

# **DOCUMENTATION**

# Terms of Reference

A report on creating a tryhackme CTF base room for fulfillment of the requirements for the module IE2012: System and Network Programming, Sri Lanka Institute of Information Technology

# Table of Contents

1. Introduction .....	4
2. Implementation.....	4
3. First part of the room .....	4
4. connection establishment .....	8
5. Second part of the room.....	11
6. First task.....	11
7. Second task.....	15
8. Third task .....	17

# Introduction

In this project, I used the ubuntu server 18.04 version as the base. And Kali Linux virtual machine to connect with the server. The full project was based on CTF and exploding web vulnerability. The host and the user have two flags plays can capture that using basic Linux command. I use apache2 and MySQL for the Webhosting

To complete the challenged player needs to have a basic idea about how apache2 and MySQL work. Also, in the second part of the challenge user need to do some cryptography and steganography challenges using the steghide tool. All so user need burp suite and encoding and decoding tools for the last two challenge

We provide a password and username for the guest user (robin) using this player can use the ssh command to connect with the server and gain access. the player can use port 80 to get access to the website, and database and find the root password

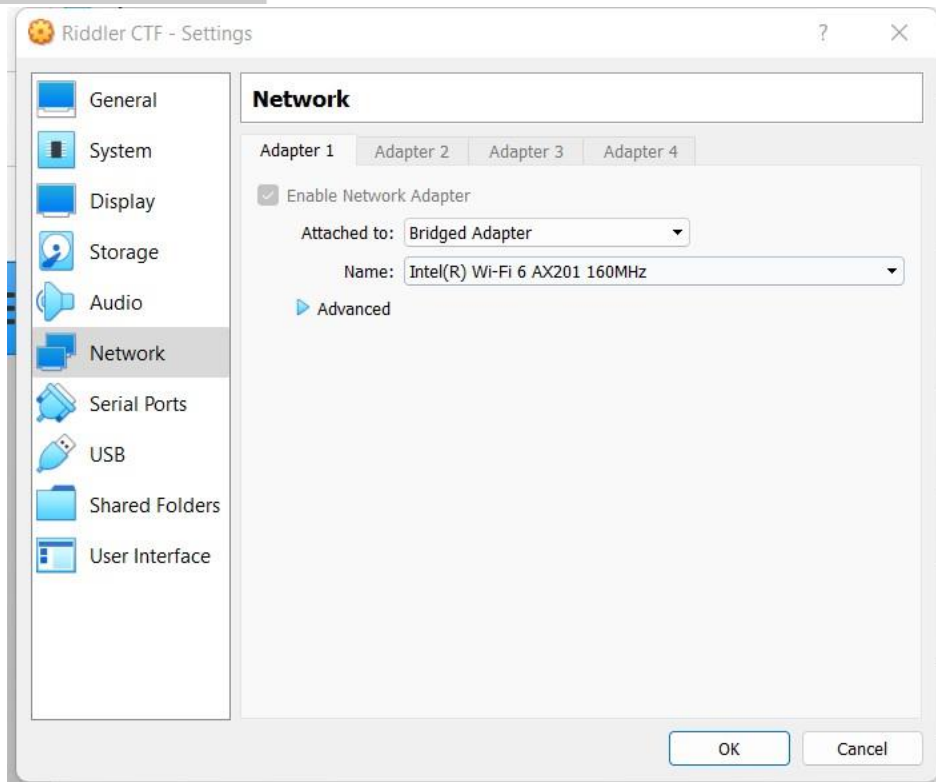
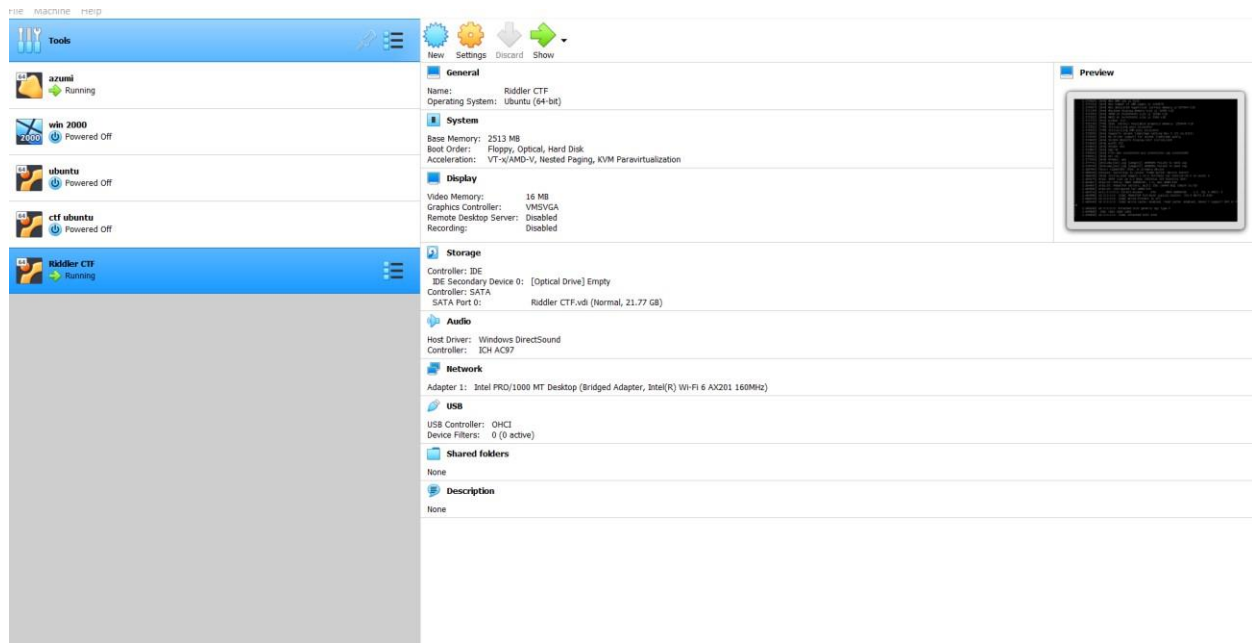
Drive LINK : [SNP Assignment](#)

[https://mysliit-my.sharepoint.com/:f:/g/personal/it21262272\\_my\\_sliit\\_lk/EgXbSD35FRtHqFpZRvQ3fv0B3hRqahJGOvEG10IAqT3mwQ?e=ZhMI5f](https://mysliit-my.sharepoint.com/:f:/g/personal/it21262272_my_sliit_lk/EgXbSD35FRtHqFpZRvQ3fv0B3hRqahJGOvEG10IAqT3mwQ?e=ZhMI5f)

# Implementation

## Installation

Use ubuntu saver 18.04 ( tryhackme only allows ubuntu savers less than 20.2). using oracle vmbox we can run it on a windows host. need to change the network adaptor of both kali Linux and ubuntu saver to bridge the network adaptor



Install LAMP stack on Ubuntu 18.04

A “LAMP” stack is a group of open-source software that is typically installed together to enable a server to host dynamic websites and web apps. This term is actually an acronym which represents the Linux operating system, with the Apache web server. The site data is stored in a MySQL database, and dynamic content is processed by PHP.

### 1) Installing Apache and Updating the Firewall

```
$ sudo apt install apache2
```

```
$ sudo ufw app list
```

```
$ sudo ufw allow "Apache Full"
```

### 2) Installing PHP

```
$ sudo apt install php libapache2-mod-php php-mysql
```

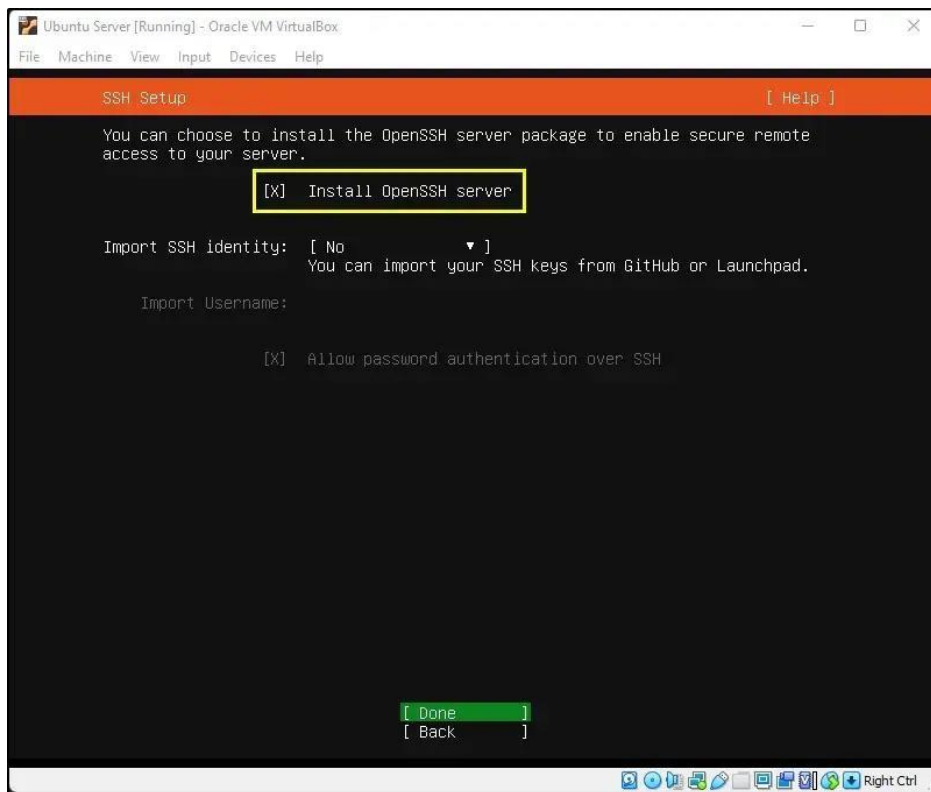
### 3) Installing MySQL

```
$ sudo apt install mysql-server
```

```
$ sudo mysql_secure_installation
```

### 4) Setting Up a Virtual Host

Install OpenSSH Server



## First part of the room

### Connection between kali Linux machine and the Ubuntu server

First, we need to create a connection between our kali Linux box and ubuntu server for this we can use

**SSH connection** between two machines

- 1) Ip configuration – **ifconfig**

```
Riddler CTF [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Usage of /: 22.9% of 19.52GB Users logged in: 0
Memory usage: 12% IP address for enp0s3: 192.168.1.23
Swap usage: 0%

* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

25 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

New release '20.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

root@riddler:~# ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.23 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 2402:d000:8118:c78e:a00:27ff:feff:65ff prefixlen 64 scopeid 0x0<global>
    inet6 fe80::a00:27ff:feff:65ff prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:ff:65:ff txqueuelen 1000 (Ethernet)
    RX packets 6650 bytes 694041 (694.0 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 404 bytes 41377 (41.3 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 84 bytes 6368 (6.3 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 84 bytes 6368 (6.3 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@riddler:~# _
```

2) SSH connection – SSH [root@192.168.1.24](ssh://root@192.168.1.24)

Root password

```
(azumi@Azumi)-[~]
$ ssh root@192.168.1.23
root@192.168.1.23's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.15.0-200-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Tue Dec 6 15:17:20 UTC 2022

System load: 0.0 Processes: 98
Usage of /: 22.9% of 19.52GB Users logged in: 1
Memory usage: 13% IP address for enp0s3: 192.168.1.23
Swap usage: 0%

* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

25 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

New release '20.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Tue Dec 6 14:58:40 2022
root@riddler:~#
```

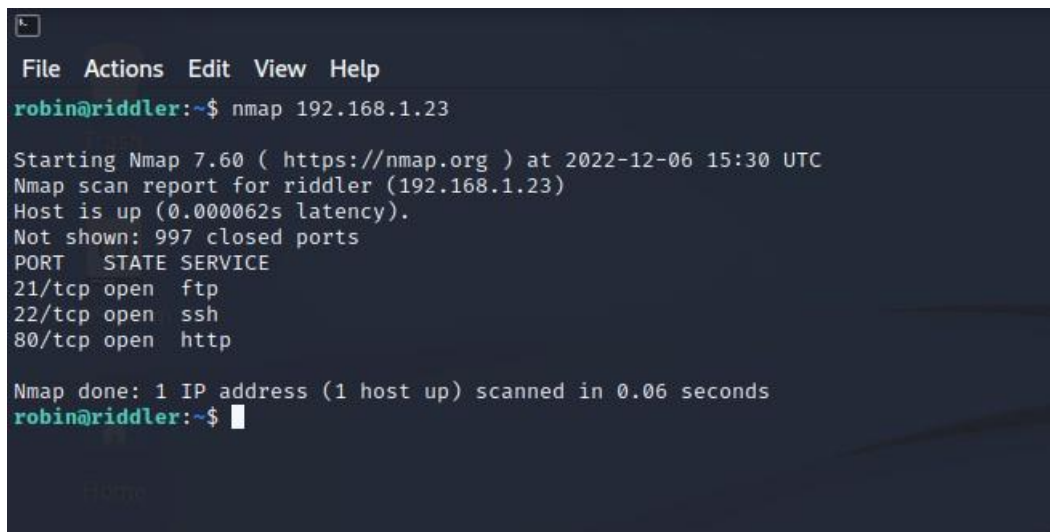


Now using the server IP we can access the files

The default port for SSH client connections is 22; to change this default, enter a port number between 1024 and 32,767.

## Nmap

Next, we can check what are the open ports on the server. For that we'll run a "nmap" scan



```
File Actions Edit View Help
robin@riddler:~$ nmap 192.168.1.23

Starting Nmap 7.60 ( https://nmap.org ) at 2022-12-06 15:30 UTC
Nmap scan report for riddler (192.168.1.23)
Host is up (0.000062s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
robin@riddler:~$
```

Now we can identify ports and protocols used by the ubuntu server

- 22-SSH
- 80-http

If port 80 is running HTTP means the website is running in port 80 and communication will be port 22

Now we can use the basic Linux command to find the user flag (robin)

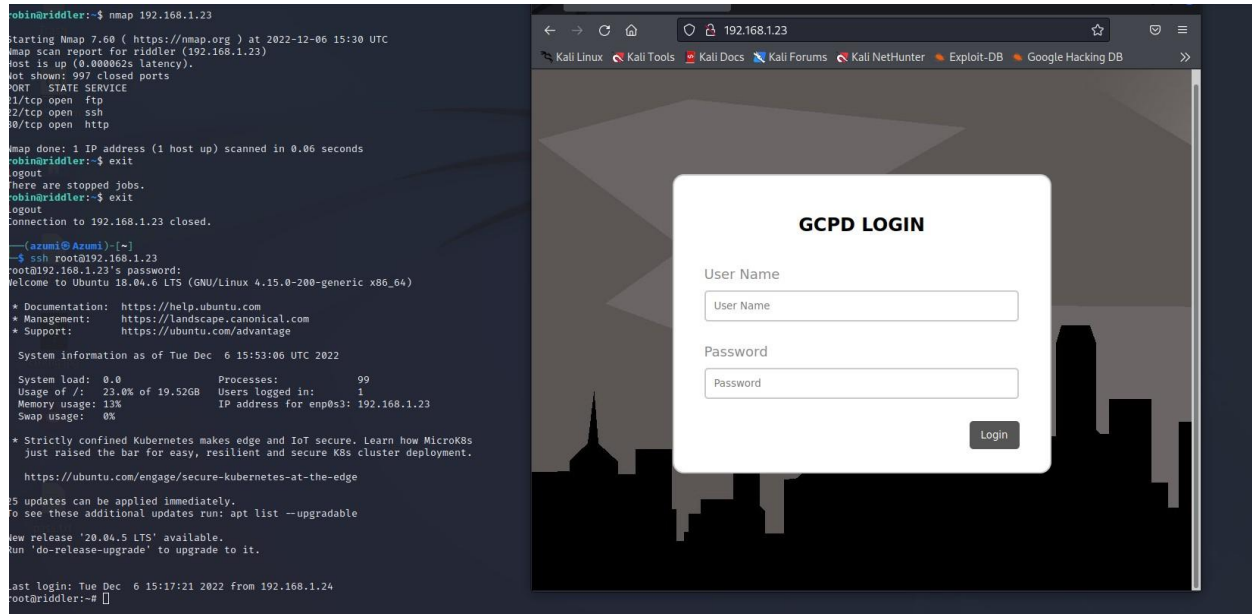
- 1) Using cat command, we can view the file
- 2) We can identify user flag as `'user_flag'`

## Second part of the room

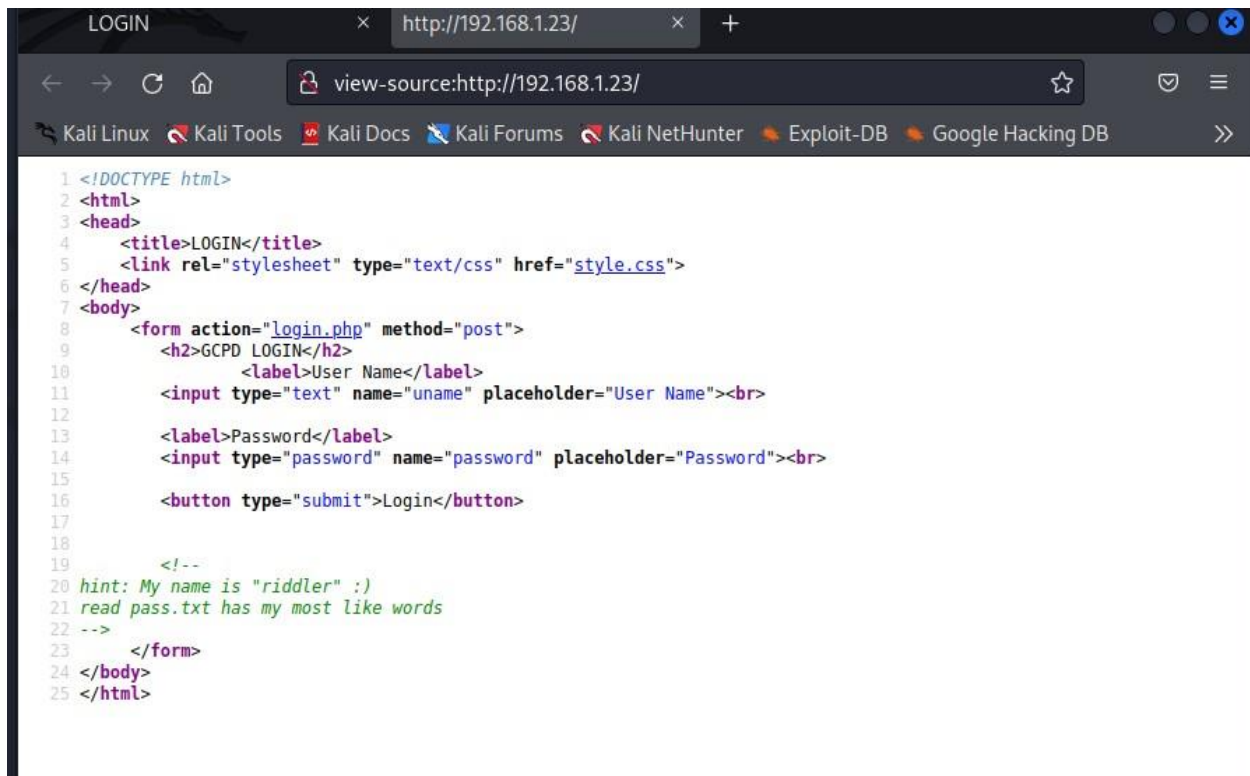
Exploding the web vulnerability

“var/www/riddler/Riddlerctf” This is the root dictionary for our web application. Players need to use that dictionary for any resources they need. user can access web applications using port 80

# First task



- 1) The user needs to find the password and username when the user goes to the source code of the web application it has some hints and flag

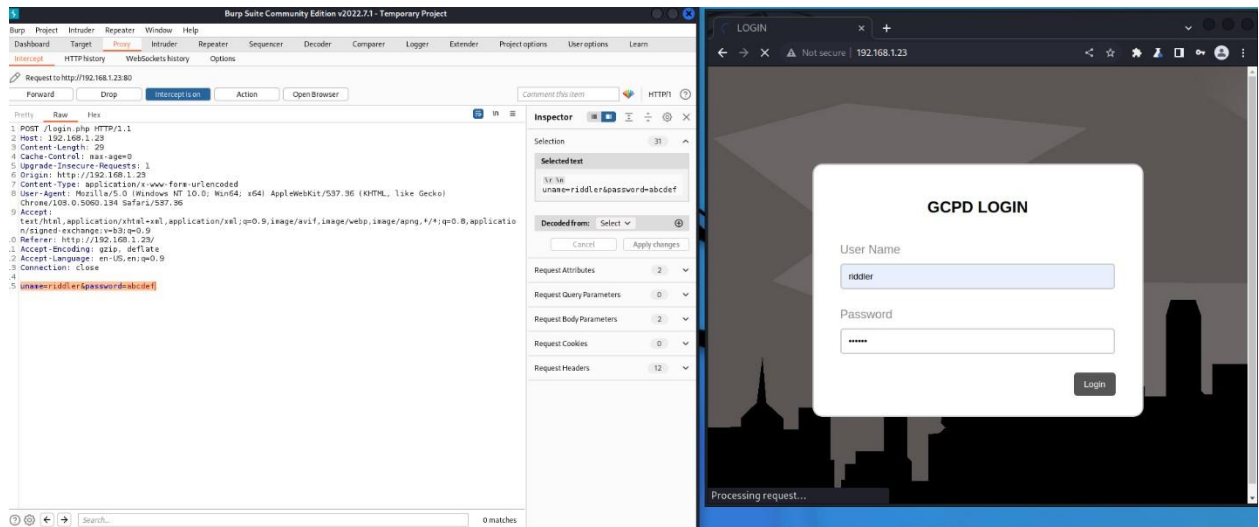


3) Username is Riddler (Given in hint as a riddle)

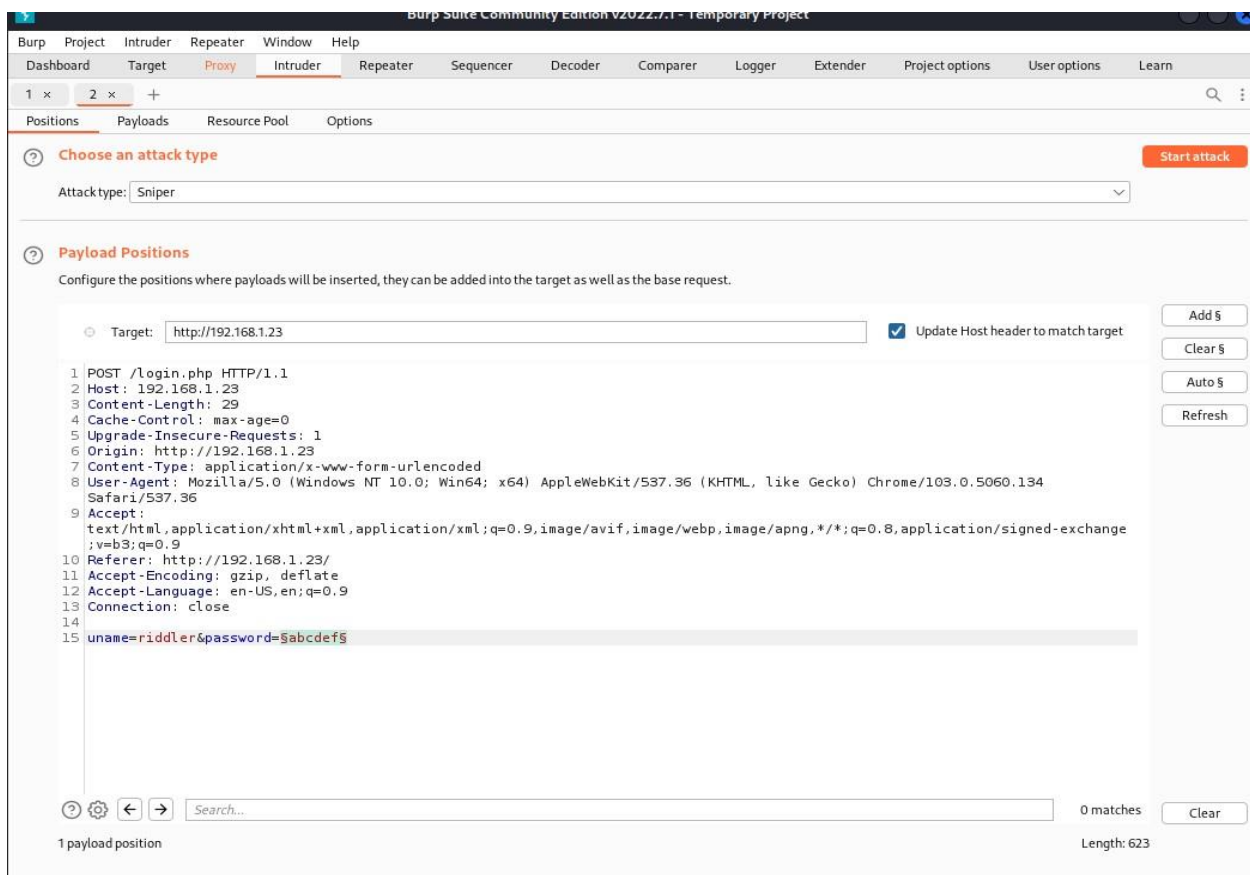
4) according to the hint, the user needs to download the pass.txt using this text file user can brute force attack the login page

```
1 Cyborg
2 Doctor Fate
3 Lex Luthor
4 Wonder Woman
5 Superman
6 batman
7 Black Canary
8 Selina Kyle
9 Darkseid
10 Alan Scott
11 Lucifer
```

5) player needs to use a burp suite to intercept the connection and gather details and then using pass.txt player can start attacking



6) Play can identify a given value for a password and using that value he can send it as an intruder



7) User can use pass.txt as played and start the attack

can be customized in different ways.

Payload set: 1

Payload count: 11

Payload type: Simple list

Request count: 11

### ? Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

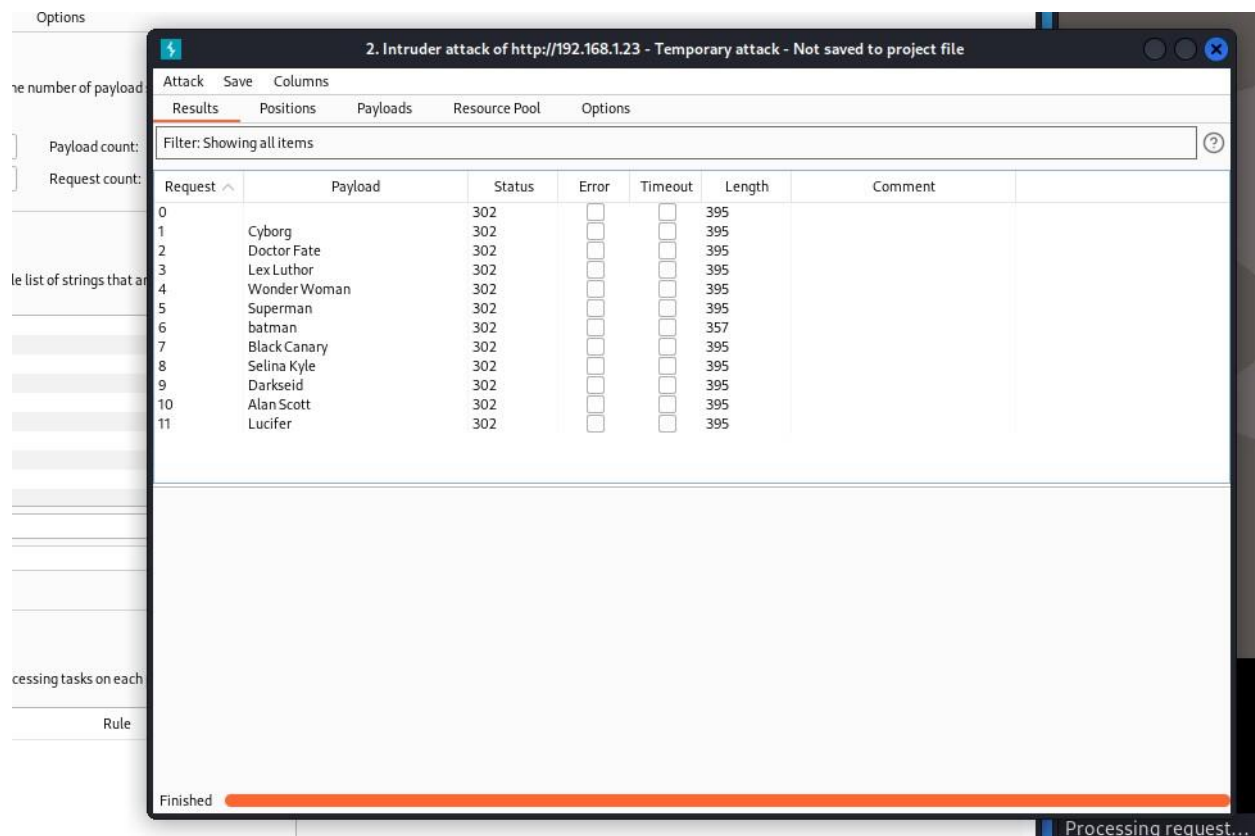
Paste	Cyborg
Load ...	Doctor Fate
Remove	Lex Luthor
Clear	Wonder Woman
Deduplicate	Superman
	batman
	Black Canary
	Selina Kyle
	Darkseid
	Alan Scott
Add	<input type="text" value="Enter a new item"/>
<input type="text" value="Add from list ... [Pro version only]"/>	

### ? Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

Add	Enabled	Rule
Edit		
Remove		
Up		
Down		

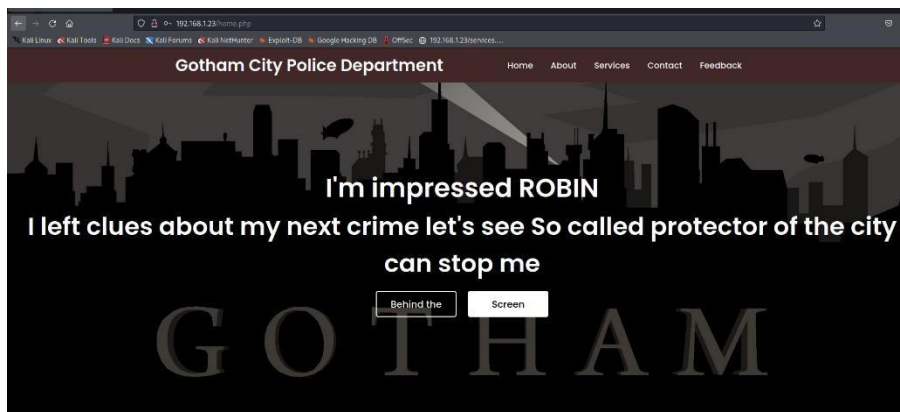
8) Users can identify passwords using the length and status of the payload



## Second task

In this task, the play needs to perform cryptography technics. the source code of the web page has some encrypted text users need to find a type of that description method and need to decrypt the data

- 1) Find the encryption algorithm by slowing the riddle



```
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <!--<title> Website Layout | CodingLab</title>-->
  <link rel="stylesheet" href="homestyles.css">
  <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/5.15.2/css/all.min.css"/>

  <style>
body {
  background-image: url('img2.png');
}
</style>

</head>
<body>
  <nav>
    <div class="menu">
      <div class="logo">
        <a href="#">Gotham City Police Department</a>
      </div>
      <ul>
        <li><a href="#">Home</a></li>
        <li><a href="aboutpass.php">About</a></li>
        <li><a href="services.php">Services</a></li>
        <li><a href="Contact.php">Contact</a></li>
        <li><a href="#">Feedback</a></li>
      </ul>
    </div>
  </nav>
  <div class="img"></div>
  <div class="center">
    <div class="title">I'm impressed ROBIN </div>
    <div class="sub_title">I left clues about my next crime let's see So called protector of the city can stop me </div>
    <div class="btns">
      <button>Behind the</button>
      <button>Screen</button>
    </div>
  </div>
</body>
</html>

<!--
64 IS MY favorite NUMBER
MjAyMi8xMi8xMiAxMi4xMlBN
Time is tiking robin :)

FLAG2:So2_done_12345
-->
```

2) Use the base 64 decoders and decode the flag



MjAyMi8xMi8xMiAxMi4xMIBN

For encoded binaries (like images, documents, etc.) use the file upload form

ISO-8859-1 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 )

< DECODE >

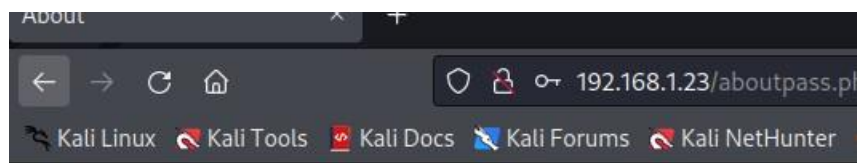
Decodes your data into the area below

2022/12/12 12.12PM

### Third task

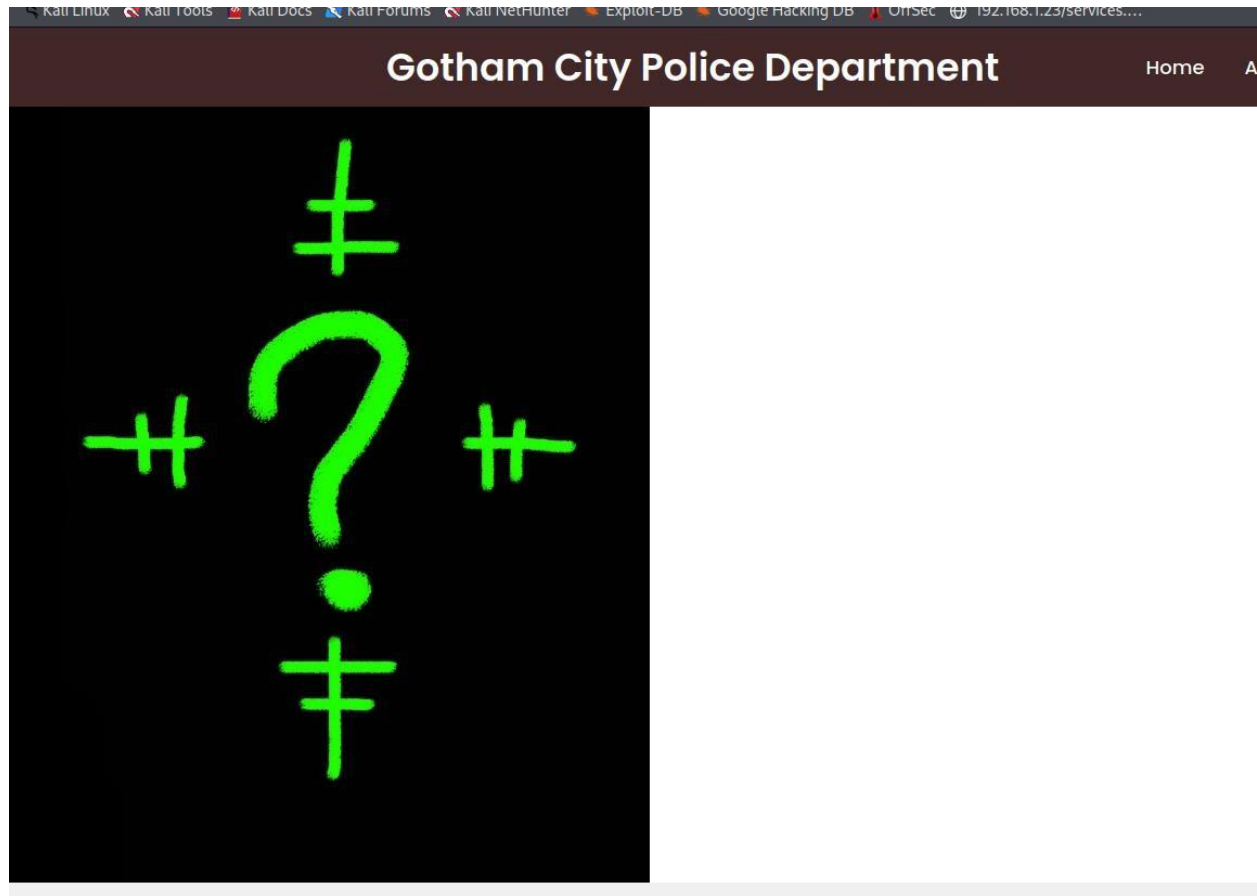
To gain access to the next page play needs to provide a password. The player needs to find it. This task uses the steganography method to hide data

- 1) user needs to go [contact.php](#) and check its source code to find the hint



## Enter password

?>



```

2 <!-- Created By CodingNepal - www.codingnepalweb.com -->
3 <html lang="en" dir="ltr">
4   <head>
5     <meta charset="UTF-8">
6     <meta name="viewport" content="width=device-width, initial-scale=1.0">
7     <!--<title> Website Layout | CodingLab</title>-->
8     <link rel="stylesheet" href="homestyles.css">
9     <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/5.15.2/css/
10
11     <style>
12 body {
13   background-image: url('img2.png');
14 }
15 </style>
16
17 <!--
18 Download the image it has what you need :)
19
20 FLAG4:5o4_done_12345
21 -->
22
23   </head>
24   <body>
25     <nav>
26       <div class="menu">
27         <div class="logo">
28           <a href="#">Gotham City Police Department</a>
29         </div>
30         <ul>
31           <li><a href="#">Home</a></li>
32           <li><a href="#">About</a></li>
33           <li><a href="#">Services</a></li>
34           <li><a href="#">Contact</a></li>
35           <li><a href="#">Feedback</a></li>
36         </ul>
37       </div>
38     </nav>
39     <!-- <div class="img"></div> -->
40
41     <ima src="ctfima.jpg" alt="More Than you can see" width="592" height="800">

```

- 2) Users need to download the image and need to extract the data from that image

A terminal window with a dark blue background and white text. The title bar at the top reads 'azumi@Azumi: ~/Downloads'. The menu bar shows 'File', 'Actions', 'Edit', 'View', and 'Help'. The prompt is '(azumi@Azumi) ~/Downloads'. The command 'steghide extract -sf ~/Downloads/ctfimg.jpg' has been entered. Below the command, the text 'Enter passphrase:' is displayed. The next line shows the message 'the file "ctf.txt" does already exist. overwrite ? (y/n)' followed by a cursor.

## Final task

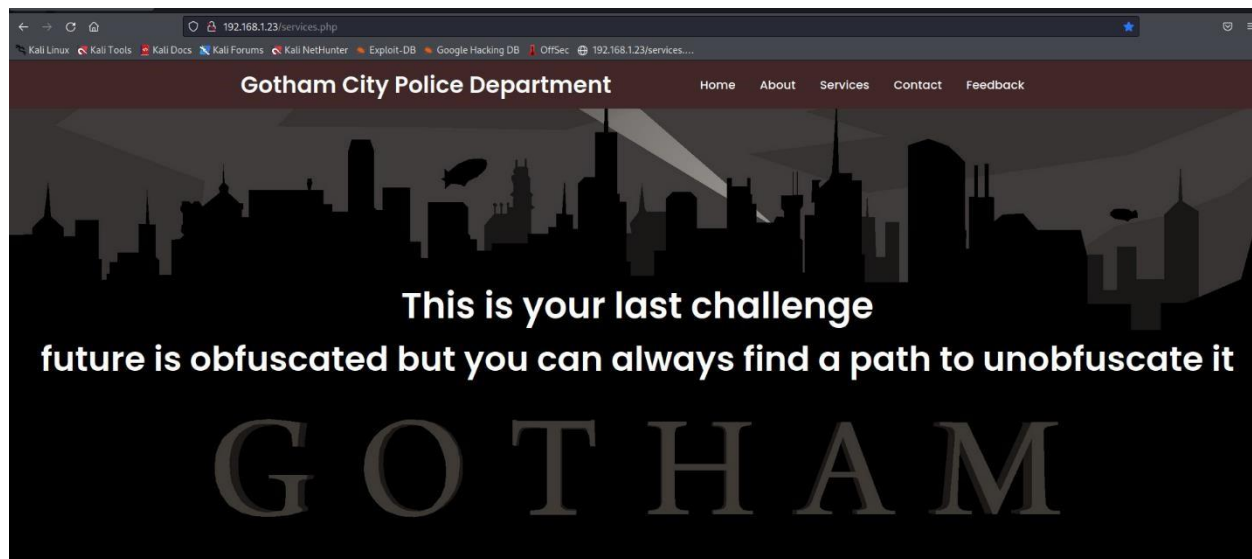
To do the final task the user needs to have knowledge about the source code protection mechanism. users needs to identify obfuscated java script code

- 1) Needs to find a hint in the source code and go to **services.js** page
- 2) Deobfuscate the JavaScript code to plaintext
- 3) Using caesar cipher user needs to decrypt the value of the js file

🌐 192.168.1.23

Zkdw Lv Wkh Ehjlqqlqj Ri Hwhuqlwb, Wkh Hqg Ri Wlph Dqg Vsdfh,  
Wkh Ehjlqqlqj Ri Hyhub Hqg, Dqg Wkh Hqg Ri Hyhub Udfh? wkh dqvzhu  
zloo eh ehjlqqlqj ri wkh qhaw fkdswu zhoo sodbhg urelq brxu ilqdo  
foxx lv wkh Edw Fdyh

OK



```
32 <li><a href="#">feedback</a></li>
33 </ul>
34 </div>
35 </nav>
36 <div class="img"></div>
37 <div class="center">
38 <div class="title">This is your last challenge </div>
39 <div class="sub_title"> future is obfuscated but you can always find a path to unobfuscate it </div>
40
41 <!--
42 has two parts..... ending with Caesar Cipher.... you will be need 3 <*_*>
43
44 FLAG5:5o5_done_12345
45 -->
46
47 </div>
48 </body>
49 </html>
50
51
```

```
var _0x6734=["\x5A\x68\x64\x77\x20\x4C\x76\x20\x57\x68\x68\x20\x45\x68\x6A\x6C\x71\x71\x6C\x71\x6A\x20\x52\x69\x20\x48\x77\x68\x75\x71\x6C\x77\x62\x2C\x20\x57\x68\x68\x2
```

Example

### Input

```
1 0\x77\x68\x68\x20\x45\x64\x77\x20\x46\x64\x79\x68";alert(_0x6734[0])
```

### Output

```
1 alert("Zkdw Lv Wkh Ehjlqqlqj Ri Hwhuqlwb, Wkh Hqg Ri Wlph Dqg Vsdhf,
```

Cipher - Shift by 3

E,F,G,H,I,...B,C

B,C,D,E,F,...Y,Z

What Is The Beginning  
Of Eternity, The End  
Of Time And Space,  
The Beginning Of  
Every End, And The  
End Of Every Race?  
the answer will be  
beginning of the next  
chapter well played  
robin your final clue  
is the Bat Cave")

### ★ CAESAR SHIFTED CIPHERTEXT ?

Zkdw Lv Wkh Ehjlqqlqj Ri Hwhuqlwb, Wkh Hqg Ri Wlph Dqg  
Vsdhf, Wkh Ehjlqqlqj Ri Hyhub Hqg, Dqg Wkh Hqg Ri Hyhub  
Udfh? wkh dqvzhu zloo eh ehjlqqlqj ri wkh qhaw fkdswu  
zhoo sodbhg urelq brxu ilqdo foxh lv wkh Edw Fdyh")

Test all possible shifts (26-letter alphabet A-Z)

► DECRYPT (BRUTEFORCE)

### MANUAL DECRYPTION AND PARAMETERS

★ SHIFT/KEY (NUMBER): 3

- ☒ USE THE ENGLISH ALPHABET (26 LETTERS FROM A TO Z)
- ☐ USE THE ENGLISH ALPHABET AND ALSO SHIFT THE DIGITS 0-9
- ☐ USE THE LATIN ALPHABET IN THE TIME OF CAESAR (23 LETTERS, NO J, U OR W)

To add