SOP of using Burp Scanner, HCL App Scan and OWASP ZAP for Web Application Vulnerability Assessment

I) Burp Scanner

Burp Suite's vulnerability scanner, a key component of Burp Suite Professional, stands out for its ability to detect a wide array of web application vulnerabilities.

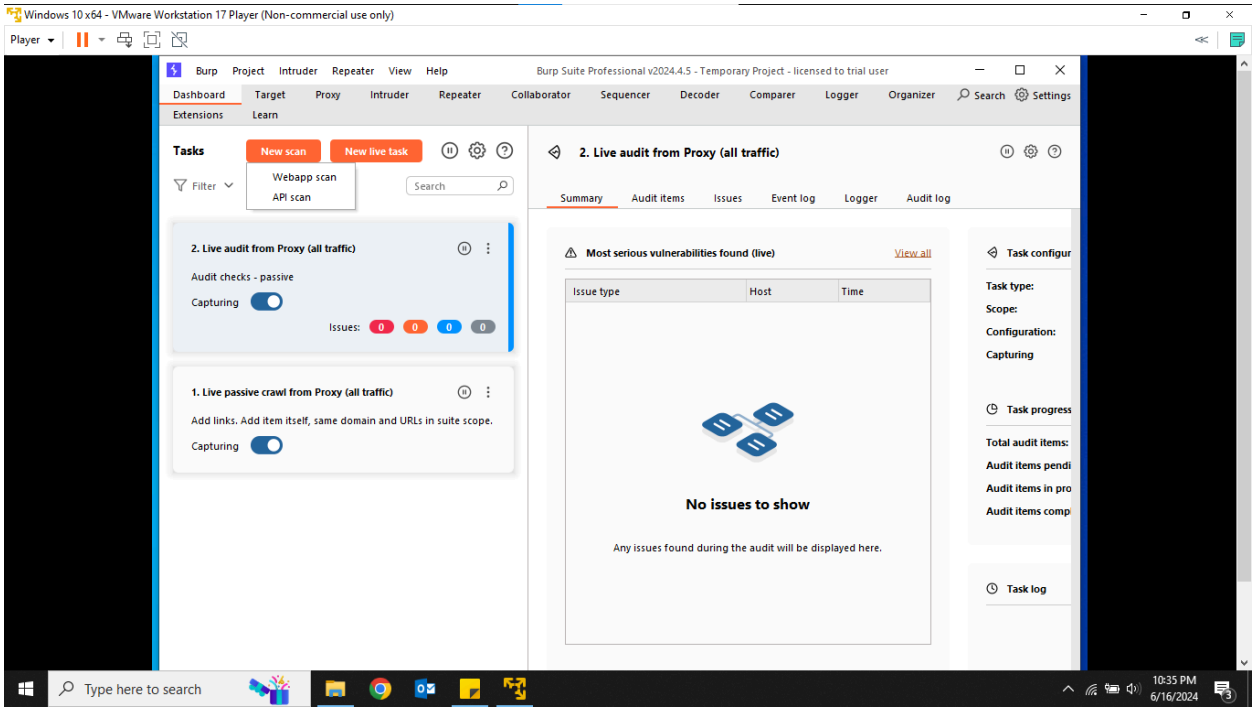
Its advanced crawl engine, embedded Chromium browser, and innovative OAST technology allow it to handle modern web applications with ease. With regular updates and a focus on the latest vulnerabilities, Burp Suite's scanner is a robust solution for both individual penetration testers and extensive security teams.

Community Insights from Gartner:

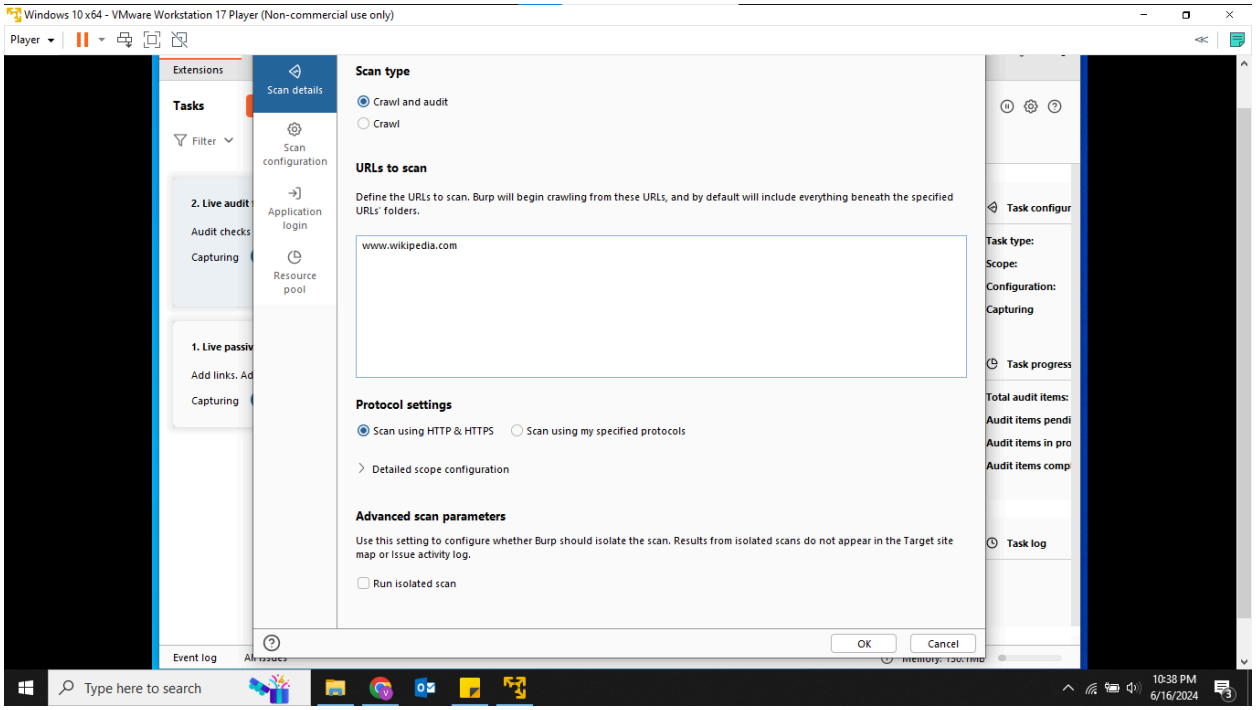
https://drive.google.com/file/d/11l4cfhmKYn_RwxcAiiQw7Hao2d8gd5La/view?usp=sharing

Step by Step Procedure:

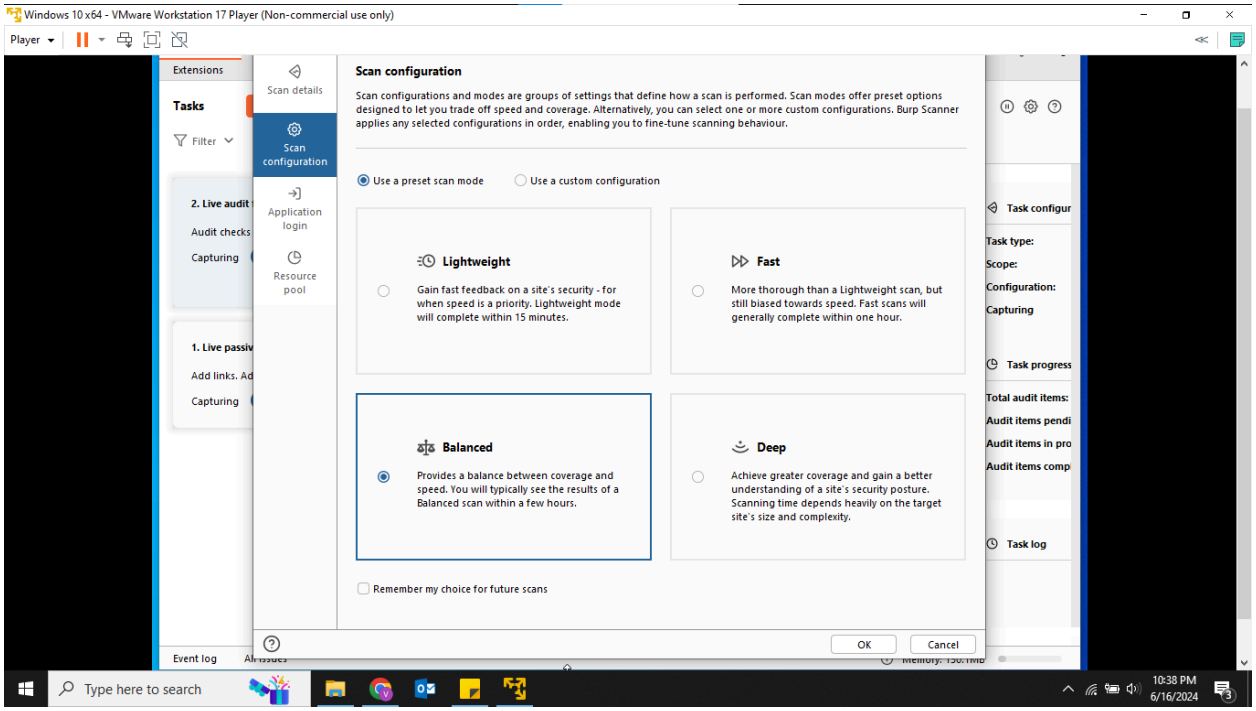
Initialization:



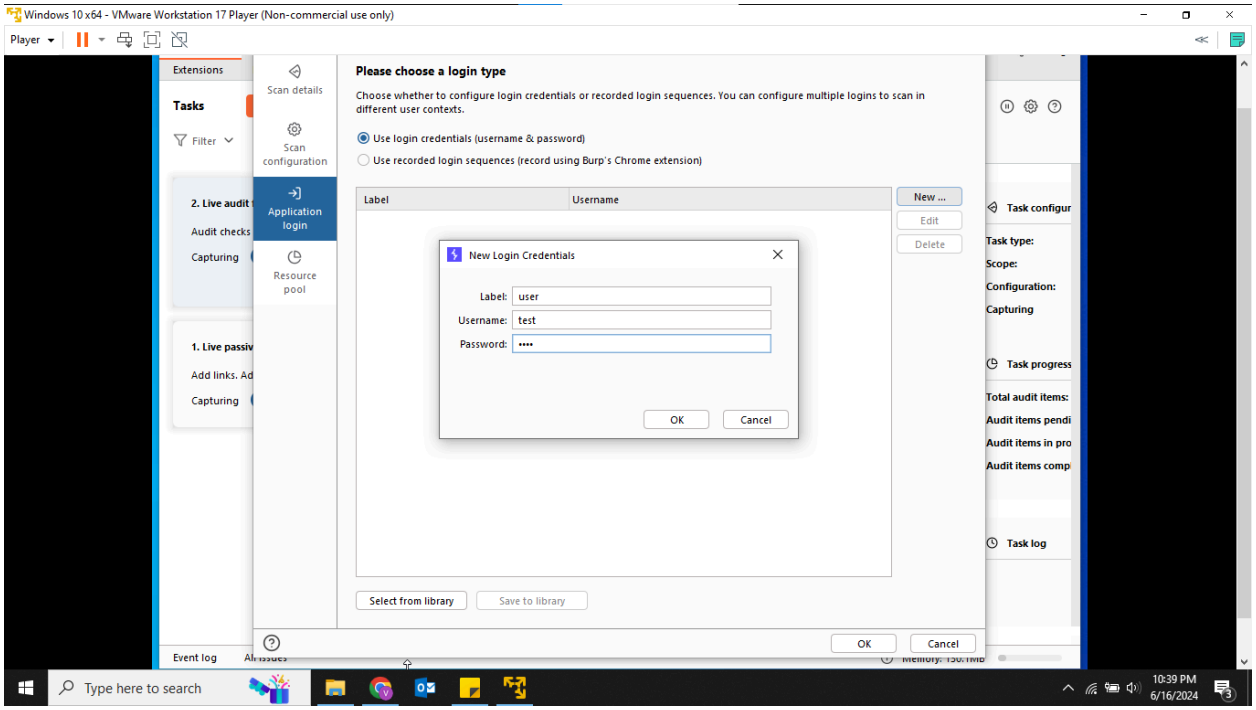
Step 01: Open Burp > New Scan > Web App Scan



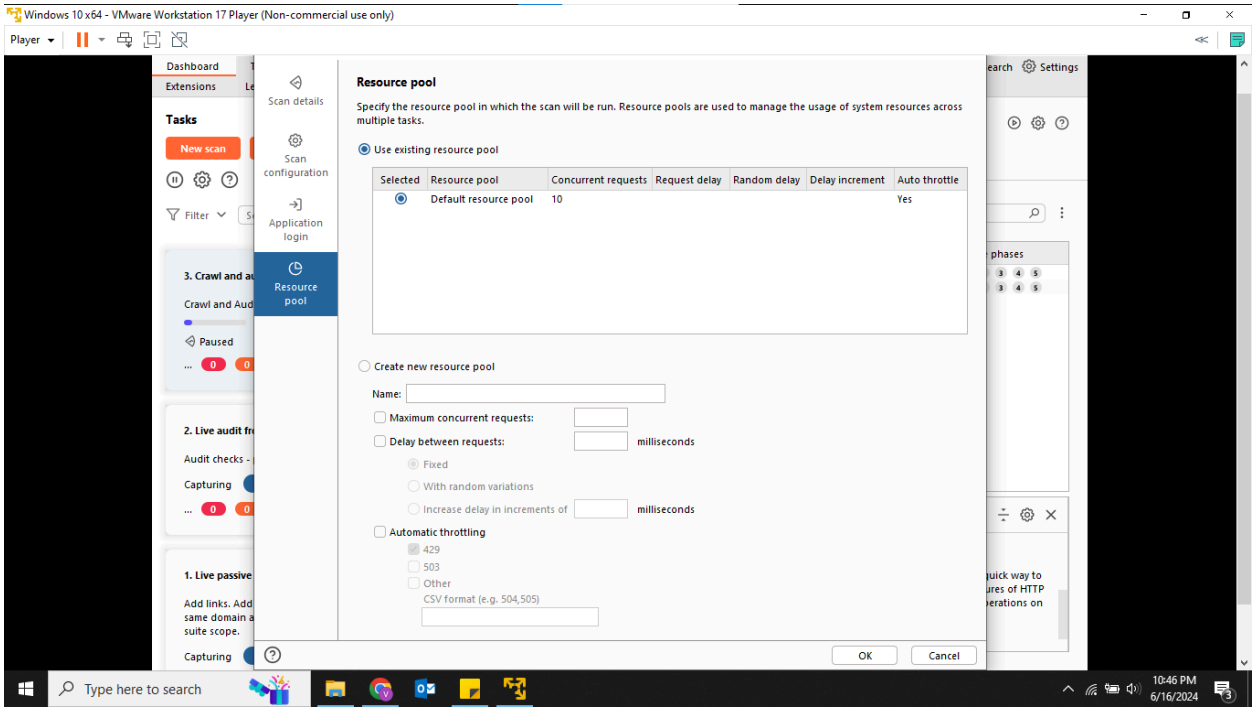
Step 02: Select Scan Type and URLs to Scan



Step 03: Choose the Scan Configuration

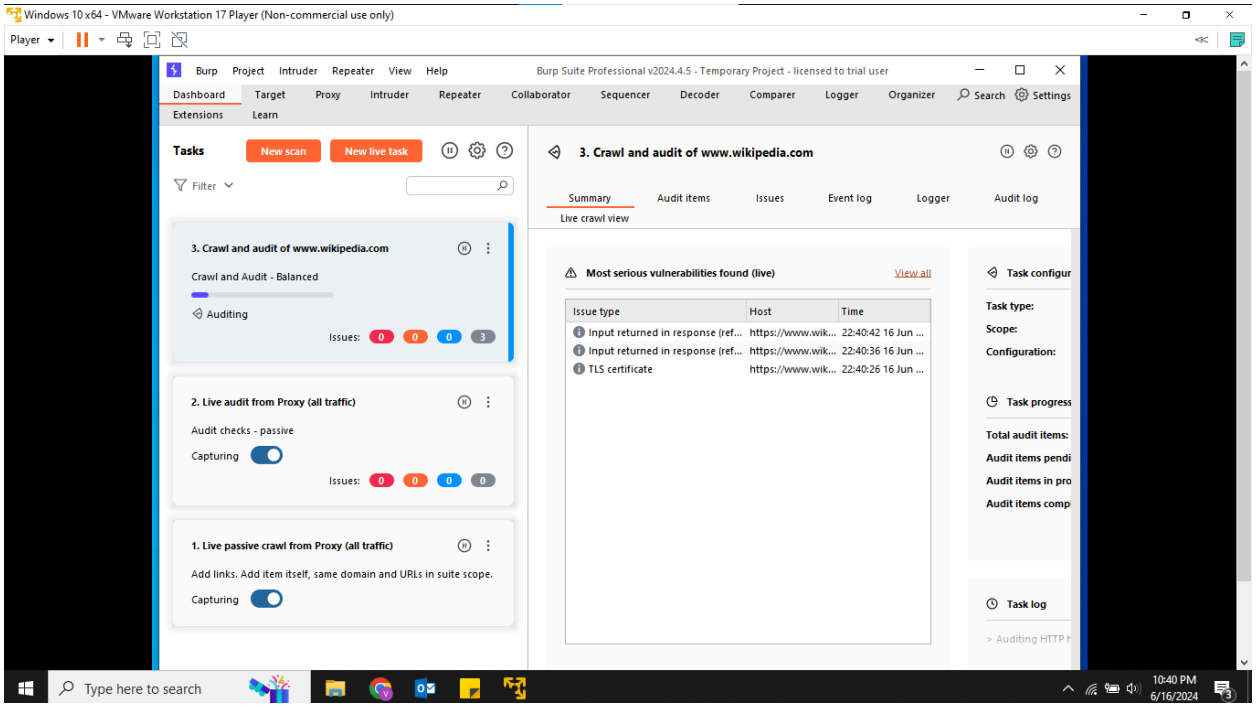


Step 04: Insert the Username and Password for authentication

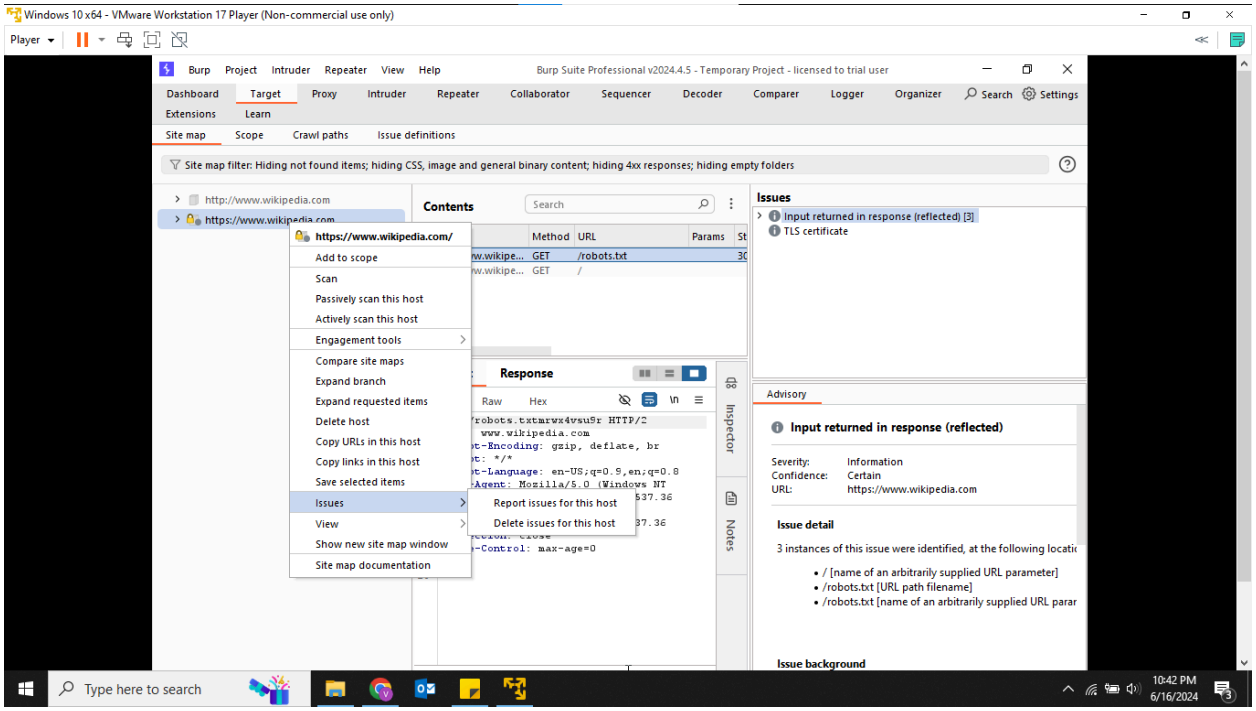


Step 05: Use default or Configure the resource pool and Start the Scan

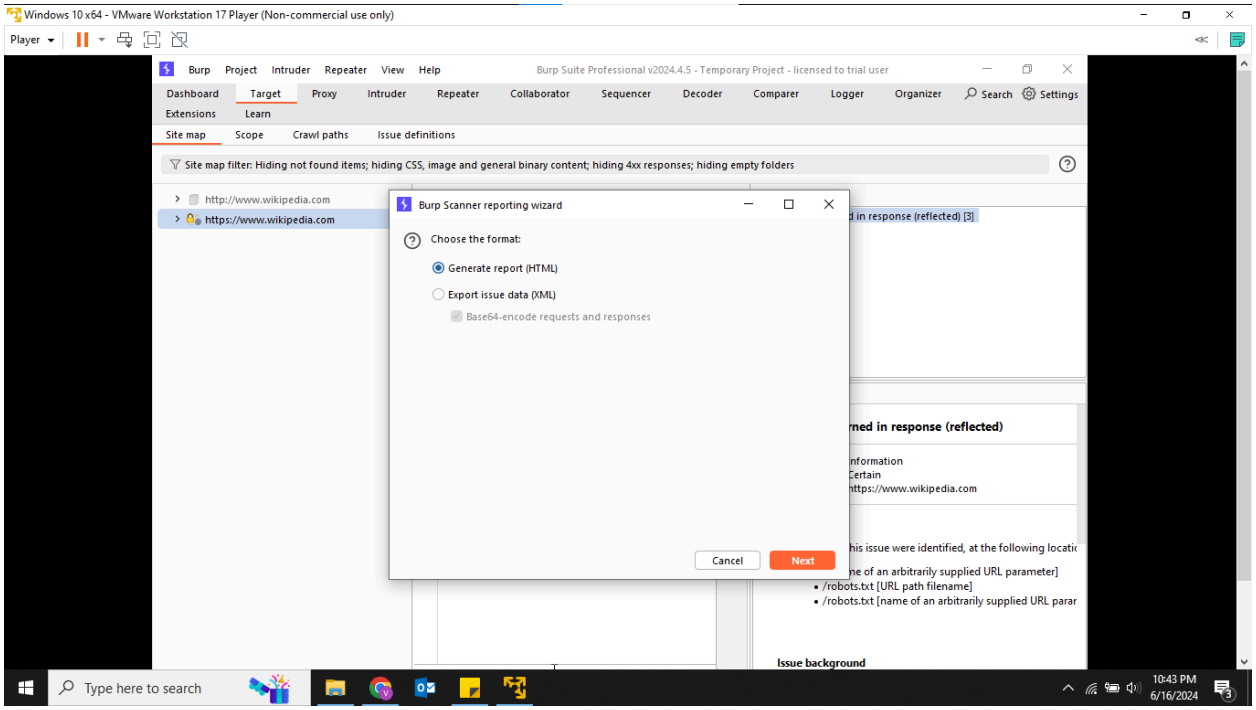
Scan in Progress:



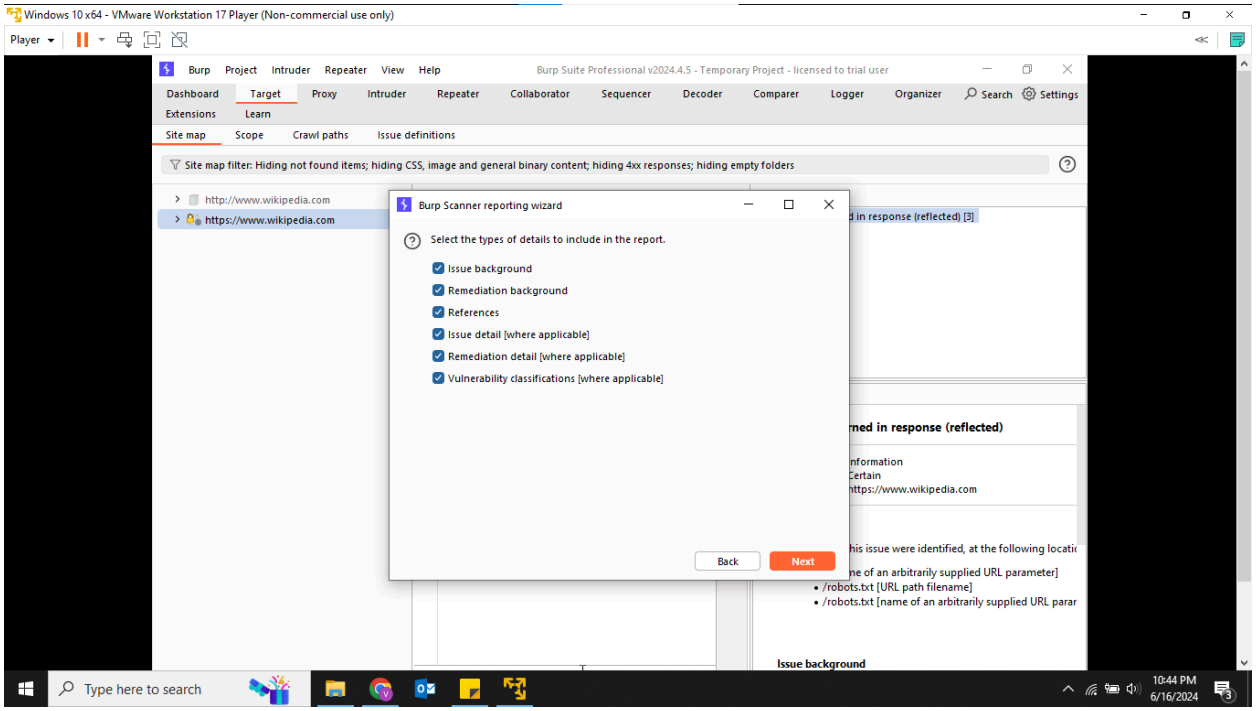
Report Generation:



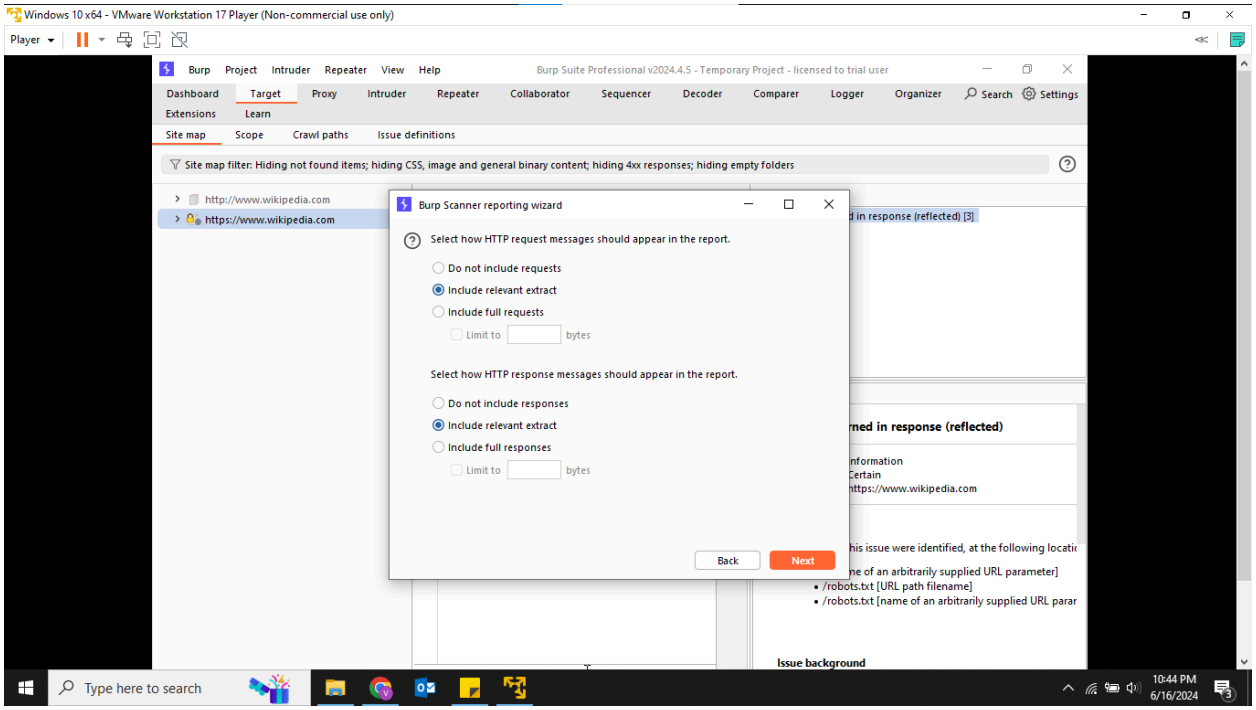
Step 01: Target >> Right Click on the site >> Issues >> Report Issues for the Host



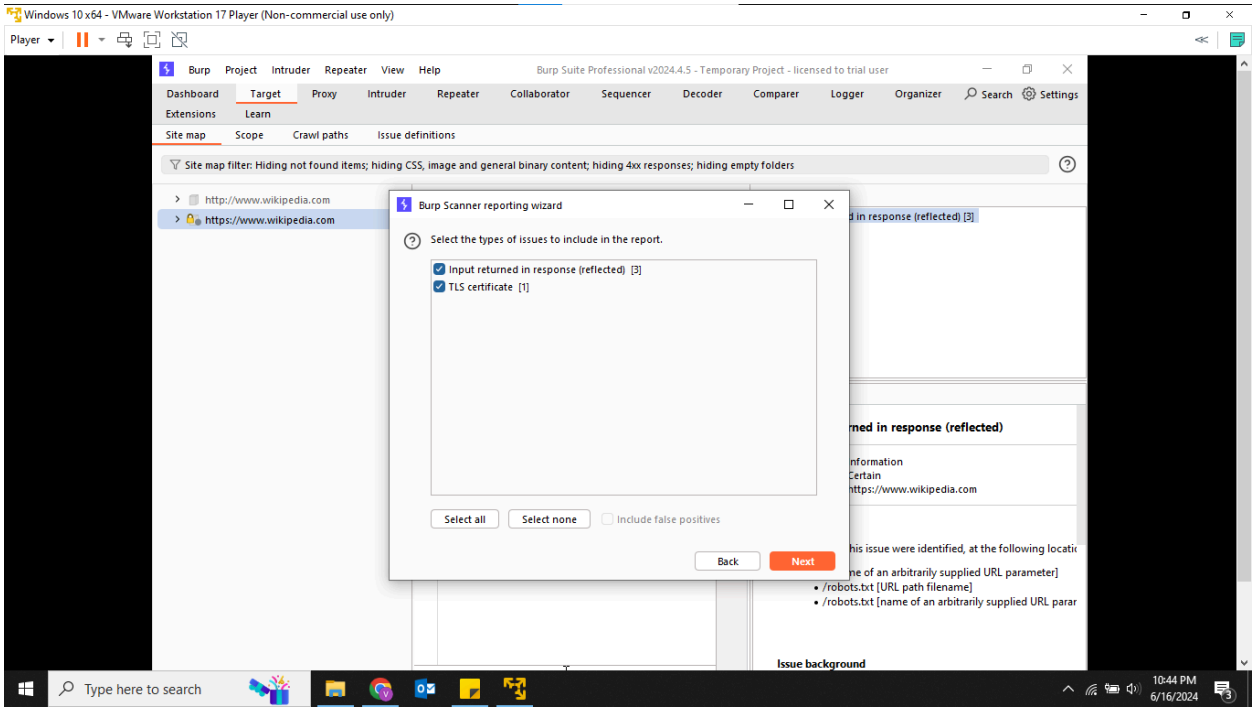
Step 02: Choose the report format



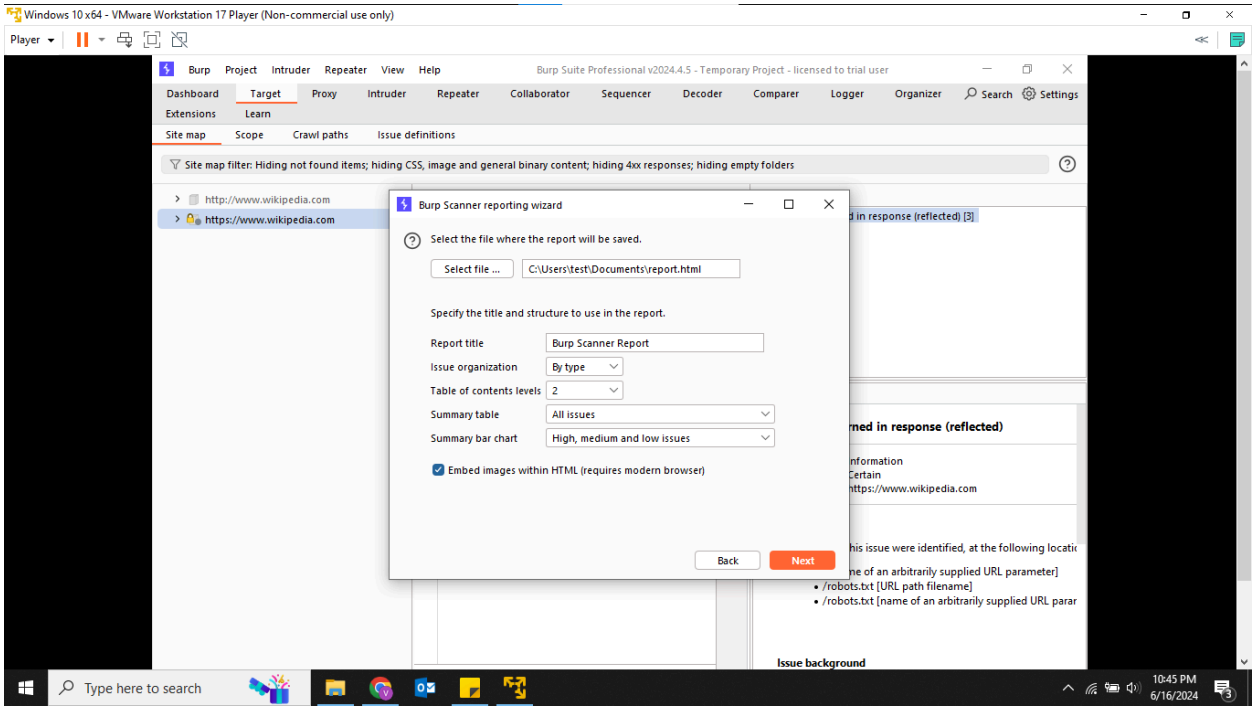
Step 03: Configure the content to be added



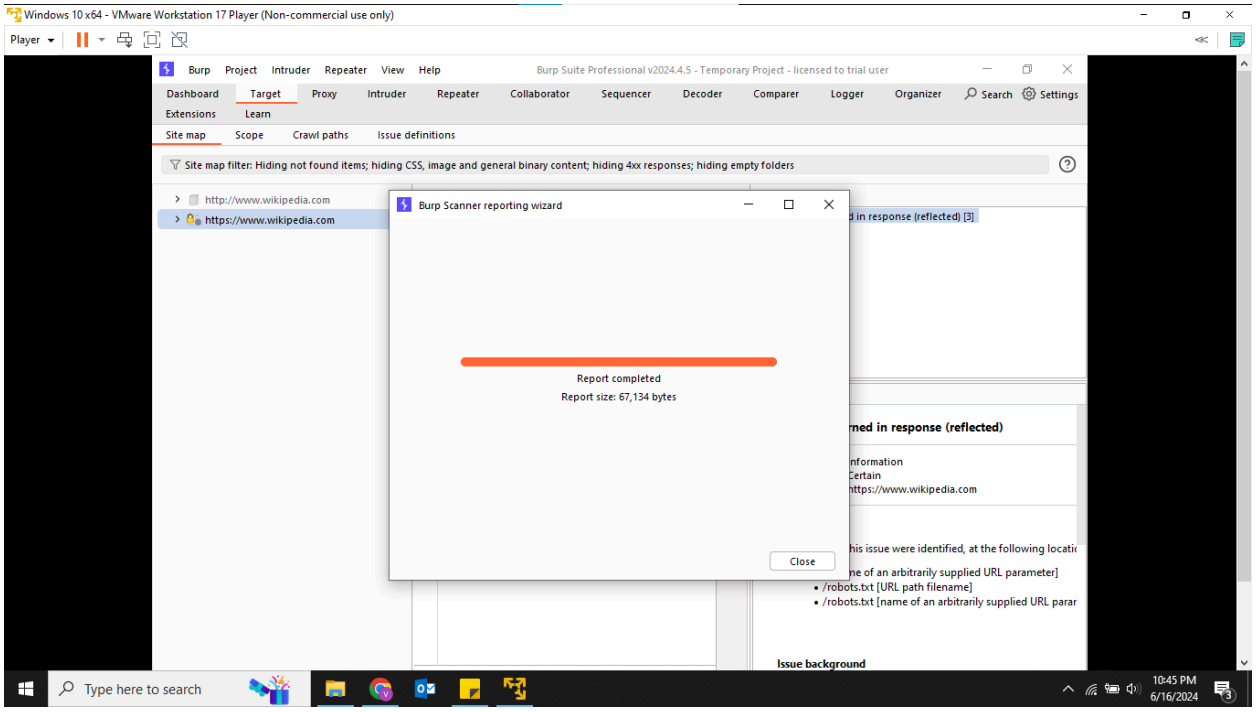
Step 04: Select how HTTP requests and responses should be appeared



Step 06: Select the issues to be included in the report



Step 07: Set the file path to save the report



Step 08: Download the report