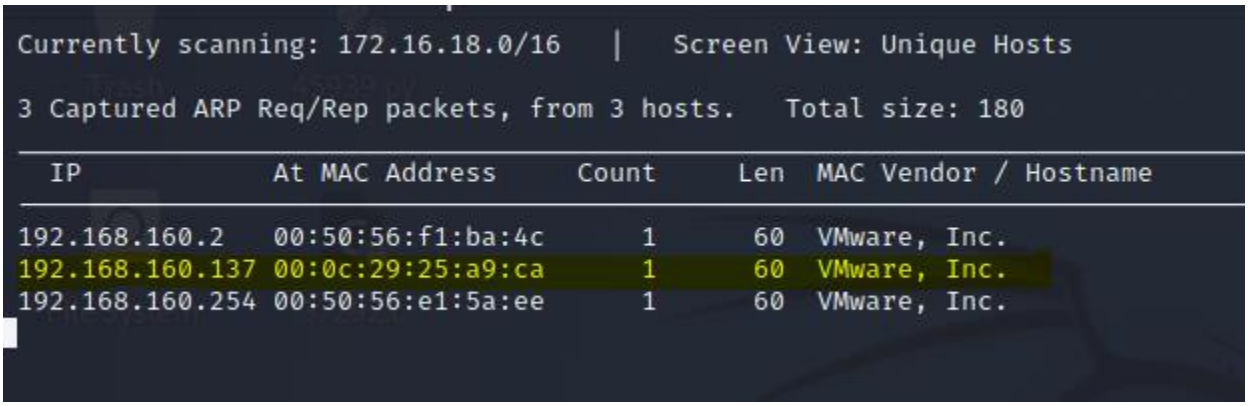
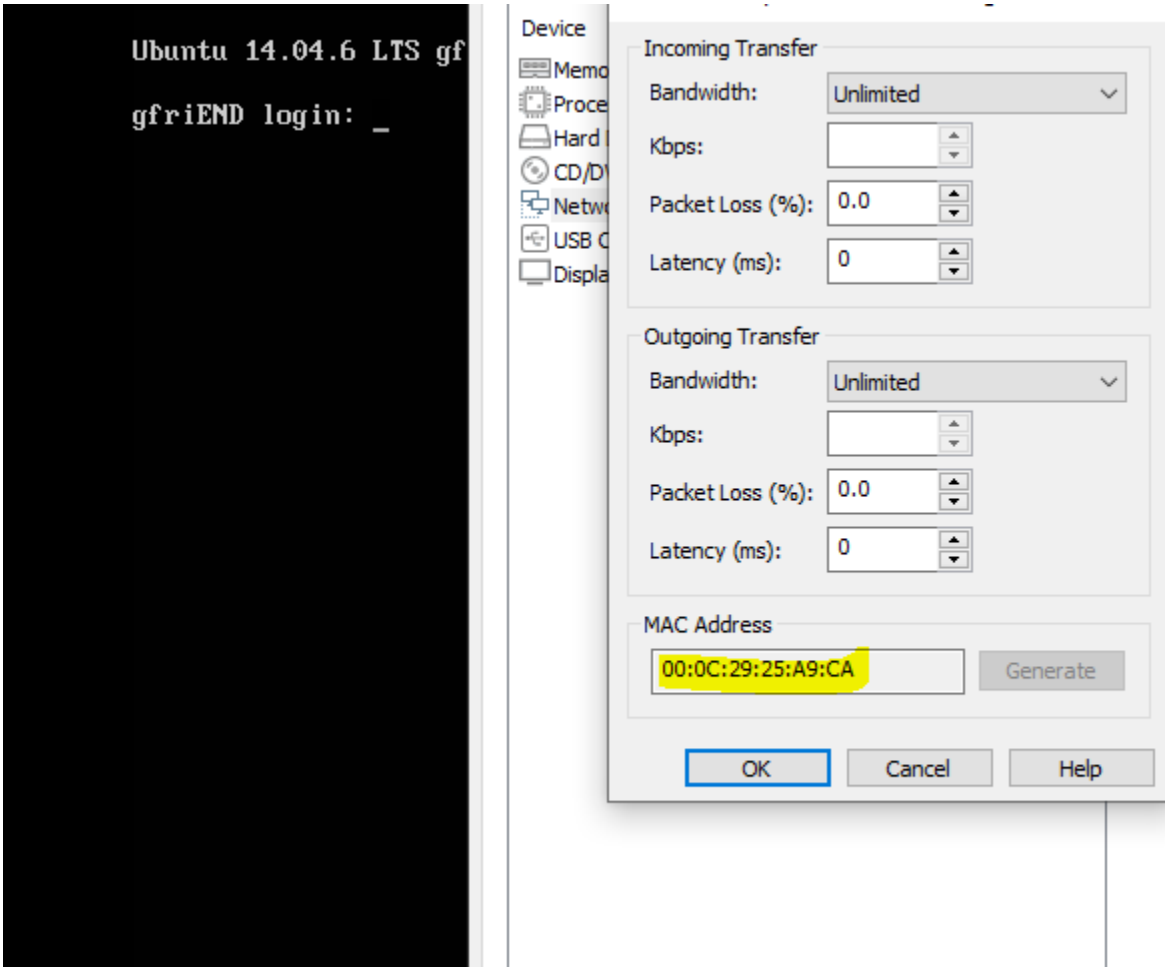
PORT AND SERVICE DISCOVERY

First I collected the ip address of the vulnerable machine using netdiscover. I confirmed the ip addressed by matching the mac address given by the VM.



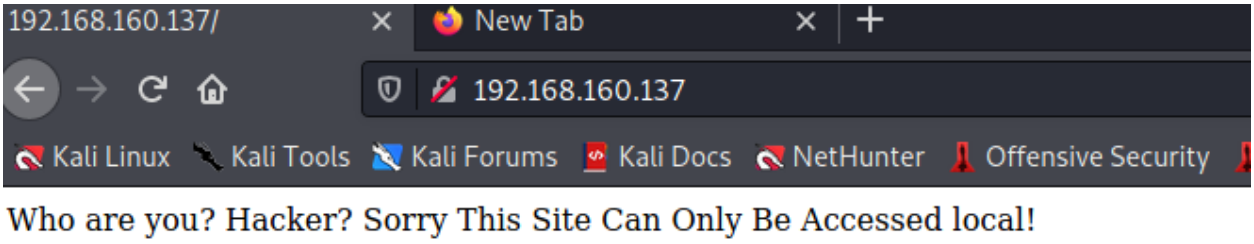


Then I did a nmap scan to find out the open ports and the running services on those ports.

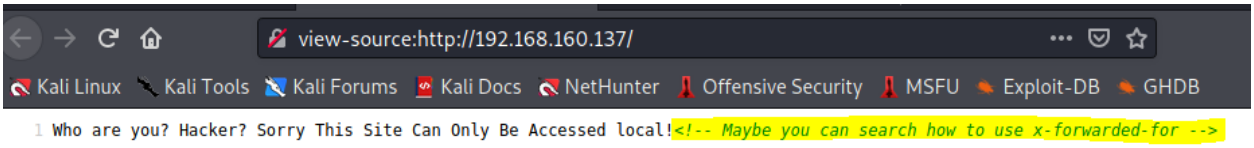
```
┌──(root💀kali)-[/home/kali]
└─# nmap -sV -sC -A -p- 192.168.160.137
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-07 05:01 EST
Nmap scan report for 192.168.160.137
Host is up (0.0011s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux
| ssh-hostkey:
|   1024 57:e1:56:58:46:04:33:56:3d:c3:4b:a7:93:ee:23:16 (DSA)
|   2048 3b:26:4d:e4:a0:3b:f8:75:d9:6e:15:55:82:8c:71:97 (RSA)
|   256 8f:48:97:9b:55:11:5b:f1:6c:1d:b3:4a:bc:36:bd:b0 (ECDSA)
|_  256 d0:c3:02:a1:c4:c2:a8:ac:3b:84:ae:8f:e5:79:66:76 (ED25519)
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 00:0C:29:25:A9:CA (VMware)
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   1.15 ms 192.168.160.137

OS and Service detection performed. Please report any incorrect resul
Nmap done: 1 IP address (1 host up) scanned in 28.39 seconds
```

HTTP ENUMERATION

Since http port was open I looked for the website.

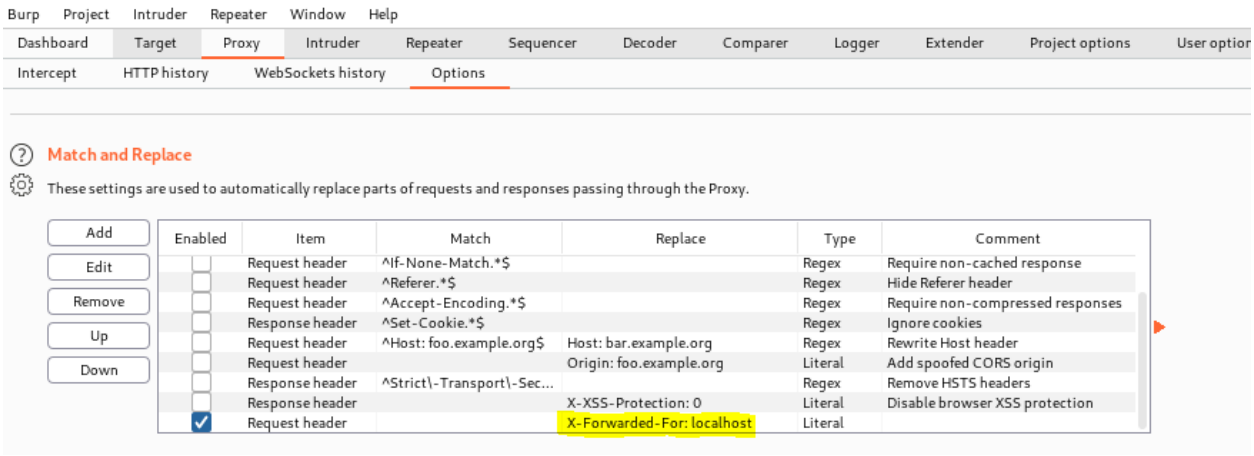


I found nothing interesting there. So I looked at the page source to find some clues.



I found a message telling me to use x-forwarded-for.

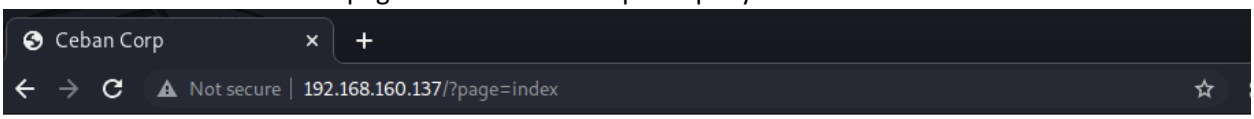
I added a new request header on burpsuite.



Then I intercepted the request and forwarded it. I looked at the http history and found an index file.

#	Host	Method	URL	Params	Edited	Status	Length	M
1	http://192.168.160.137	GET	/			200	332	scr
2	http://192.168.160.137	GET	/favicon.ico			404	468	HT
3	http://192.168.160.137	GET	/			302	213	HT
4	http://192.168.160.137	GET	/?page=index	✓		200	1083	HT

I was able to access the web page for the Ceban Corp company.

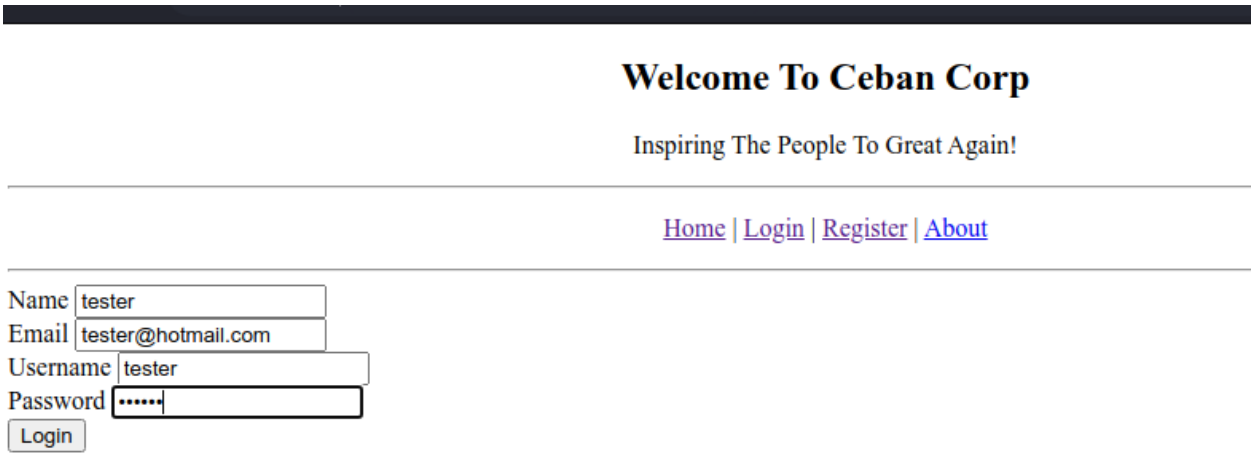


Welcome To Ceban Corp

Inspiring The People To Great Again!

Home | Login | Register | About

I didn't know what to do further so I decided to register a test account so I can use that account to test further.



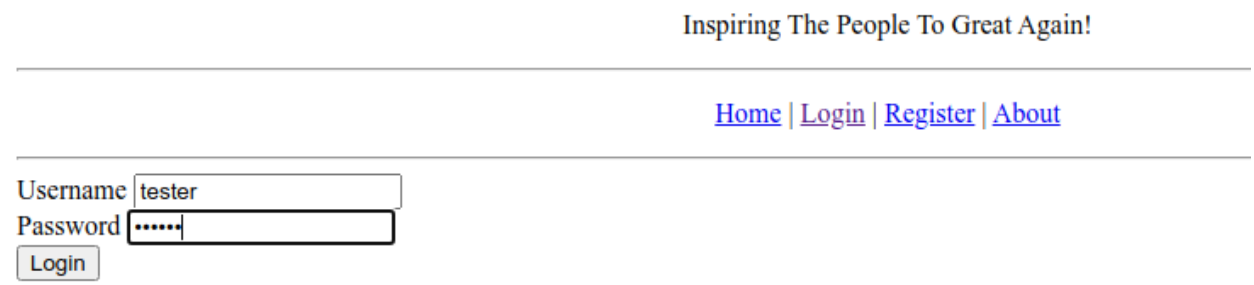
Welcome To Ceban Corp

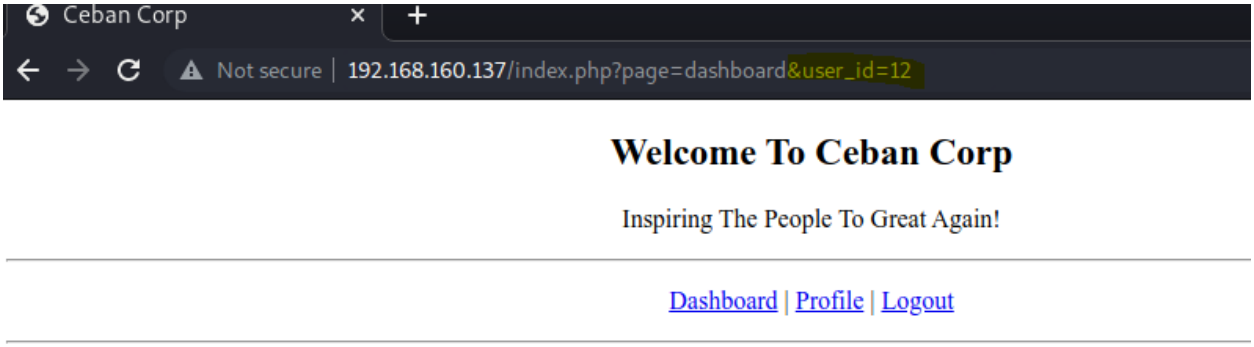
Inspiring The People To Great Again!

Home | Login | Register | About

Name tester
Email tester@hotmail.com
Username tester
Password ••••••
Login

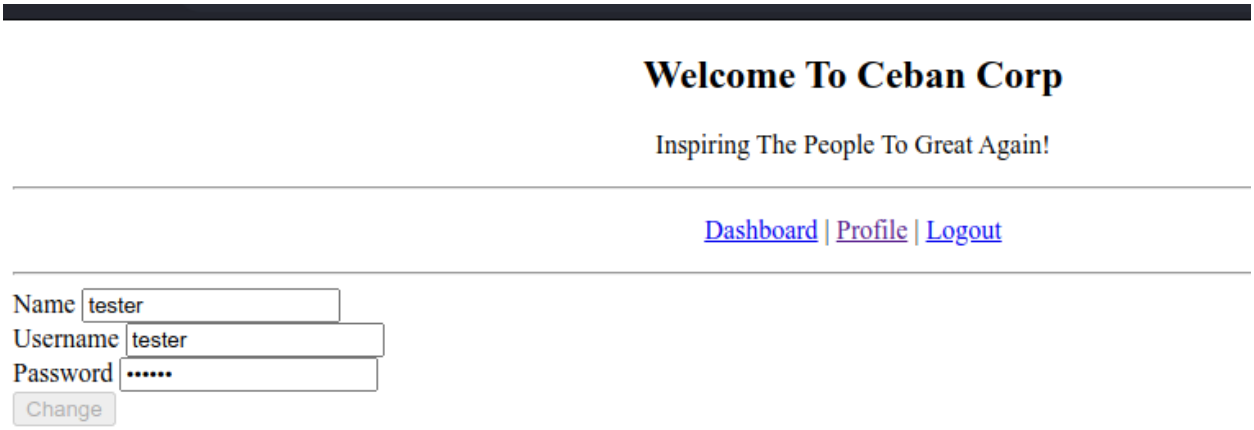
Then I logged in using my test user credentials.



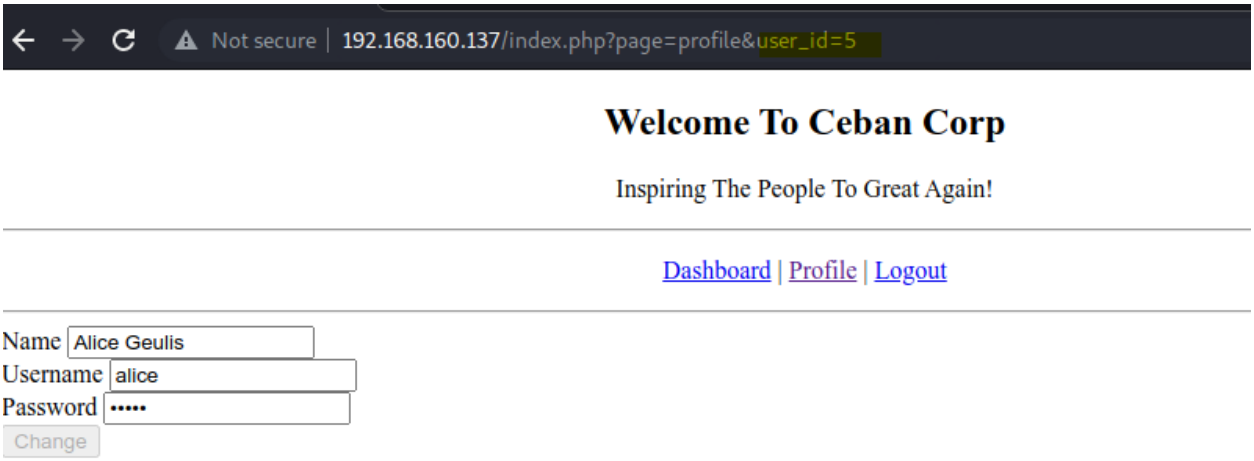


Looked like there is possibility of SQL injection.

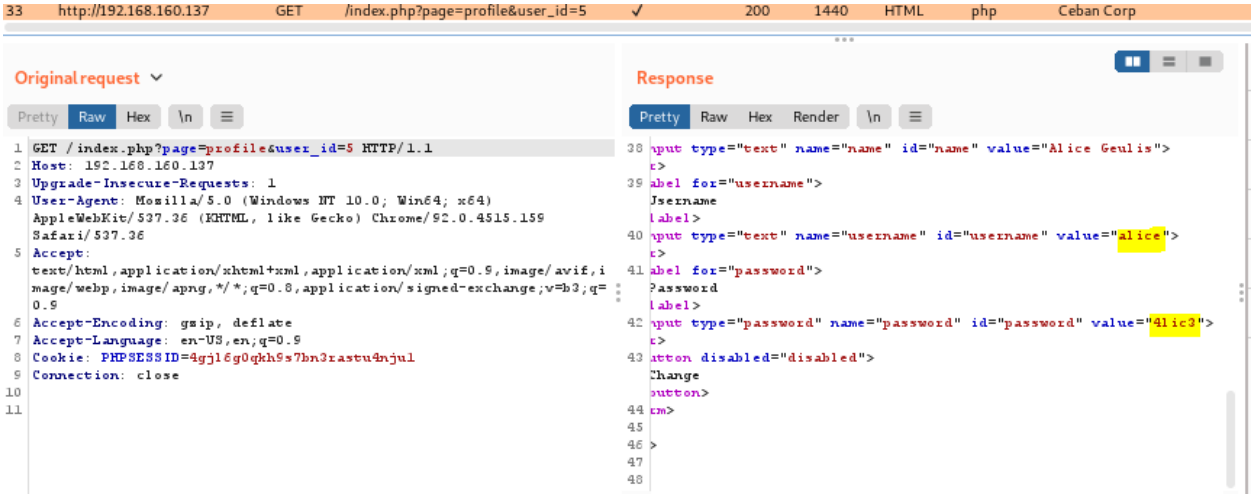
I found something interesting, the profile page as the credentials autofilled. I tried to find other users.



I found alice's account by changing the value of the user_id.



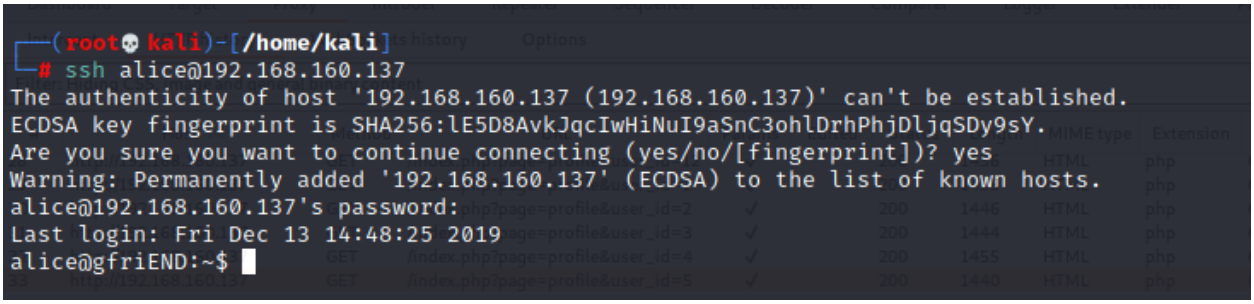
I looked at the burpsuite http history and inspected the response and found alice's password.

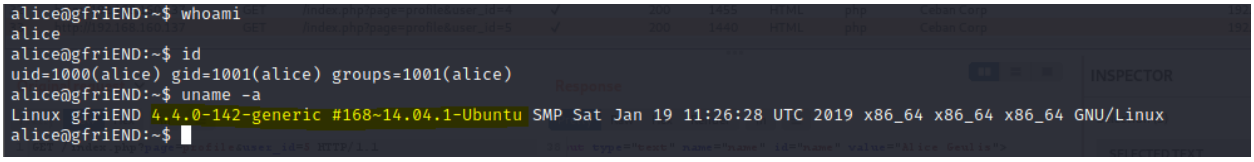


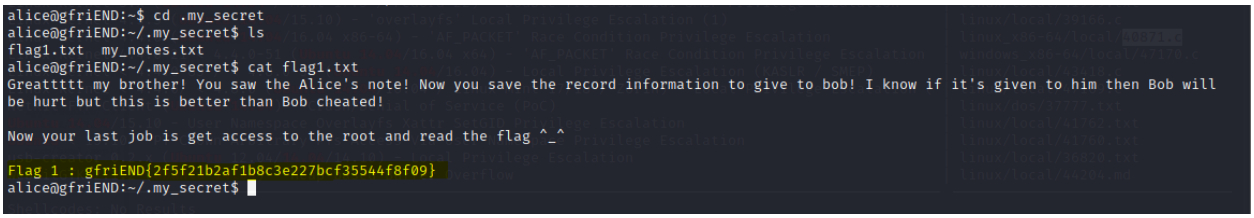
SSH USER ACCESS

I tried to login via ssh using alice's credentials.

I was able to successfully login.



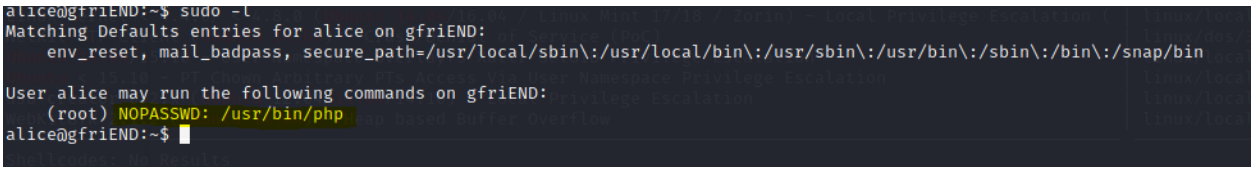




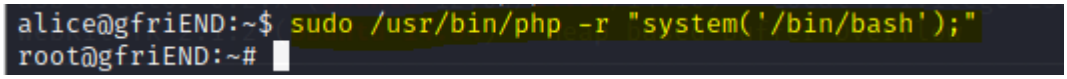
Flag1: gfriEND{2f5f21b2af1b8c3e227bcf35544f8f09}

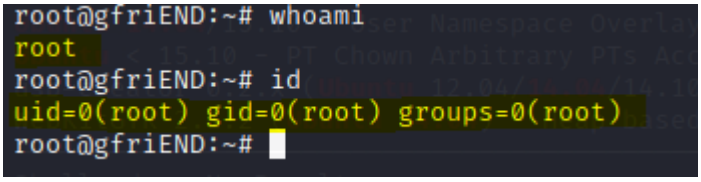
PRIVILEGE ESCALATION

First I looked for sudo rights. I found that alice can run the php program as a sudo user.



So I executed the /bin/bash command using /bin/php.





I was able to access to root finally. Then I looked for the final flag.

Finally I found the flag.

Flag2: gfriEND{56fbeef560930e77ff984b644fde66e7}