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

28 / 09 / 2020

Declaration

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

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

Table of Contents

Introduction

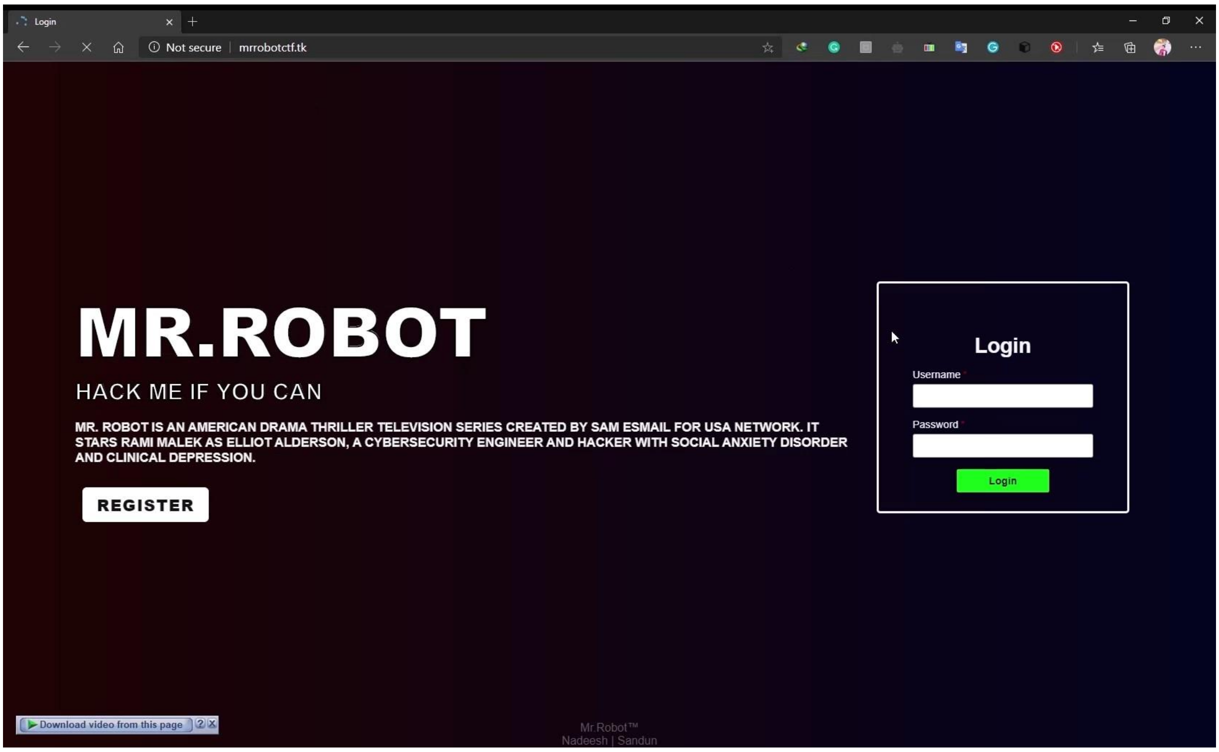
Capture the Flag (CTF) is an event that is usually hosted at information security conferences, including the various events. This event consists of a series of challenges that varies in their degree of difficulty, and that require participants to exercise different skill sets to solve. Once an individual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

Audience

Security Researchers

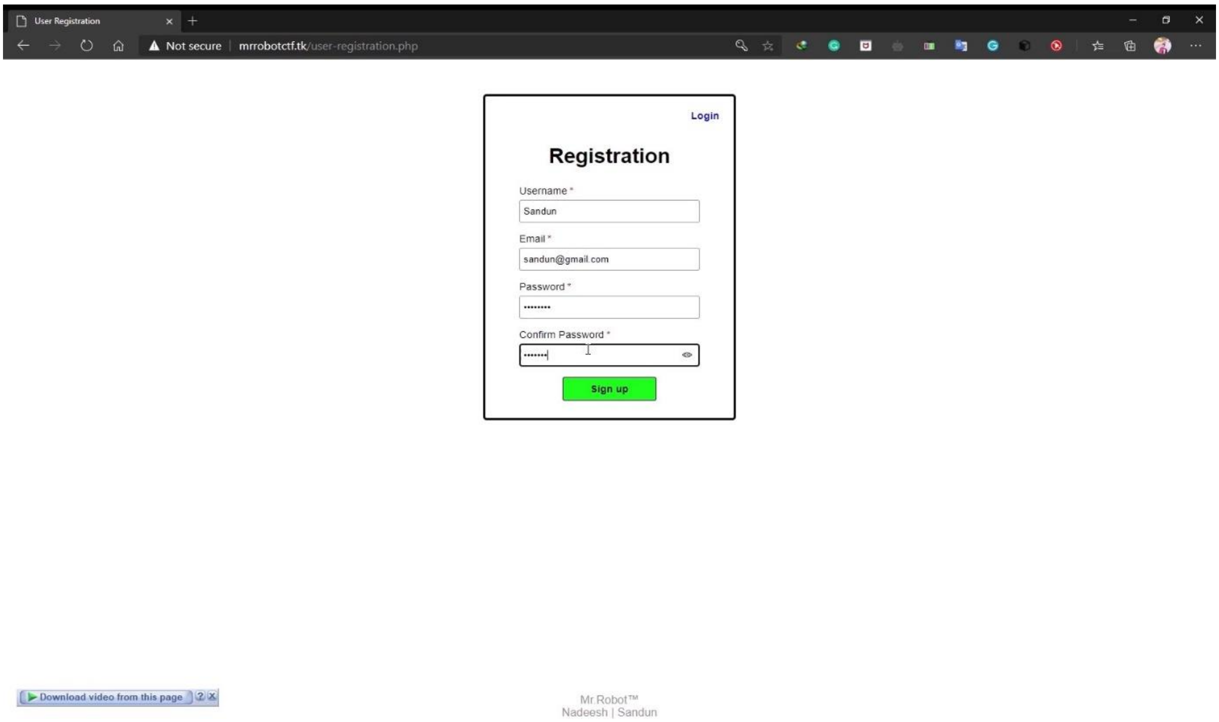
How to setup?

1. Goto mrrobotctf.tk
   Or goto 20.195.41.0



MR. ROBOT IS AN AMERICAN DRAMA THRILLER TELEVISION SERIES CREATED BY SAM ESMAIL FOR USA NETWORK. IT STARS RAMI MALEK AS ELLIOT ALDERSON, A CYBERSECURITY ENGINEER AND HACKER WITH SOCIAL ANXIETY DISORDER AND CLINICAL DEPRESSION.

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


User Registration
Not secure
mrrobotctf.tk/user-registration.php
Login
Sign up
Download video from this page

Registration

Username * Sandun

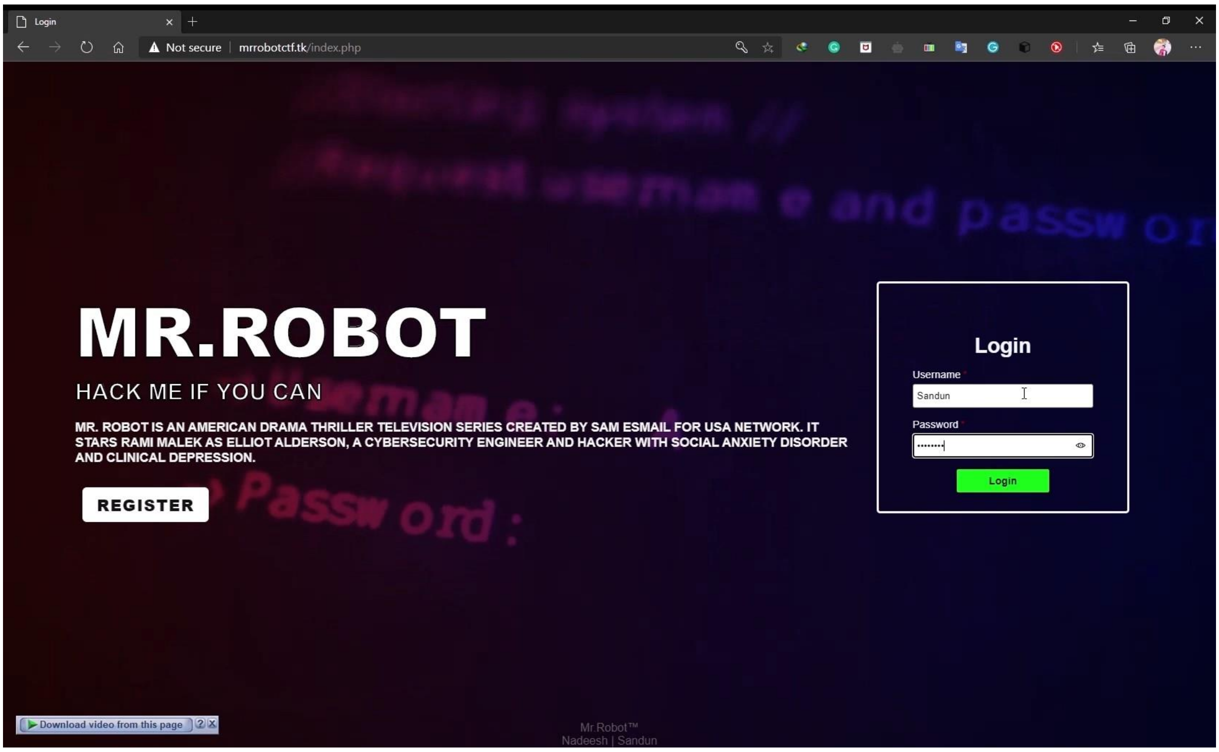
Email * sandun@gmail.com

Password * ••••••••

Confirm Password * •••••••

Mr.Robot™
Nadeesh | Sandun

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



MR.ROBOT

HACK ME IF YOU CAN

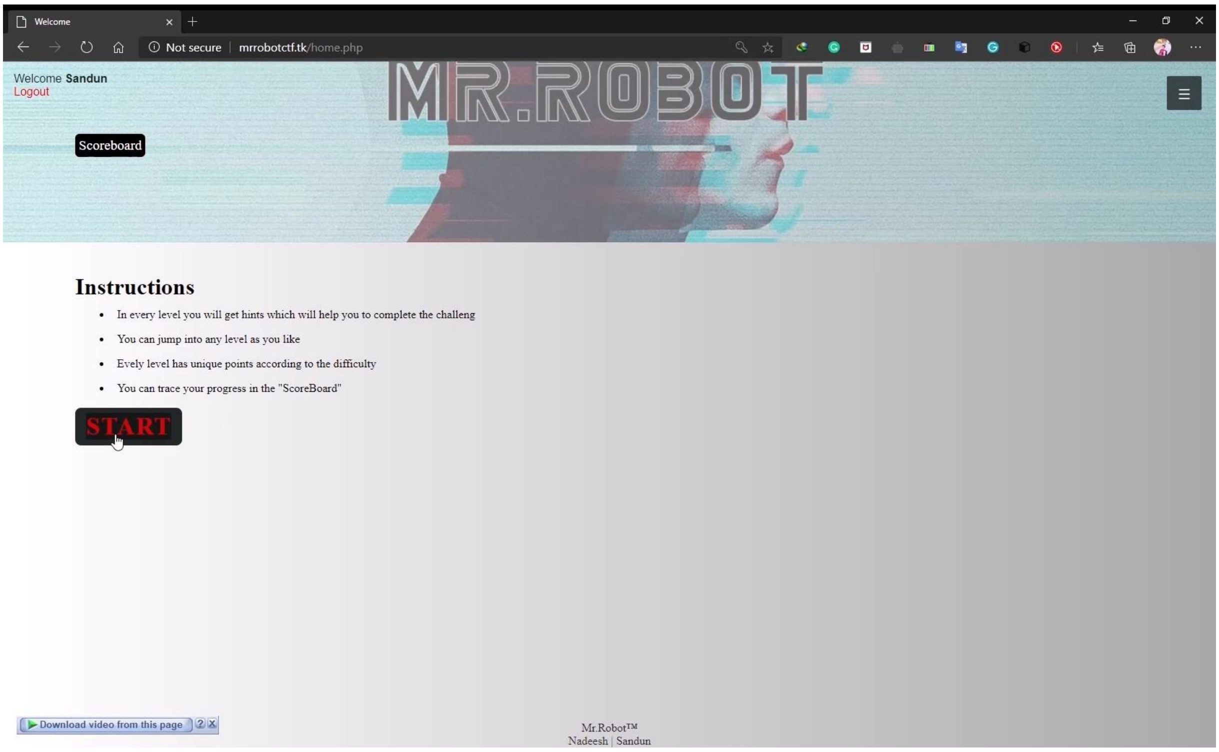
MR. ROBOT IS AN AMERICAN DRAMA THRILLER TELEVISION SERIES CREATED BY SAM ESMAIL FOR USA NETWORK. IT STARS RAMI MALEK AS ELLIOT ALDERSON, A CYBERSECURITY ENGINEER AND HACKER WITH SOCIAL ANXIETY DISORDER AND CLINICAL DEPRESSION.

Login

Username * Sandun

Password * •••••••

Mr.Robot™
Nadeesh | Sandun



Welcome **Sandun**
Logout

Scoreboard

Instructions

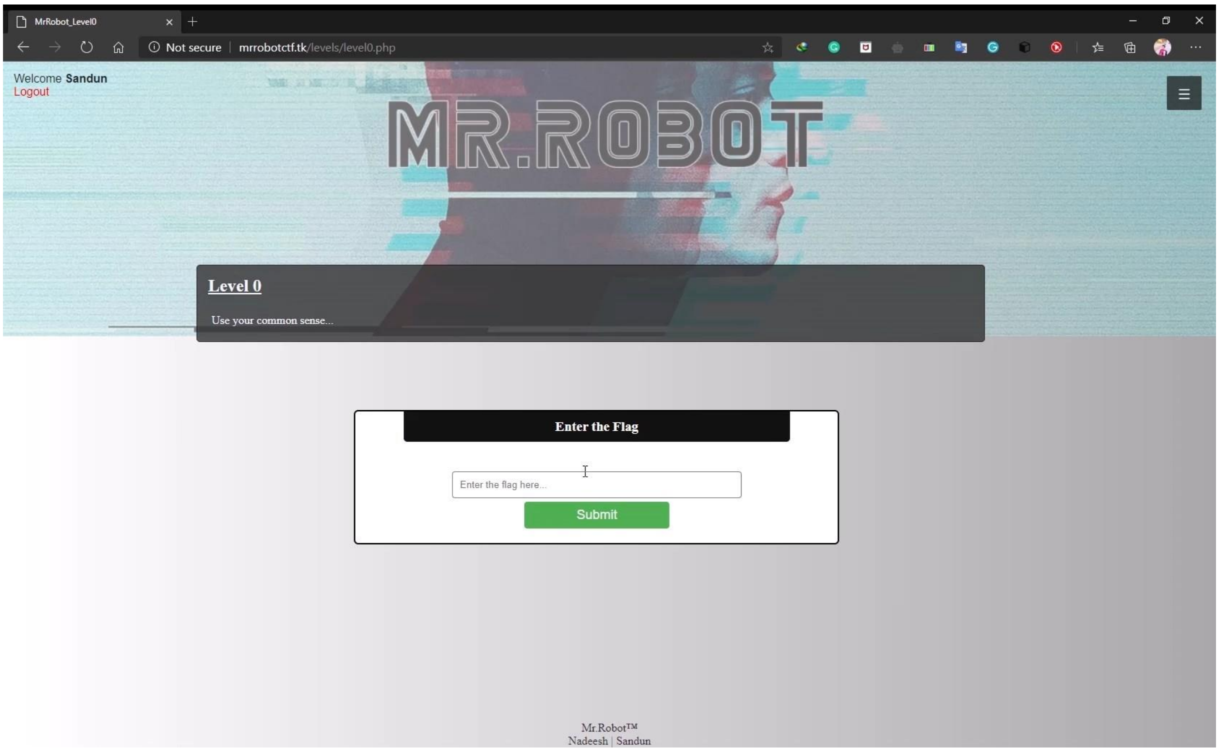
- In every level you will get hints which will help you to complete the challeng
- You can jump into any level as you like
- Evely level has unique points according to the difficulty
- You can trace your progress in the "ScoreBoard"

START

Mr.Robot™
Nadeesh | Sandun

Walkthrough of the levels.

Level 0



Welcome **Sandun**
Logout

Level 0

Use your common sense...

Enter the Flag

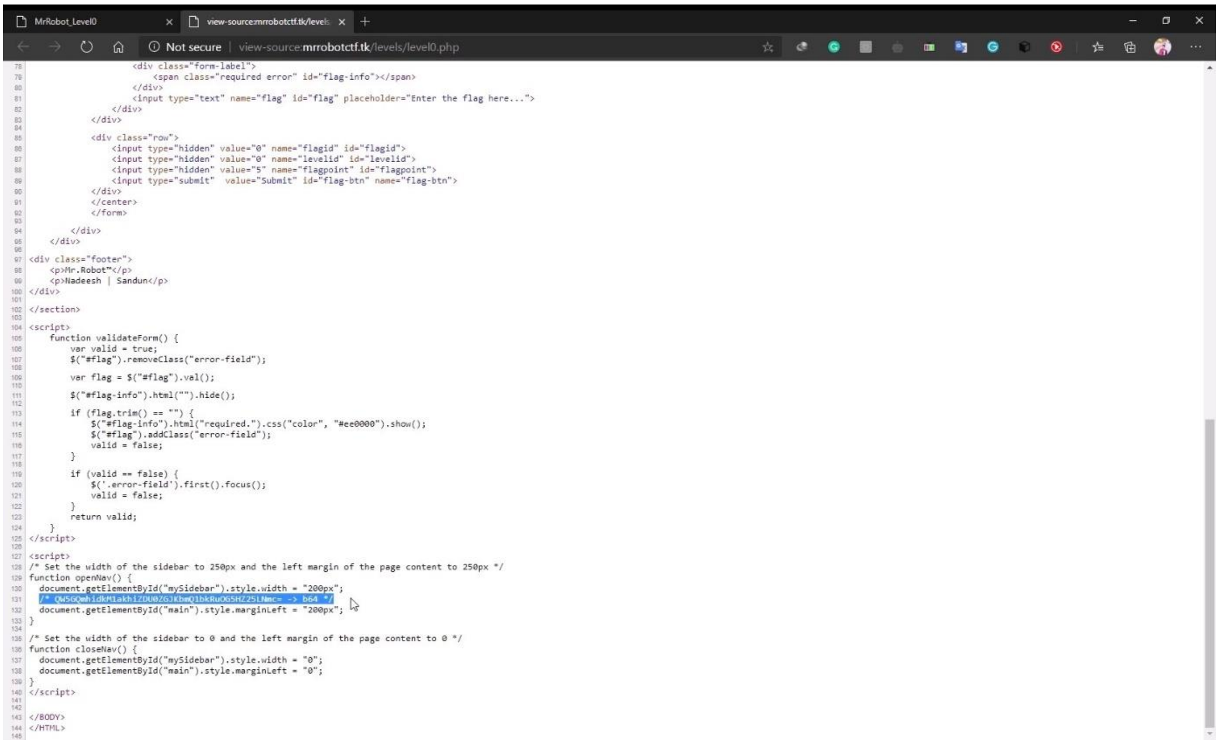
Enter the flag here...

Submit

Mr.Robot™
Nadeesh | Sandun

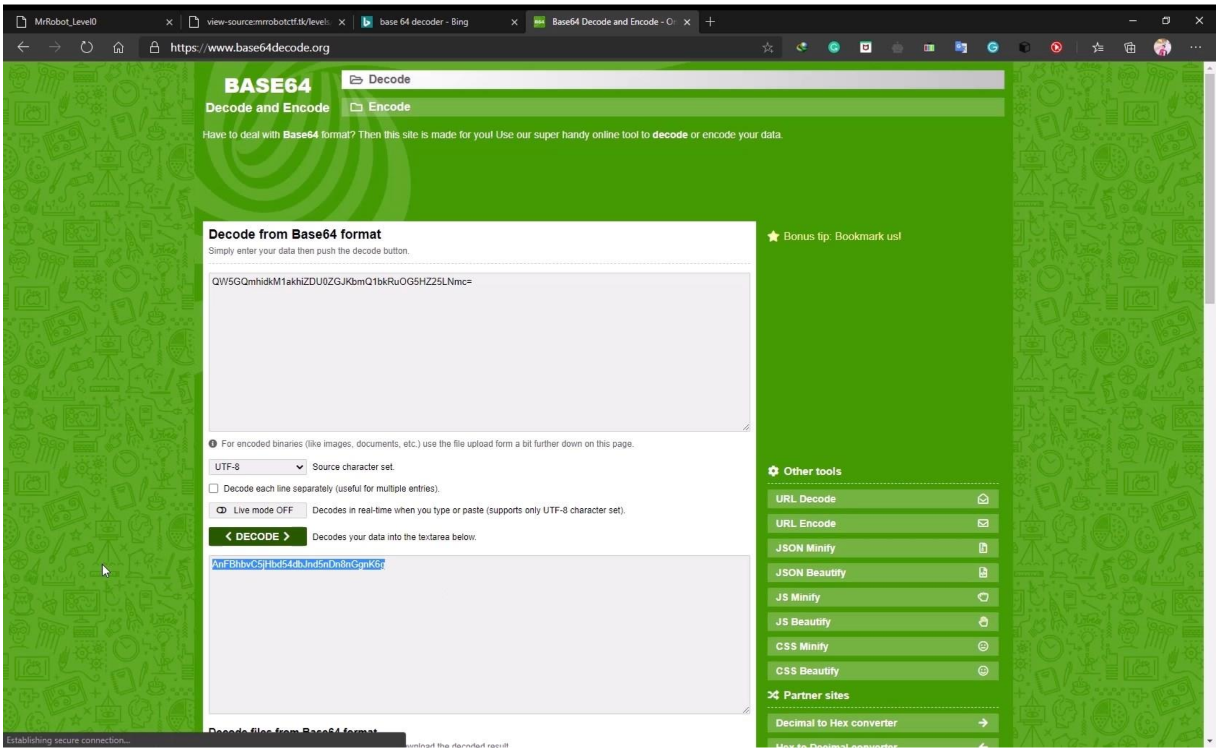
After getting the instructions, the 1st level is level 0. After clicking on level 0 a small hint will be shown.

Go to the page source and find the flag.


MrRobot_Level0
view-source:mrrobotctf.tk/levels
Not secure
view-source:mrrobotctf.tk/levels/level0.php

```
                <div class="form-label">
                    <span class="required error" id="flag-info"></span>
                </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 class="footer">
  <p>Mr.Robot™</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", "#ee0000").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";
  /* QW5GQmhidkM1akhiZDU0ZGJKbmQ1bkRuOG5HZ25LNmc= -> b64 */
  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.



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.

```
QW5GQmhidkM1akhiZDU0ZGJKbmQ1bkRuOG5HZ25LNmc=
```

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

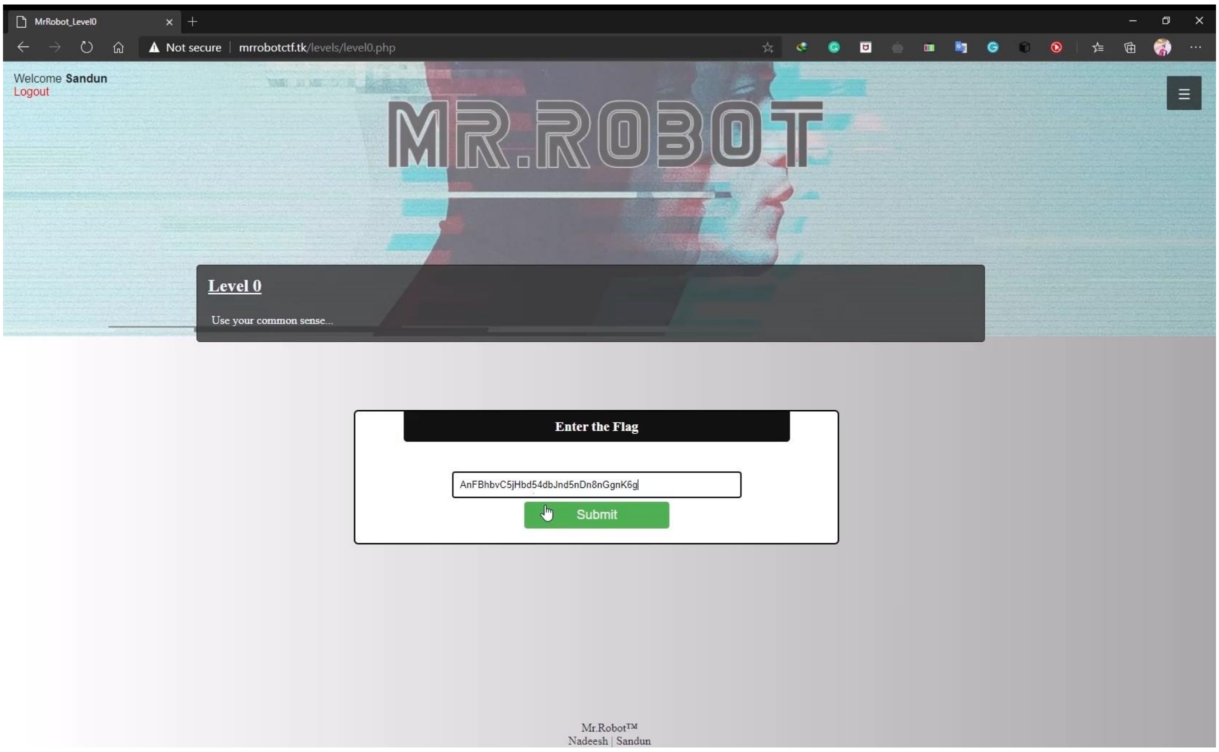
UTF-8 Source character set.

□ 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.

```
AnFBhbvC5jHbd54dbJnd5nDn8nGgnK6g
```

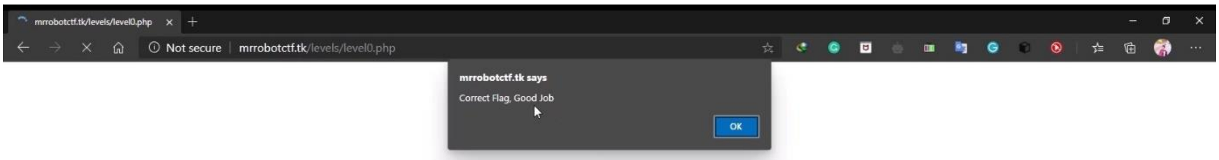


Level 0

Use your common sense...

Enter the Flag

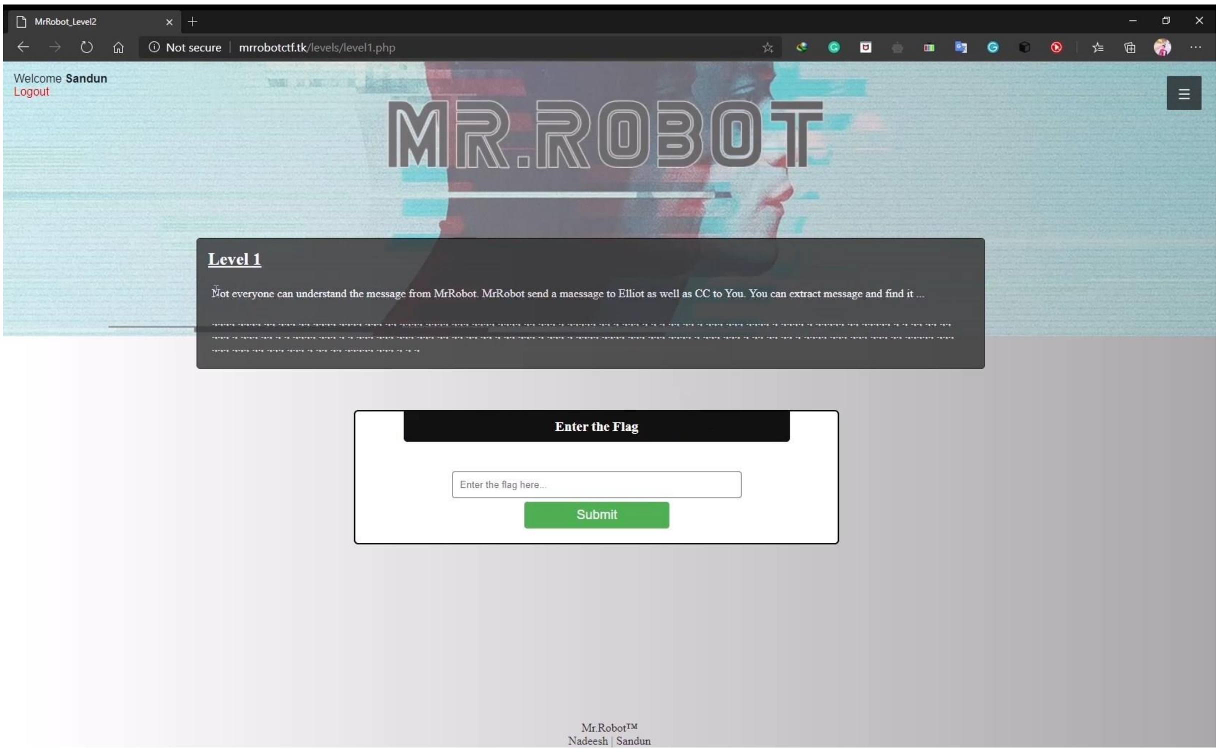
AnFBhbvC5jHbd54dbJnd5nDn8nGgnK6g


mrrobotctf.tk/levels/level0.php
Not secure | mrrobotctf.tk/levels/level0.php

mrrobotctf.tk says

Correct Flag, Good Job

Level 1



Level 1

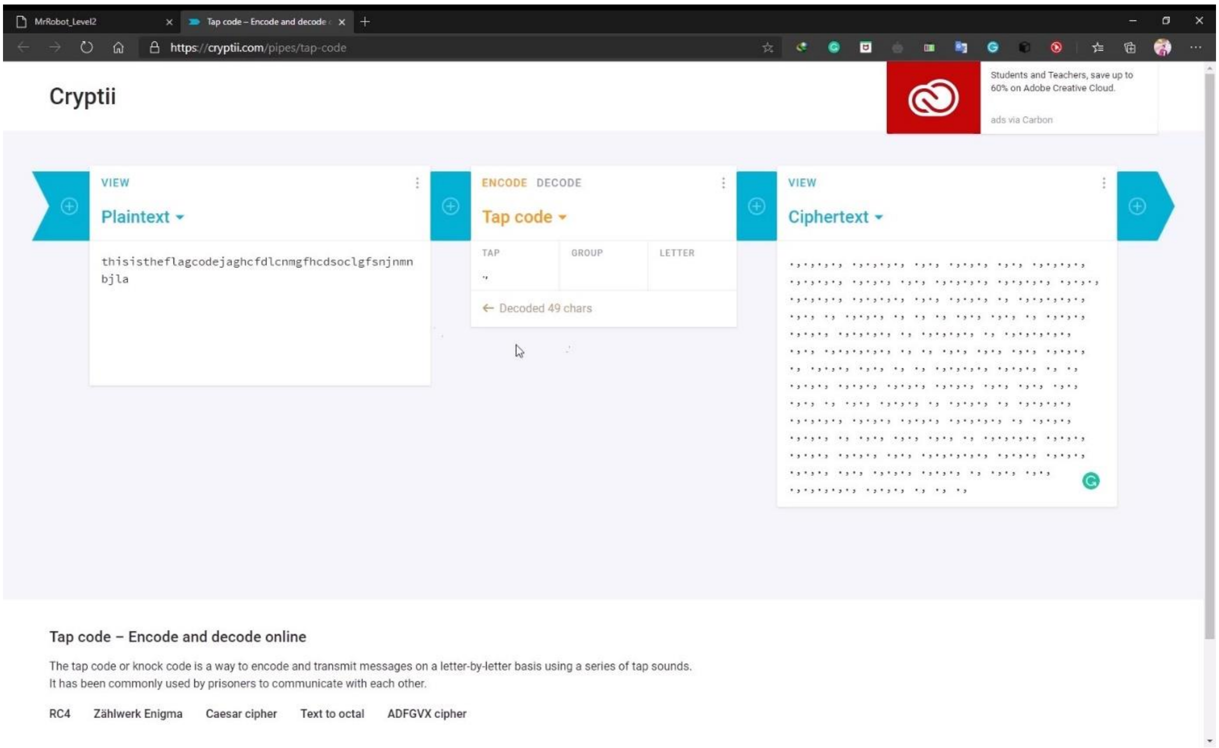
Not everyone can understand the message from MrRobot. MrRobot send a maessage to Elliot as well as CC to You. You can extract message and find it ...

[illegible]

Enter the Flag

Enter the flag here...

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



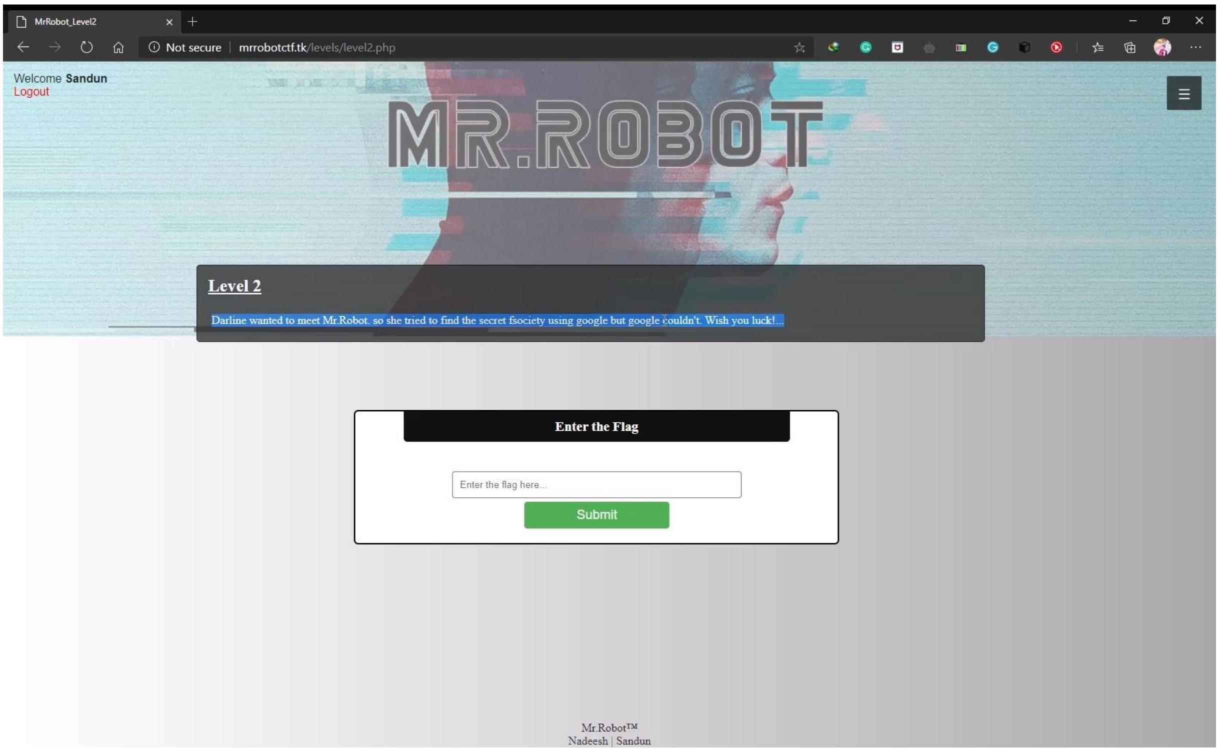
```
thisistheflagcodejaghcfdlcnmgfhcdsoclgfsnjnmnbjla
```

← Decoded 49 chars

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.

Level 2

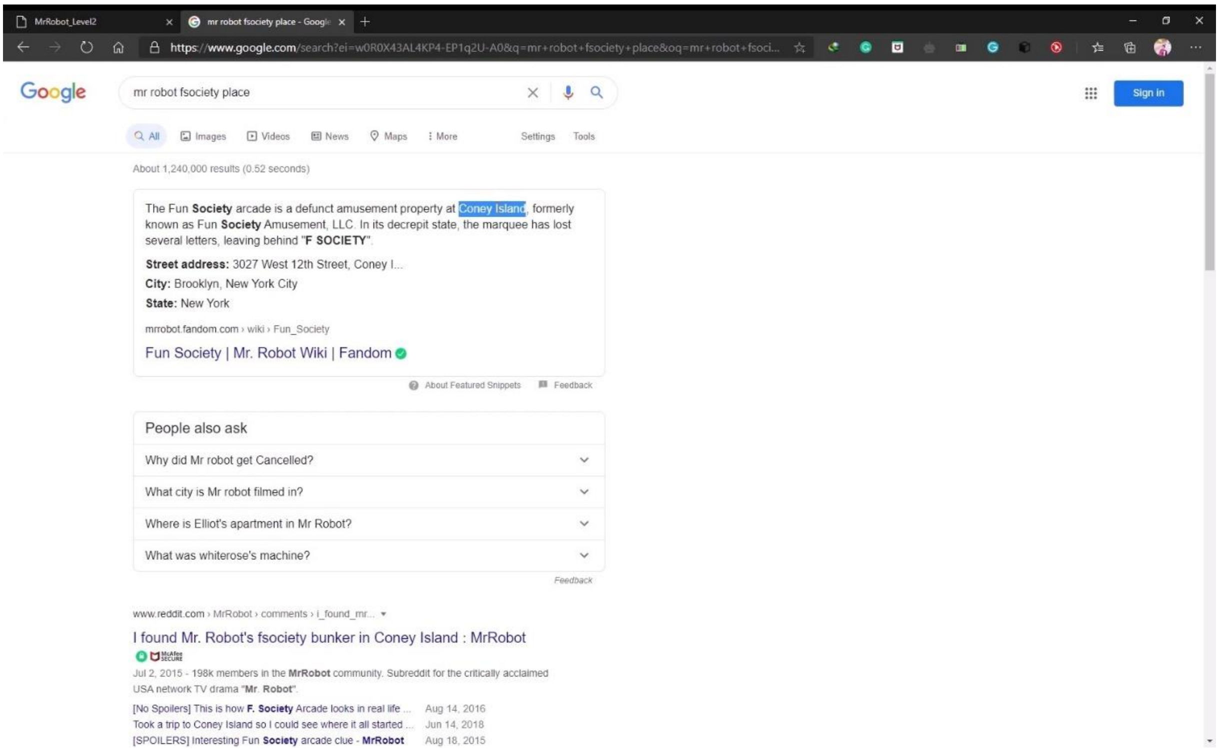


Level 2

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

Enter the Flag

Mr.Robot™
Nadeesh | Sandun


MrRobot_Level2
mr robot fsociety place - Google
https://www.google.com/search?ei=w0R0X43AL4KP4-EP1q2U-A0&q=mr+robot+fsociety+place&oq=mr+robot+fsoci...
Google
mr robot fsociety place
Sign in
All
Images
Videos
News
Maps
More
Settings
Tools

About 1,240,000 results (0.52 seconds)

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

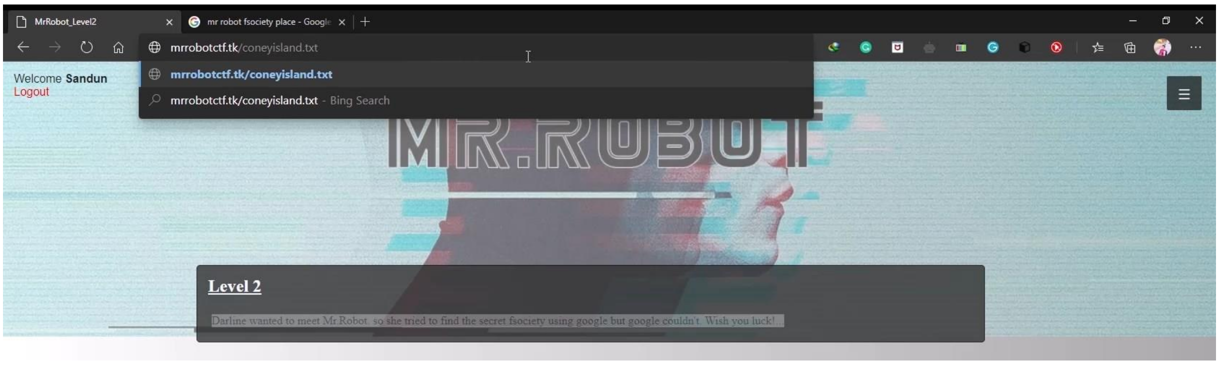
- Why did Mr robot get Cancelled?
- What city is Mr robot filmed in?
- Where is Elliot's apartment in Mr Robot?
- What was whiterose's machine?

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**".

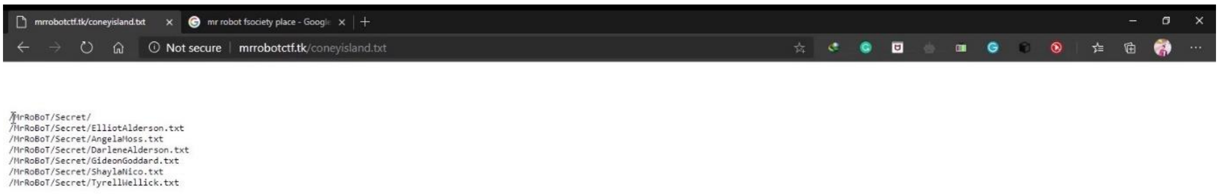
[No Spoilers] This is how **F. Society** Arcade looks in real life ...	Aug 14, 2016
Took a trip to Coney Island so I could see where it all started ...	Jun 14, 2018
[SPOILERS] Interesting Fun **Society** arcade clue - **MrRobot**	Aug 18, 2015

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


MrRobot_Level2
mr robot fsociety place - Google
mrrobotctf.tk/coneyisland.txt
mrrobotctf.tk/coneyisland.txt
mrrobotctf.tk/coneyisland.txt - Bing Search
Welcome Sandun
Logout
MR.ROBOT

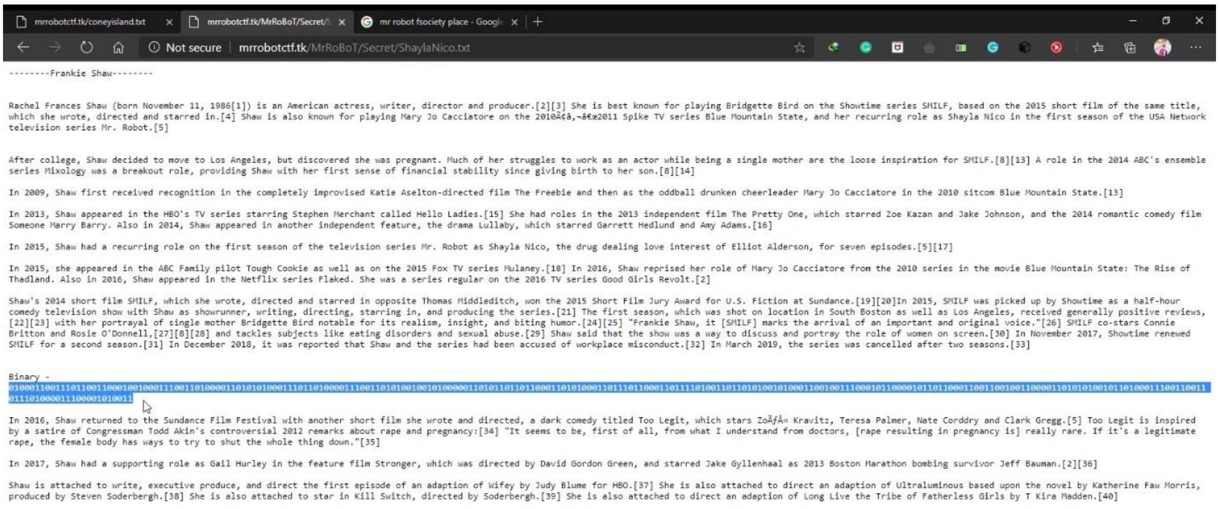
Level 2

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


mrrobotctf.tk/coneyisland.txt
mr robot fsociety place - Google
Not secure
mrrobotctf.tk/coneyisland.txt

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

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


mrrobotctf.tk/coneyisland.txt
mrrobotctf.tk/MrRoBoT/Secret/S
mr robot fsociety place - Google
Not secure
mrrobotctf.tk/MrRoBoT/Secret/ShaylaNico.txt

--------Frankie Shaw--------

Rachel Frances Shaw (born November 11, 1986[1]) is an American actress, writer, director and producer.[2][3] She is best known for playing Bridgette Bird on the Showtime series SMILF, based on the 2015 short film of the same title, which she wrote, directed and starred in.[4] Shaw is also known for playing Mary Jo Cacciatore on the 2010Ã¢â‚¬â€œ2011 Spike TV series Blue Mountain State, and her recurring role as Shayla Nico in the first season of the USA Network television series Mr. Robot.[5]

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 SMILF.[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 Someone Marry 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]

In 2015, she appeared in the ABC Family pilot Tough Cookie as well as on the 2015 Fox TV series Mulaney.[18] In 2016, Shaw reprised her role of Mary Jo Cacciatore from the 2010 series in the movie Blue Mountain State: The Rise of Thadland. Also in 2016, Shaw appeared in the Netflix series Flaked. She was a series regular on the 2016 TV series Good Girls Revolt.[2]

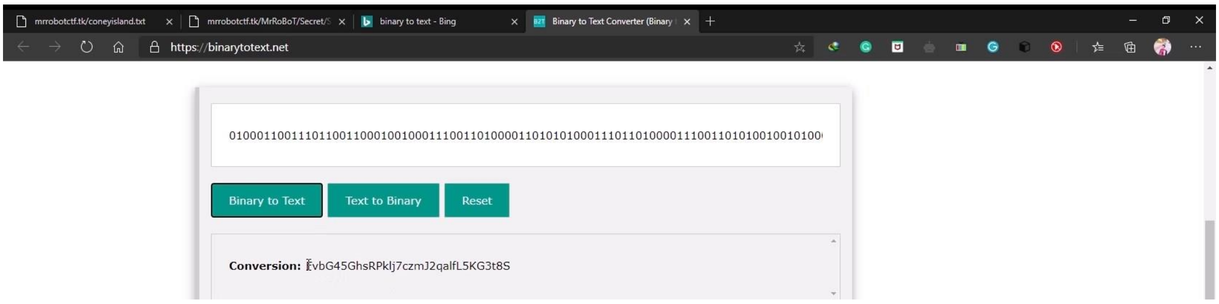
Shaw's 2014 short film SMILF, which she wrote, directed and starred in opposite Thomas Middleditch, won the 2015 Short Film Jury Award for U.S. Fiction at Sundance.[19][20]In 2015, SMILF was picked up by Showtime as a half-hour comedy television show with Shaw as showrunner, writing, directing, starring in, and producing the series.[21] The first season, which was shot on location in South Boston as well as Los Angeles, received generally positive reviews,[22][23] with her portrayal of single mother Bridgette Bird notable for its realism, insight, and biting humor.[24][25] "Frankie Shaw, it [SMILF] marks the arrival of an important and original voice."[26] SMILF co-stars Connie Britton and Rosie O'Donnell,[27][8][28] 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 on screen.[30] In November 2017, Showtime renewed SMILF 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]

```
Binary -
0100011001110110011000100100011100110100001101010100011101101000011100110101001001010000011010110110110001101010001101110110001101111010011011010100101000110010011100010110000101101100011001100100110000110101010010110100011100110011
011101000011100001010011
```

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 ZoÃƒÂ« 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] really rare. 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 an adaption of Wifey by Judy 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 star 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]

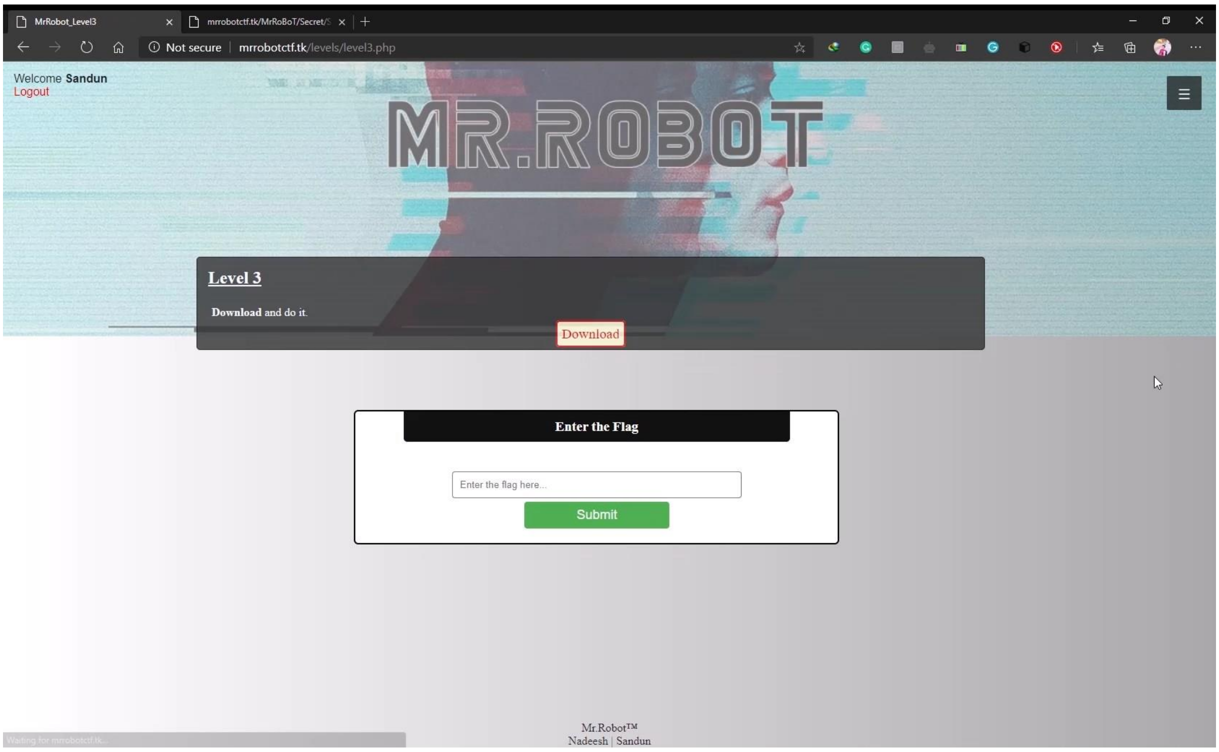

mrrobotctf.tk/coneyisland.txt
mrrobotctf.tk/MrRoBoT/Secret/S
binary to text - Bing
Binary to Text Converter (Binary
https://binarytotext.net
Binary to Text
Text to Binary
Reset

```
0100011001110110011000100100011100110100001101010100011101101000011100110101001001010000
```

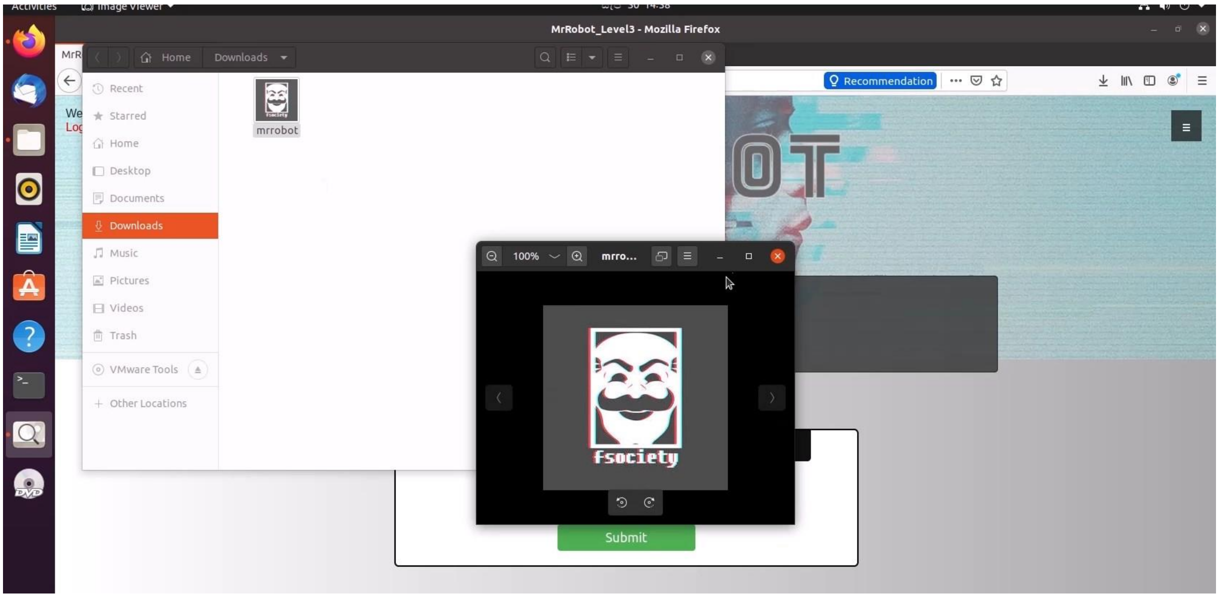
Conversion: FvbG45GhsRPklj7czmJ2qalfL5KG3t8S

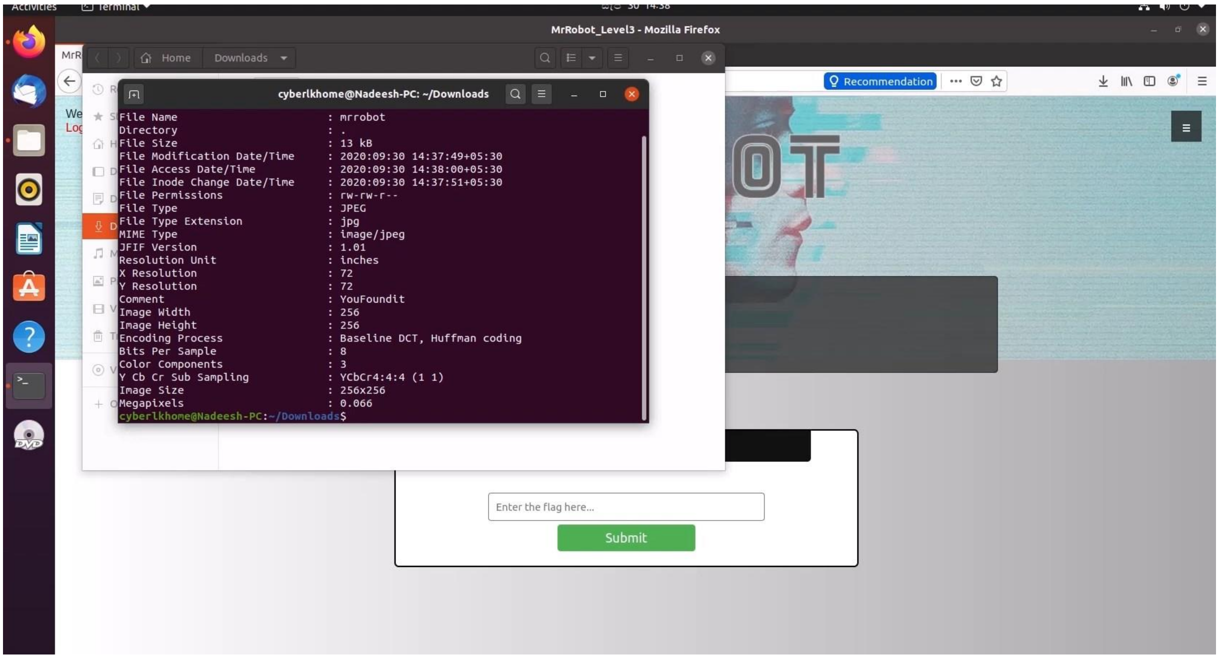
According to the above image the flag is encoded. Use any binary decoder to decode the flag and later on submit in the submission form.

Level 3



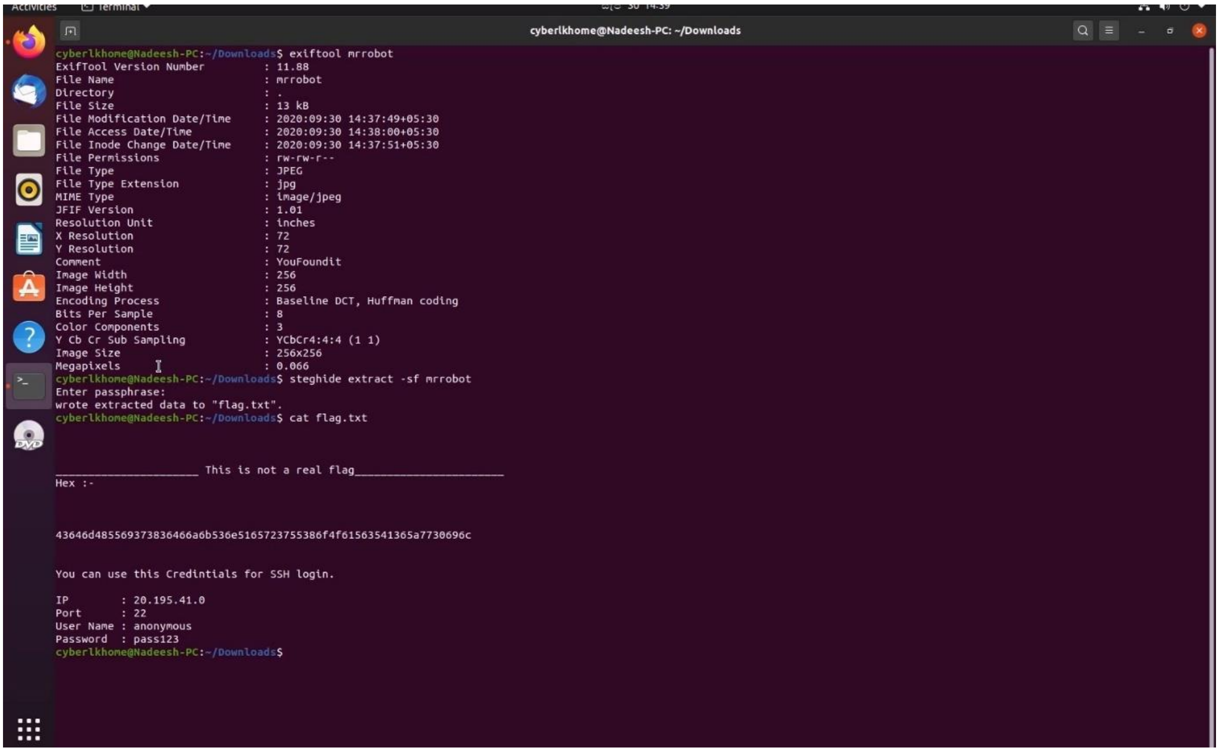
After downloading the Image file to a Linux environment. Scan the image for file type. The hints suggest of the METADATA, because of that we need a tool to see METADATA of the image. After enough research and the hint suggests Exiftool. Download and install the tool with the command: “sudo apt-get install 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.





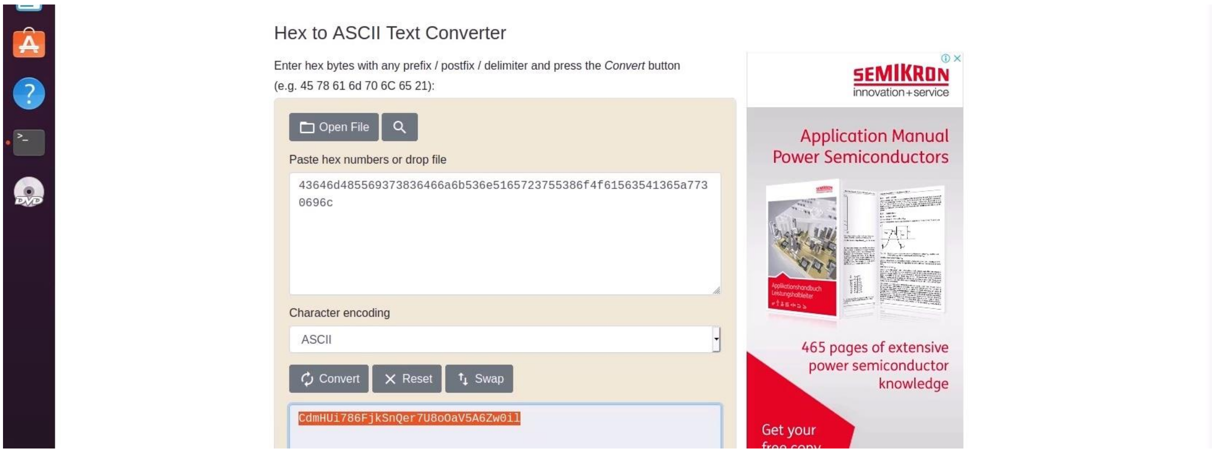
```
cyberlkhome@Nadeesh-PC: ~/Downloads
File Name                       : mrrobot
Directory                       : .
File Size                       : 13 kB
File Modification Date/Time     : 2020:09:30 14:37:49+05:30
File Access Date/Time           : 2020:09:30 14:38:00+05:30
File Inode Change Date/Time     : 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                    : 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
cyberlkhome@Nadeesh-PC:~/Downloads$
```

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:



```
cyberlkhome@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                    : 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
cyberlkhome@Nadeesh-PC:~/Downloads$ steghide extract -sf mrrobot
Enter passphrase:
wrote extracted data to "flag.txt".
cyberlkhome@Nadeesh-PC:~/Downloads$ cat flag.txt



______________________ This is not a real flag_______________________
Hex :-



43646d485569373836466a6b536e5165723755386f4f61563541365a7730696c


You can use this Credintials for SSH login.

IP        : 20.195.41.0
Port      : 22
User Name : anonymous
Password  : pass123
cyberlkhome@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):

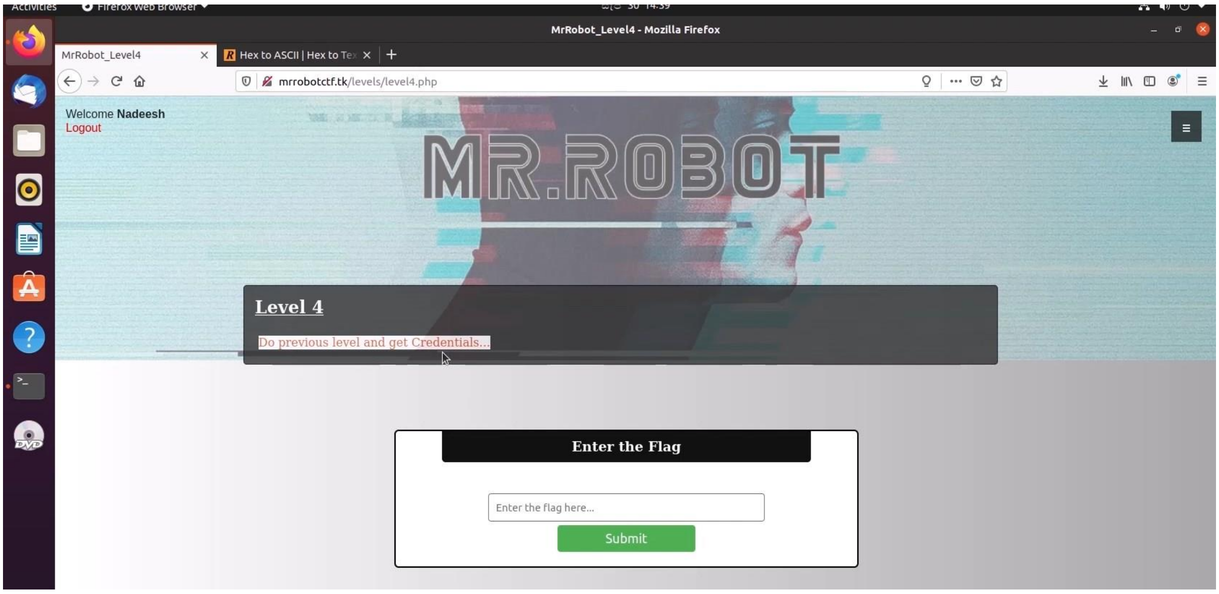
Paste hex numbers or drop file

```
43646d485569373836466a6b536e5165723755386f4f61563541365a773
0696c
```

Character encoding: ASCII

```
CdmHUi786FjkSnQer7U8oOaV5A6Zw0il
```

Level 4

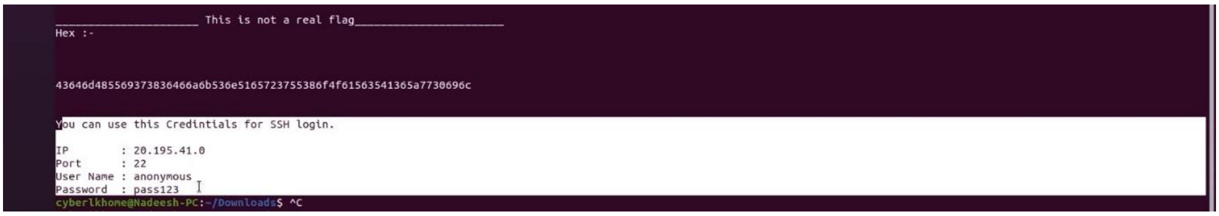

MrRobot_Level4 - Mozilla Firefox
MrRobot_Level4
Hex to ASCII | Hex to Tex
mrrobotctf.tk/levels/level4.php
Welcome Nadeesh
Logout
MR.ROBOT
Enter the flag here...
Submit

Level 4

Do previous level and get Credentials...

Enter the Flag

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

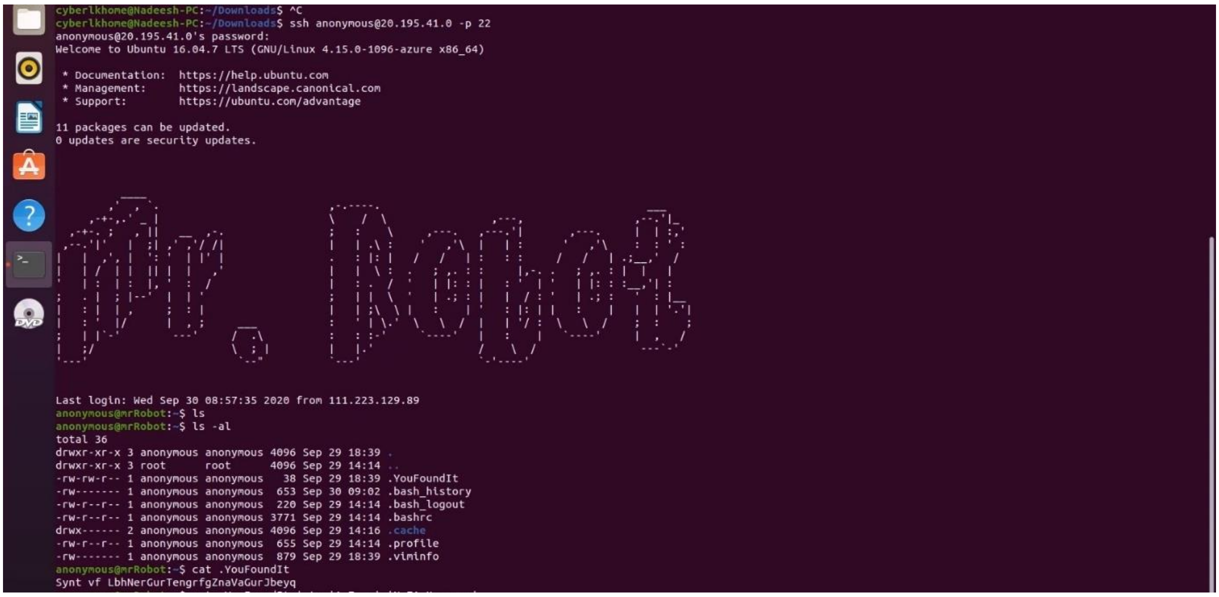


```
______________________ This is not a real flag_______________________
Hex :-


43646d4855693738364 66a6b536e5165723755386f4f61563541365a7730696c

You can use this Credintials for SSH login.

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

And login through SSH using those credential,

the flag file is hidden

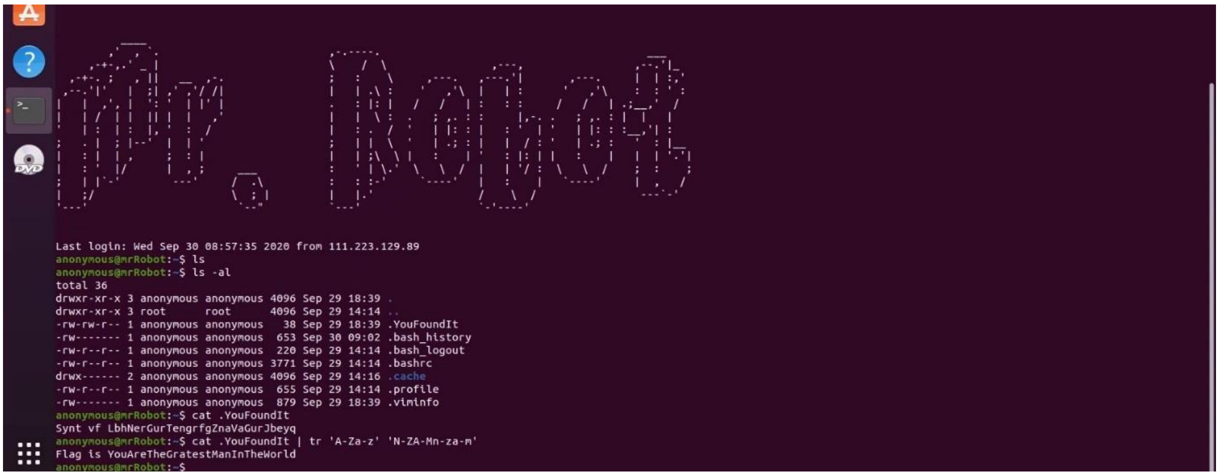
use cat .YouFountIt to read the file



```
cyberlkhome@Nadeesh-PC:~/Downloads$ ^C
cyberlkhome@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 .YouFoundIt
-rw------- 1 anonymous anonymous  653 Sep 30 09:02 .bash_history
-rw-r--r-- 1 anonymous anonymous  220 Sep 29 14:14 .bash_logout
-rw-r--r-- 1 anonymous anonymous 3771 Sep 29 14:14 .bashrc
drwx------ 2 anonymous anonymous 4096 Sep 29 14:16 .cache
-rw-r--r-- 1 anonymous anonymous  655 Sep 29 14:14 .profile
-rw------- 1 anonymous anonymous  879 Sep 29 18:39 .viminfo
anonymous@mrRobot:~$ cat .YouFoundIt
Synt vf LbhNerGurTengrfgZnaVaGurJbeyq
```

And it need to decode

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



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