NWIT 291 – Lab 5: Burp Suite Intercept Requests

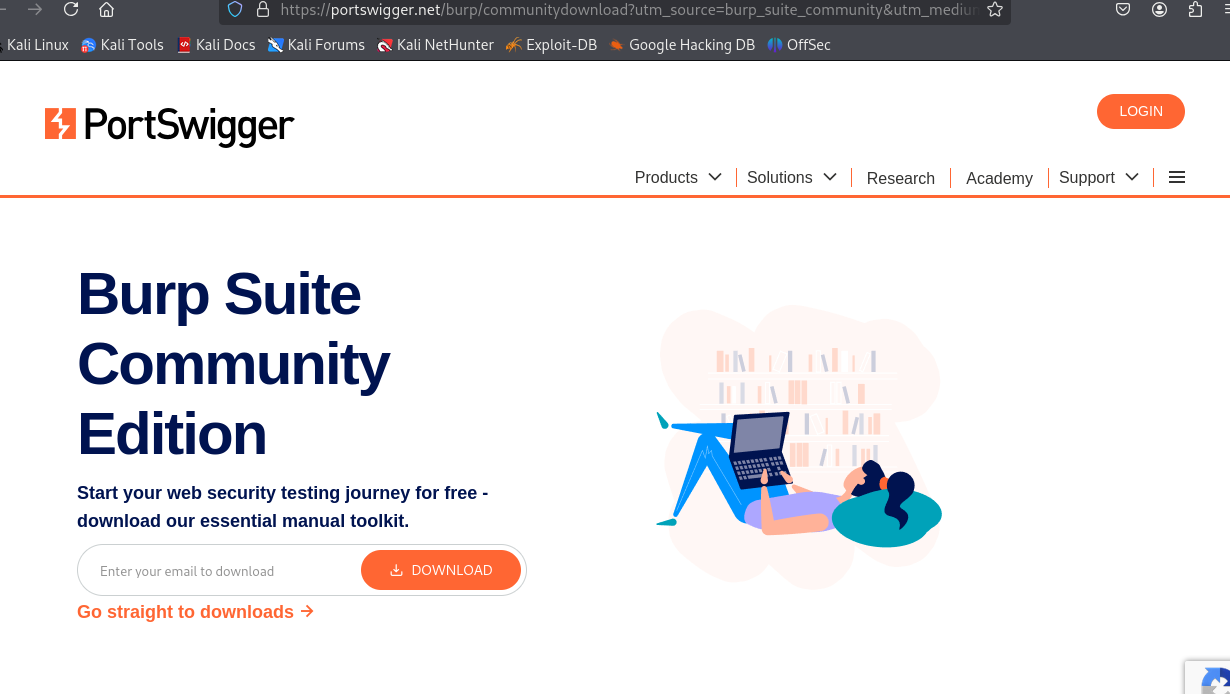
Name: Damon Torres

Course: NWIT 291 – Cybersecurity Capstone

Lab: 5 – Burp Suite Intercept Requests

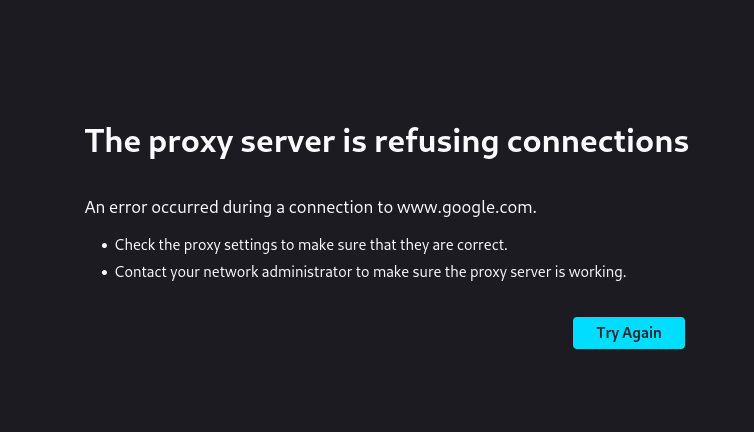
Date: July 20, 2025

This lab demonstrates the setup and use of Burp Suite to intercept, inspect, and manipulate HTTP/HTTPS traffic. Tools used include FoxyProxy, Burp’s Proxy, Repeater, and Inspector features.

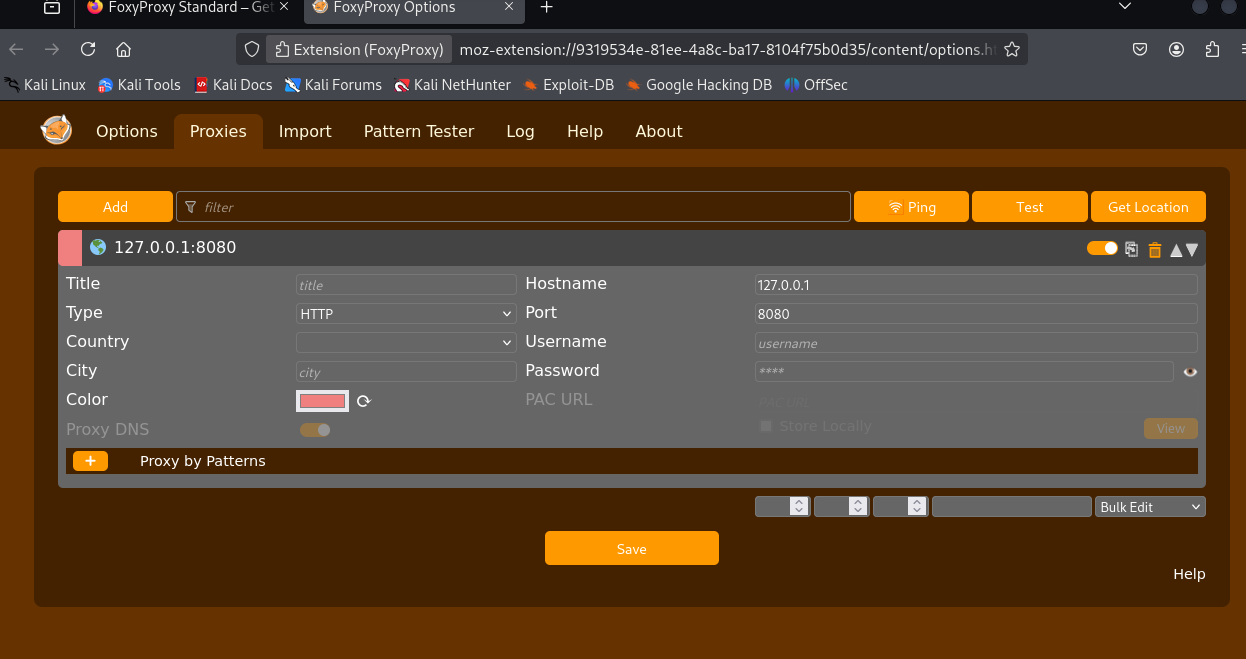


Accessing the Burp Suite Community Edition download page from PortSwigger.

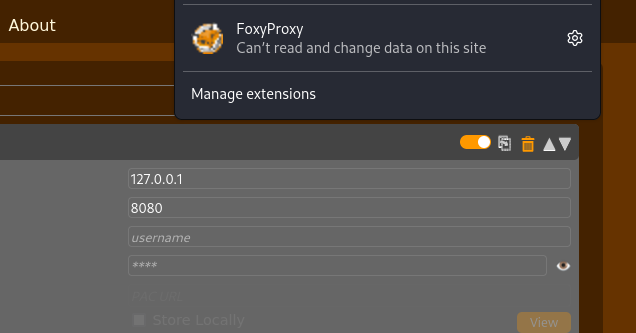
Firefox failed to connect due to Burp Suite not listening on proxy port.



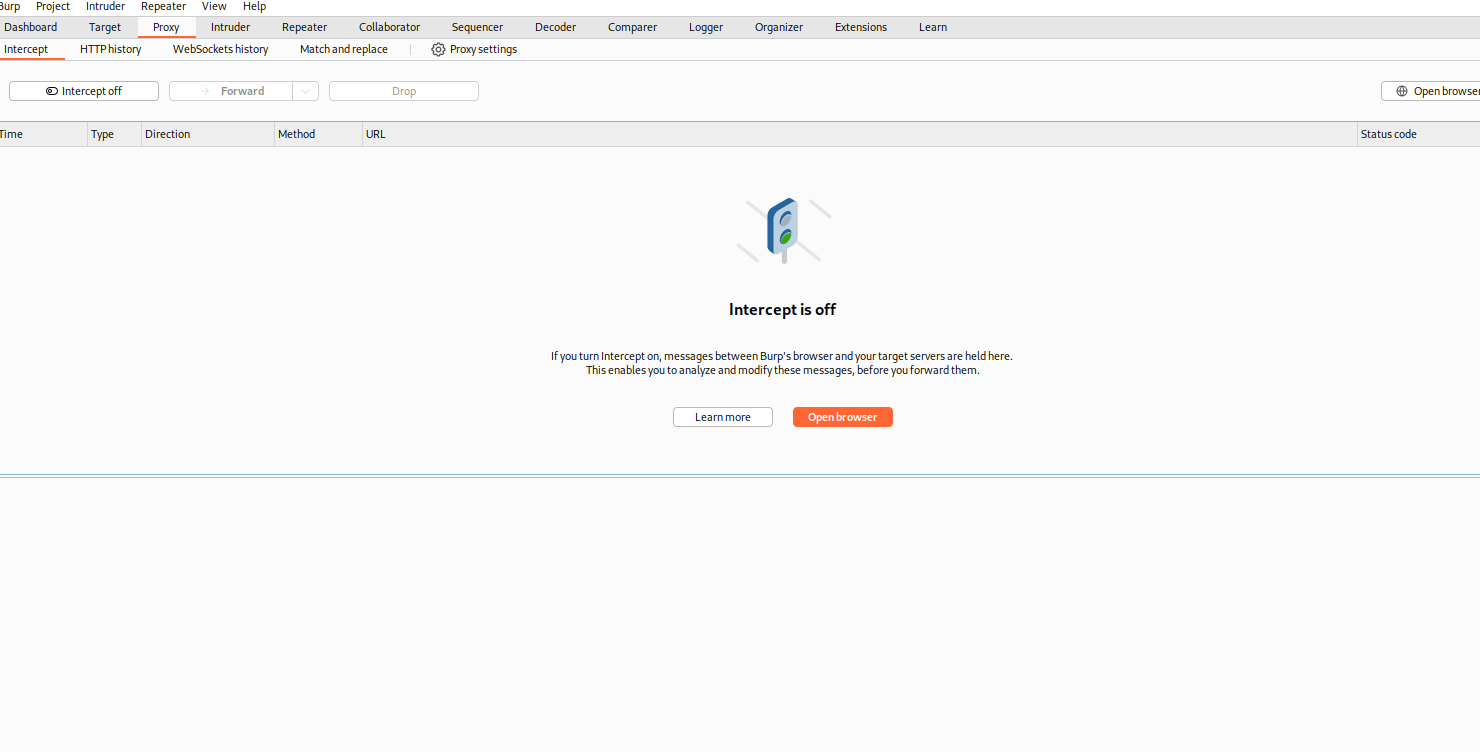
FoxyProxy configured to send browser traffic to Burp Suite at localhost:8080.



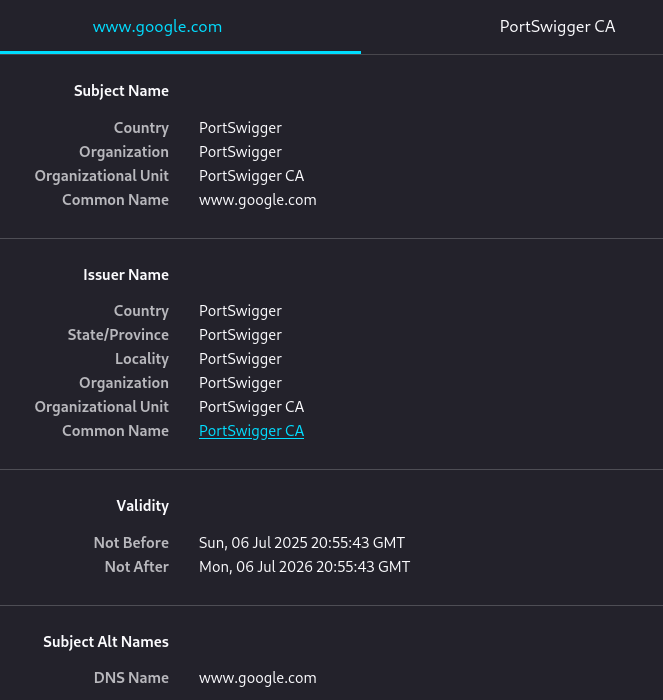
Accessing Firefox extension settings for FoxyProxy.



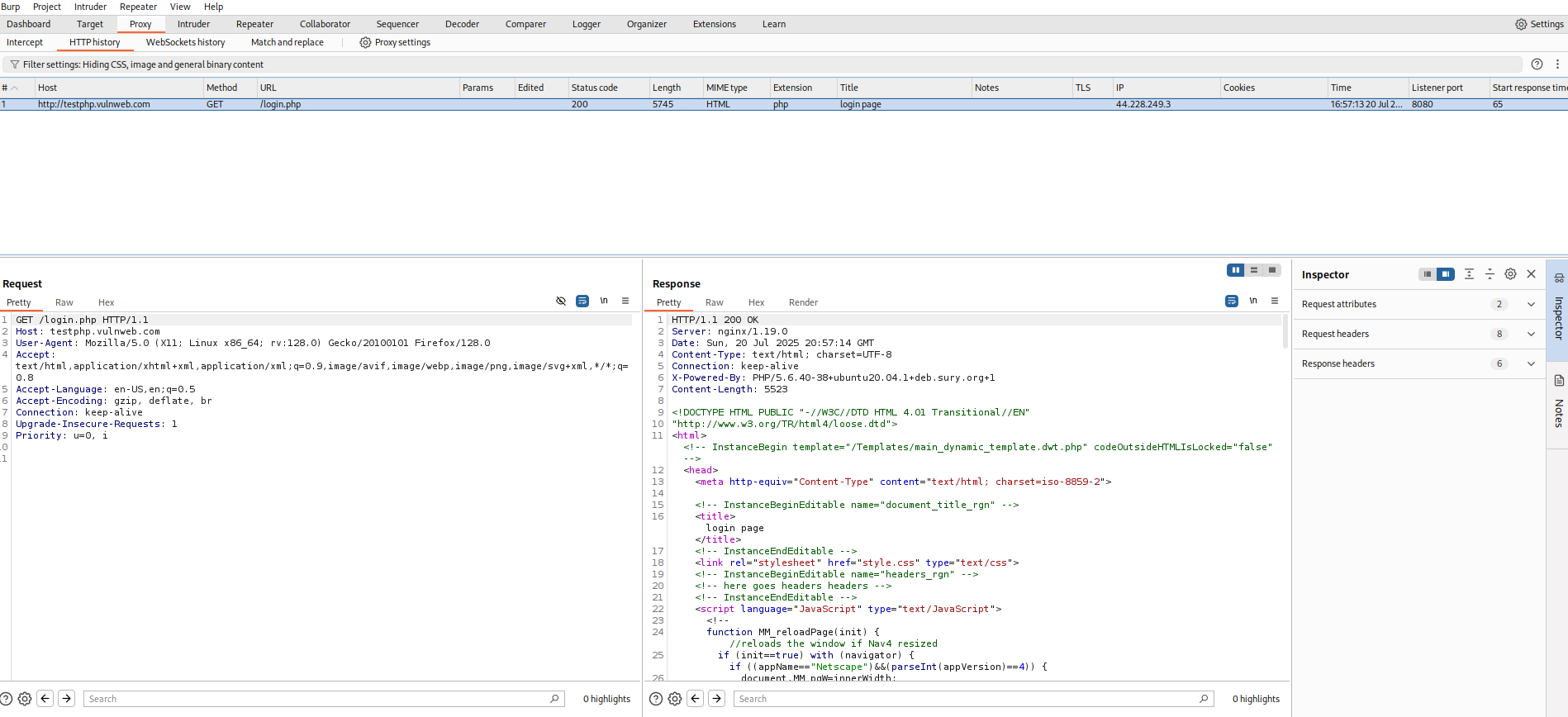
Burp Suite ready to intercept with Intercept turned off initially.



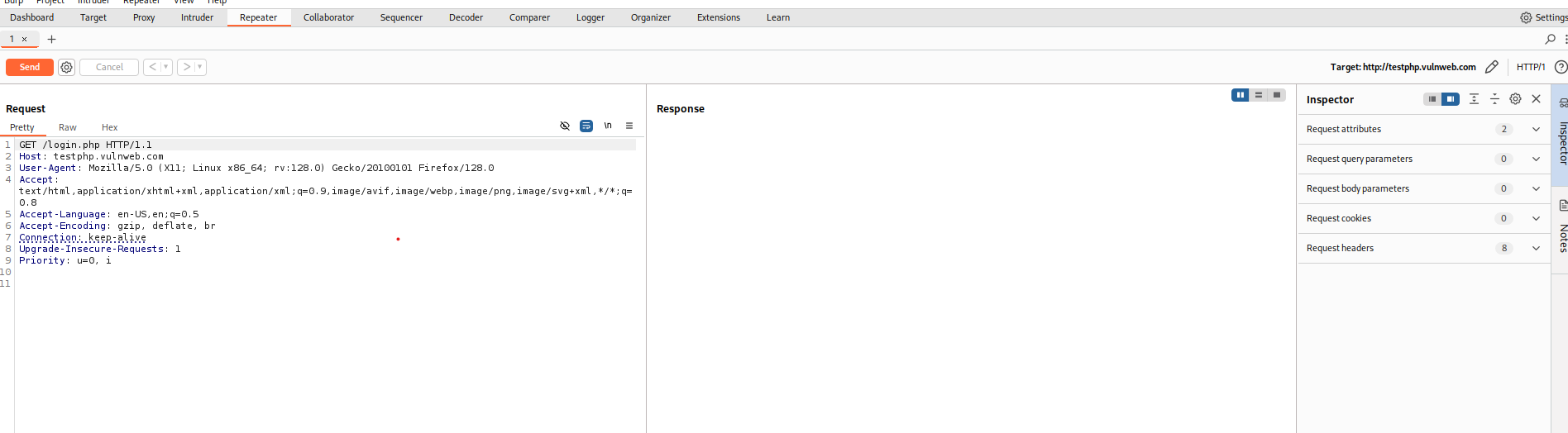
Burp Suite CA certificate is now trusted by Firefox, allowing interception of HTTPS traffic (e.g., www.google.com).



Burp Suite intercepting and displaying HTTP request and response data from testphp.vulnweb.com/login.php.



Using Burp Suite's Repeater tool to resend and analyze HTTP request to testphp.vulnweb.com with Inspector tab showing request details.



## Conclusion:

Through this lab, I was able to configure Burp Suite with Firefox using FoxyProxy, install and trust the CA certificate, and successfully intercept HTTP and HTTPS traffic. I also explored Burp's Repeater and Inspector features to analyze and replay requests, which are essential tools in web application security testing. This hands-on experience helped reinforce how Burp Suite supports testing for vulnerabilities such as XSS and SQL injection.