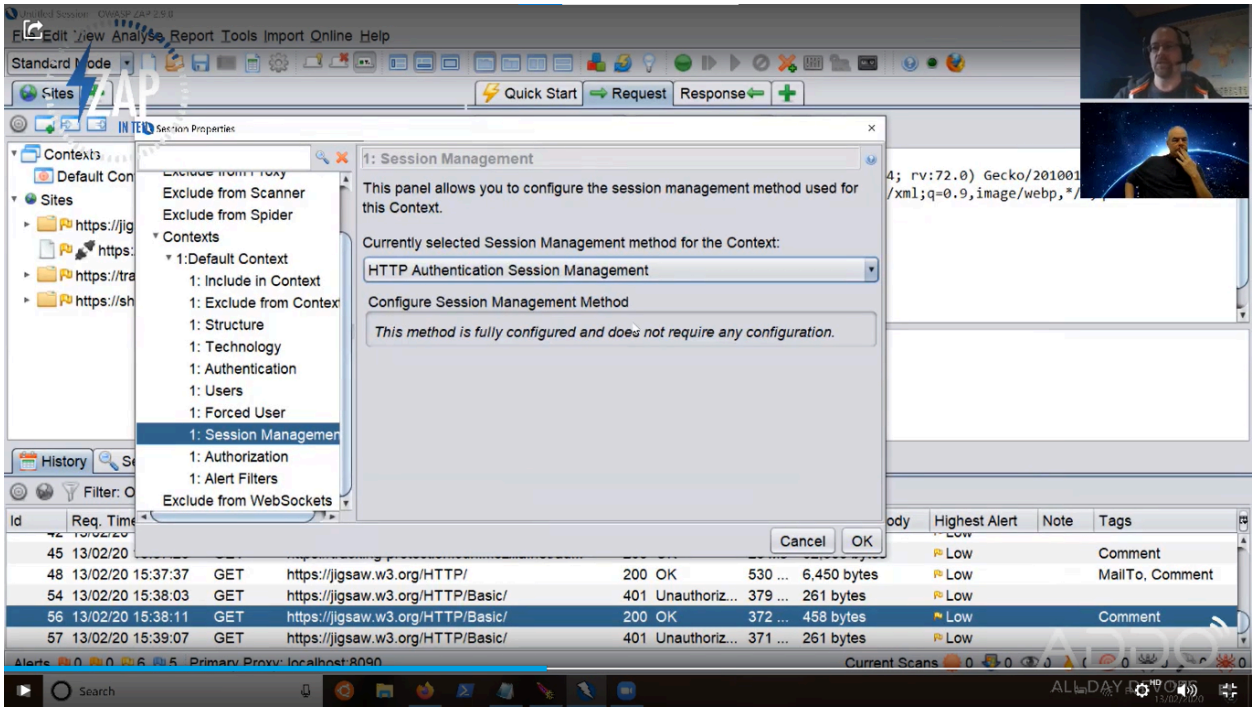
Step 04: Go back to ZAP and In History, Find the Auth Request



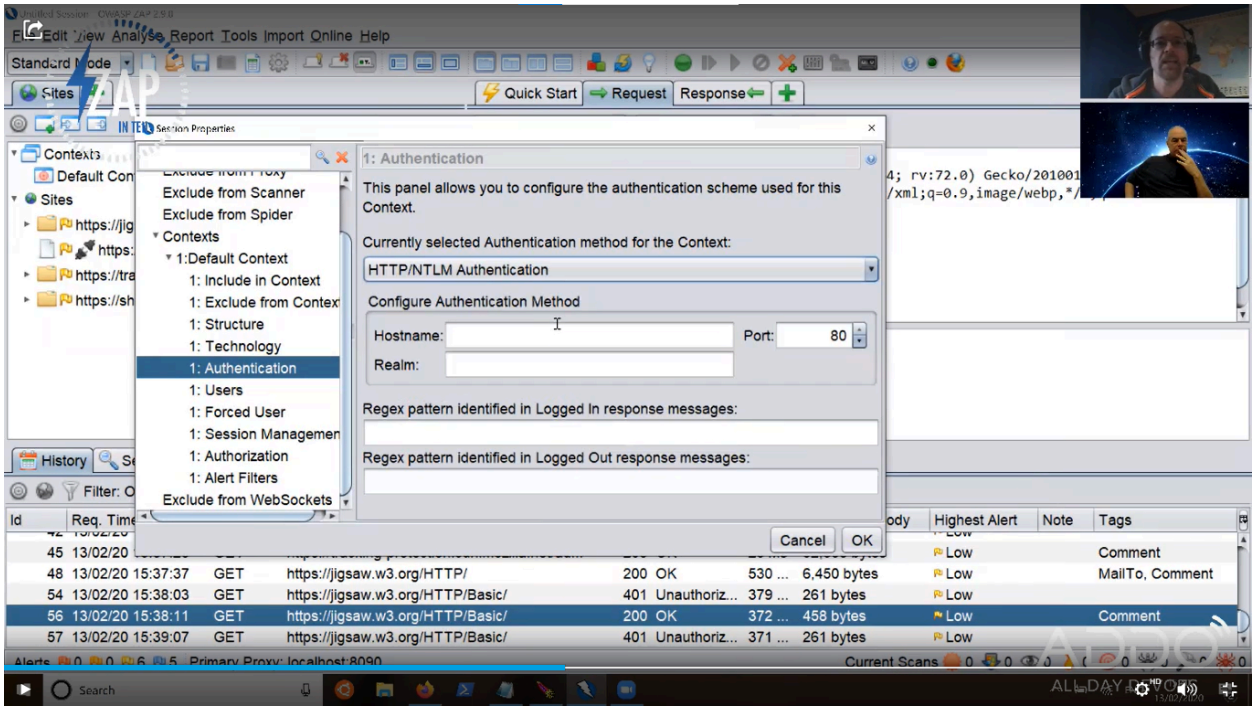
Step 05: Right Click > Include in Context > Default Context



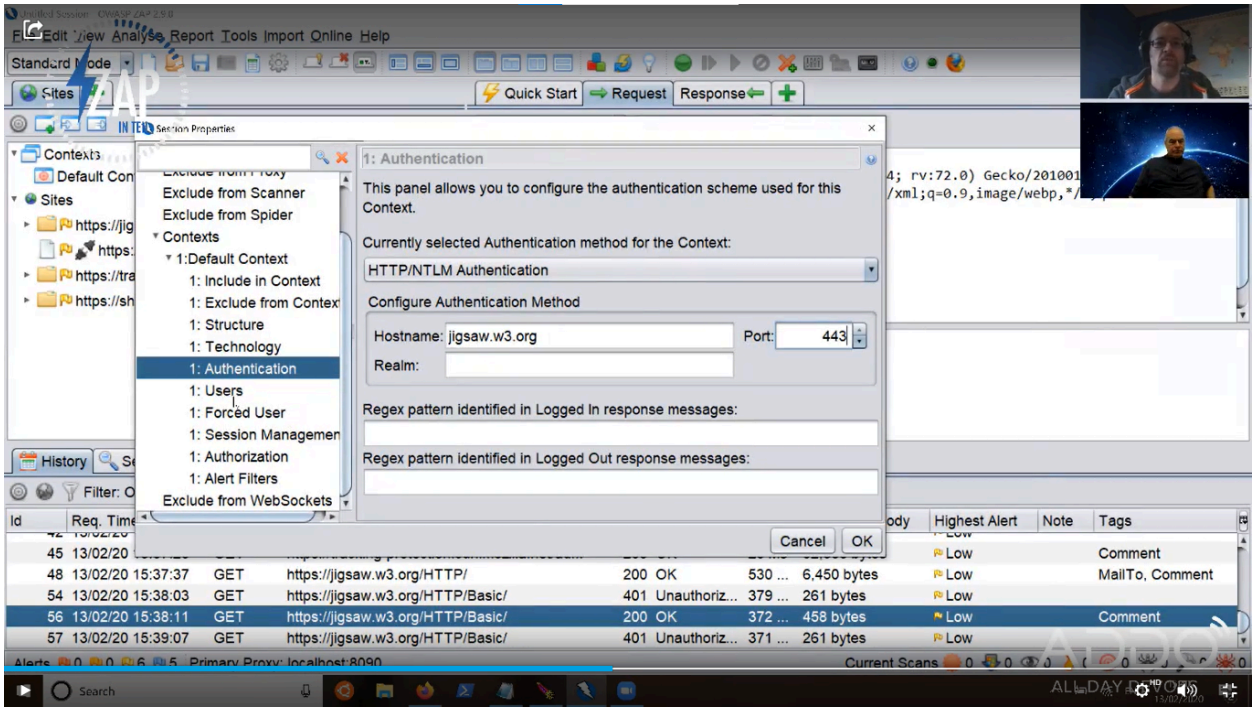
Step 06: Check the URL as a Regex in Include in Context Section



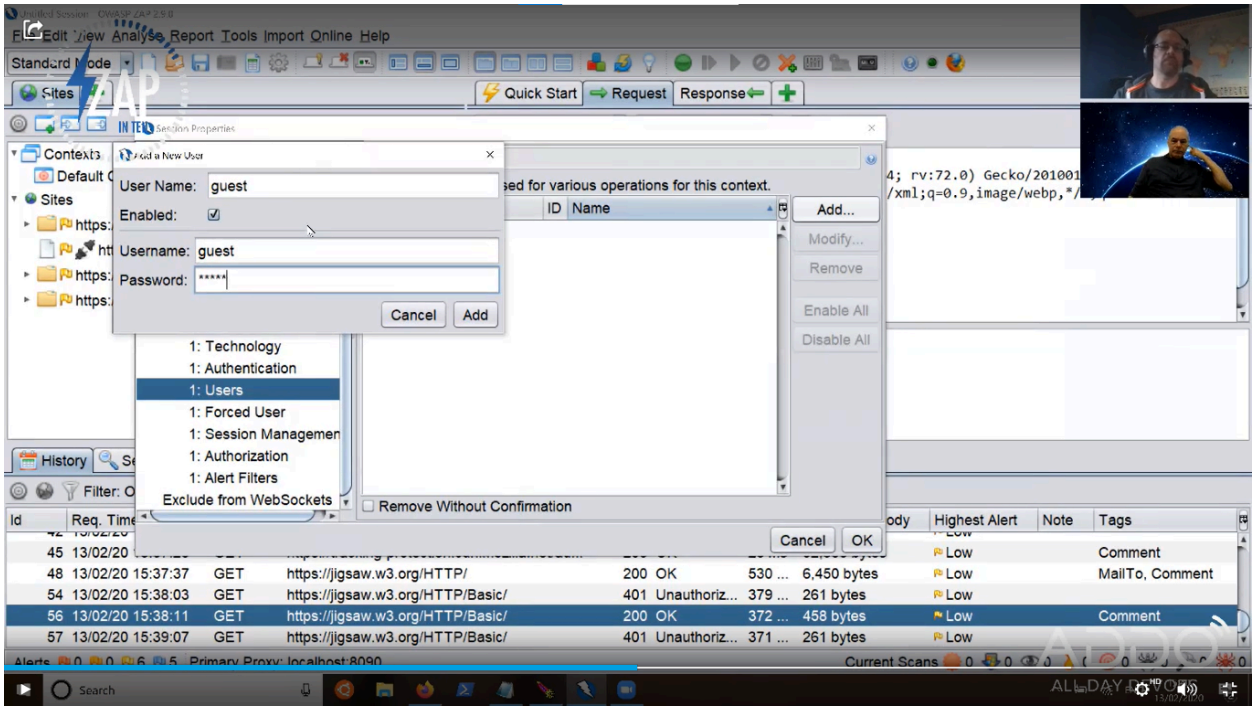
Step 07: Change the Session Mgt as HTTP Auth Session Mgt



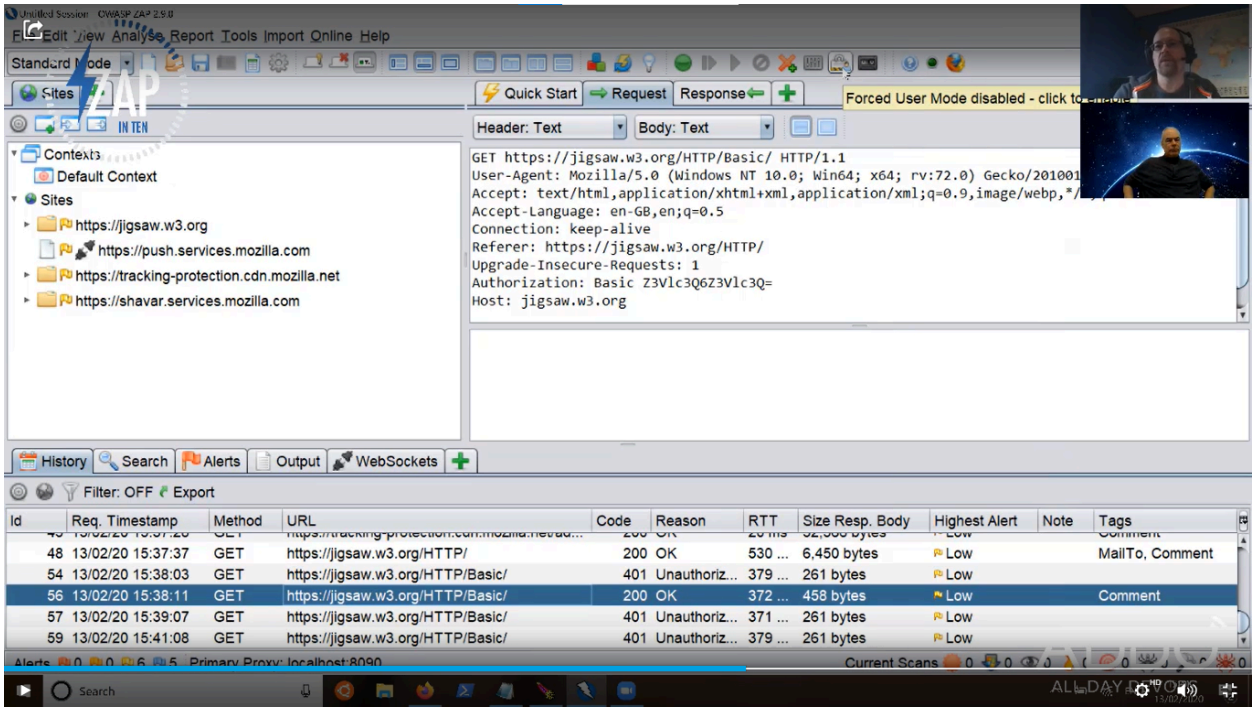
Step 08: Choose Authentication Method as HTTP/NTLM Authentication



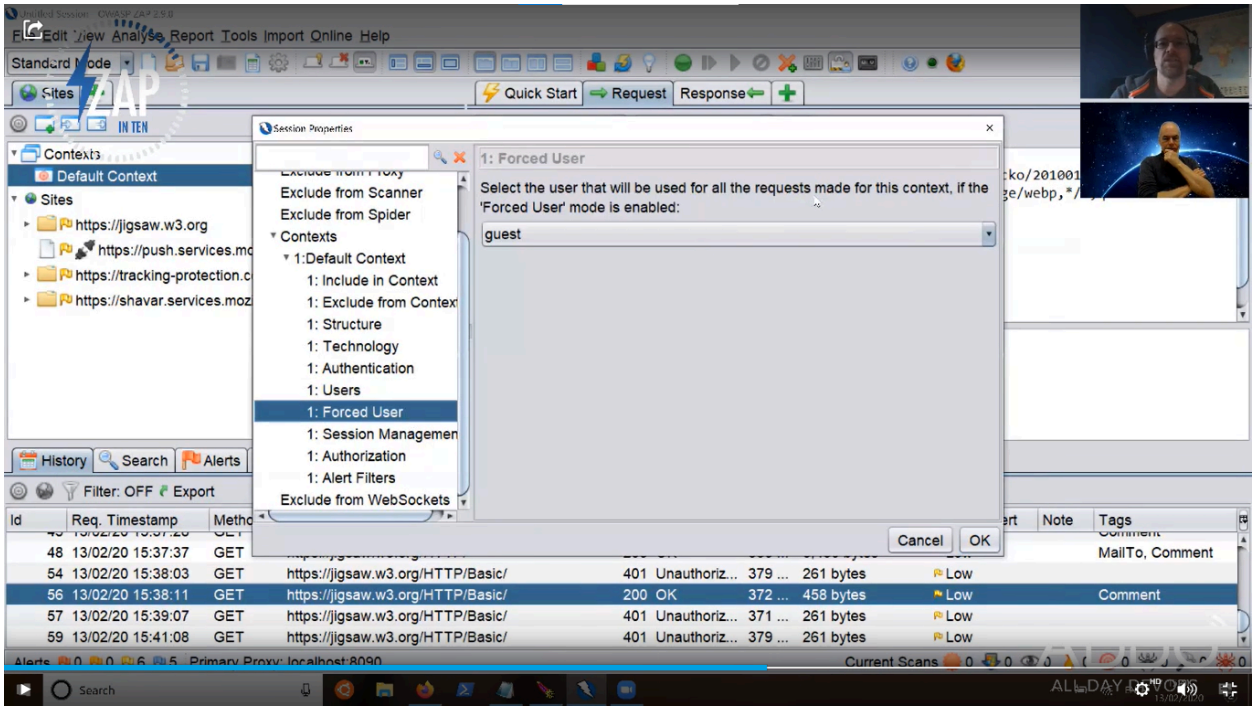
Step 09: Configure Hostname and Port Number



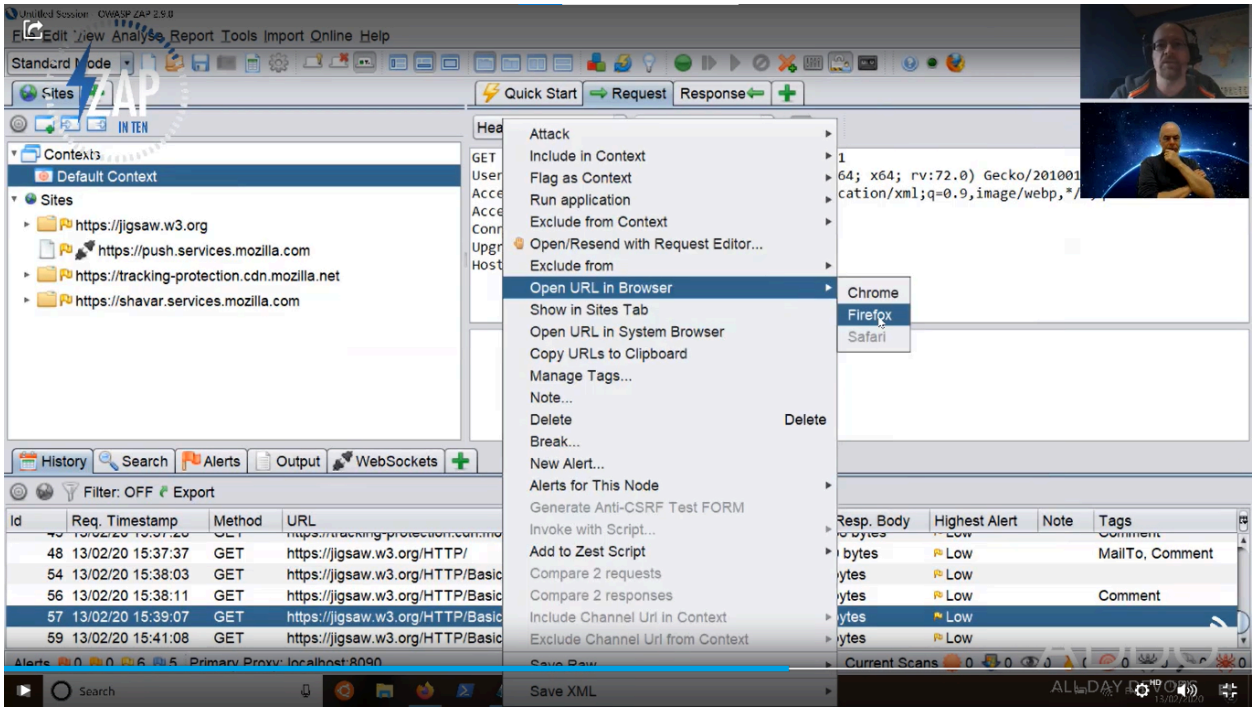
Step 10: Add the user in User Section



Step 11: Enable Forced User Mode

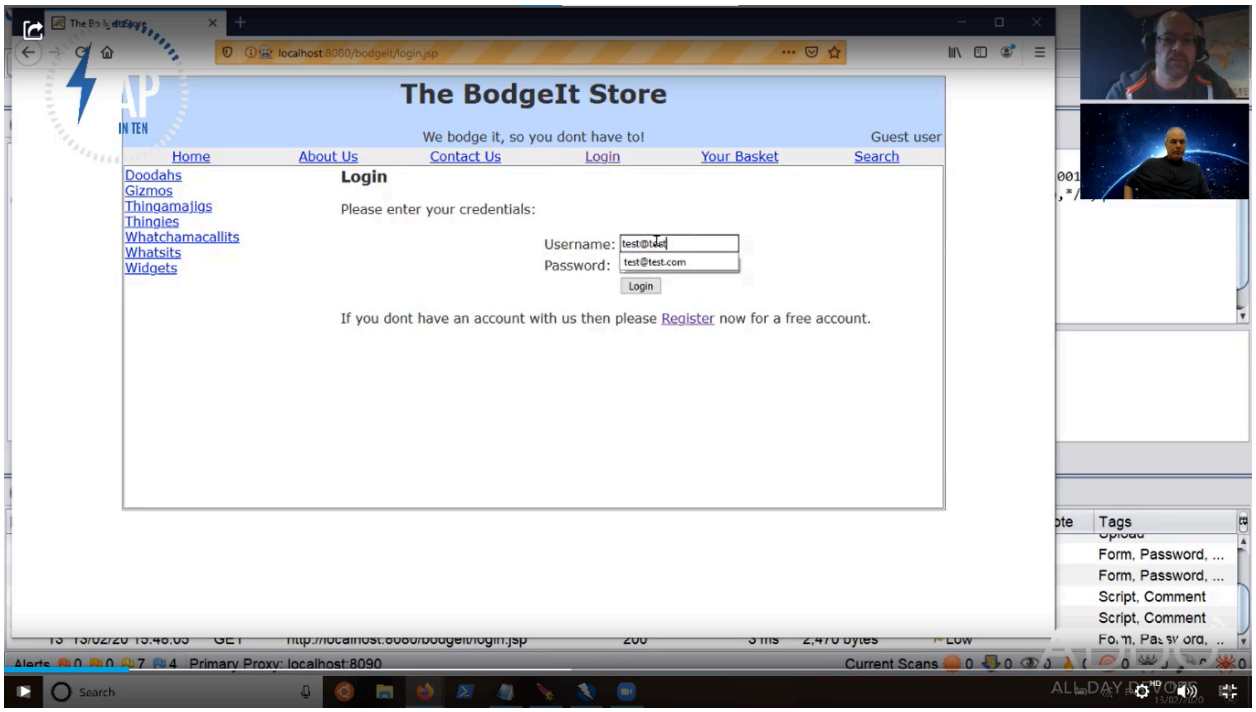


Step 12: Choose the Forced User as the User entered

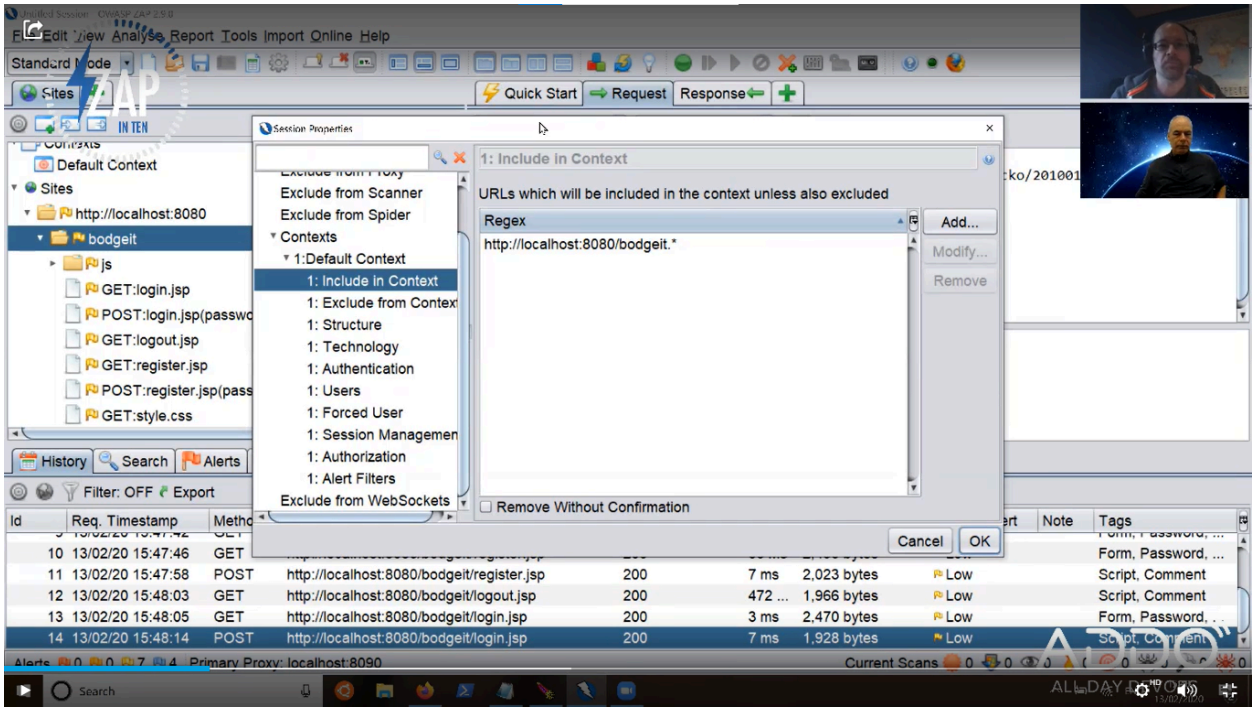


Step 13: Open the request from the browser and verify automatic authentication

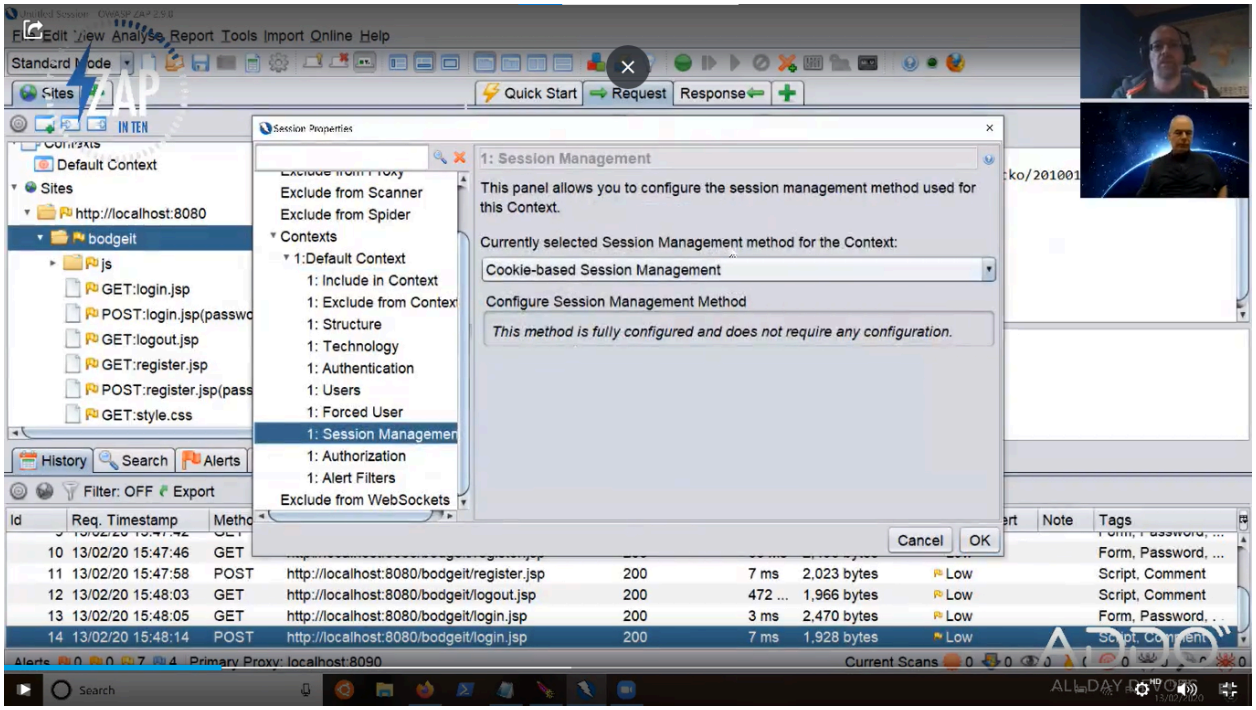
Method II) Enabling Automatic Form based Authentication



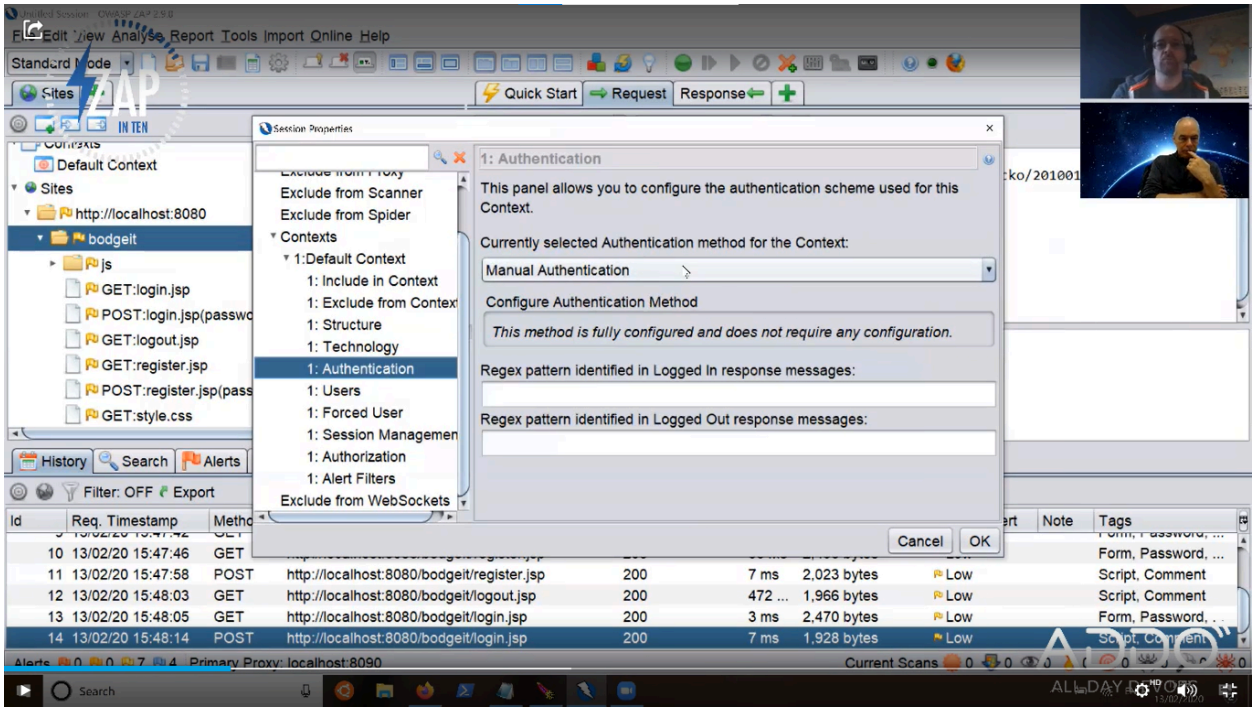
Step 01: Access the login using ZAP through Firefox



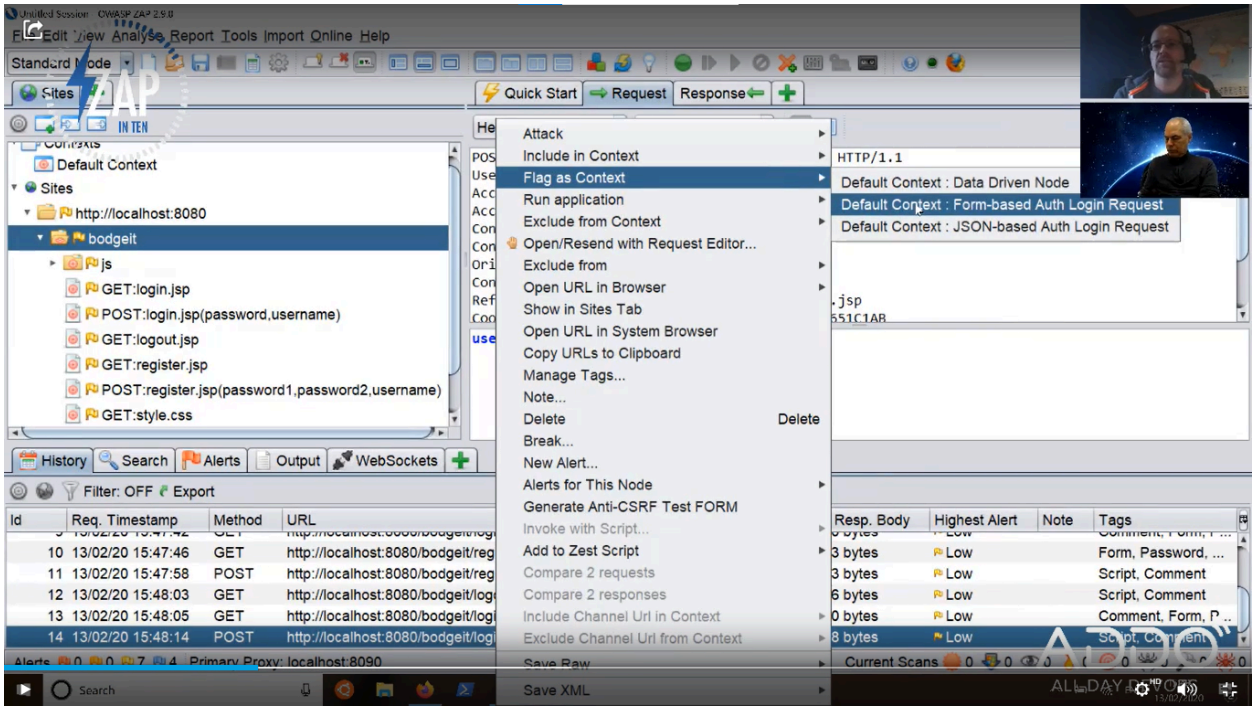
Step 02: Access site from sitemap and include in context and verify the URL



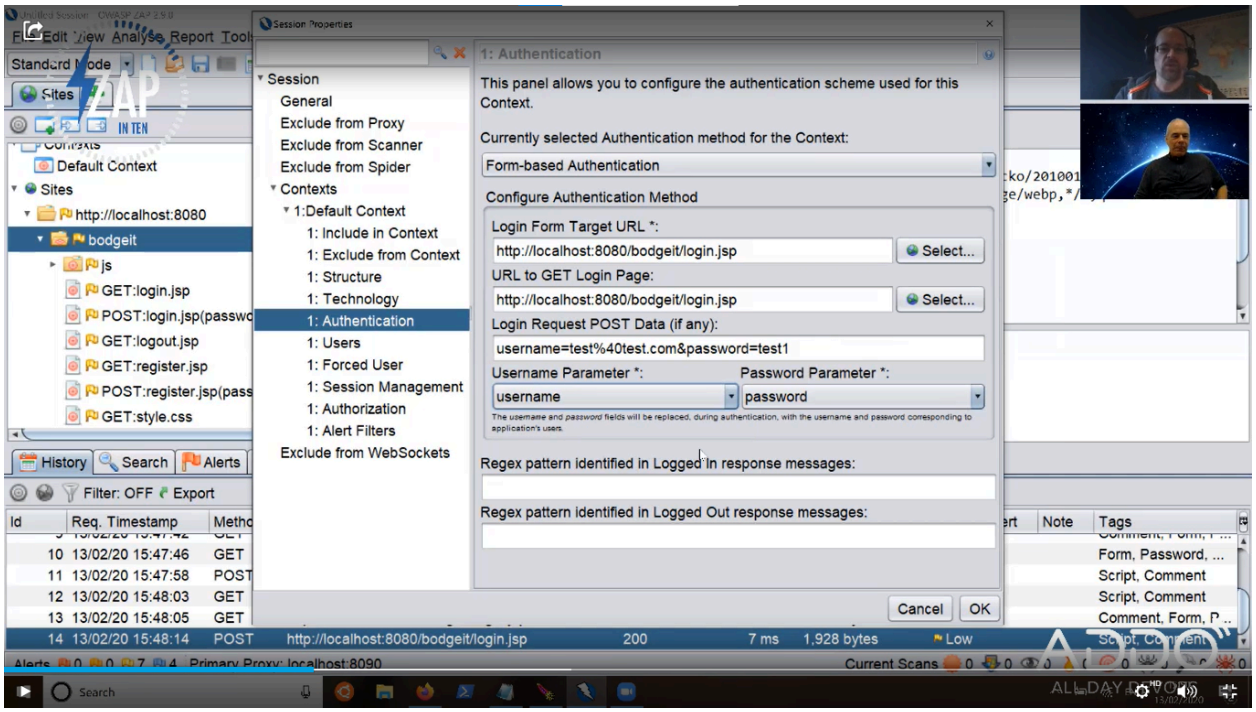
Step 03: Set session mgt as Cookie based session mgt



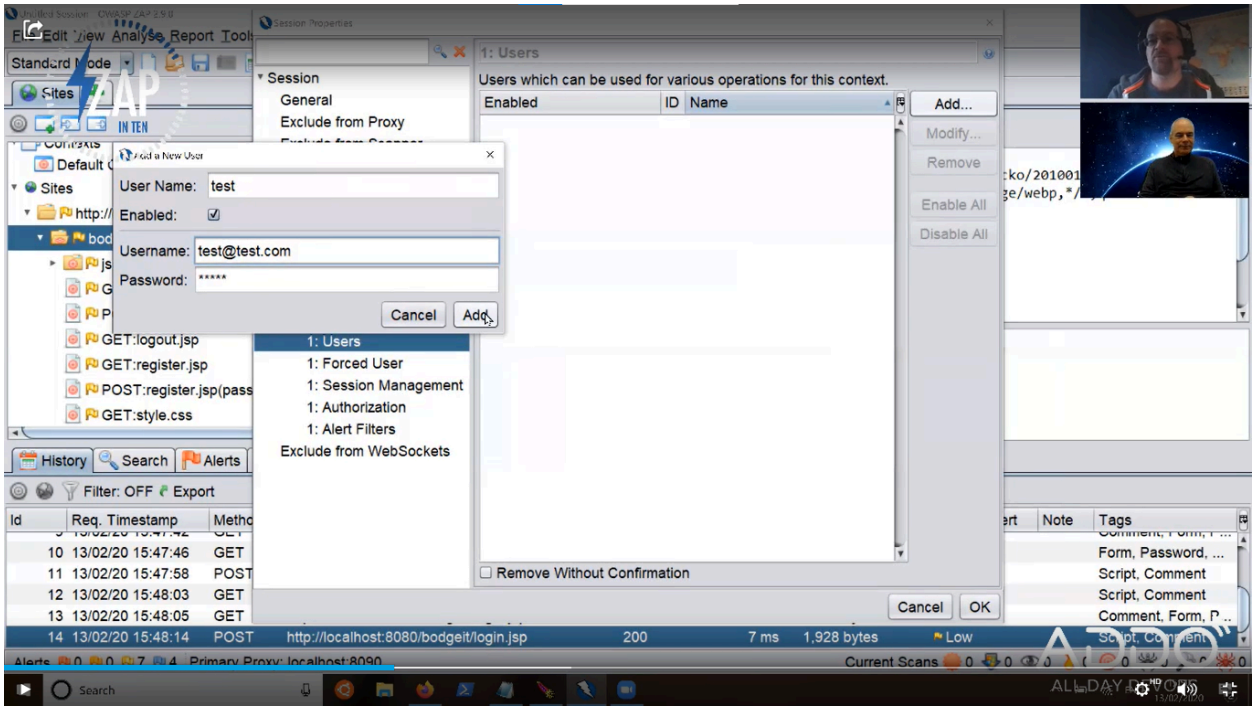
Step 04: Choose authentication mode as manual authentication



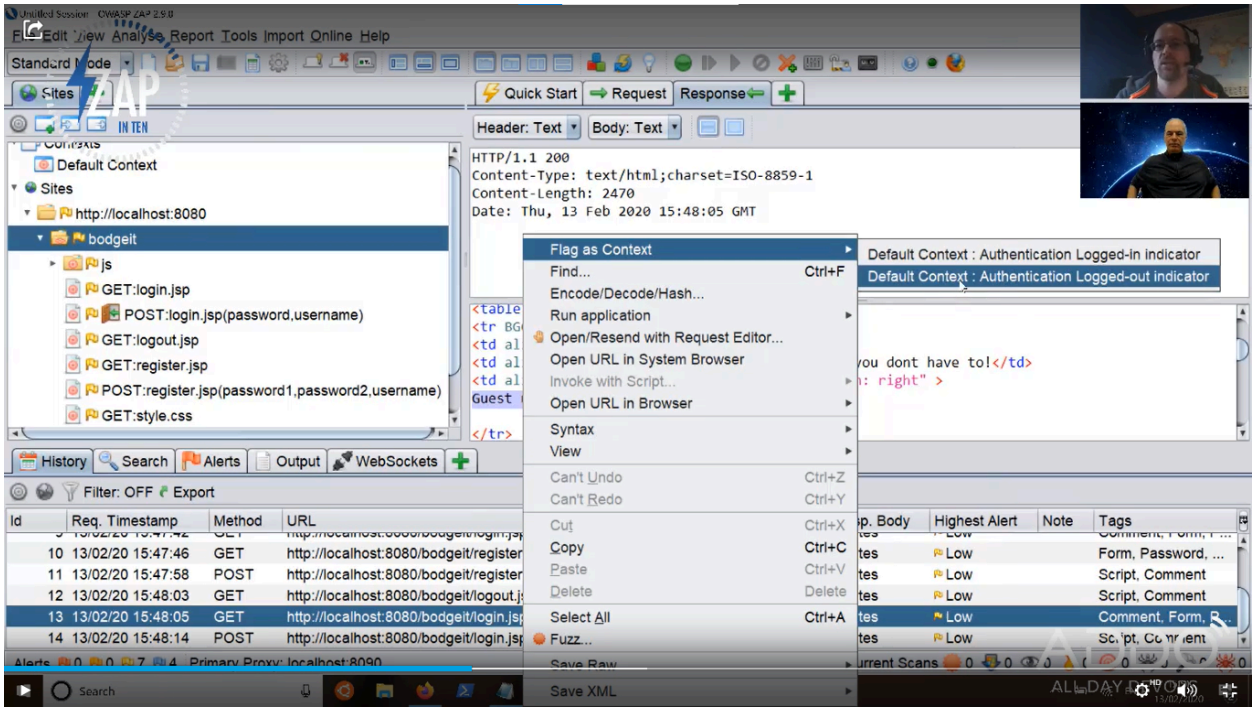
Step 05: Choose the Auth POST request from the history and set it as Default context: Form based Auth Login Request



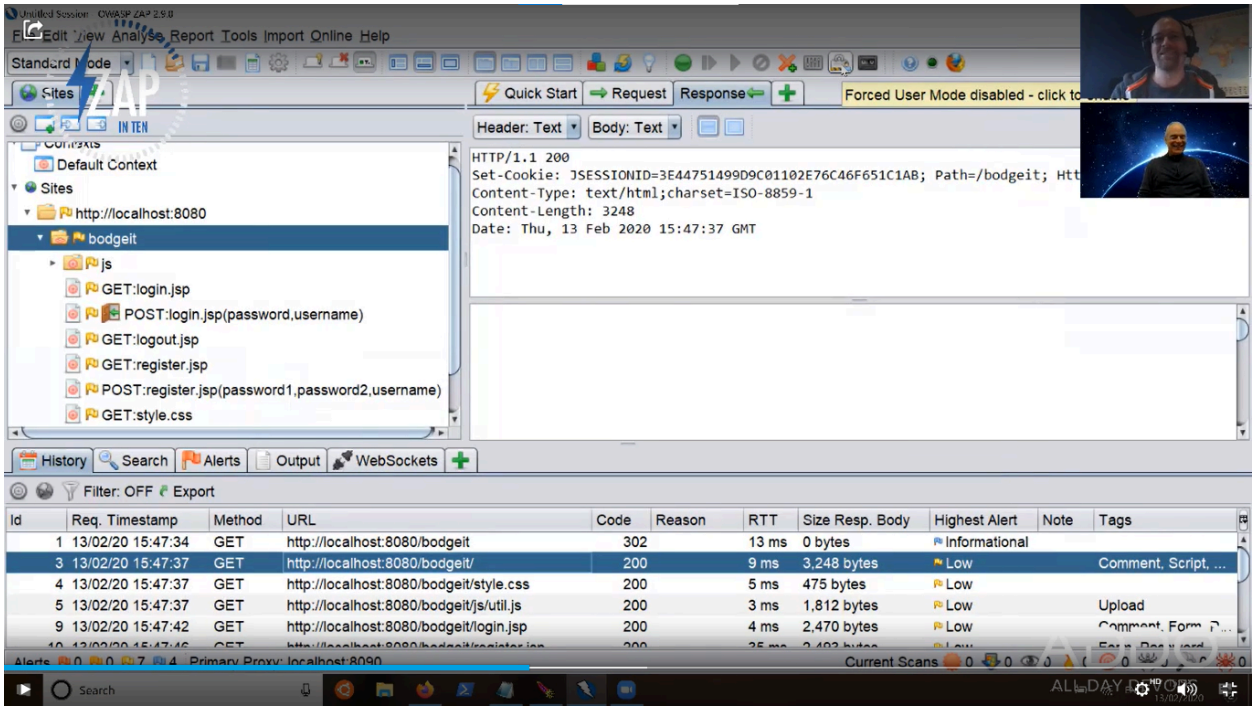
Step 06: Verify the auto filled data as required



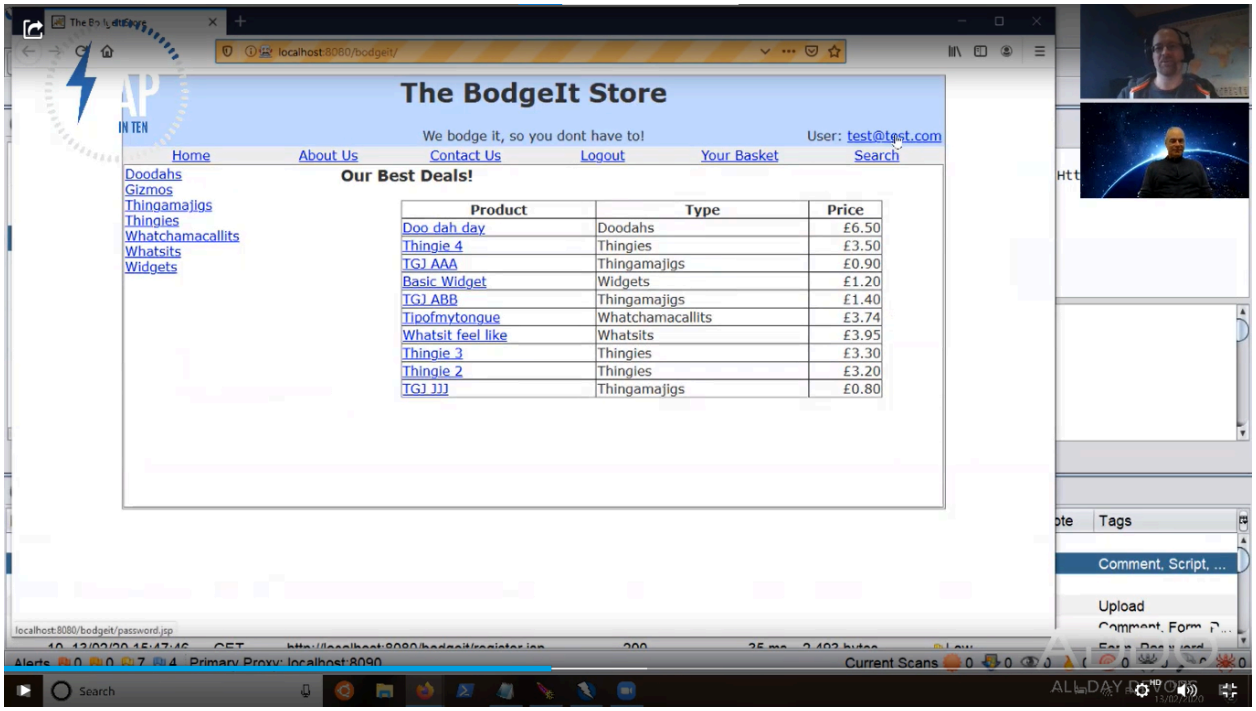
Step 07: Add User in User Section



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

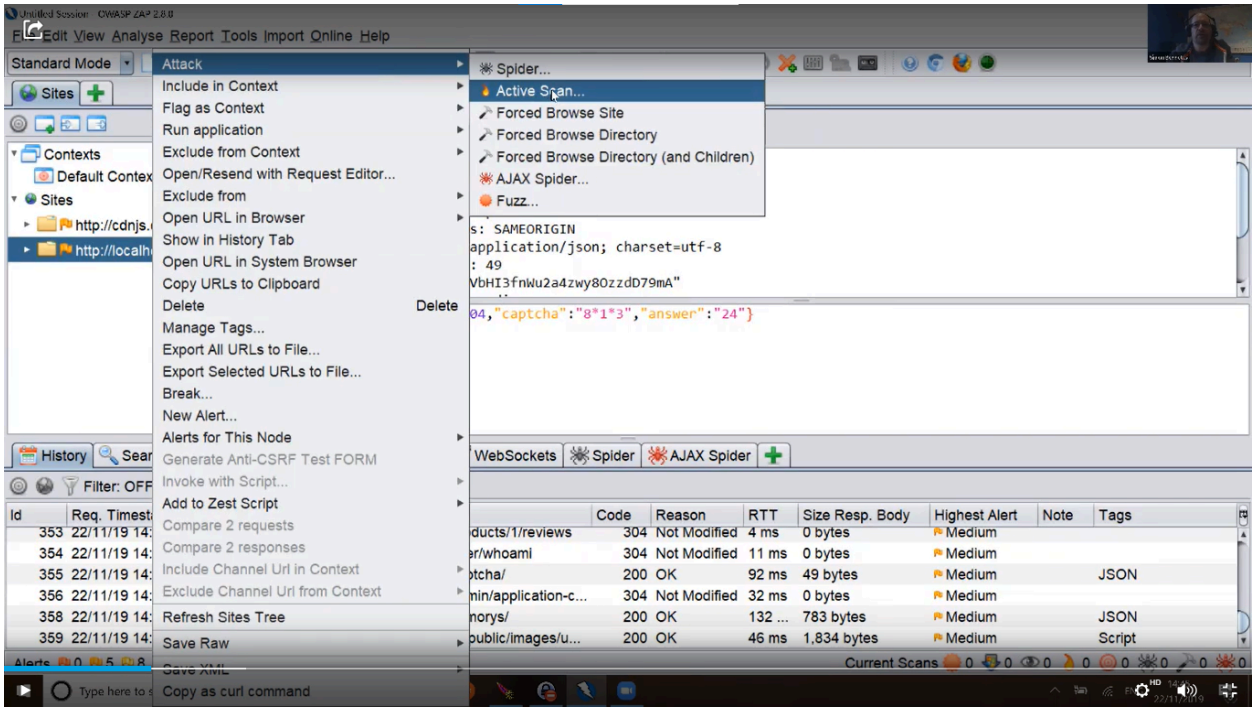


Step 09: Enable Forced user mode



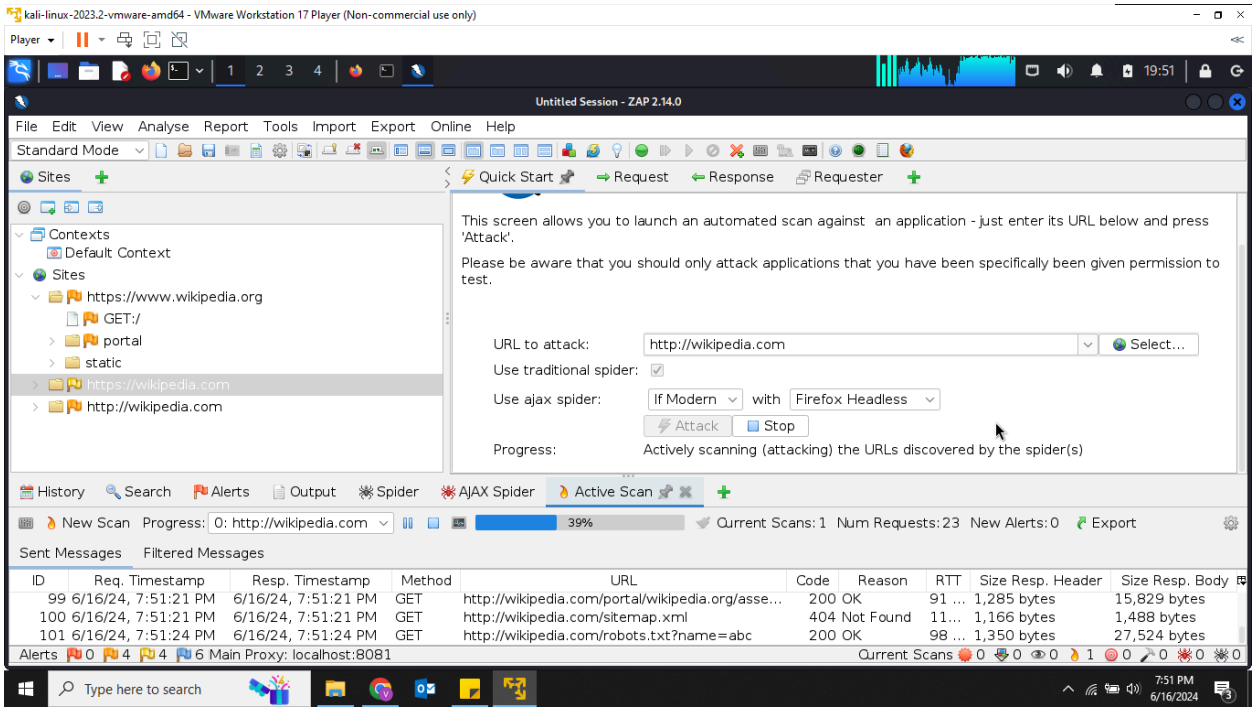
Step 10: Open the login request in the browser and verify automatic login

To Run the scan:

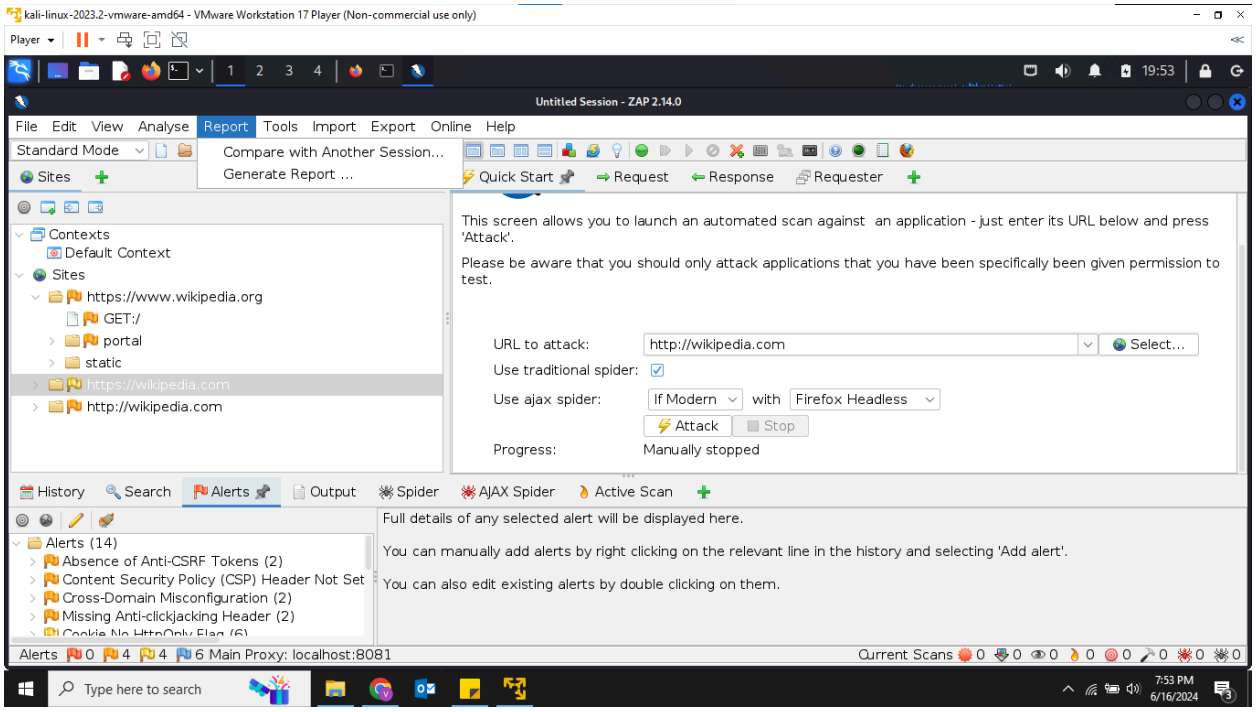


Step 01: Choose Site from the Sites > Attack > Active Scan

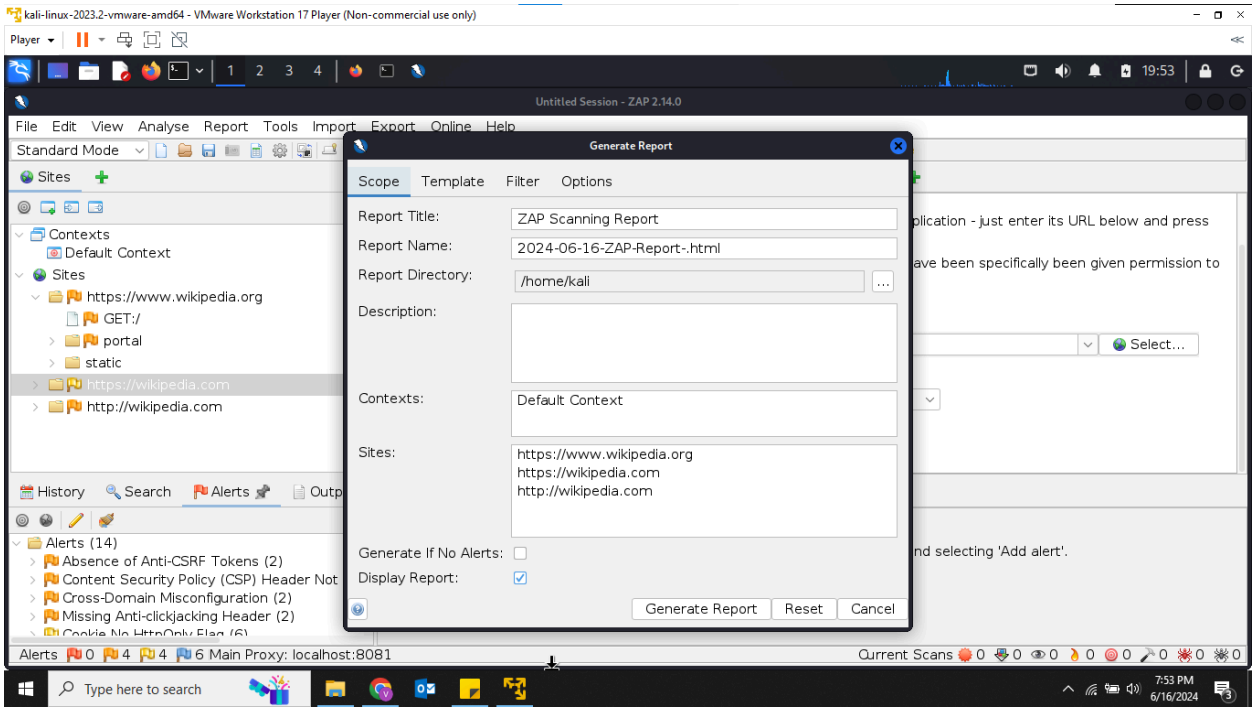
Scan In Progress:



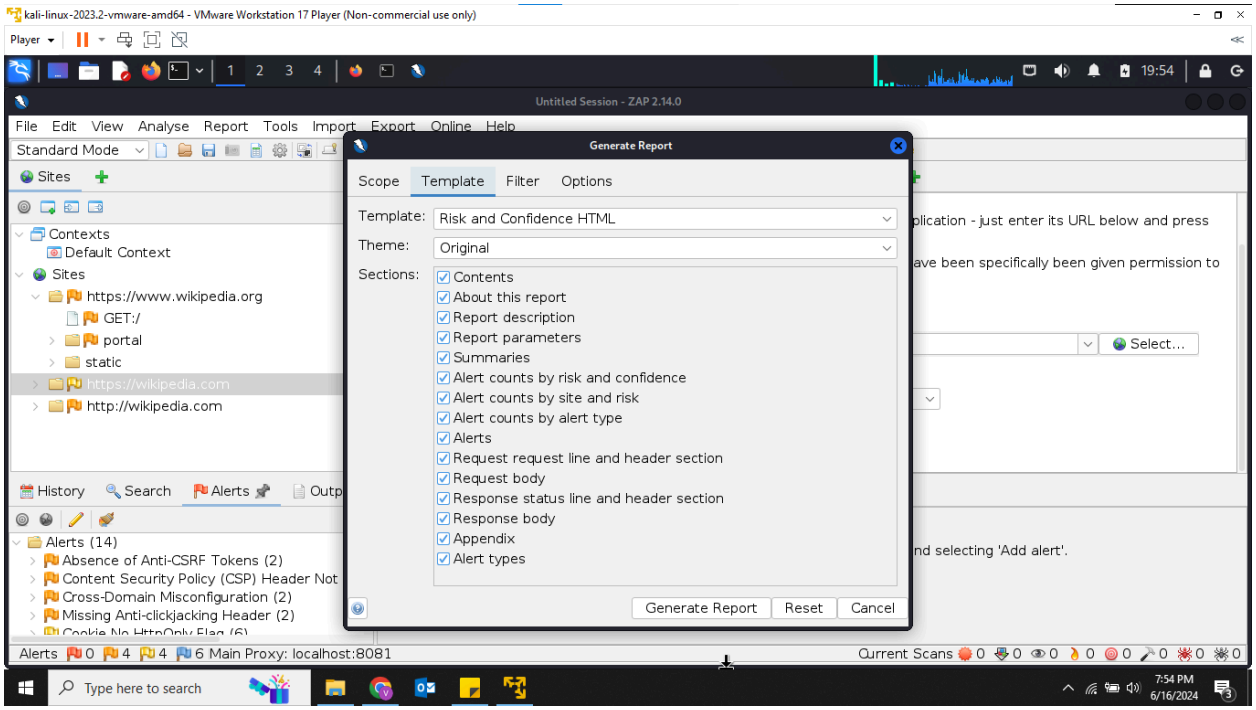
Report Generation:



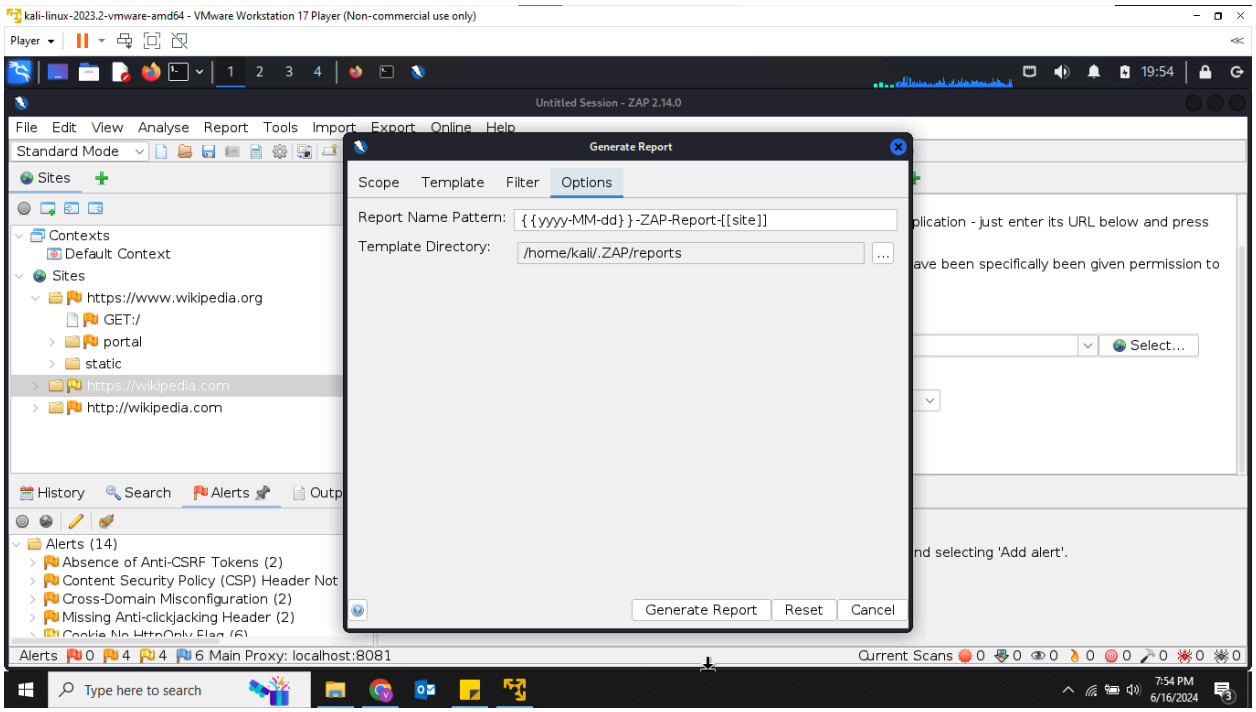
Step 01: Report >> Generate Report



Step 02: Choose the Scope



Step 03: Configure the template



Step 04: Generate the Report