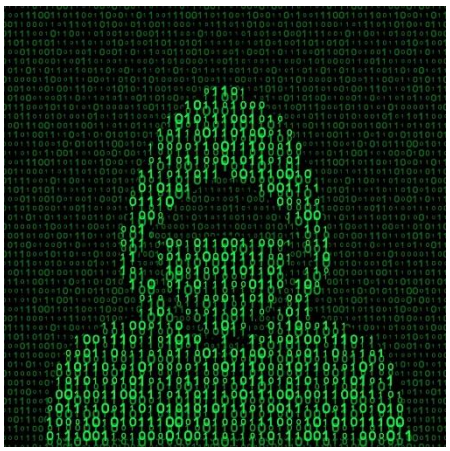
SLIIT

COMPUTING | BUSINESS | ENGINEERING

IE3092
Information Security Project
3rd Year 2nd Semester



M@+R|X 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

29 / 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.

P.M.I.N.Kumara

Table of Contents

Introduction to CTF

Catch the Flag is an occasion that is generally facilitated at data security meetings, including the different occasions. This occasion comprises of a progression of difficulties that shifts in their level of trouble, and that expect members to practice distinctive ranges of abilities to illuminate. When an individual test is unraveled, a "banner" is given to the player and they present this banner to the CTF worker to acquire focuses. Players can be solitary wolves who endeavor the different difficulties without anyone else, or they can work with others to endeavor to score the most noteworthy number of focuses as a group.

Audience

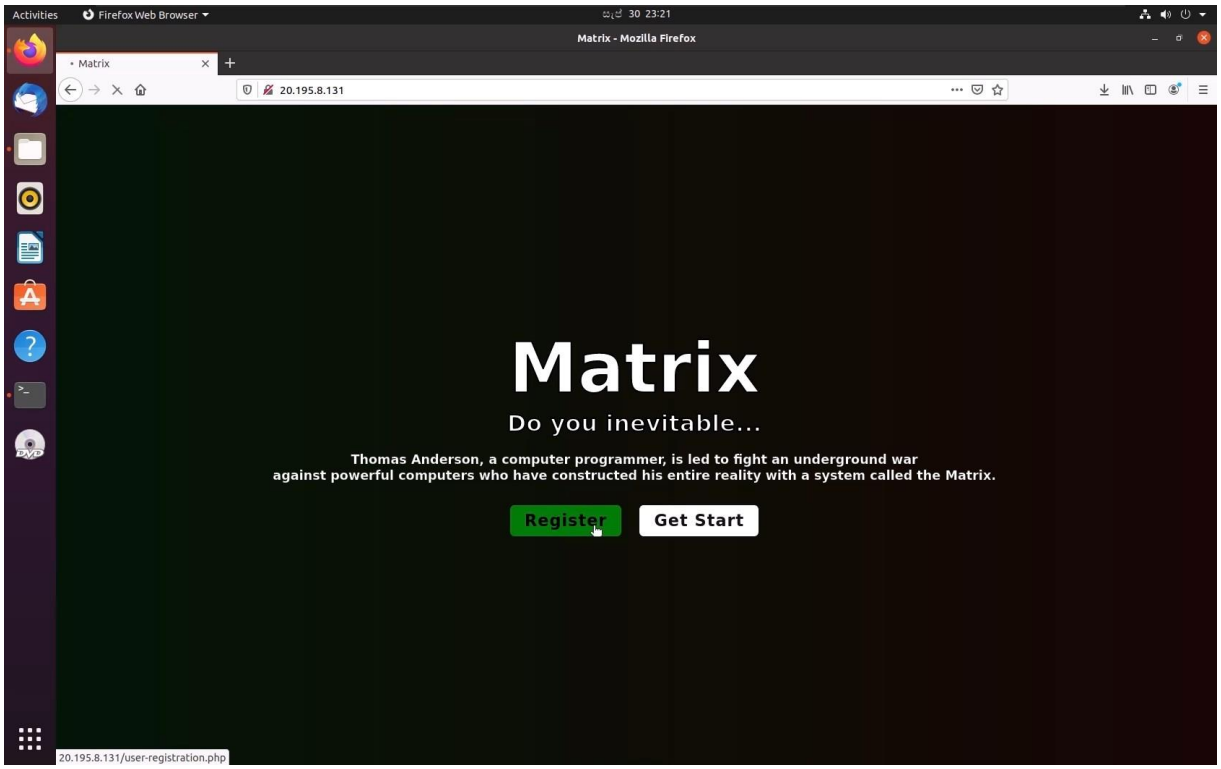
- Cyber security researchers (industrial)
- Cyber security undergraduates
- People who interested in cyber security

The way to setup?

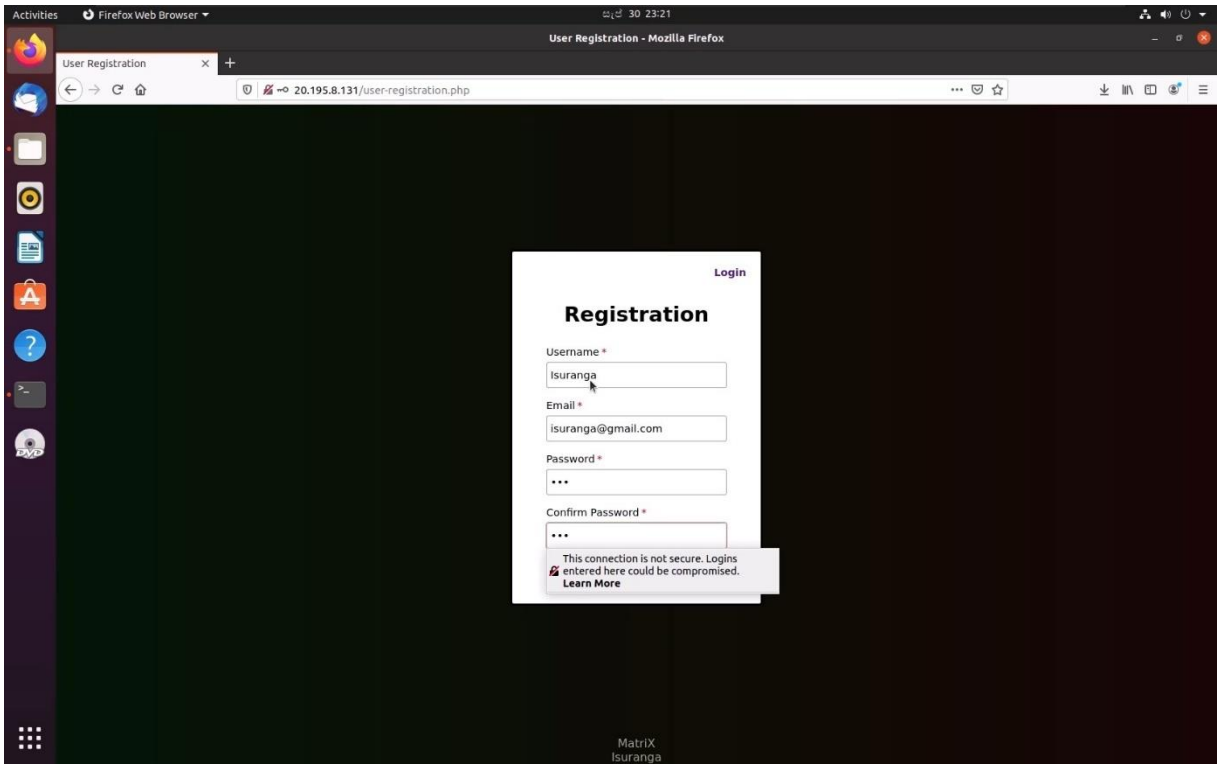
1. Import the virtual CTF box to any virtualization platform such as VMware, Virtual Box.

2. Run the imported VM and all the services will be run automatically.

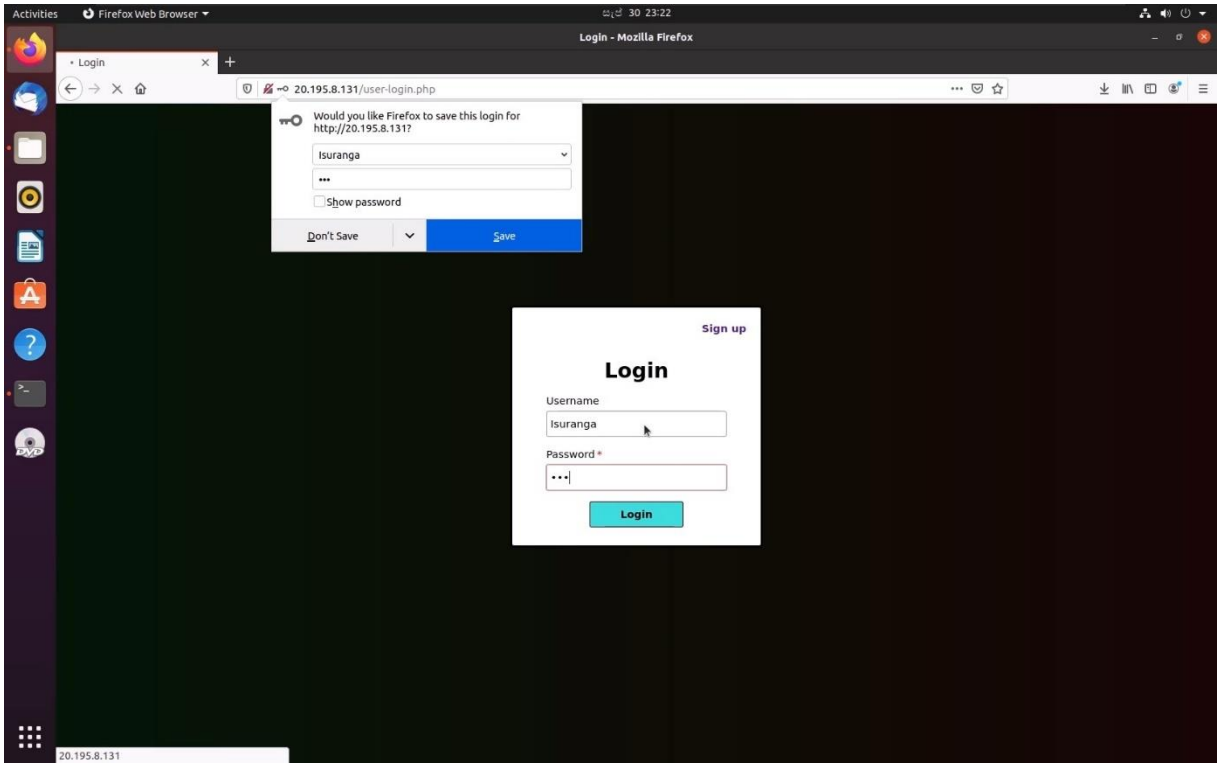
3. Get the ip address of the running VM and paste the address in a browser in order to access to the web app.



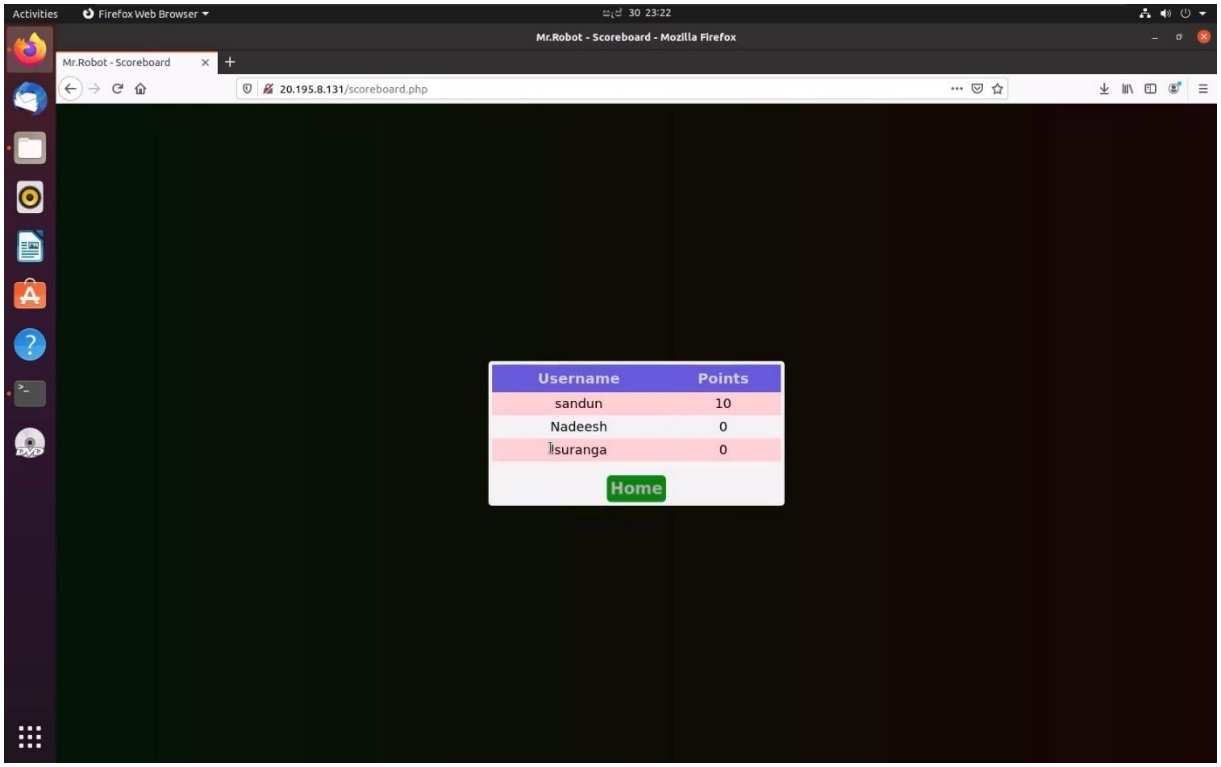
4. In the web app, the registration should be done first.



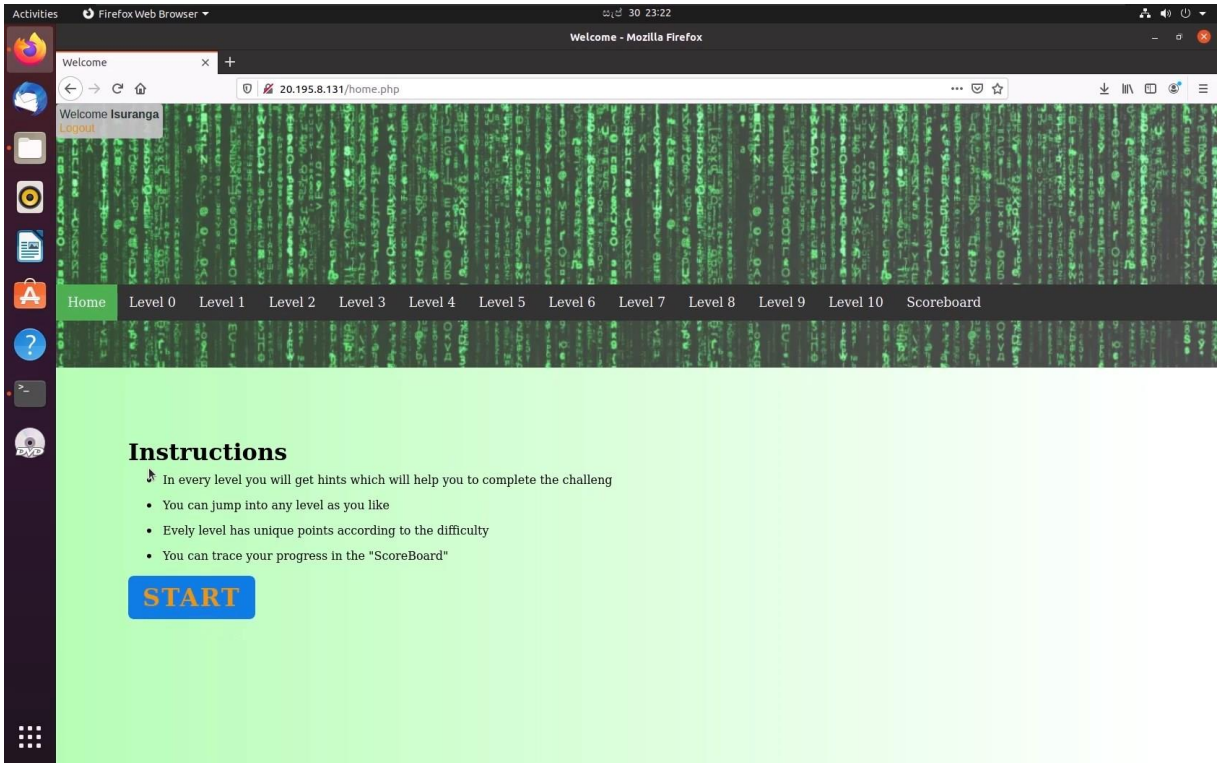
5. Next login in to created account.



6. At the begging, the score bord is at 0.

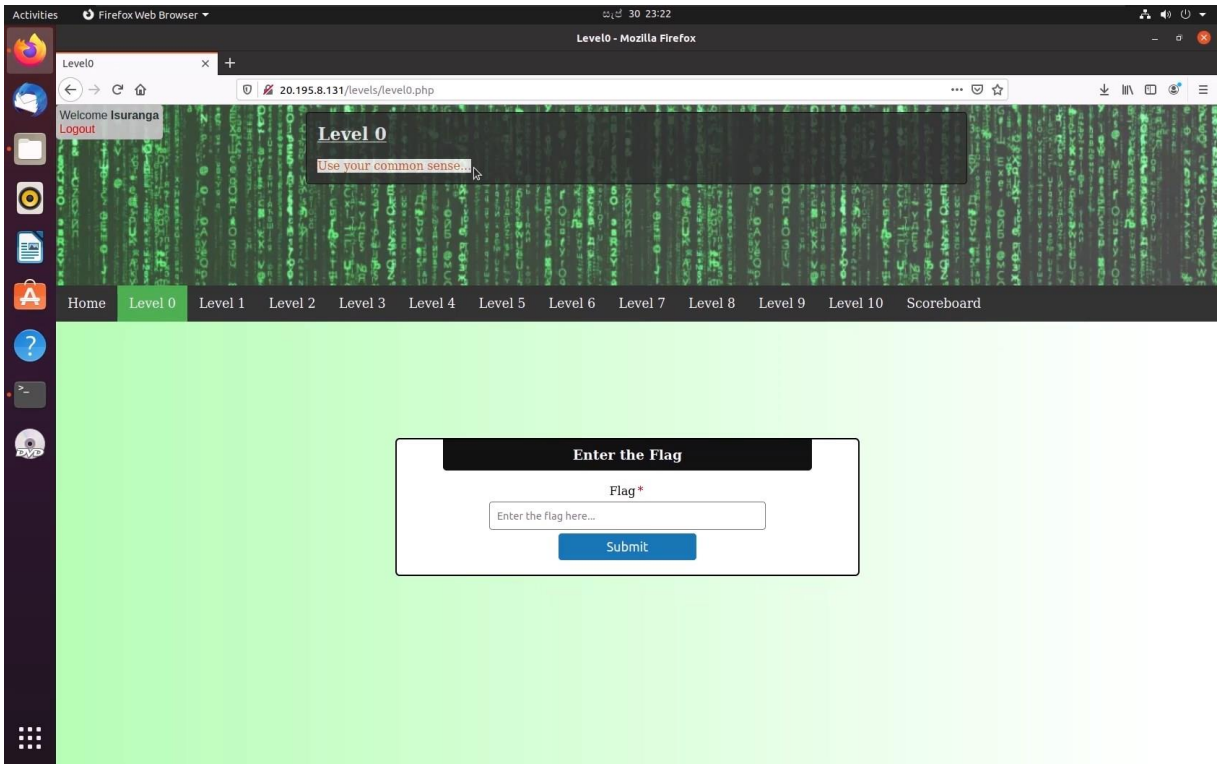


7. Then login to the web app, the instructions will be shown.

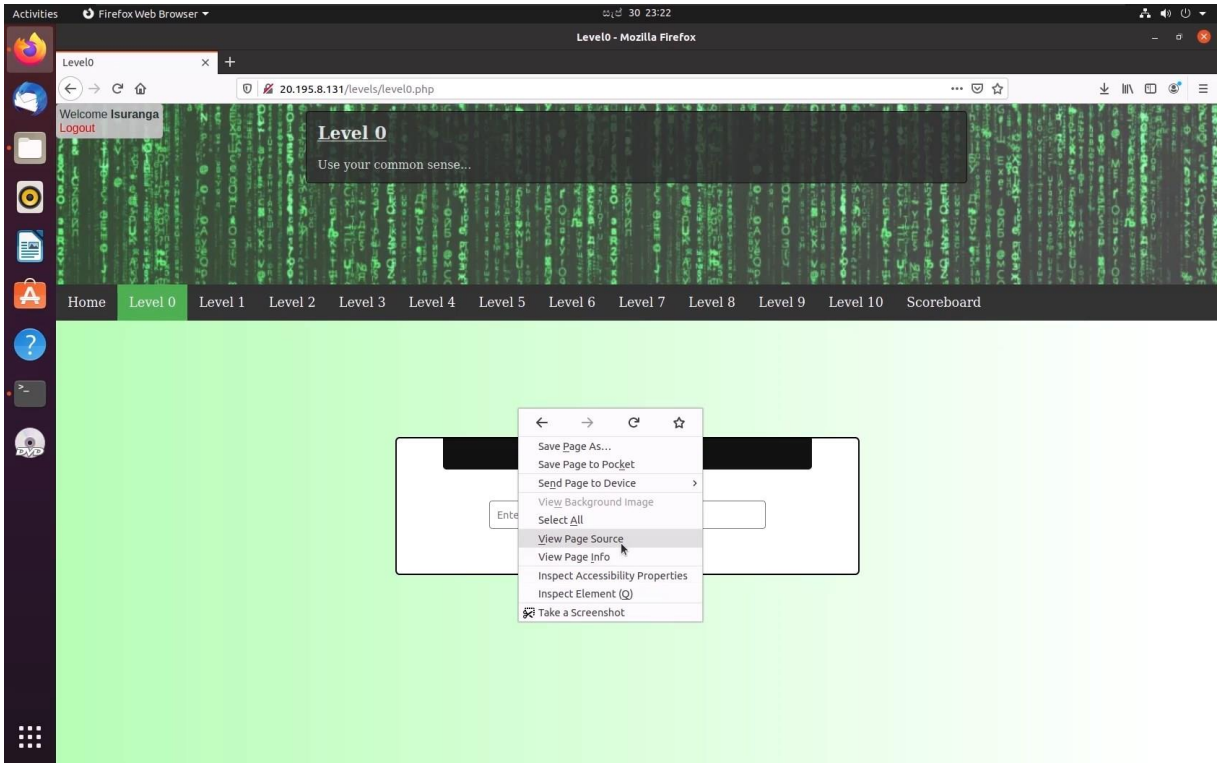


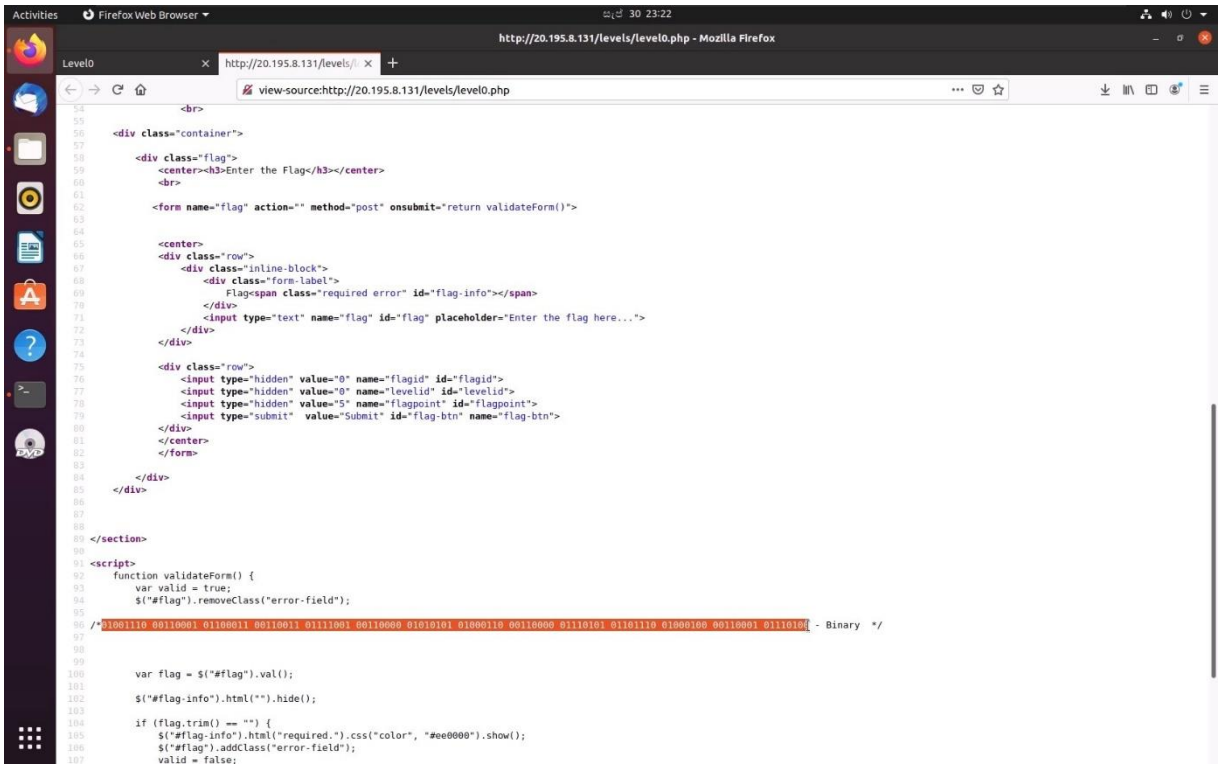
Walkthrough of the levels.

Level 0

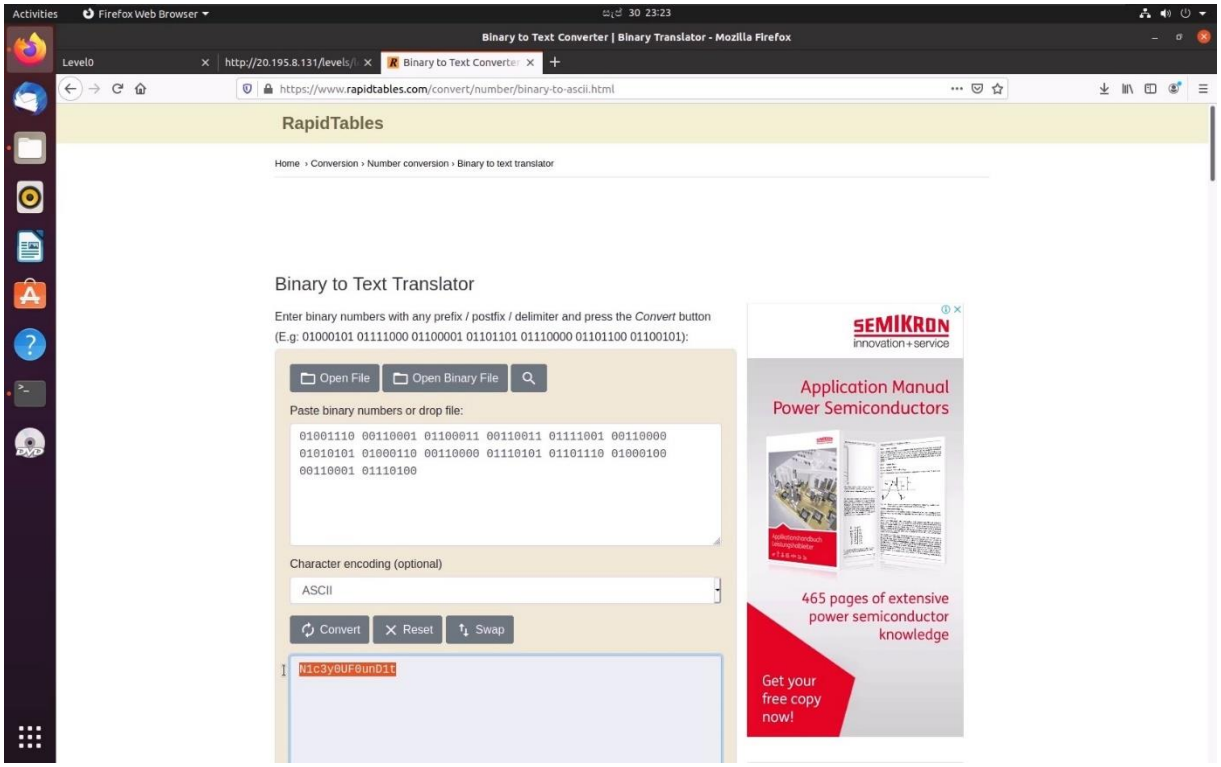


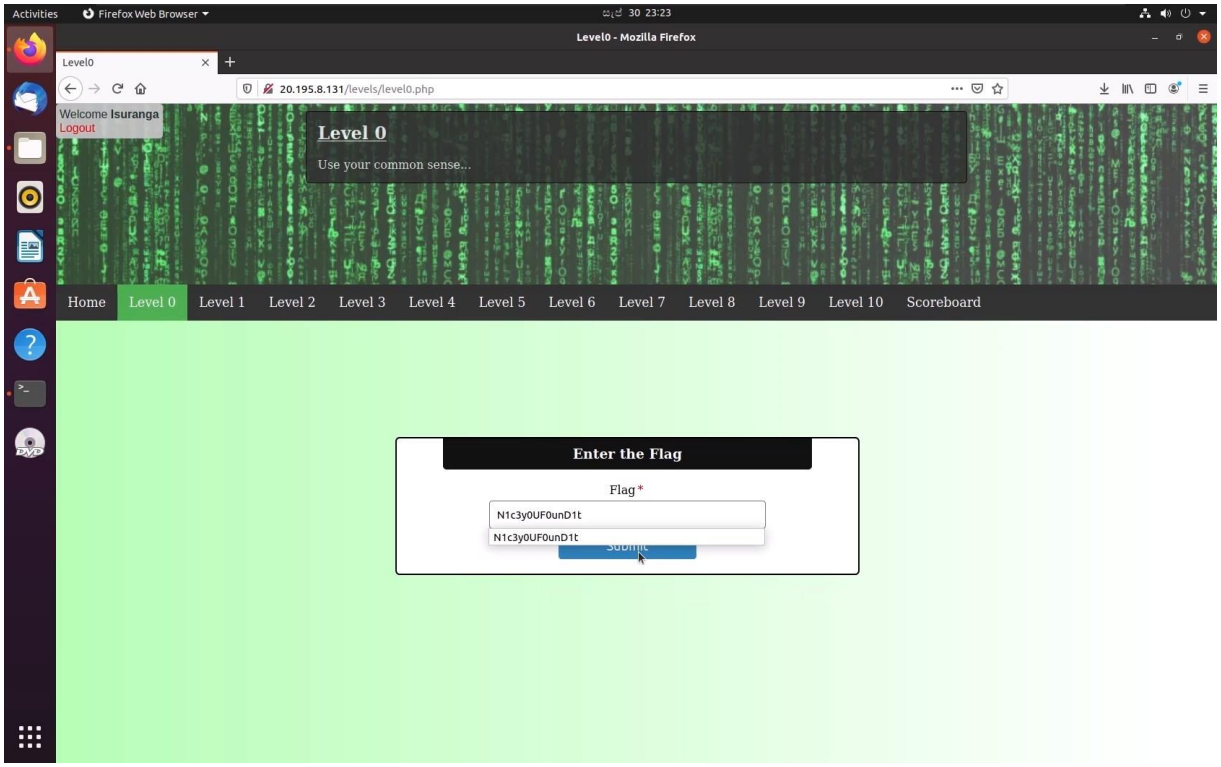
- After getting the instructions, the 1st level is level 0. After clicking on level 0 a small hint will be shown.
- Go to the page source and find the flag.



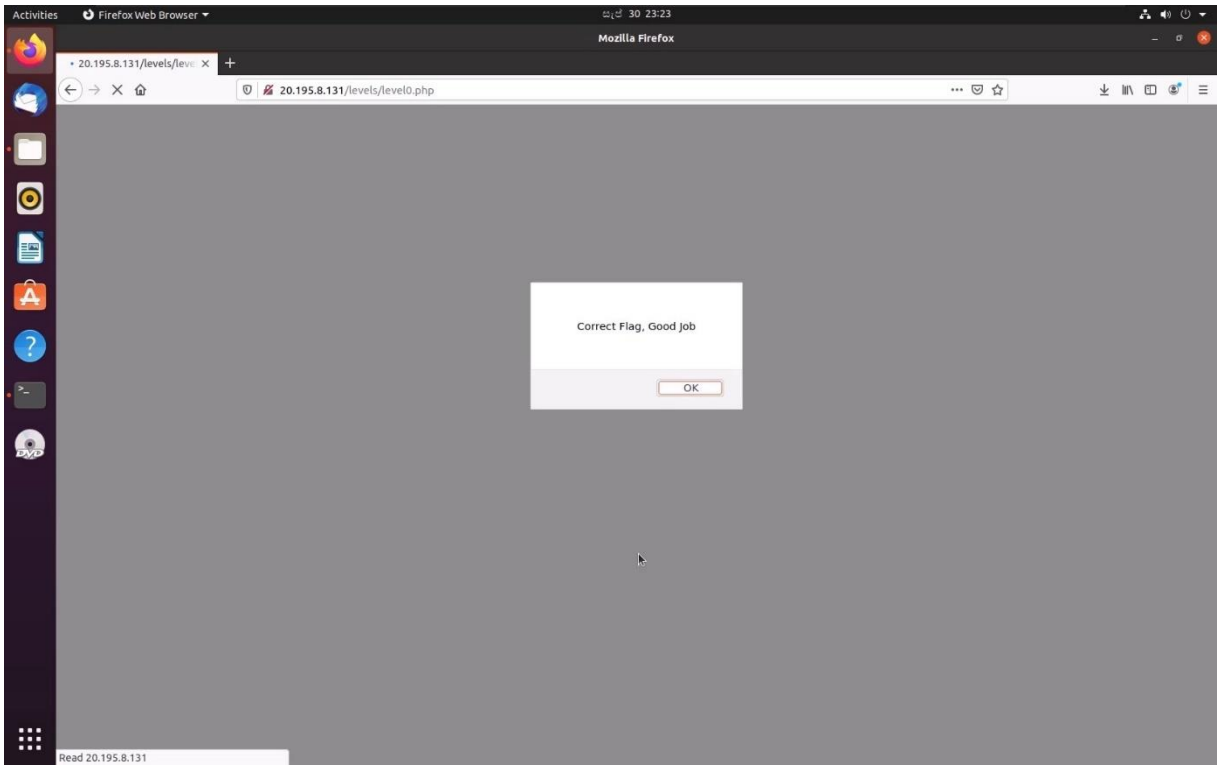


- According to the above image the flag is encoded. Use any binary to text translator to decode the flag and later on submit in the submission form.

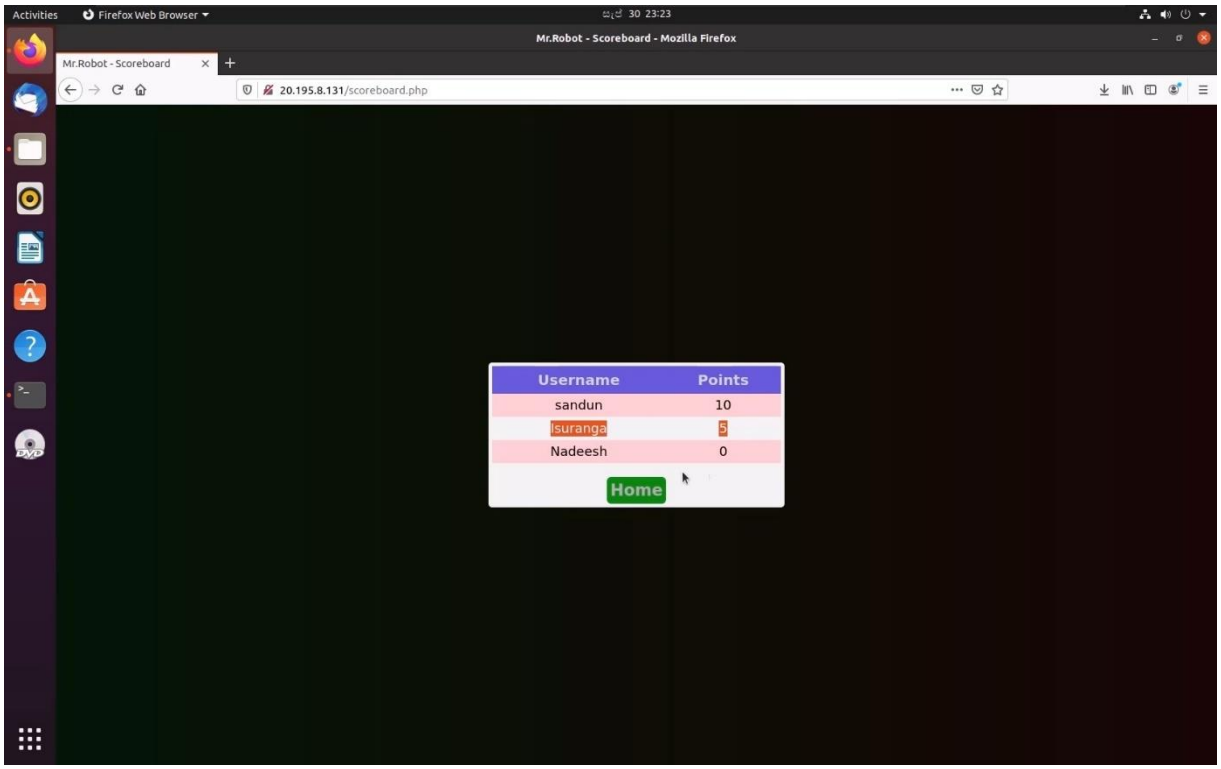

Activities
Firefox Web Browser
30 23:23
Binary to Text Converter | Binary Translator - Mozilla Firefox
Level0
http://20.195.8.131/levels/
Binary to Text Converter
https://www.rapidtables.com/convert/number/binary-to-ascii.html
RapidTables
Home › Conversion › Number conversion › Binary to text translator
Binary to Text Translator
Enter binary numbers with any prefix / postfix / delimiter and press the Convert button
(E.g: 01000101 01111000 01100001 01101101 01110000 01101100 01100101):
Open File
Open Binary File
Paste binary numbers or drop file:
01001110 00110001 01100011 00110011 01111001 00110000
01010101 01000110 00110000 01110101 01101110 01000100
00110001 01110100
Character encoding (optional)
ASCII
Convert
Reset
Swap
N1c3y0UF0unD1t
SEMIKRON
innovation+service
Application Manual
Power Semiconductors
465 pages of extensive
power semiconductor
knowledge
Get your
free copy
now!


Activities
Firefox Web Browser
30 23:23
Level0 - Mozilla Firefox
Level0
20.195.8.131/levels/level0.php
Welcome Isuranga
Logout
Level 0
Use your common sense...
Home
Level 0
Level 1
Level 2
Level 3
Level 4
Level 5
Level 6
Level 7
Level 8
Level 9
Level 10
Scoreboard
Enter the Flag
Flag *
N1c3y0UF0unD1t
N1c3y0UF0unD1t
Submit

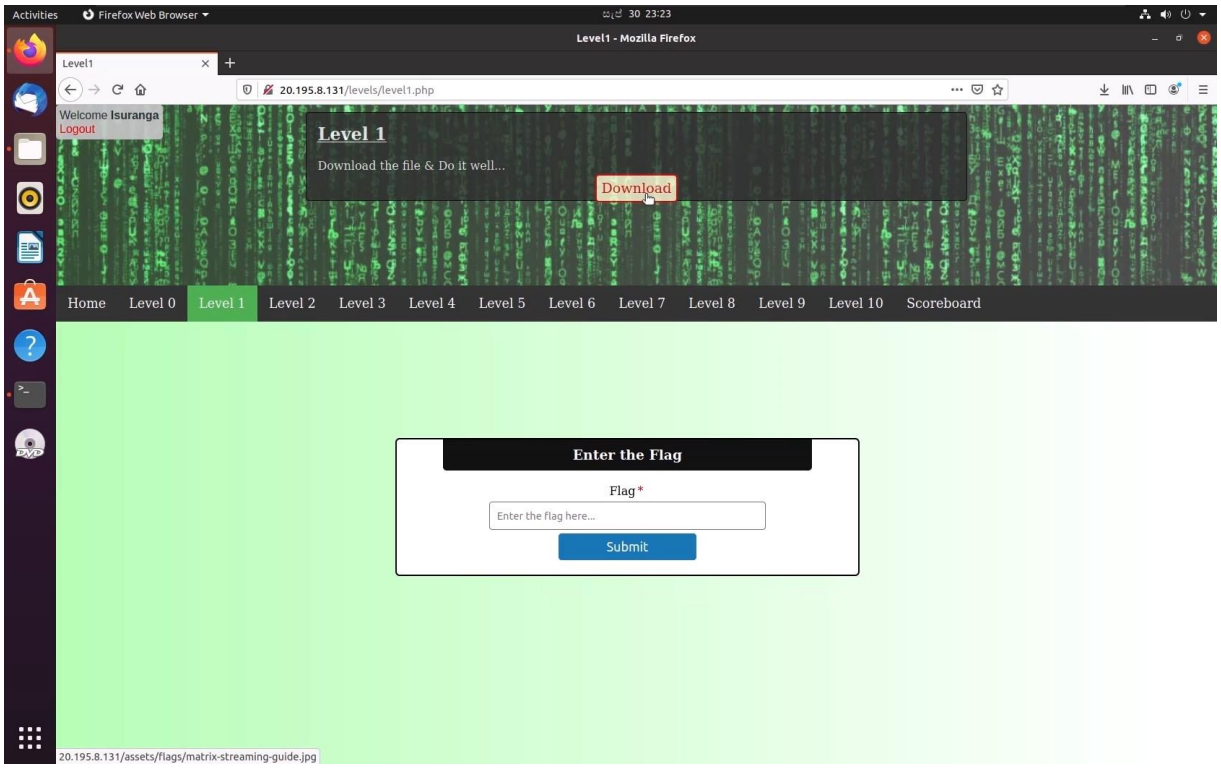
- After entering the flag, if it is correct the level will be completed.



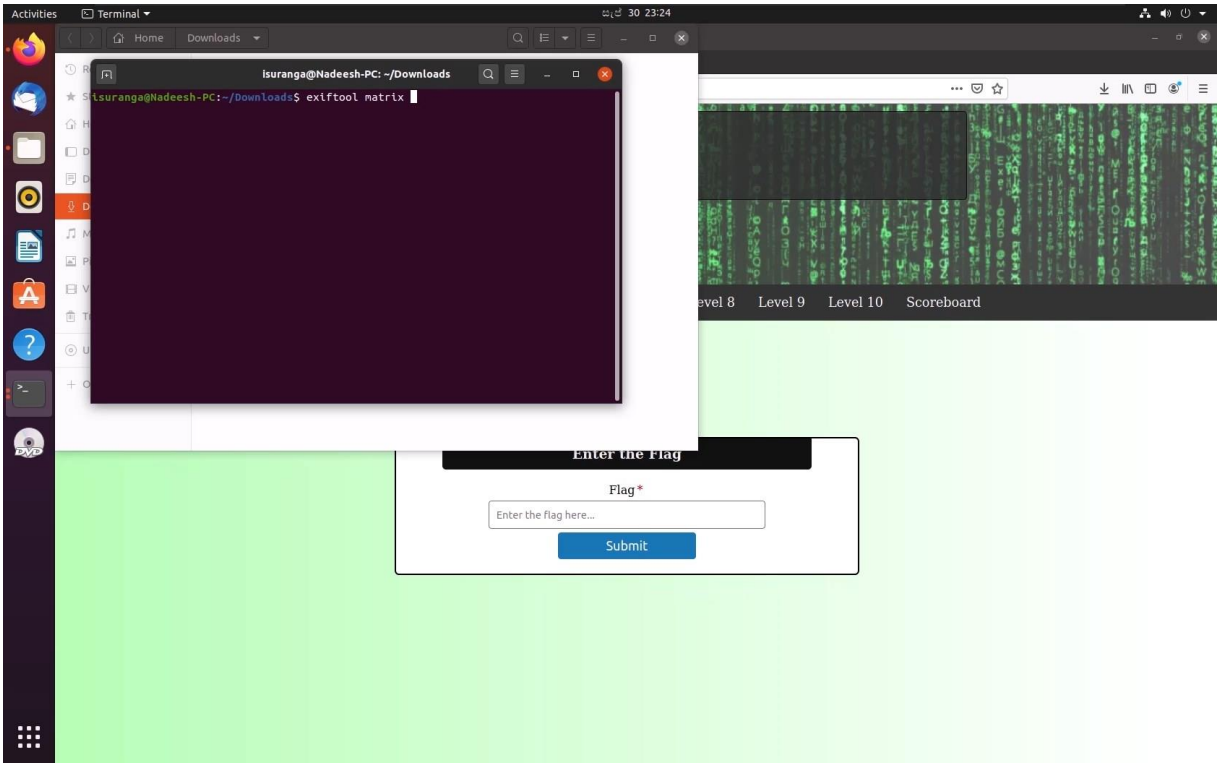
- And the sore bord show the mark that obtained.

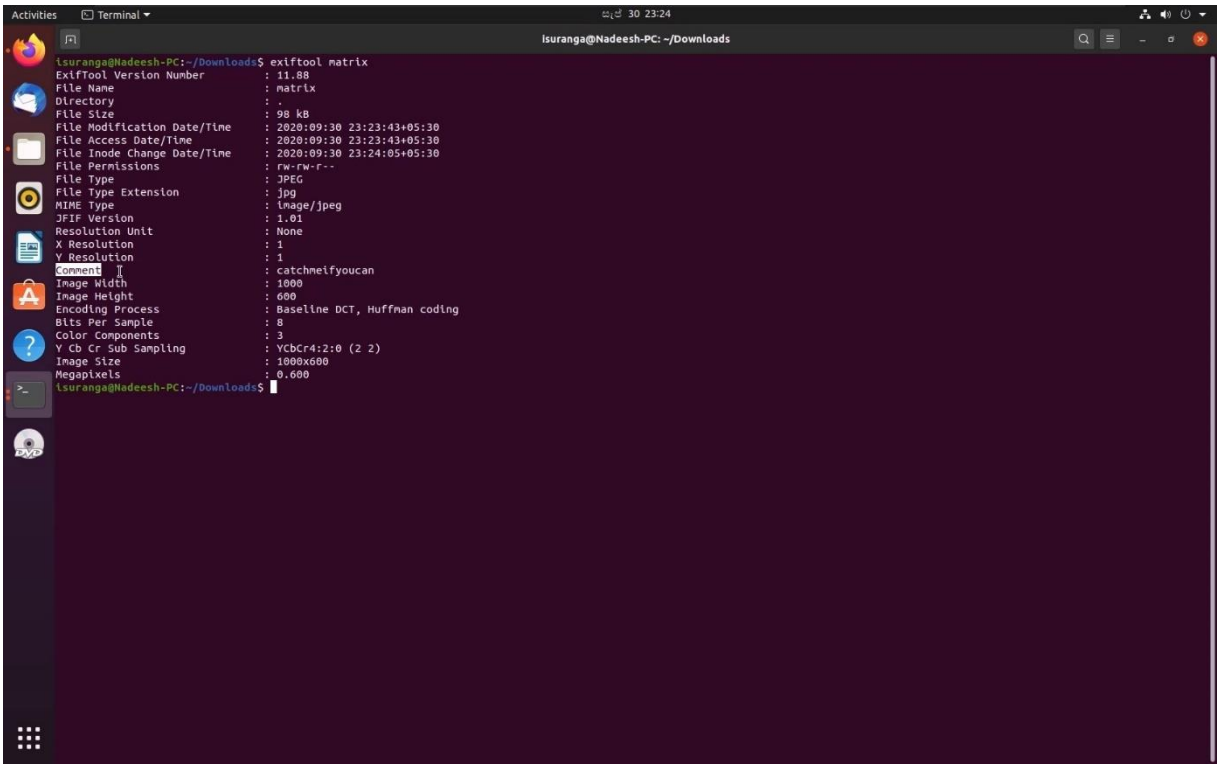


Level 1



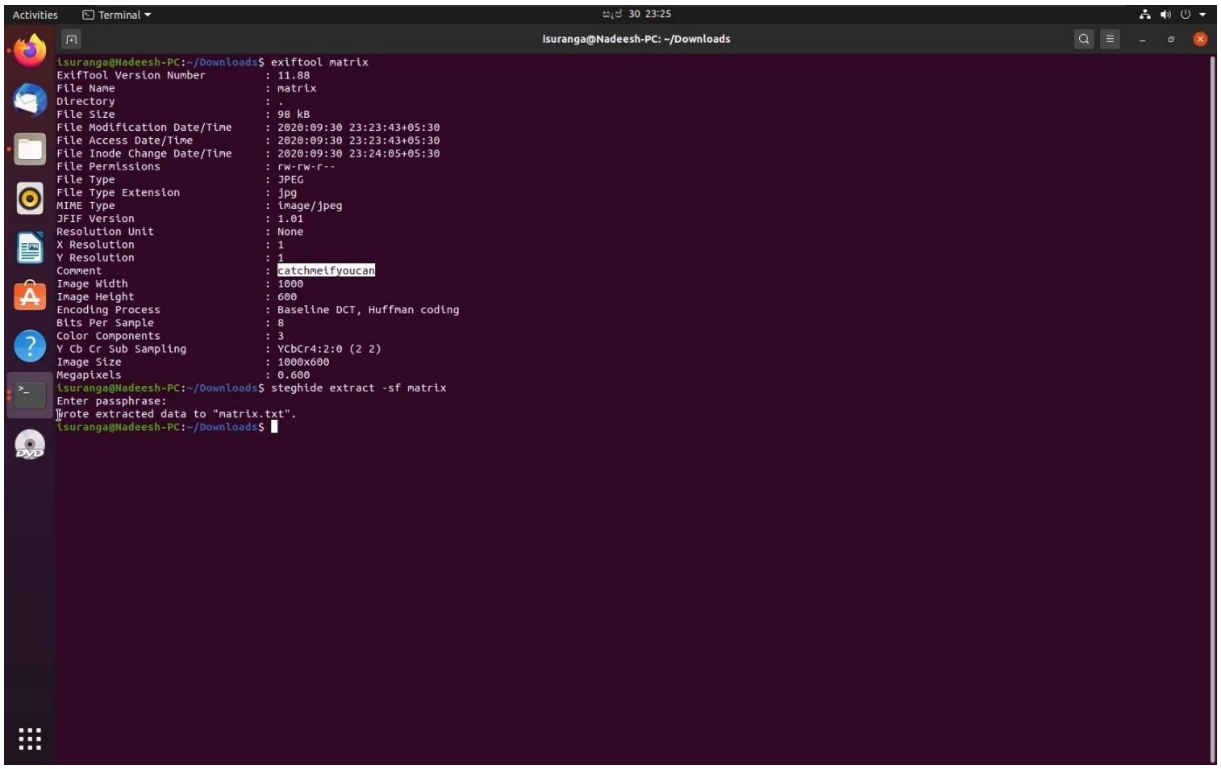
- After getting the Image file to a Linux environment. Scan the image for file type. That we need a tool to see METADATA of the image. After enough research and the hint suggests Exiftool. Download and install the tool with the command: “sudo apt-get install exiftool”. After installing check, the image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



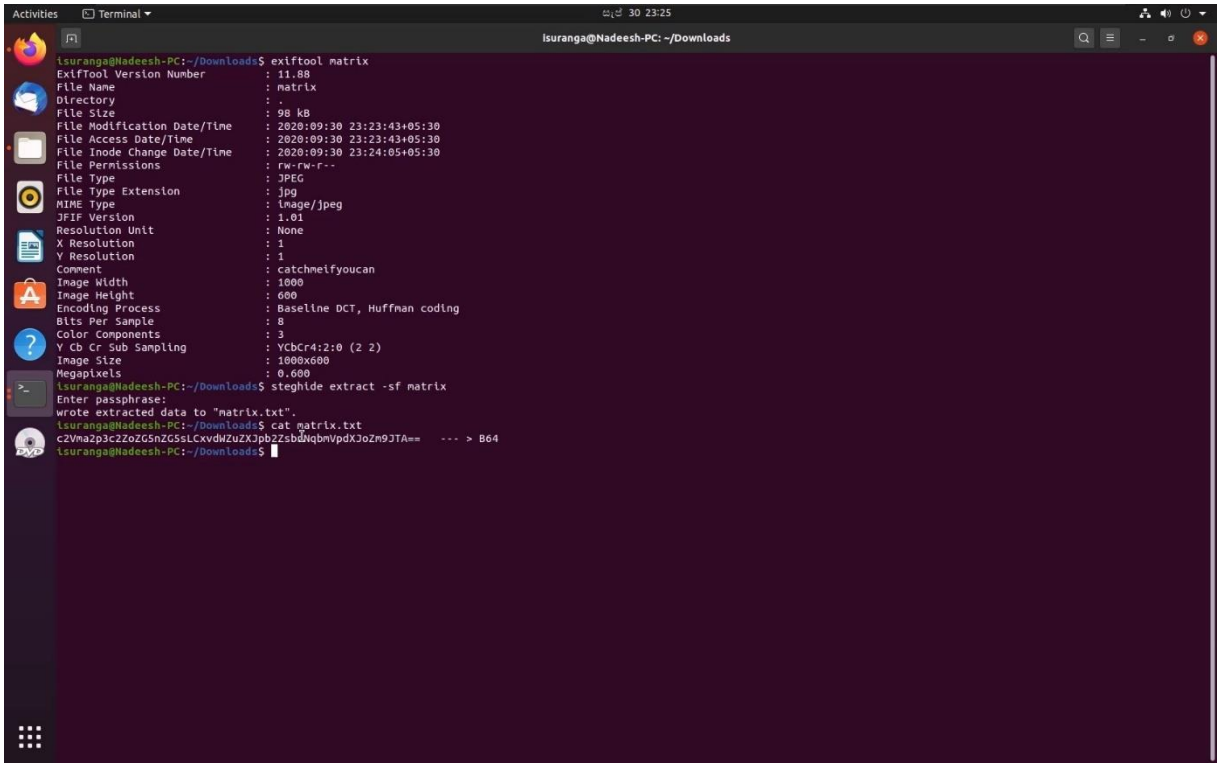


- Install: “sudo apt-get install steghide”. Run the command: “steghide extract -sf matrix.jpg”. Next the passphrase will be required, enter it. New file “secret” without an extension is extracted out of the image. Open it to find the next step:
- In under the comment tab there have a hint as passphrase.

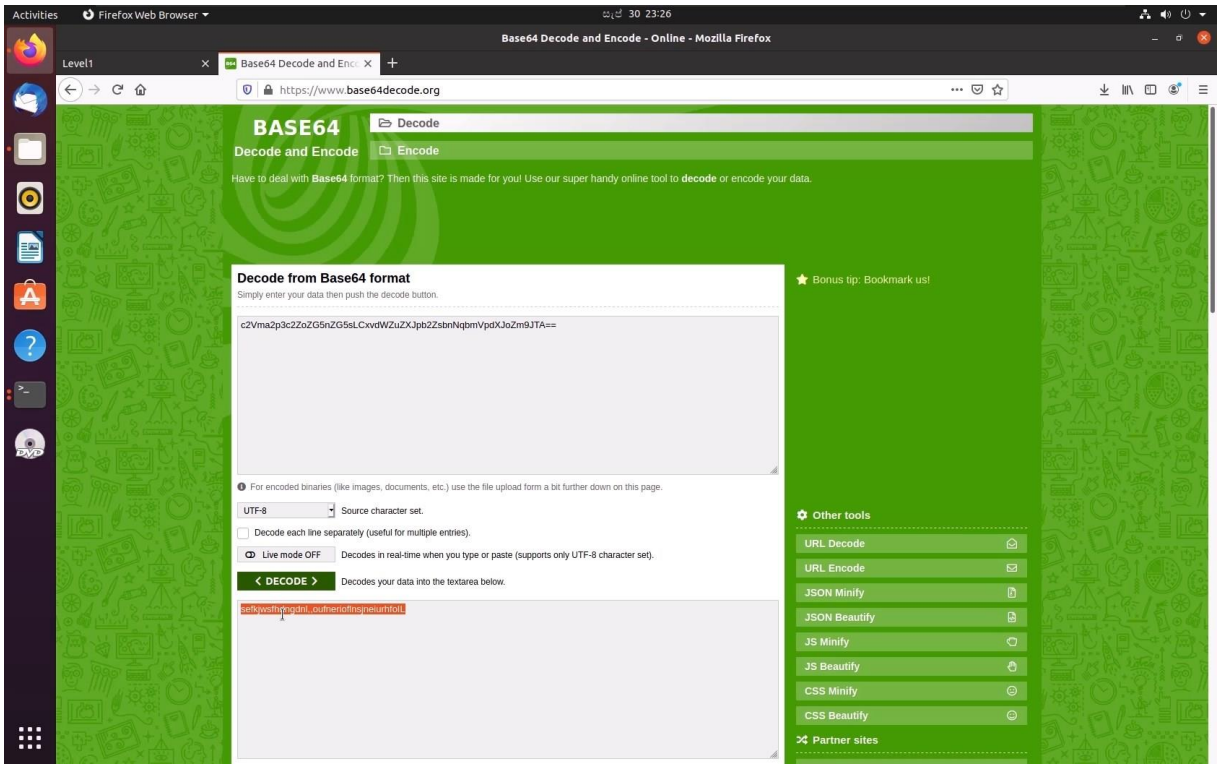
- After including passphrase, it will show the message to read the matrix.txt file.



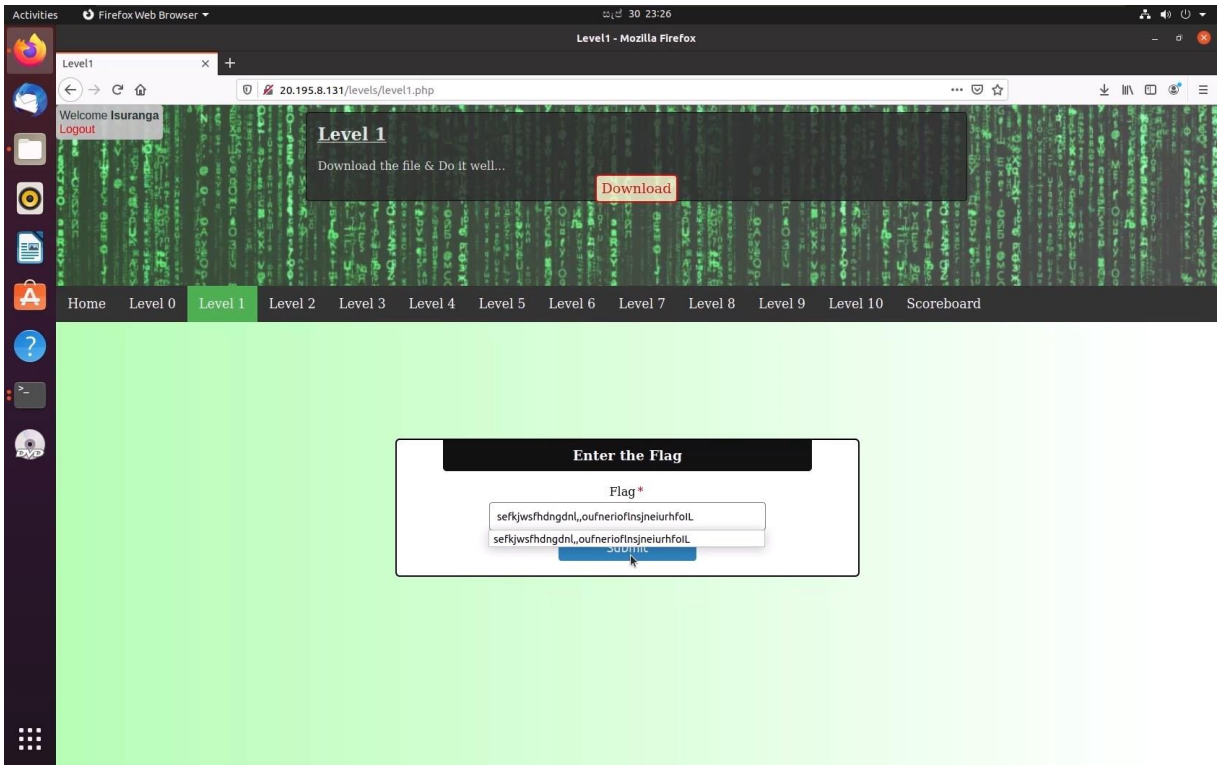
- That will show a encoded text there.



- To decode the text should use any base 64 decoder.

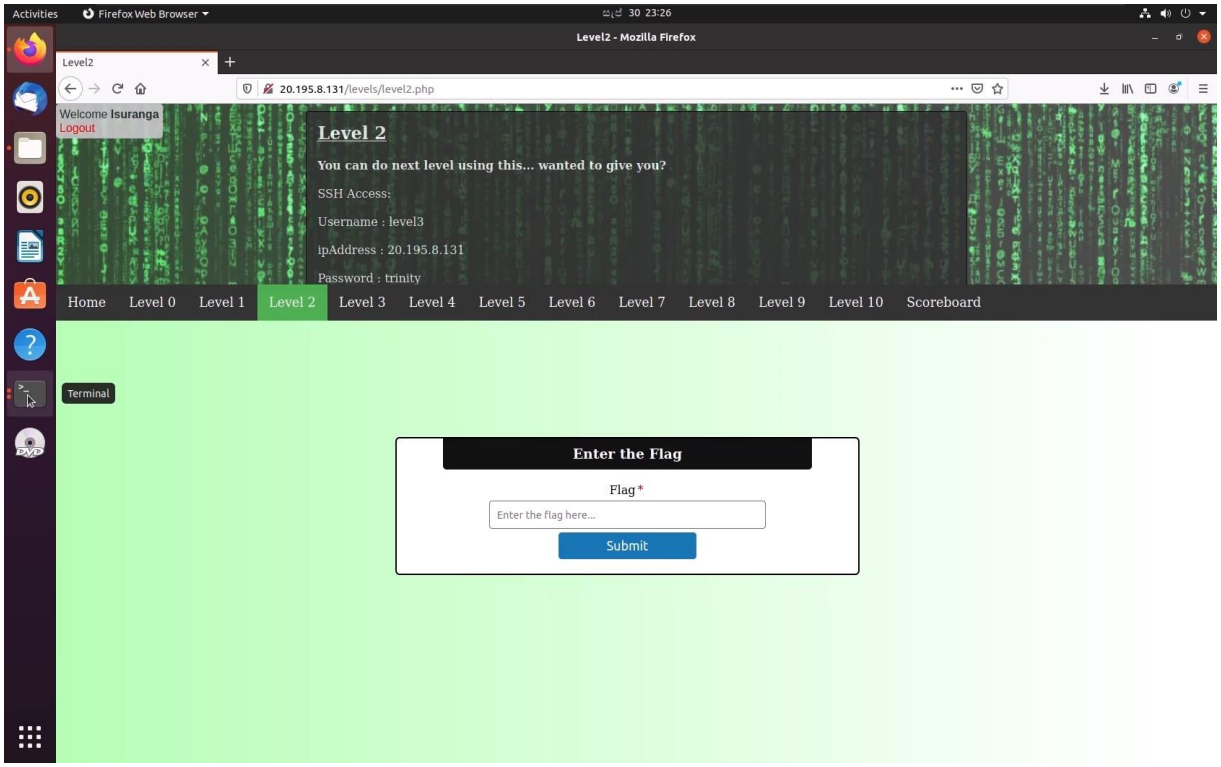


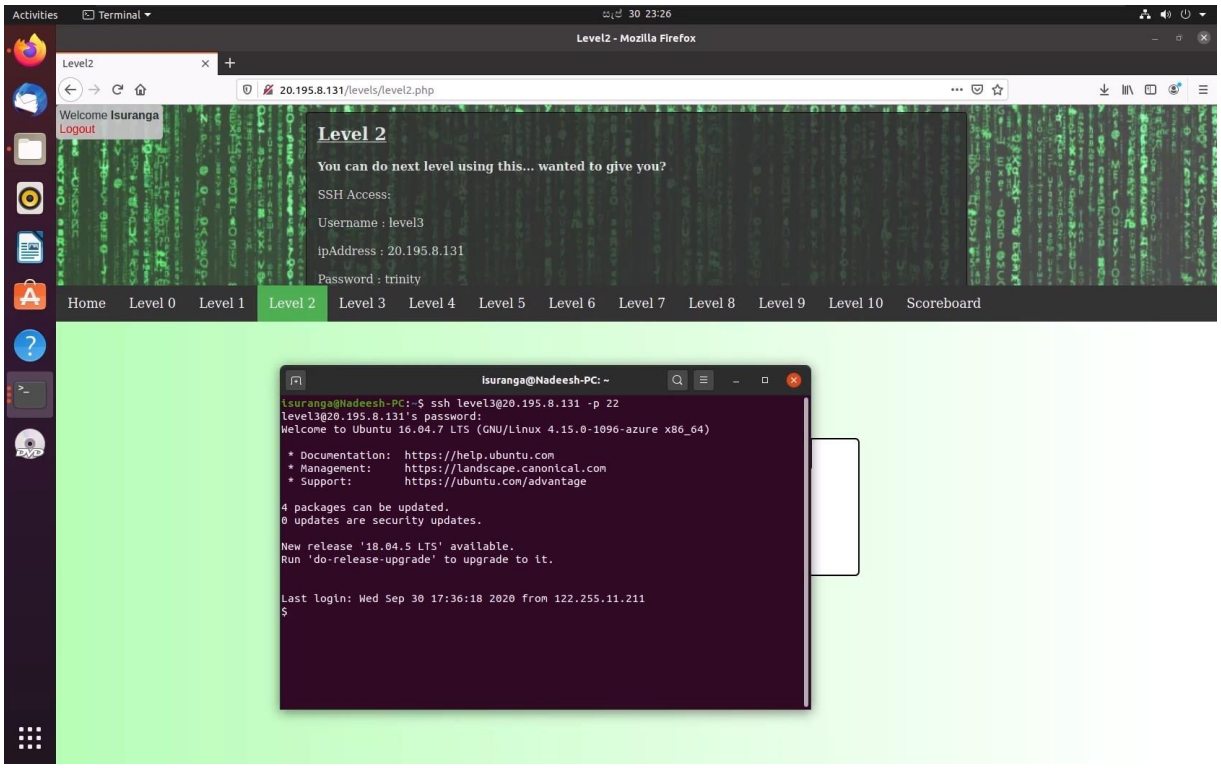
- After decoding text can use it as the flag 😊.



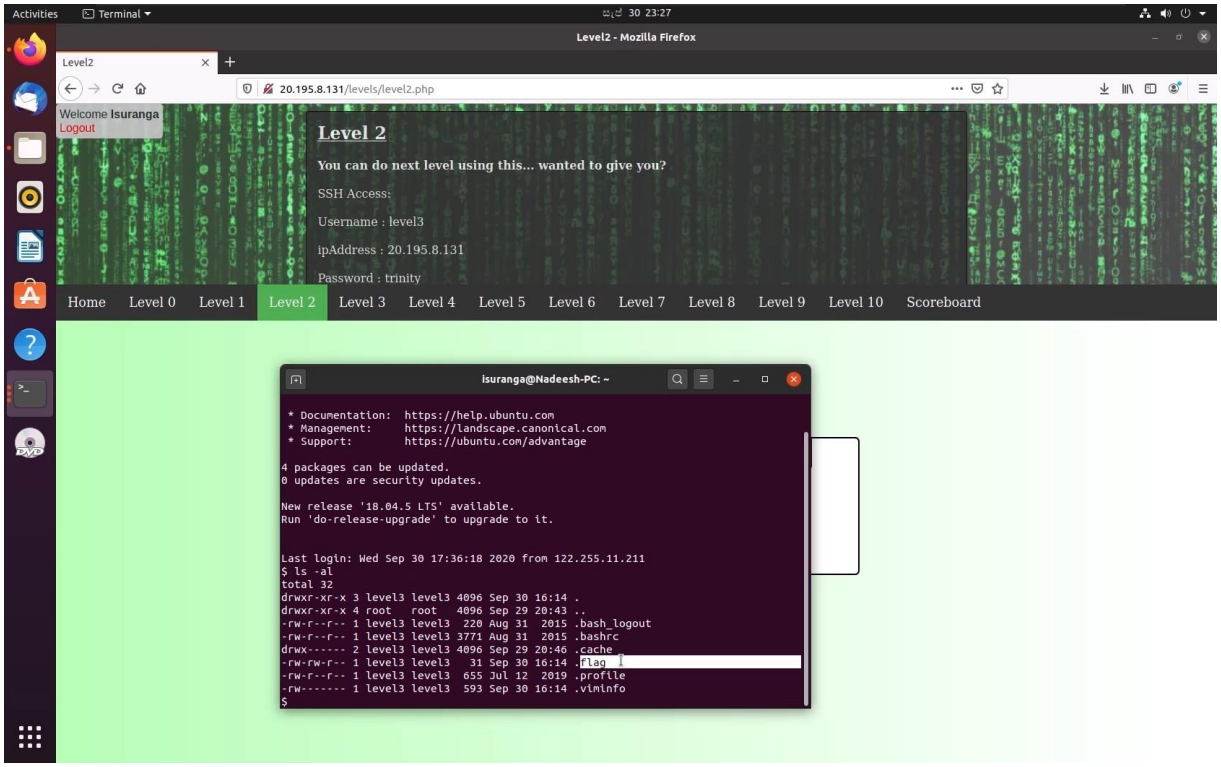
Level 2

- At the level 2 In this level, the ssh access is provided.

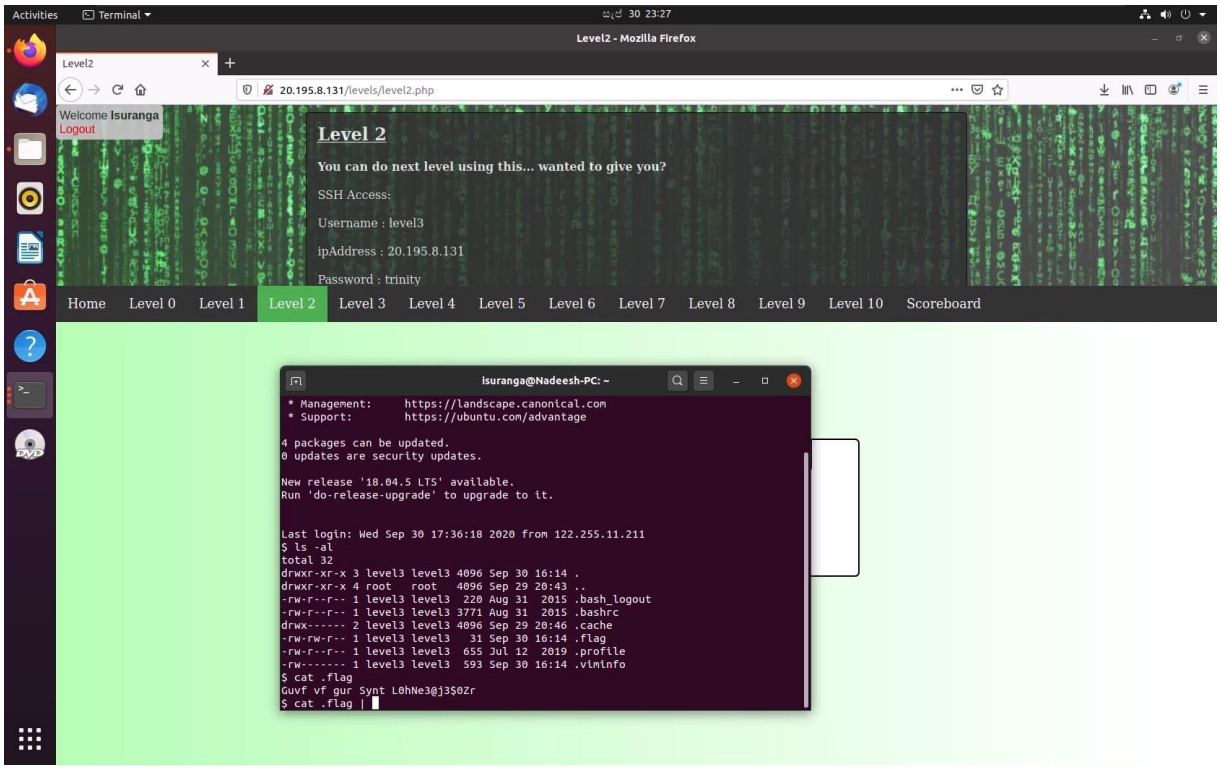




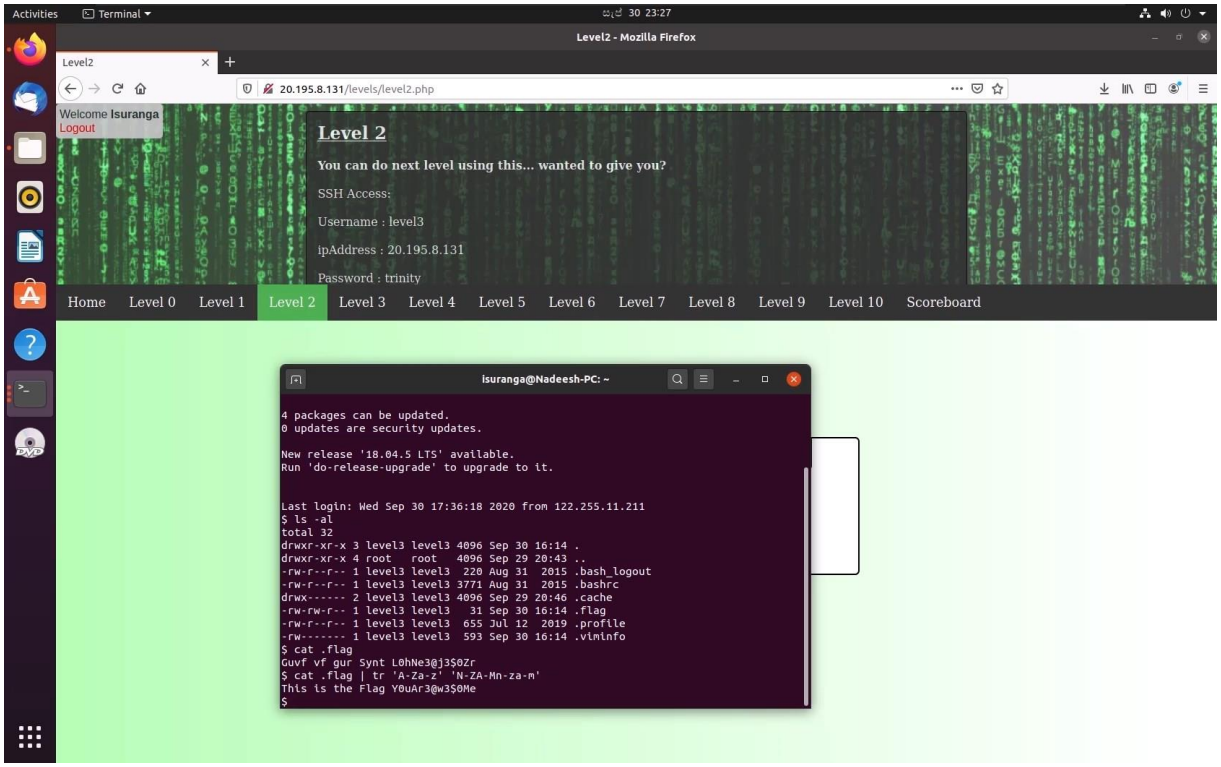
- After getting into the ssh access a file called “flag”.

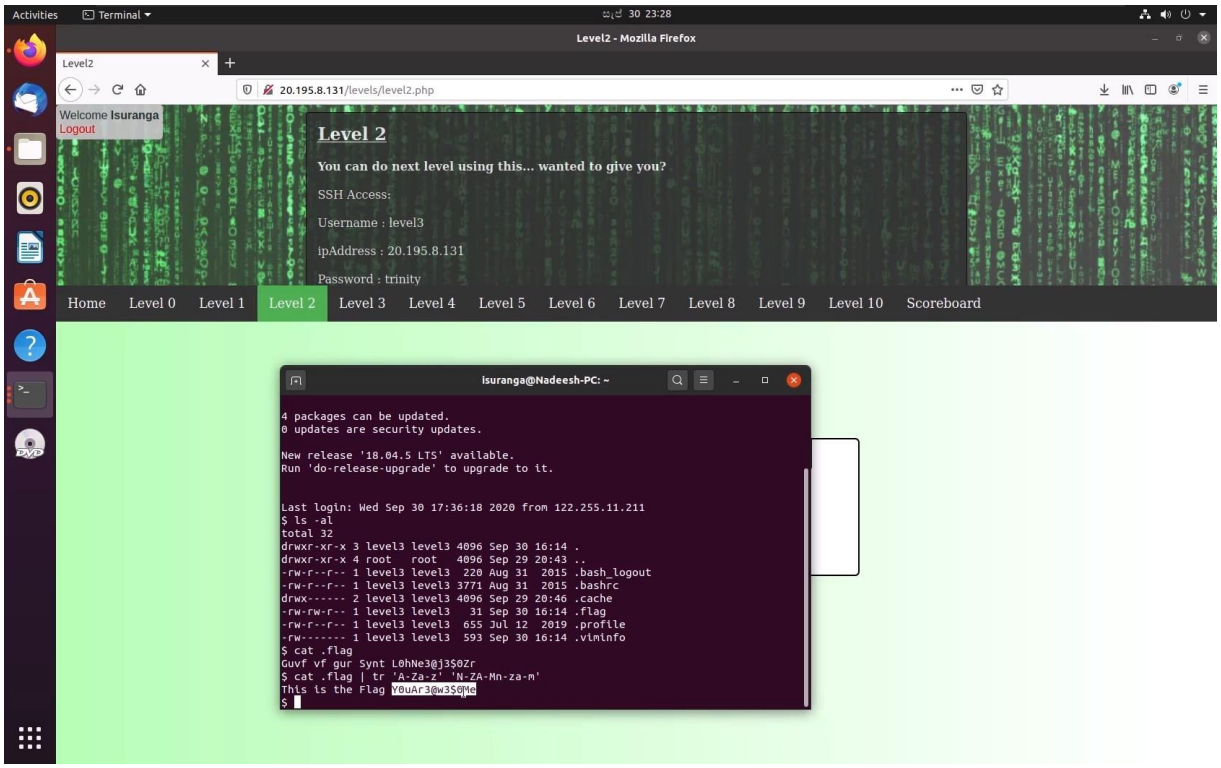


- Read the file to get the hint.

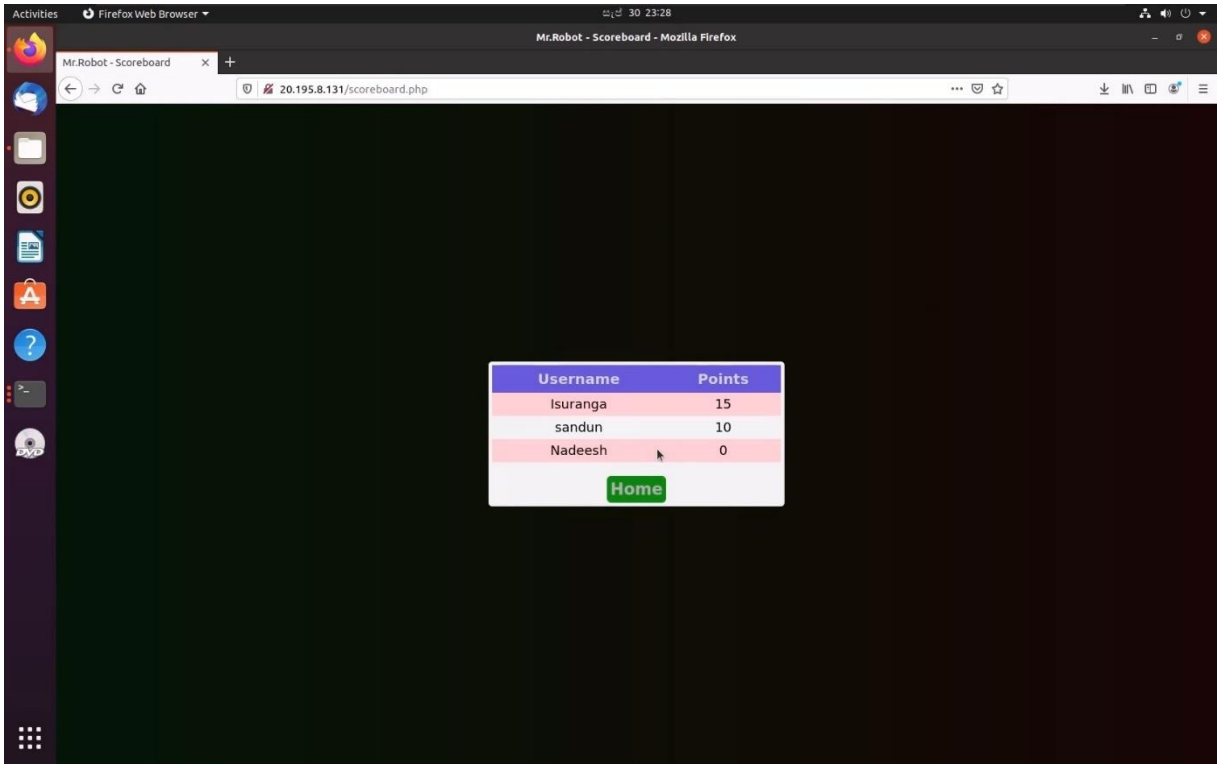


- The file contains the flag,
- The hint is the encrypted using ROT 13 chipper method.
- But it is encrypted. To decrypt use, rotate 13 and the following command:
  $ cat .flag | tr ‘A-Za-z’ ‘N-ZA-za-m’





- After completing 3 levels the score board show marks as 15.



Level 3

Level 4

Level 5

Level 6

Level 7

Level 8

Level 9

Level 10