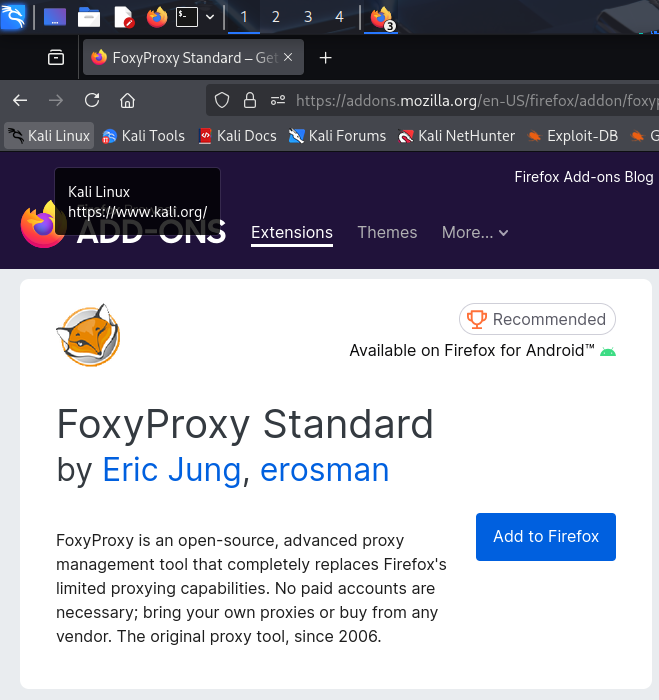
**Author: Widmarck Francois**

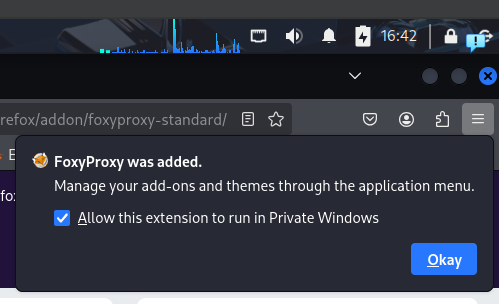
**Burp Suite Lab Report**

**Description:**I launched Kali Linux and opened the Firefox browser. I searched for “FoxyProxy for Firefox” and selected the first result. I then added the extension to Firefox when prompted.

****

**Description:**

Firefox prompted me to grant FoxyProxy permissions. I clicked Add and then checked "Allow this extension to run in Private Windows."



**Description:**

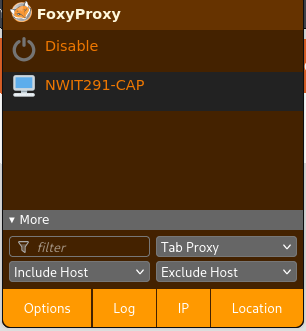
I clicked on the Extensions icon in Firefox, selected FoxyProxy, and accessed its Options menu to begin proxy configuration.

A screenshot of a computer

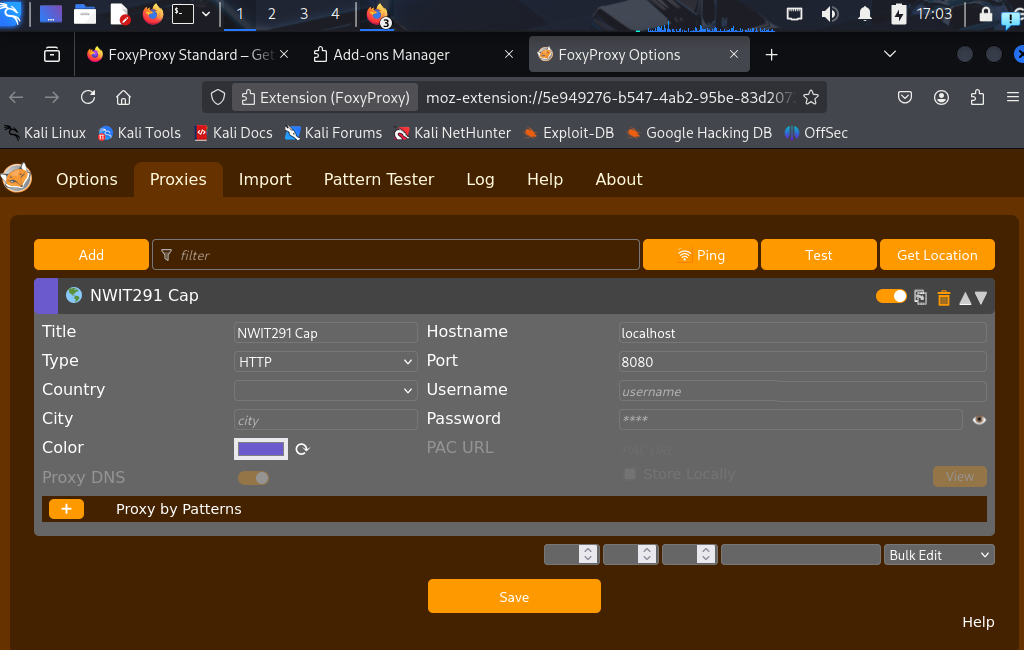
AI-generated content may be incorrect.

**Description:**

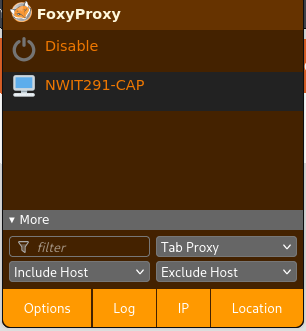
After clicking on the on the Extension icon on Firefox before configuration, I am presented with this screen that show the proxy is disabled.



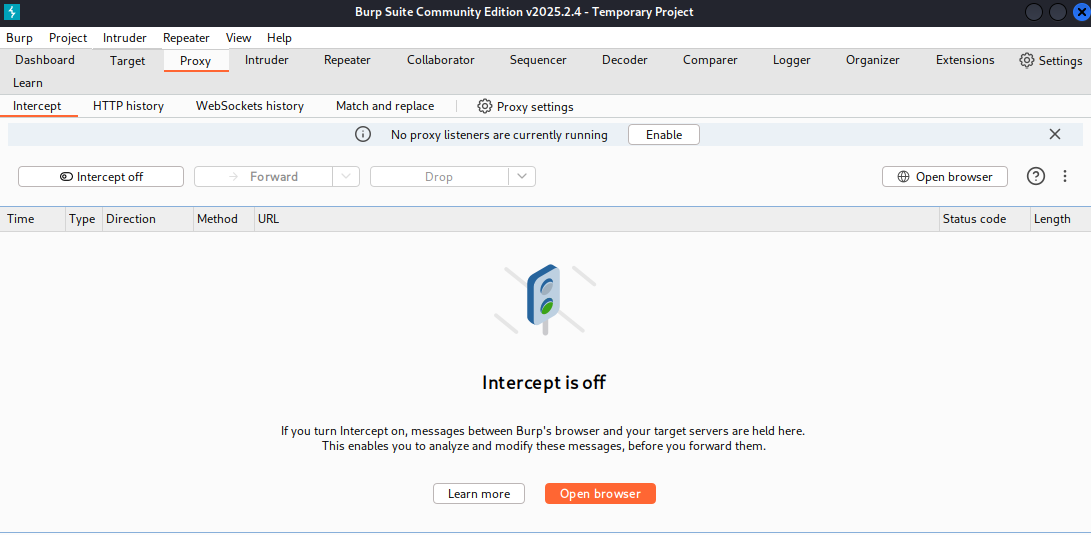
**Description:**  
Under the Proxies tab, I added a new proxy configuration. I set the hostname to localhost, and the port to 8080, then saved the settings.



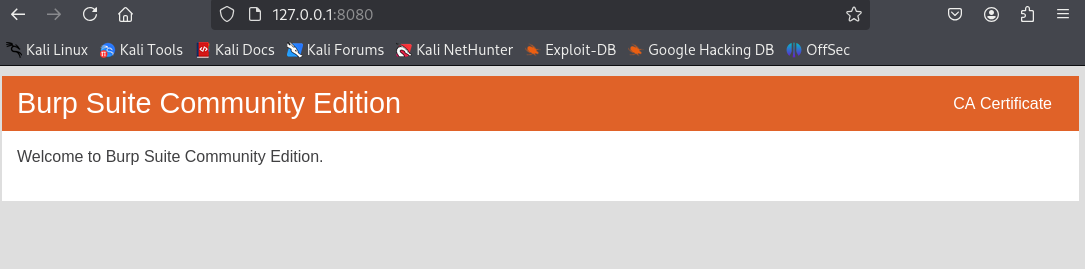
**Description:**  
I clicked on the extension icon again and enabled FoxyProxy to begin intercepting traffic through Burp Suite on port 8080.



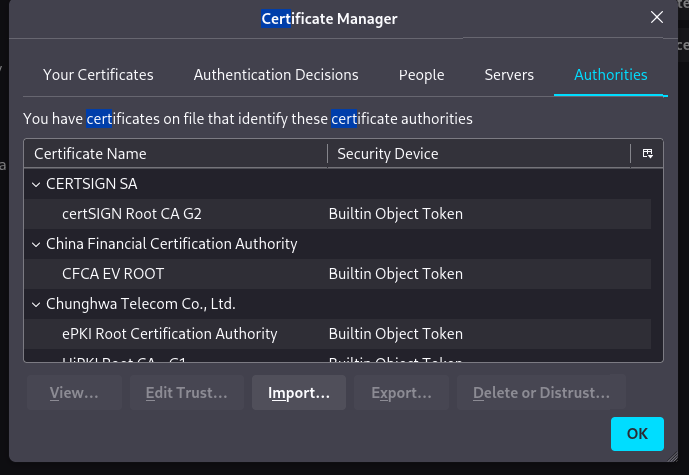
**Description:**  
To verify that Burp Suite is listening on the correct port, I opened a new Firefox tab and visited 127.0.0.1:8080 or localhost:8080.



**Description:**  
After opening the Burp browser interface, I clicked the CA Certificate button to download the file cacertificate.der, needed to intercept HTTPS traffic.

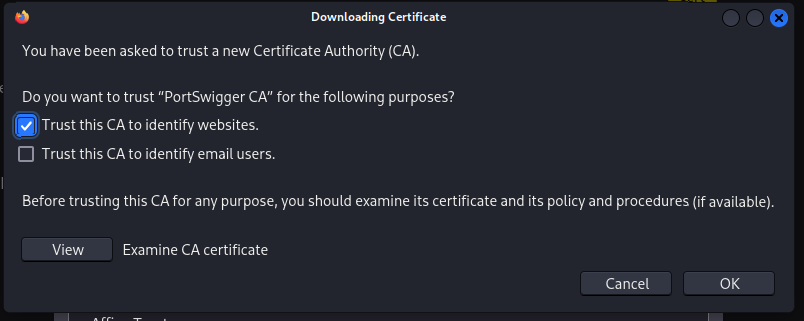


**Description:**I opened Firefox settings by clicking the ellipses (⋮), searched for "cert", clicked View Certificates, then Import, and selected the downloaded cacertificate.der file to trust it.

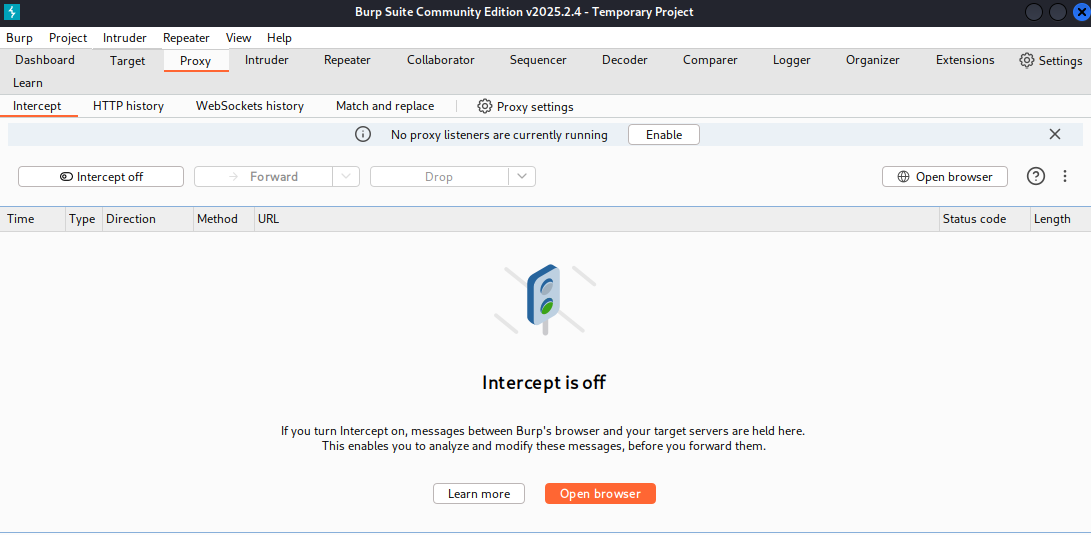


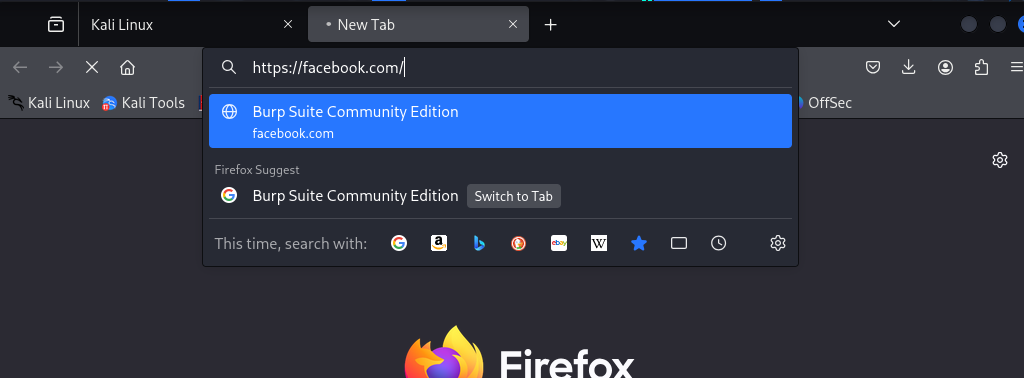
**Description:**

After the certificate manager appeared, I clicked import, to find the downloaded certificate to open. Once found, I opened it trust and/or inspection.

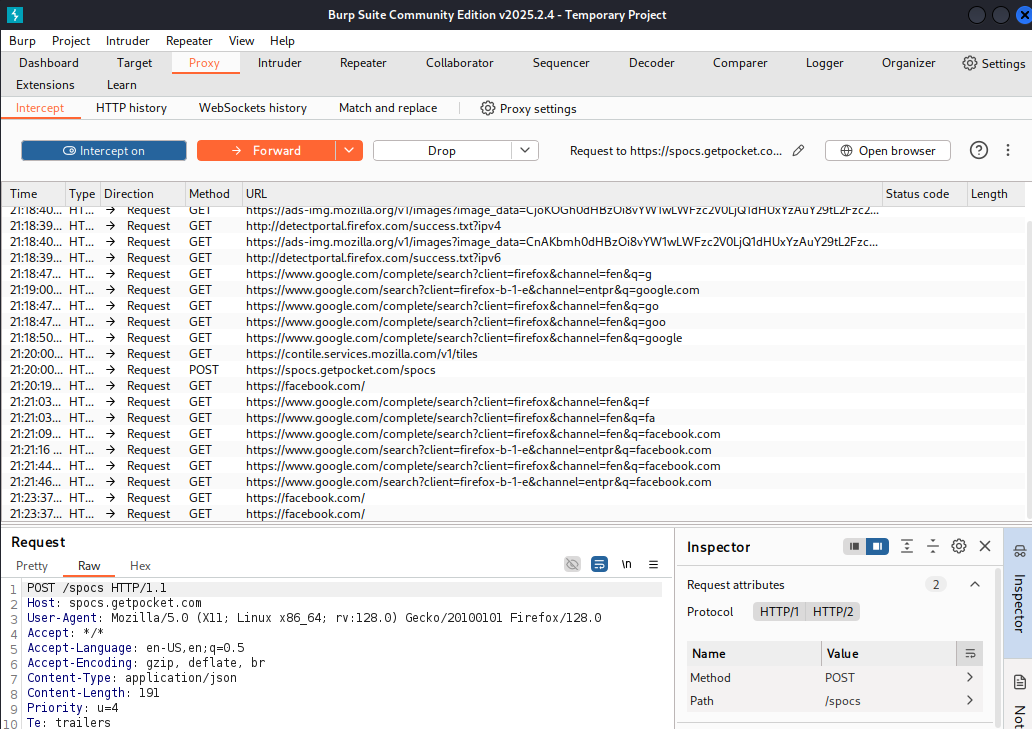


**Description:**  
I visited a website with a login page to generate traffic that I could intercept and analyze using Burp Suite.





**Description:**  
In Burp Suite, I navigated to the Proxy tab and turned Intercept ON. I was able to capture the login request in real time.



**Description:**  
I clicked through tabs under the Inspector pane, exploring tools such as Repeater, Intruder, and Decoder to understand how Burp Suite allows for deeper testing and modification of requests.

