IE3092
Information Security Project
3rd Year 2nd Semester

Mr.ROBOT CTF Walkthrough

Submitted to
Sri Lanka Institute of Information Technology

In partial fulfillment of the requirements for the
Bachelor of Science Special Honors Degree in Information Technology

14 / 12 / 2020

Declaration

We certify that this report does not incorporate without acknowledgement, any material previously submitted for a degree or diploma in any university, and to the best of our knowledge and belief it does not contain any material previously published or written by another person, except where due reference is made in text.

- **K.G.S. Dananjay - IT18095104**
- **N.P.N.H. Amarasena - IT18095340**

Contents

Introduction

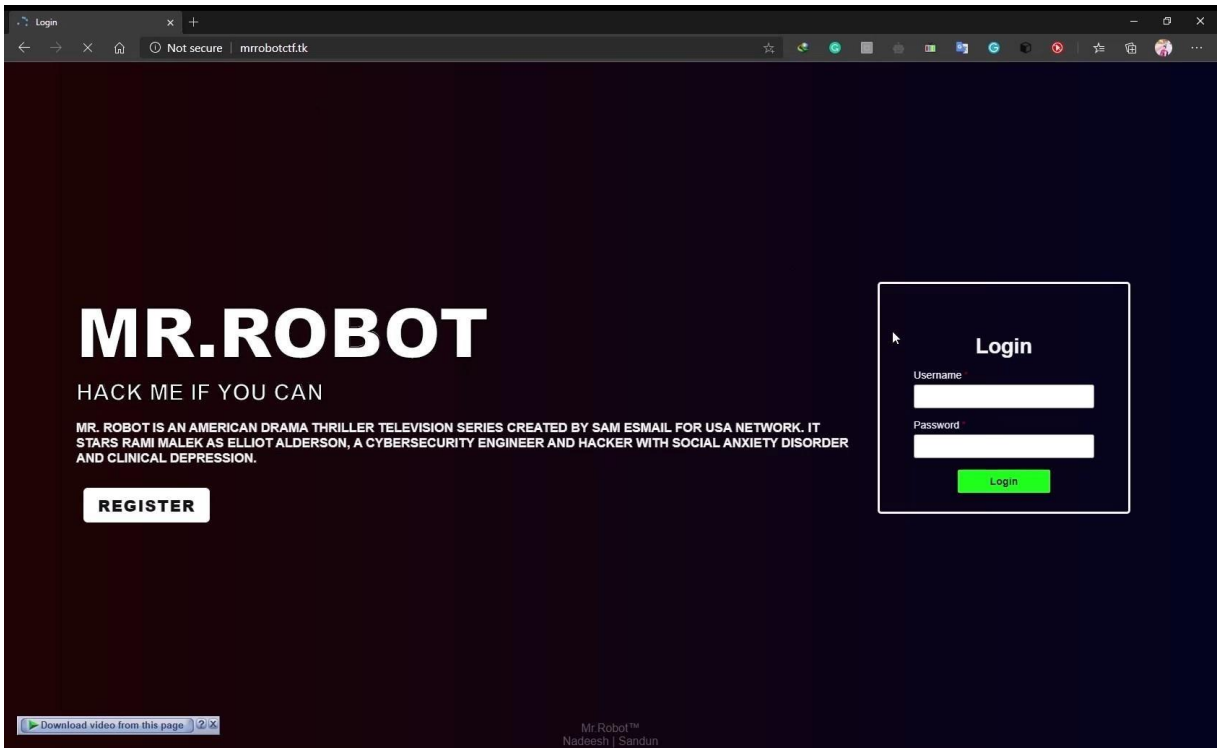
Capture the Flag (CTF) is an event that is usually hosted at information security conferences, including the various events. This event consists of a series of challenges that varies in their degree of difficulty, and that require participants to exercise different skill sets to solve. Once an individual challenge is solved, a “flag” is given to the player and they submit this flag to the CTF server to earn points. Players can be lone wolves who attempt the various challenges by themselves, or they can work with others to attempt to score the highest number of points as a team.

Audience

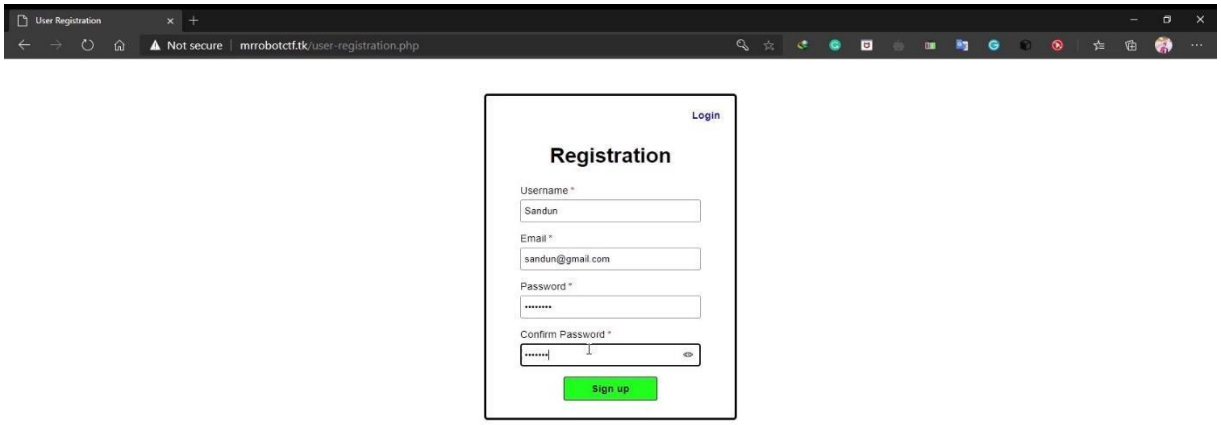
Security Researchers

How to setup?

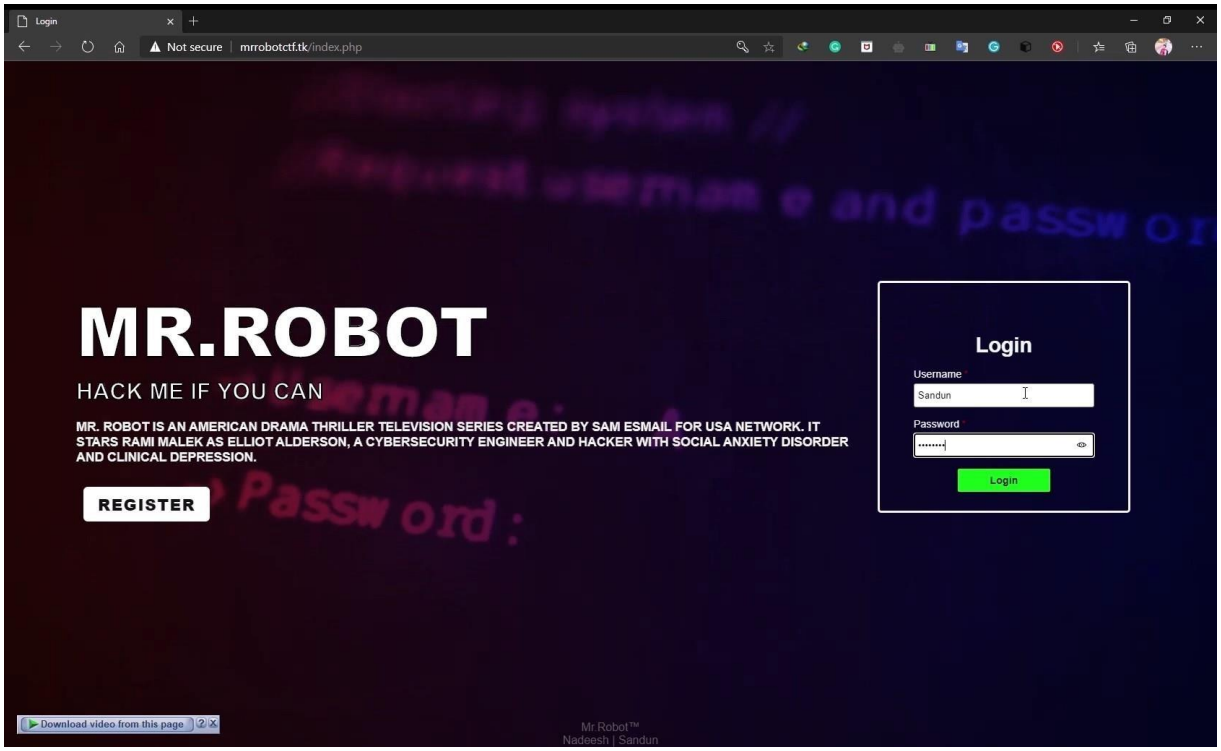
1. Goto mrrobotctf.cf

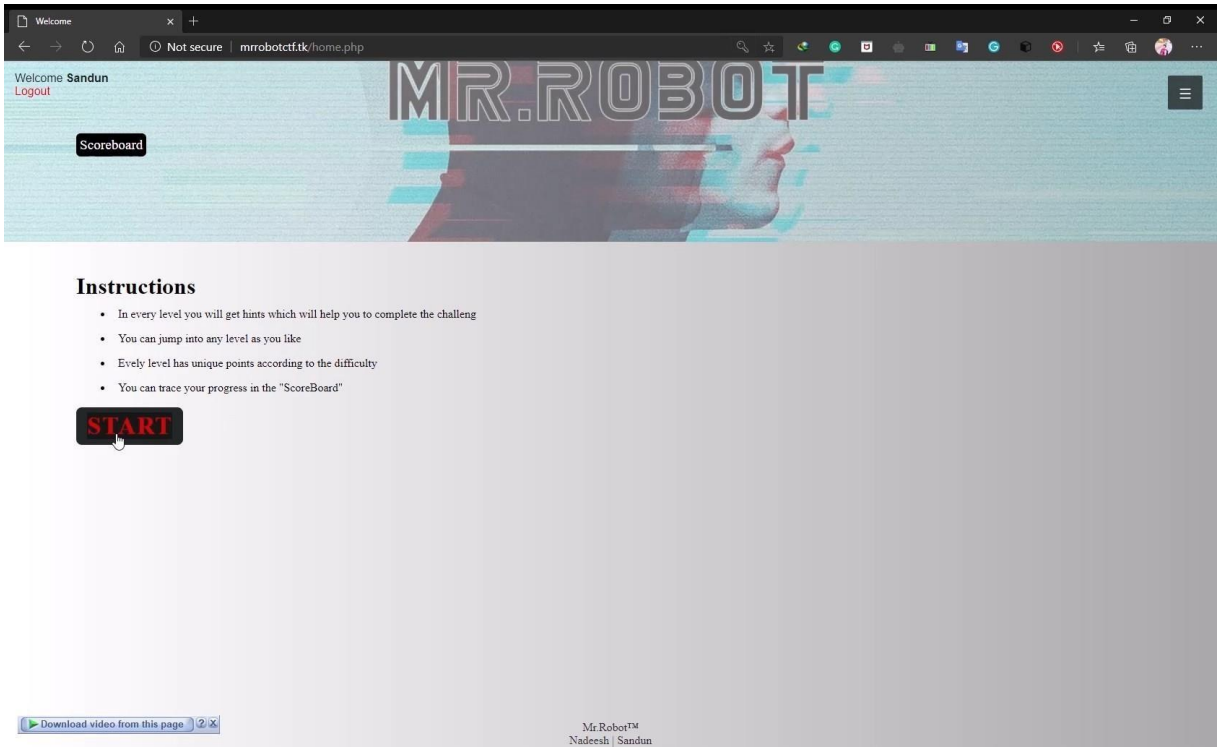


2. In the web app, the registration should be done first.



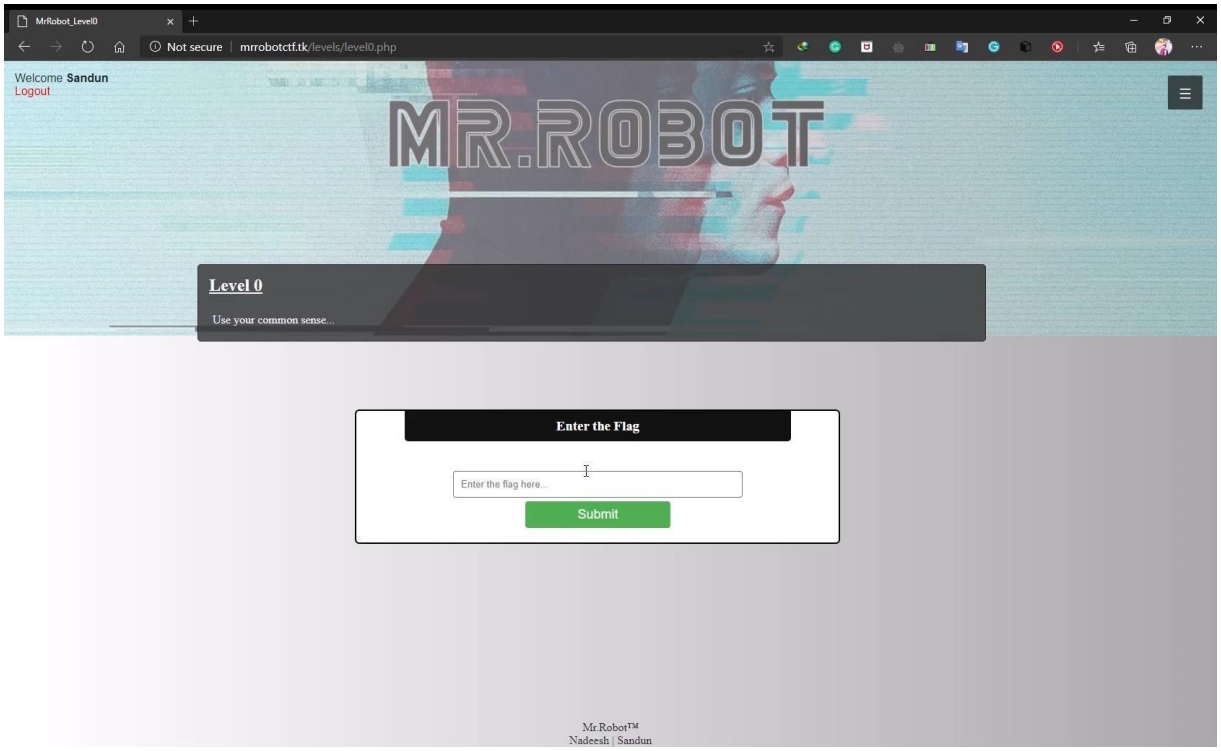
3. Then login to the web app, the instructions will be shown.





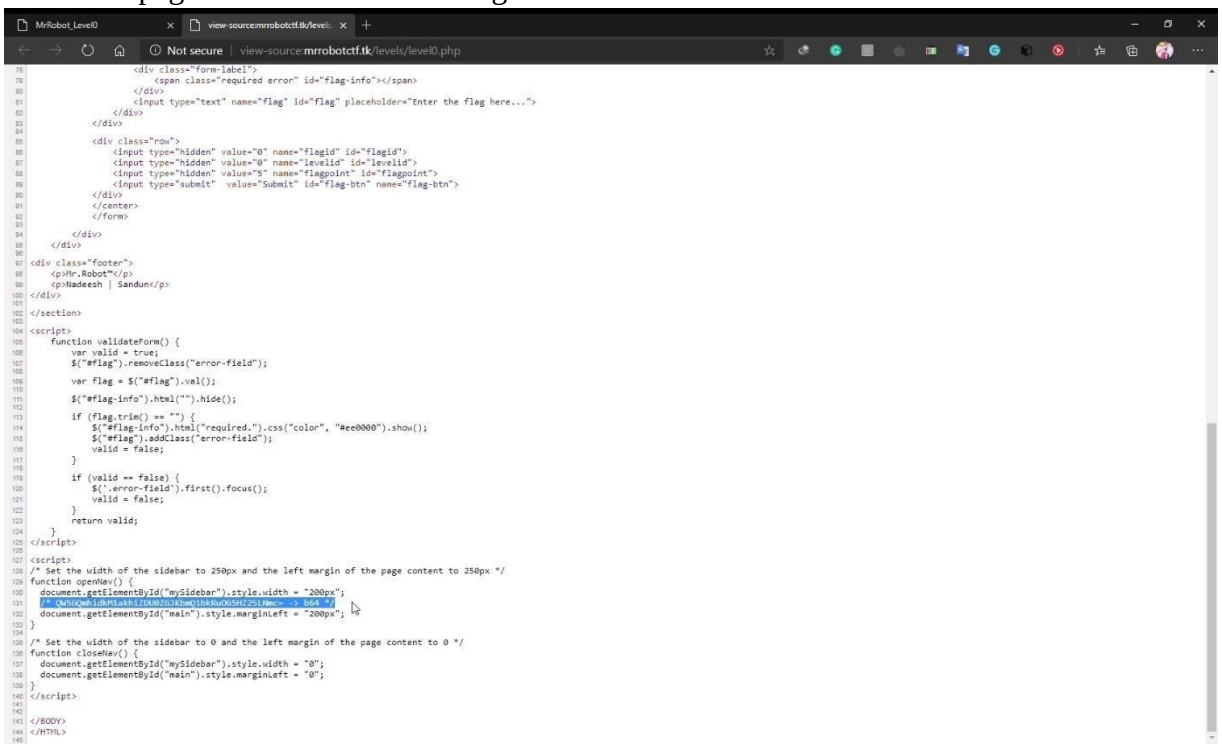
Walkthrough of the levels.

Level 0

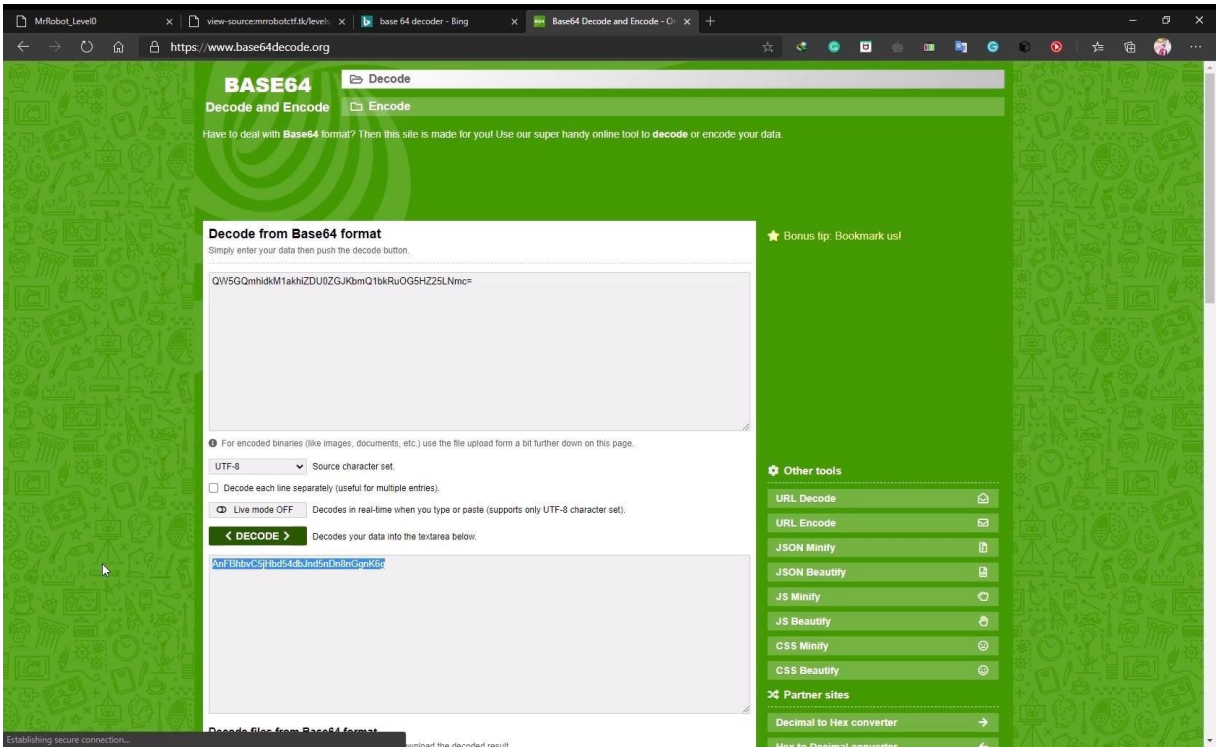


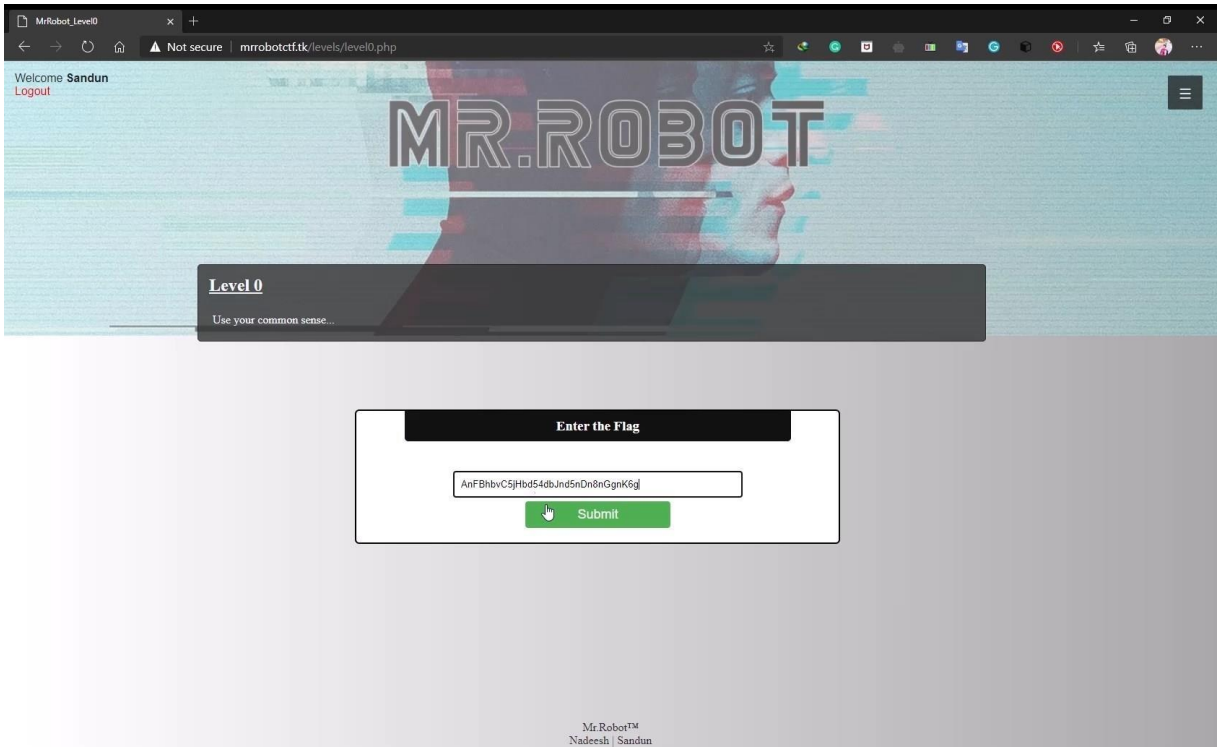
After getting the instructions, the 1st level is level 0. After clicking on level 0 a small hint will be shown.

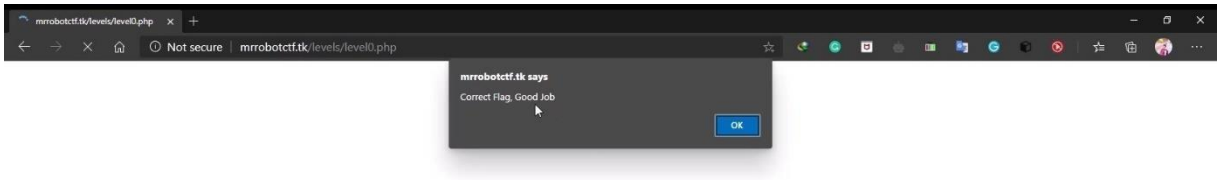
Go to the page source and find the flag.



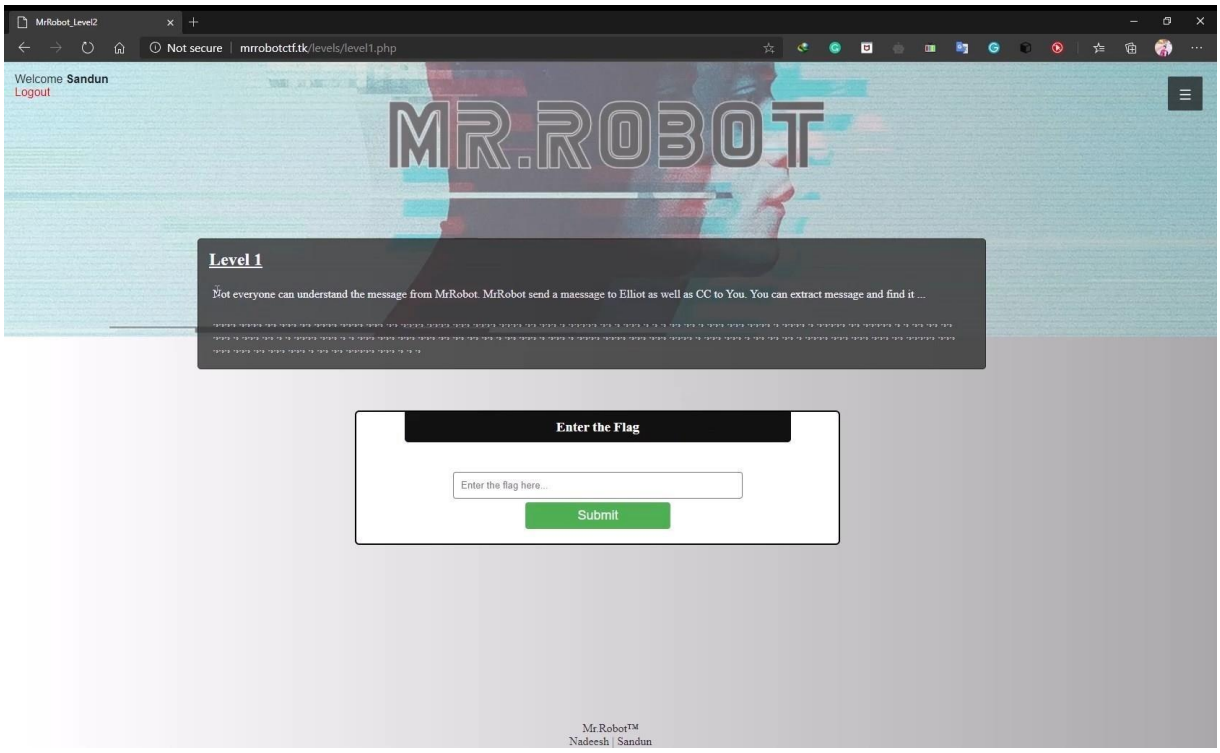
According to the above image the flag is encoded. Use any base64 decoder to decode the flag and later on submit in the submission form.



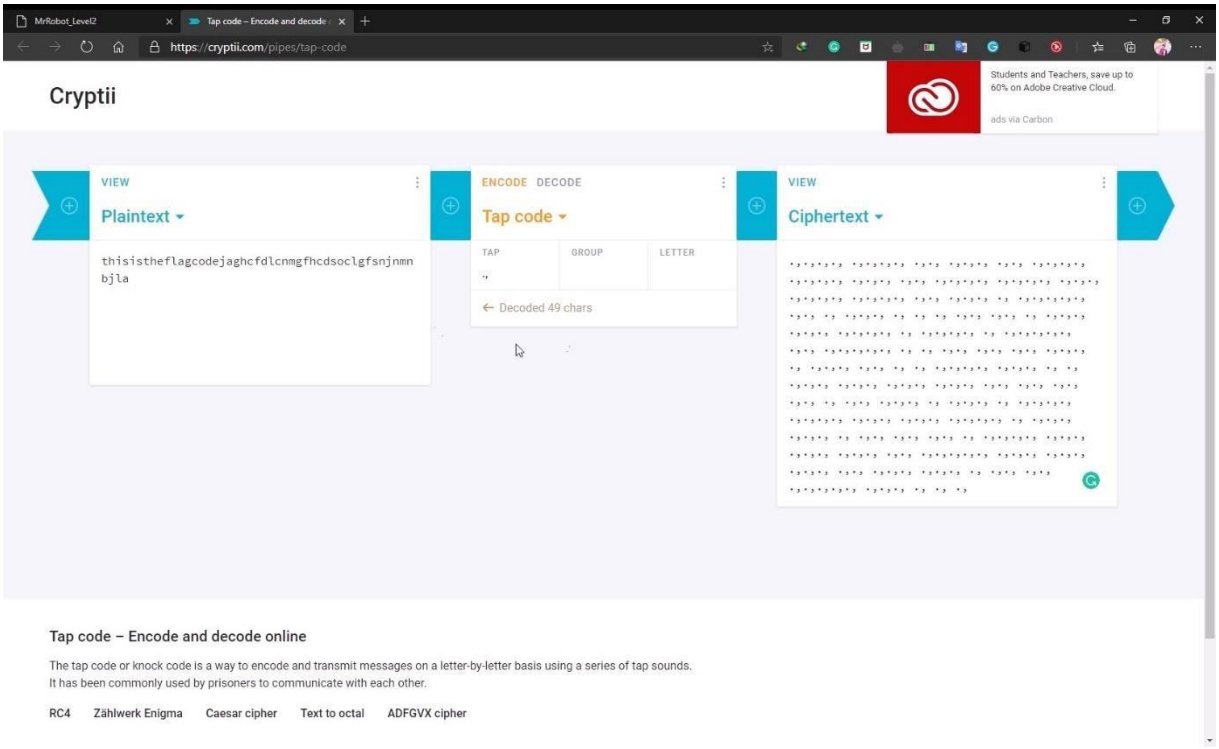




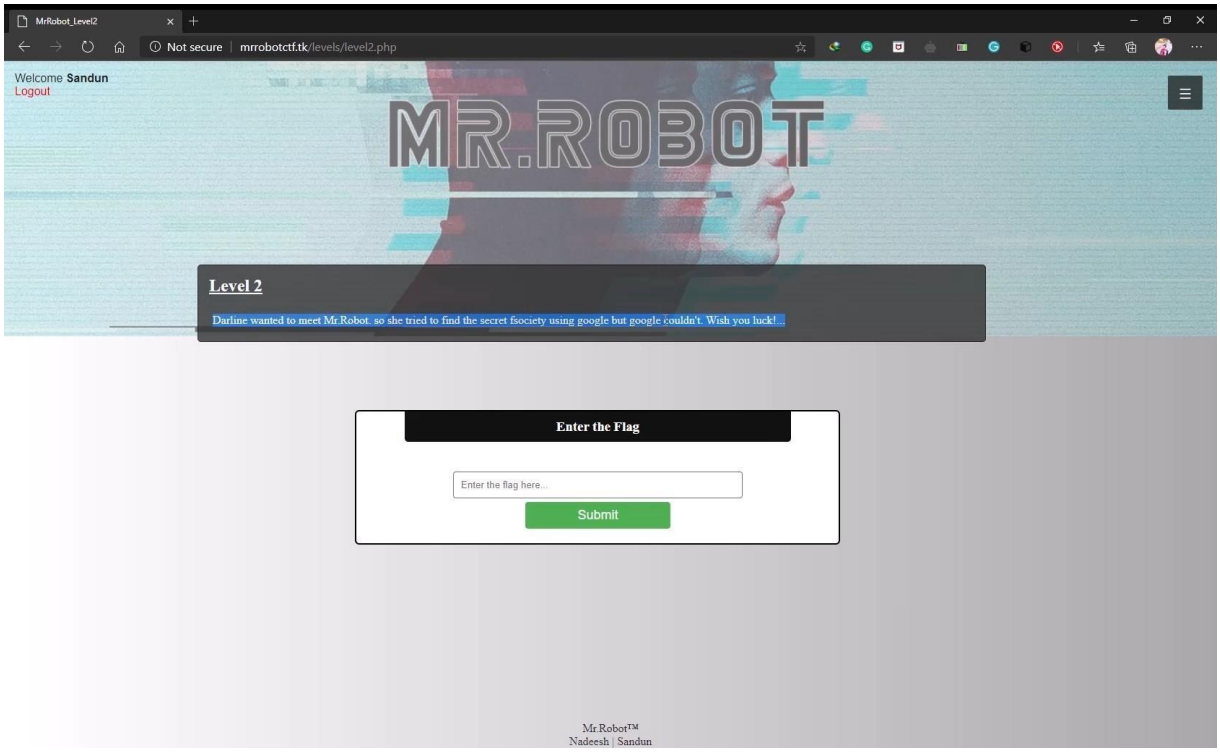
Level 1

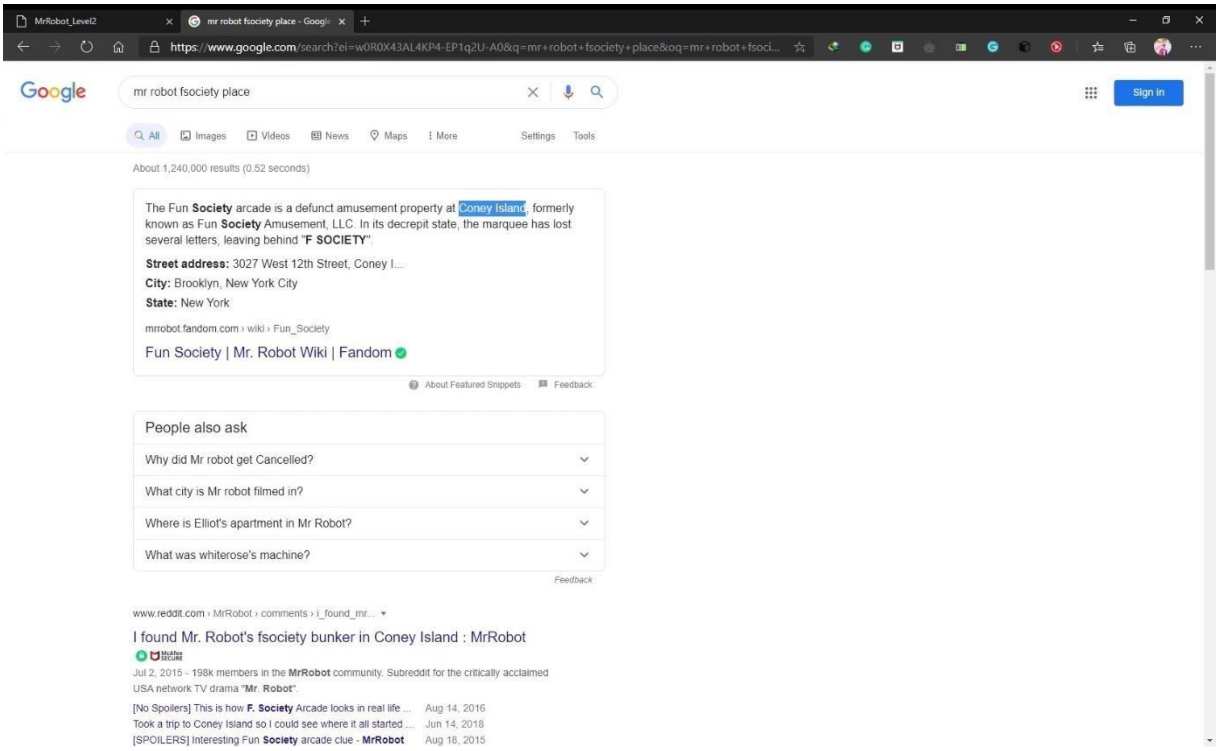


Since the code is encoded in tap code, it should be decoded in the meaningful format.

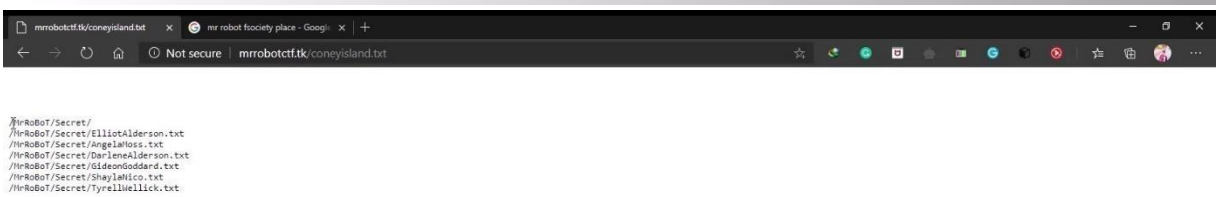

MrRobot_Level2
Tap code – Encode and decode
https://cryptii.com/pipes/tap-code
Cryptii
Students and Teachers, save up to 60% on Adobe Creative Cloud.
ads via Carbon
VIEW
Plaintext
thisistheflagcodejaghcfdlcnmgfhcdsoclgfsnjnmnbjla
ENCODE DECODE
Tap code
TAP
GROUP
LETTER
Decoded 49 chars
VIEW
Ciphertext
Tap code – Encode and decode online
The tap code or knock code is a way to encode and transmit messages on a letter-by-letter basis using a series of tap sounds. It has been commonly used by prisoners to communicate with each other.
RC4
Zählwerk Enigma
Caesar cipher
Text to octal
ADFGVX cipher

Level 2


MrRobot_Level2
Not secure
mrrobotctf.tk/levels/level2.php
Welcome Sandun
Logout
MR.ROBOT
Level 2
Darline wanted to meet Mr.Robot. so she tried to find the secret fsociety using google but google couldn't. Wish you luck!...
Enter the Flag
Enter the flag here...
Submit
Mr.Robot™
Nadeesh | Sandun

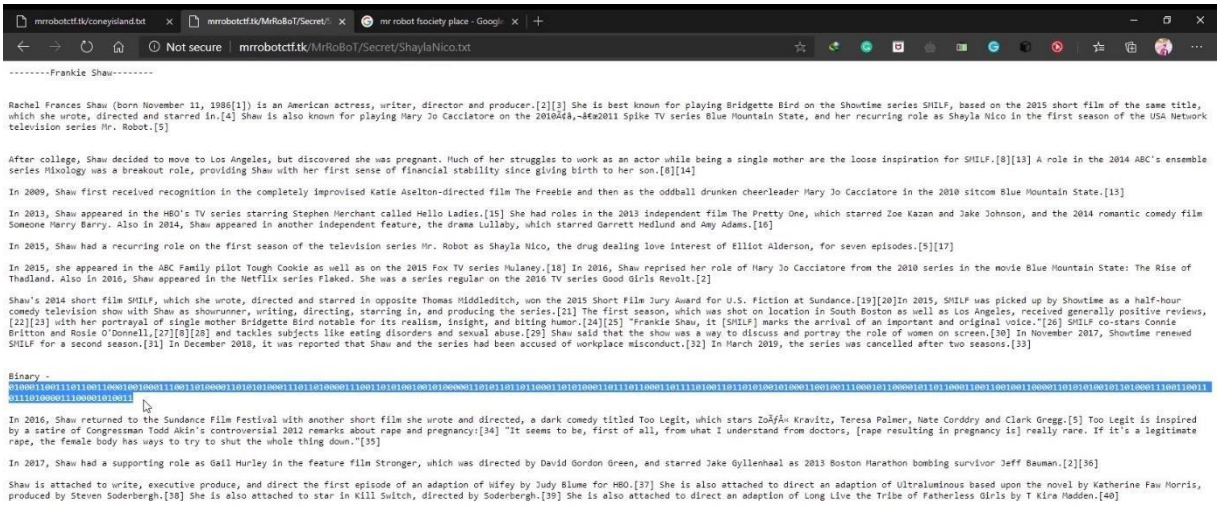


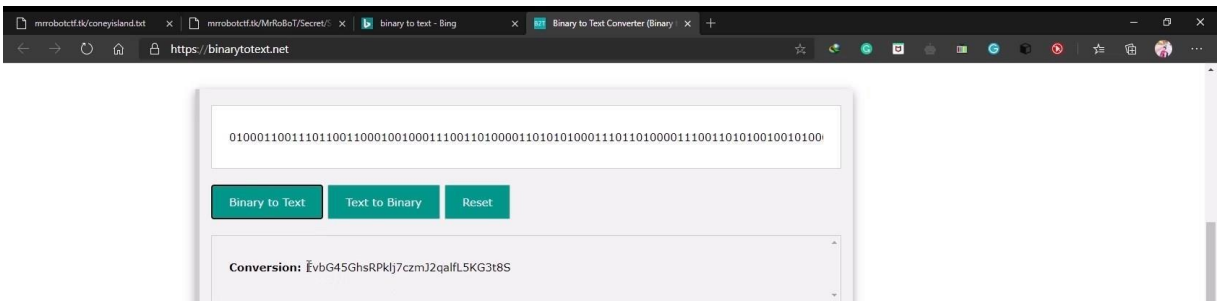
According to the hints given, it shows coneyisland.txt file deals with the google search. So, open the coneyisland.txt.




```
/MrRoBoT/Secret/
/MrRoBoT/Secret/ElliotAlderson.txt
/MrRoBoT/Secret/AngelaMoss.txt
/MrRoBoT/Secret/DarleneAlderson.txt
/MrRoBoT/Secret/GideonGoddard.txt
/MrRoBoT/Secret/ShaylaNico.txt
/MrRoBoT/Secret/TyrellWellick.txt
```

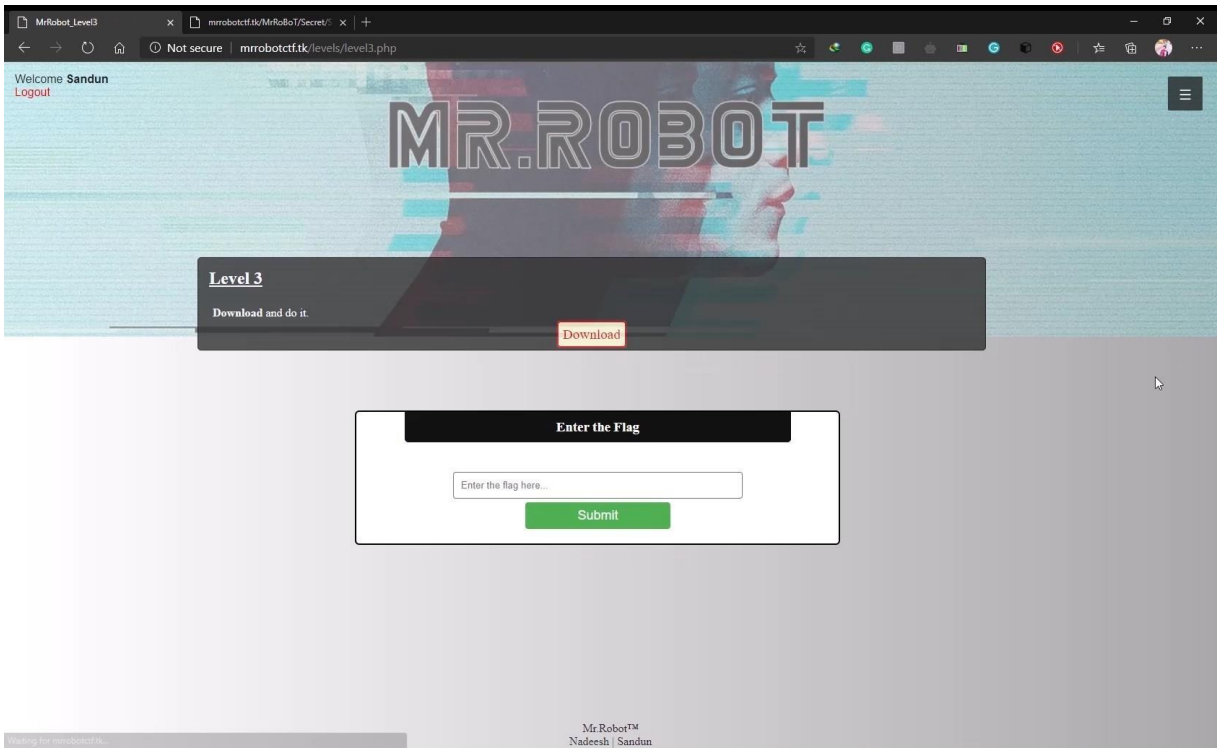
Find the directory called /MrRobotCTF/Secret/. Inside the directory there is a text file called ShaylaNico.txt.



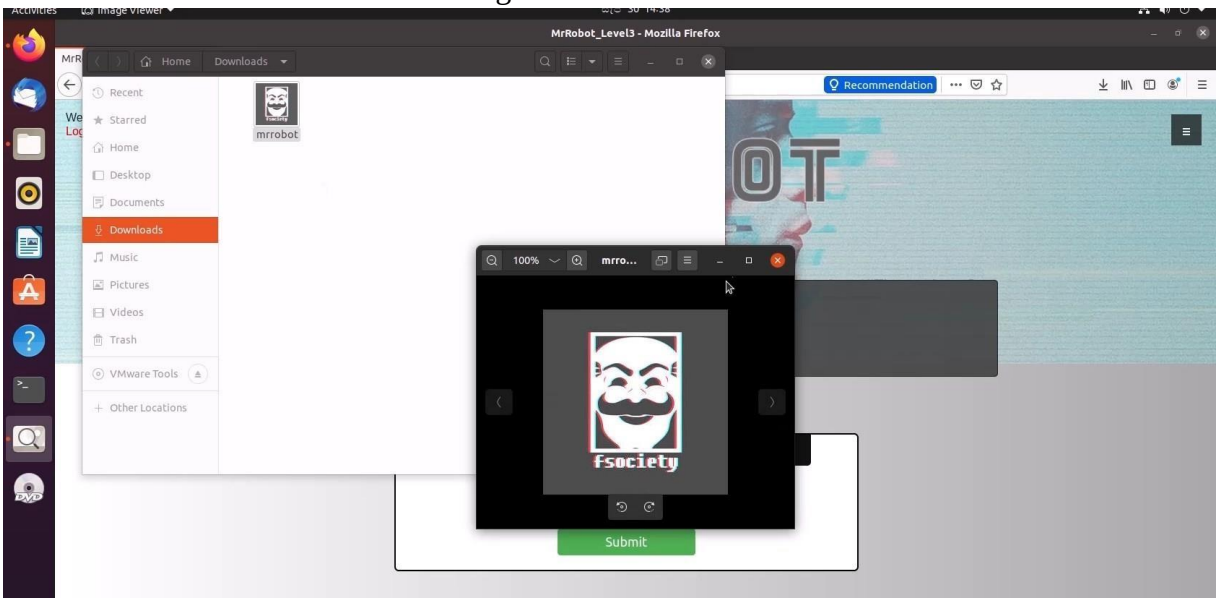


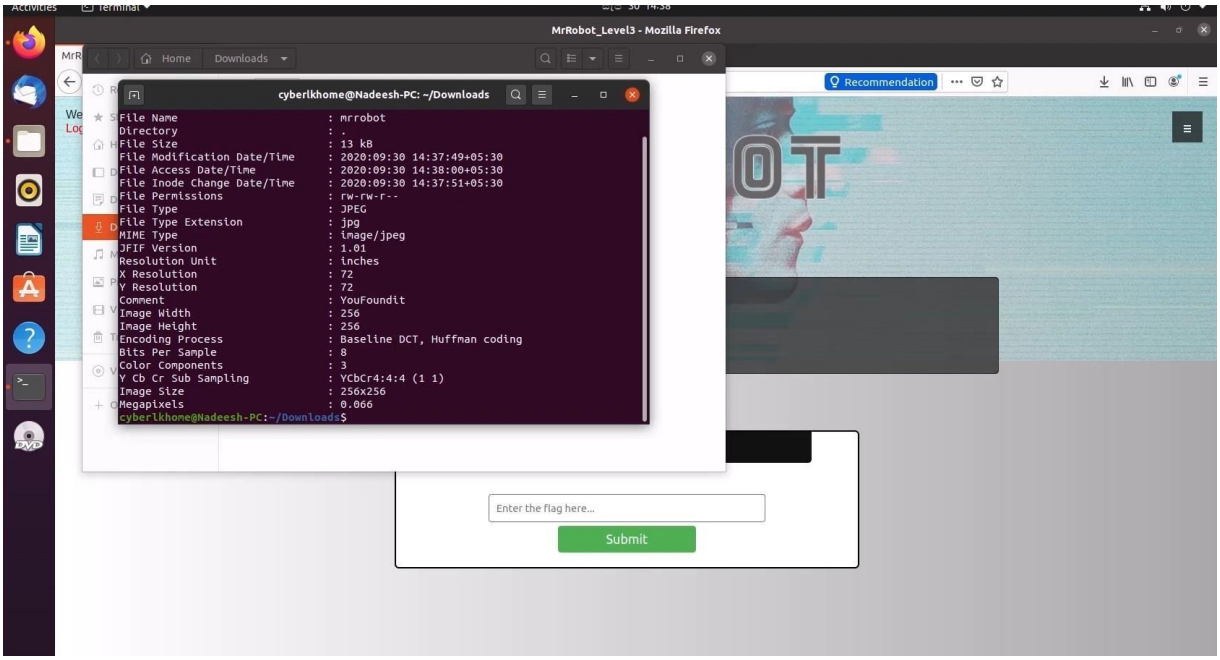
According to the above image the flag is encoded. Use any binary decoder to decode the flag and later on submit in the submission form.

Level 3

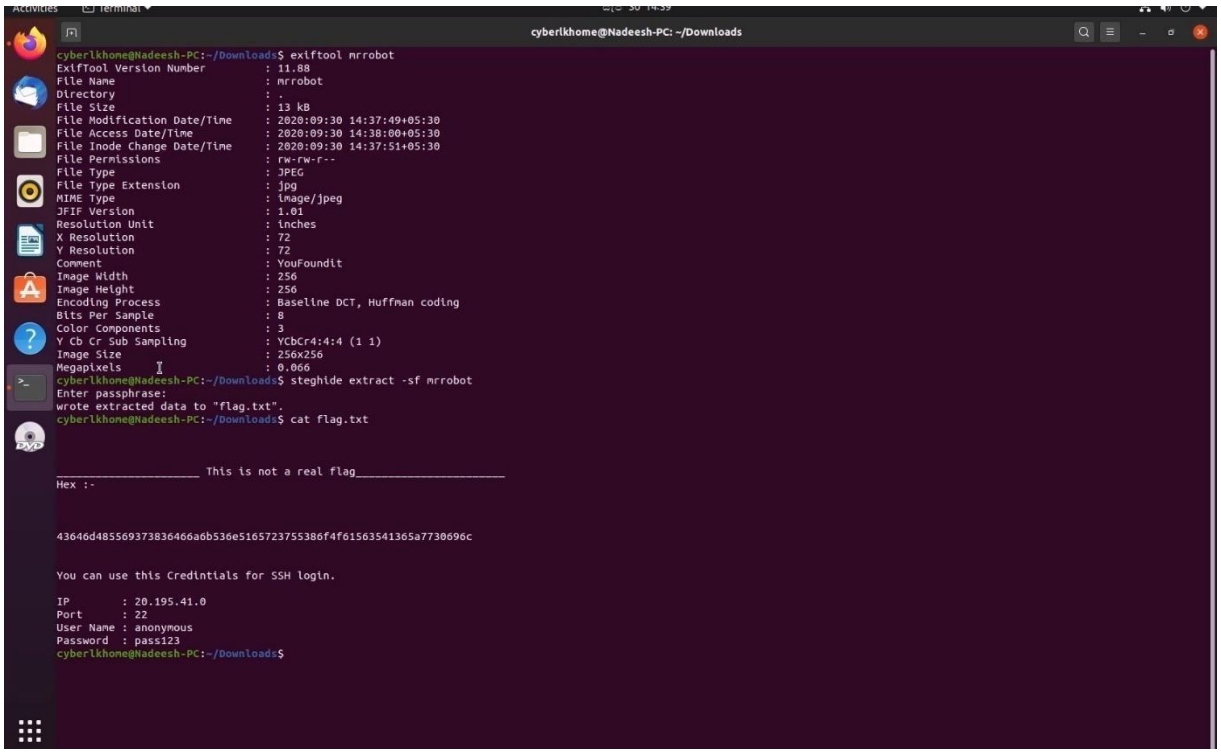


After downloading the Image file to a Linux environment. Scan the image for file type. The hints suggest of the METADATA, because of that we need a tool to see METADATA of the image. After enough research and the hint suggests Exiftool. Download and install the tool with the command: “sudo apt-get install exiftool”. After installing check, the image with the tool: “exiftool mrrobot.jpg”. It shows a Comment with a passphrase. Next the hint points us of a tool to extract data hidden in the image.

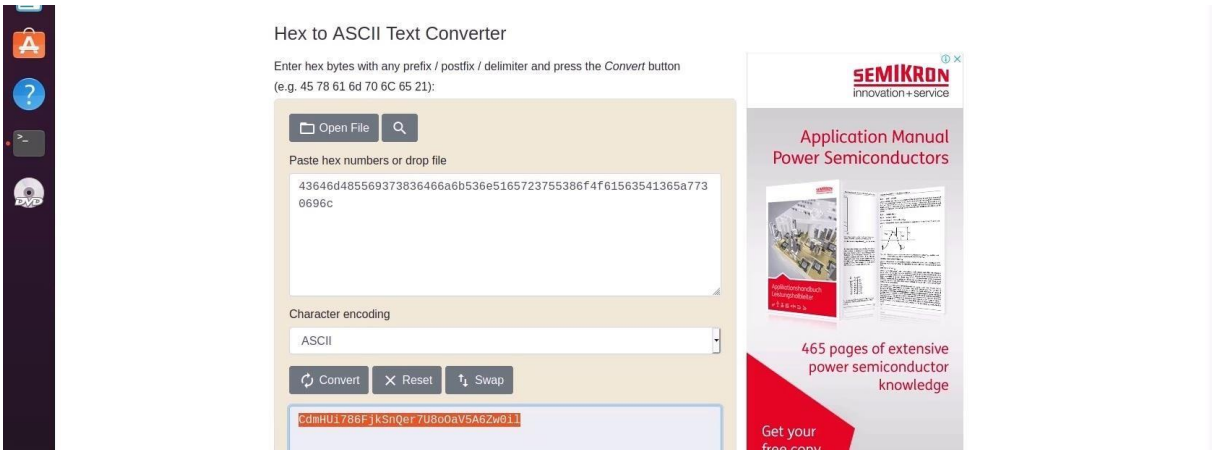




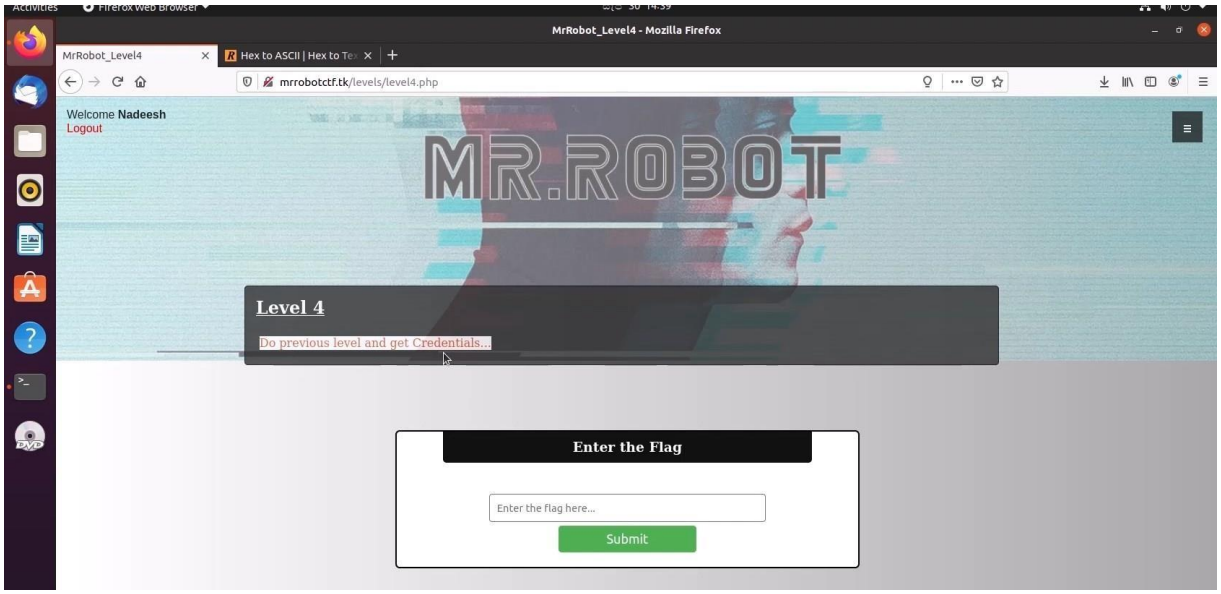
Install: “sudo apt-get install steghide”. Run the command: “steghide extract -sf mrrobot.jpg”. Next the passphrase will be required, enter it. New file “secret” without an extension is extracted out of the image. Open it to find the FLAG:



According to the above image the flag is encoded. Use any hex decoder to decode the flag and later on submit in the submission form.

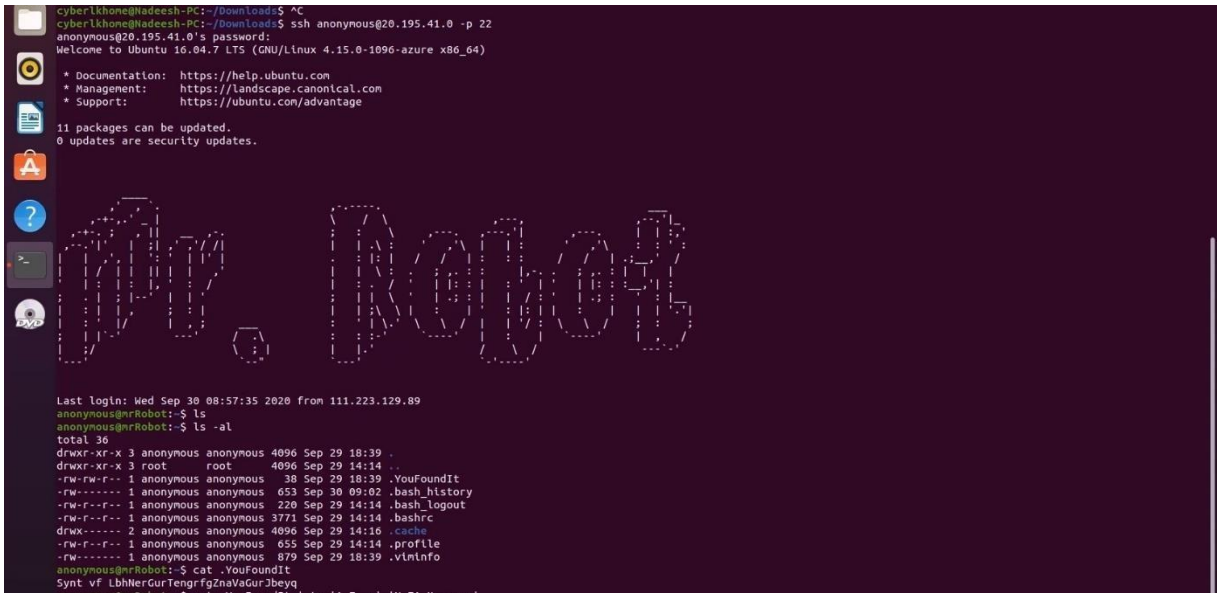


Level 4



To do this level you must need to do the previous level,

And login through SSH using those credential, the flag file is hidden use cat .YouFountIt to read the file

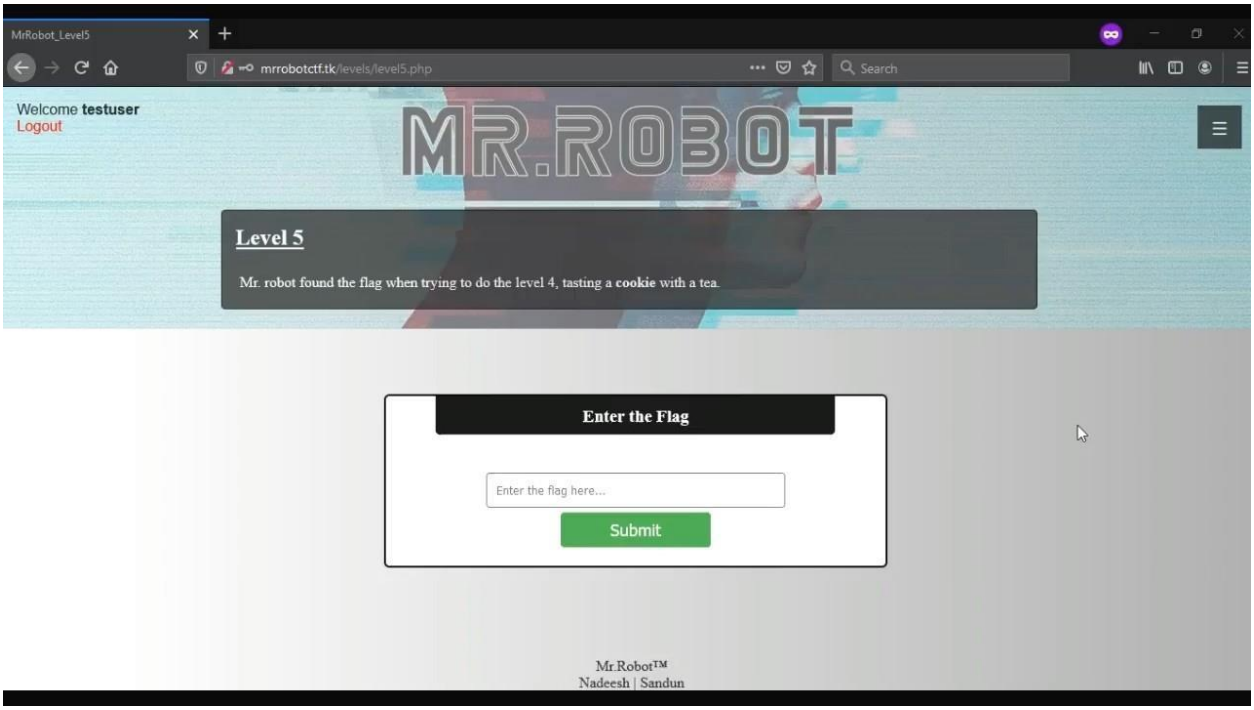


And it need to decode

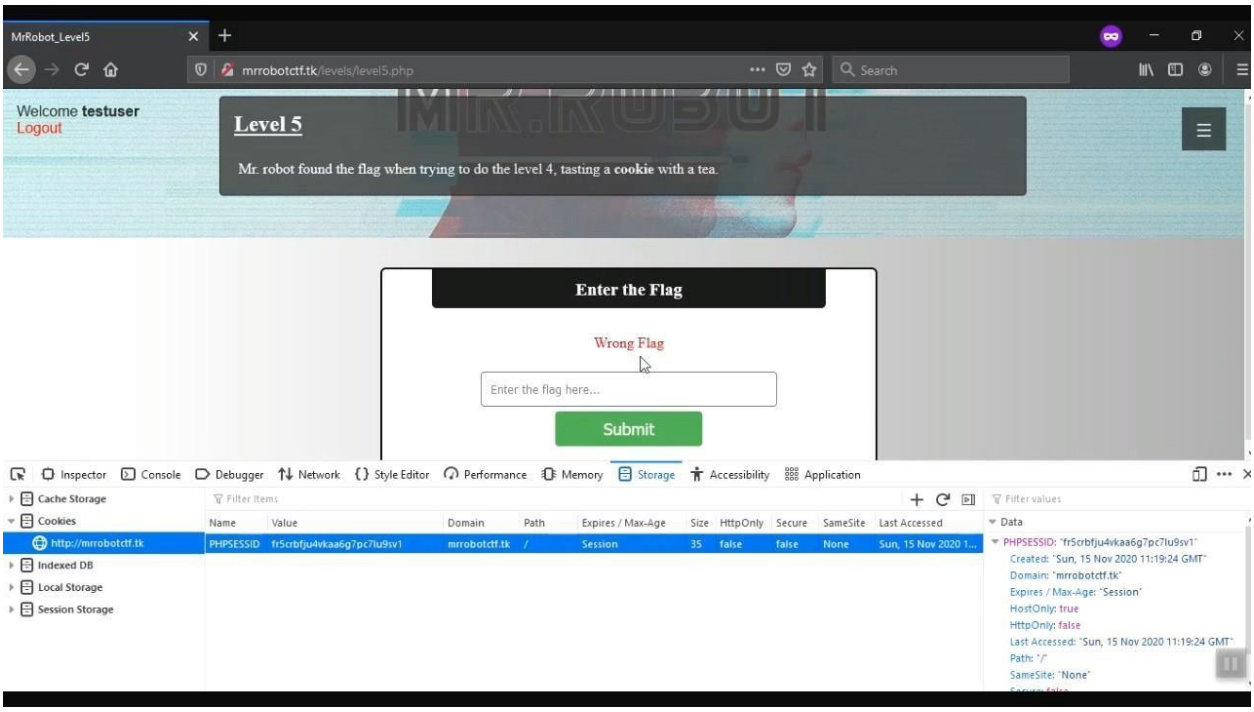
Cat .YouFountIt | tr ‘A-Za-z’ ‘N-ZA-Mn-za-m’

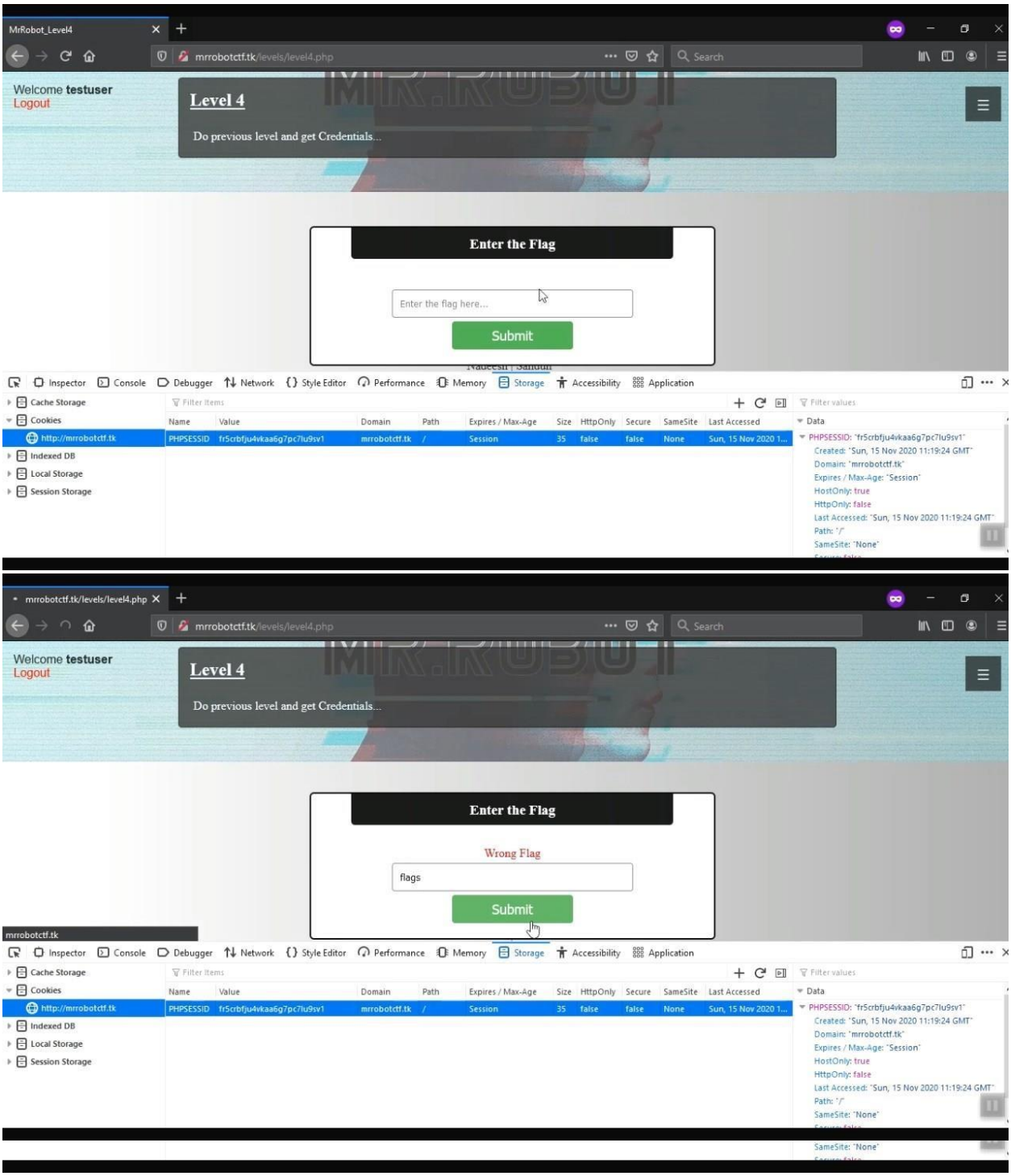

Last login: Wed Sep 30 08:57:35 2020 from 111.223.129.89
anonymous@mrRobot:~$ ls
anonymous@mrRobot:~$ ls -al
total 36
drwxr-xr-x 3 anonymous anonymous 4096 Sep 29 18:39 .
drwxr-xr-x 3 root root 4096 Sep 29 14:14 ..
-rw-rw-r-- 1 anonymous anonymous 38 Sep 29 18:39 .YouFoundIt
-rw------- 1 anonymous anonymous 653 Sep 30 09:02 .bash_history
-rw-r--r-- 1 anonymous anonymous 220 Sep 29 14:14 .bash_logout
-rw-r--r-- 1 anonymous anonymous 3771 Sep 29 14:14 .bashrc
drwx------ 2 anonymous anonymous 4096 Sep 29 14:16 .cache
-rw-r--r-- 1 anonymous anonymous 655 Sep 29 14:14 .profile
-rw------- 1 anonymous anonymous 879 Sep 29 18:39 .viminfo
anonymous@mrRobot:~$ cat .YouFoundIt
Synt vf LbhNerGurTengrfgZnaVaGurJbeyq
anonymous@mrRobot:~$ cat .YouFoundIt | tr 'A-Za-z' 'N-ZA-Mn-za-m'
Flag is YouAreTheGratestManInTheWorld
anonymous@mrRobot:~$

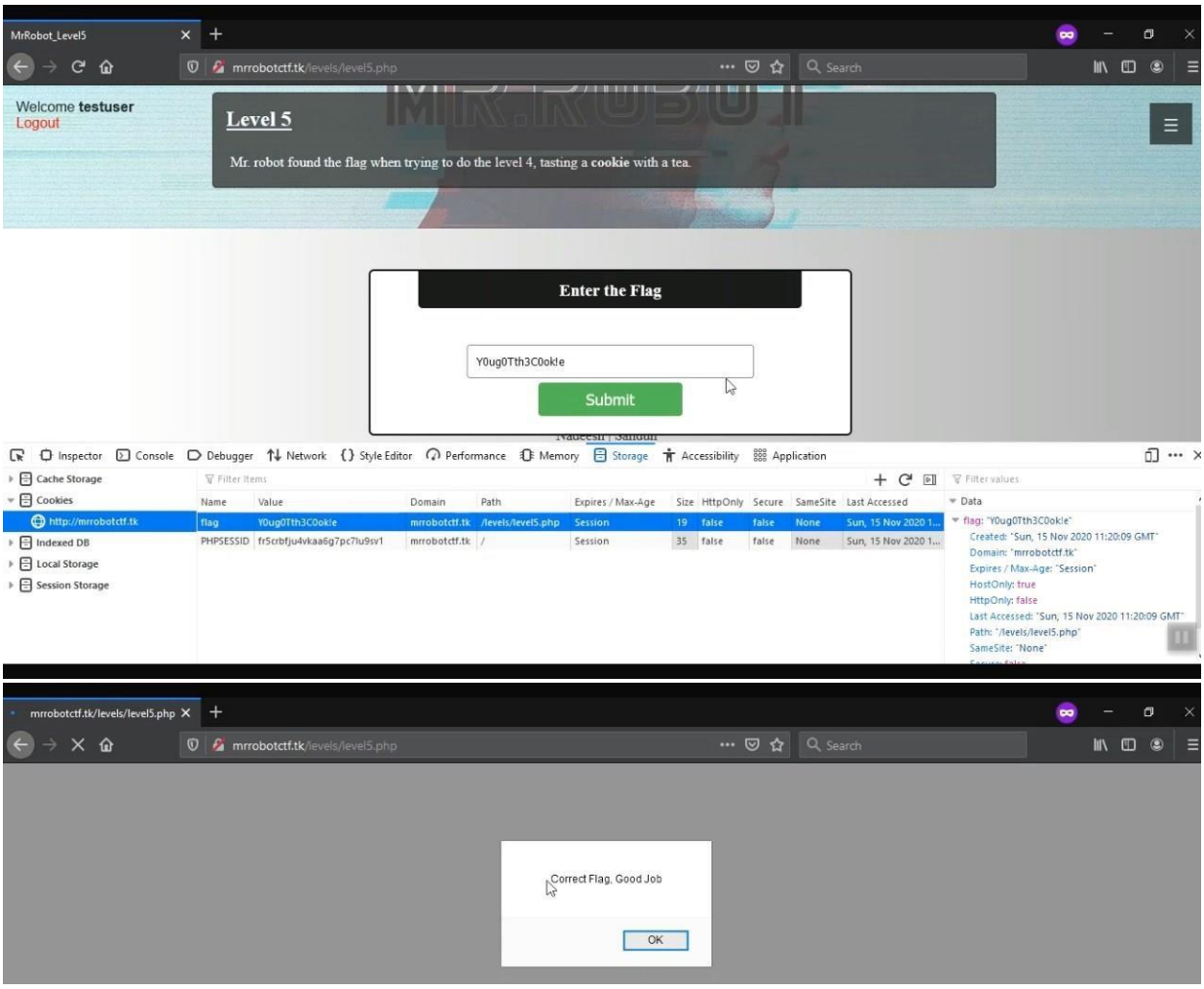
Level 5



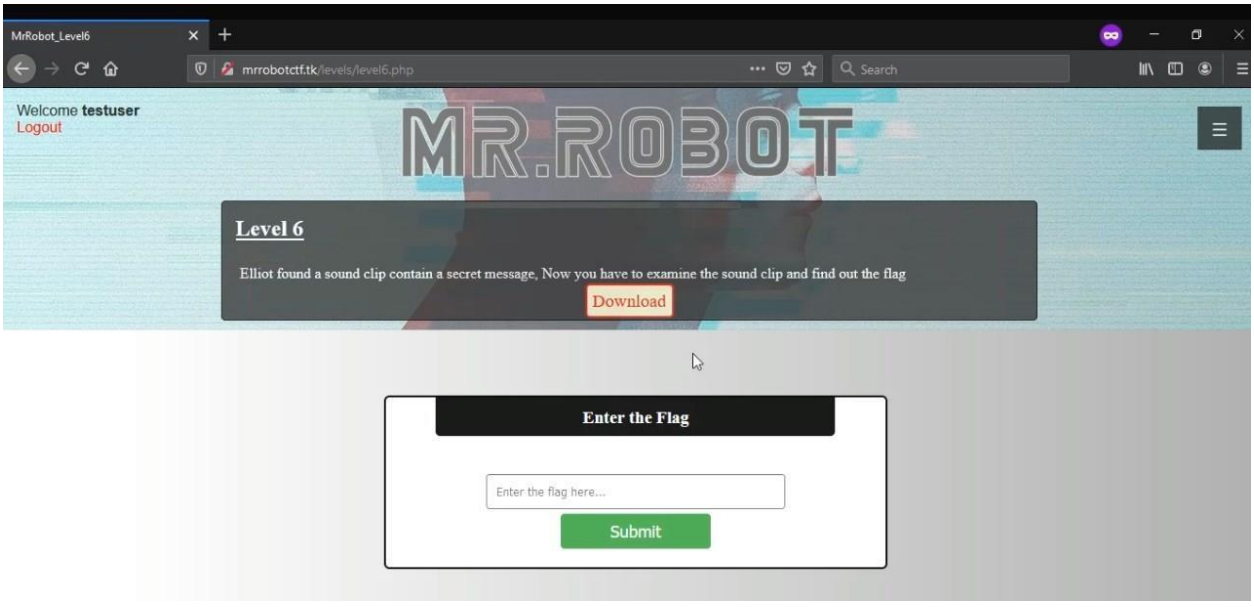
In hint there is a mentioned about cookie so,
First open the Inspector Element Mode and go to Storage tab (in Firefox), then select Cookies and https://mrrobotctf.cf. then type any value in flag submission field. The flag is not in the Level 5 submission it's on the level4.php page. Mr. Robot give a hint for that. He said to try the level 4, that is mean flags is in with Level 4 Cookies (if you already done the level 4 there will be another cookie Named 'flag'). Sometime that not come first time then enter another value in that field. Then you can see the flag in the cookie section.



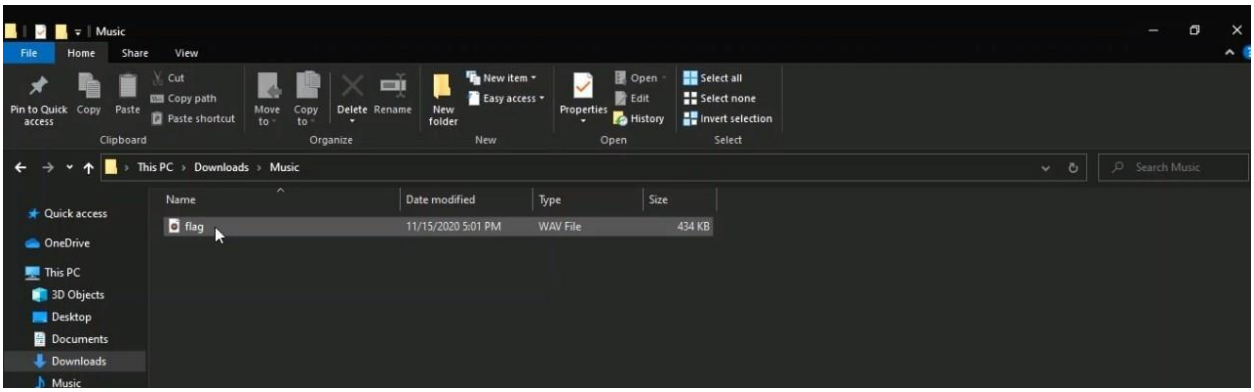

MrRobot_Level4
mrrobotctf.tk/levels/level4.php
Search
Welcome testuser
Logout
Level 4
Do previous level and get Credentials...
Enter the Flag
Enter the flag here...
Submit
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Application
Cache Storage
Cookies
http://mrrobotctf.tk
Indexed DB
Local Storage
Session Storage
Name
Value
Domain
Path
Expires / Max-Age
Size
HttpOnly
Secure
SameSite
Last Accessed
PHPSESSID
fr5crbfju4vkaa6g7pc7lu9sv1
mrrobotctf.tk
/
Session
35
false
false
None
Sun, 15 Nov 2020 1...
Data
PHPSESSID: "fr5crbfju4vkaa6g7pc7lu9sv1"
Created: "Sun, 15 Nov 2020 11:19:24 GMT"
Domain: "mrrobotctf.tk"
Expires / Max-Age: "Session"
HostOnly: true
HttpOnly: false
Last Accessed: "Sun, 15 Nov 2020 11:19:24 GMT"
Path: "/"
SameSite: "None"
mrrobotctf.tk/levels/level4.php
Wrong Flag
flags
Submit
mrrobotctf.tk


MrRobot_Level5
mrrobotctf.tk/levels/level5.php
Search
Welcome testuser
Logout
Level 5
Mr. robot found the flag when trying to do the level 4, tasting a cookie with a tea.
Enter the Flag
Y0ug0Tth3C0ok!e
Submit
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Application
Cache Storage
Cookies
http://mrrobotctf.tk
Indexed DB
Local Storage
Session Storage
Name
Value
Domain
Path
Expires / Max-Age
Size
HttpOnly
Secure
SameSite
Last Accessed
flag
Y0ug0Tth3C0ok!e
mrrobotctf.tk
/levels/level5.php
Session
19
false
false
None
Sun, 15 Nov 2020 1...
PHPSESSID
fr5crbfju4vkaa6g7pc7lu9sv1
mrrobotctf.tk
/
Session
35
false
false
None
Sun, 15 Nov 2020 1...
Data
flag: "Y0ug0Tth3C0ok!e"
Created: "Sun, 15 Nov 2020 11:20:09 GMT"
Domain: "mrrobotctf.tk"
Expires / Max-Age: "Session"
HostOnly: true
HttpOnly: false
Last Accessed: "Sun, 15 Nov 2020 11:20:09 GMT"
Path: "/levels/level5.php"
SameSite: "None"
mrrobotctf.tk/levels/level5.php
mrrobotctf.tk/levels/level5.php
Search
Correct Flag, Good Job
OK

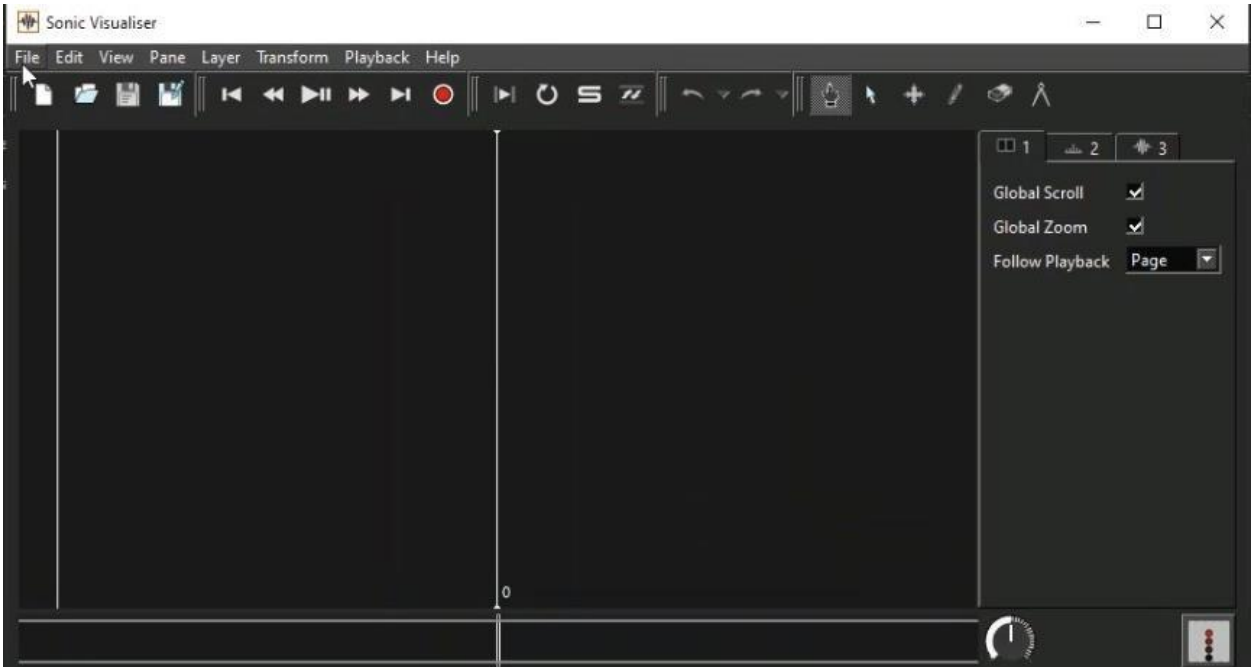
Level 6


MrRobot_Level6
mrrobotctf.tk/levels/level6.php
Search
Welcome testuser
Logout
MR.ROBOT
Level 6
Elliot found a sound clip contain a secret message, Now you have to examine the sound clip and find out the flag
Download
Enter the Flag
Enter the flag here...
Submit

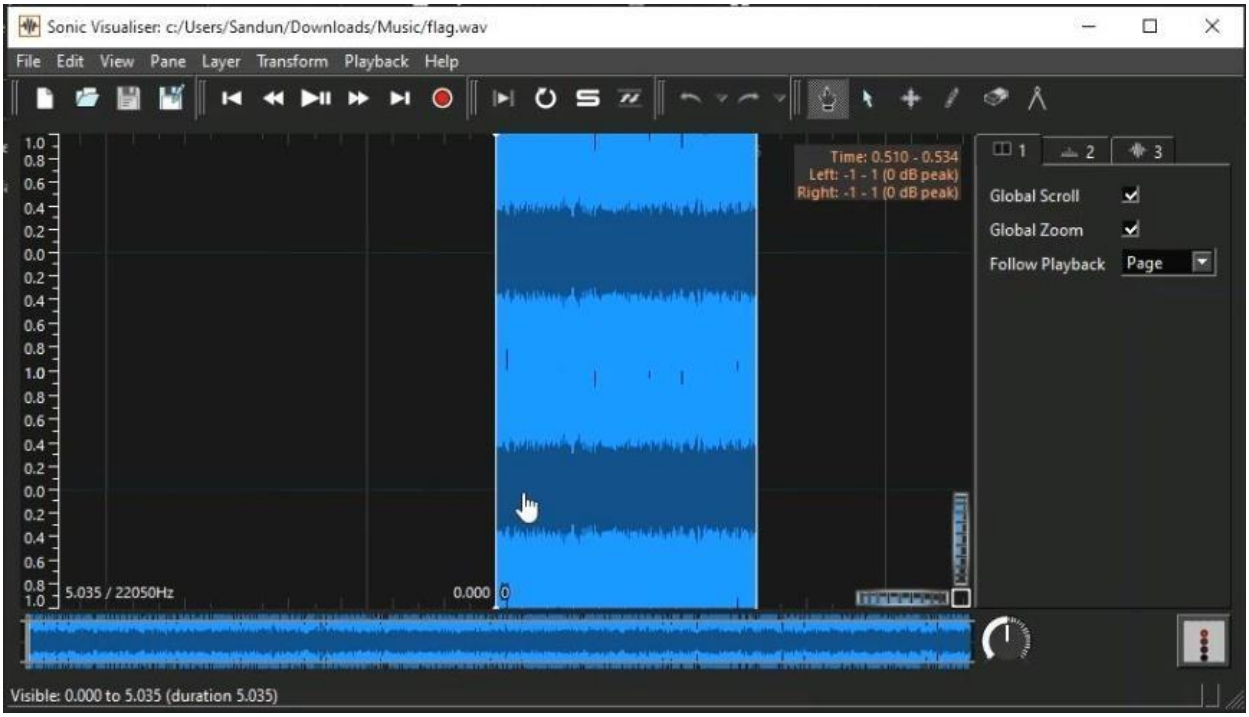
First download the sound clip.



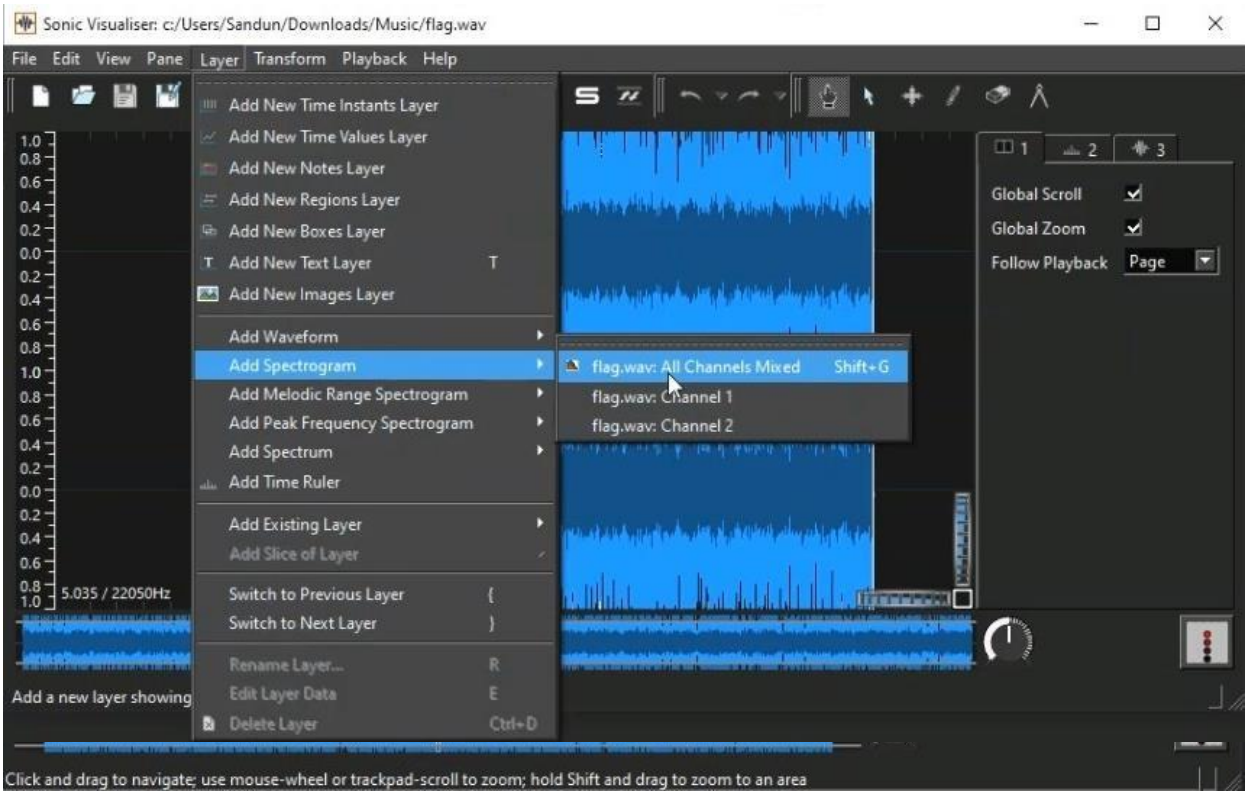
Then we want a **Sonic Visualiser** software**.**



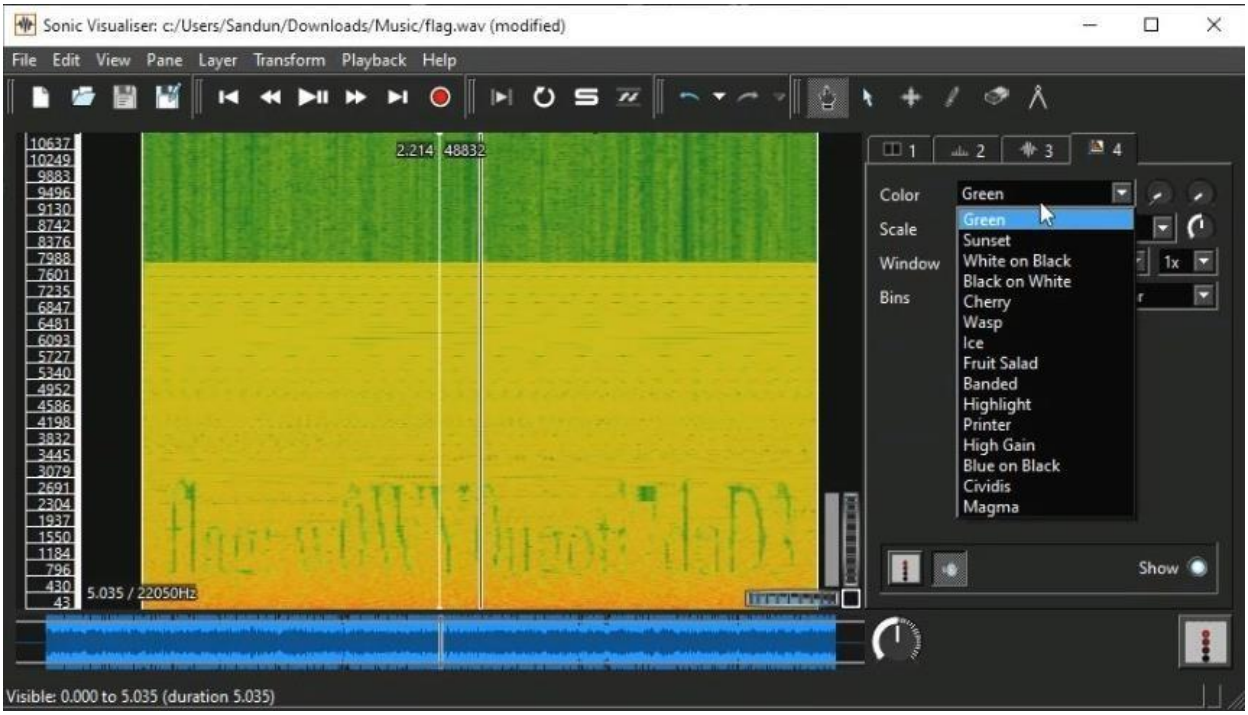
Then open the sound clip on Sonic Visualiser.



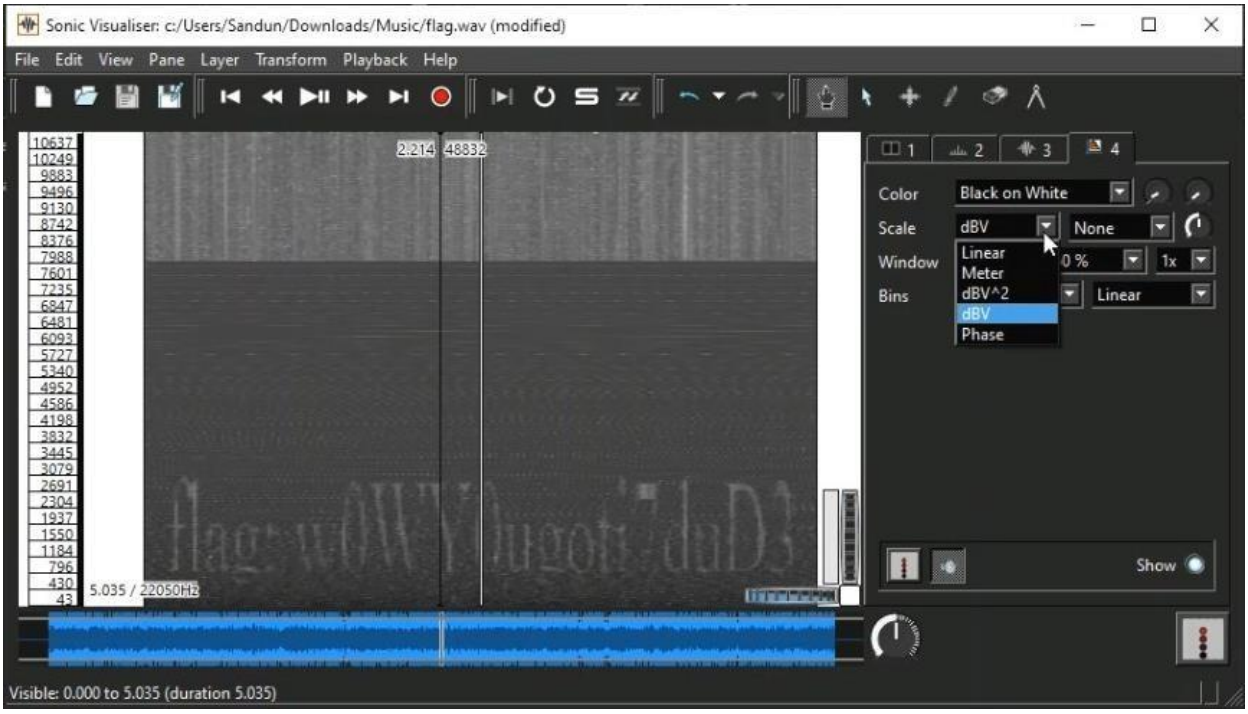
Then go to **Layer** > **Add Spectrogram** > **flag.wav: All Channels Mixed** and add that. Then we want to change **Color, Scale, Window and Bins** to get clear Image in Spectrogram layer. Then we can saw the flag in that.



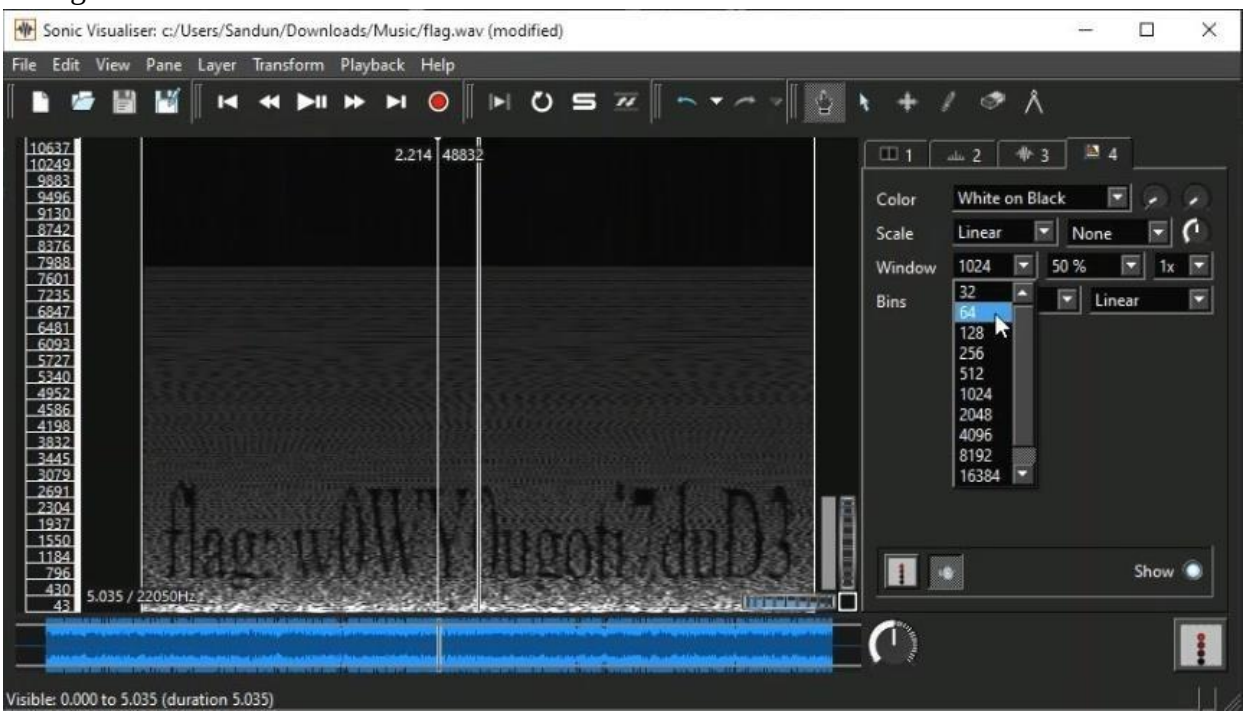
Change **Color** to black and white



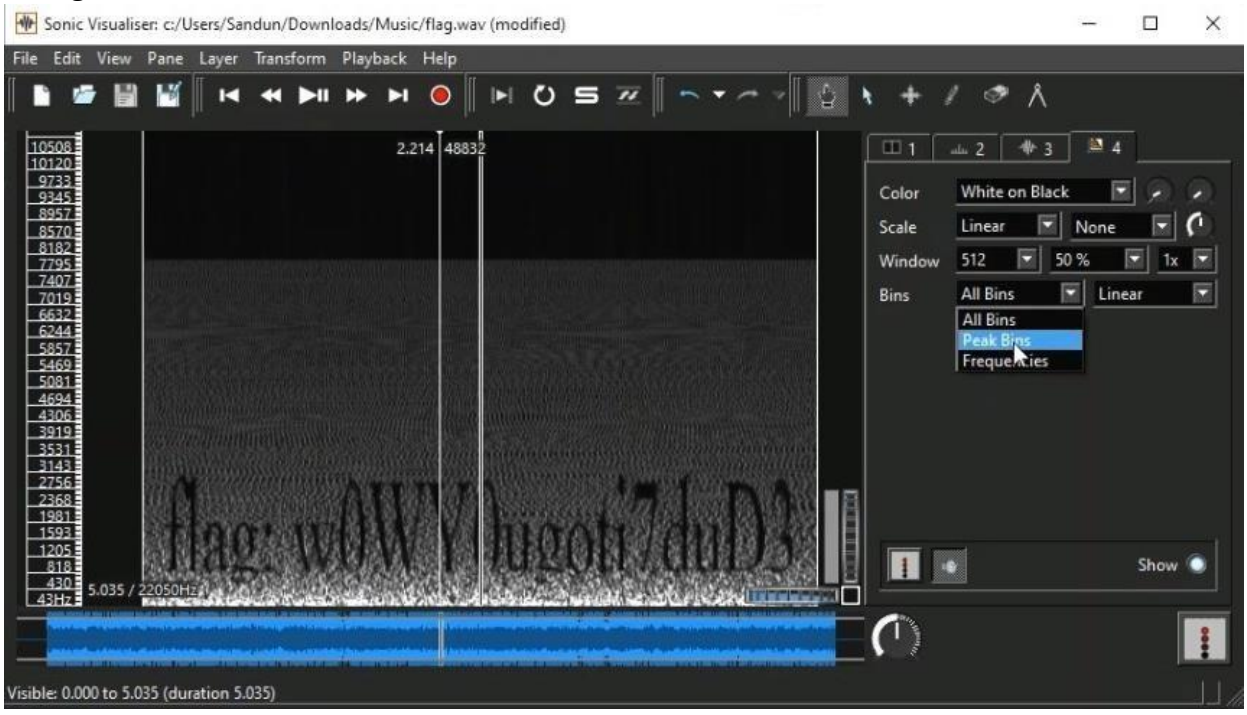
Change **Scale to linear**



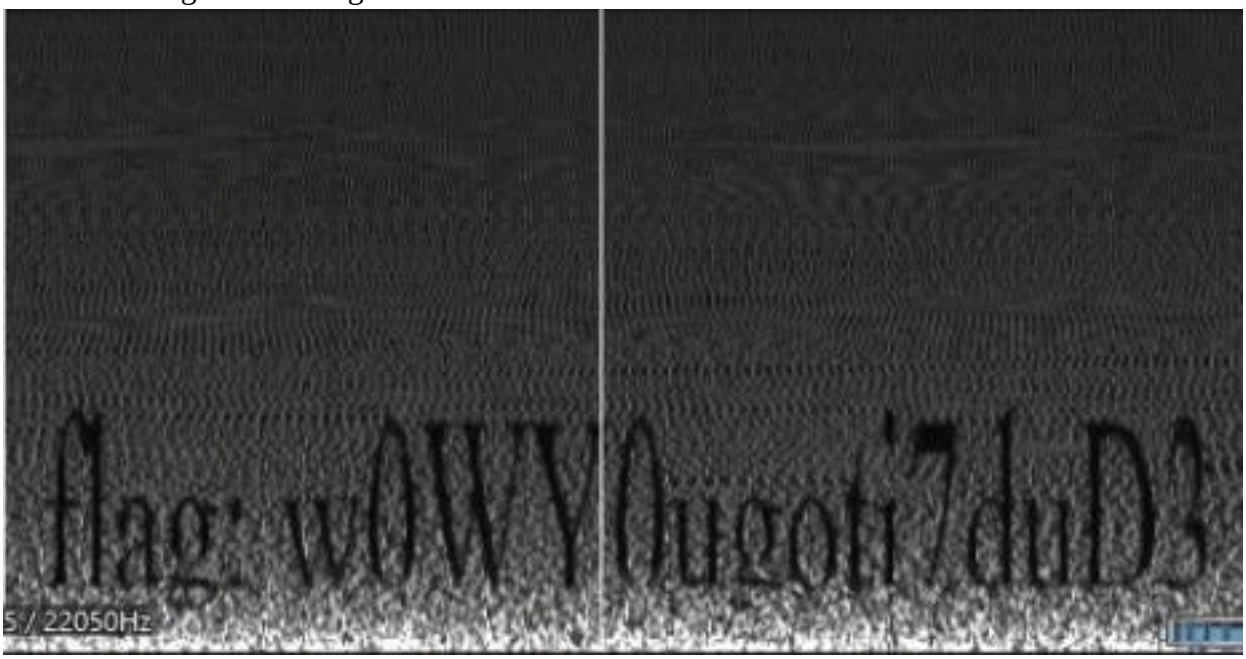
Change **Window to 512**



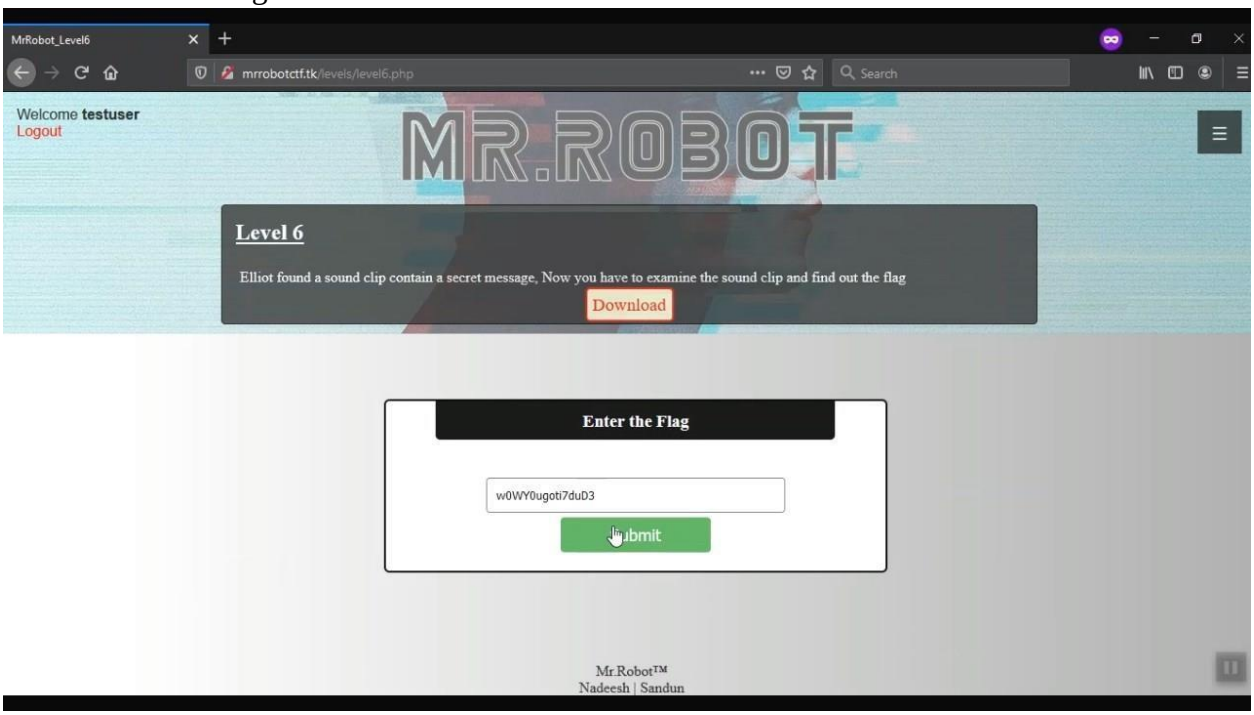
Change **Bins**



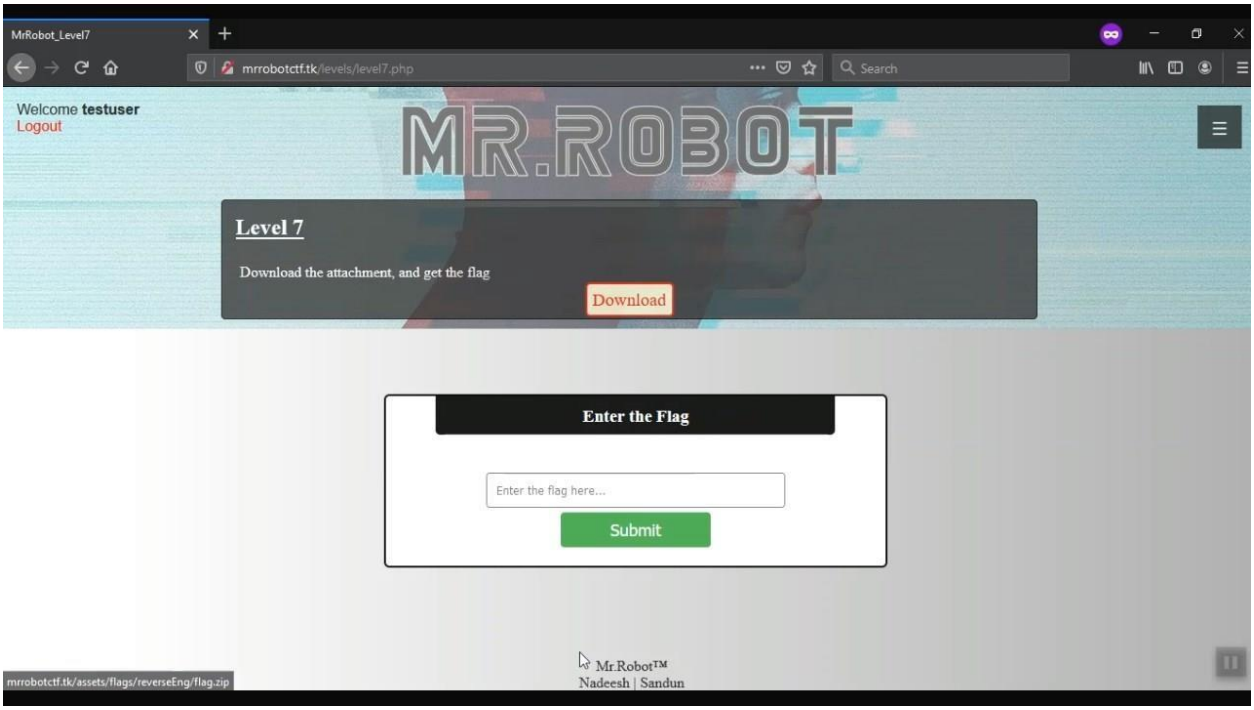
Then We can get clear Image.



Then submit the flag.



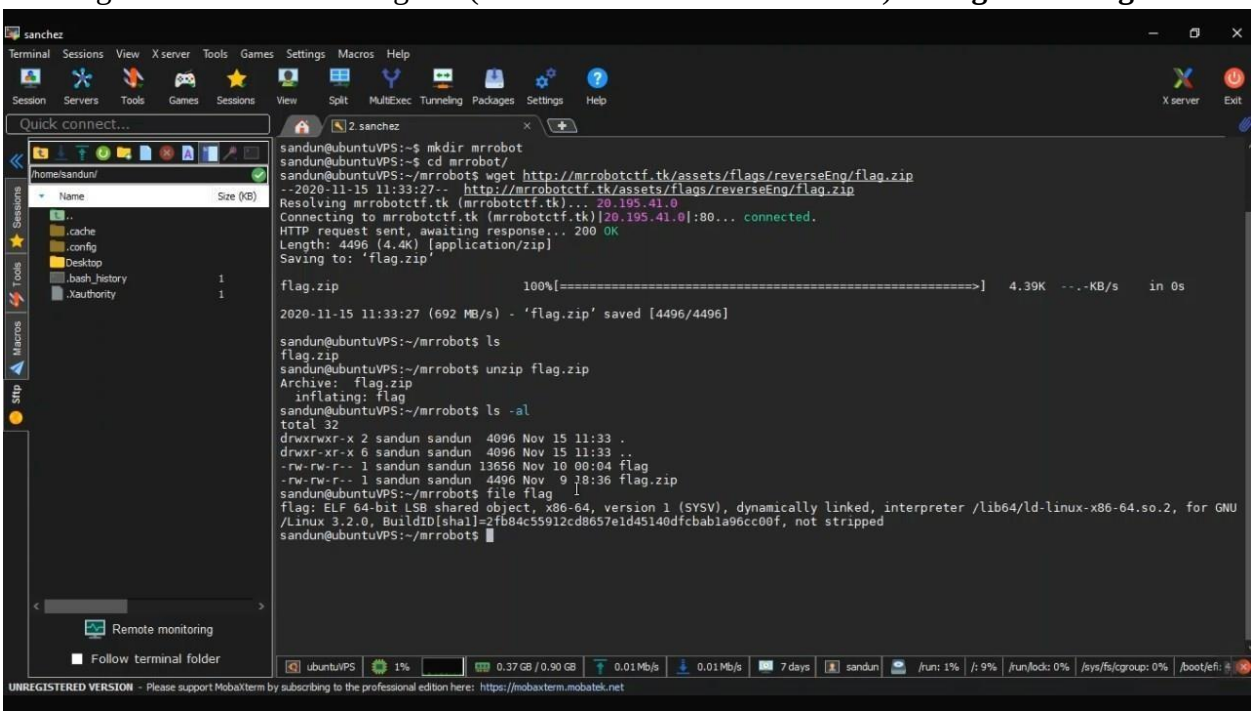
Level 7



First, I download the attachment on my Linux machine -> **Using wget 'path' command.**

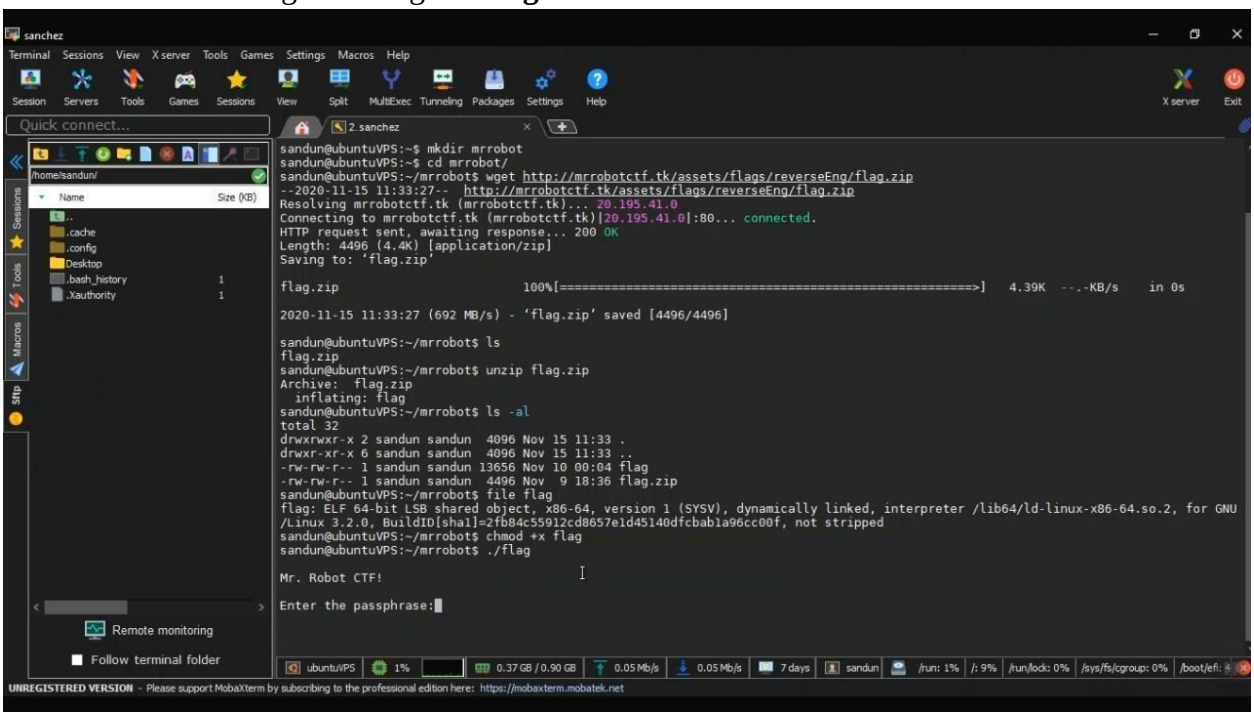
and then I unzip the .zip file. -> **Using unzip flag.zip**

Then I get the details about flag file (to know about what kind of file). **Using -> file flag**

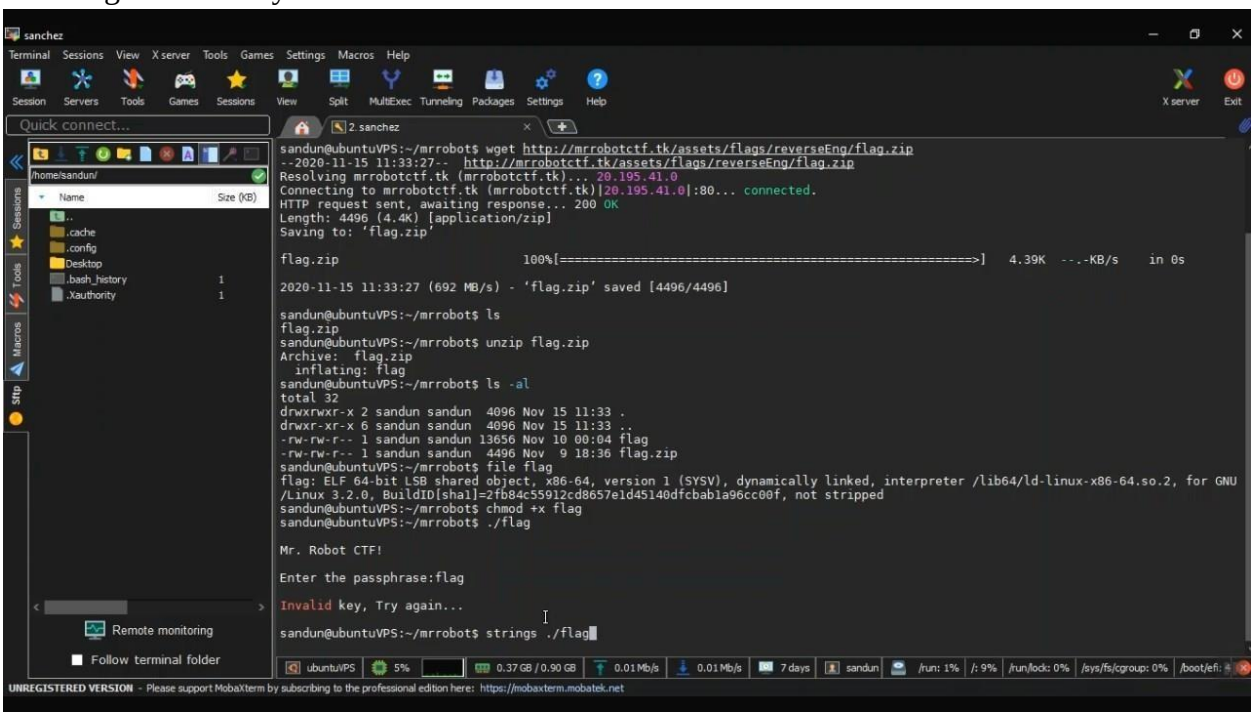


That flag file is executable file. but file can't execute because of their wasn't permission. So I use command as -> **chmod +x flag**

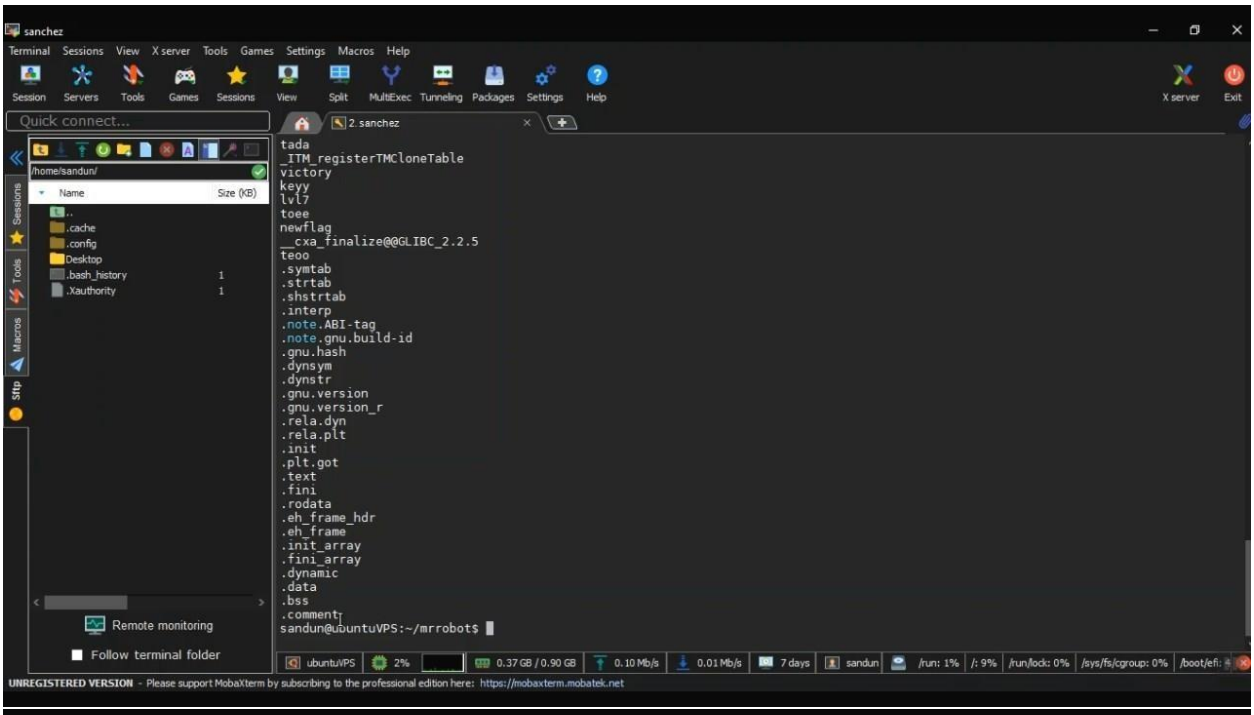
Then I execute the flag file using -> **./flag** command.

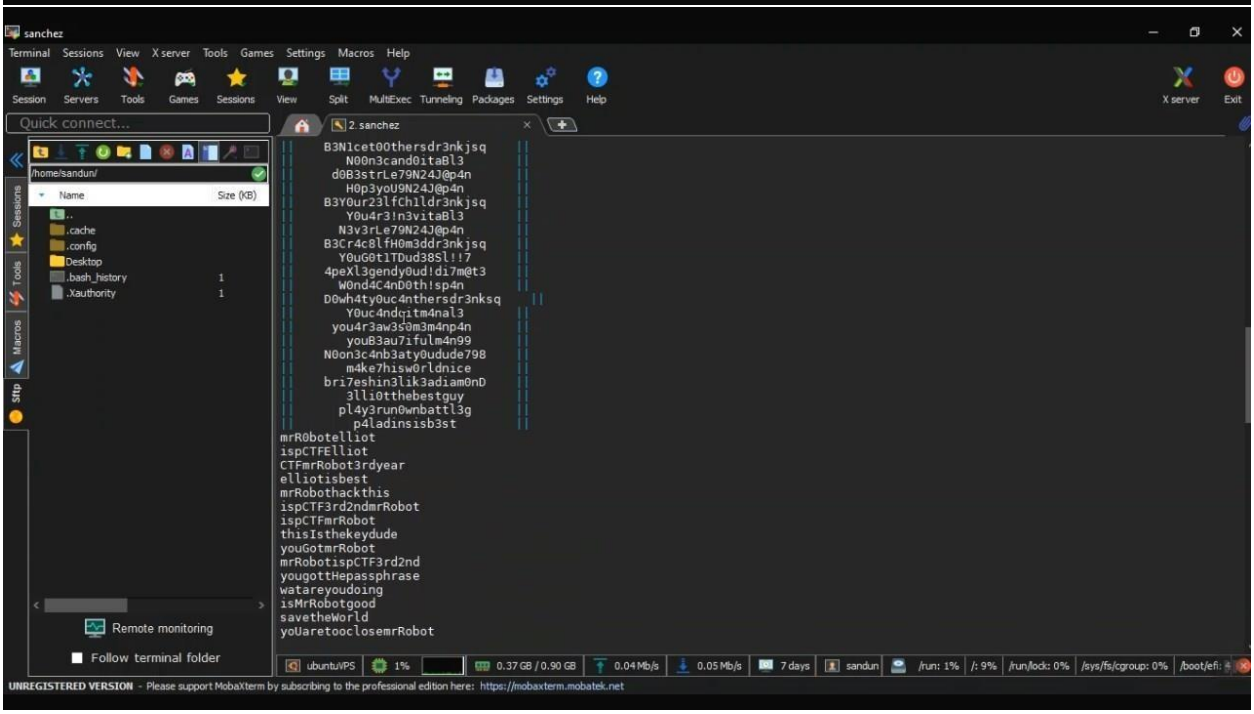


That ask Passphrase, But I do not know the passphrase. I tried random password as flag their was a message Invalid key.



Then I use **strings ./flag** command to determine the contents of and to extract text from binary files.





There are so many strings I cannot all of those as passphrase key.

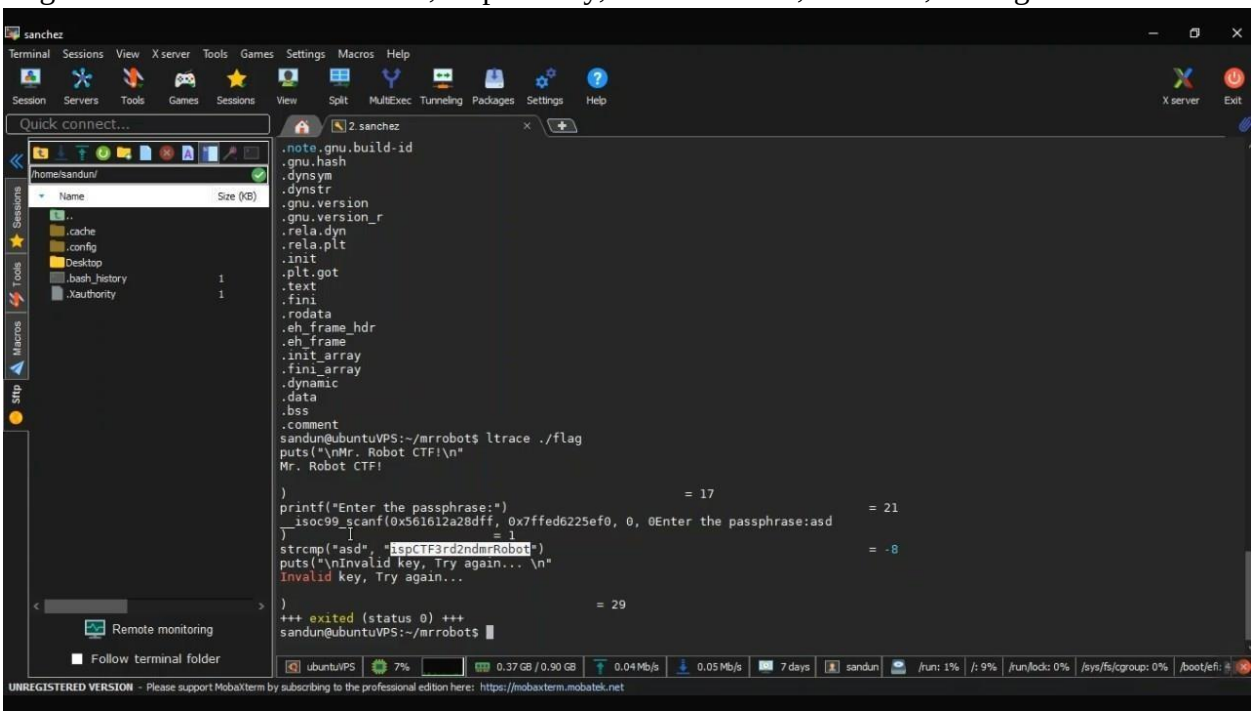
Then I use **ltrace ./flag** command to find passphrase.

After using **ltrace** command that ask Passphrase I do not know the Passphrase. Then I Enter **asd** for passphrase, but you can use any value as passphrase.

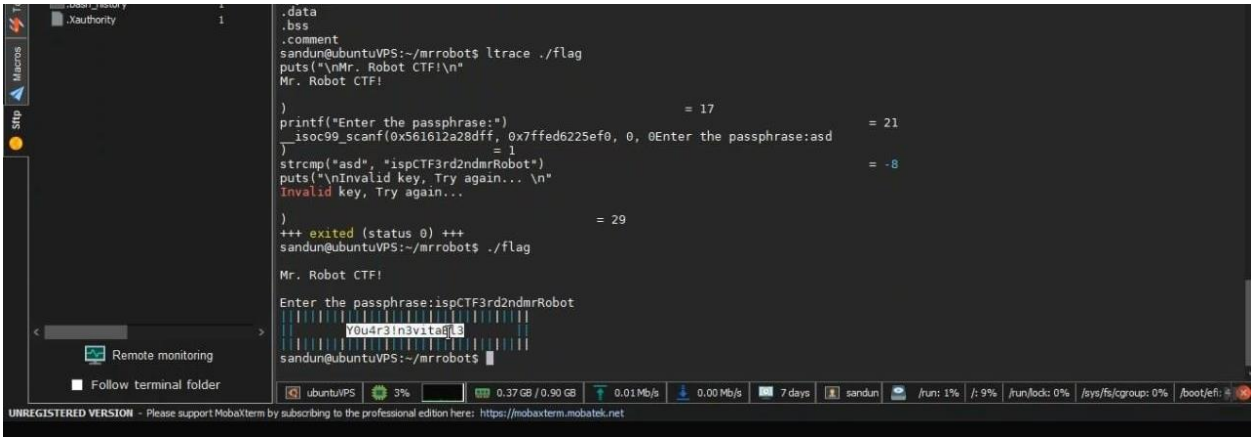
That compare Entered value and matched passphrase under **strcmp.**

ltrace is a program that simply runs the specified command until it exits. It intercepts and records the dynamic library calls which are called by the executed process and the signals which are received by that process. It can also intercept and print the system calls executed by the program.

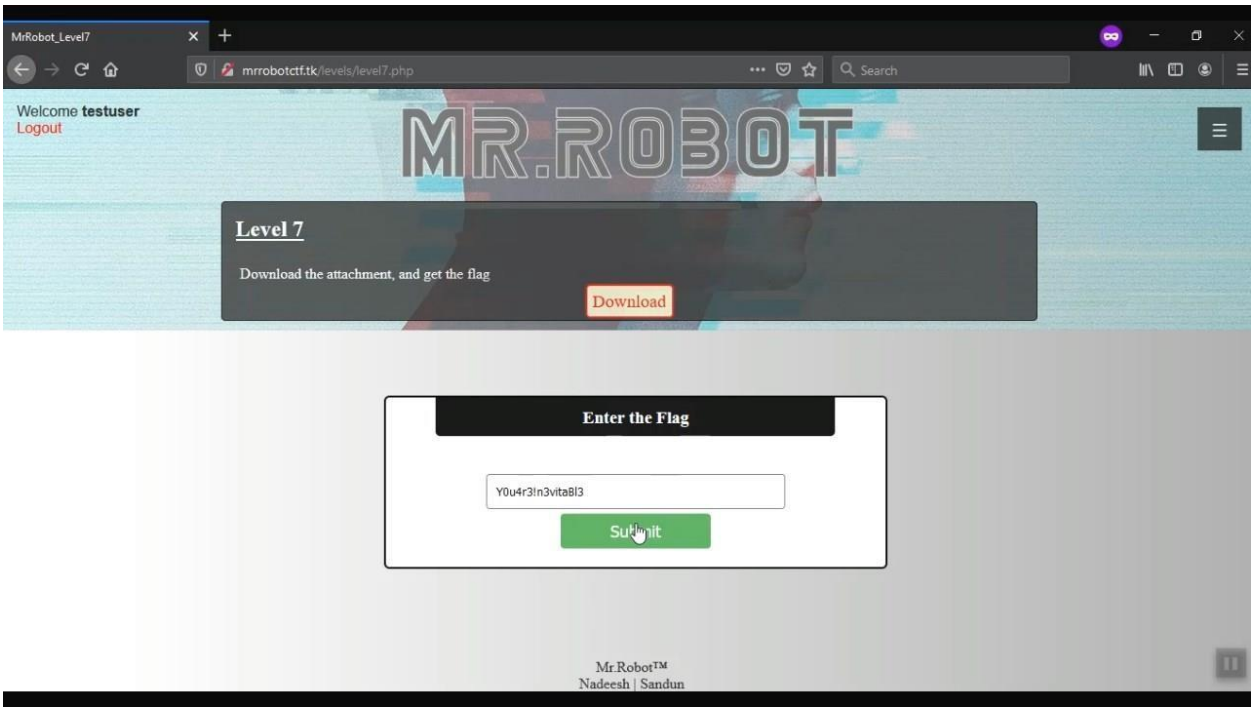
The **strcmp**() function compares the two strings s1 and s2. It returns an integer less than, equal to, or greater than zero if s1 is found, respectively, to be less than, to match, or be greater than s2.



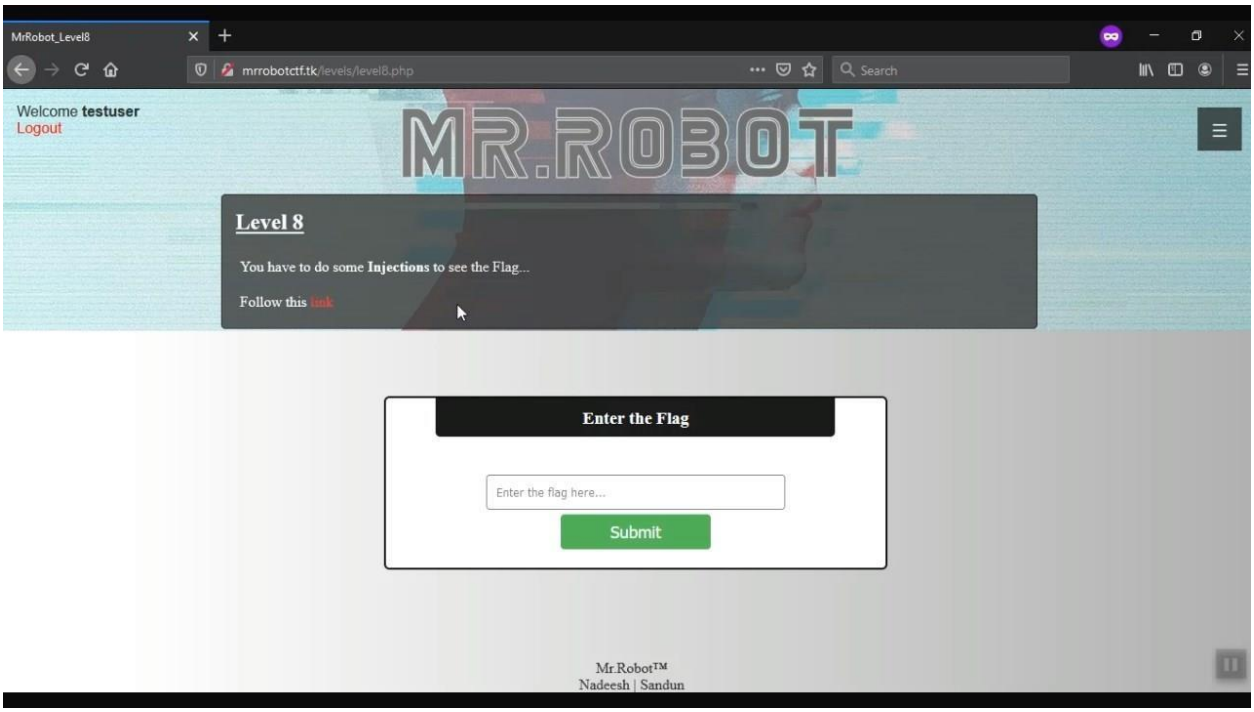
That selected value is the Passphrase of the flag file. Then I enter that value for passphrase in flag file.



That highlighted value is the Level 7 flag.

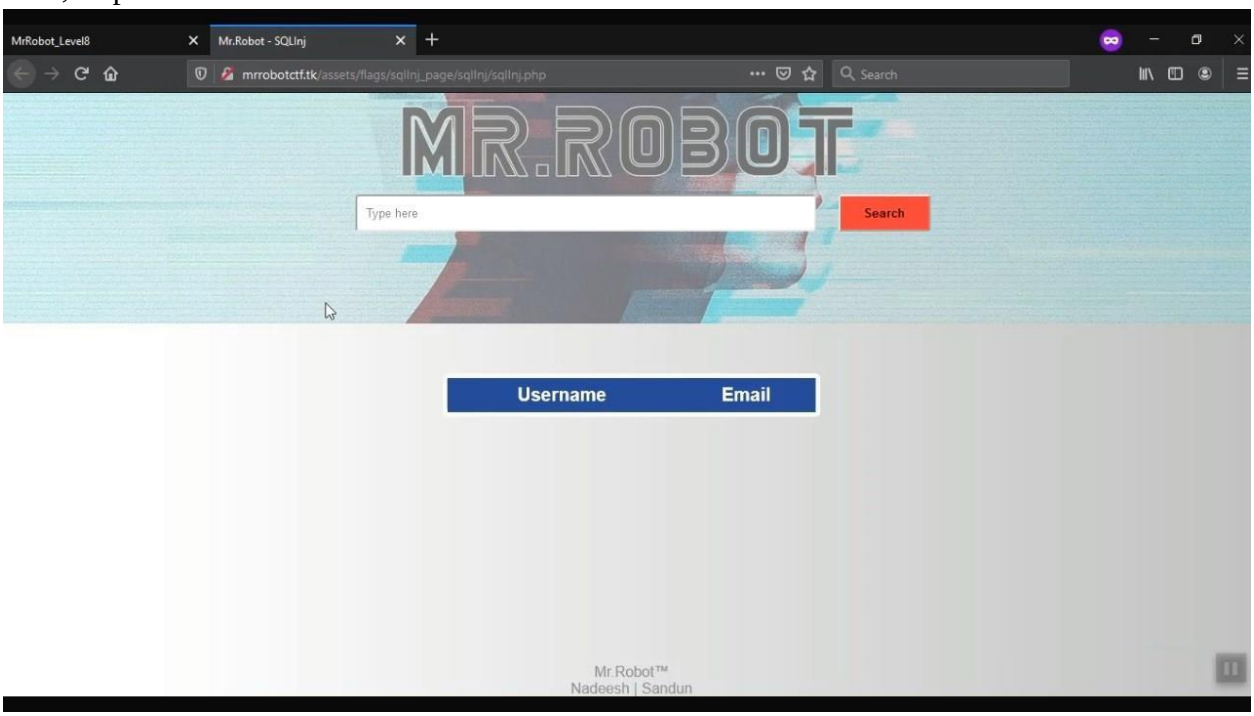


Level 8

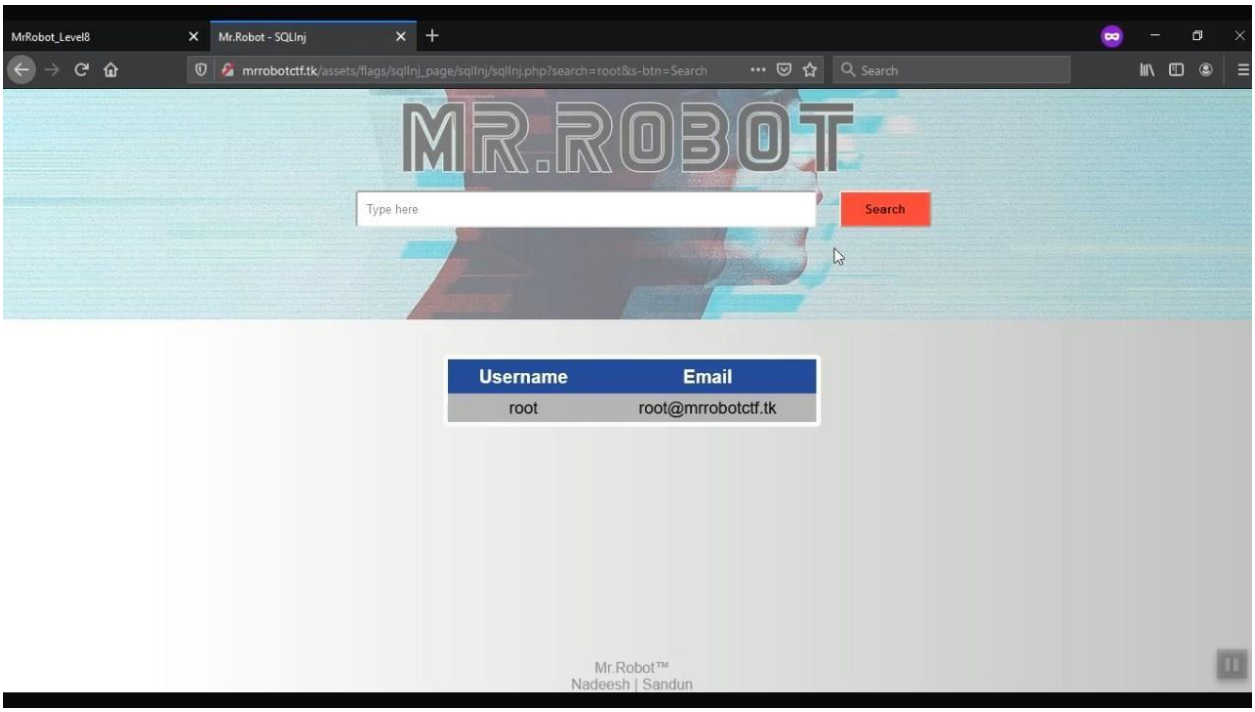


This is SQL Injection related flag.

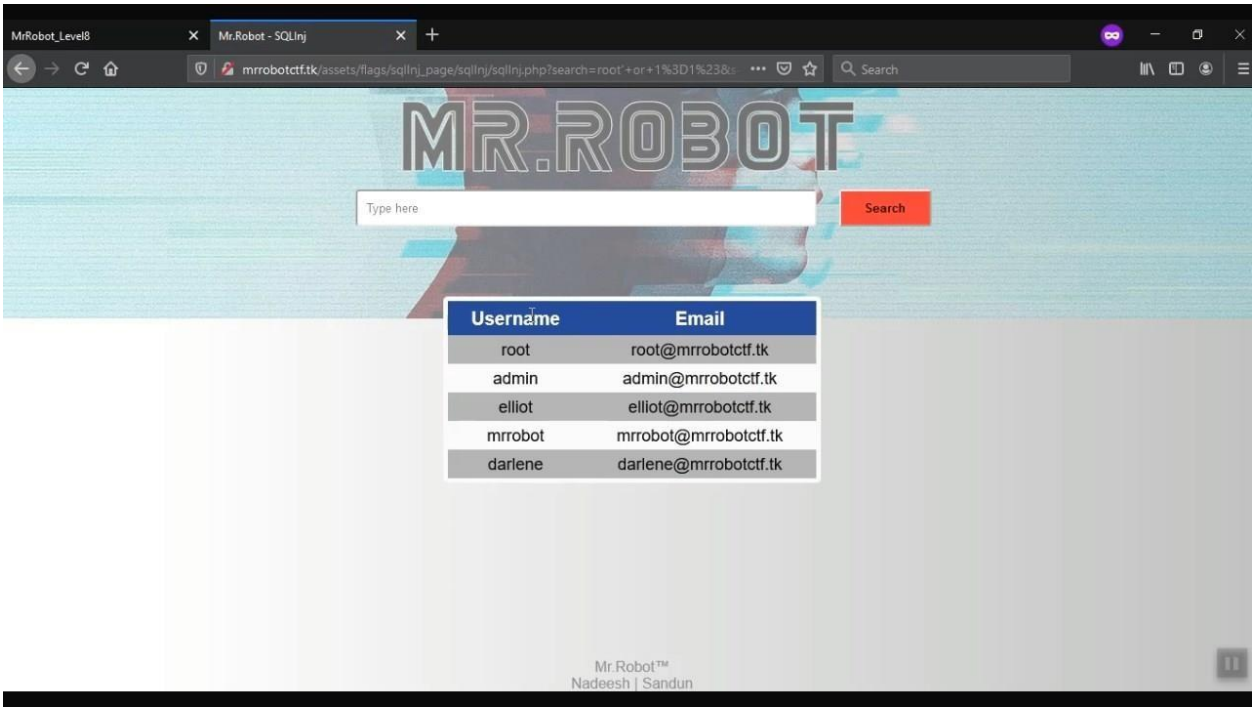
First, I open the link and search for the users.



I enter **root** in search box and click search button for search user.

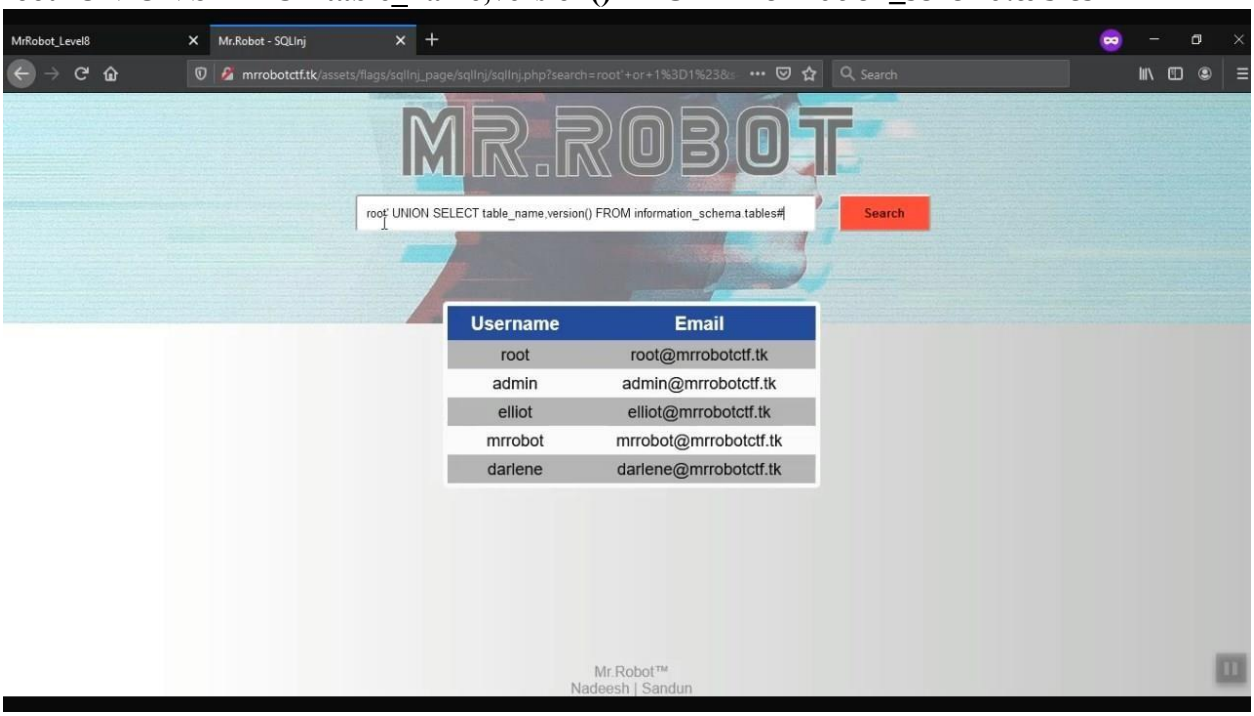


Then I use **root' or 1=1#** SQL command to list all users.



Then I find all tables using this command.

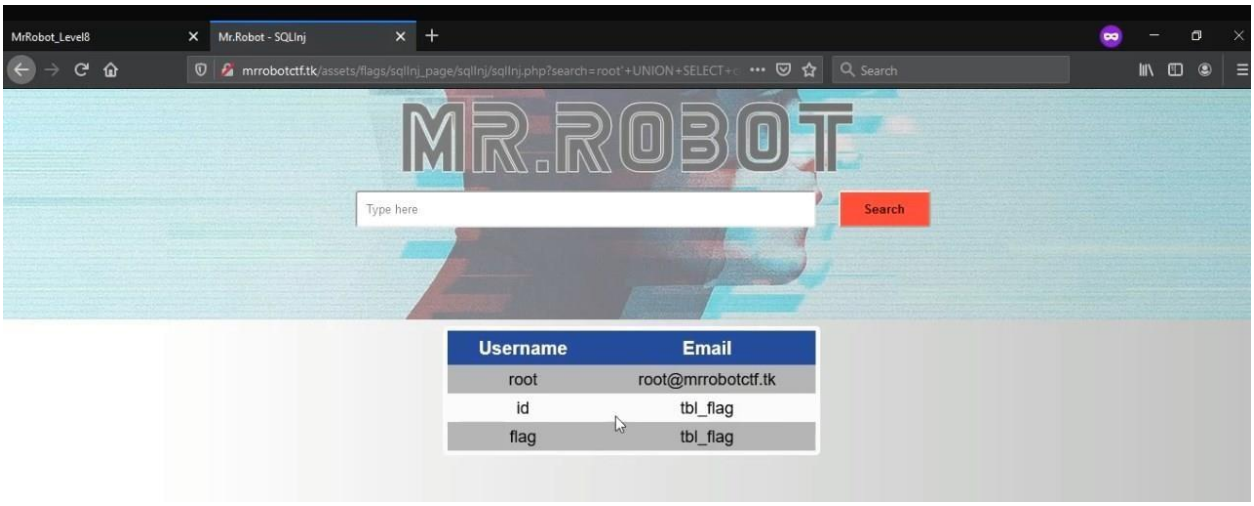
root' UNION SELECT table_name,version() FROM information_schema.tables#



Then I found that there are a table named **tbl_flag**.

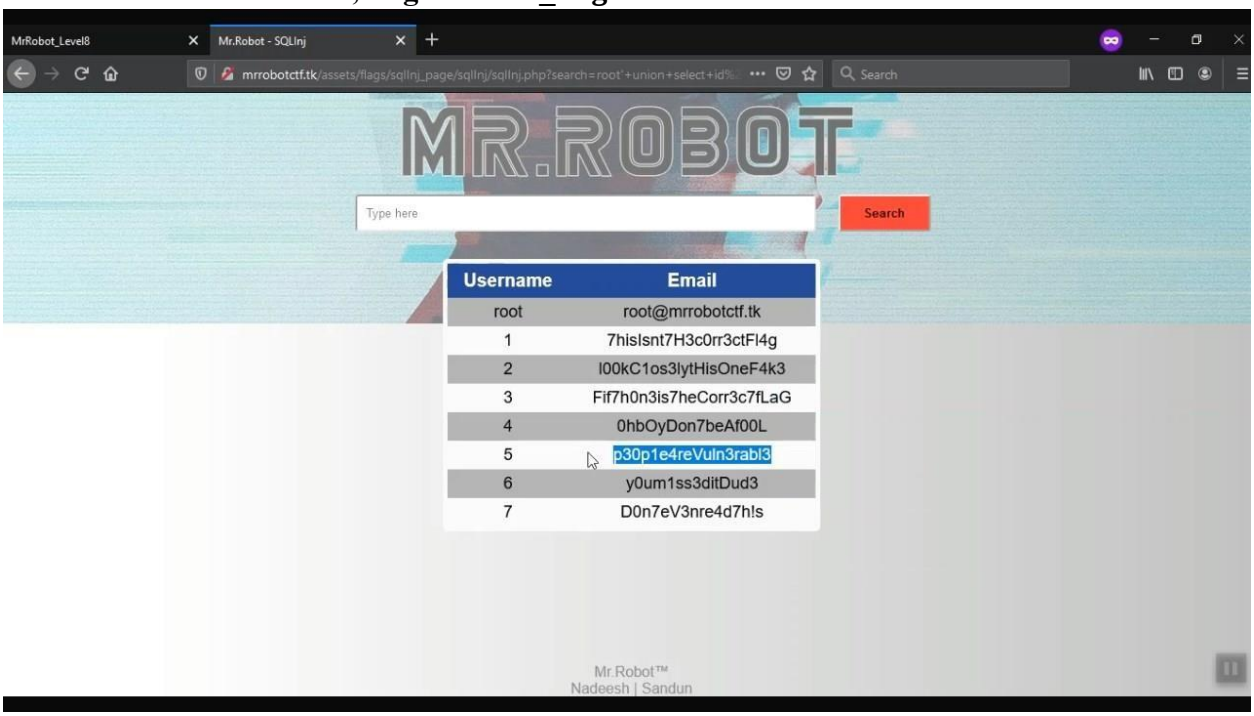
Then I use below injection command to see columns of tbl_flag table.

root' UNION SELECT column_name,table_name FROM information_schema.columns WHERE table_name='tbl_flag

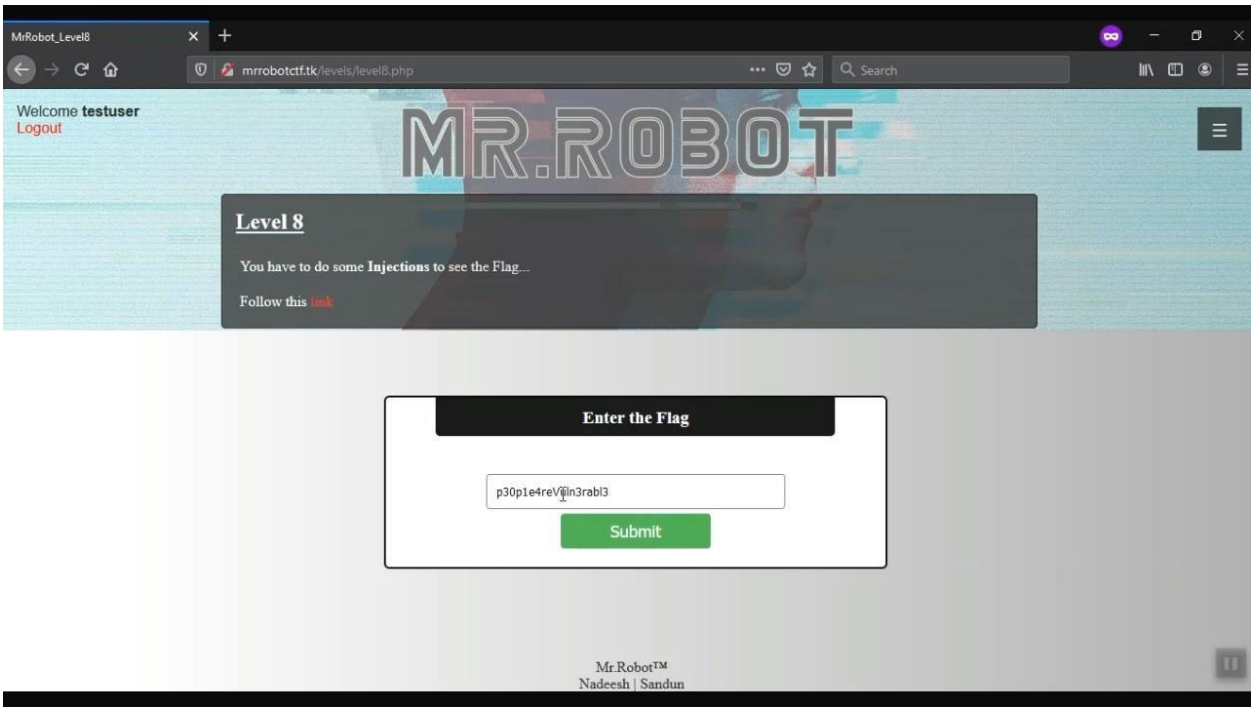


There are two columns **id** and **flag**,
I use below command to show all the rows of **tbl_flag** table.

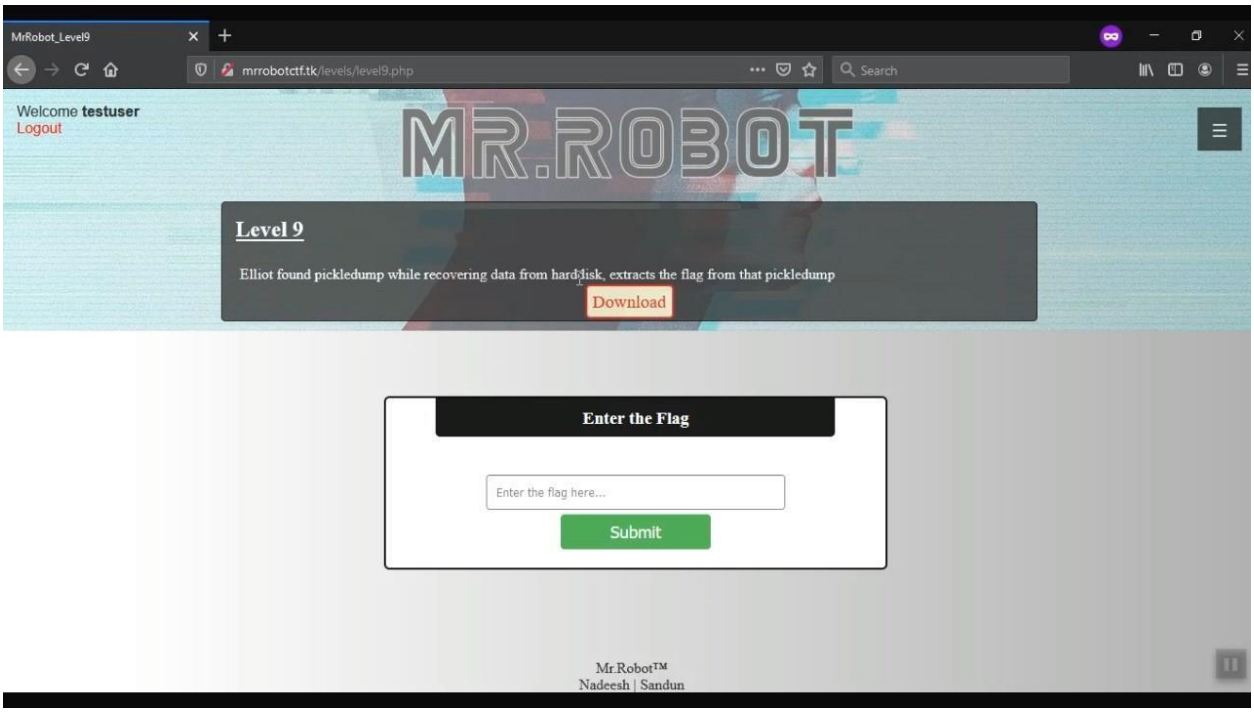
root' UNION SELECT id, flag from tbl_flag#



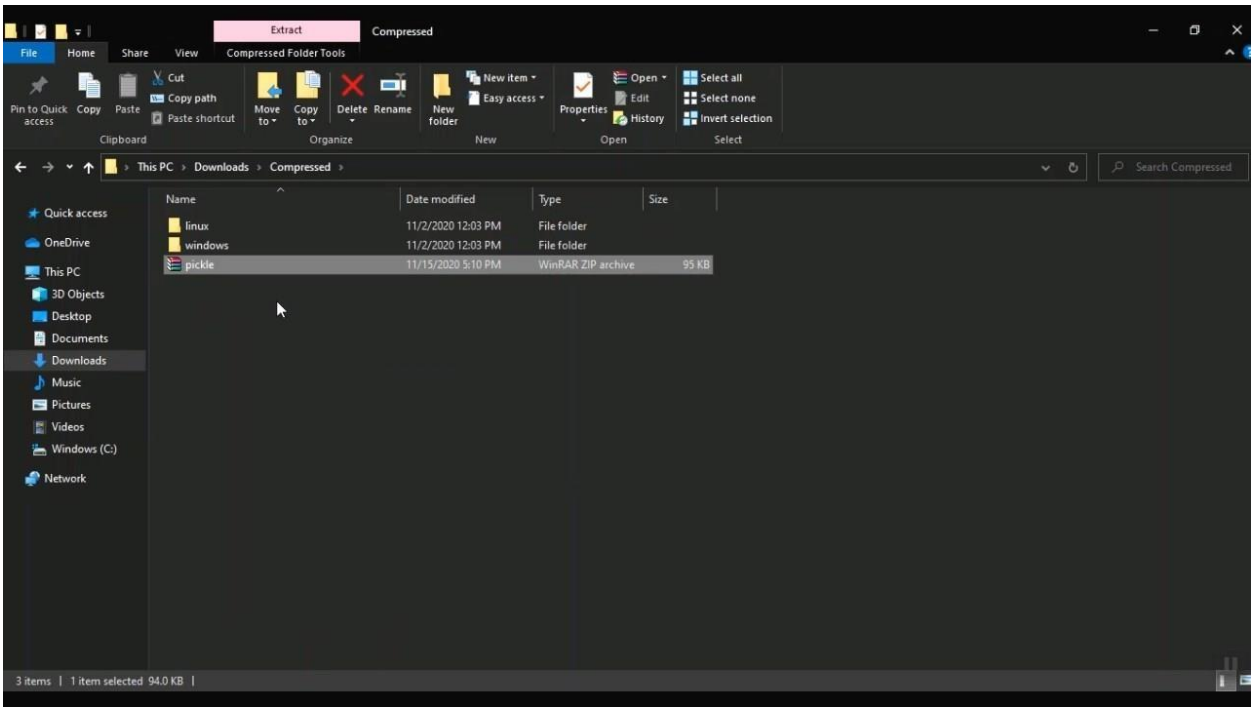
This highlighted value(id number 5) is the Level 8 flag. (in 3rd row saying fifth one is the correct flag)



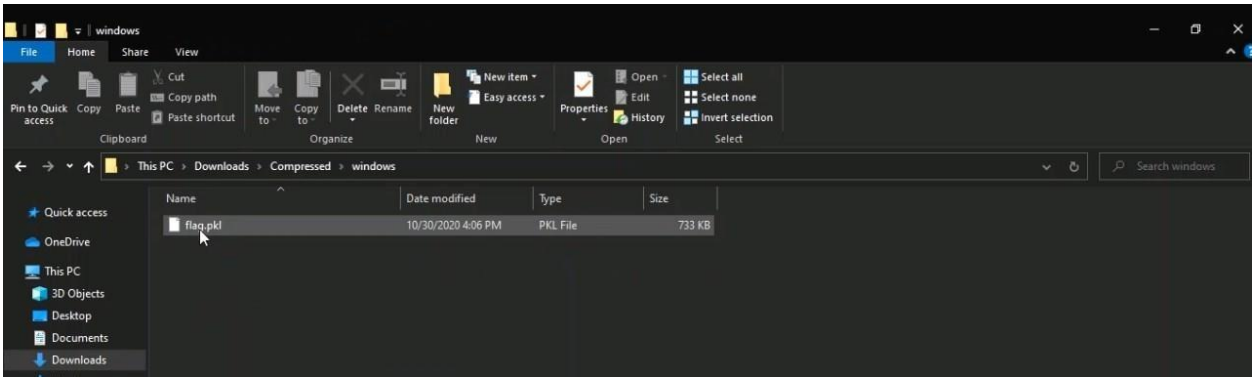
Level 9



First, I download the file and extract it.



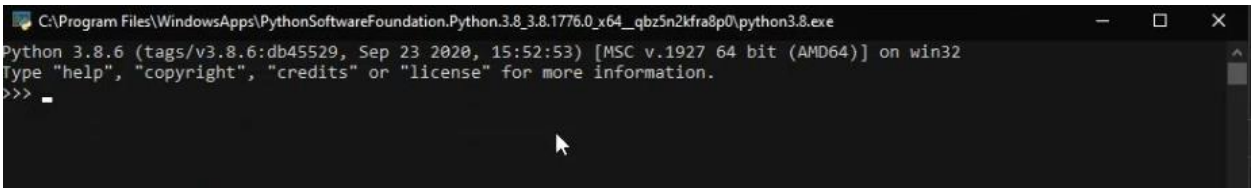
I will do that in a Windows environment because of that I opened the windows folder.



This is a pickle file.

"Any object in Python can be pickled so that it can be saved on disk. What **pickle** does is that it 'serializes' the object first before writing it to file. Pickling is a way to convert a python object (list, dict, etc.) into a character stream."

Then I open python terminal.



Since this is pickle file I import pickle using **import pickle**

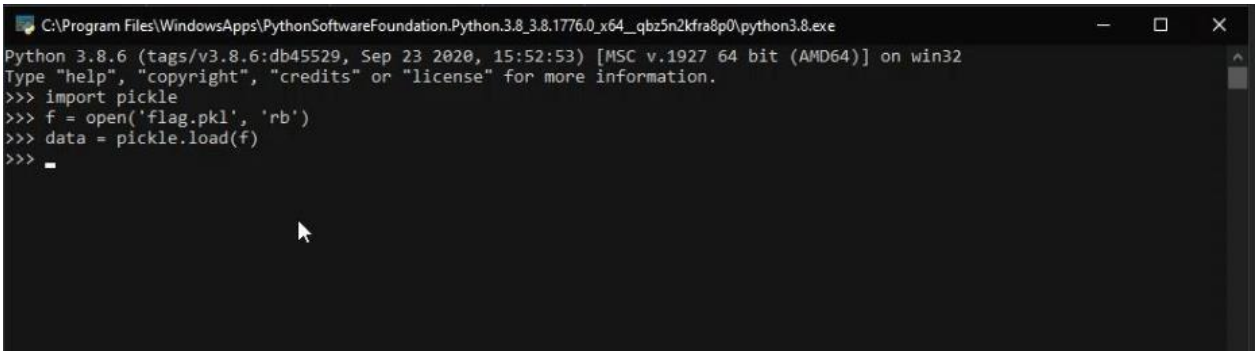
Then I create a variable call f and open that pickle file.

f = open('flag.pkl', 'rb')

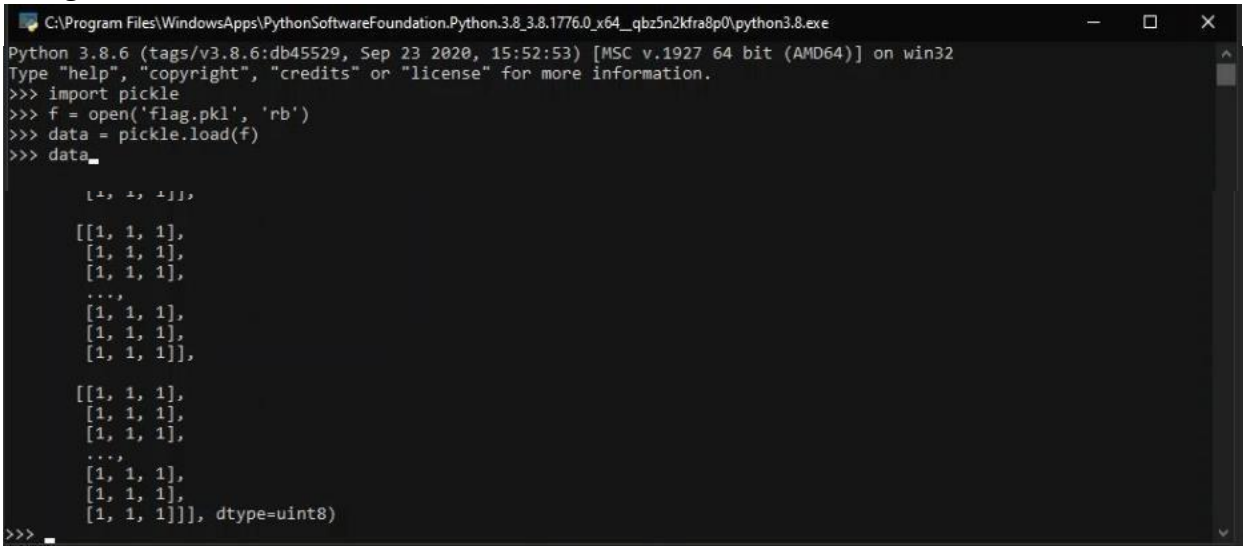
The **open()** function opens a file in text format by default. To **open** a file in binary format, add 'b' to the mode parameter. Hence the "**rb**" mode opens the file in binary format for reading

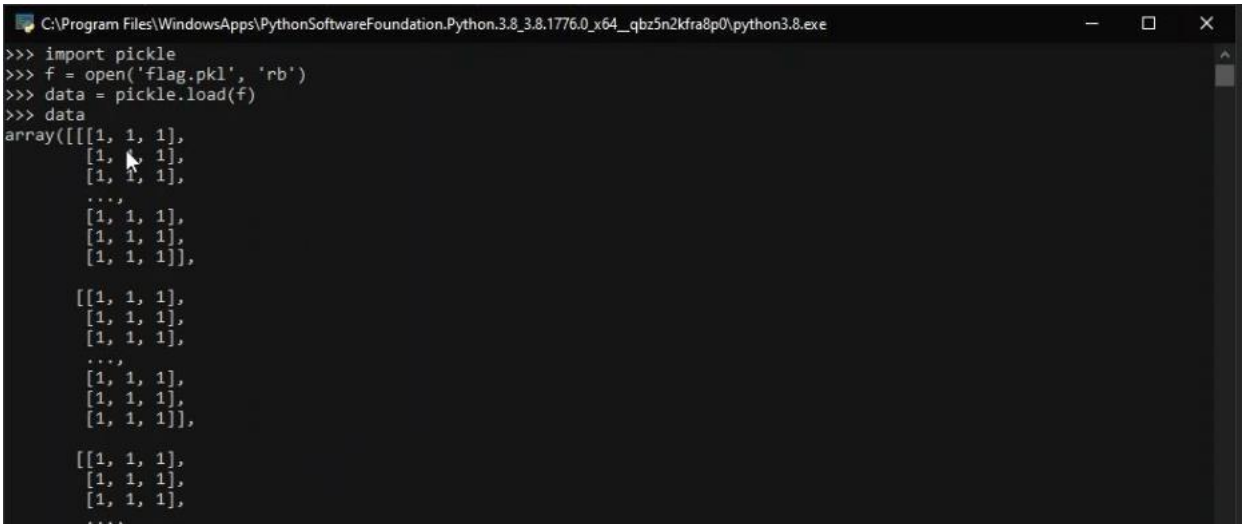
Then I create another variable called **data** and retrieve pickled data (f) to the data variable.

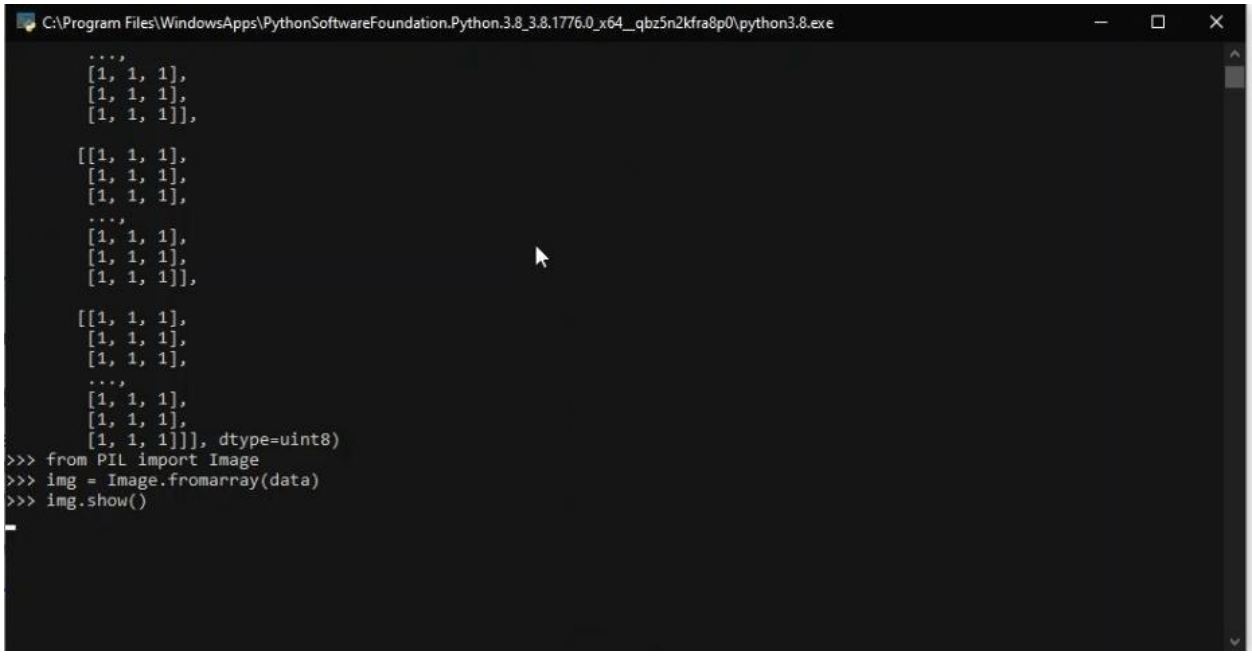
pickle.load(f)



Then lets see the data
Using **data**







This is a 3d array in this array there is a **dtype=uint8**

Google it and you will be see it's contain a image.

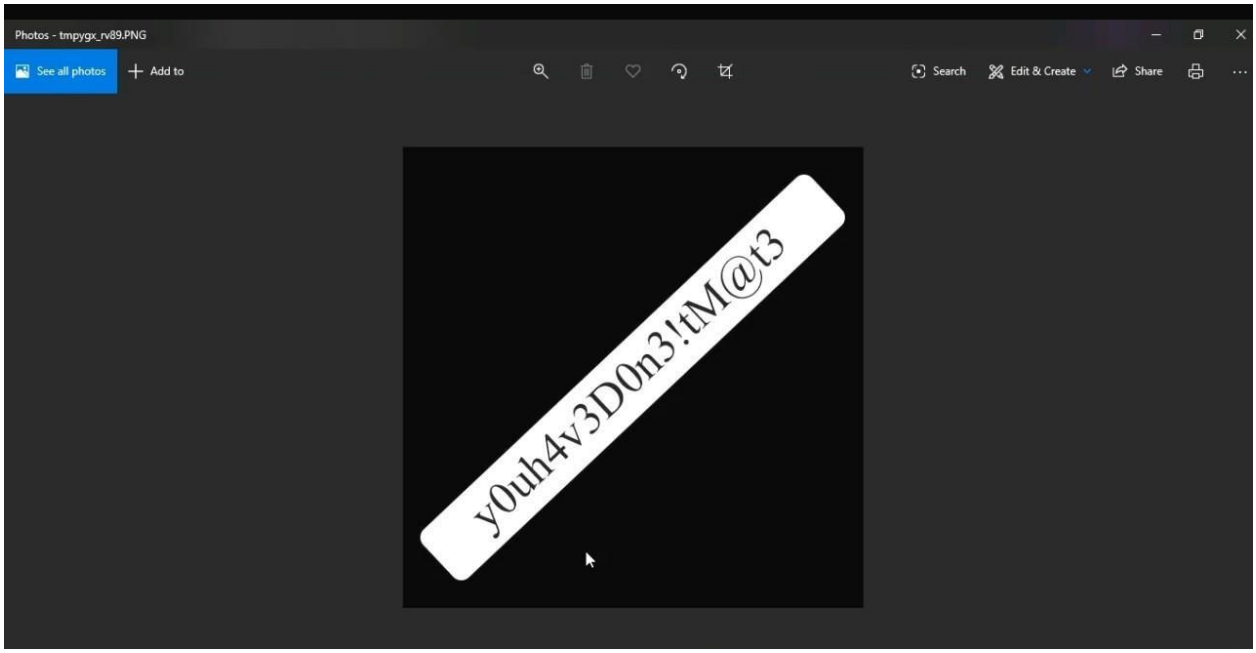
So I used to below commands to create image using array data.

from PIL import Image

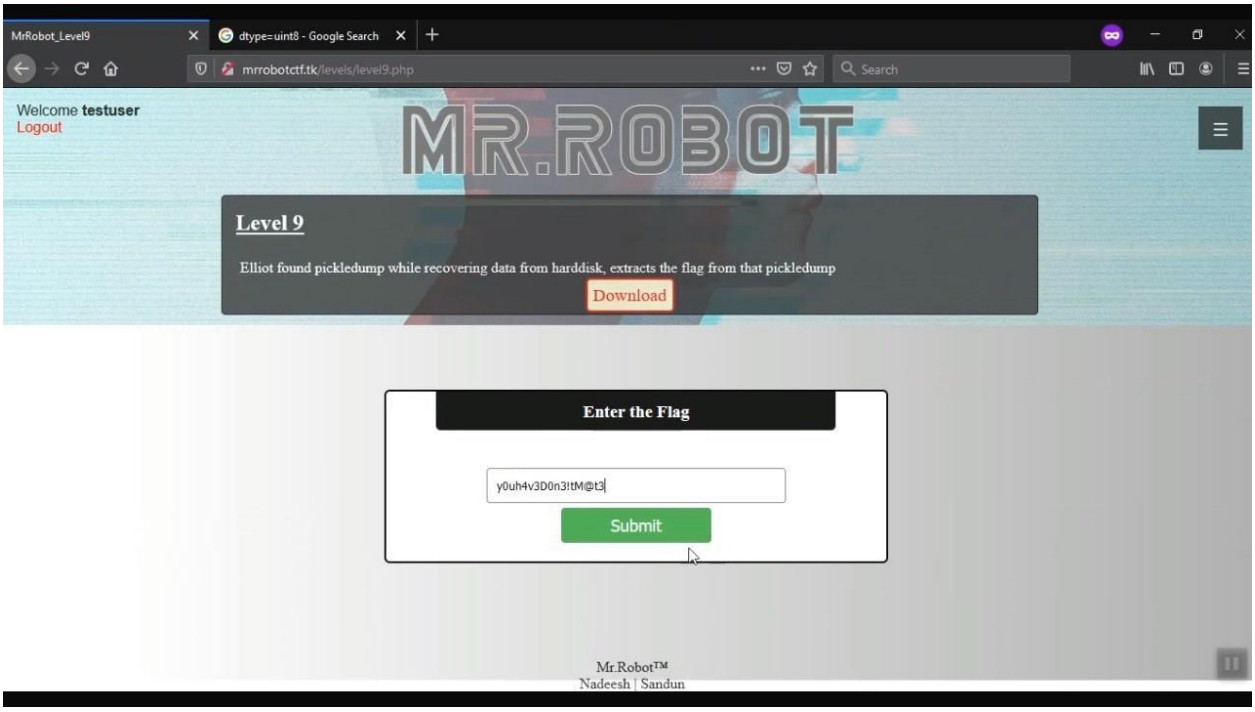
img = Image.fromarray(data)

img.show()

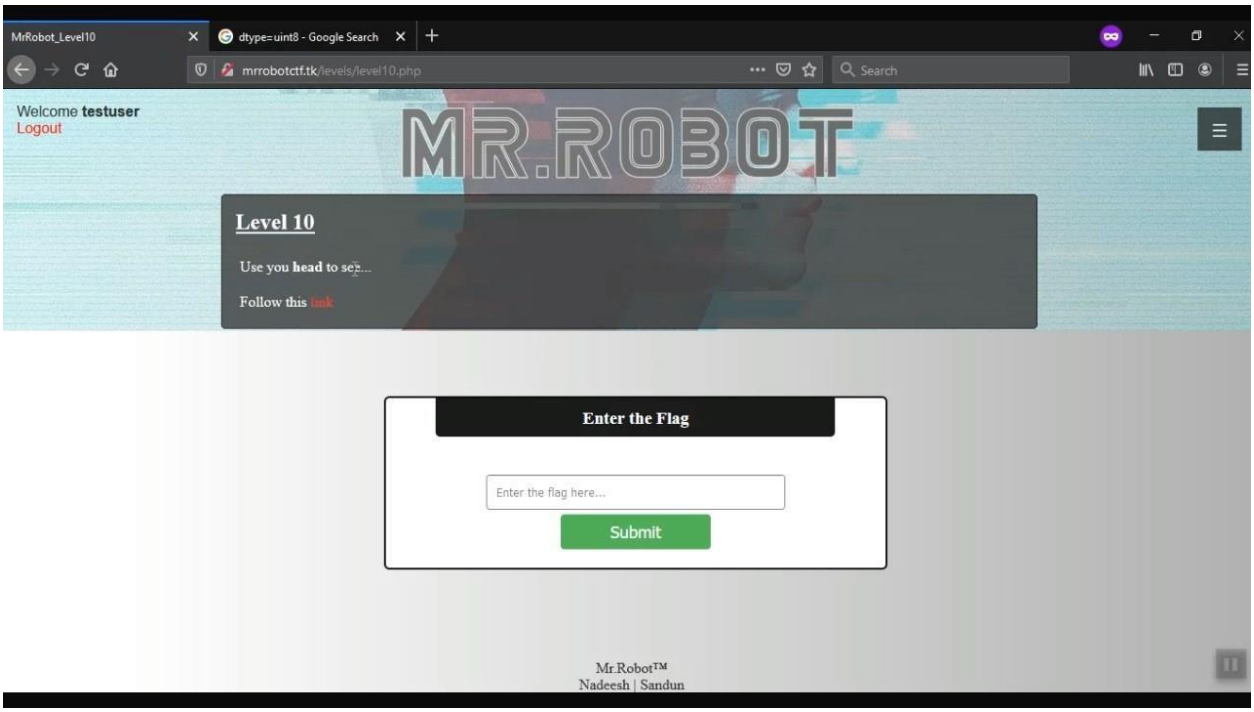
After the use those commands I got this Image. And its contains the flag.



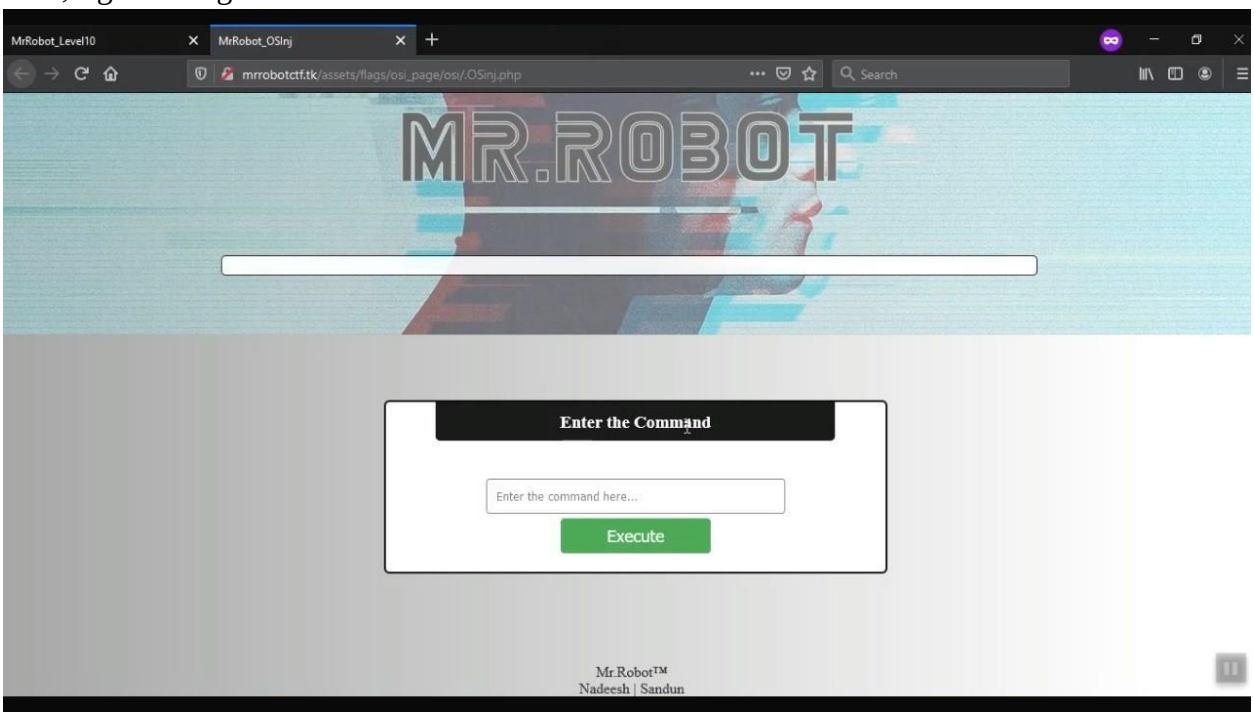
I submitted the flag.



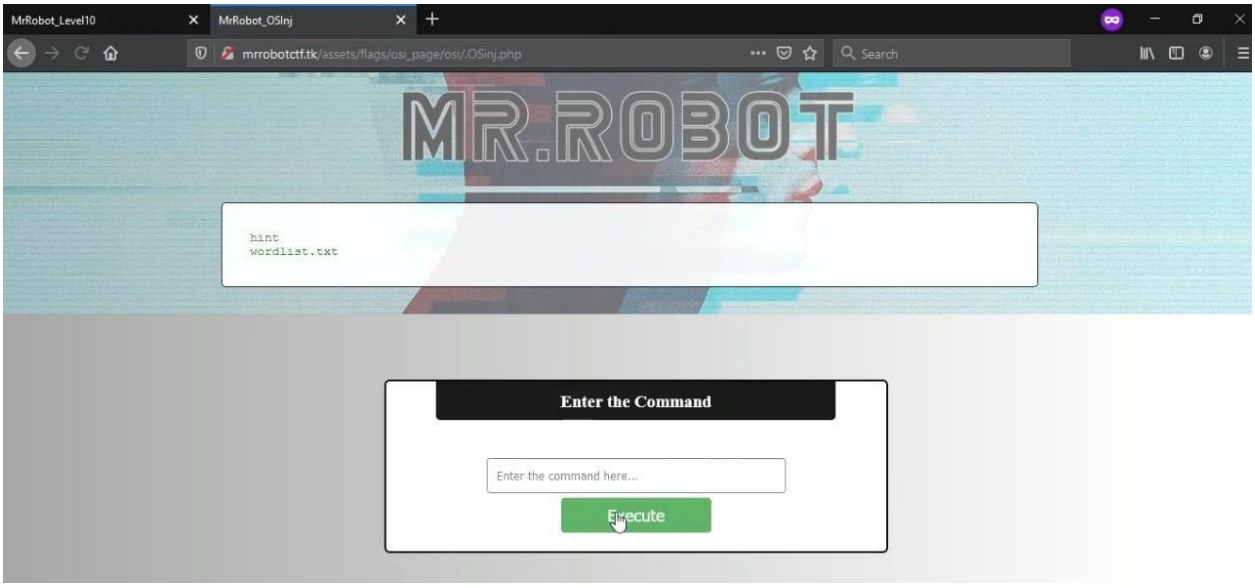
Level 10



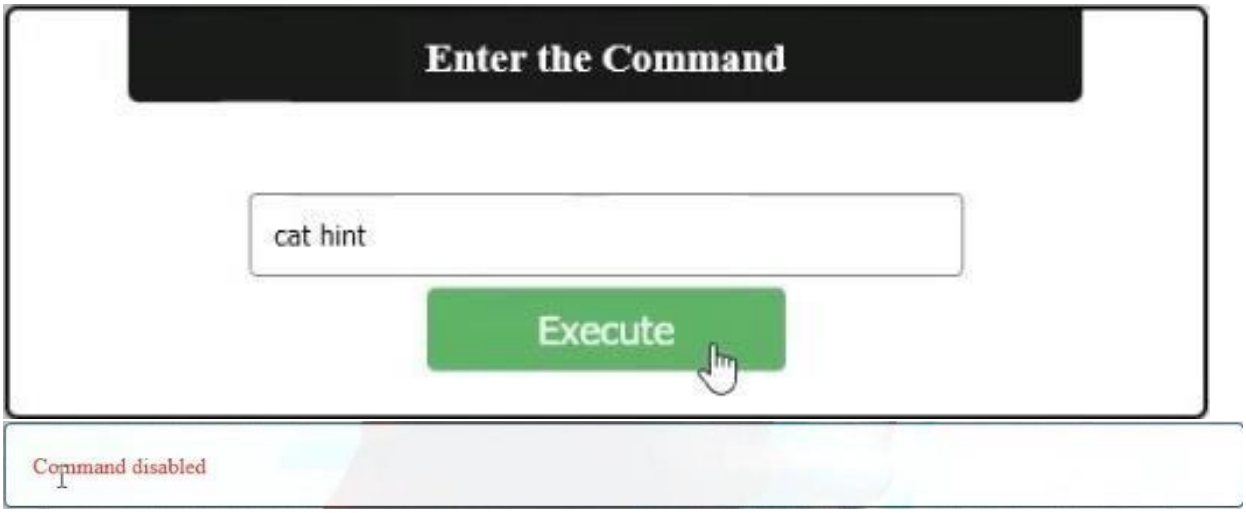
First, I go to the given link.



This command field work as terminal. first I use **ls** command to list the file.

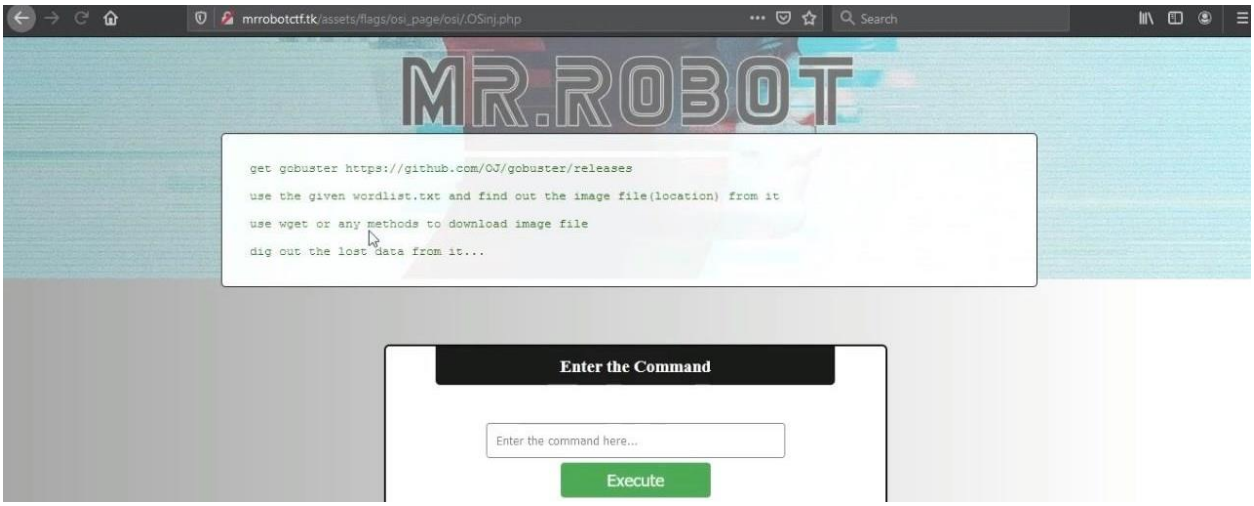


Then I use cat command to view file, but it does not work. Because of some command disabled.



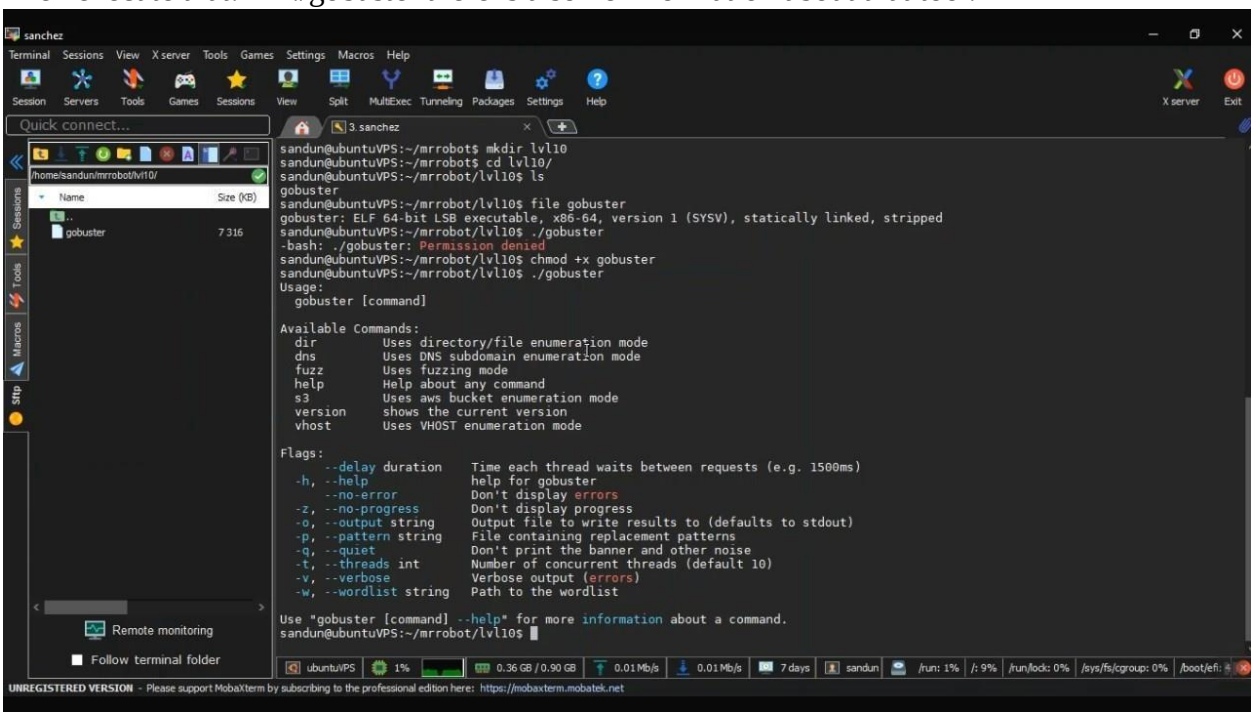
Level hints give a very useful hint for us. He said **use you head to see..** that's mean we can use head command to view files.

First, I view the hint file.

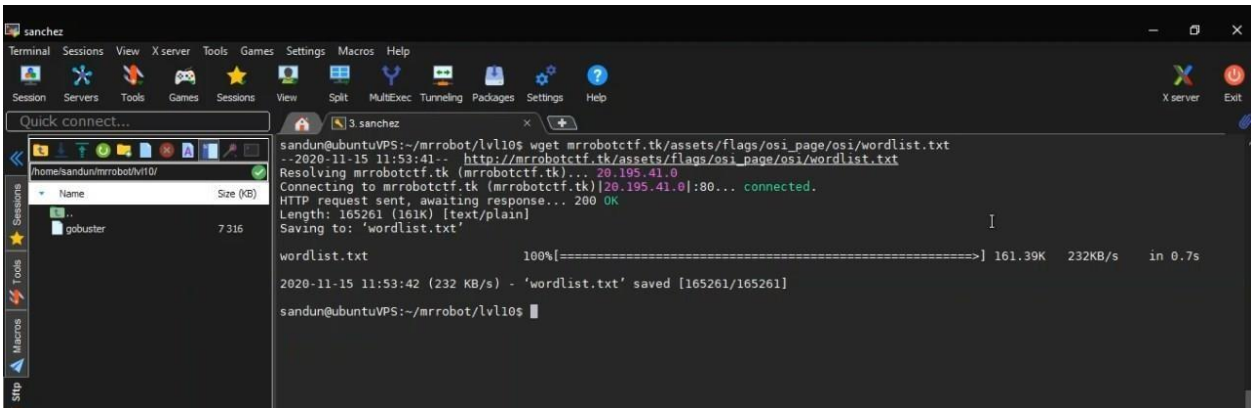


There are link to download a tool called gobuster.
Go buster used to directory listing in the website.
I so download the **gobuster-linux-amd64.7z (because I using Ubuntu)** file from that GitHub link. Then I execute the gobuster file. But I can't execute that. Then I give permission for execute that file.
chmod +x gobuster

Then execute that. -> ./gobuster there is a some information about that tool.

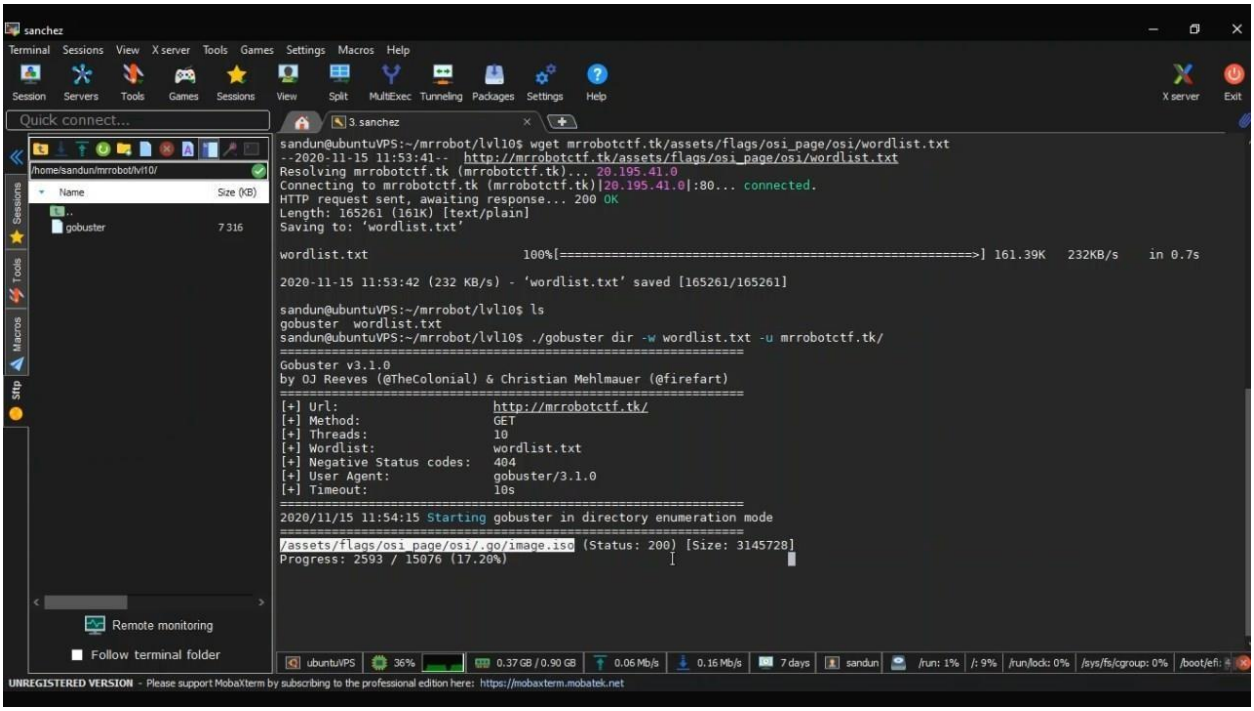


Then get the wordlist.txt file location from the CTF website and download it for pc.

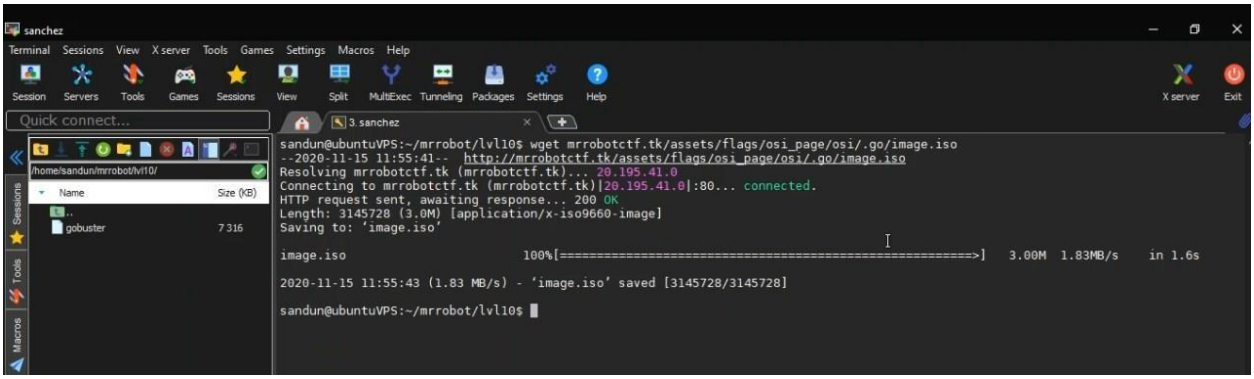


Then I use that wordlist file to find out the image file containing this website
./gobuster dir -w wordlist.txt -u mrrobotctf.tk

Then I find the ISO file.

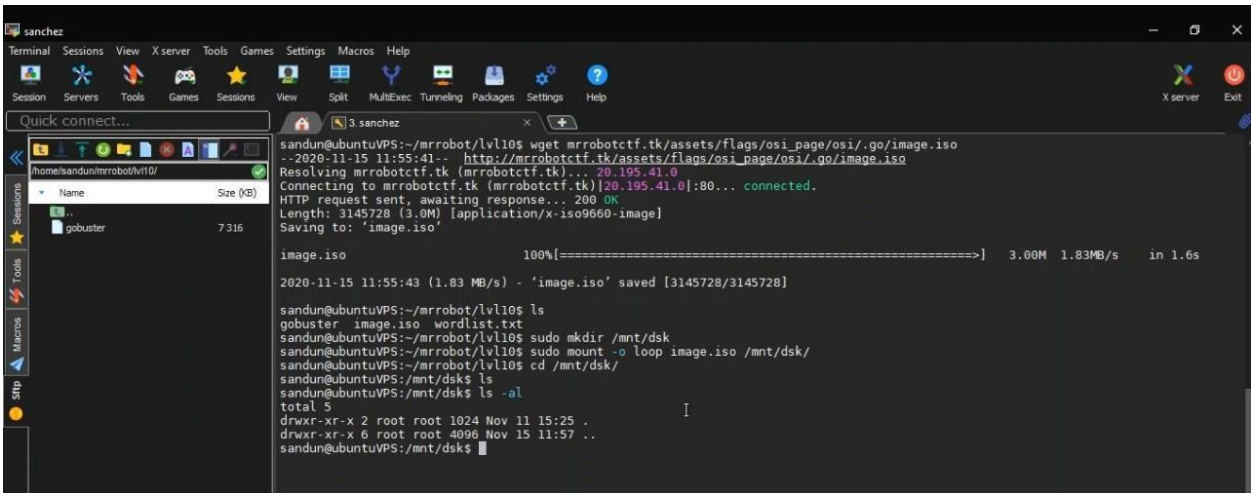


Then I download it to my pc.

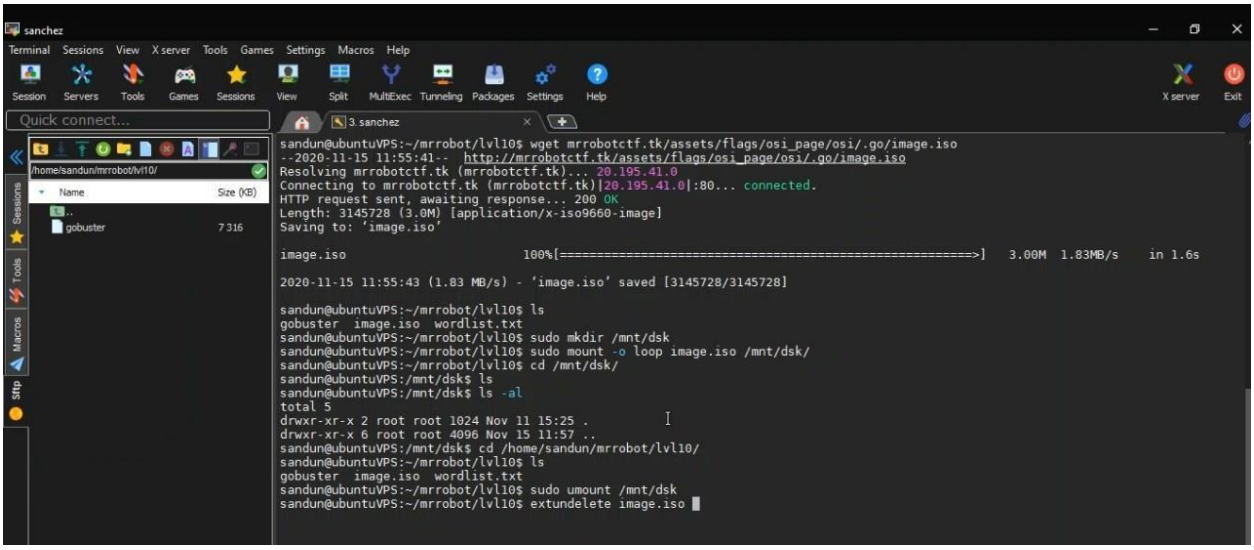


Then I mount the .ISO image to the system.
Sudo mkdir /mnt/disk/
Sudo mount -o loop image.iso /mnt/dsk/

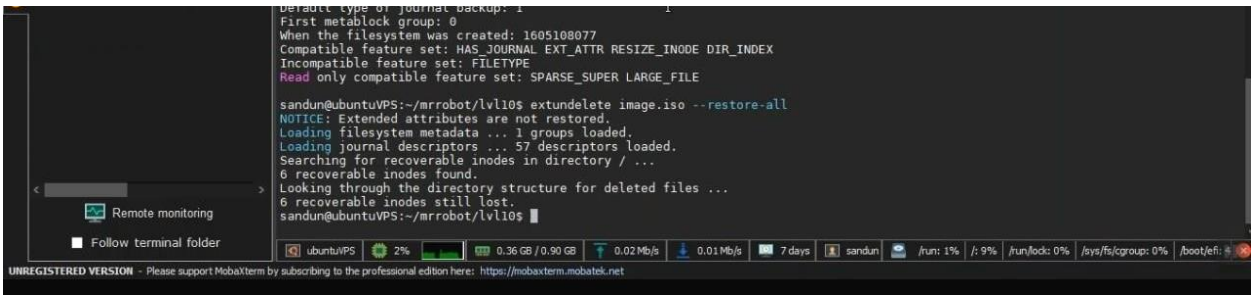
Go to the image location and list files. There are no files in it.
ls -al



Then Unmount and find the filesystem type. Best tool for get filetype is Extundelete.
Sudo unmount /mnt/dsk/

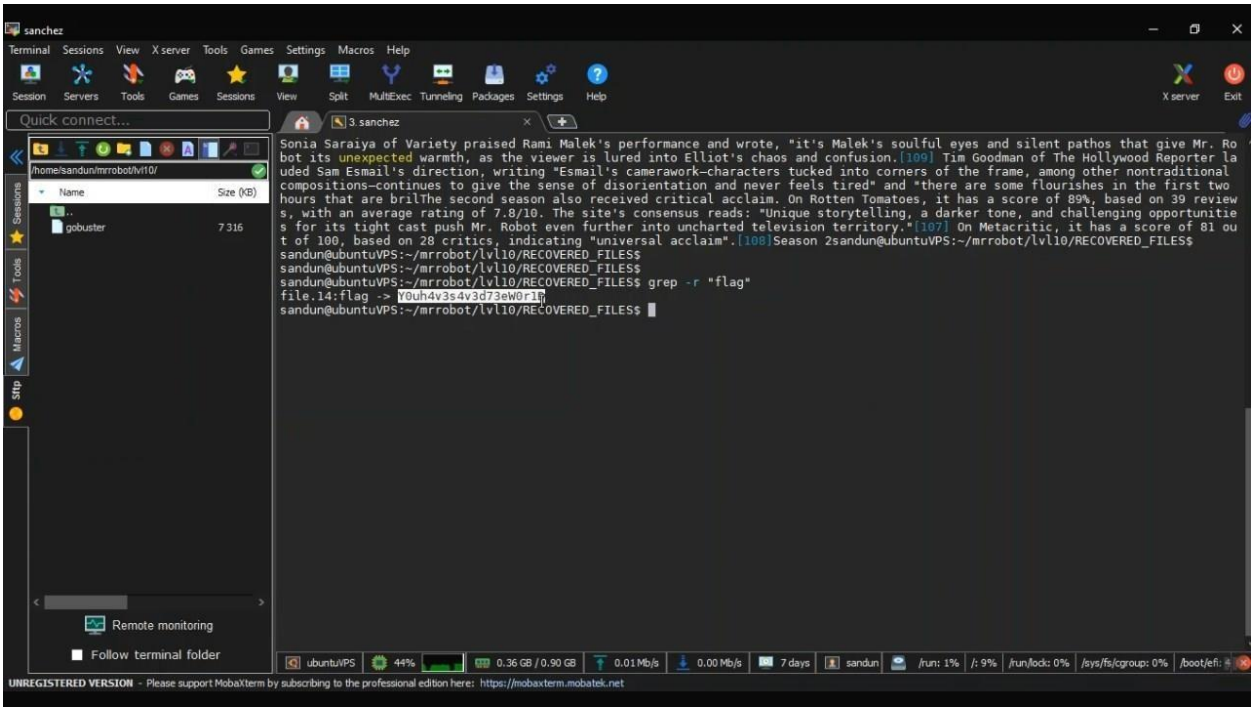


Using the command "extundelete" we can recover the files.
extundelete image.iso –restore-all

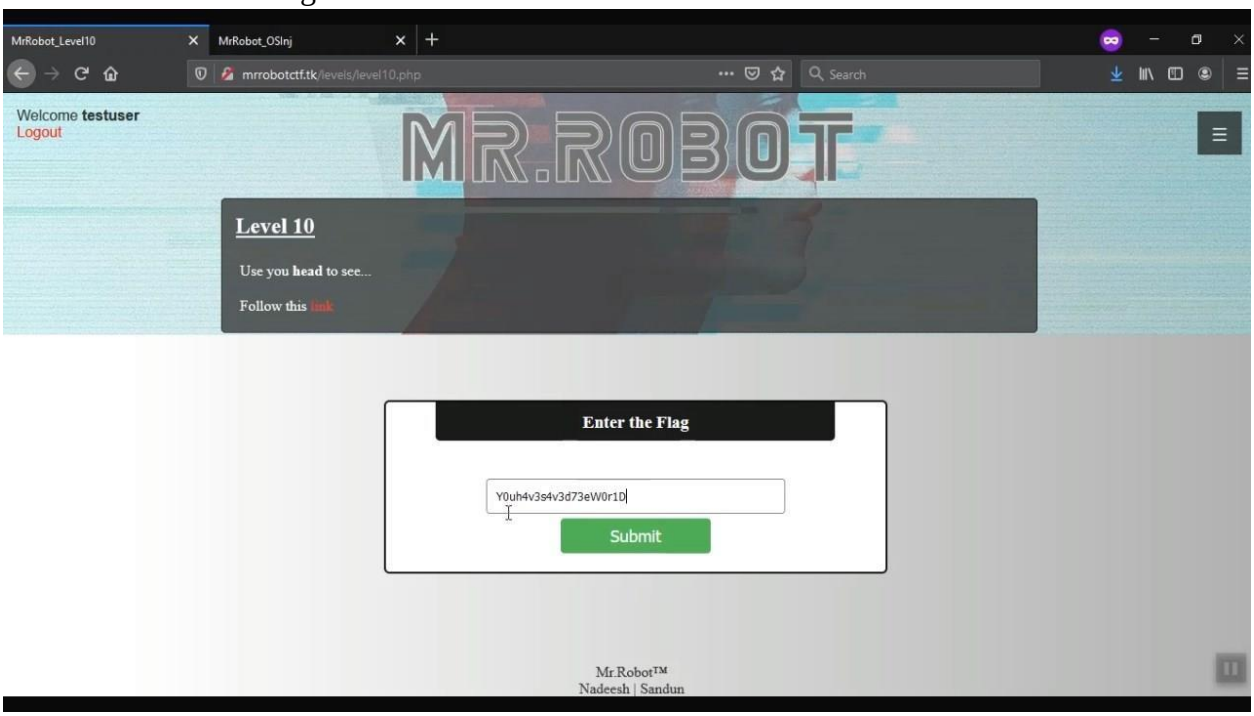


Then I go to RECOVERED FILES folder.
There are some file I see some file but couldn't find the flag
Then I used grep tool to get the flag

grep -r ‘flag’



That is the Level 10 flag. I submitted that.



Video Walkthrough Link:

https://mysliit-my.sharepoint.com/:v:/g/personal/it18095340_my_sliit_lk/EXFHalso4pBGqiV2Kvp76I8B3flWj4eDmr9wZ8Dy7BxIAA?e=zBuX9R

Github Link:

https://github.com/sandundananjaya/Mr.Robot-CTF