Cyber Security and Ethical Hacking Internship Program
CTF Challenge

Introduction

Capture the Flag (CTF) in cyber security is an exercise in which "flags" are secretly hidden in purposefully vulnerable programs or websites. Security CTFs are usually designed to serve as an educational exercise to give participants experience in securing a machine and conducting and reacting to the sort of attacks found in the real world.

Requirements

- **Recommended operating system is Kali Linux.**
- **Virtual Box, Burp Suite, dirb/dirbuster must be installed.**
- **Must know enumeration and assume potential services that run on a server.**

Goal

- **Infer the basics of web application penetration testing**
- **Learn to manually scan a target and identify potential vulnerability Points of Interest and obtain flags.**
- **Identify the six flags planted in the vulnerable machine.**

Task

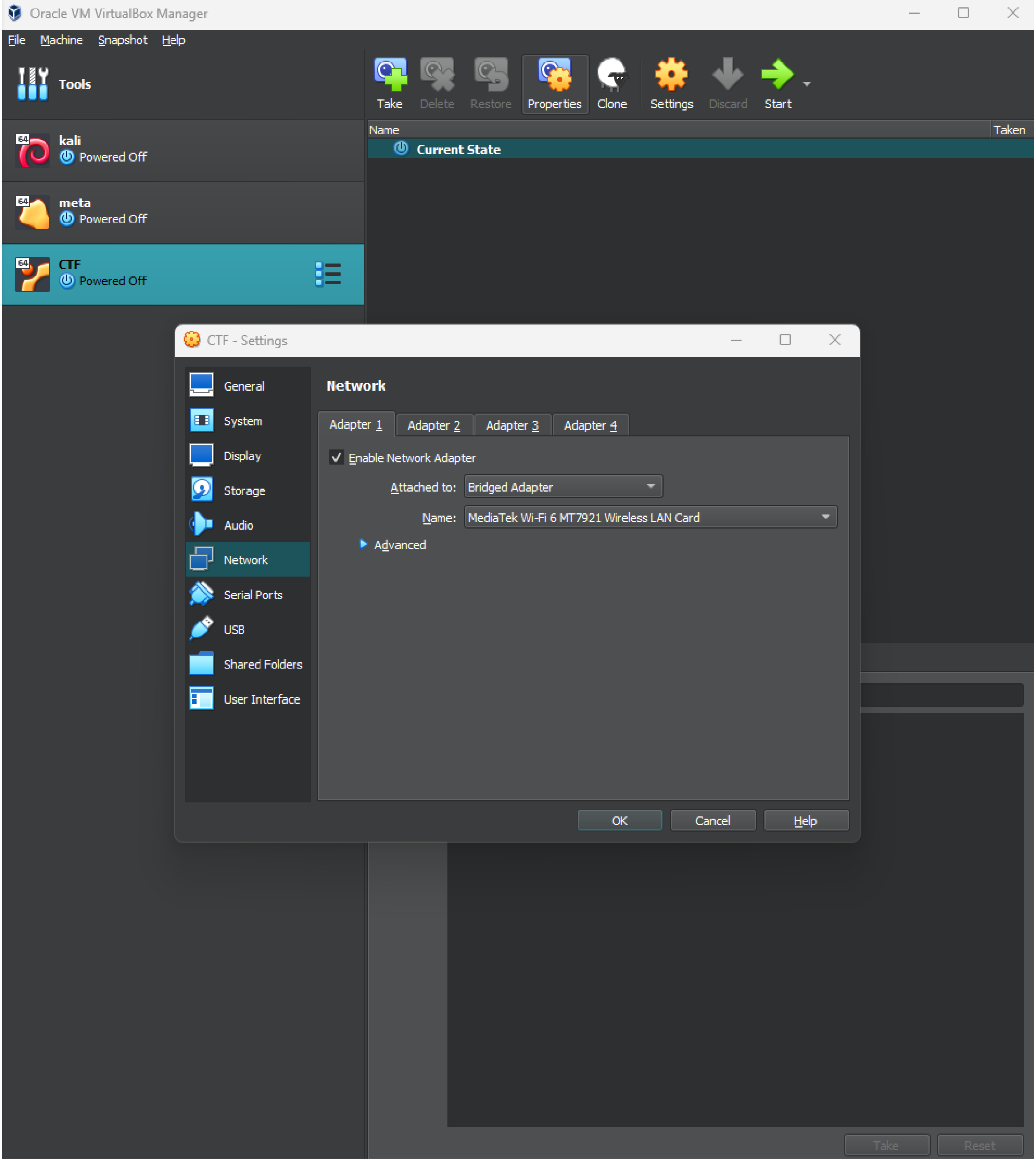
- **Deploy the given appliance with the network set to bridged.**
- **Use the IP address displayed and perform reconnaissance on the deployed machine.**
- **After completing reconnaissance, manually perform vulnerability analysis on the appliance.**
- **You are free to use any open-sourced tools to find the flags.**

NAME : **Gaurav Uttam Ghandat**

Scenario

As an internal ethical hacker in your company, a new product is being prepared for production, but before roll-out, you are tasked with hacking into the product website in the form of a Virtual Machine Snapshot (Sandbox). Before the website goes public, all potential vulnerabilities must be identified. Any information that should not be accessible externally to the public is considered a vulnerability to be tested with high priority. Instead of the actual information data, the developers have planted “flags” or “strings” in the place of the critical data. The developers want to know how these flags / critical data could be leaked so the product website could be re-programmed and secured.

TASK 1 : Deploy the given appliance with the network set to bridged.



☑ Enable Network Adapter

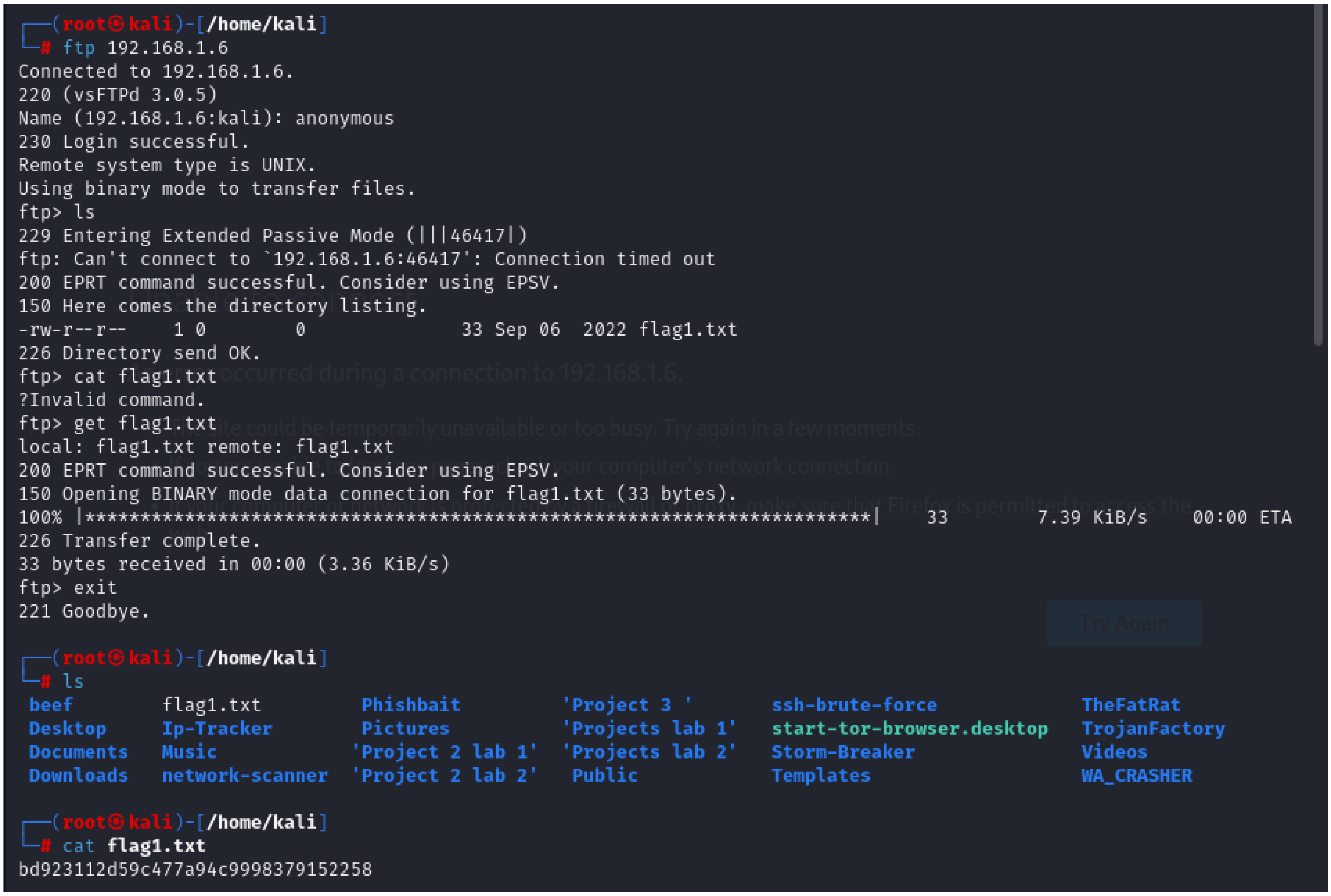
Attached to: Bridged Adapter

Name: MediaTek Wi-Fi 6 MT7921 Wireless LAN Card

TASK 2 : Use the IP address displayed and perform reconnaissance on the deployed machine. After completing reconnaissance, manually perform vulnerability analysis on the appliance.

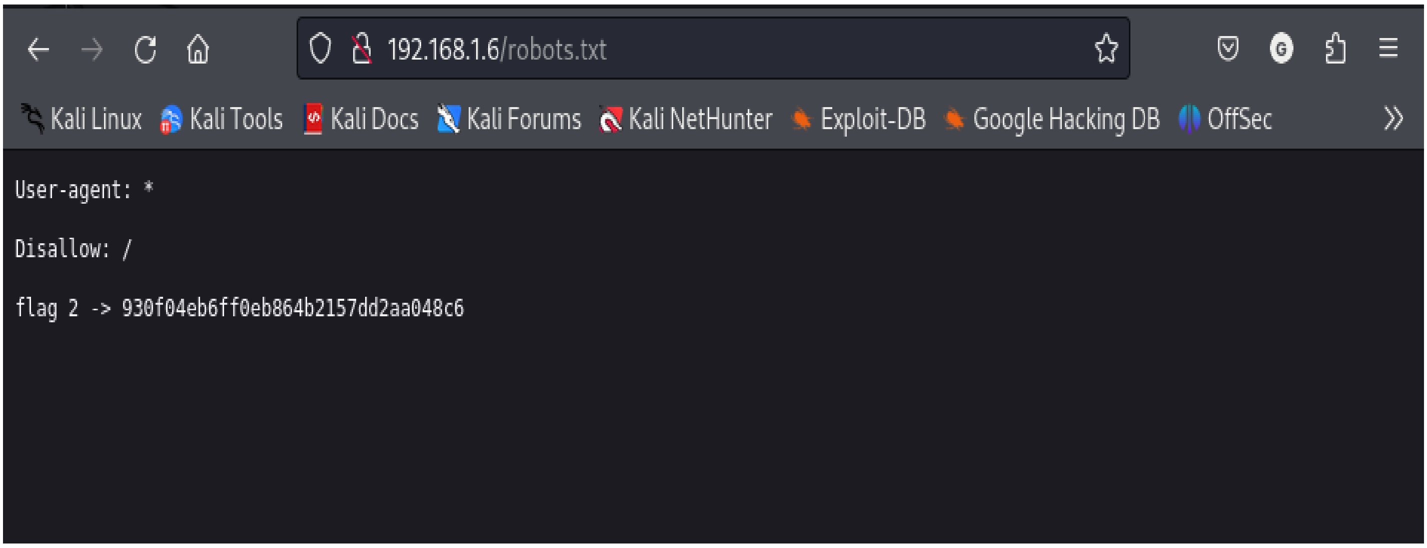
Use the IP address and capture the flag from the machine .we have to capture the 6 flag from the machine .

FLAG 1 :



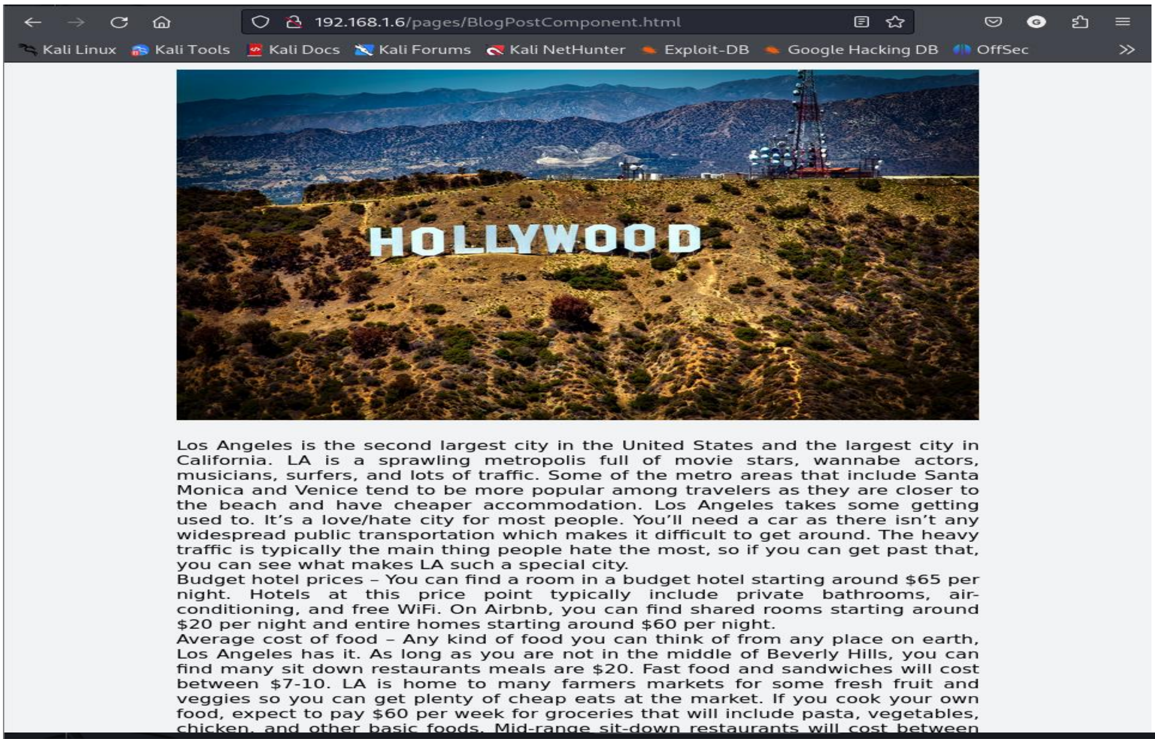
```
┌──(root㉿kali)-[/home/kali]
└─# ftp 192.168.1.6
Connected to 192.168.1.6.
220 (vsFTPd 3.0.5)
Name (192.168.1.6:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||46417|)
ftp: Can't connect to `192.168.1.6:46417': Connection timed out
200 EPRT command successful. Consider using EPSV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0              33 Sep 06  2022 flag1.txt
226 Directory send OK.
ftp> cat flag1.txt
?Invalid command.
ftp> get flag1.txt
local: flag1.txt remote: flag1.txt
200 EPRT command successful. Consider using EPSV.
150 Opening BINARY mode data connection for flag1.txt (33 bytes).
100% |***********************************************************************|    33        7.39 KiB/s    00:00 ETA
226 Transfer complete.
33 bytes received in 00:00 (3.36 KiB/s)
ftp> exit
221 Goodbye.

┌──(root㉿kali)-[/home/kali]
└─# ls
 beef        flag1.txt        Phishbait           'Project 3 '         ssh-brute-force              TheFatRat
 Desktop     Ip-Tracker       Pictures            'Projects lab 1'     start-tor-browser.desktop    TrojanFactory
 Documents   Music           'Project 2 lab 1'    'Projects lab 2'     Storm-Breaker                Videos
 Downloads   network-scanner 'Project 2 lab 2'     Public              Templates                    WA_CRASHER

┌──(root㉿kali)-[/home/kali]
└─# cat flag1.txt
bd923112d59c477a94c9998379152258
```

FLAG 2 :



```
User-agent: *

Disallow: /

flag 2 -> 930f04eb6ff0eb864b2157dd2aa048c6
```

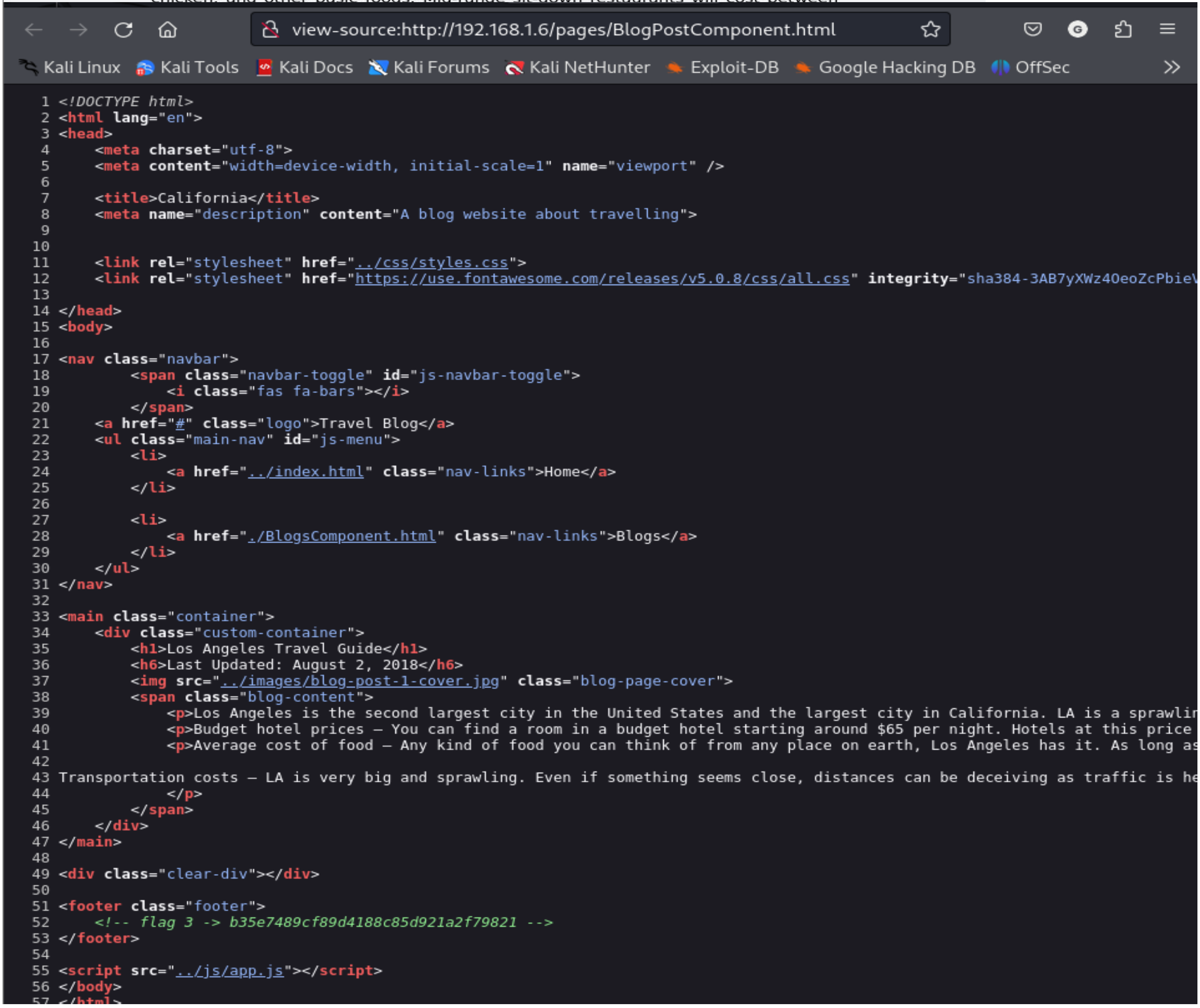
FLAG 3 :



Los Angeles is the second largest city in the United States and the largest city in California. LA is a sprawling metropolis full of movie stars, wannabe actors, musicians, surfers, and lots of traffic. Some of the metro areas that include Santa Monica and Venice tend to be more popular among travelers as they are closer to the beach and have cheaper accommodation. Los Angeles takes some getting used to. It's a love/hate city for most people. You'll need a car as there isn't any widespread public transportation which makes it difficult to get around. The heavy traffic is typically the main thing people hate the most, so if you can get past that, you can see what makes LA such a special city.

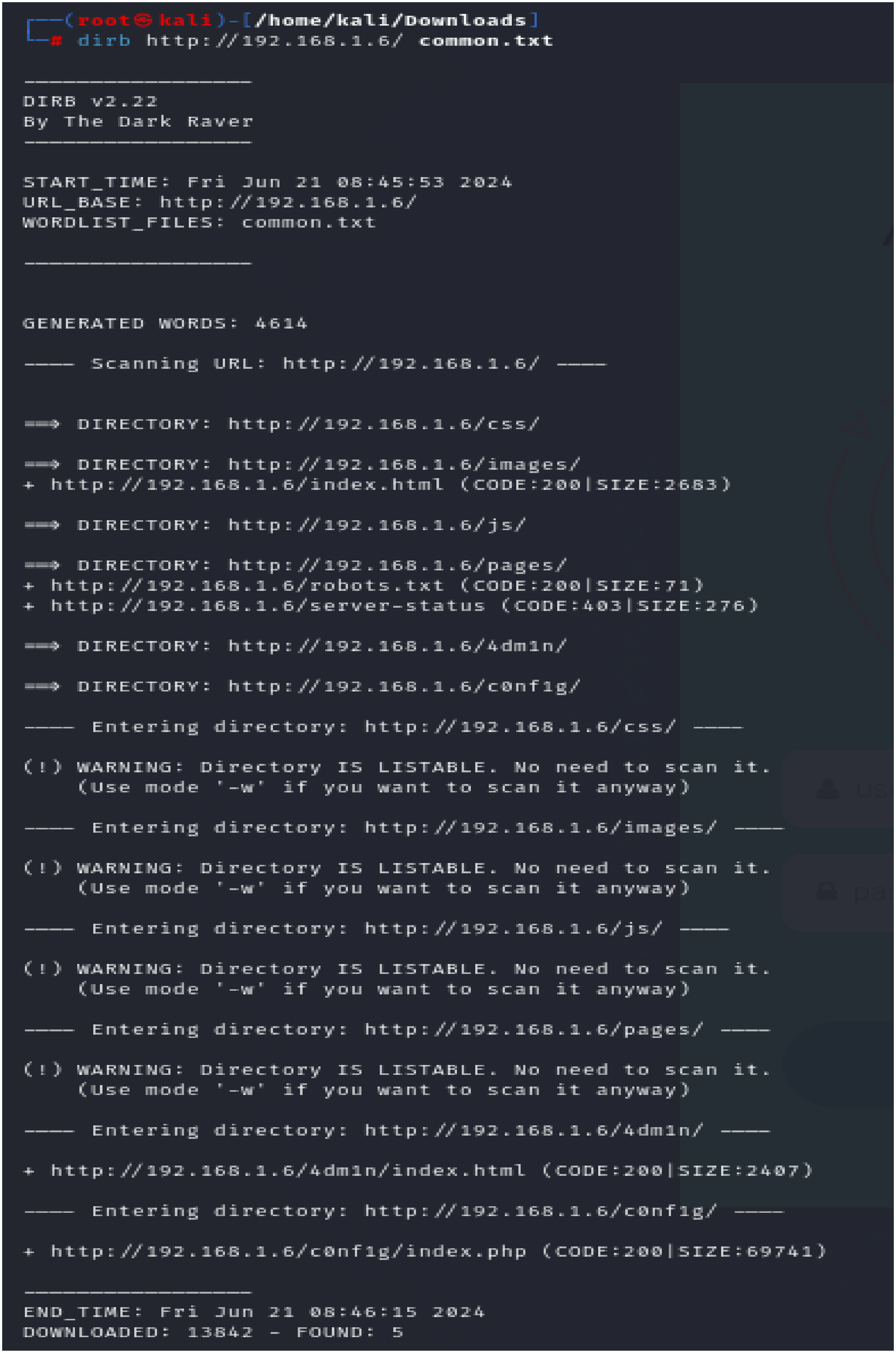
Budget hotel prices – You can find a room in a budget hotel starting around $65 per night. Hotels at this price point typically include private bathrooms, air-conditioning, and free WiFi. On Airbnb, you can find shared rooms starting around $20 per night and entire homes starting around $60 per night.

Average cost of food – Any kind of food you can think of from any place on earth, Los Angeles has it. As long as you are not in the middle of Beverly Hills, you can find many sit down restaurants meals are $20. Fast food and sandwiches will cost between $7-10. LA is home to many farmers markets for some fresh fruit and veggies so you can get plenty of cheap eats at the market. If you cook your own food, expect to pay $60 per week for groceries that will include pasta, vegetables, chicken, and other basic foods. Mid-range sit-down restaurants will cost between



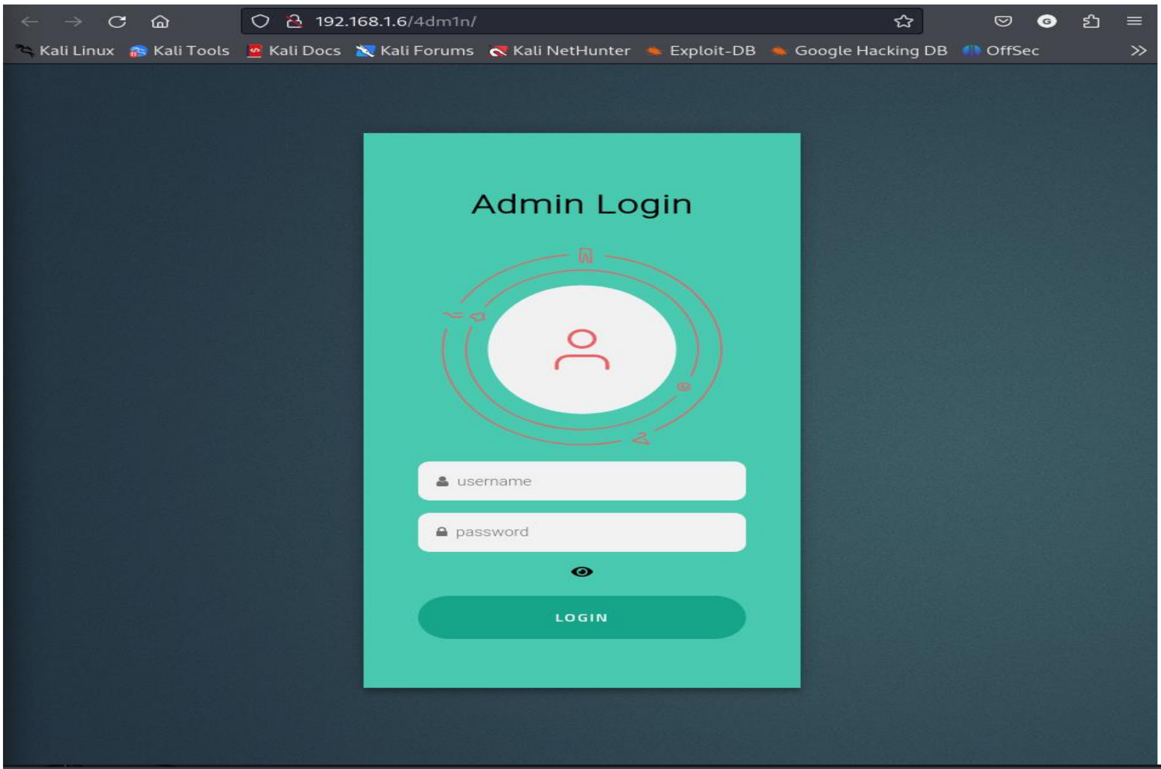
```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="utf-8">
    <meta content="width=device-width, initial-scale=1" name="viewport" />

    <title>California</title>
    <meta name="description" content="A blog website about travelling">


    <link rel="stylesheet" href="../css/styles.css">
    <link rel="stylesheet" href="https://use.fontawesome.com/releases/v5.0.8/css/all.css" integrity="sha384-3AB7yXWz40eoZcPbie\

</head>
<body>

<nav class="navbar">
        <span class="navbar-toggle" id="js-navbar-toggle">
            <i class="fas fa-bars"></i>
        </span>
    <a href="#" class="logo">Travel Blog</a>
    <ul class="main-nav" id="js-menu">
        <li>
            <a href="../index.html" class="nav-links">Home</a>
        </li>

        <li>
            <a href="./BlogsComponent.html" class="nav-links">Blogs</a>
        </li>
    </ul>
</nav>

<main class="container">
    <div class="custom-container">
        <h1>Los Angeles Travel Guide</h1>
        <h6>Last Updated: August 2, 2018</h6>
        <img src="../images/blog-post-1-cover.jpg" class="blog-page-cover">
        <span class="blog-content">
            <p>Los Angeles is the second largest city in the United States and the largest city in California. LA is a sprawlin
            <p>Budget hotel prices – You can find a room in a budget hotel starting around $65 per night. Hotels at this price
            <p>Average cost of food – Any kind of food you can think of from any place on earth, Los Angeles has it. As long as

Transportation costs – LA is very big and sprawling. Even if something seems close, distances can be deceiving as traffic is he
            </p>
        </span>
    </div>
</main>

<div class="clear-div"></div>

<footer class="footer">
    <!-- flag 3 -> b35e7489cf89d4188c85d921a2f79821 -->
</footer>

<script src="../js/app.js"></script>
</body>
</html>
```

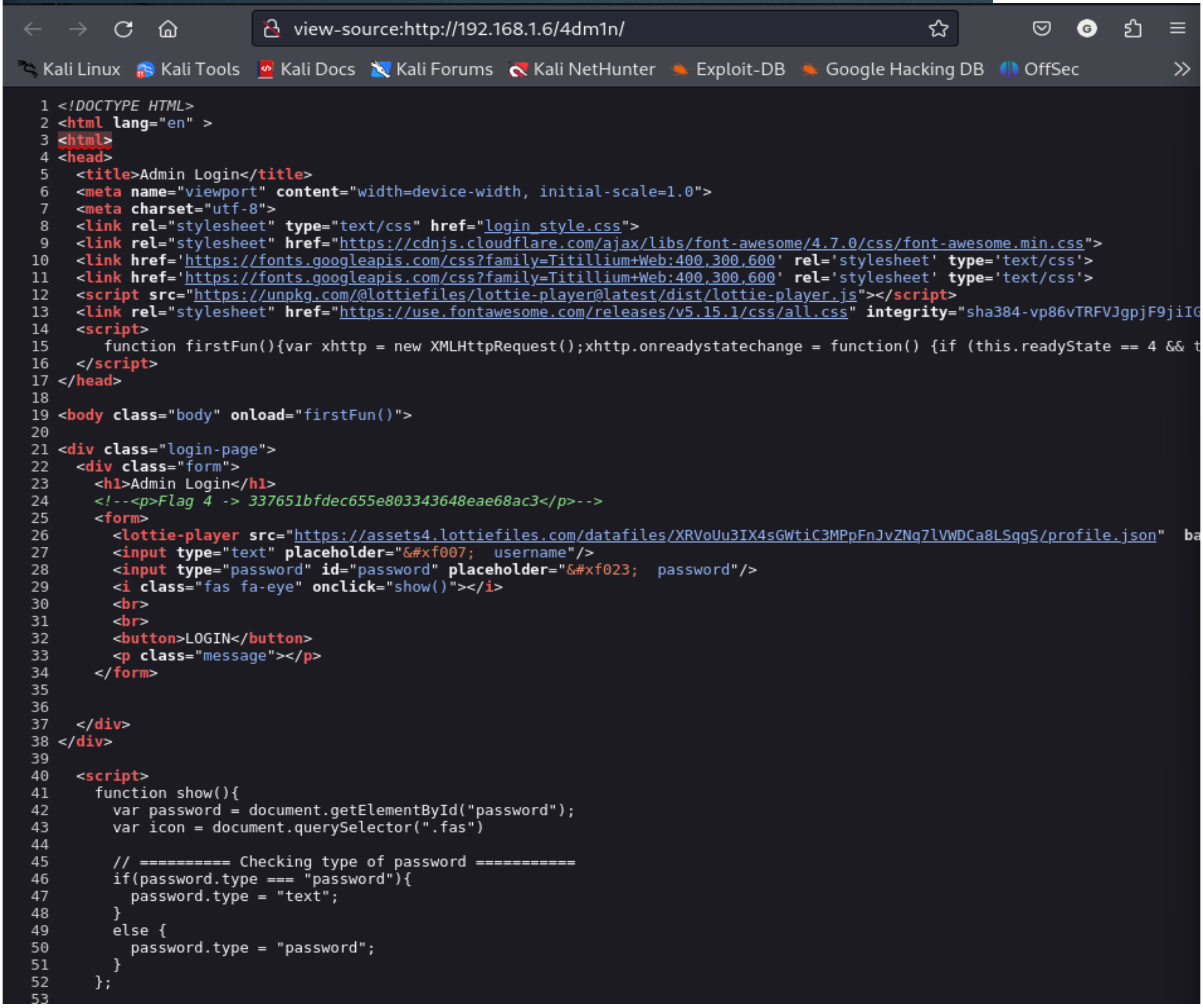
TASK 3 : You are free to use any open-sourced tools to find the flags.
We are open-sourced tool called dirb for capturing the flag 4 and 5 using cooman.txt wordlist. And for capturing 6 flag we use the open-sourced tools called Burp Suite.



```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# dirb http://192.168.1.6/ common.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Fri Jun 21 08:45:53 2024
URL_BASE: http://192.168.1.6/
WORDLIST_FILES: common.txt

-----------------


GENERATED WORDS: 4614

---- Scanning URL: http://192.168.1.6/ ----


==> DIRECTORY: http://192.168.1.6/css/

==> DIRECTORY: http://192.168.1.6/images/
+ http://192.168.1.6/index.html (CODE:200|SIZE:2683)

==> DIRECTORY: http://192.168.1.6/js/

==> DIRECTORY: http://192.168.1.6/pages/
+ http://192.168.1.6/robots.txt (CODE:200|SIZE:71)
+ http://192.168.1.6/server-status (CODE:403|SIZE:276)

==> DIRECTORY: http://192.168.1.6/4dm1n/

==> DIRECTORY: http://192.168.1.6/c0nf1g/

---- Entering directory: http://192.168.1.6/css/ ----

(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.6/images/ ----

(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.6/js/ ----

(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.6/pages/ ----

(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.6/4dm1n/ ----

+ http://192.168.1.6/4dm1n/index.html (CODE:200|SIZE:2407)

---- Entering directory: http://192.168.1.6/c0nf1g/ ----

+ http://192.168.1.6/c0nf1g/index.php (CODE:200|SIZE:69741)

-----------------
END_TIME: Fri Jun 21 08:46:15 2024
DOWNLOADED: 13842 - FOUND: 5
```

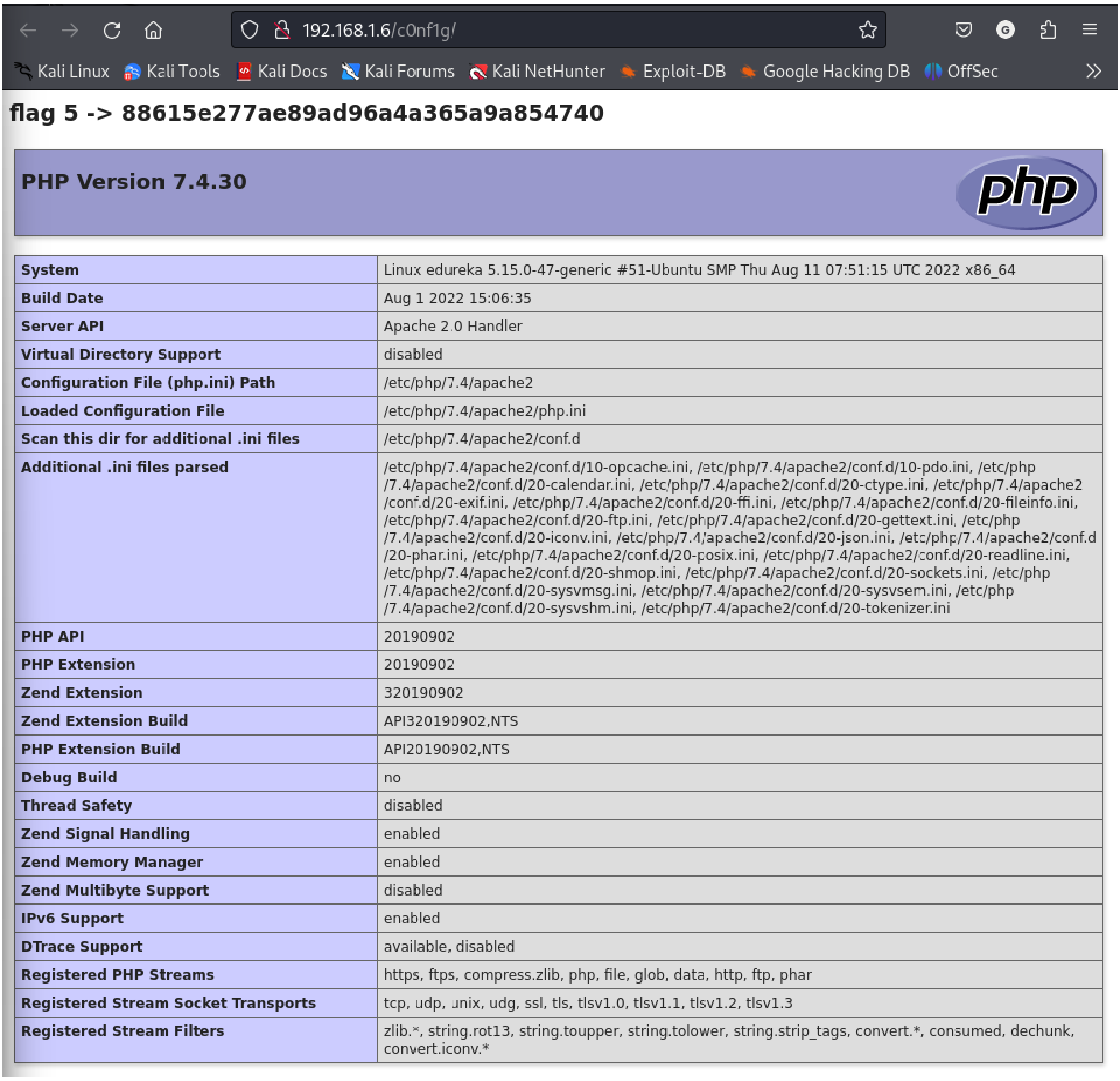
FLAG 4





```
<!DOCTYPE HTML>
<html lang="en" >
<html>
<head>
  <title>Admin Login</title>
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <meta charset="utf-8">
  <link rel="stylesheet" type="text/css" href="login_style.css">
  <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.min.css">
  <link href='https://fonts.googleapis.com/css?family=Titillium+Web:400,300,600' rel='stylesheet' type='text/css'>
  <link href='https://fonts.googleapis.com/css?family=Titillium+Web:400,300,600' rel='stylesheet' type='text/css'>
  <script src="https://unpkg.com/@lottiefiles/lottie-player@latest/dist/lottie-player.js"></script>
  <link rel="stylesheet" href="https://use.fontawesome.com/releases/v5.15.1/css/all.css" integrity="sha384-vp86vTRFVJgpjF9jiIG
  <script>
     function firstFun(){var xhttp = new XMLHttpRequest();xhttp.onreadystatechange = function() {if (this.readyState == 4 && t
  </script>
</head>

<body class="body" onload="firstFun()">

<div class="login-page">
  <div class="form">
    <h1>Admin Login</h1>
    <!--<p>Flag 4 -> 337651bfdec655e803343648eae68ac3</p>-->
    <form>
      <lottie-player src="https://assets4.lottiefiles.com/datafiles/XRVoUu3IX4sGWtiC3MPpFnJvZNq7lVWDCa8LSqgS/profile.json"  ba
      <input type="text" placeholder="&#xf007;  username"/>
      <input type="password" id="password" placeholder="&#xf023;  password"/>
      <i class="fas fa-eye" onclick="show()"></i>
      <br>
      <br>
      <button>LOGIN</button>
      <p class="message"></p>
    </form>


  </div>
</div>

  <script>
    function show(){
      var password = document.getElementById("password");
      var icon = document.querySelector(".fas")

      // ========== Checking type of password ===========
      if(password.type === "password"){
        password.type = "text";
      }
      else {
        password.type = "password";
      }
    };
```

FLAG 5 :

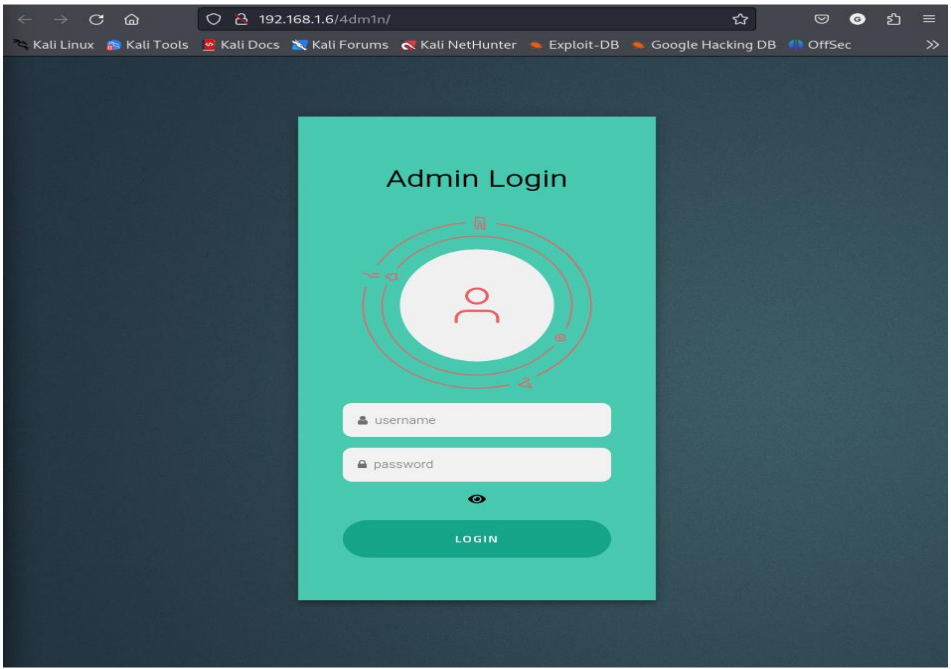


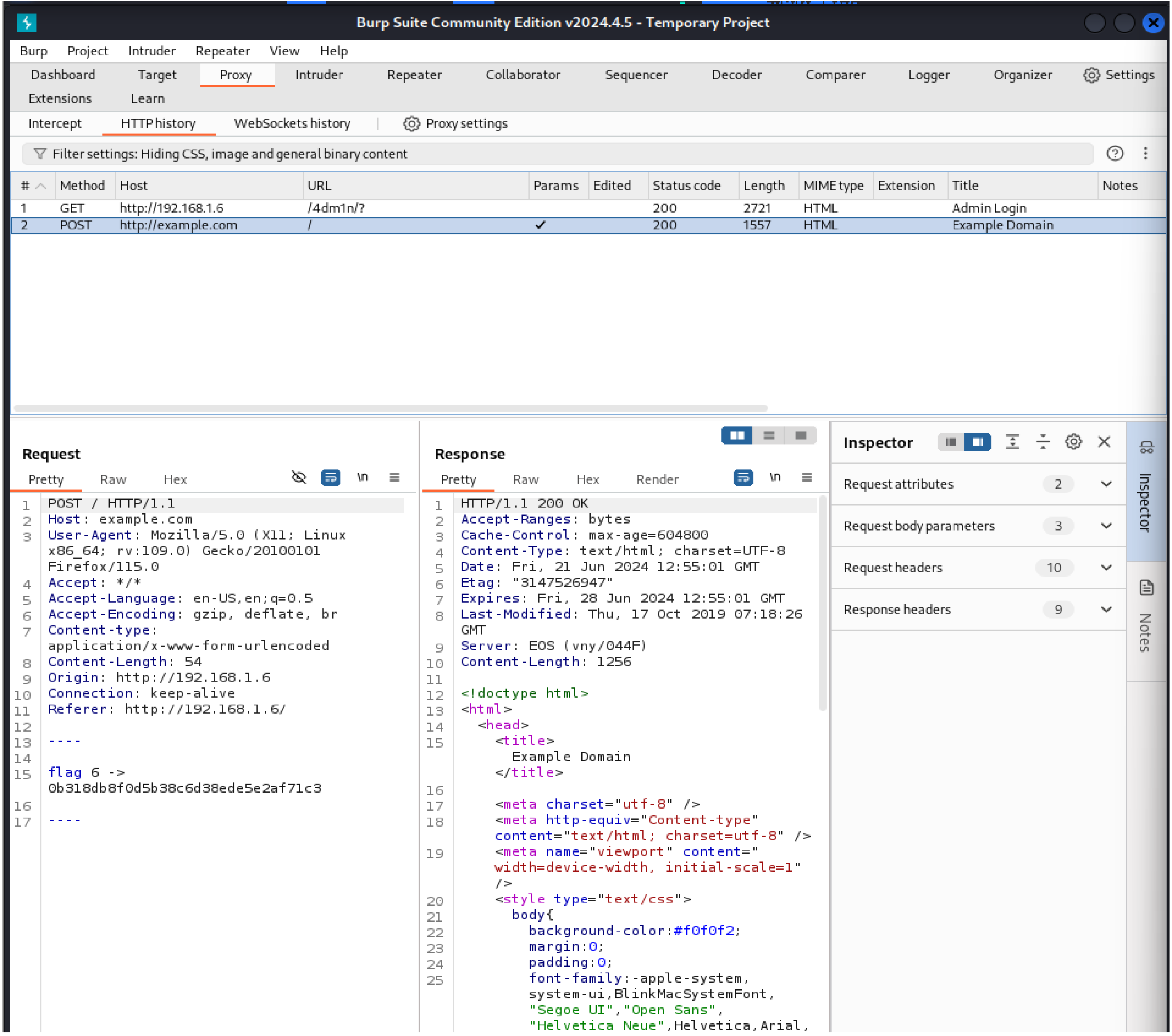
flag 5 -> 88615e277ae89ad96a4a365a9a854740

PHP Version 7.4.30

System	Linux edureka 5.15.0-47-generic #51-Ubuntu SMP Thu Aug 11 07:51:15 UTC 2022 x86_64
Build Date	Aug 1 2022 15:06:35
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.4/apache2
Loaded Configuration File	/etc/php/7.4/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.4/apache2/conf.d
Additional .ini files parsed	/etc/php/7.4/apache2/conf.d/10-opcache.ini, /etc/php/7.4/apache2/conf.d/10-pdo.ini, /etc/php/7.4/apache2/conf.d/20-calendar.ini, /etc/php/7.4/apache2/conf.d/20-ctype.ini, /etc/php/7.4/apache2/conf.d/20-exif.ini, /etc/php/7.4/apache2/conf.d/20-ffi.ini, /etc/php/7.4/apache2/conf.d/20-fileinfo.ini, /etc/php/7.4/apache2/conf.d/20-ftp.ini, /etc/php/7.4/apache2/conf.d/20-gettext.ini, /etc/php/7.4/apache2/conf.d/20-iconv.ini, /etc/php/7.4/apache2/conf.d/20-json.ini, /etc/php/7.4/apache2/conf.d/20-phar.ini, /etc/php/7.4/apache2/conf.d/20-posix.ini, /etc/php/7.4/apache2/conf.d/20-readline.ini, /etc/php/7.4/apache2/conf.d/20-shmop.ini, /etc/php/7.4/apache2/conf.d/20-sockets.ini, /etc/php/7.4/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.4/apache2/conf.d/20-sysvsem.ini, /etc/php/7.4/apache2/conf.d/20-sysvshm.ini, /etc/php/7.4/apache2/conf.d/20-tokenizer.ini
PHP API	20190902
PHP Extension	20190902
Zend Extension	320190902
Zend Extension Build	API320190902,NTS
PHP Extension Build	API20190902,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled
IPv6 Support	enabled
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2, tlsv1.3
Registered Stream Filters	zlib.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, convert.iconv.*

FLAG 6 :





Filter settings: Hiding CSS, image and general binary content

#	Method	Host	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes
1	GET	http://192.168.1.6	/4dm1n/?			200	2721	HTML		Admin Login	
2	POST	http://example.com	/	✓		200	1557	HTML		Example Domain	

```
POST / HTTP/1.1
Host: example.com
User-Agent: Mozilla/5.0 (X11; Linux
x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-type:
application/x-www-form-urlencoded
Content-Length: 54
Origin: http://192.168.1.6
Connection: keep-alive
Referer: http://192.168.1.6/

----

flag 6 ->
0b318db8f0d5b38c6d38ede5e2af71c3

----
```

```
HTTP/1.1 200 OK
Accept-Ranges: bytes
Cache-Control: max-age=604800
Content-Type: text/html; charset=UTF-8
Date: Fri, 21 Jun 2024 12:55:01 GMT
Etag: "3147526947"
Expires: Fri, 28 Jun 2024 12:55:01 GMT
Last-Modified: Thu, 17 Oct 2019 07:18:26
GMT
Server: EOS (vny/044F)
Content-Length: 1256

<!doctype html>
<html>
  <head>
    <title>
      Example Domain
    </title>

    <meta charset="utf-8" />
    <meta http-equiv="Content-type"
    content="text/html; charset=utf-8" />
    <meta name="viewport" content="
    width=device-width, initial-scale=1"
    />
    <style type="text/css">
      body{
        background-color:#f0f0f2;
        margin:0;
        padding:0;
        font-family:-apple-system,
        system-ui,BlinkMacSystemFont,
        "Segoe UI","Open Sans",
        "Helvetica Neue",Helvetica,Arial,
```