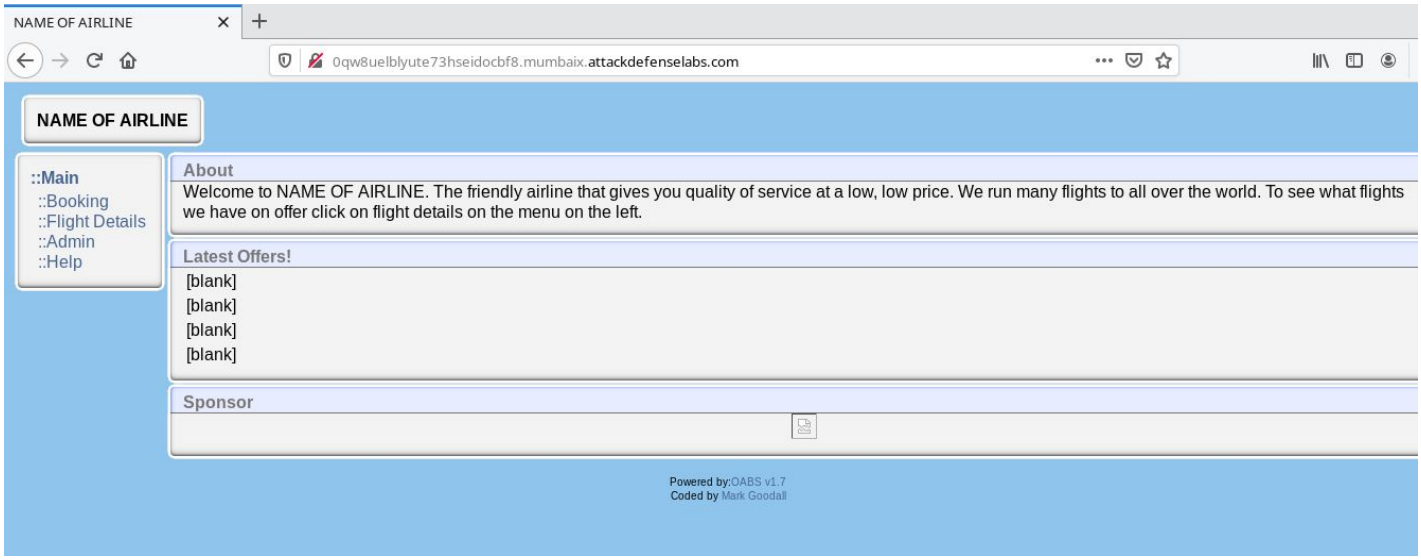

ATTACK
DEFENSE
by PentesterAcademy

Name	Online Airline Booking System
URL	https://www.attackdefense.com/challengedetails?cid=438
Type	Real World Webapps : Broken Authentication

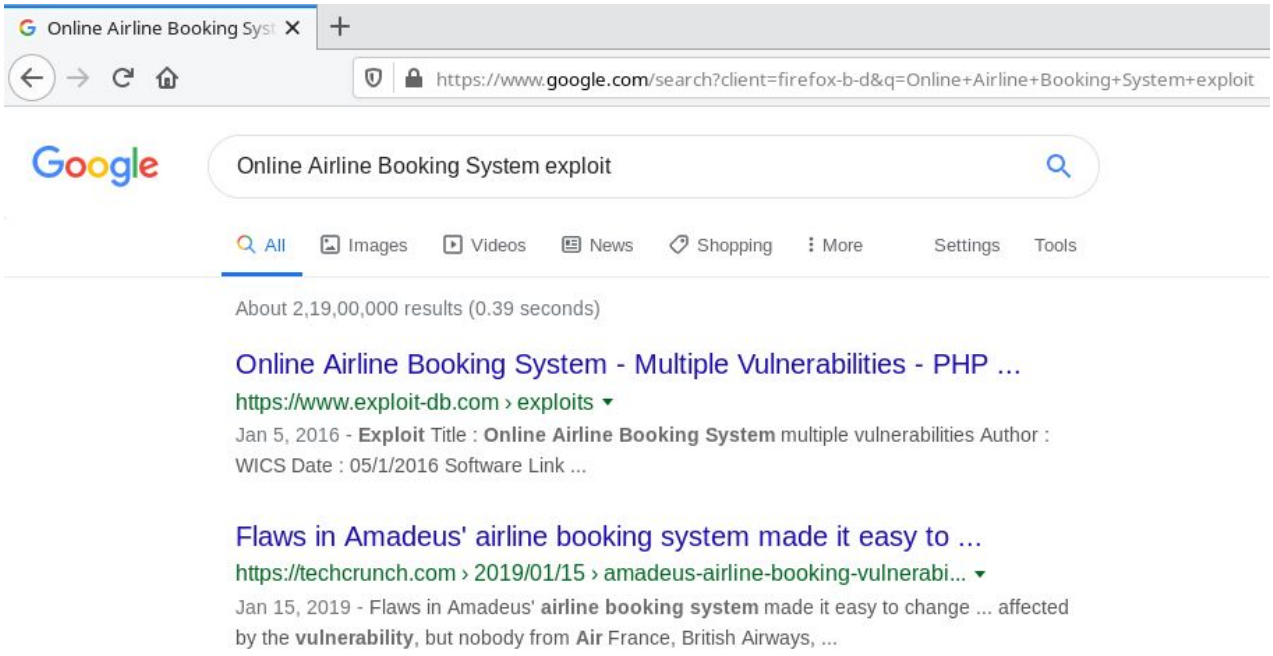
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Solution:

Step 1: Inspect the web application.

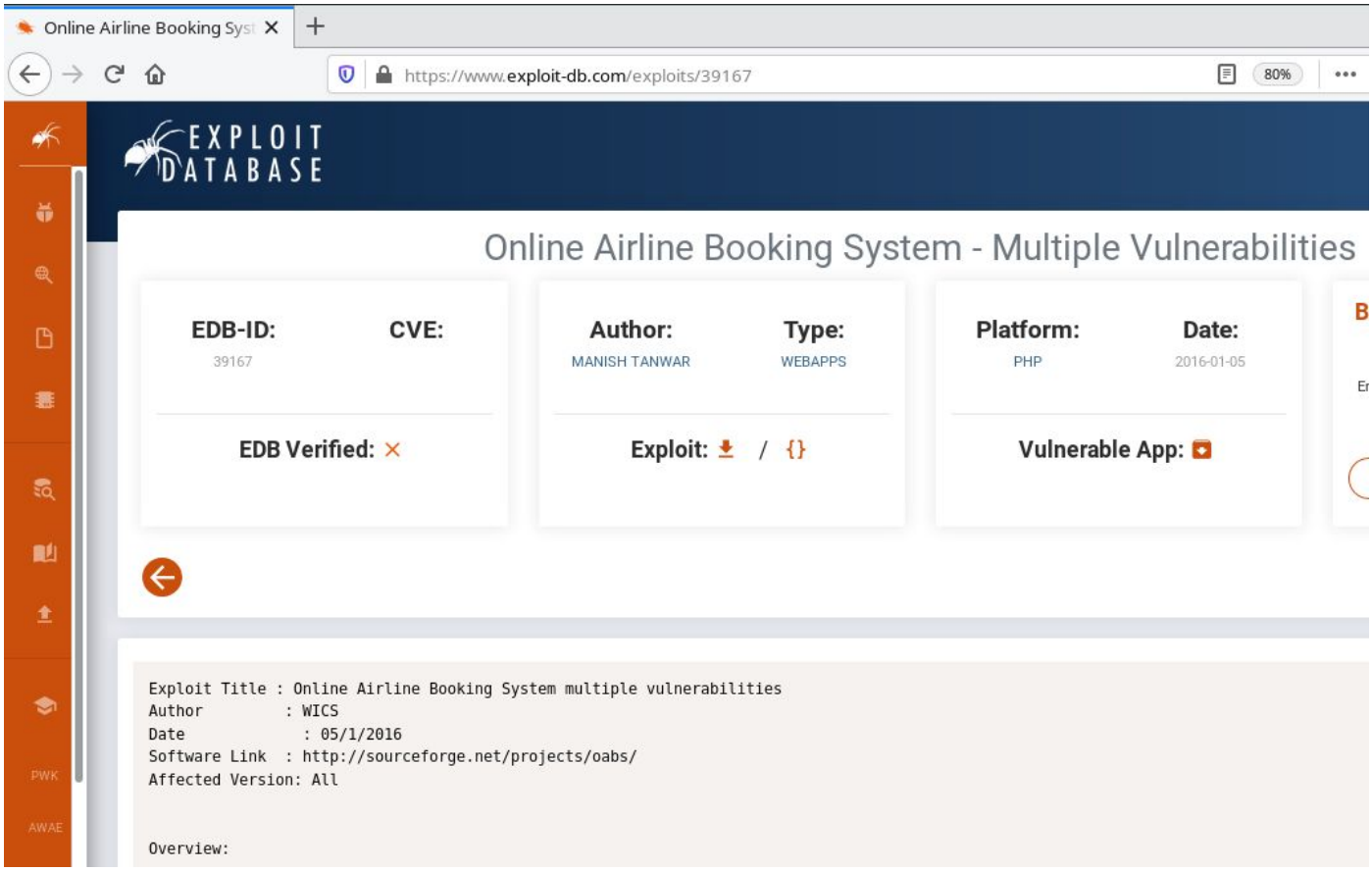


Step 2: Search on google “Online Airline Booking System exploit” and look for publicly available exploits.

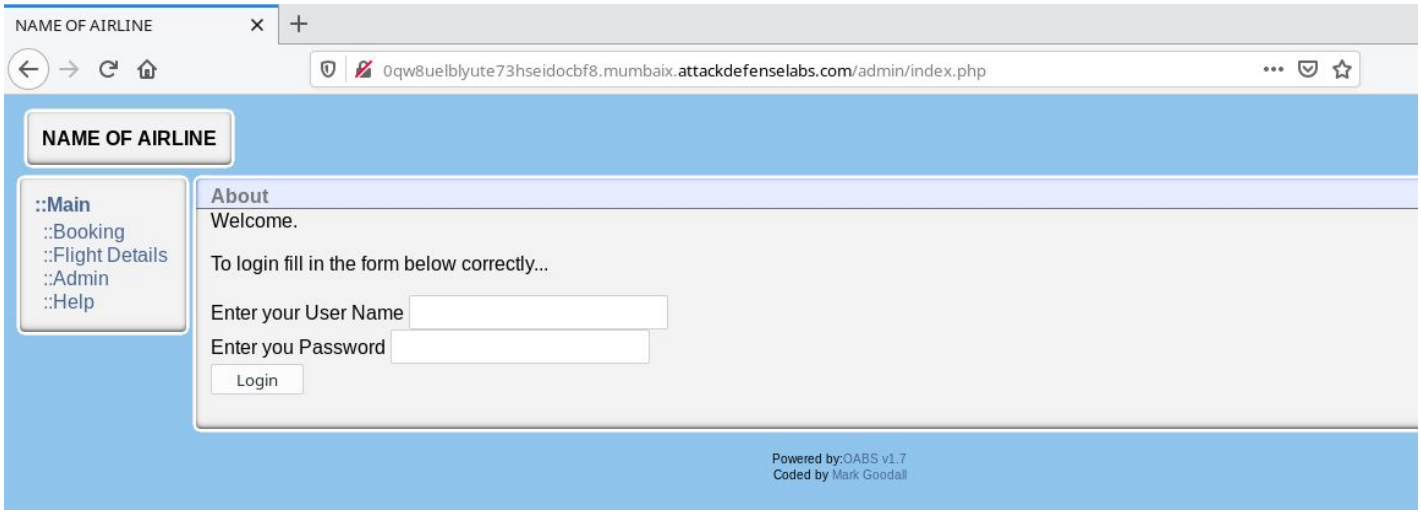


The exploit db link contains the steps to be followed to exploit the vulnerability.

Exploit DB Link: https://www.exploit-db.com/exploits/39167



Step 3: Navigate to admin panel by clicking on the "::Admin" button.

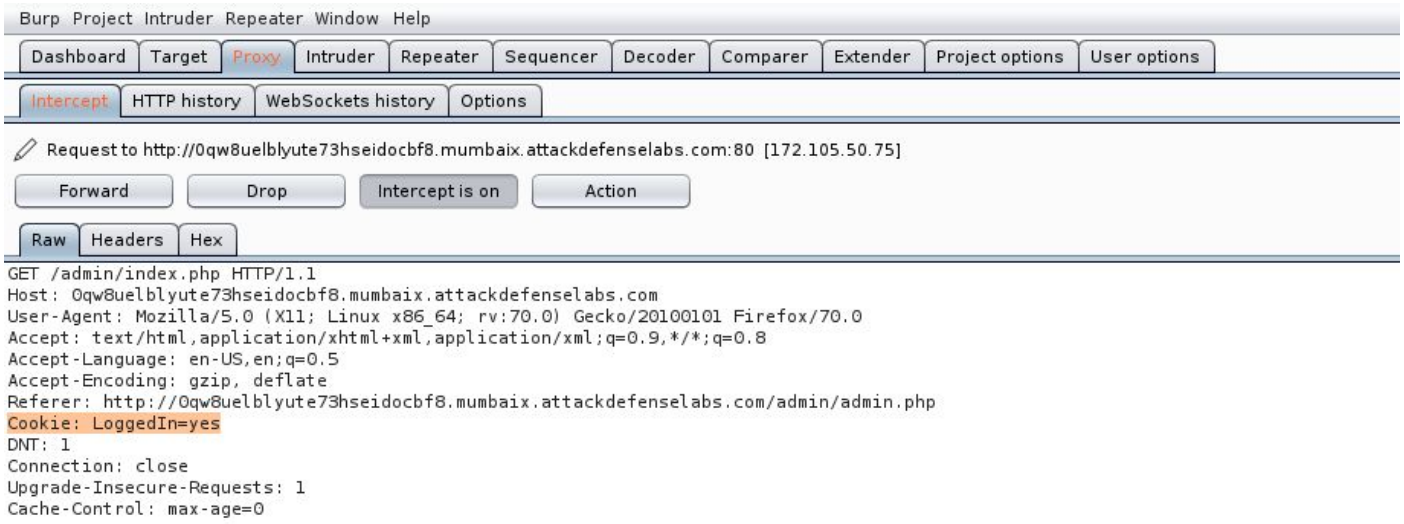


Step 4: Reload the page and Intercept the GET request with burp suite.

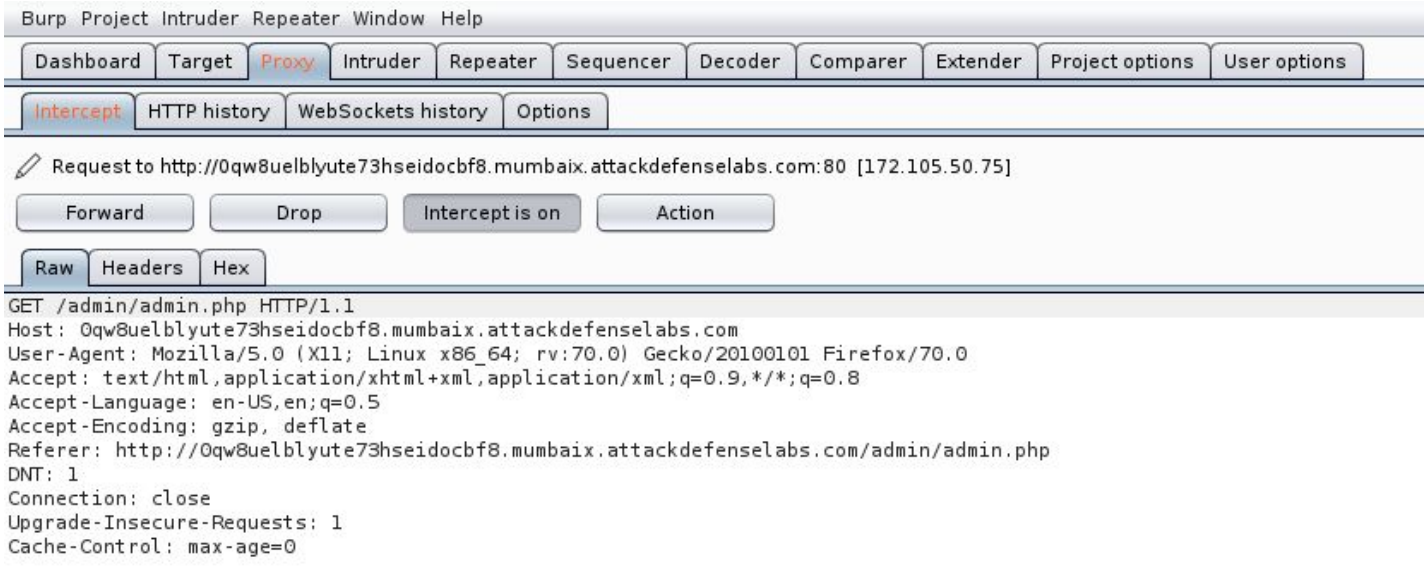
Check Appendix to learn how to configure Burp Suite.

Step 5: Modify the request and add the LoggedIn cookie required to bypass authentication

Cookie: LoggedIn=yes

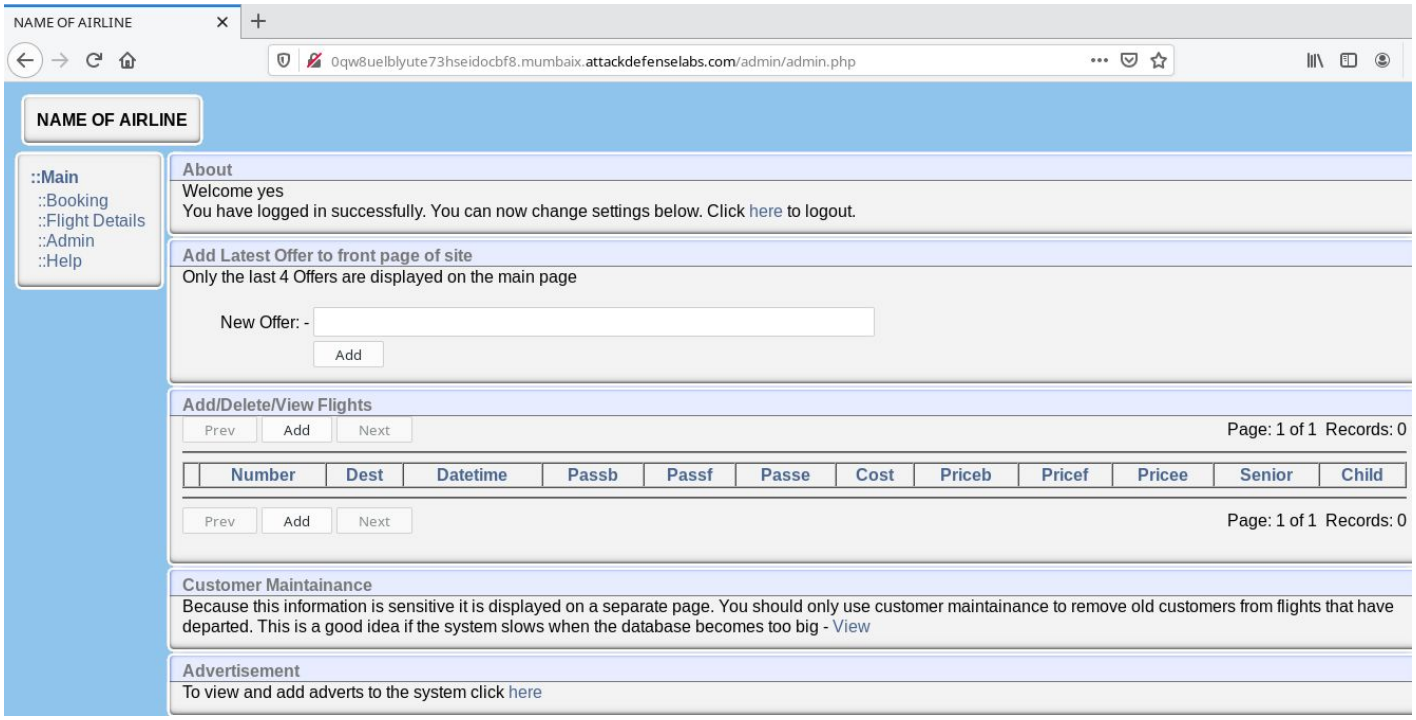


Step 6: Click on “forward” button and keep intercepting the subsequent requests.



Step 7: Modify the request and inject the cookie mentioned in step 5.

Step 8: Click on “forward” button and check the browser.



Authentication was bypassed successfully.

References:

1. Online Airline Booking System (http://sourceforge.net/projects/oabs/)
2. Online Airline Booking System - Multiple Vulnerabilities (https://www.exploit-db.com/exploits/39167)

Appendix

Appendix A: Configuration for Windows OS

A.1 Google Chrome with Burp Suite

A.2 Mozilla Firefox with Burp Suite

Appendix B: Configuration for Kali OS

B.1 Google Chrome with Burp Suite

B.2 Mozilla Firefox with Burp Suite

Appendix C: Configuration for FoxyProxy Standard plugin

C.1 FoxyProxy on Google Chrome with Burp Suite

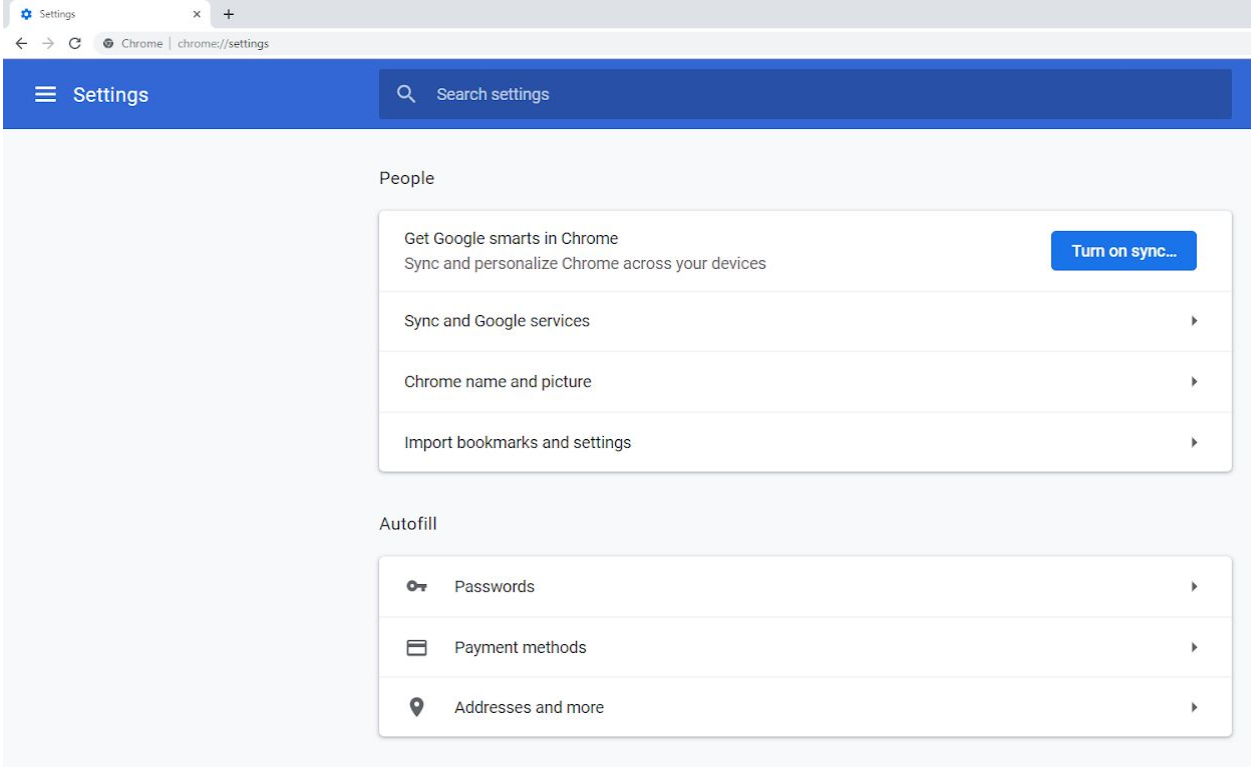
C.2 FoxyProxy on Mozilla Firefox with Burp Suite

Appendix A

A.1 Google Chrome with Burp Suite (Windows OS)

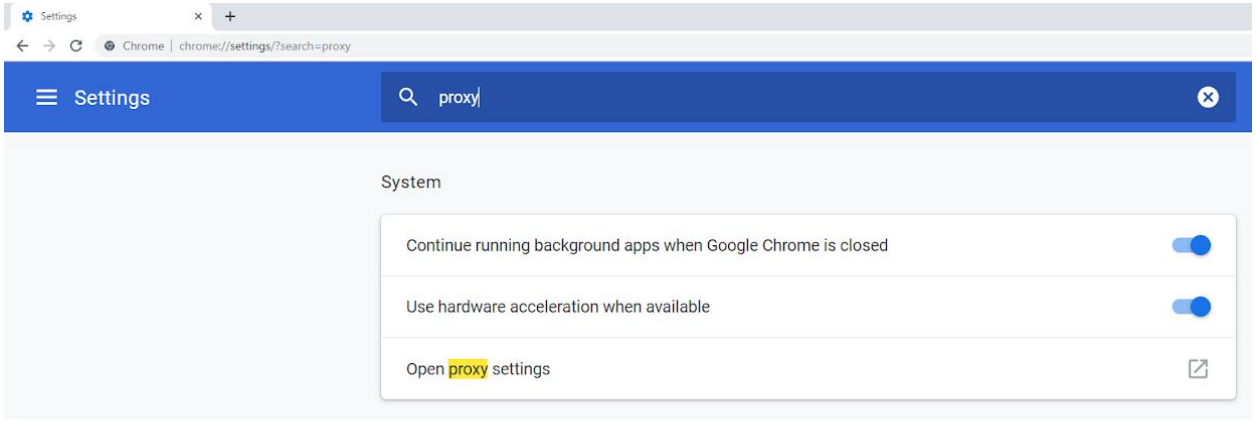
Step 1: Open Google Chrome and navigate to the URL given below.

URL: chrome://settings

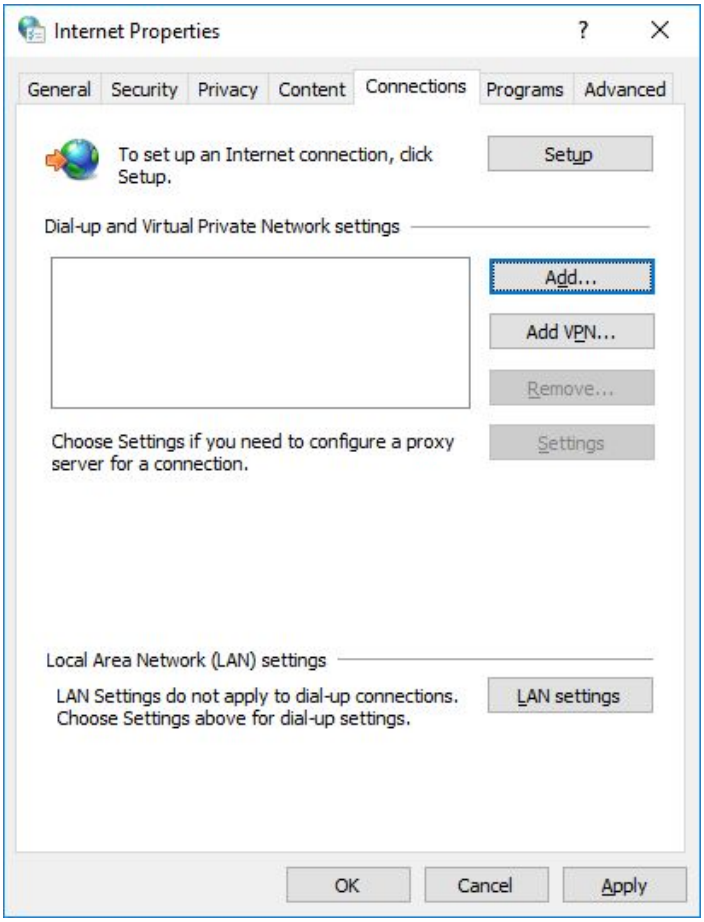


Google Chrome Settings page will appear.

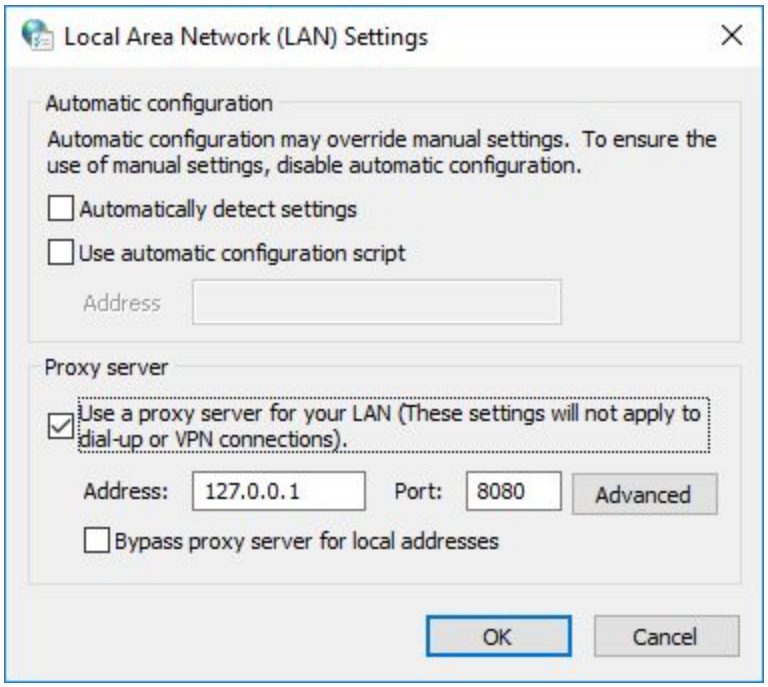
Step 2: Search for “proxy” in the search box.



Step 3: Upon clicking on “Open proxy settings”, Windows “Internet Properties” settings dialog box will appear. Click on “LAN settings” button.

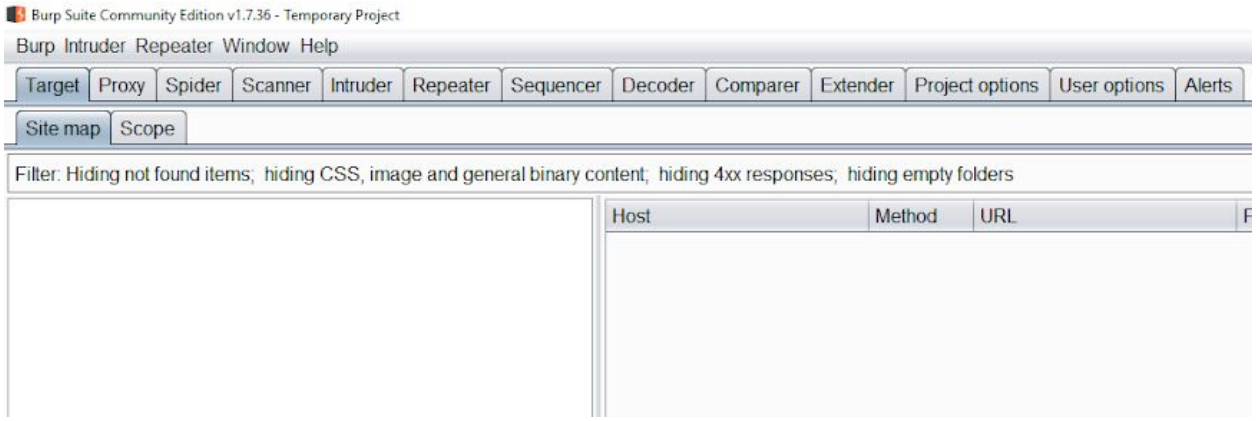


Step 4: Select the checkbox “Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections)”. And enter “127.0.0.1” and “8080” in “Address” textbox and “Port” textbox respectively.

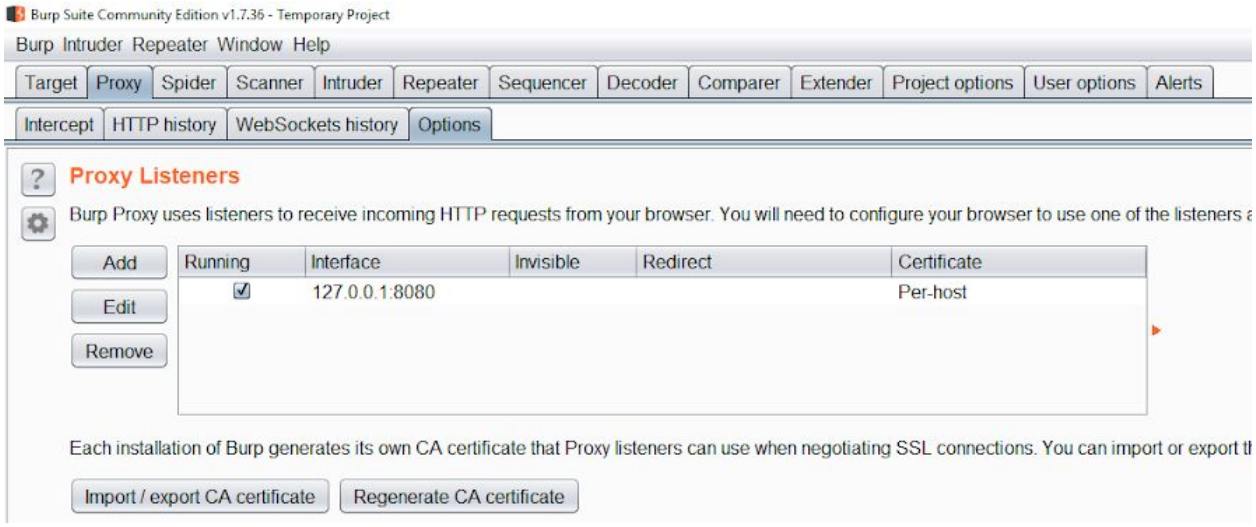


Click “OK” on the “Local Area Network (LAN) Settings” dialog box and close the “Internet Properties” dialog box.

Step 5: Start Burp suite.



Step 6: Navigate to “Options” tab under “Proxy” tab and verify that the “running” checkbox is selected for the interface “127.0.0.1:8080”.

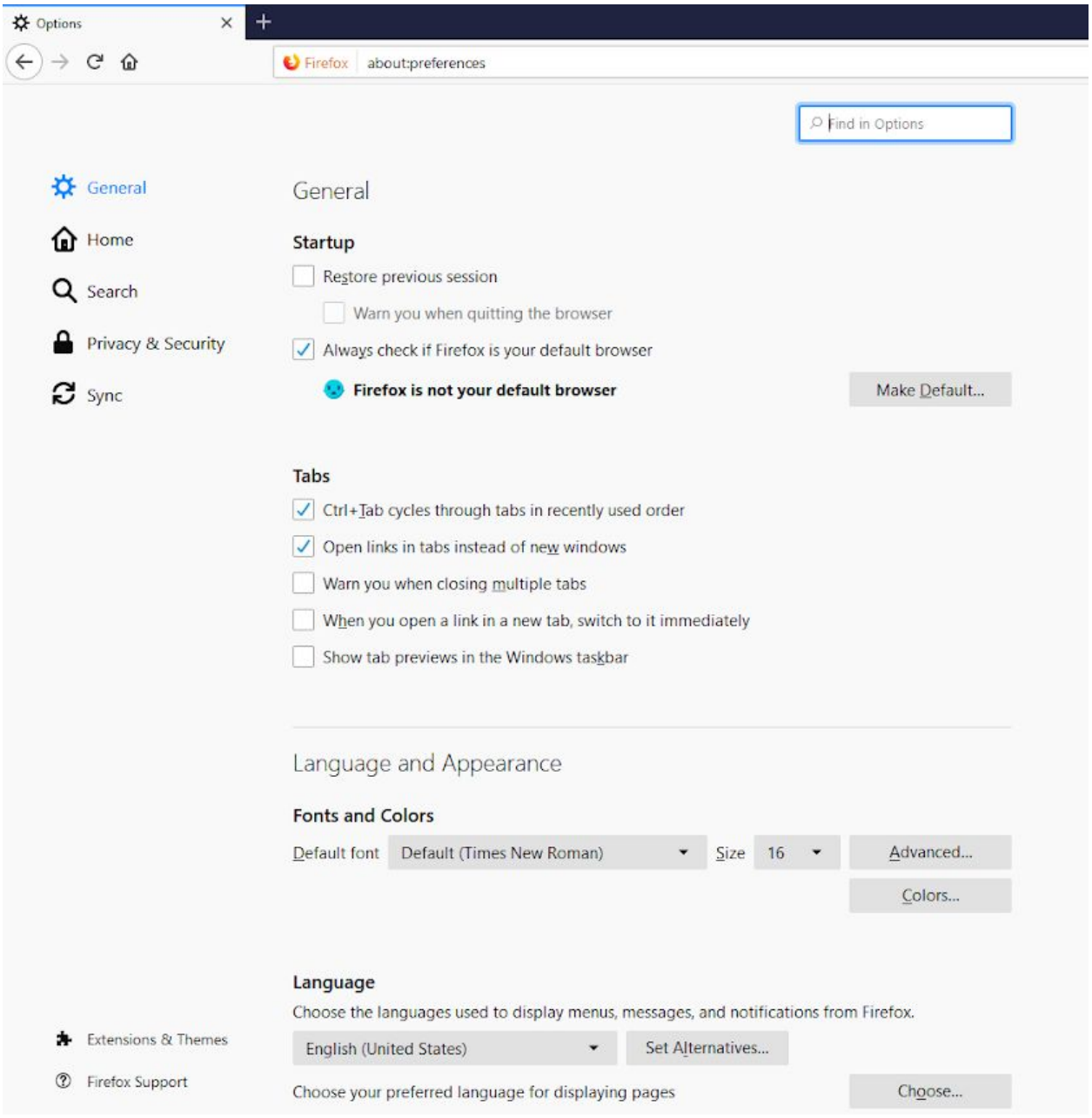


All the HTTP request made by Google Chrome will be intercepted by Burp Suite.

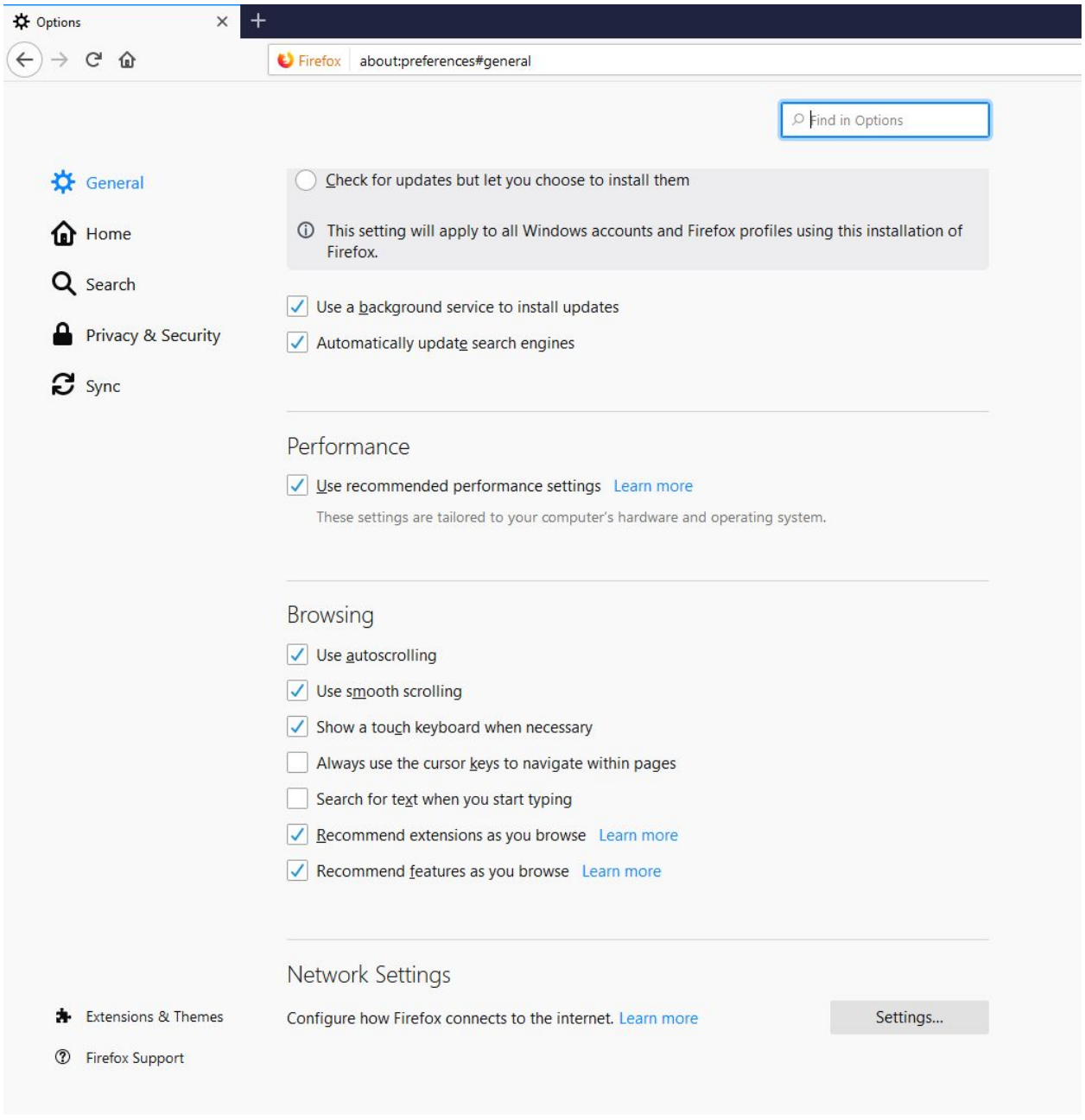
A.2 Mozilla Firefox with burp suite (Windows OS)

Step 1: Open Mozilla Firefox and navigate to the URL given below.

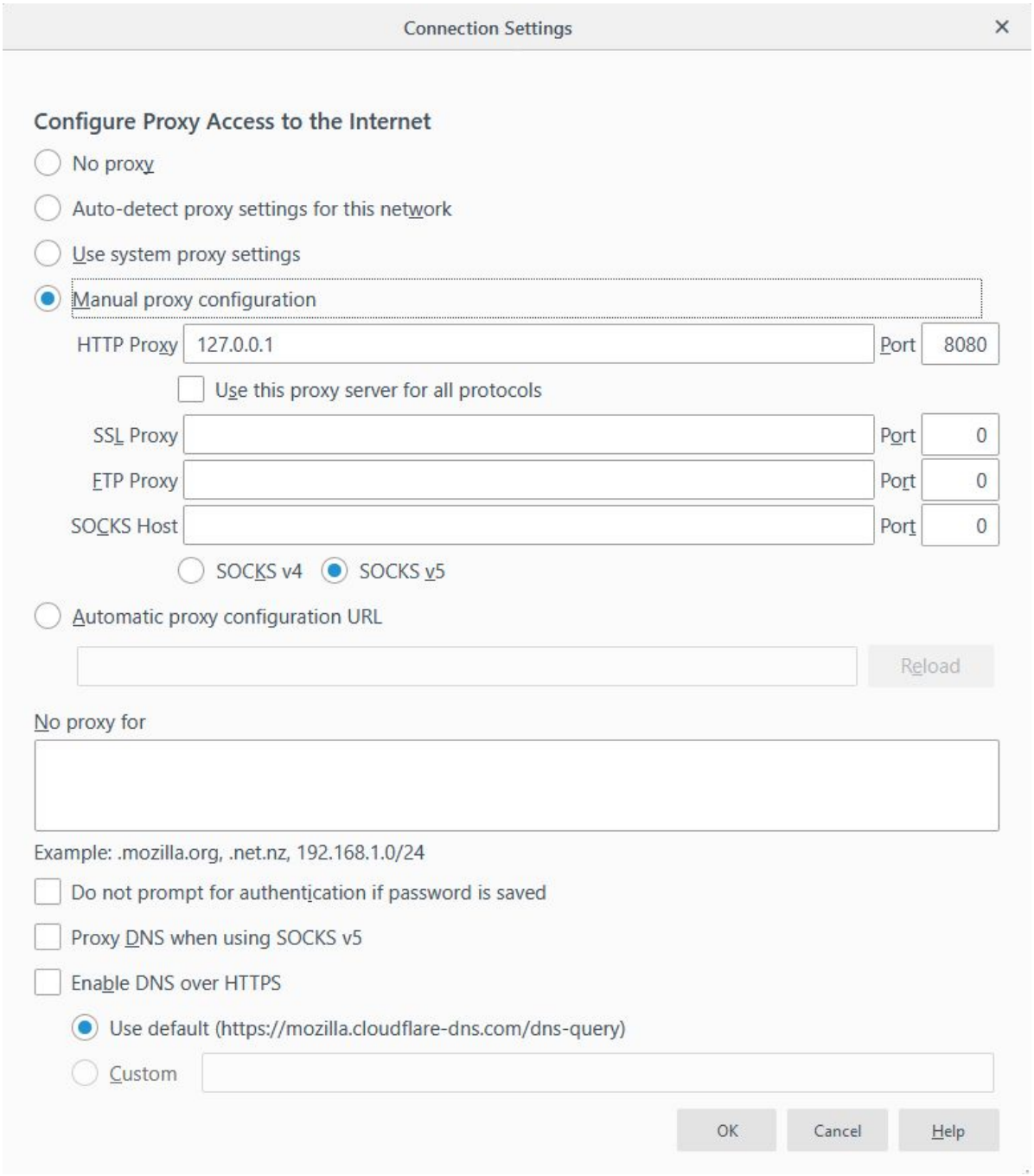
URL: about:preferences



Step 2: Scroll down to the bottom of the page and click on “Settings” button under “Network Settings” section.

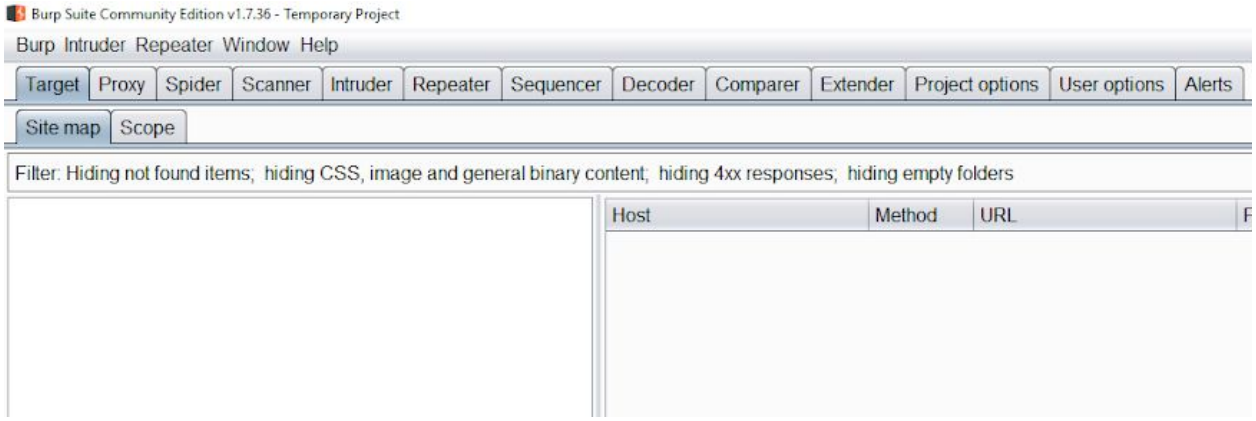


Step 3: Enter “127.0.0.1” and “8080” in “HTTP Proxy” textbox and “Port” textbox respectively.

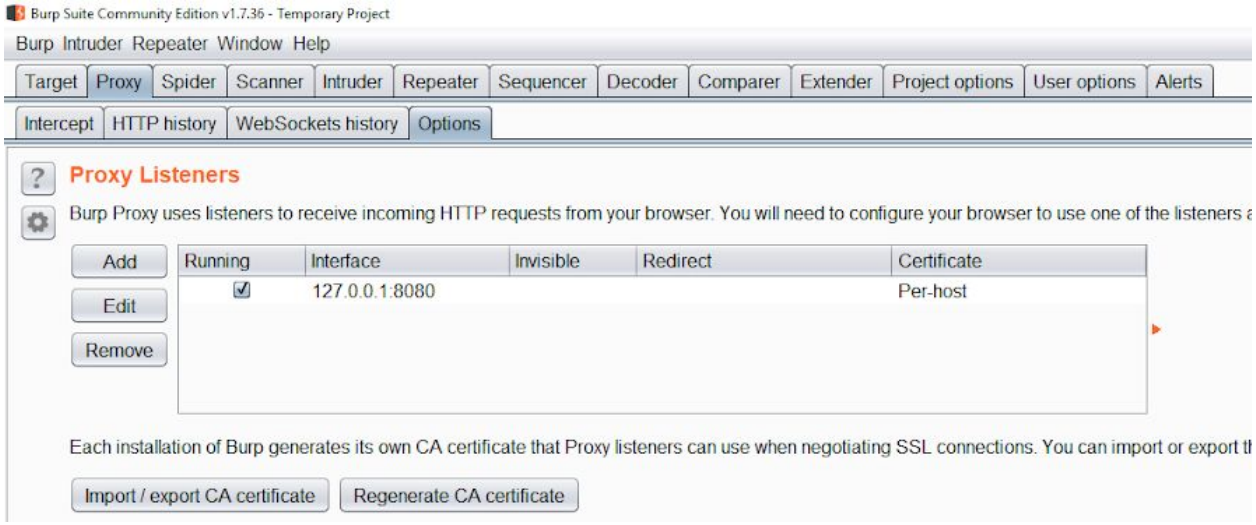


Click on the OK button.

Step 4: Start Burp suite.



Step 5: Navigate to “Options” tab under “Proxy” tab and verify that the “running” checkbox is selected for the interface “127.0.0.1:8080”.



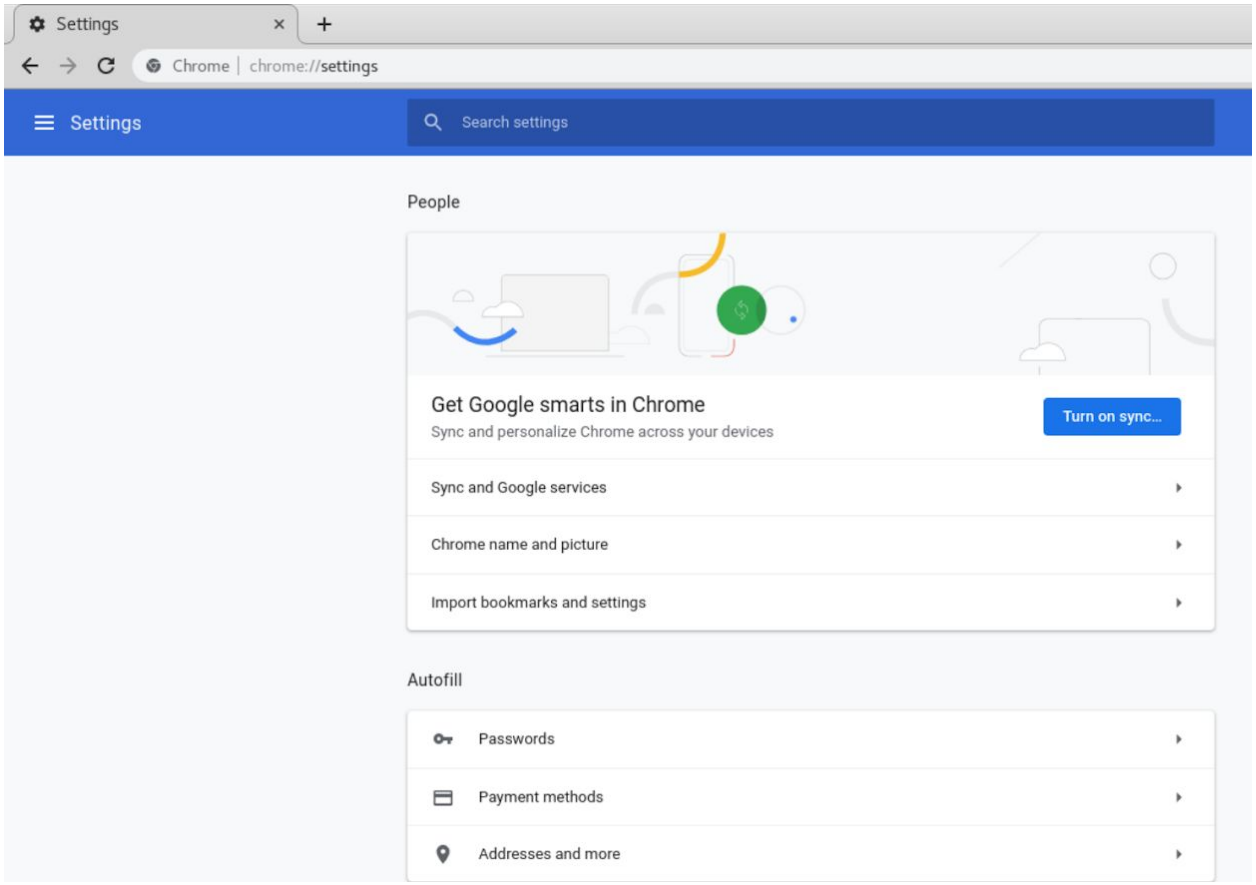
All the HTTP request made by Mozilla Firefox will be intercepted by Burp Suite.

Appendix B

B.1 Google Chrome with Burp Suite (Kali OS)

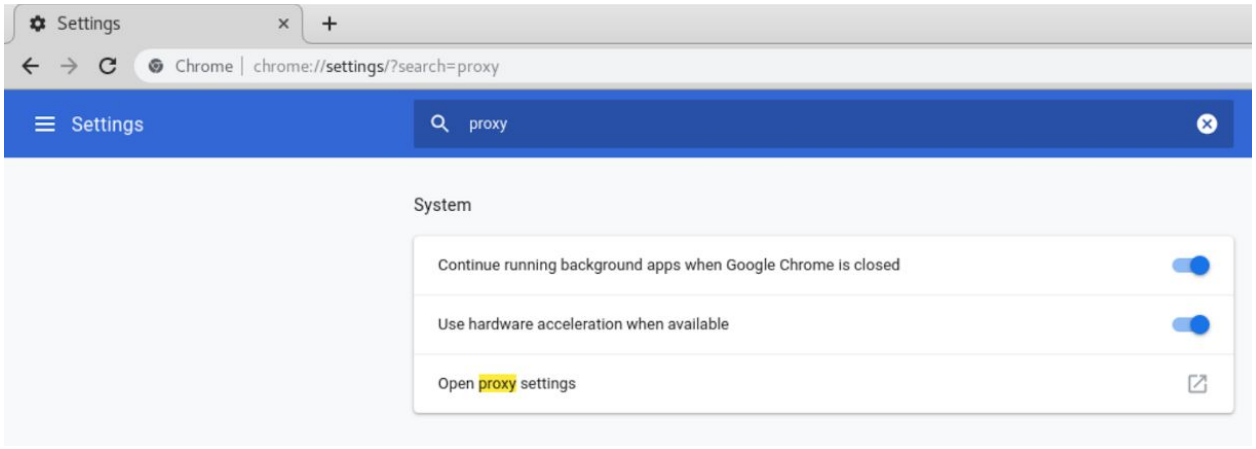
Step 1: Open Google Chrome and navigate to the URL given below.

URL: chrome://settings

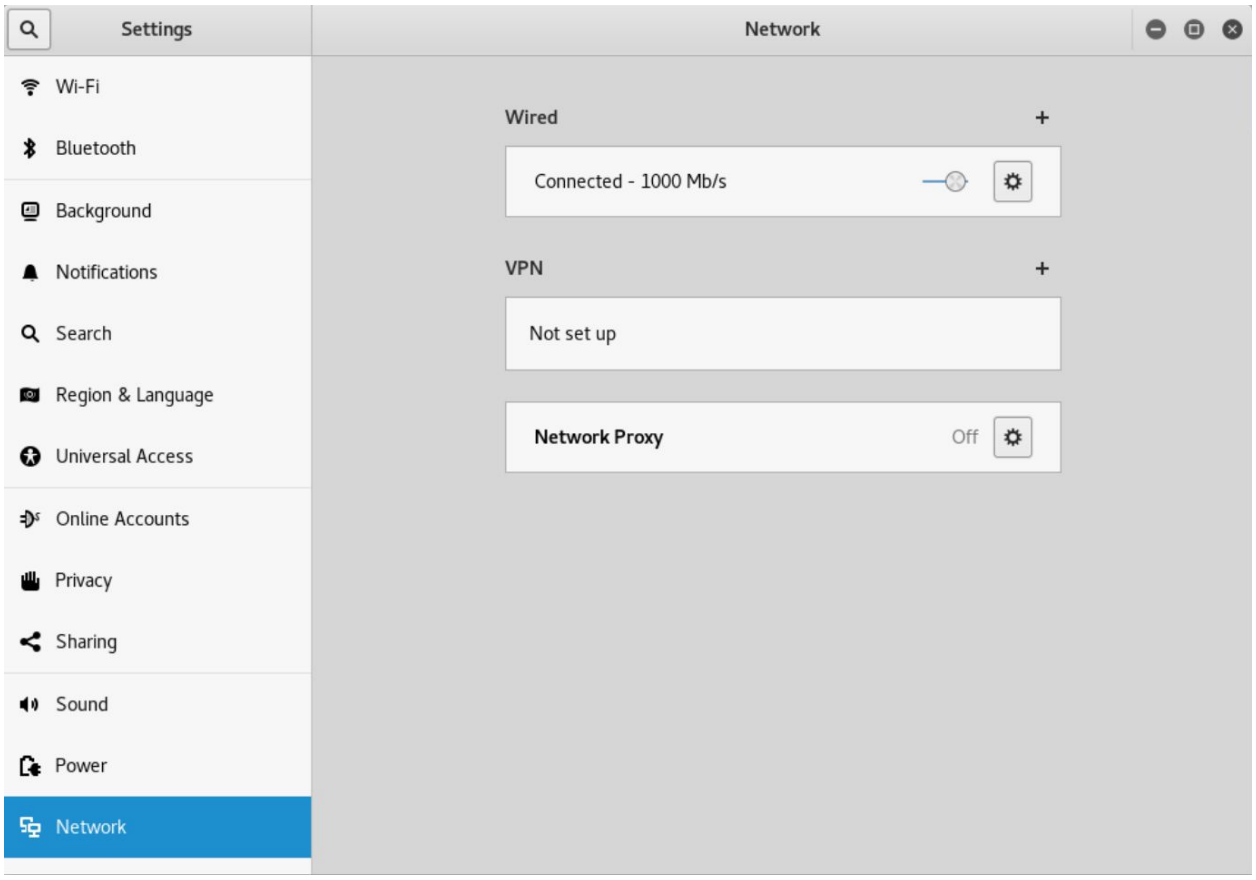


Google Chrome Settings page will appear.

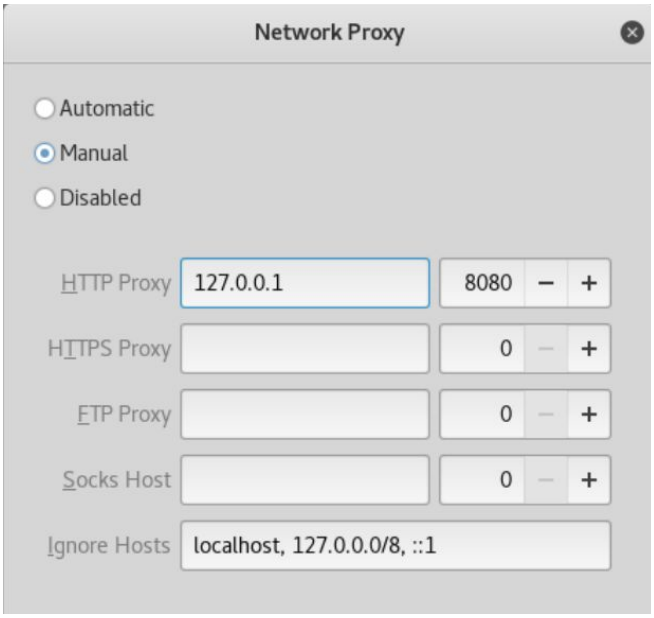
Step 2: Search for “proxy” in the search box.



Step 3: Upon clicking on “Open proxy settings”, The “Networks” settings window will appear. Click on Network Proxy option.

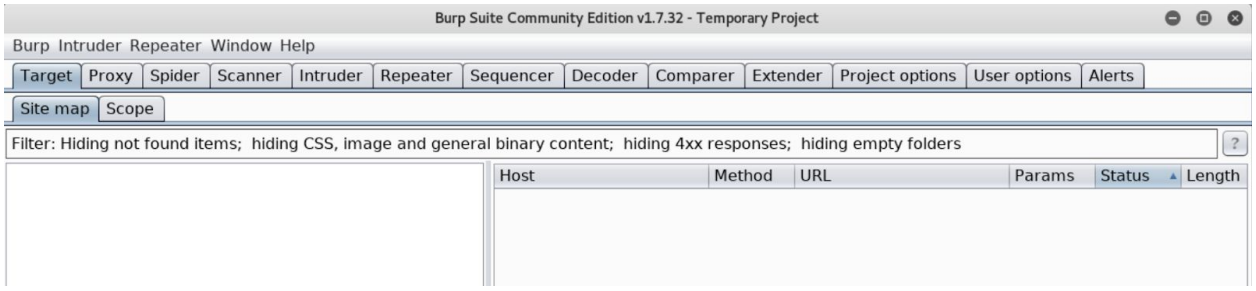


Step 4: Enter “127.0.0.1” in “HTTP Proxy” textbox and enter 8080 as port.

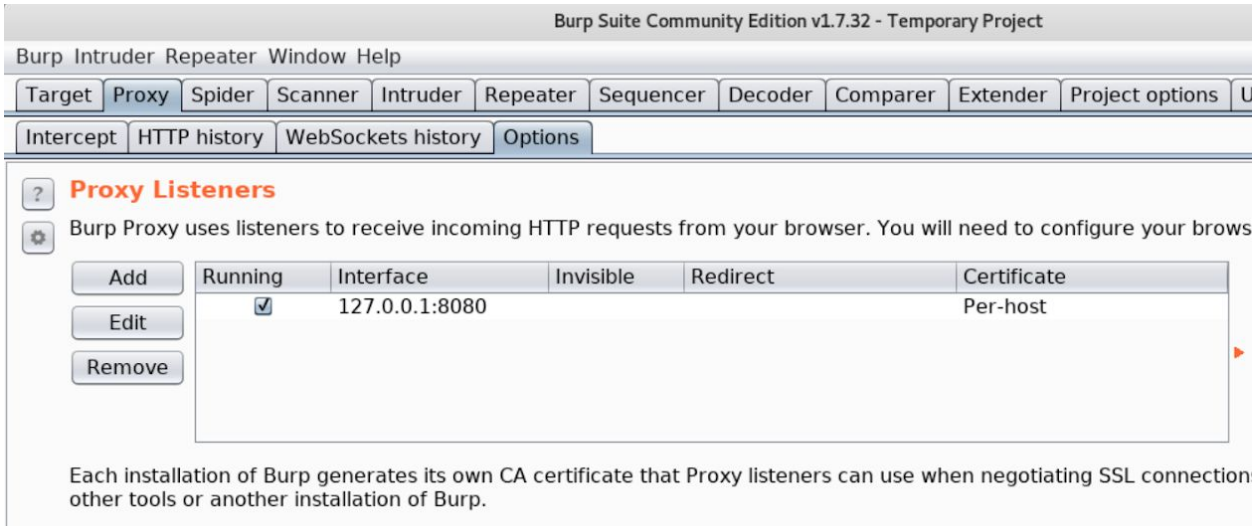


Close the dialog box.

Step 5: Start Burp suite.



Step 6: Navigate to “Options” tab under “Proxy” tab and verify that the “running” checkbox is selected for the interface “127.0.0.1:8080”.

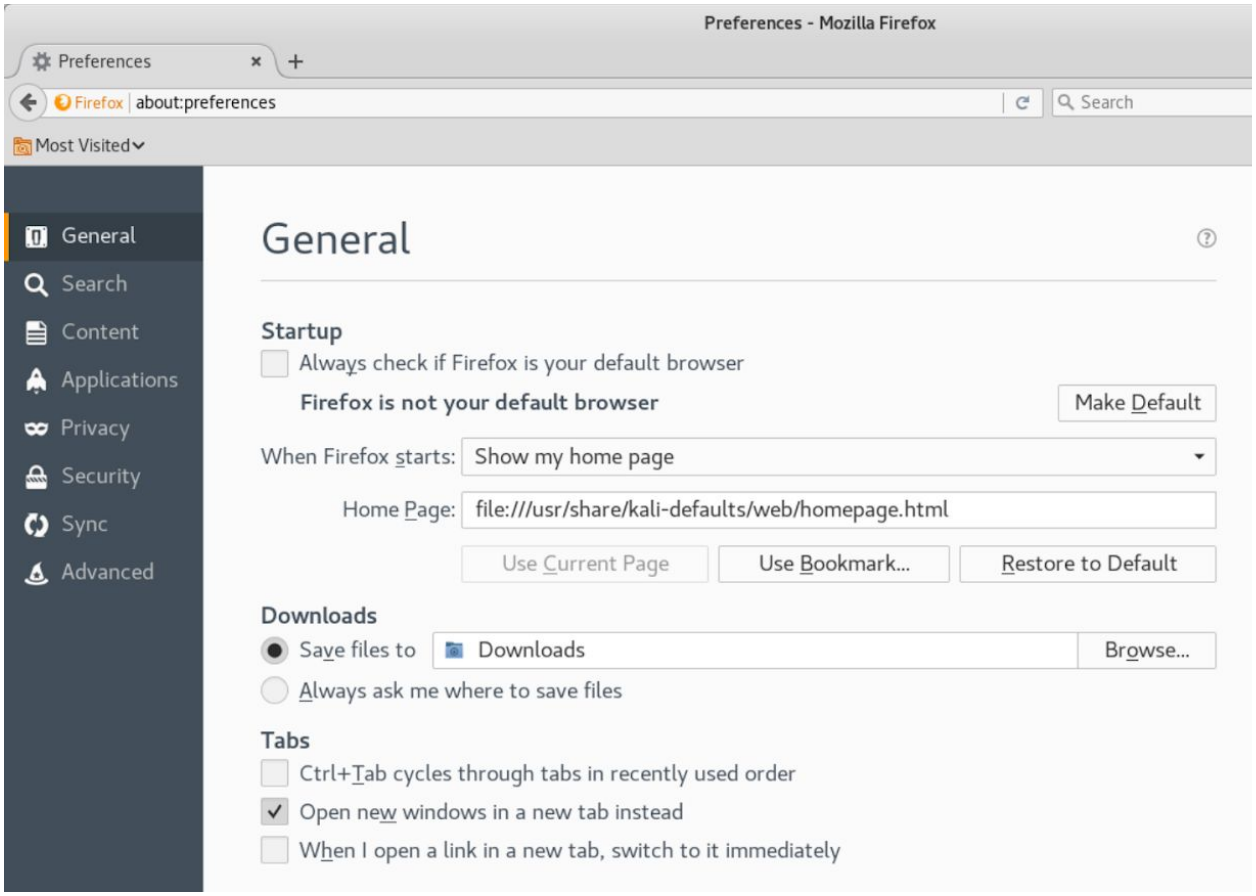


All the HTTP/HTTPS request made by Google Chrome will be intercepted by Burp Suite.

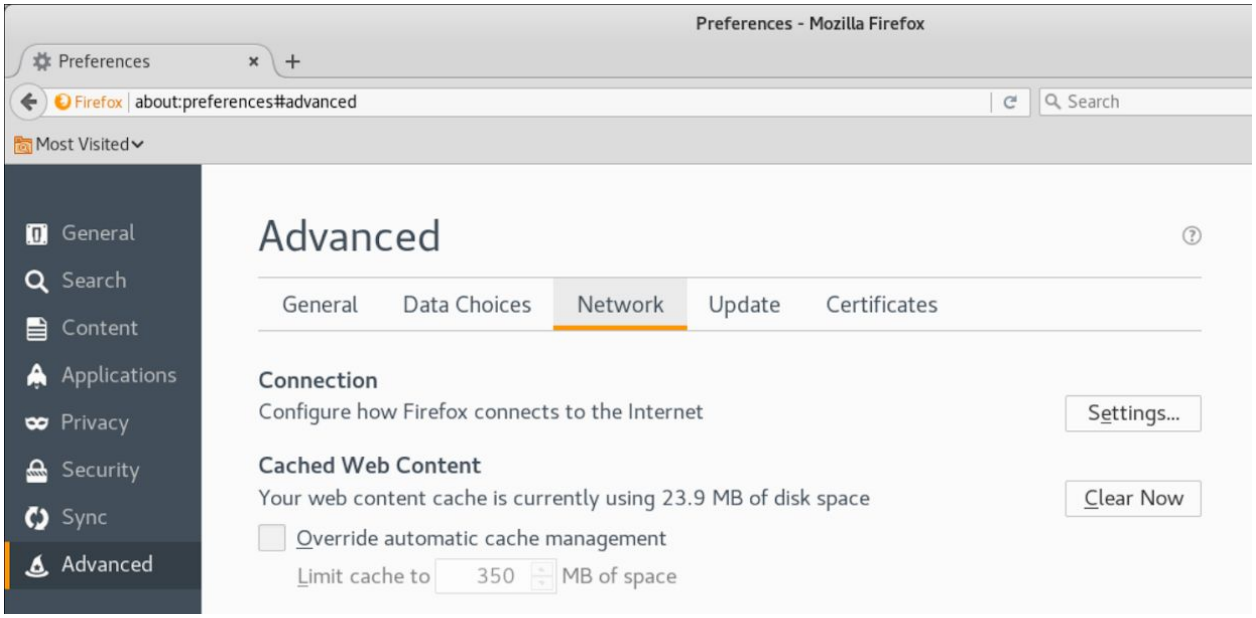
B.2 Mozilla Firefox with burp suite (Kali OS)

Step 1: Open Mozilla Firefox and navigate to the URL given below.

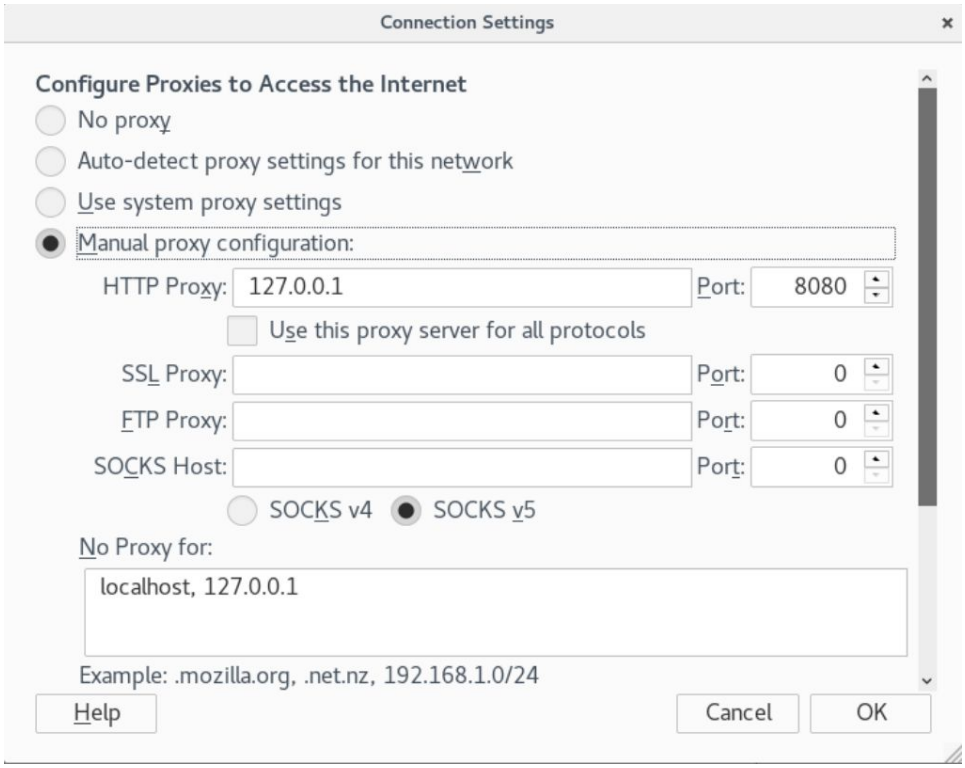
URL: about:preferences



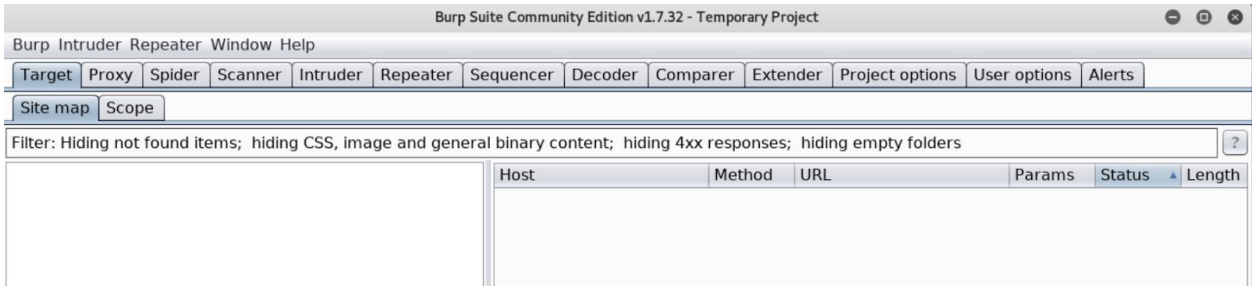
Step 2: Click on “Advanced” tab on the left panel and then click on “Settings” button under “Network” tab.



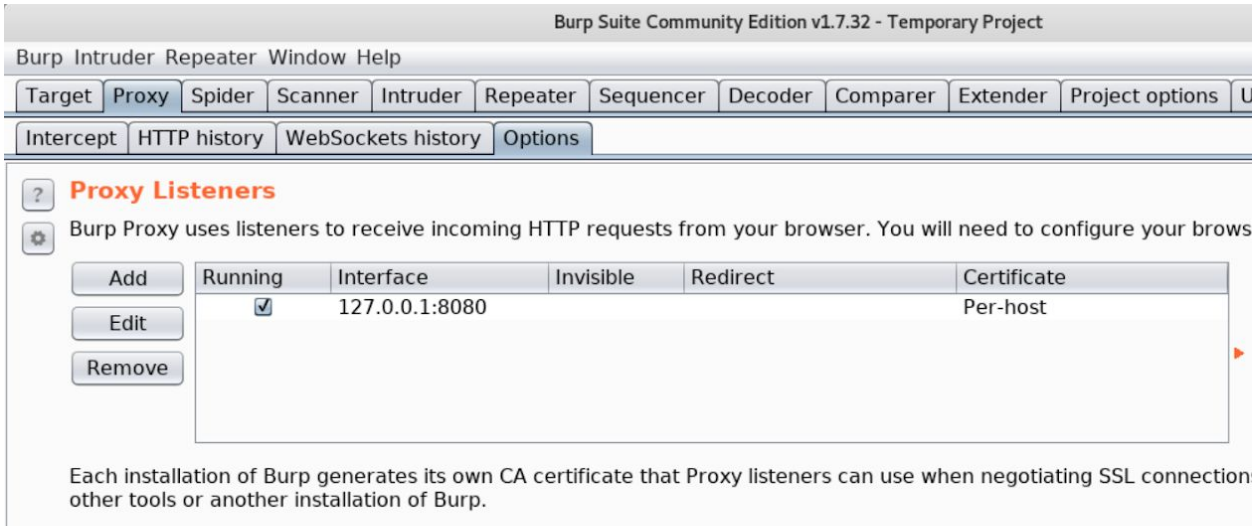
Step 3: Enter “127.0.0.1” and “8080” in “HTTP Proxy” textbox and “Port” textbox respectively.



Step 4: Start Burp suite.



Step 5: Navigate to “Options” tab under “Proxy” tab and verify that the “running” checkbox is selected for the interface “127.0.0.1:8080”.



All the HTTP request made by Mozilla Firefox will be intercepted by Burp Suite.

Appendix C

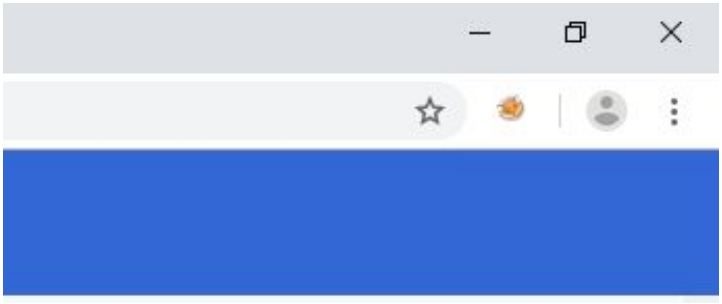
C.1 FoxyProxy on Google Chrome with Burp Suite

Step 1: Installing FoxyProxy.

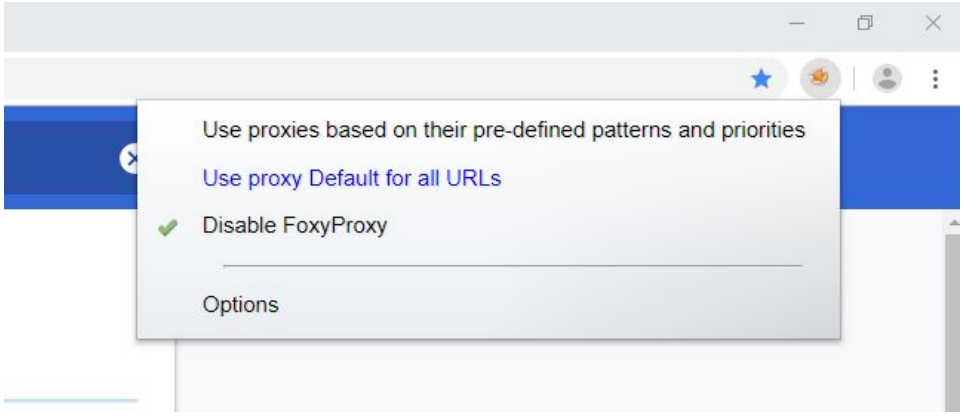
FoxyProxy Standard plugin for Google Chrome can be installed from the URL given below:

URL:
https://chrome.google.com/webstore/detail/foxyproxy-standard/gcknhkkoolaabfmlnjonogaaifnjlfnp?hl=en

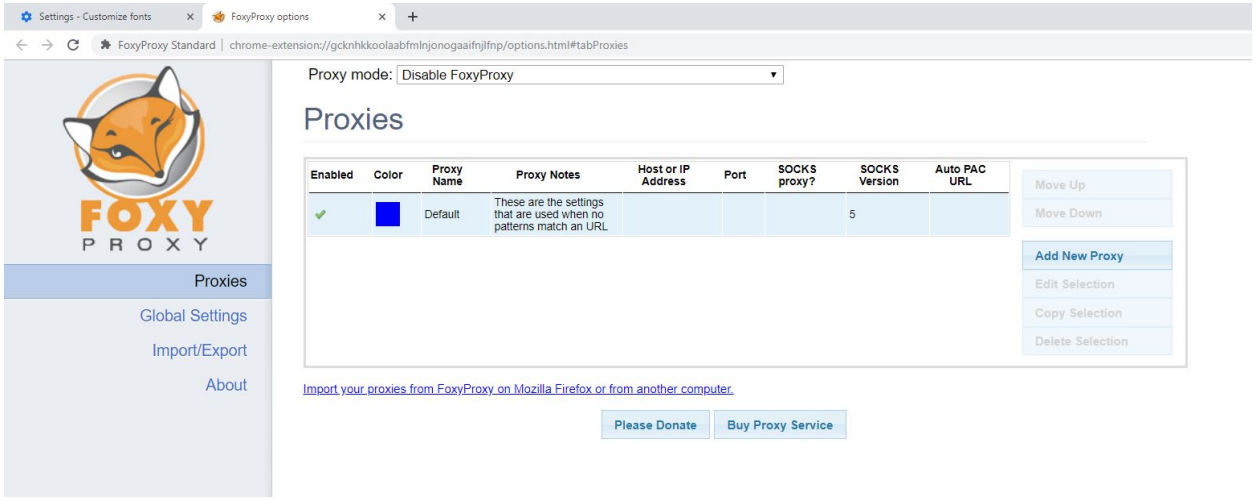
After installing FoxyProxy, a small fox icon will appear on the right side of the address bar.



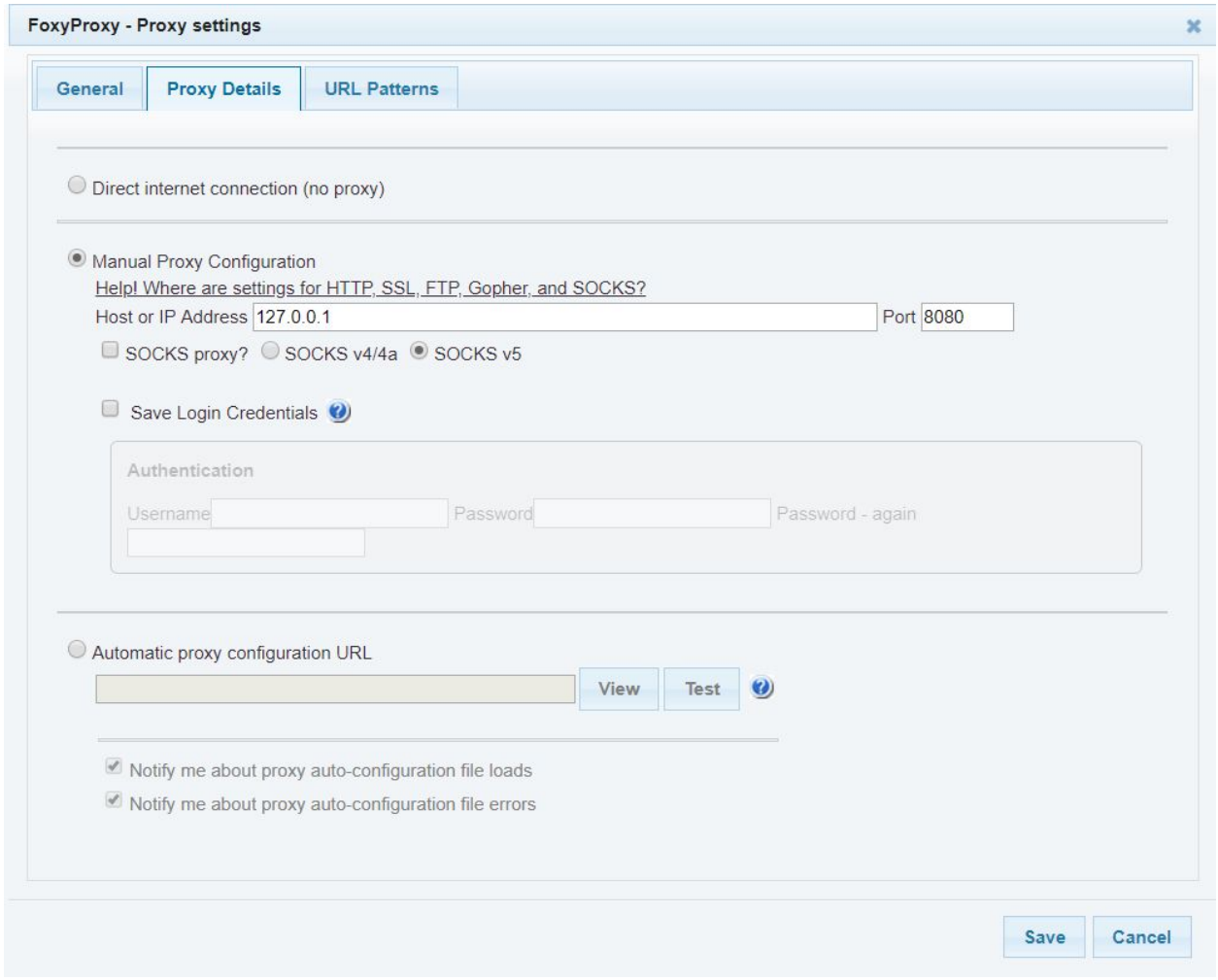
Step 2: Click on the FoxyProxy icon and click on Options.



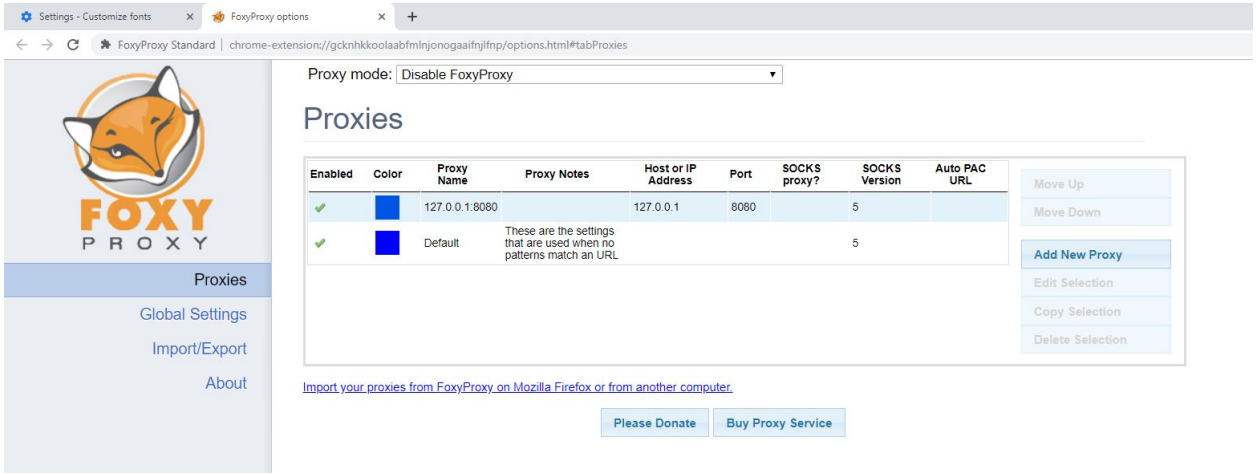
Step 3: Click on the “Add New Proxy” Button.



Step 4: Enter “127.0.0.1” in “Host or IP Address” textbox and enter “8080” in Port textbox.



Click on the Save button.



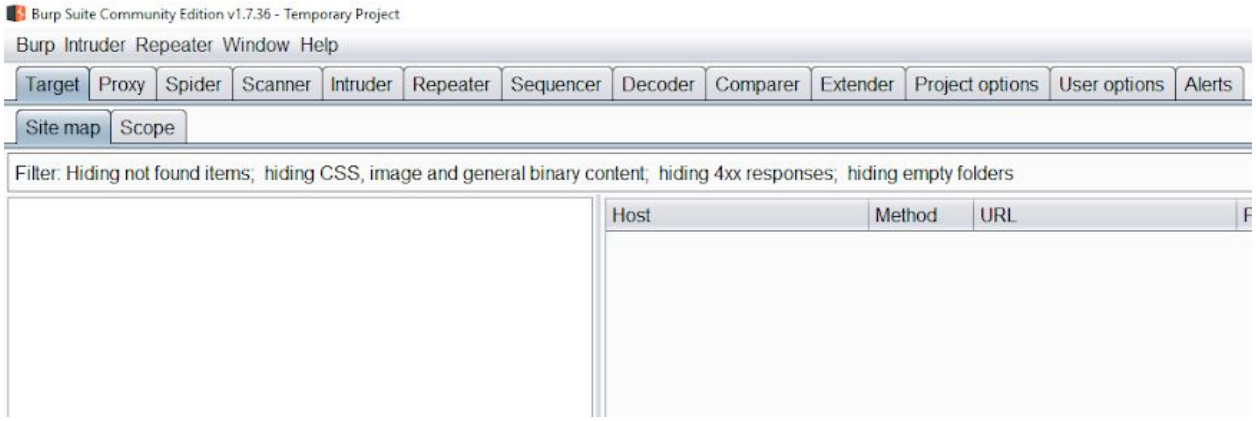
The configured proxy will appear in the proxies table.

Step 5: Enable the proxy.

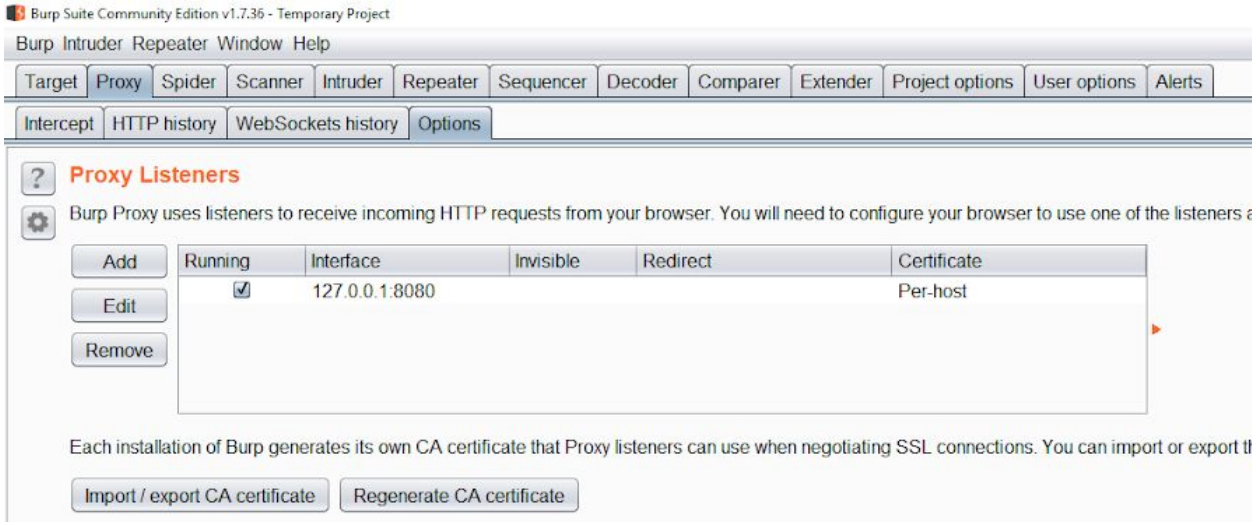
Click on the FoxyProxy icon and select the option “Use proxy 127.0.0.1:8080 for all URLs”

The FoxyProxy icon will change its color (In this case it is blue).

Step 6: Start Burp suite.



Step 7: Navigate to “Options” tab under “Proxy” tab and verify that the “running” checkbox is selected for the interface “127.0.0.1:8080”.



All the HTTP/HTTPS request made by Google Chrome will be intercepted by Burp Suite.

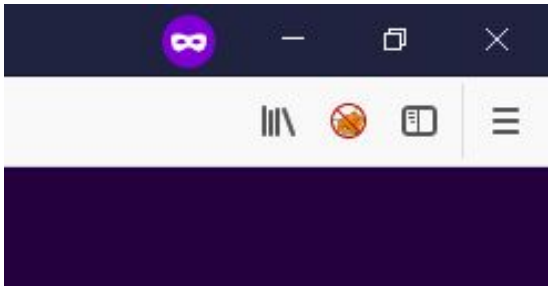
C.2 FoxyProxy on Mozilla Firefox with Burp Suite

Step 1: Installing FoxyProxy.

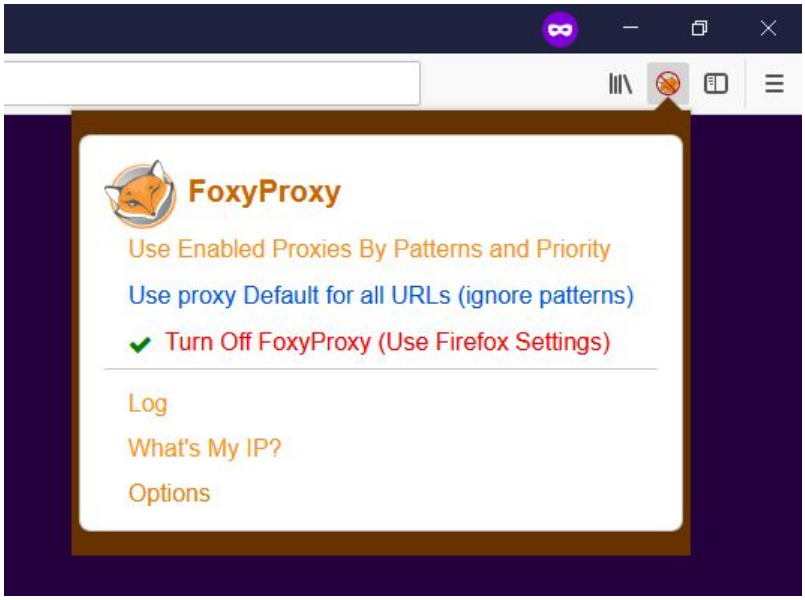
FoxyProxy Standard plugin for Mozilla Firefox can be installed from the URL given below:

URL: https://addons.mozilla.org/en-US/firefox/addon/foxyproxy-standard/

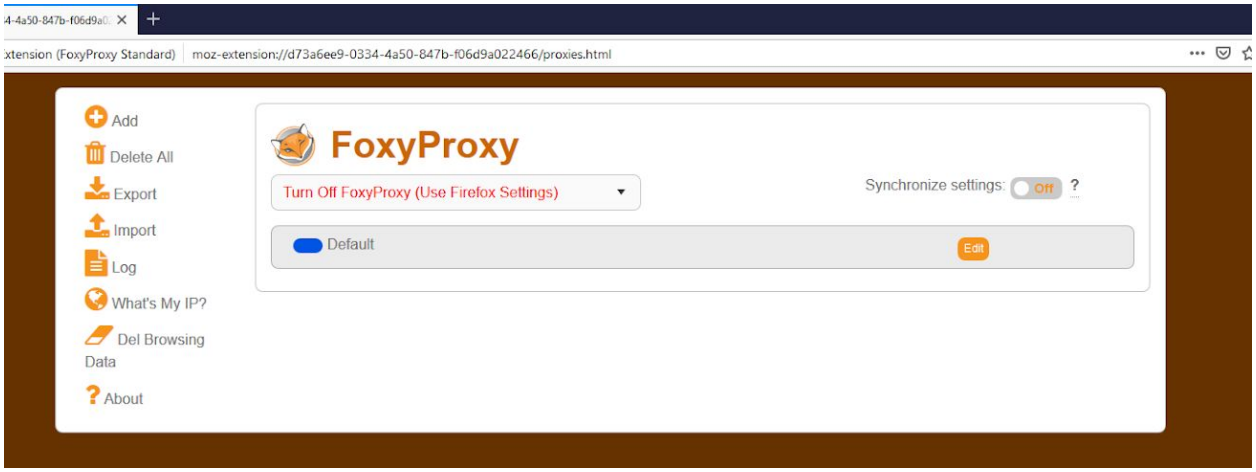
After installing FoxyProxy, a small fox icon will appear on the right side of the address bar.



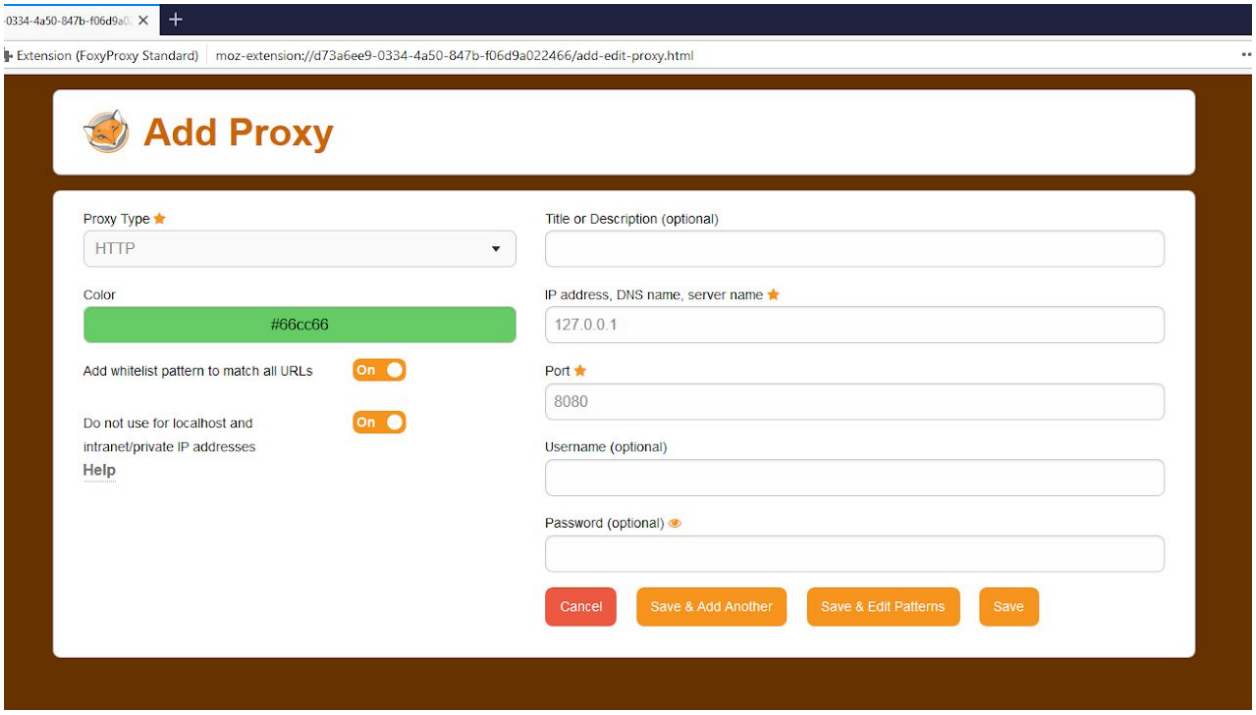
Step 2: Click on the FoxyProxy icon and click on Options.



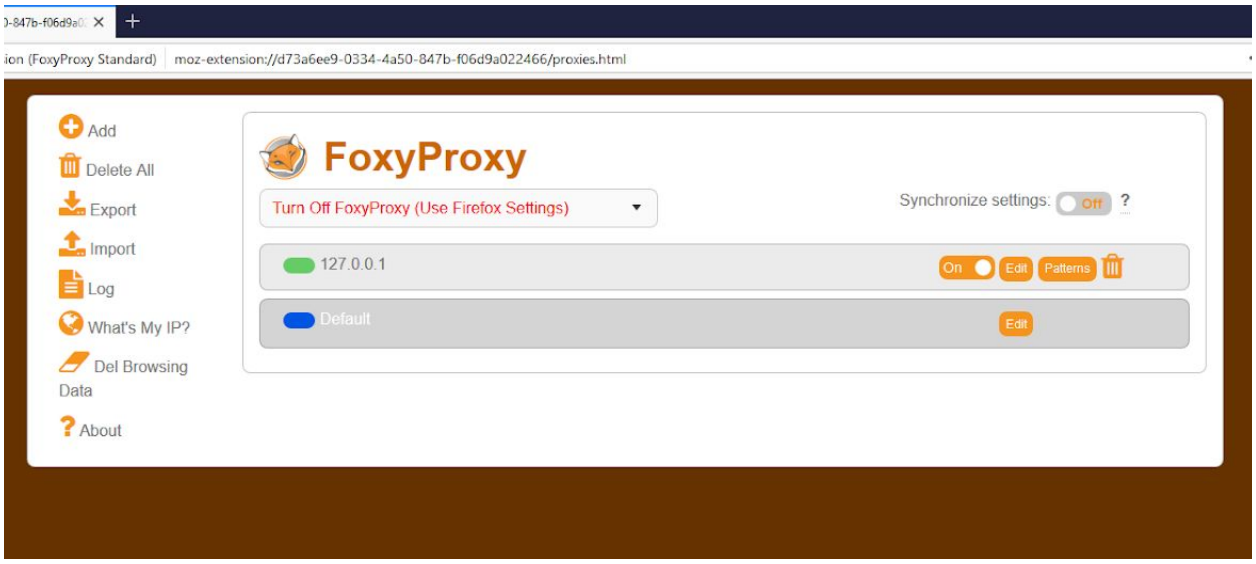
Step 3: Click on the add button on the left panel



Step 4: Enter “127.0.0.1” in “IP Address, DNS name, server name” textbox and enter “8080” in Port textbox.



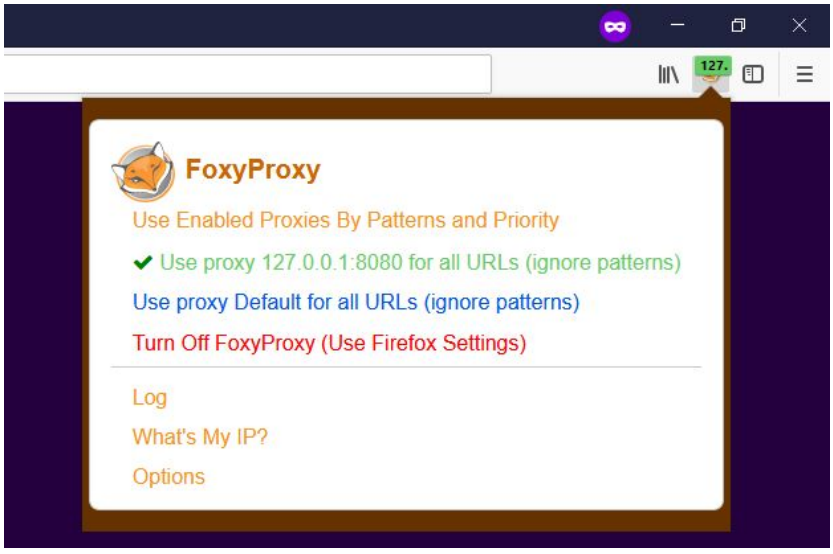
Click on the Save button.



The proxy will appear in the proxies table.

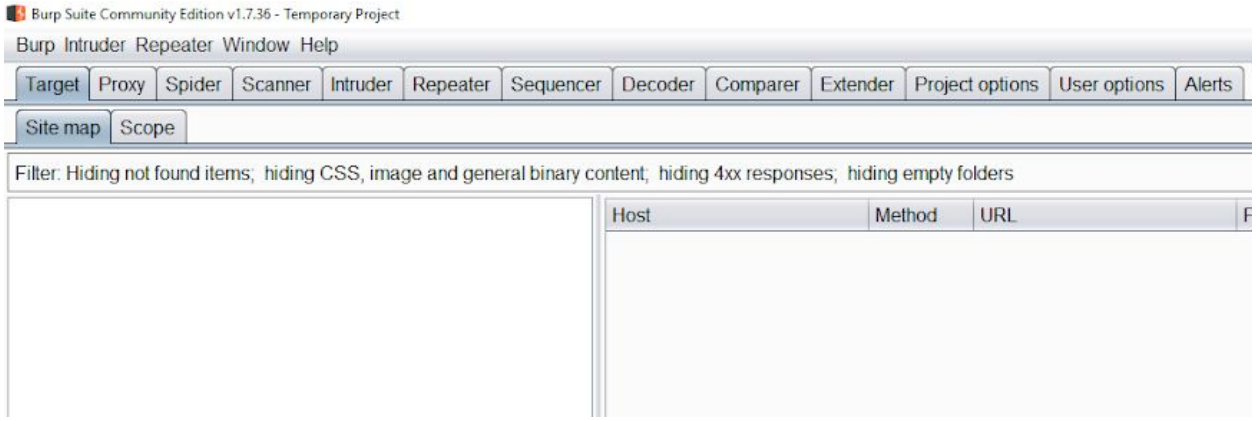
Step 5: Enable the proxy.

Click on the FoxyProxy icon and select the option “Use proxy 127.0.0.1:8080 for all URLs (ignore patterns)”

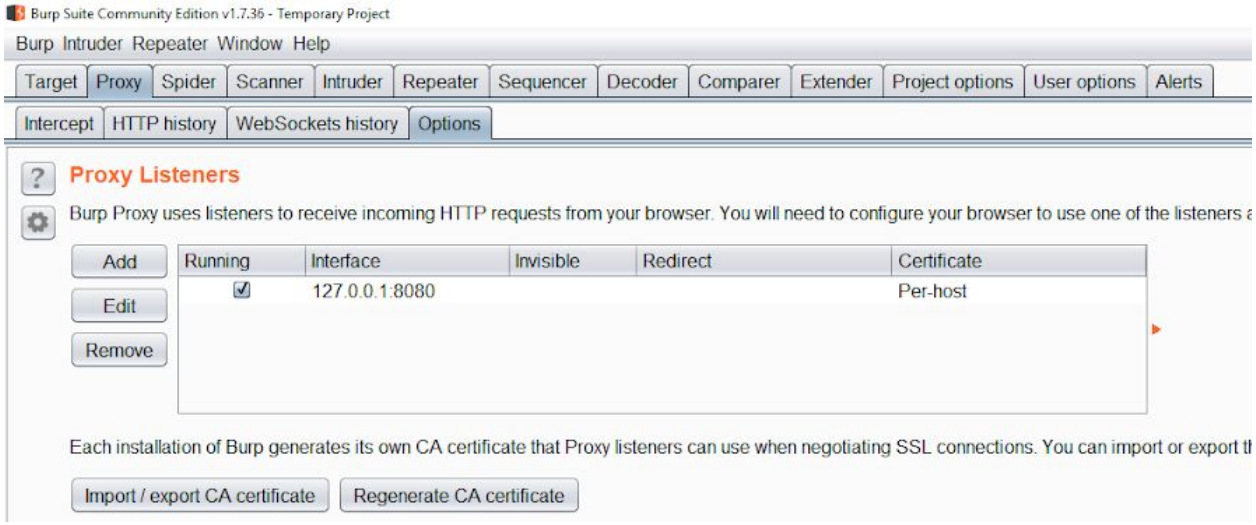


The FoxyProxy icon will change its color (In this case it is green).

Step 6: Start Burp suite.



Step 7: Navigate to “Options” tab under “Proxy” tab and verify that the “running” checkbox is selected for the interface “127.0.0.1:8080”



All the HTTP/HTTPS request made by Mozilla Firefox will be intercepted by Burp Suite.