



Sri Lanka Institute of Information Technology

Final Project Report

ISP Project Report

Information Security Project 2022

Project ID: 19

Submitted by:

IT Number	Name
IT19154640	Weerasiri H.A.K.D.
IT19990200	K A P A K P Kathriarachchi

Date of submission

06th June 2022

Abstract

The world around us is rapidly digitalizing, as well as the internet is nearly ubiquitous, making cyber security an unavoidable aspect of our daily life. Capture-the-flag games have had a good influence on Individuals' levels of motivation and involvement Capture-the-flag games were found to lead to vastly higher learning outcomes and a greater awareness of cybersecurity in several research.

Additional benefits included improved practical understanding in cyber security, higher grades, and more assurance in cyber security abilities.

Organizing such games was discovered to be a difficult task, and as a result, knowledge is required from both organizers and participants in capture-the-flag games. Capture-the-flag game settings are complicated, and support personnel are required to organize such games. It was discovered that designing the tasks to be properly hard was a difficult process, and a related challenge was difficulty avoidance. This document describes the Introduction, Methodology, and Evaluation of our CTF box "TheBlackList."

Acknowledgement

The authors are grateful to Dr. Lakmal Rupasinghe, our lecturer in charge of the Information Security Project module, who has offered advice and inspiration since the start of this study. I would also want to thank Ms. Laneesha Ruggahakotuwa, Ms. Chathu Udagedara, and Ms. Menaka Moonamaldeniya for their assistance in understanding the topic and ensuring the success of this event. Finally, I'd want to express my heartfelt appreciation to everyone who contributed knowledge and opportunities to assist us finish this job on schedule.

Declaration

We certify that even this project document, or any section of it, is not really a copy of a based on the discovery by any institution, college, or other organization, or a prior student project group at SLIIT, and that it was not taken from the Internet or other sources.

Project Details

Project Title	The Black List
Project ID	ISP-22-REG-19

Group Members



Reg. No	Name	Signature
IT19154640	Weerasiri H.A.K.D.	
IT19990200	K A P A K P Kathriarachchi	

Table of Contents

Abstract.....	i
Acknowledgement.....	iii
Declaration.....	iv
Table of Contents	vi
List of Figures.....	Error! Bookmark not defined.
List of Tables	Error! Bookmark not defined.
1. Introduction.....	1
1.1 Problem Statement.....	1
1.2 Product Scope.....	1
1.3 Project Report Structure	1
2. Methodology	3
2.1 Requirements and Analysis	3
2.2 Design.....	3
2.3 Implementation.....	5
2.4 Testing	8
3. Evaluation.....	9
3.1 Assessment of the Project results	9
3.2 Lessons Learned	9
3.3 Future Work.....	9
4. Conclusion	10
5. References.....	Error! Bookmark not defined.
Appendix A: Test Results.....	6

1. Introduction

1.1 Problem Statement

Capture-the-flag (CTF) games are challenges in which the aim is to uncover concealed flags in a specific computer space. The ecosystem might be as little as a single website or as large as a whole network of computers. Jeopardy and attack-defense are the two most prevalent forms of CTF games. A Jeopardy-style tournament often includes numerous categories with various tasks to complete. In an attack-defense competition, each team is assigned a network or a host computer to protect while attempting to exploit the other teams.

The primary goal of this research is to investigate how CTF games help education while also investigating potential downsides and obstacles associated with the format. The scope of this study is not limited to CTF games. Other kinds of gamified and offensive cyber security education being investigated as needed. As a result, the main study question is "what are the benefits and drawbacks of adopting capture-the-flag games in cyber security education?" A supplementary research question is "is there any quantitative proof of discovered benefits and drawbacks?" CTF activities are a fun and gratifying method to learn different areas of cyber security, and the world around us is rapidly digitalizing, with the internet nearly everywhere, making cyber security an unavoidable, albeit often seemingly inconsequential, part of our lives. The advantages of employing CTF games in cyber security education include increased student motivation and improved practical understanding because of the method. The format's challenges included significant educational requirements both from organizers and the performers, as well as complicated technological needs.

1.2 Product Scope

Challenge type is **WEB**

This sort of challenge focuses on locating and exploiting software vulnerabilities. This might include assessing the participants' understanding of SQL Injection, XSS (Cross-Site Scripting), CSRF, and other topics.

Audience

- This project directly affects Linux users, and it may be able to impact their existing Linux OS settings or configuration.

- This would be a great aid in fixing flaws and vulnerabilities that have already happened in the Linux environment in order to carry out work for Linux Developers / Backend Developers.
- It is recommended that research students study all sections of this manual to gain a general understanding of the workflow and technical aspects of the program.
- This is beneficial to testers and may be used as documentation to learn about the interfaces.
- Threat Intelligence would be able to obtain information in a variety of methods after exhausting all possibilities, which is also a great approach to inspire them when they are involved in such a scenario.

Scenario

The world's most wanted fugitive was taken to the custody by the FBI. They found a laptop that was used by the fugitive to monitor his tasks. This laptop contains a list of deadly criminals which is called “The Blacklist” and the FBI needs access to that list. Attacker Used to put info about other ranked hackers’ details into his created databased, which stored on web page, with Tight secure involved it. For that FBI chooses professionals with security skills. To get access to The Blacklist they must use security and hacking techniques.

Specific Target System – web applications and databases

Technologies use – HTTP,PHP,SQL,CSS,Javascript,html,apache,Kali linux O/S

Main expected outcomes of the project:

Our CTF challenge is perfect for experts in threat intelligence and security operations centers. They may efficiently hone their security expertise and Sell it to an organization, Host in TryHackMe.

1.3 Project Report Structure

The following chapters will be covered in this project report. Requirements and analysis, design, implementation, and testing are all part of the technique. The review and conclusion contain an evaluation of the results, lessons were learned, and next steps.

2. Methodology

2.1 Requirements and Analysis

The following chapters will be covered in this project report. Requirements and analysis, design, implementation, and test are all part of the technique. The review and conclusion contain an evaluation of the results, lessons were learned, and next steps.

Various difficulties, A variety of challenge categories, Increasing the level of difficulty, Adequate instruction for novices, such as offering reading material Information on the comparison of real-world attack vectors and CTF challenges.

2.2 Design

Based on findings, a prototype CTF was created to introduce people to critical cyber security principles. We used a prioritizing strategy to prioritize the needs pertaining to content because there are several CTF challenge types. Competitions were chosen based on the shortest possible design time.

This analysis resulted in the design of:

Web difficulties using OWASP web top ten examples Cryptography problems with samples of various encryption and encoding systems Forensics difficulties, including file forensics and steganography instances, Various tasks that put broad abilities to the test, such as Linux command line expertise, programming knowledge, and the ability to utilize a number of tools, OSINT obstacles that foster creativity and renaissance.

Although Pwn and Reverse Engineering tasks were also possible, they would take a long time to construct due to the substantial knowledge and proficiency required in low level programming languages and assembly code. Although Pwn and Reverse Engineering tasks were also possible, they would take a long time to construct due to the substantial knowledge and expertise required in low level programming languages and assembly code.

Here is the overview of the design of CTF box.



2.3 Implementation

Tools and techniques used to create web interface

- Xampp - XAMPP is a free and open-source cross-platform web server solution stack package developed by Apache Friends, consisting mainly of the Apache HTTP Server, MariaDB database, and interpreters for scripts written in the PHP and Perl programming languages.
- Html
- Css
- JQuery

Tools and techniques used to create CTF challenges

- Level 0 - Base 64 decoder
- Level 1 – Fernet decoder,cyberchef,malborge interpreter
- Level 2 – dirbuster & gobuster
- Level 3 - Exif tool and steghide(in linux environment)
- Level 4 - Wireshark packet analysis
- Level 5 - This flag based on cryptography with cease cipher
- Level 6 - Sonic visualizer
- Level 7 - zip tools and Linux commands (chmod +x,ltrace,strings,strcmp)

Implementation of DBMS

- 'tbl_flag' creating

```

26 --
27 -- Table structure for table `tbl_flag`
28 --
29
30 CREATE TABLE `tbl_flag` (
31   `id` int(2) NOT NULL,
32   `flag` varchar(255) NOT NULL
33 ) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4;
34
35 --
36 -- Dumping data for table `tbl_flag`
37 --
38
39 INSERT INTO `tbl_flag` (`id`, `flag`) VALUES
40 (0, 'f4fc80e5e72d80c4ced184f0f9dec60c'),
41 (1, 'c98b8b5385c34b66da50d038de45eb46');

```

New

tbl_flag

tbl_member

information_schema

☐ Show all | Number of rows: 25 | Filter rows: Search this table

+ Options

	id	flag
<input type="checkbox"/> Edit <input type="checkbox"/> Copy <input type="checkbox"/> Delete	0	f4fc80e5e72d80c4ced184f0f9dec60c
<input type="checkbox"/> Edit <input type="checkbox"/> Copy <input type="checkbox"/> Delete	1	76075accfd8e58eff92e2edd731b504a
<input type="checkbox"/> Edit <input type="checkbox"/> Copy <input type="checkbox"/> Delete	2	8ed9075e56a43476ecbf15faceb5ea11
<input type="checkbox"/> Edit <input type="checkbox"/> Copy <input type="checkbox"/> Delete	3	49e0739521348ed967033a90949cbad3
<input type="checkbox"/> Edit <input type="checkbox"/> Copy <input type="checkbox"/> Delete	4	9feae1f63856249b03de58258c5a234a
<input type="checkbox"/> Edit <input type="checkbox"/> Copy <input type="checkbox"/> Delete	5	f9a175ce76ba7778c2336cbe36cfe67
<input type="checkbox"/> Edit <input type="checkbox"/> Copy <input type="checkbox"/> Delete	6	628a2dea872fb6df3872f01dd8c31d2a
<input type="checkbox"/> Edit <input type="checkbox"/> Copy <input type="checkbox"/> Delete	7	6fe48c97c5697704f7896af2b1c52768
<input type="checkbox"/> Edit <input type="checkbox"/> Copy <input type="checkbox"/> Delete	8	4e8cd6d15aae9ab0b5bf660b21e789d9b
<input type="checkbox"/> Edit <input type="checkbox"/> Copy <input type="checkbox"/> Delete	9	4e8cd6d15aae9ab0b5bf660b21e789d9b

☐ Check all | With selected: ☐ Edit ☐ Copy ☐ Delete ☐ Export

- “tbl_member” creating

```

48 --
49 CREATE TABLE `tbl_member` (
50   `id` int(11) NOT NULL,
51   `username` varchar(255) NOT NULL,
52   `password` varchar(200) NOT NULL,
53   `email` varchar(255) NOT NULL,
54   `lv10` int(11) NOT NULL DEFAULT 0,
55   `lv11` int(11) NOT NULL DEFAULT 0,
56   `lv12` int(11) NOT NULL DEFAULT 0,
57   `lv13` int(11) NOT NULL DEFAULT 0,
58   `lv14` int(11) NOT NULL DEFAULT 0,
59   `lv15` int(11) NOT NULL DEFAULT 0,
60   `lv16` int(11) NOT NULL DEFAULT 0,
61   `lv17` int(11) NOT NULL DEFAULT 0,
62   `lv18` int(11) NOT NULL DEFAULT 0,
63   `lv19` int(11) NOT NULL DEFAULT 0,
64   `lv110` int(11) NOT NULL DEFAULT 0,
65   `points` int(2) NOT NULL DEFAULT 0,
66   `create_at` timestamp NOT NULL DEFAULT current_timestamp() ON UPDATE current_timestamp()
67 ) ENGINE=InnoDB DEFAULT CHARSET=latin1;
68
69 --
70 -- Dumping data for table `tbl_member`
71 --
72
73 INSERT INTO `tbl_member` (`id`, `username`, `password`, `email`, `lv10`, `lv11`, `lv12`, `lv13`, `lv14`, `lv15`, `lv16`, `lv17`, `lv18`, `lv19`, `lv110`, `points`, `create_at`
74 (1, 'sandun', '$2y$10$9Rp3b1T18CKcWQeB3e09VRwzRnPHtzy3SWoxH9...', 'sandundananjaya@sd.com', 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, '2020-09-28 19:35:08'),
75 (2, 'nadeesh', '$2y$10$A9ATV1NX2zWC.TMLAcTruedrNTAOiqG5534meUD...', 'saasndundananjaya@asdi.com', 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, '2020-09-22 15:51:03'),
76 (3, 'ac', '$2y$10$UgQosG007a/eOTXgWfUdunt2PcglwJf72xaAs1M1x8dFnbSC/Hm', 'ac@abs.com', 5, 5, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, '2020-09-28 20:22:16'),
77
78

```

New

tbl_flag

tbl_member

information_schema

☐ Profiling [Edit inline] [Edit] [Explain SQL] [Create PHP code] [Refresh]

☐ Show all | Number of rows: 25 | Filter rows: Search this table | Sort by key: None

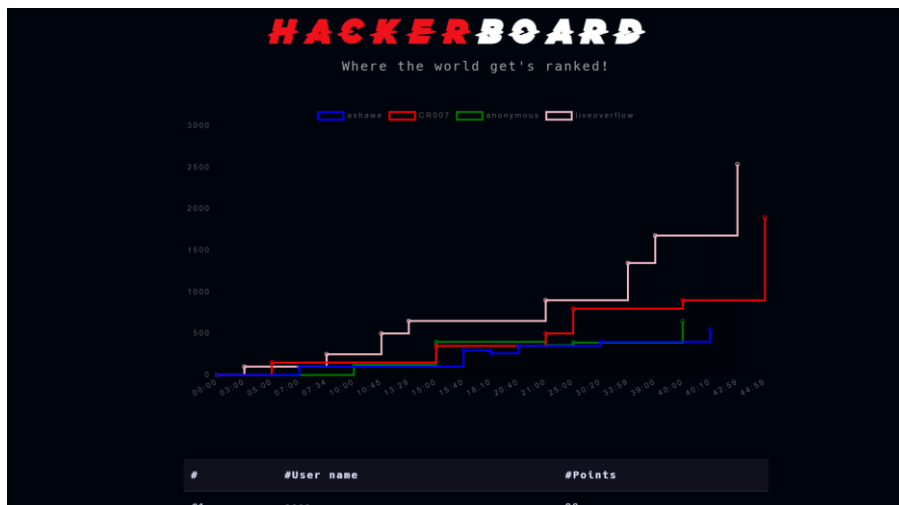
+ Options

	id	username	password	email	lv10	lv11	lv12	lv13	lv14	lv15	lv16	lv17	lv18	lv19	lv110	points	create_at
<input type="checkbox"/> Edit <input type="checkbox"/> Copy <input type="checkbox"/> Delete	1	sandun	\$2y\$10\$9Rp3b1T18CKcWQeB3e09VRwzRnPHtzy3SWoxH9...	sandundananjaya@sd.com	0	0	0	0	0	0	0	0	0	0	0	0	2020-09-28 19:35:08
<input type="checkbox"/> Edit <input type="checkbox"/> Copy <input type="checkbox"/> Delete	2	nadeesh	\$2y\$10\$A9ATV1NX2zWC.TMLAcTruedrNTAOiqG5534meUD...	saasndundananjaya@asdi.com	0	0	0	0	0	0	0	0	0	0	0	0	2020-09-22 15:51:03
<input type="checkbox"/> Edit <input type="checkbox"/> Copy <input type="checkbox"/> Delete	3	ac	\$2y\$10\$UgQosG007a/eOTXgWfUdunt2PcglwJf72xaAs1M1x8dFnbSC/Hm	ac@abs.com	5	5	0	0	0	0	0	0	0	0	0	0	2020-09-28 20:22:16
<input type="checkbox"/> Edit <input type="checkbox"/> Copy <input type="checkbox"/> Delete	10	aces	\$2y\$10\$6AE8ak2pq1w8znWek3D.BuYTsK3ymwvwiRgUJzeQ...	aces@gg.com	5	5	10	0	0	0	0	0	0	0	0	0	2020-09-28 20:22:16

☐ Check all | With selected: ☐ Edit ☐ Copy ☐ Delete ☐ Export

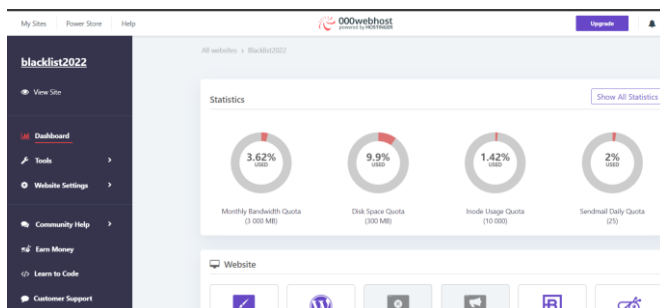
Scoreboard Implementation

```
1 k?php
2 const HOST = 'localhost';
3
4 const USERNAME = 'id19050723_dakshina_uname';
5
6 const PASSWORD = 'WkPvGR4P=nw9^I{g';
7
8 const DATABASENAME = 'id19050723_dakshina';
9
10 // Create connection
11 $conn = new mysqli(HOST, USERNAME, PASSWORD, DATABASENAME);
12 // Check connection
13 if ($conn->connect_error) {
14     die("Connection failed: " . $conn->connect_error);
15 }
16 ?>
17
18 <!DOCTYPE html>
19 <html lang="en">
20
21 <head>
22     <!-- Required meta tags -->
23     <meta charset="utf-8">
24     <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
25     <title>TheGambit</title>
26
```



Host website in a live server

We import web pages and the databases to a free domain hosting server



Tryhackme Implementation

tryhackme.com/jr/blacklist2022



2.4 Testing

Testing is the most important component of the project. The Try hack me implementation required to be tested unit by unit. We performed a test to see if the jobs were compatible with the website and could be properly executed once each one was done while they were being produced stepwise. We had ten tasks in our project, and we examined each one to determine if it could be played by a user by looking at the features that the developers had included. Whenever it comes to website creation, we created pages to assist with the process. Following completion, the developers were required to test each page individually. If the current page has a link to a different page.

During the testing implementation, a few small flaws were detected and swiftly resolved. Following that, developers must inspect the application's backend to ensure that the data entered by the users is valid. Specific users of the web application were brought in for integrated testing.

The following stage is to ensure that all jobs contribute to the different online tools and platforms. During the testing implementation, a few small difficulties were detected and swiftly resolved. Following that, developers must inspect the application's backend to ensure that the data entered by the users is valid. A system check is conducted after unit and integrated testing. Following that,

there should be a discussion with all of the project's developers and others, and then acceptance testing should commence. The project was completed after those test runs. Both the "Try Hack Me" implementation and the website were verified to be bug-free following the tests.

3. Evaluation

3.1 Assessment of the Project results

Walkthroughs were conducted with three people, each lasting roughly 30 minutes, to assess the tool's usability. The participants were final-year computing students, two of whom had never participated in a CTF before.

The assessment comments were mostly favorable, showing that the tool has the ability to pique students' interest in cybersecurity and lead them while developing their practical abilities. Furthermore, the study found that the CTF experience (use) discouraged certain students from pursuing a profession in cyber security or ethical hacking in particular.

3.2 Lessons Learned

We learned following things by creating this CTF.

- Basic enumeration of HTTP.
- Steganography using steghide.
- Basics of SSH.
- Abuse sudo to get root privilege escalation.

3.3 Future Work

Customized CTF challenges focusing on the learning perspective and providing considerable educational context will be produced in the future. In this approach, certain components may be updated or developed to provide enhanced gamification features, quizzes, and evaluation methods.

One crucial element would be to integrate storytelling components to discover and evaluate the potential of using CTF systems and customizable CTF challenges for educational purpose, not only in information security but also in related topics like user privacy and privacy-aware data governance, and to capitalize on the outcomes of based tasks.

4. Conclusion

The main purpose of this study was to learn to think creatively on how a system may be attacked and to look at how CTF games could improve education. We conducted a comparison study for various aspects of cyber security, highlighting the specific operating systems, technologies, and tools for each level of our CTF box, and we were able to draw conclusions about the advantages and disadvantages of chosen innovations. Considering each technology, we chose the most appropriate technologies and tools for our CTF based on the purpose and audience that we chose. Additional elements that may enhance the platforms were also suggested.

5. References

2022, C. M. (n.d.). *Learning Resources*. Retrieved from picoCTF: <https://picoctf.org/resources>

aurelius. (2018, 04 22). *Tools and resources to prepare for a hacker CTF competition or challenge*. Retrieved from INFOSEC: <https://resources.infosecinstitute.com/topic/tools-of-trade-and-resources-to-prepare-in-a-hacker-ctf-competition-or-challenge/>

Capture The Flag 101. (n.d.). Retrieved from ctf101.org: <https://ctf101.org/>

CTFs. (n.d.). *Introduction*. Retrieved from CTF Resources: <https://ctfs.github.io/resources/index.html>

Lightfoot, J. (n.d.). *So, You Want to CTF? (A Beginner's Guide to CTFing)*. Retrieved from J Lightfoot: <https://jaimelightfoot.com/blog/so-you-want-to-ctf-a-beginners-guide/>

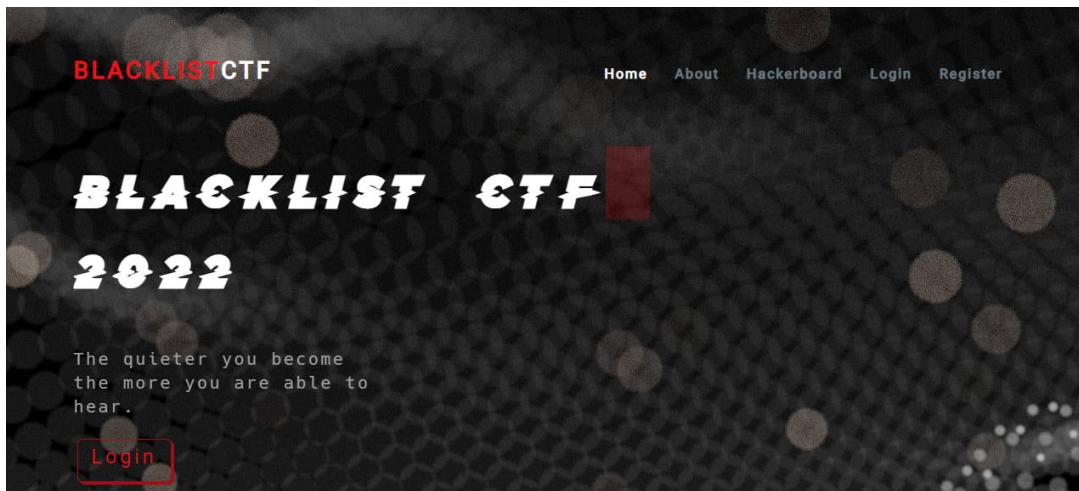
Appendix A: Test Results

Walkthrough for setup

1. Link to the main website(CTF):

When the user is new to the CTF, that user must be registered to the site,

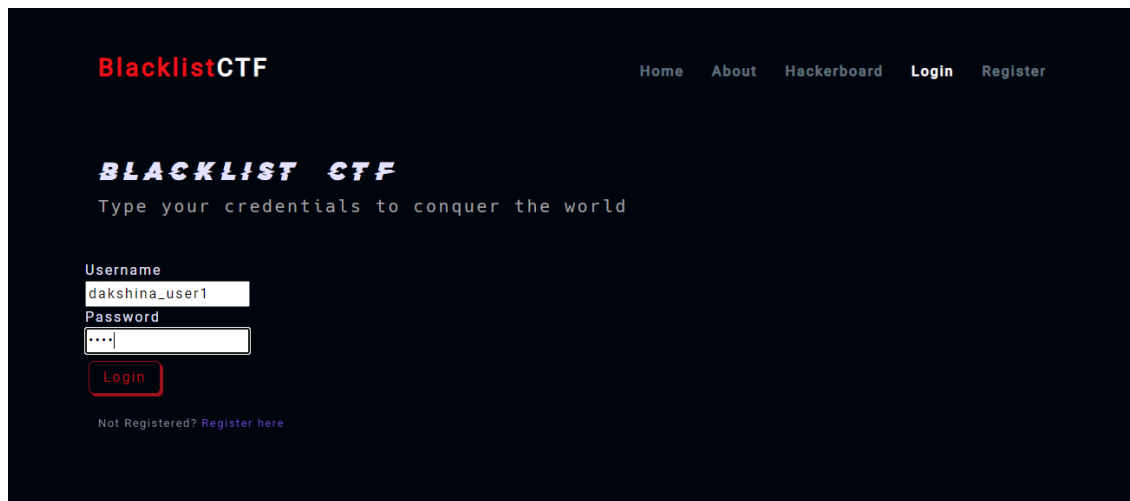
After the registration, user can grab the way to CTF and all of instruction are given in there.



Interface



Register as new user



The image shows the login page of the BlacklistCTF website. At the top, the logo "BlacklistCTF" is displayed in red and white. To the right, there are navigation links: "Home", "About", "Hackerboard", "Login", and "Register". Below the logo, the text "BLACKLIST CTF" is written in a stylized, bold font. Underneath, it says "Type your credentials to conquer the world". The login form consists of two input fields: "Username" with the value "dakshina_user1" and "Password" with masked characters "....". A red "Login" button is positioned below the password field. At the bottom, there is a link "Not Registered? Register here" in purple.

BlacklistCTF

Home About Hackerboard Login Register

BLACKLIST CTF

Type your credentials to conquer the world

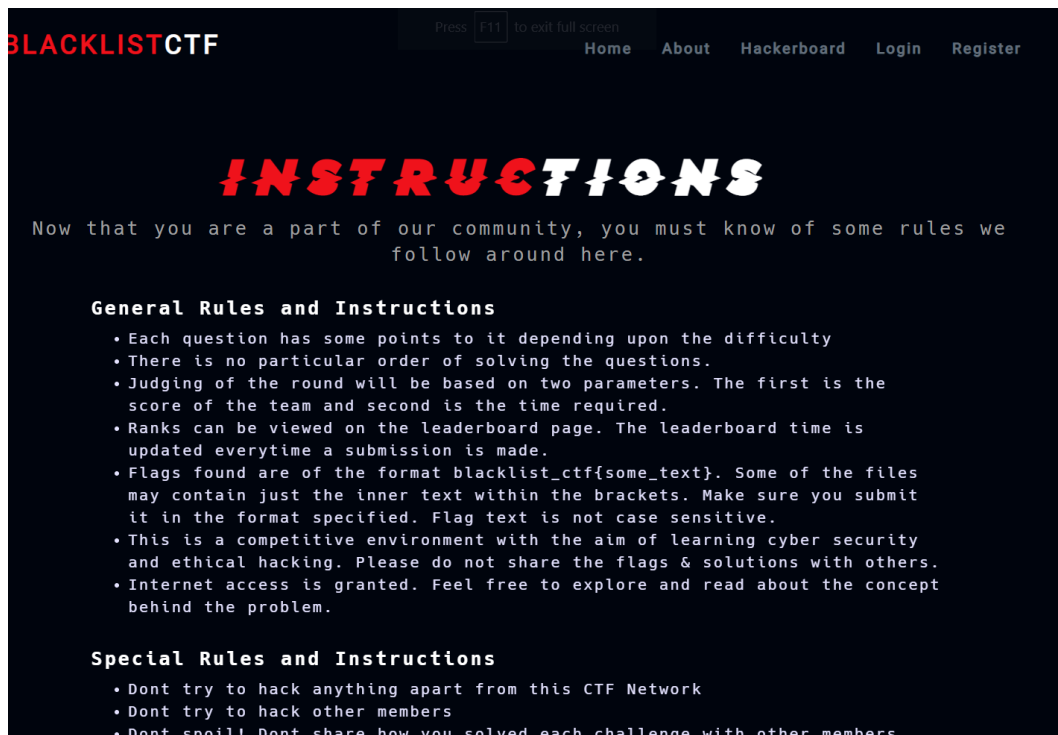
Username
dakshina_user1

Password
....

Login

Not Registered? Register here

Register user must logging from here.



The image shows the "INSTRUCTIONS" page of the BlacklistCTF website. At the top, the logo "BLACKLISTCTF" is displayed in red and white. To the right, there are navigation links: "Home", "About", "Hackerboard", "Login", and "Register". Below the logo, the word "INSTRUCTIONS" is written in a large, bold, red font. Underneath, it says "Now that you are a part of our community, you must know of some rules we follow around here." The page is divided into two sections: "General Rules and Instructions" and "Special Rules and Instructions".

BLACKLISTCTF

Press F11 to exit full screen

Home About Hackerboard Login Register

INSTRUCTIONS

Now that you are a part of our community, you must know of some rules we follow around here.

General Rules and Instructions

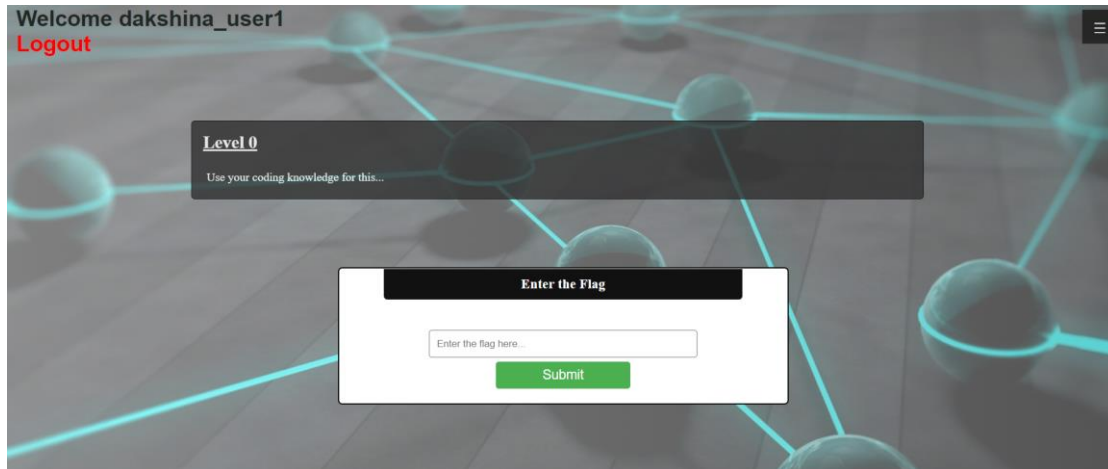
- Each question has some points to it depending upon the difficulty
- There is no particular order of solving the questions.
- Judging of the round will be based on two parameters. The first is the score of the team and second is the time required.
- Ranks can be viewed on the leaderboard page. The leaderboard time is updated everytime a submission is made.
- Flags found are of the format `blacklist_ctf{some_text}`. Some of the files may contain just the inner text within the brackets. Make sure you submit it in the format specified. Flag text is not case sensitive.
- This is a competitive environment with the aim of learning cyber security and ethical hacking. Please do not share the flags & solutions with others.
- Internet access is granted. Feel free to explore and read about the concept behind the problem.

Special Rules and Instructions

- Dont try to hack anything apart from this CTF Network
- Dont try to hack other members
- Dont spoil! Dont share how you solved each challenge with other members

Instruction will be given to further go.

Walkthrough of Level



Level 0

Can be use small code knowledge, user has to view the source code of the site. After going to scroll down , there is a hint to flag,

```
122     $('.error-field').first().focus();
123     valid = false;
124 }
125 return valid;
126 }
127 </script>
128
129 <script>
130 /* Set the width of the sidebar to 250px and the left margin of the page content to 250px */
131 function openNav() {
132     document.getElementById("mySidebar").style.width = "200px";
133     /* QW5GQmhIdkMiakhizDU0ZGJKbmQ1bkRuOG5HZ25LNmc= -> b64 */
134     document.getElementById("main").style.marginLeft = "200px";
135 }
136
137 /* Set the width of the sidebar to 0 and the left margin of the page content to 0 */
138 function closeNav() {
139     document.getElementById("mySidebar").style.width = "0";
140     document.getElementById("main").style.marginLeft = "0";
141 }
142 </script>
143
144 <style>.footer,.generic-footer{margin-bottom:98px}@media (min-width:374px){.footer,.generic-footer{margin-bott
145 </HTML>
```

Small hint to use base 64, user must be decode it with base 64 decoder,

Do you have to deal with **Base64** format? Then this site is perfect for you! Use our super handy online tool to encode or **decode** your data.

Decode from Base64 format

Simply enter your data then push the decode button.

QW5GQmhidkM1akhiZDU0ZGJKbmQ1bkRuOG5HZ25LNmc=

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

UTF-8 Source character set.

☐ Decode each line separately (useful for when you have multiple entries).

☒ Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

< DECODE > Decodes your data into the area below.

AnFBhbvC5jHbd54dbJnd5nDn8nGgnK6g

Flag is : **AnFBhbvC5jHbd54dbJnd5nDn8nGgnK6g**

Level 01

Welcome dakshina_user1
Logout

Level 1

Download and Decipher the key to the next level

Download

Enter the Flag

Enter the flag here...

Submit

First download the files,

Essential links that need to go ,

<https://asecuritysite.com/encryption/ferdecode>

- for fernet

<https://gchq.github.io/CyberChef/>

-for decrypt

<https://malbolge.doleczek.pl>

- for find the flag

```
DPQAnNPe5y8wjwROoxeKUr4z7TwAEPXCioOSons7Ctjvw=  
gAAAAABfbD3bh9_Vav50imX4uho8VdVmdashtko80D9p5HaVVRrb0AE2wvAJC8w6mGpDPvgjgnF--BkEyV48BML_Le0hrVcv1-PZ0tLb0266PoiDDFZmY1LrmtUGm  
52oEVNRIqsaoJwCBYi54tBnK3zXqCRfY62Vg4h1FqDdTjF7_DcWNOwTEQLVOnv088fHcYyJvqpbCvrxFeD9EvaYtY5ssTLyBs1u9Ddg-aOyc9c_fkrP9-S40m0t  
uVAZ8eOneDp0mgDu40w_rKyOddjj_Yj7swQ3tvj8mP4e9ucqjK8TPRNUZENv2h21hNpTKENMbsIsjoGDq80uqxGg650Dw0Q3PCn_3zQtvzuVEHksELy1SNjksUq  
S_s15Nxr2IE_5q7RUpbBnU6cp0bSVDFAHcuIsngJJnfwsvuEDseDSRgkBIqc0hrLOvc3AvJATHrYC9HWreJKVvh79yaYigcPeKHeivsFTfiJxRd3TnrDLP6SChVM  
tmt4JZYsBF7s8xbMr4-ACodAAorW3CSaQw8POBNN-sv36I5SZHqNCsrvuZ1GwvtFBL08GvQe_jyXq1LRI7h8qAPk1yUtKRgRRC0bzZWkx4v5DZGieKwxUgj7Hdk4_  
GmJmo4mU=
```

In this level gives us a value. Its looks like a base 64 value, but it's not a base 64, it's an encryption key for the AES encryption called Fernet. It's a URL safe encryption. There are so many online tools for decryption. We had to decrypt the message as well.

[Encryption Home][Home]

Fernet is a symmetric encryption method which makes sure that the message encrypted cannot be manipulated/read without the key. It uses URL safe encoding for the keys. Fernet uses 128-bit AES in CBC mode and PKCS7 padding, with HMAC using SHA256 for authentication. The IV is created from `os.random()`. This page decodes the token. Generate a token here: [\[Fernet\]](#)

Token:	<code>tmt4JZYsBF7s8xbMr4-ACodAAorW3CSaQw8POBNN-sv36I5SZHqNCsrvuZ1GwvtFBL08GvQe_jyXq1LRI7h8qAPk1yUtKRgRRC0bzZWkx4v5DZGieKwxUgj7Hdk4_GmJmo4mU=</code>
Key:	<code>QAnNPe5y8wjwROoxeKUr4z7TwAEPXCioOSons7Ctjvw=</code>

Determine

Decoded:
`LXFzbl6gYCVdF6Q3obgQnKHQnKVLYsoj6rFgCDMeKvMjZud3tmjbiSVBTj1ryYLx3SW5YTAcmPBXA6giGbmNxHhDRNudaUZe3FBTxDRmiFUHfchFRy3qskfr2n7arFUSIoFzwZdwB
CFbKabxmTvt1FjcGGY2SwaBGdd8xzid7pGqsXjm8PBWH2Q8fy7nUbMrAMLEf1euFGZCYHT9Vv29zUoRu2fJJsG7V4hzNv4QZ2qEtjZxeTHtCuF2vo1kQqMG1nch4rUZ5t9DMGg3gZsnj
ZVcAagAgtdkytkR4K59eRFgocMPoeztPBZebemMeFqTVzMveDCwfk3X1N2fZM5an9cQgsCdDnZKpi5YoJ8wCqzkSwZLeS425aDU69G9nNzadmQNe7sL1vcFCYFqQgwFKk7nGe
Date created: Thu Sep 24 06:34:03 2020`

gchq.github.io/CyberChef/#recipe=Magic(3,false,false,"")&input=ThhGemJMNmdZQ1ZKqjZRM29IZ1FuS0hRbkt2VxoSc...

Download CyberChef Last build: 2 days ago Options About / S

Operations

- magi
- Magic**
- Image Filter
- Image Opacity
- Image Brightness / Contrast
- Image Hue/Saturation/Lightness
- Detect File Type
- Scan for Embedded Files
- Favourites
- Data format
- Encryption / Encoding
- Public Key
- Arithmetic / Logic
- Networking

Recipe

Magic

Depth 3 ☐ Intensive mode ☐ Extensive language support

Crib (known plaintext string or regex)

Input

Length: 411 Lines: 1

LxFzbl6gYCVdF6Q3obgQnKHQnkvLysoj6rFgCDMeKvMjZud3tmjbisvBTJjryYLX3SWSYACmpBXA6gigbmUxhh3FTXDrmIFUHFchFRy3qskfr2n7arfUS1oFzwZdwbCfbKabxhtv1FjcGGY2SwaBgdd8xZID7pGgsXjm8PBW4Q8FYEf1euFGZCYHT9Vv29zuOru2fJjsG7V4hzhV4QZ2qEtjZxetHTCuF2vo1kQqMG1nch4rUZ5t9DMGg3gZsnjZvcAagAk59eRFgocMPoeztPBZebemMeFqTVzVveDCwfk3X1N2fzMSan9cQgscdDNzKpi5YoJ8wCqzKswZLeS425aDU69G9nHLL1vcFCYfqqgwFKk7nGe

Output

start: 49 time: 23ms
end: 128 length: 13025
length: 79 lines: 477

Recipe (click to load)	Result snippet	Properties
From Base58('123456789ABCDEFGHJKLMNPQRSTUVWXYZabcdefghijkmnopqrstuvwxyz', false)	D';*#n]lkzMD6BRR?Oaqoo8I[6F432U#cb?ON)9xq7on4lkjoh.fhdchgfed]#[C_X\][ZYXW90TMq430Hl/EDIBff?'C...]	Valid UTF8 Entropy: 6.29
LxFzbl6gYCVdF6Q3obgQnKHQnkvLysoj6rFgCDMeKvMjZud3tmjbisvBTJjryYLX3SWSYACmpBXA6gigbmUxhhRNUdaU...	LxFzbl6gYCVdF6Q3obgQnKHQnkvLysoj6rFgCDMeKvMjZud3tmjbisvBTJjryYLX3SWSYACmpBXA6gigbmUxhhRNUdaU...	Matching ops: From Base64 Valid UTF8 Entropy: 5.75

Recipe

From Base58

Alphabet 123456789ABCDEFGHJKLMNPQRSTUVWXYZabcdefgh...

☐ Remove non-alphabet chars

Input

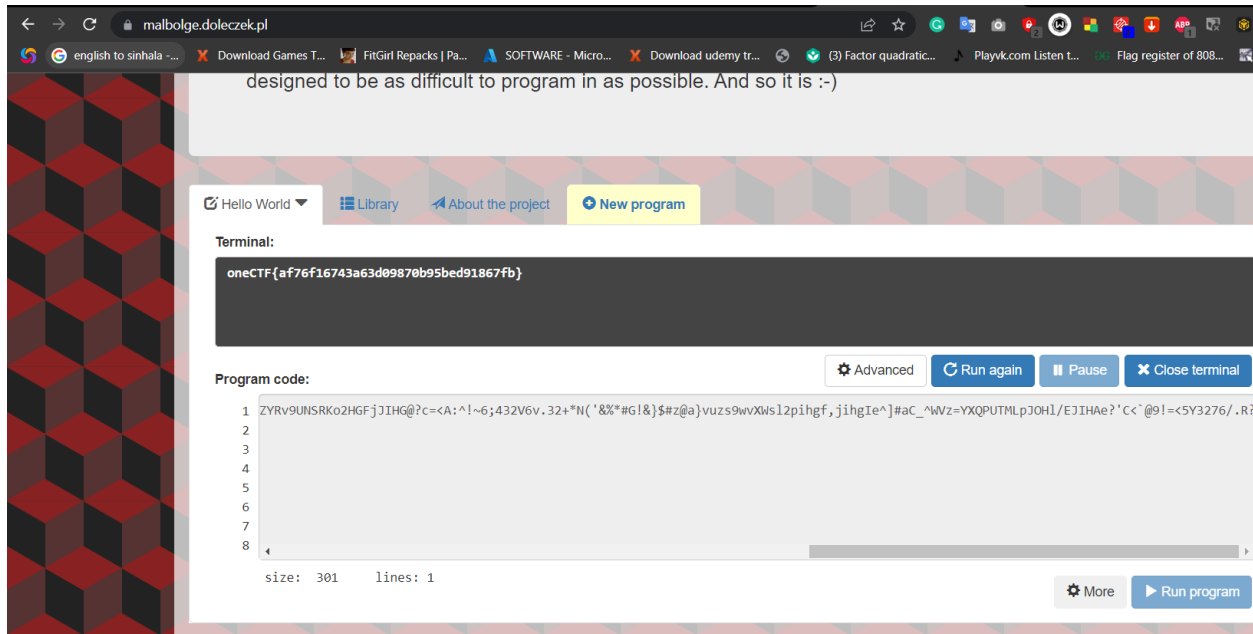
Lines: 1

LxFzbl6gYCVdF6Q3obgQnKHQnkvLysoj6rFgCDMeKvMjZud3tmjbisvBTJjryYLX3SWSYACmpBXA6gigbmUxhhRNUdaUZe3FTXDrmIFUHFchFRy3qskfr2n7arfUS1oFzwZdwbCfbKabxhtv1FjcGGY2SwaBgdd8xZID7pGgsXjm8PBW4Q8FYEf1euFGZCYHT9Vv29zuOru2fJjsG7V4hzhV4QZ2qEtjZxetHTCuF2vo1kQqMG1nch4rUZ5t9DMGg3gZsnjZvcAagAgtdkvtKR4K59eRFgocMPoeztPBZebemMeFqTVzVveDCwfk3X1N2fzMSan9cQgscdDNzKpi5YoJ8wCqzKswZLeS425aDU69G9nHnZadmQNe7sL1vcFCYfqqgwFKk7nGe

Output

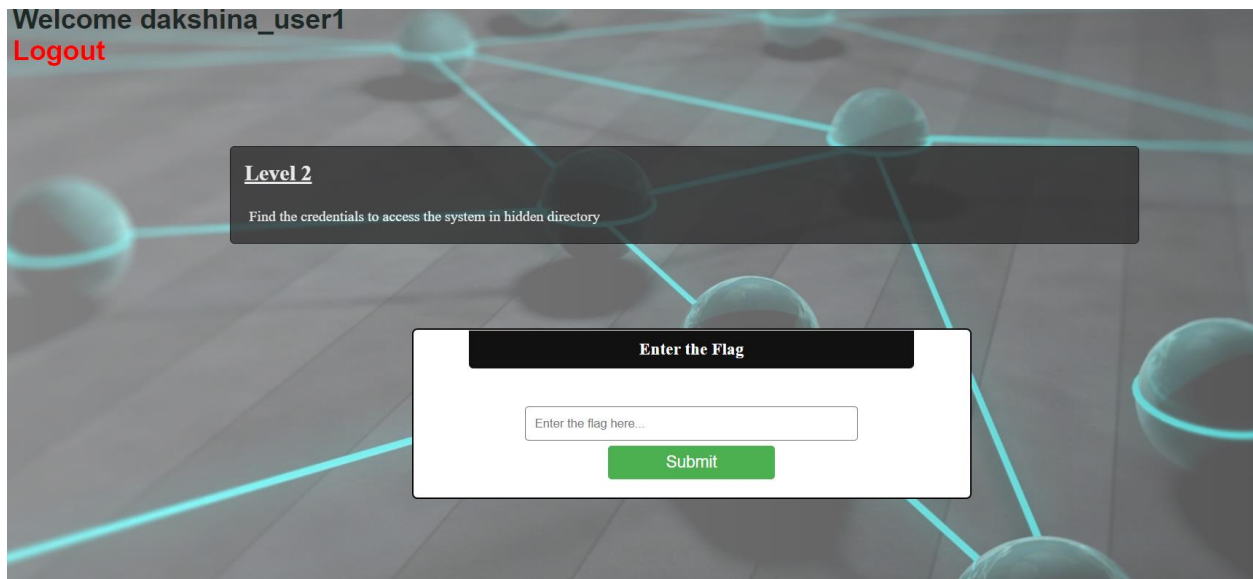
start: 0 time: 2ms
end: 301 length: 301
length: 301 lines: 1

D';*#n]lkzMD6BRR?Oaqoo8I[6F432U#cb?ON)9xq7on4lkjoh.fhdchgfed]#[C_X\][ZYXW90TMq430Hl/EDIBff?'C<#"8\6;4xy70T4-,10)Mnm%\$#(1~)C#cy?][u]s9qvon4UTjijh.leMihg'&d]bazYz}\[ZYRv9UMSRko2HGfjJIHG@?c= [ZYRv9UMSRko2HGfjJIHG@?c= <A:~!~6;432V6v.32+*N('8%#G|&)\$#z@a}vuzs9wvXws12pihgf,jihgle^]#aC_~Wz=VXQPUTMLpJOHl/EJiHae?'C< @9l=<SY3276/.R?



Flag is : **oneCTF{af76f16743a63d09870b95bed91867fb}**

Level 02



In this level user need to find the hidden directory to get the flag. User can use directory brute force tools like gobuster, dirbuster, ffuf. For this demonstration we gonna use ffuf tool.


```
(root@kali)~  
# ffuf -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt:FUZZ -u https://theblacklistctf.000webhostapp.com//FUZZ  
  
v1.3.1 Kali Exclusive <3  
  
:: Method : GET  
:: URL : https://theblacklistctf.000webhostapp.com//FUZZ  
:: Wordlist : FUZZ: /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt  
:: Follow redirects : false  
:: Calibration : false  
:: Timeout : 10  
:: Threads : 40  
:: Matcher : Response status: 200,204,301,302,307,401,403,405  
  
[Status: 403, Size: 20474, Words: 5432, Lines: 661]  
serial [Status: 403, Size: 20474, Words: 5432, Lines: 661]  
logo [Status: 403, Size: 20474, Words: 5432, Lines: 661]  
privacy [Status: 403, Size: 20474, Words: 5432, Lines: 661]  
about [Status: 403, Size: 20474, Words: 5432, Lines: 661]  
# directory-list-lowercase-2.3-medium.txt [Status: 403, Size: 20474, Words: 5432, Lines: 661]  
blog [Status: 403, Size: 20474, Words: 5432, Lines: 661]  
news [Status: 403, Size: 20474, Words: 5432, Lines: 661]
```

```
# directory-list-lowercase-2.3-medium.txt [Status: 200, Size: 14670, Words: 1674, Lines: 102]  
[Status: 200, Size: 14670, Words: 1674, Lines: 102]  
# [Status: 200, Size: 14670, Words: 1674, Lines: 102]  
# Copyright 2007 James Fisher [Status: 200, Size: 14670, Words: 1674, Lines: 102]  
assets [Status: 301, Size: 5645, Words: 280, Lines: 8]  
css [Status: 301, Size: 5642, Words: 280, Lines: 8]  
test [Status: 301, Size: 5643, Words: 280, Lines: 8]  
lib [Status: 301, Size: 5642, Words: 280, Lines: 8]  
js [Status: 301, Size: 5641, Words: 280, Lines: 8]  
com [Status: 301, Size: 5642, Words: 280, Lines: 8]  
vendor [Status: 301, Size: 5645, Words: 280, Lines: 8]  
sql [Status: 301, Size: 5642, Words: 280, Lines: 8]  
fonts [Status: 301, Size: 5644, Words: 280, Lines: 8]  
secret [Status: 301, Size: 5645, Words: 280, Lines: 8]  
:: Progress: [5450/207643] :: Job [1/1] :: 129 req/sec :: Duration: [0:00:46] :: Errors:  
zsh: suspended ffuf -w -u https://theblacklistctf.000webhostapp.com//FUZZ
```

Find the directory called /Secret/. Inside the directory there is a few text files available.

Name	Last modified	Size	Description
Parent Directory	-	-	-
AngelaMoss.txt	2022-06-05 07:33	2.5K	
DarleneAlderson.txt	2022-06-05 07:33	1.7K	
ElliotAlderson.txt	2022-06-05 07:33	1.5K	
GideonGoddard.txt	2022-06-05 07:33	955	
ShaylaNico.txt	2022-06-05 11:14	4.6K	
TyrellWellick.txt.txt	2022-06-05 07:33	2.5K	

Go with each file, and there is a one file that keeping binary code,

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

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

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

Shaw's 2014 short film SMILF, which she wrote, directed and starred in opposite Thomas Middleditch, won the 2015 Short Film Jury Award for U.S. Fiction at Sundance.[19][20] In 2015, SMILF was picked up by Showtime as a half-hour comedy television show with Shaw as showrunner, writing, directing, starring in, and producing the series.[21] The first season, which was shot on location in South Boston as well as Los Angeles, received generally positive reviews, [22][23] with her portrayal of single mother Bridgette Bird notable for its realism, insight, and biting humor.[24][25] "Frankie Shaw, it [SMILF] marks the arrival of an important and original voice." [26] SMILF co-stars Connie Britton and Rosie O'Donnell, [27][8][28] and tackles subjects like eating disorders and sexual abuse. [29] Shaw said that the show was a way to discuss and portray the role of women on screen. [30] In November 2017, Showtime renewed SMILF for a second season. [31] In December 2018, it was reported that Shaw and the series had been accused of workplace misconduct. [32] In March 2019, the series was cancelled after two seasons. [33]

Binary - 01101111 01101110 01100101 01000011 01010100 01000110 01111011 01010000 01101100 01100101 01100001 01110011 01100101 01001110 01101111 01110100 01100101 01110100 01101000 01100001 01110100 01010100 01101000 01101001 01110011 01001001 01110011 01000010 01101100 01100001 01100011 01101011 01001100 01101001 01110011 01110100 01111101

In 2016, Shaw returned to the Sundance Film Festival with another short film she wrote and directed, a dark comedy titled Too Legit, which stars Zoë Kravitz, Teresa Palmer, Nate Corddry and Clark Gregg.[5] Too Legit is inspired by a satire of Congressman Todd Akin's controversial 2012 remarks about rape and pregnancy:[34] "It seems to be, first of all, from what I understand from doctors, [rape resulting in pregnancy is] really rare. If it's a legitimate rape, the female body has ways to try to shut the whole thing down." [35]

Inside the ShaylaNico.txt have a binary code. Use any binary decoder to decode the flag and later on submit in the submission form

push the convert button. You can convert up to 1024 binary characters to ascii text. Decode *binary* to *ascii* text readable format.

Facebook

Twitter

Binary Value

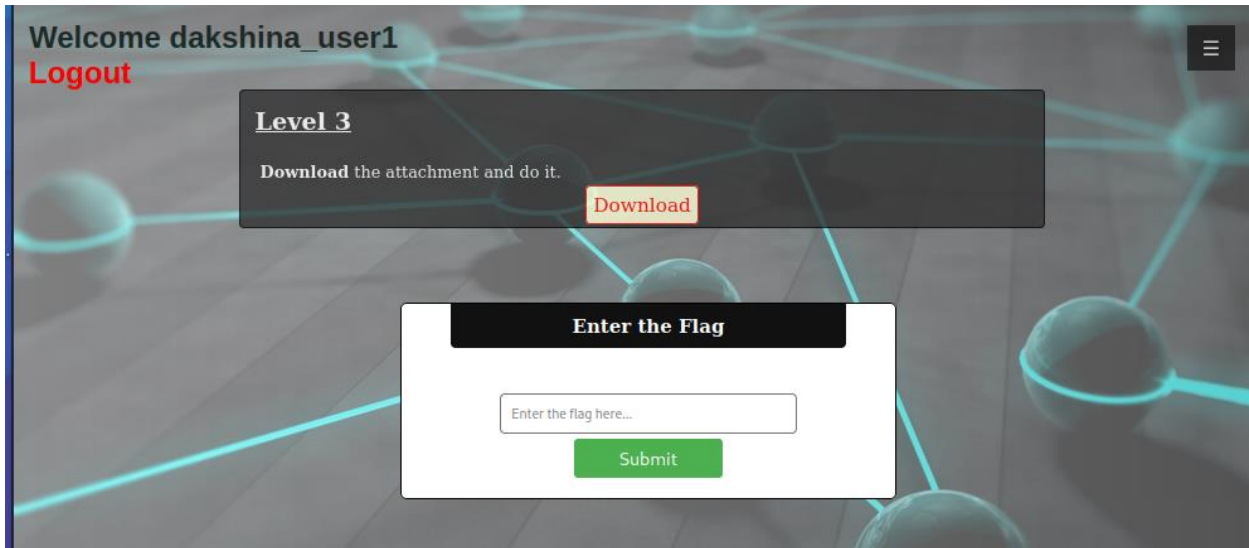
Ascii Text Value

```
01101111011011100110010101000011010101000
10001100111101101010000011011000110010101
10000101110011011001010100111001101111011
10100011001010111010001101000011000010111
01000101010001101000011010010111001101001
```

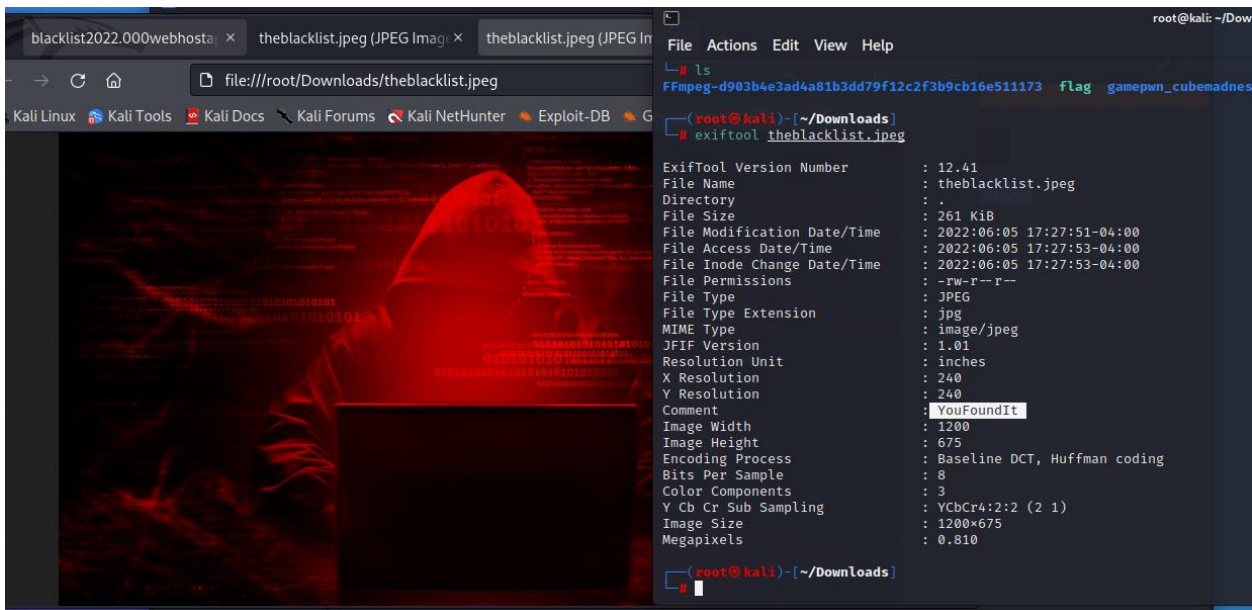
```
oneCTF{PleaseNotethatThisIsBlackList}
```

Flag is : **oneCTF{PleaseNotethatThisIsBlackList}**

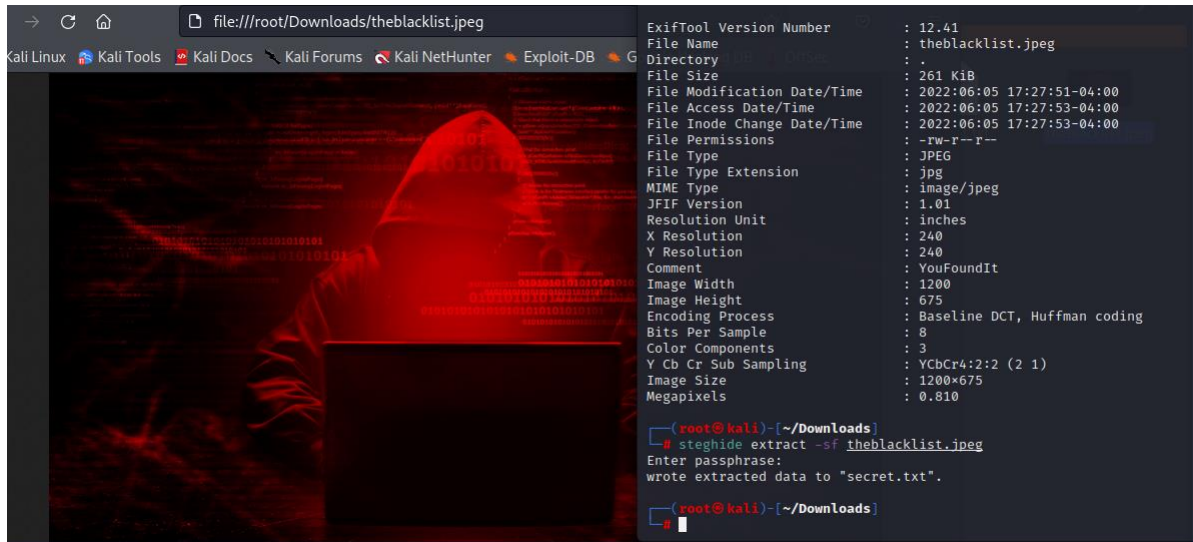
Level 03



This is a steganography challenge. After downloading the Image file to a Linux environment. Scan the image for file type. The hints suggest of the METADATA, because of that we need a tool to see METADATA of the image. After enough research and the hint suggests Exiftool. Download and install the tool with the command: “sudo apt-get install exiftool”. After installing check, the image with the tool: “exiftool thegambit.jpg”. It shows a Comment with a passphrase. Next the hint points us of a tool to extract data hidden in the image



Install: “sudo apt-get install steghide”. Run the command: “steghide extract -sf thegambit.jpg”. Next the passphrase will be required, enter it. New file “secret” without an extension is extracted out of the image. Open it to find the FLAG:

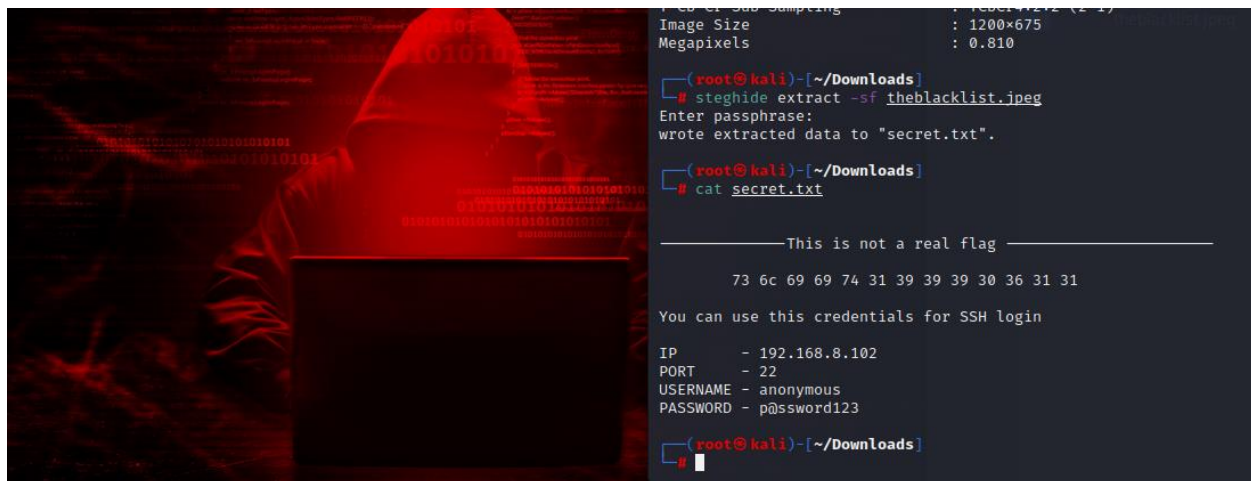


The screenshot shows a Kali Linux terminal window. On the left, there is a preview of a red-tinted image featuring a hooded figure and binary code. The terminal output on the right shows the execution of the 'steghide extract' command on 'thelacklist.jpeg'. It prompts for a passphrase, which is entered as 'wrote extracted data to "secret.txt"'. Below this, the command 'cat secret.txt' is entered, leading to the next screenshot.

```
ExifTool Version Number : 12.41
File Name                : thelacklist.jpeg
Directory                : .
File Size                : 261 KiB
File Modification Date/Time : 2022:06:05 17:27:51-04:00
File Access Date/Time    : 2022:06:05 17:27:53-04:00
File Inode Change Date/Time : 2022:06:05 17:27:53-04:00
File Permissions         : -rw-r--r--
File Type                : JPEG
File Type Extension      : jpg
MIME Type                : image/jpeg
JFIF Version             : 1.01
Resolution Unit          : inches
X Resolution              : 240
Y Resolution              : 240
Comment                  : YouFoundIt
Image Width              : 1200
Image Height              : 675
Encoding Process          : Baseline DCT, Huffman coding
Bits Per Sample           : 8
Color Components          : 3
Y Cb Cr Sub Sampling     : YCbCr4:2:2 (2 1)
Image Size                : 1200x675
Megapixels                : 0.810

(root@kali) ~/Downloads
# steghide extract -sf thelacklist.jpeg
Enter passphrase:
wrote extracted data to "secret.txt".

(root@kali) ~/Downloads
#
```



This screenshot continues the terminal session. It shows the output of the 'cat secret.txt' command, which displays an encoded flag and SSH login information. The flag is '73 6c 69 69 74 31 39 39 39 30 36 31 31'. Below it, a message states 'You can use this credentials for SSH login' followed by the IP, port, username, and password.

```

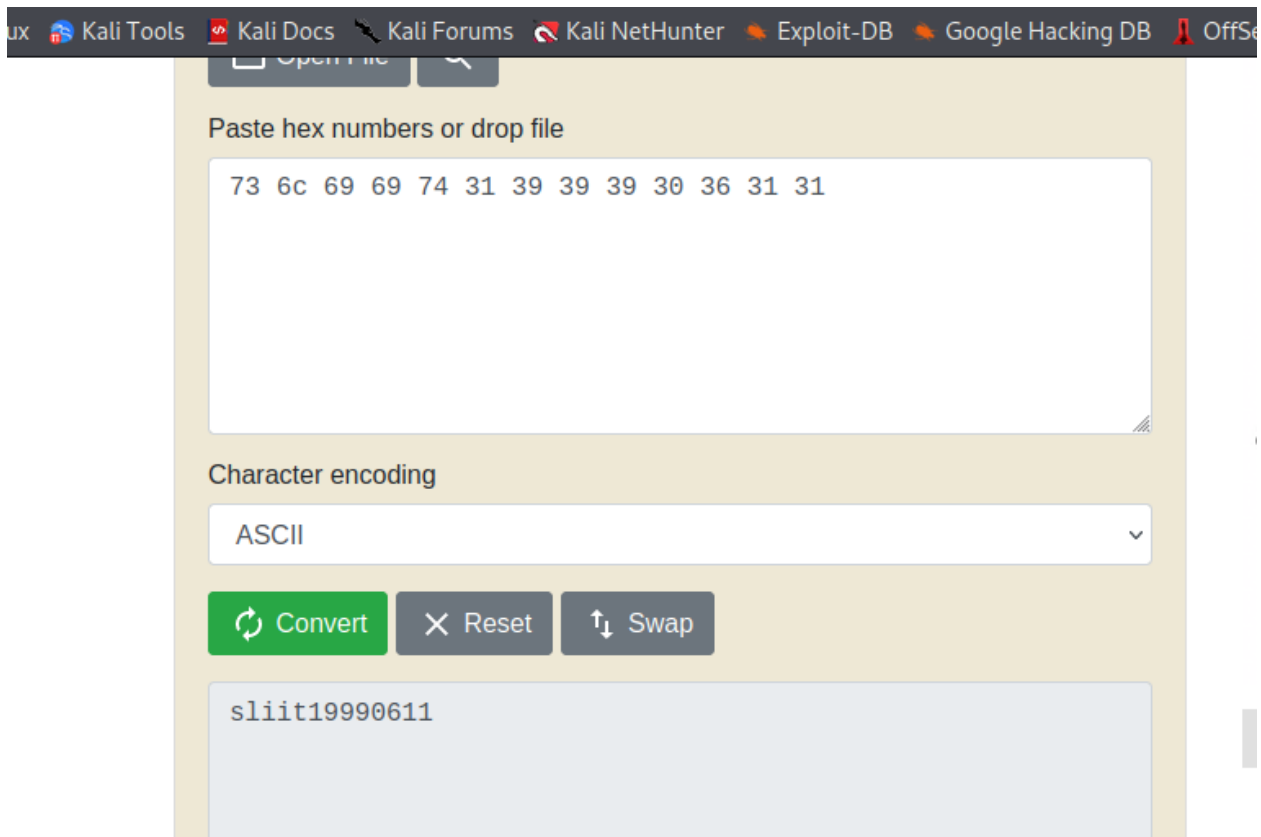
-----This is not a real flag -----
73 6c 69 69 74 31 39 39 39 30 36 31 31

You can use this credentials for SSH login

IP      - 192.168.8.102
PORT    - 22
USERNAME - anonymous
PASSWORD - p@ssword123

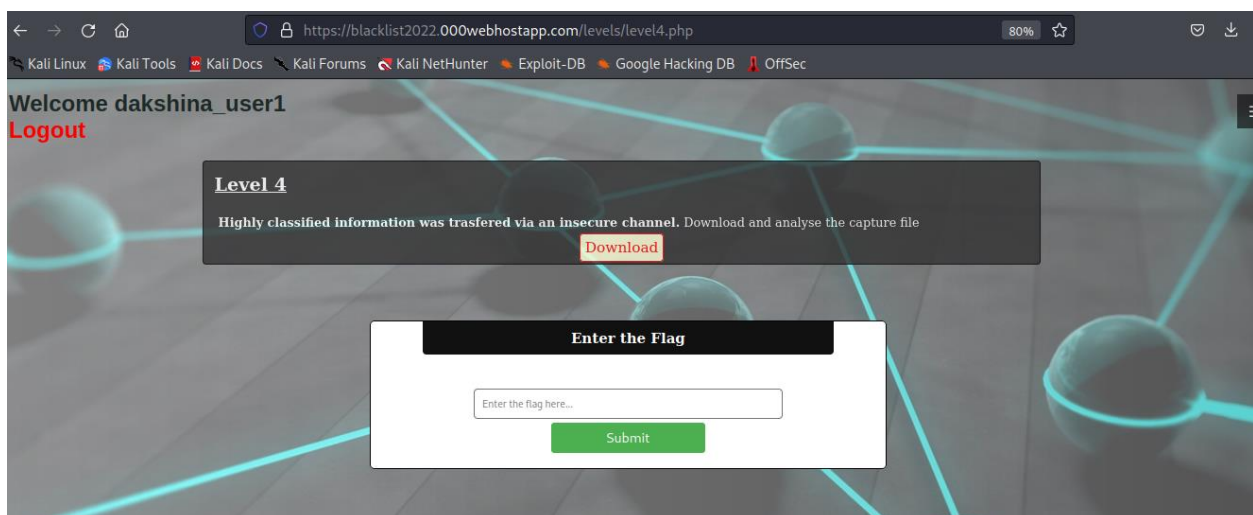
(root@kali) ~/Downloads
#
```

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



Flag is : **sliit19990611**

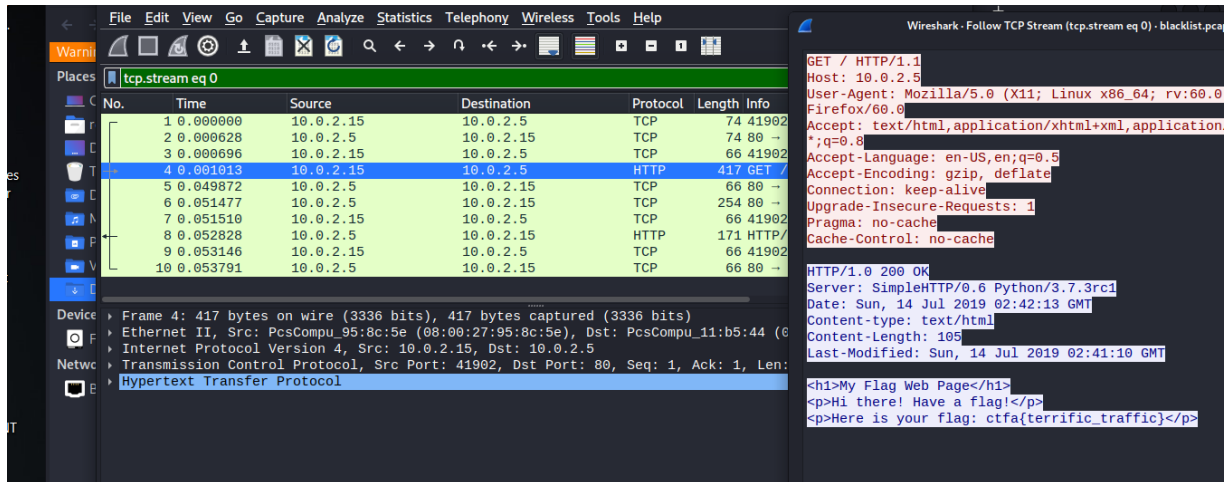
Level 04



This is a forensics challenge. User need to download the pcap file open it from Wireshark.

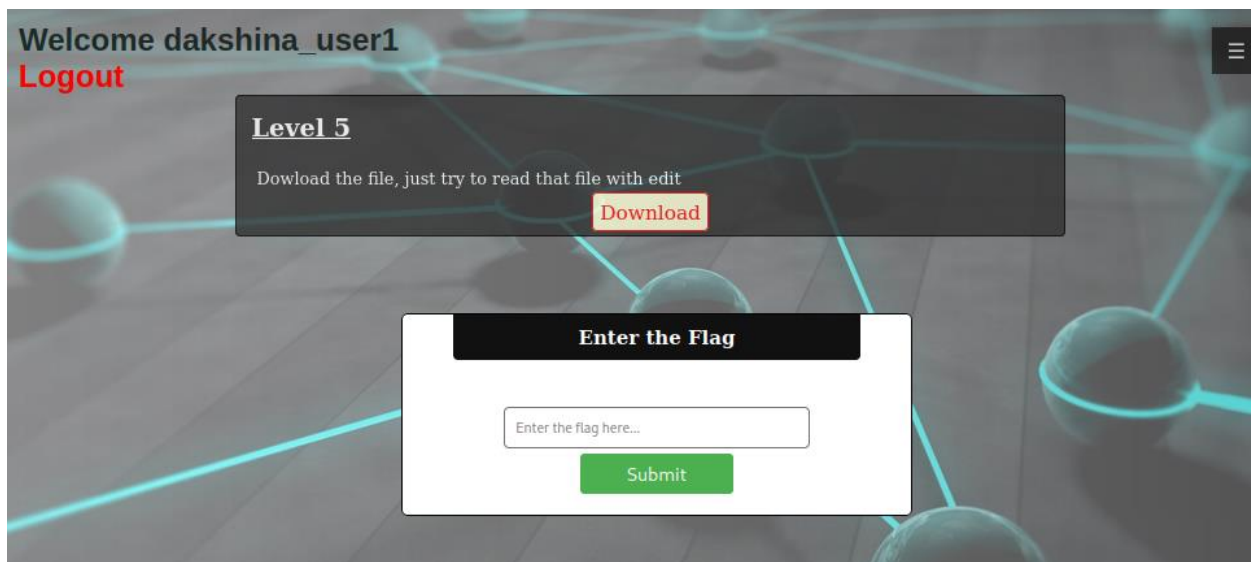
Then click on a packet and right click->follow tcp stream

Then click on a packet and right click->follow tcp stream

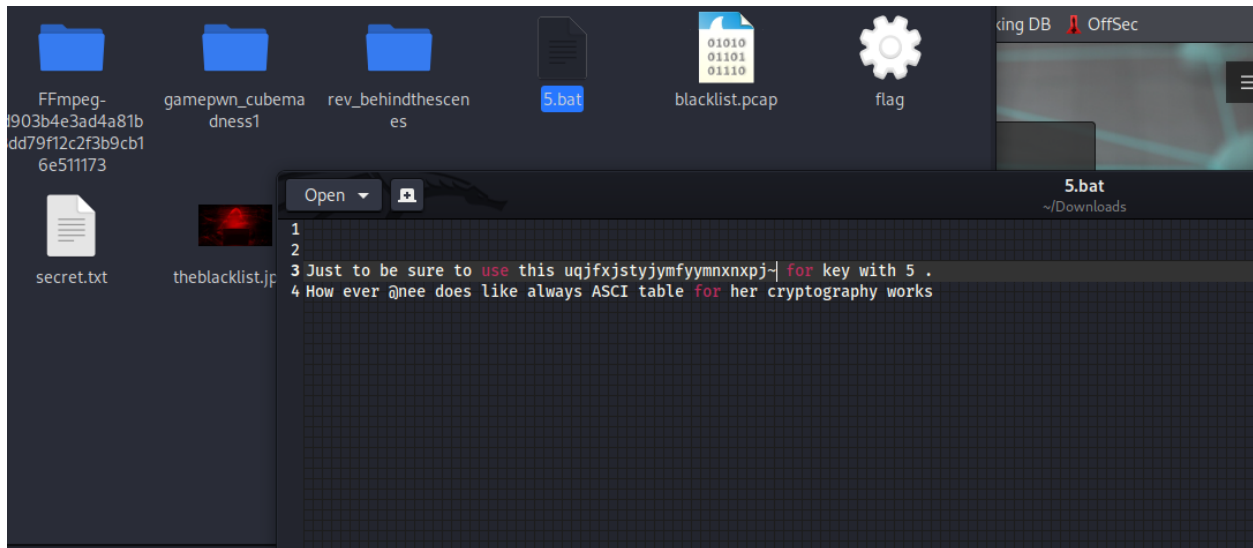


Flag is : `ctfa{terrific_traffic}`

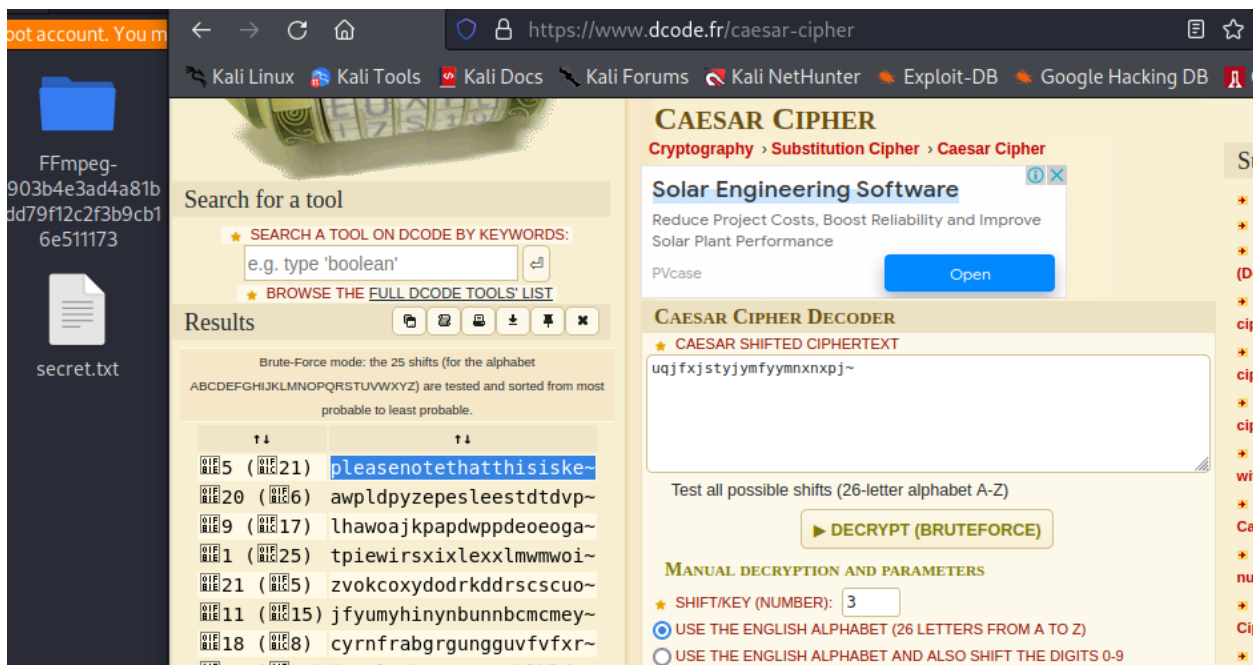
Level 05



This is the implementation of cease cipher,

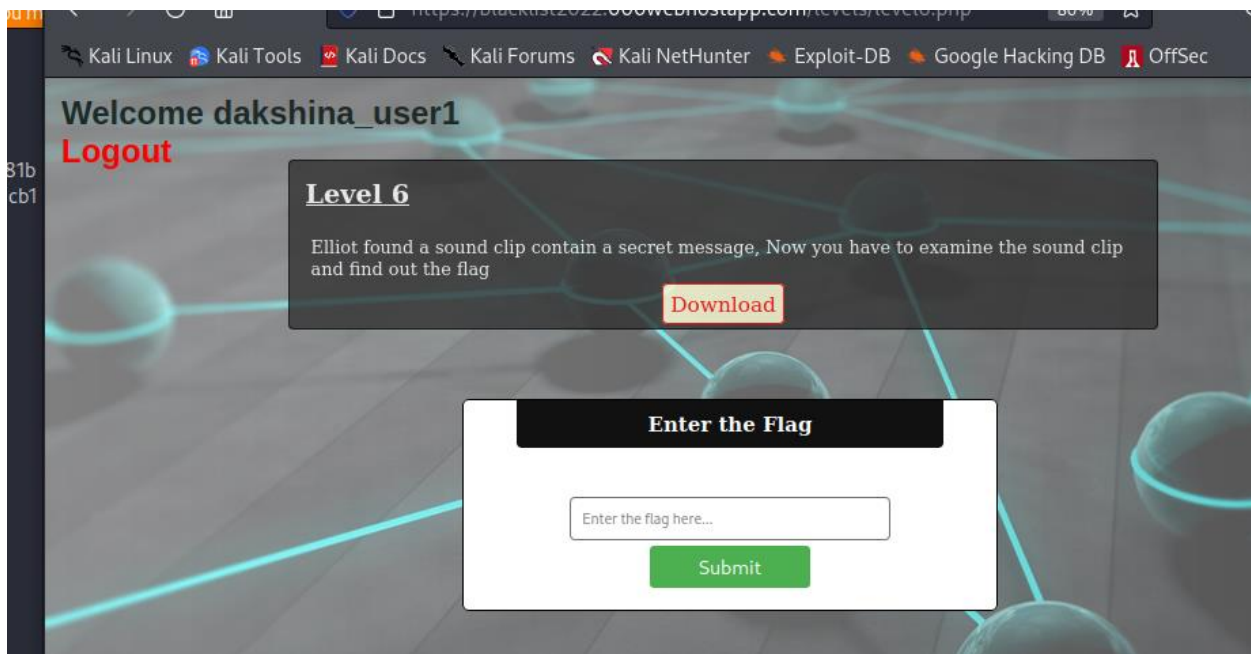


With the given scenario, encrypted message must decrypt with 5 keys in cease cipher with ASCII Table,



Flag is: **pleasenotethatthisiskey**

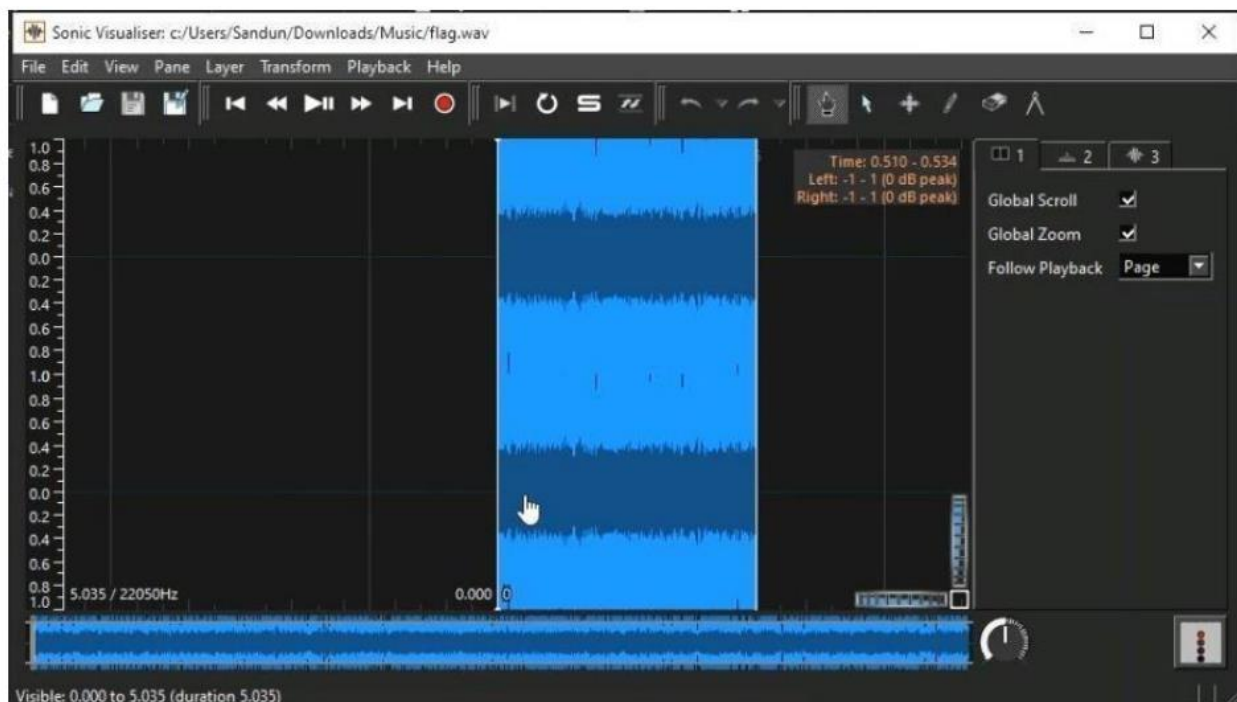
Level 06



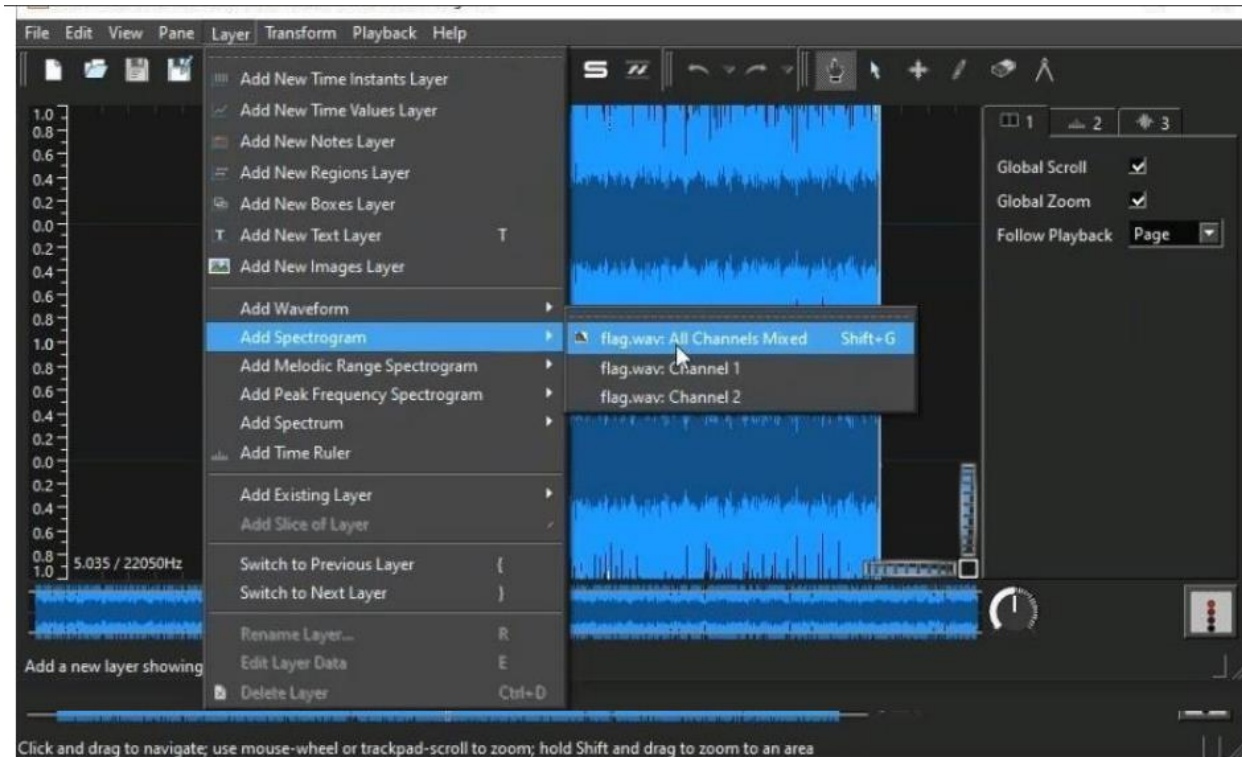
First download the sound clip.

Then we want a Sonic Visualiser software.

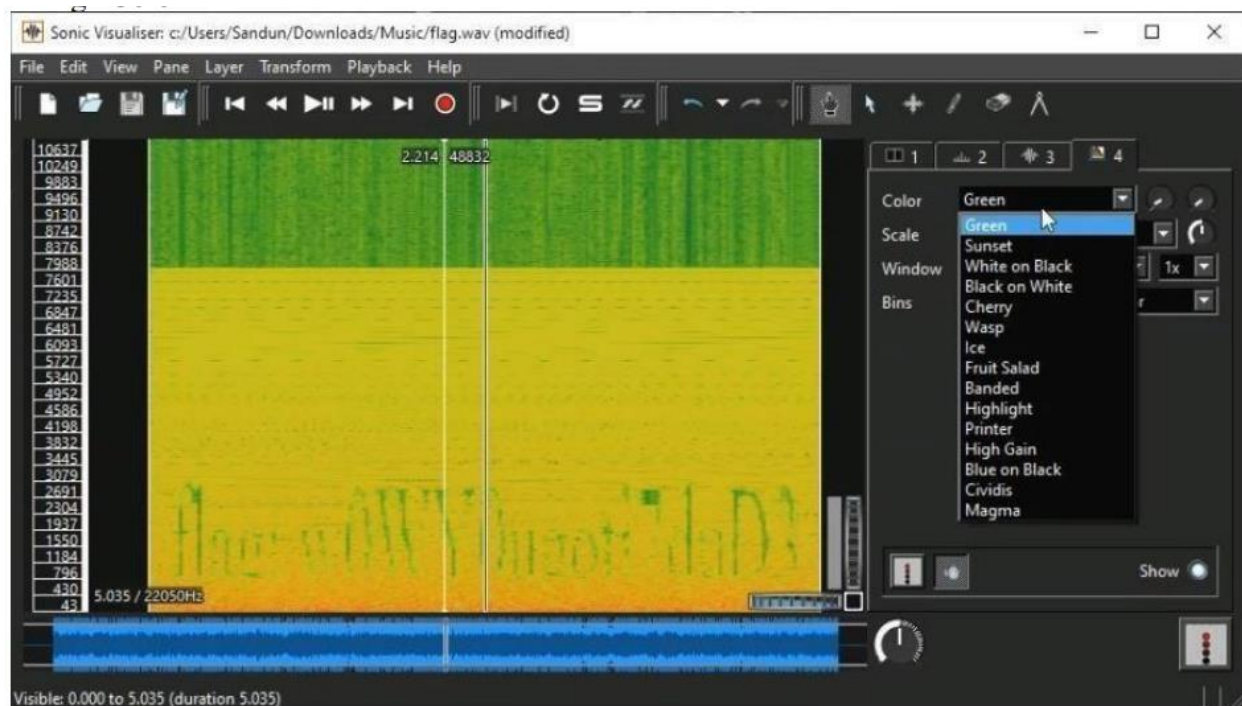
Then open the sound clip on Sonic Visualiser.



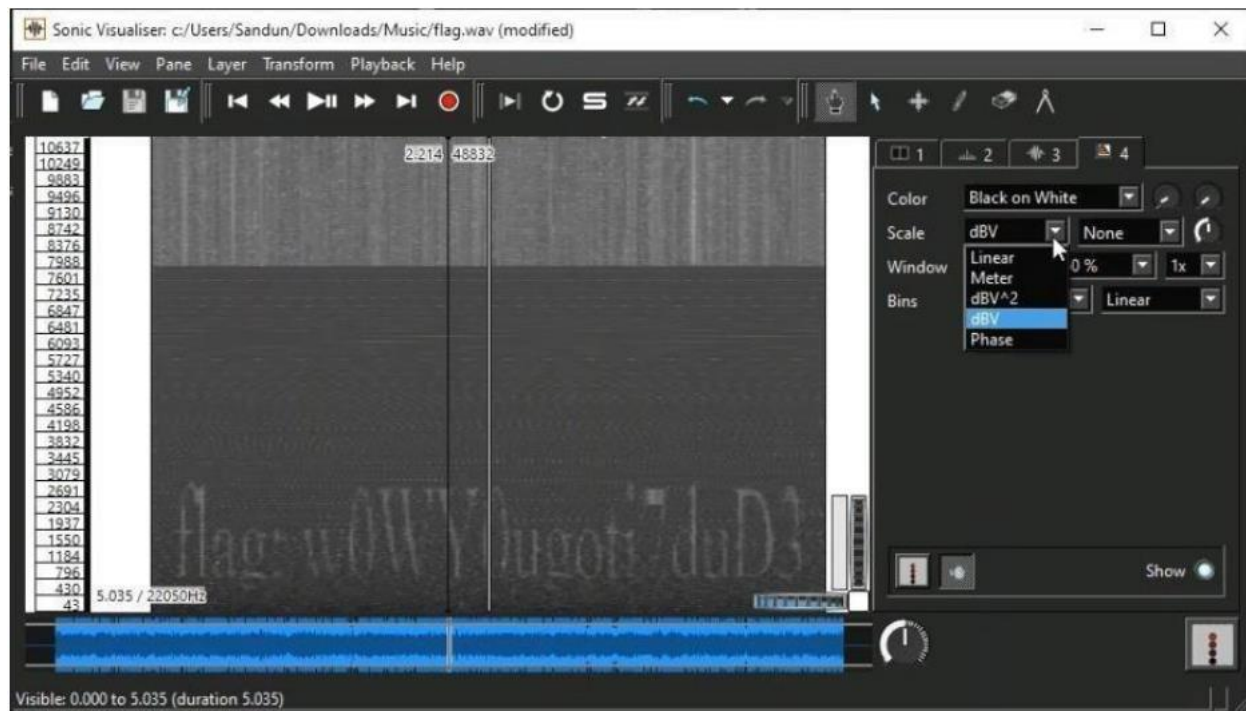
Then go to Layer > Add Spectrogram > flag.wav: All Channels Mixed and add that. Then we want to change Color, Scale, Window and Bins to get clear Image in Spectrogram layer. Then we can saw the flag in that.



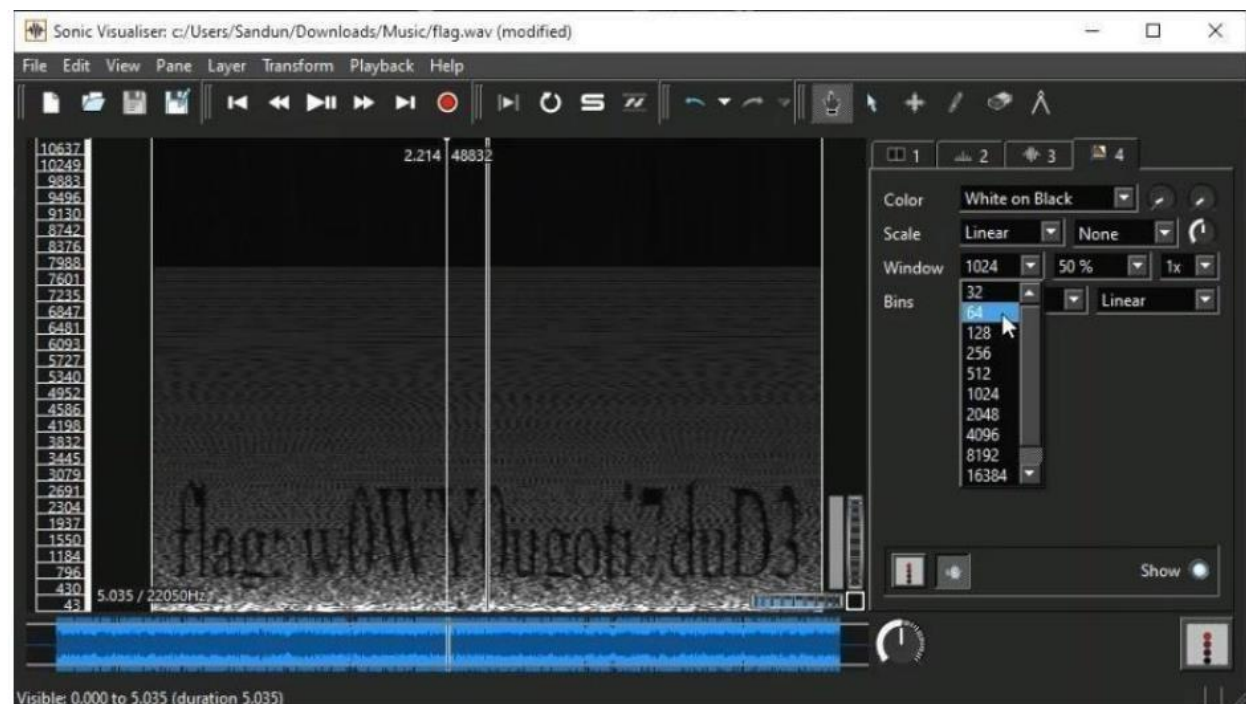
Change Color to black and white



Change Scale to linear



Change Window to 512

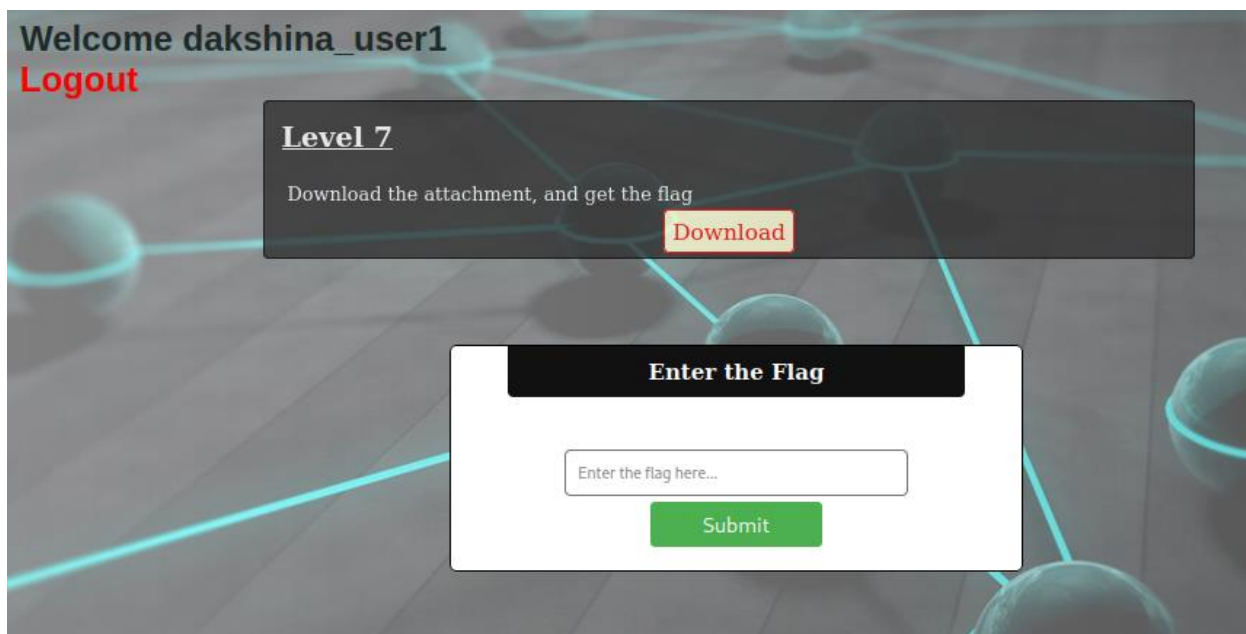


Change Bins



Flag can be seen as above : **woWYOugoti7duD3**

Level 07



First, I download the attachment on my Linux machine -> Using wget 'path' command. and then I unzip the .zip file. -> Using unzip flag.zip Then I get the details about flag file (to know about what kind of file). Using -> file flagfile flag

That flag file is executable file. but file can't execute because of their wasn't permission. So I use command as -> `chmod +x flag` Then I execute the flag file using -> `./flag` command.

```
MrR 5.bat FFmpeg-d903b4e3ad4a81b3dd79f12c2f3b9cb16e511173 gamepwn_cubemadness1 secret.txt
blacklist.pcap flag theblacklist.jpeg UPEG Image Caesar Cipher (Shift) - C

(root@kali)~/Downloads
# unzip flag
Archive: flag
replace flag? [y]es, [n]o, [A]ll, [N]one, [r]ename: y
inflating: flag

(root@kali)~/Downloads
# ls
5.bat FFmpeg-d903b4e3ad4a81b3dd79f12c2f3b9cb16e511173 gamepwn_cubemadness1 secret.txt
blacklist.pcap flag theblacklist.jpeg

(root@kali)~/Downloads
# chmod +x flag

(root@kali)~/Downloads
# file flag
flag: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Linux 3.2.0, BuildID[sha1]=2fb84c55912cd8657e1d45140dfcaba1a96cc00f, not stripped

(root@kali)~/Downloads
# ./flag
Enter the Flag

Mr. Robot CTF!
Enter the passphrase:
```

That ask Passphrase, But I do not know the passphrase. I tried random password as flag their was a message Invalid key

Then I use strings `./flag` command to determine the contents of and to extract text from binary files.

```
File Actions Edit View Help
(root@kali)~/Downloads
# strings ./flag
/lib64/ld-linux-x86-64.so.2
libc.so.6
__isoc99_scanf
puts
__stack_chk_fail
printf
__cxa_finalize
strcmp
__libc_start_main
GLIBC_2.7
GLIBC_2.4
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
AWAVI
AUATL
[]A\A]A^A_
Mr. Robot CTF!
Enter the passphrase:
Invalid key, Try again...
|||||
|| N0oneC4nD0th!sp4n ||
|| B3N1cet00thersdr3nkjsq ||
|| N00n3cand0itaB13 ||
|| d0B3strLe79N24J@p4n ||
|| H0p3yoU9N24J@p4n ||
```

There are so many strings I cannot all of those as passphrase key. Then I use `ltrace ./flag` command to find passphrase. After using `ltrace` command that ask Passphrase I do not know the Passphrase.

Then I Enter asde for passphrase, but you can use any value as passphrase. That compare Entered value and matched passphrase under strcmp. ltrace is a program that simply runs the specified command until it exits. It intercepts and records the dynamic library calls which are called by the executed process and the signals which are received by that process. It can also intercept and print the system calls executed by the program. The strcmp() function compares the two strings s1 and s2. It returns an integer less than, equal to, or greater than zero if s1 is found, respectively, to be less than, to match, or be greater than s2.

```

i Lin .dynamic
.data
.bss
.comment
cc (root@kali)-[~/Downloads]
# ltrace ./flag
puts("\nMr. Robot CTF!\n")
Mr. Robot CTF!

)
printf("Enter the passphrase:")
_isoc99_scanf(0x5566b400dfff, 0x7ffcd791dc0, 0, 0Enter the passphrase:asde
)
strcmp("asde", "ispCTF3rd2ndmrRobot")
puts("\nInvalid key, Try again... \n")
Invalid key, Try again...

)
+++ exited (status 0) +++

(root@kali)-[~/Downloads]
#

```

That selected value is the Passphrase of the flag file. Then I enter that value for passphrase in flag file.

```

li Lin )
printf("Enter the passphrase:")
_isoc99_scanf(0x5566b400dfff, 0x7ffcd791dc0, 0, 0Enter the passphrase:asde
)
strcmp("asde", "ispCTF3rd2ndmrRobot")
puts("\nInvalid key, Try again... \n")
Invalid key, Try again...

)
Level 7
+++ exited (status 0) +++

(root@kali)-[~/Downloads]
# ./flag

Mr. Robot CTF!

Enter the passphrase:ispCTF3rd2ndmrRobot
|||||
|| Y0u4r3!n3vitaBl3 ||
|||||

(root@kali)-[~/Downloads]
#

```

