

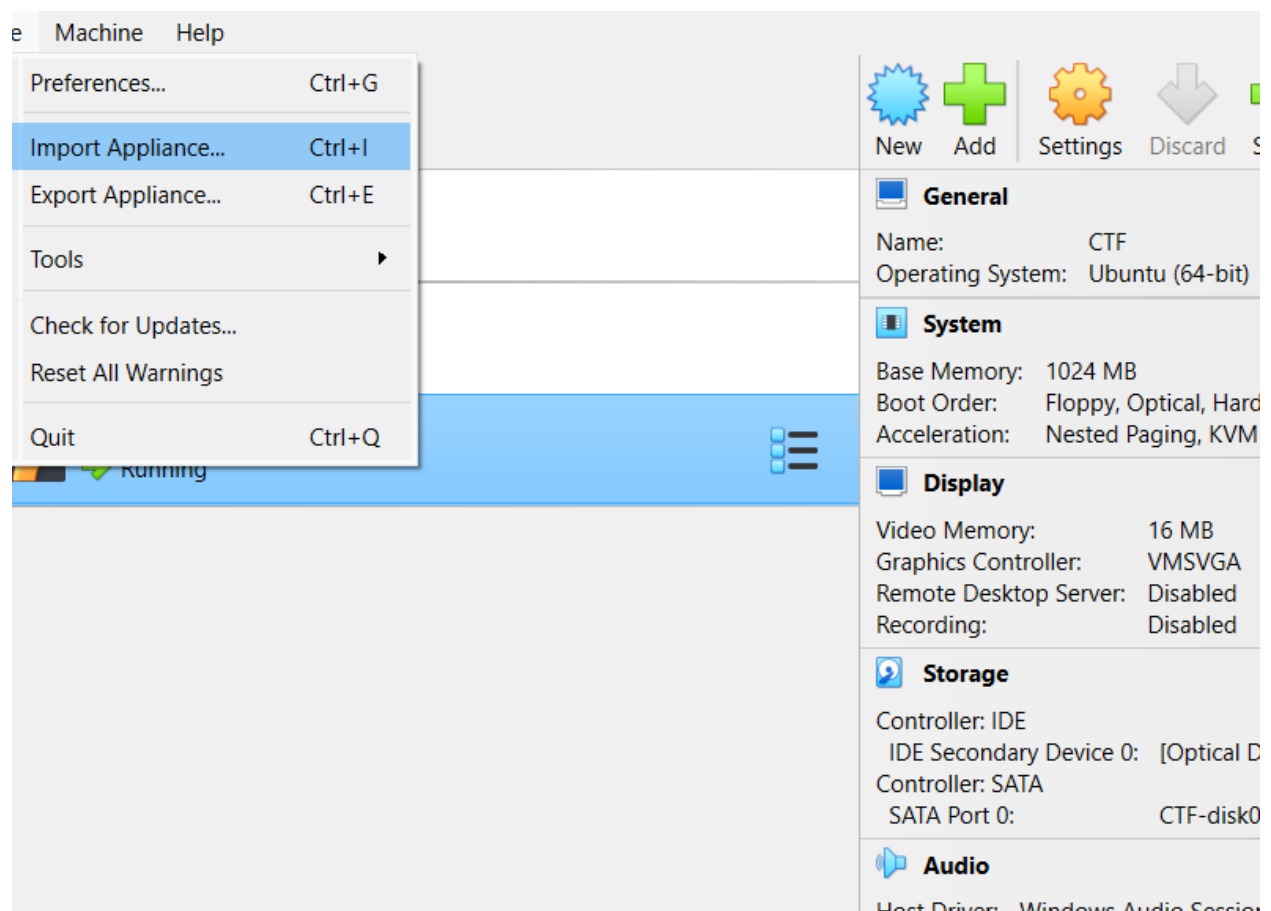
PROJECT-4

CTF CHALLENGE

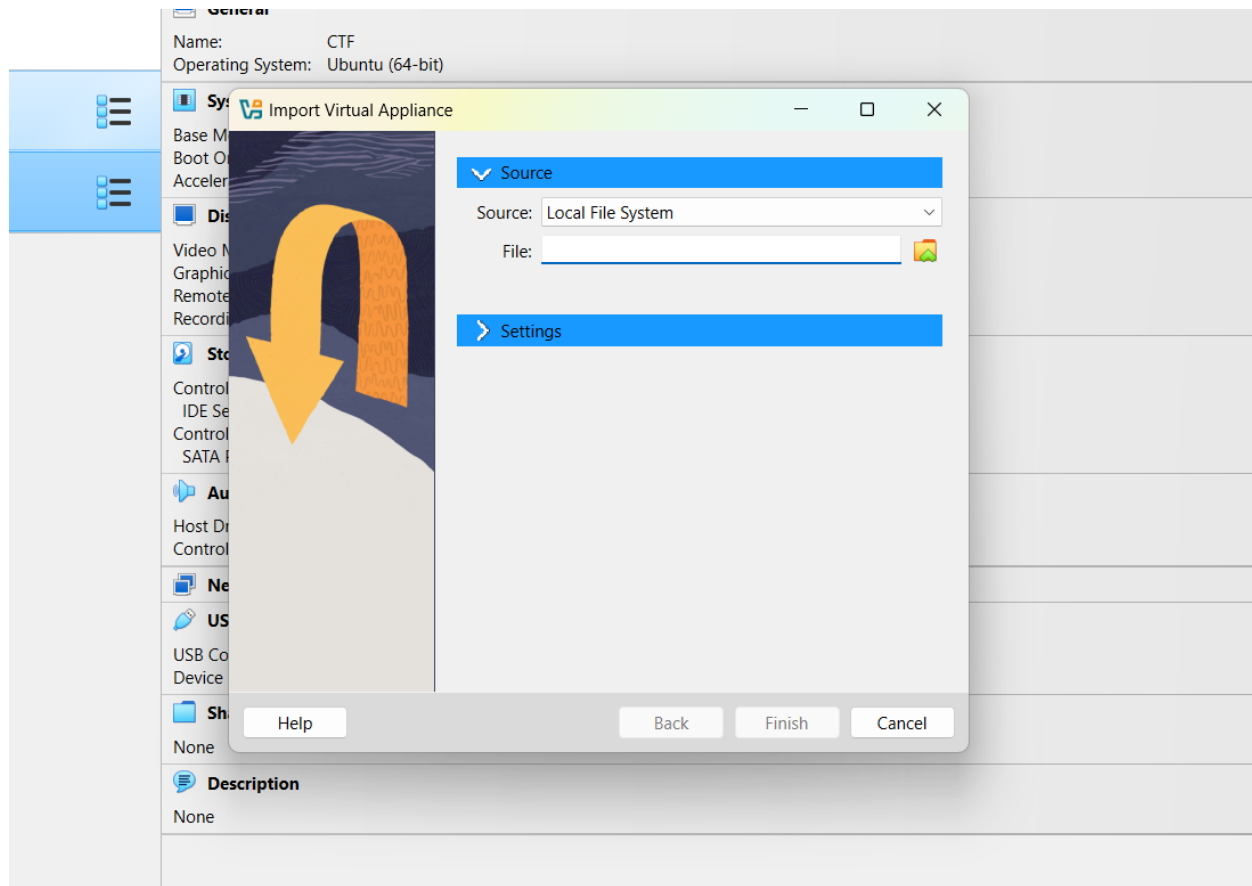
In this project the goal is to find all the six flags to do that we should follow few steps given below :-

Go to Lms download the files ctf and common.txt then open virtual box there is a file option at the top left upload the ctf file from there.

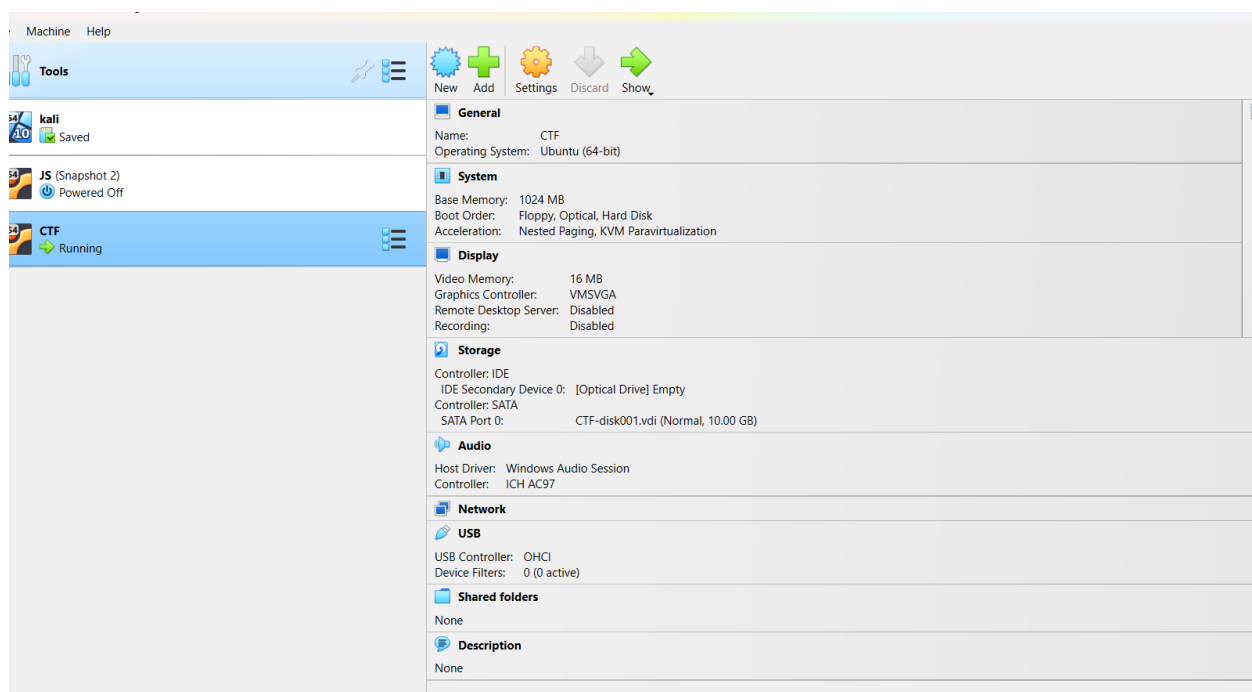
After clicking file option we have this import appliance click it .



Now choose the location from desktop and upload ctf and finish it.



now in the below picture we can clearly see ctf lab imported then click start which is indicated by small arrow.



The lab will be started and the ip will be displayed.

```
Ubuntu 22.04.1 LTS edureka tty1

Machine IP: 192.168.1.5
edureka login: [ 31.539878] cloud-init[998]: Cloud-init v. 22.2-0ubuntu1~22.04.3 running 'modules:
config' at Sat, 10 May 2025 07:51:40 +0000. Up 31.37 seconds.
[ 32.154853] cloud-init[1015]: Cloud-init v. 22.2-0ubuntu1~22.04.3 running 'modules:final' at Sat,
10 May 2025 07:51:40 +0000. Up 32.06 seconds.
[ 32.332505] cloud-init[1015]: Cloud-init v. 22.2-0ubuntu1~22.04.3 finished at Sat, 10 May 2025 07
:51:41 +0000. Datasource DataSourceNone. Up 32.32 seconds
[ 32.334107] cloud-init[1015]: 2025-05-10 07:51:41,100 - cc_final_message.py[WARNING]: Used fallback
datasource
```

Now open kali linux and to find all the flags we need to gather some information of this ctf lab so we use nmap to know more about .

Use the command :`sudo nmap -v -A 192.168.1.5`

```
kali@kali:~$ sudo nmap -v -A 192.168.1.5
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-10 03:59 EDT
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 03:59
Completed NSE at 03:59, 0.00s elapsed
Initiating NSE at 03:59
Completed NSE at 03:59, 0.00s elapsed
Initiating NSE at 03:59
Completed NSE at 03:59, 0.00s elapsed
Initiating ARP Ping Scan at 03:59
Scanning 192.168.1.5 [1 port]
Completed ARP Ping Scan at 03:59, 0.12s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 03:59
Completed Parallel DNS resolution of 1 host. at 03:59, 0.04s elapsed
Initiating SYN Stealth Scan at 03:59
Scanning 192.168.1.5 [1000 ports]
Discovered open port 80/tcp on 192.168.1.5
Discovered open port 21/tcp on 192.168.1.5
Discovered open port 22/tcp on 192.168.1.5
Completed SYN Stealth Scan at 03:59, 4.74s elapsed (1000 total ports)
Initiating Service scan at 03:59
Scanning 3 services on 192.168.1.5
Completed Service scan at 03:59, 6.15s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against 192.168.1.5
Retrying OS detection (try #2) against 192.168.1.5
NSE: Script scanning 192.168.1.5.
Initiating NSE at 03:59
NSE: [ftp-bounce] PORT response: 500 Illegal PORT command.
Completed NSE at 04:00, 30.51s elapsed
Initiating NSE at 04:00
Completed NSE at 04:00, 0.15s elapsed
Initiating NSE at 04:00
Completed NSE at 04:00, 0.00s elapsed
Nmap scan report for 192.168.1.5
Host is up (0.0019s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
20/tcp    closed ftp-data
```

```
kali@kali: ~  
File Actions Edit View Help  
PORT    STATE SERVICE  VERSION  
20/tcp  closed ftp-data  
21/tcp  open  ftp      vsftpd 3.0.5  
| ftp-anon: Anonymous FTP login allowed (FTP code 230)  
|_ Can't get directory listing: TIMEOUT  
| ftp-syst:  
|   STAT:  
| FTP server status:  
|   Connected to ::ffff:192.168.1.100  
|   Logged in as ftp  
|   TYPE: ASCII  
|   No session bandwidth limit  
|   Session timeout in seconds is 300  
|   Control connection is plain text  
|   Data connections will be plain text  
|   At session startup, client count was 1  
|   vsFTPD 3.0.5 - secure, fast, stable  
|_ End of status  
22/tcp  open  ssh      OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol 2.0)  
| ssh-hostkey:  
|   256 21:ed:bf:e2:7c:62:18:0d:5c:94:23:6f:5b:10:5d:12 (ECDSA)  
|   256 17:db:f4:63:63:b2:fe:38:7b:d0:12:b0:71:1a:ab:70 (ED25519)  
80/tcp  open  http     Apache httpd 2.4.52 ((Ubuntu))  
|_ http-server-header: Apache/2.4.52 (Ubuntu)  
|_ http-title: Travel Blog  
| http-robots.txt: 1 disallowed entry  
|_/  
|_ http-methods:  
|_ Supported Methods: OPTIONS HEAD GET POST  
443/tcp closed https  
8080/tcp closed http-proxy  
MAC Address: 08:00:27:14:4D:28 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
Aggressive OS guesses: Linux 5.0 - 5.14 (98%), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3) (98%), Linux 4.15 - 5.19 (94%), OpenWrt 21.02 (Linux 5.4) (94%), Linux 2.6.32 - 3.13 (93%), Linux 5.1 - 5.15 (93%), Linux 6.0 (93%), Linux 2.6.39 (93%), OpenWrt 22.03 (Linux 5.10) (93%), Linux 4.19 (92%)  
No exact OS matches for host (test conditions non-ideal).  
Uptime guess: 26.353 days (since Sun Apr 13 19:32:20 2025)  
Network Distance: 1 hop  
TCP Sequence Prediction: Difficulty=259 (Good luck!)  
IP ID Sequence Generation: ALL zeros  
Service Info: OSs: Unix, Linux; CPE: o:/o:linux:linux_kernel  
  
TRACEROUTE
```

```
kali@kali: ~  
File Actions Edit View Help  
|_End of status  
22/tcp open  ssh      OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol 2.0)  
|_ssh-hostkey:  
| 256 21:ed:bf:e2:7c:62:18:0d:5c:94:23:6f:5b:10:5d:12 (ECDSA)  
| 256 17:d8:f4:63:63:b2:fe:38:7b:d0:12:b0:71:1a:ab:70 (ED25519)  
80/tcp open  http      Apache httpd 2.4.52 ((Ubuntu))  
|_http-server-header: Apache/2.4.52 (Ubuntu)  
|_http-title: Travel Blog  
|_http-robots.txt: 1 disallowed entry  
|_  
|_http-methods:  
|_Supported Methods: OPTIONS HEAD GET POST  
443/tcp closed https  
8080/tcp closed http-proxy  
MAC Address: 08:00:27:14:4D:28 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
Aggressive OS guesses: Linux 5.0 - 5.14 (98%), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3) (98%), Linux 4.15 - 5.19 (94%), OpenWrt 21.02 (Linux 5.4) (94%), Linux 2.6.32 - 3.13 (93%), Linux 5.1 - 5.15 (93%), Linux 6.0 (93%), Linux 2.6.39 (93%), OpenWrt 22.03 (Linux 5.10) (93%), Linux 4.19 (92%)  
No exact OS matches for host (test conditions non-ideal).  
Uptime guess: 26.353 days (since Sun Apr 13 19:32:20 2025)  
Network Distance: 1 hop  
TCP Sequence Prediction: Difficulty=259 (Good luck!)  
IP ID Sequence Generation: All zeros  
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel  
  
TRACEROUTE  
HOP RTT ADDRESS  
1 1.92 ms 192.168.1.5  
  
NSE: Script Post-scanning.  
Initiating NSE at 04:00  
Completed NSE at 04:00, 0.00s elapsed  
Initiating NSE at 04:00  
Completed NSE at 04:00, 0.00s elapsed  
Initiating NSE at 04:00  
Completed NSE at 04:00, 0.00s elapsed  
Read data files from: /usr/share/nmap  
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 46.52 seconds  
Raw packets sent: 2053 (93.736KB) | Rcvd: 33 (2.068KB)  
  
kali@kali:~$
```

We can find the details here like ftp login is allowed by name anonymous so to login use the command :

[ftp 192.168.1.5](ftp://192.168.1.5)

ftp>ls

```
kali@kali: ~  
File Actions Edit View Help  
226 Directory send OK.  
ftp> chmod 777 flag1.txt  
421 Timeout.  
ftp> ls  
Not connected.  
ftp> exit  
  
kali@kali:~$ ftp 192.168.1.5  
Connected to 192.168.1.5.  
220 (vsFTPd 3.0.5)  
Name (192.168.1.5:kali): anonymous  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> ls  
229 Entering Extended Passive Mode (|||39565|)  
ftp: Can't connect to '192.168.1.5:39565': 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> ftp> get flag1.txt  
?Invalid command.  
ftp> nano flag1.txt  
?Invalid command.  
ftp> edit flag1.txt  
usage: edit [ on | off ]  
ftp> edit on  
Editing mode on.  
ftp> flag1.txt  
?Invalid command.  
ftp> edit flag1.txt  
usage: edit [ on | off ]  
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 3.25 KiB/s 00:00 ETA  
226 Transfer complete.  
33 bytes received in 00:00 (2.46 KiB/s)  
ftp>
```

```
kali@kali ~  
File Actions Edit View Help  
| http-robots.txt: 1 disallowed entry  
|_/   
| http-methods:  
|_ Supported Methods: OPTIONS HEAD GET POST  
443/tcp closed https  
8080/tcp closed http-proxy  
MAC Address: 08:00:27:14:4D:28 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
Aggressive OS guesses: Linux 5.0 - 5.14 (98%), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3) (98%), Linux 4.15 - 5.19 (94%), OpenWrt 21.02 (Linux 5.4) (94%), Linux 2.6.32 - 3.13 (93%), Linux 5.1 - 5.15 (93%), Linux 3.10 - 3.16 (93%), Linux 2.6.18 - 2.6.32 (93%), Linux 2.6.39 (93%), OpenWrt 22.03 (Linux 5.10) (93%), Linux 4.19 (92%)  
No exact OS matches for host (test conditions non-ideal).  
Uptime guess: 26.353 days (since Sun Apr 13 19:32:20 2025)  
Network Distance: 1 hop  
TCP Sequence Prediction: Difficulty=259 (Good luck!)  
IP ID Sequence Generation: All zeros  
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel  
  
TRACEROUTE  
HOP RTT ADDRESS  
1 1.92 ms 192.168.1.5  
  
NSE: Script Post-scanning.  
Initiating NSE at 04:00  
Completed NSE at 04:00, 0.00s elapsed  
Initiating NSE at 04:00  
Completed NSE at 04:00, 0.00s elapsed  
Initiating NSE at 04:00  
Completed NSE at 04:00, 0.00s elapsed  
Read data files from: /usr/share/nmap  
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 46.52 seconds  
Raw packets sent: 2053 (93.736KB) | Rcvd: 33 (2.068KB)  
  
kali@kali ~$  
kali@kali ~$ pwd  
/home/kali  
kali@kali ~$  
kali@kali ~$ cat flag1.txt  
b0923112d59c477a94c9998379152258  
kali@kali ~$  
kali@kali ~$
```

Here by using get flag1.txt we have downloaded flag1.txt file to home directory

So see the content use the command cat flag1.txt.

To know whether there are directories or not we can use dirb command

dirb http:// 192.168.1.5 comman.txt

```
kali@kali ~/Desktop  
File Actions Edit View Help  
START TIME: Sat May 3 09:38:21 2025  
URL BASE: http://192.168.167.184/  
WORDLIST_FILES: common.txt  
  
/images  
GENERATED WORDS: 4614  
Scanning URL: http://192.168.167.184/ Description  
(!) FATAL: Too many errors connecting to host  
(Possible cause: COULDN'T CONNECT)  
  
END TIME: Sat May 3 09:39:24 2025 10:23:13AM  
DOWNLOADED: 0 - FOUND: 0  
kali@kali ~/Desktop$  
$ dirb http://192.168.1.4 common.txt 23 DIRB  
10:23:13AM 10:23:13AM  
DIRB v2.22 10:23:13AM 10:23:13AM  
By The Dark Raver 10:23:13AM 10:23:13AM  
START TIME: Sat May 3 09:41:46 2025 10:23:20AM  
URL BASE: http://192.168.1.4/ 10:23:20AM  
WORDLIST_FILES: common.txt 10:23:20AM  
  
/images  
GENERATED WORDS: 4614  
Scanning URL: http://192.168.1.4/ Description  
=> DIRECTORY: http://192.168.1.4/css/  
=> DIRECTORY: http://192.168.1.4/images/  
+ http://192.168.1.4/index.html (CODE:200|SIZE:2683)  
=> DIRECTORY: http://192.168.1.4/js/  
=> DIRECTORY: http://192.168.1.4/pages/  
+ http://192.168.1.4/robots.txt (CODE:200|SIZE:74)  
+ http://192.168.1.4/serve-status (CODE:403|SIZE:276)  
=> DIRECTORY: http://192.168.1.4/admin/
```



```
File Actions Edit View Help
=> DIRECTORY: http://192.168.1.4/pages/
+ http://192.168.1.4/robots.txt (CODE:200|SIZE:71)
+ http://192.168.1.4/server-status (CODE:403|SIZE:276)
=> DIRECTORY: http://192.168.1.4/admin/
=> DIRECTORY: http://192.168.1.4/c0nfig/

-- Entering directory: http://192.168.1.4/css/ --
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

-- Entering directory: http://192.168.1.4/images/ --
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

-- Entering directory: http://192.168.1.4/js/ --
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

-- Entering directory: http://192.168.1.4/pages/ --
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

-- Entering directory: http://192.168.1.4/4dm1n/ --
+ http://192.168.1.4/4dm1n/index.html (CODE:200|SIZE:2407)

-- Entering directory: http://192.168.1.4/c0nfig/ --
+ http://192.168.1.4/c0nfig/index.php (CODE:200|SIZE:69739)

END_TIME: Sat May 3 09:41:59 2025
DOWNLOADED: 13842 - FOUND: 5

(kali@kali) ~/Desktop
$ xdg-open common.txt

(kali@kali) ~/Desktop
$ echo "TFm0ExRb0tabXh0wn1BmK1DMctJREJpTxpFNfphSTRaak3rTldJek9HTTJaRE0WldSBESXVX1ZV1kzTVdNekNnb3RMUzB0" | base64 -d
LS0tLQoKZmxhZyA2IC0tIDBIMzE4ZGI4ZjBkNWJlZGMzMGM4ZWRLNWUyYWY3MMMzMzCgotLS0t

(kali@kali) ~/Desktop
$
```

We can open all the directories one by one

When we open robot.txt there is flag2

```
File Actions Edit View Help
./mozilla/firefox/qy8lrba6.default/times.json
./mozilla/firefox/installs.ini
./mozilla/firefox/Pending Pings
./mozilla/firefox/Crash Reports
./mozilla/firefox/Crash Reports/events
./mozilla/firefox/Crash Reports/InstallTime20240115170312
./backup.zip
./java
./java/.userPrefs
./java/.userPrefs/burp
./java/.userPrefs/burp/prefs.xml
./java/.userPrefs/burp/community
./java/.userPrefs/burp/community/prefs.xml
./java/.userPrefs/burp/community/detached-frames
./java/.userPrefs/burp/community/detached-frames/prefs.xml
./java/.userPrefs/.userRootModFile.kali
./java/.userPrefs/.user.lock.kali
./java/fonts
./java/fonts/21.0.7-ea
./java/fonts/21.0.7-ea/fcinfo-1-kali-kali-2025.1-en-US.properties

(kali@kali) ~
$ curl http://192.168.1.5/robots.txt
curl http://192.168.1.5/sitemap.xml

User-agent: *

Disallow: /

Flag 2 -> 930f04eb6ff0eb864b2157dd2aa048c6
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.52 (Ubuntu) Server at 192.168.1.5 Port 80</address>
</body></html>

(kali@kali) ~
$
```

Type curl <http://192.168.1.5/robot.txt>.

When we open blogcomponent directory we easily found flag3 by using the same curl command.

```
File Actions Edit View Help
</nav>

<main class="container">
  <div class="custom-container">
    <h1>Los Angeles Travel Guide</h1>
    <h2>Last Updated: August 2, 2018</h2>
    
    <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 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.</p>
      <p>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.</p>
      <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 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 $10-15 for a meal and drink. Prices go up from there and the sky is the limit.

      Transportation costs - LA is very big and sprawling. Even if something seems close, distances can be deceiving as traffic is heavy. Although public transportation exists, LA is not a public transportation-friendly city. LA has a metro but it doesn't go too many places. The bus system is better but it is also subject to the heavy traffic. A single fare valid on the bus or the metro is $1.75 and be purchased from ticket vending machines in the stations. Week-long passes can be bought using the TAP card system, a rechargeable system. If you want to get out of the city center, you'll need a car. If you're not renting a car, then Uber or Lyft aren't too bad on the wallet if used sparingly. For example, Beverly Hills to Hollywood costs about $7-10 (UberX costs about $1 per mile). Taxis are expensive and have a base fare of $3 and cost about $3 per mile. For shorter distances, you can use Lime or Bird, two ridesharing companies that provide dockless scooter rentals around the city. Just download the app for either Bird or Lime and find a nearby scooter. They cost 1 USD to rent and then fifteen cents for every minute after. It's a great budget-friendly way to go shorter distances in the city.
    </span>
  </div>
</main>

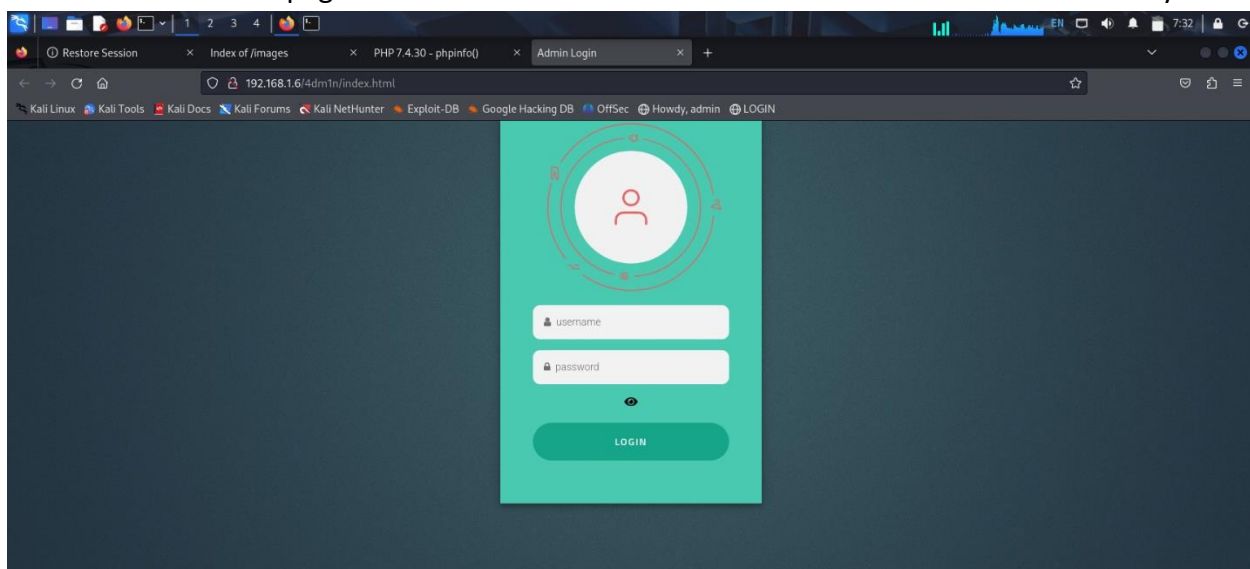
<div class="clear-div"></div>

<footer class="footer">
  <p>← flag 3 → b35e7489cf89d4188c85d921a2f79821 →</p>
</footer>

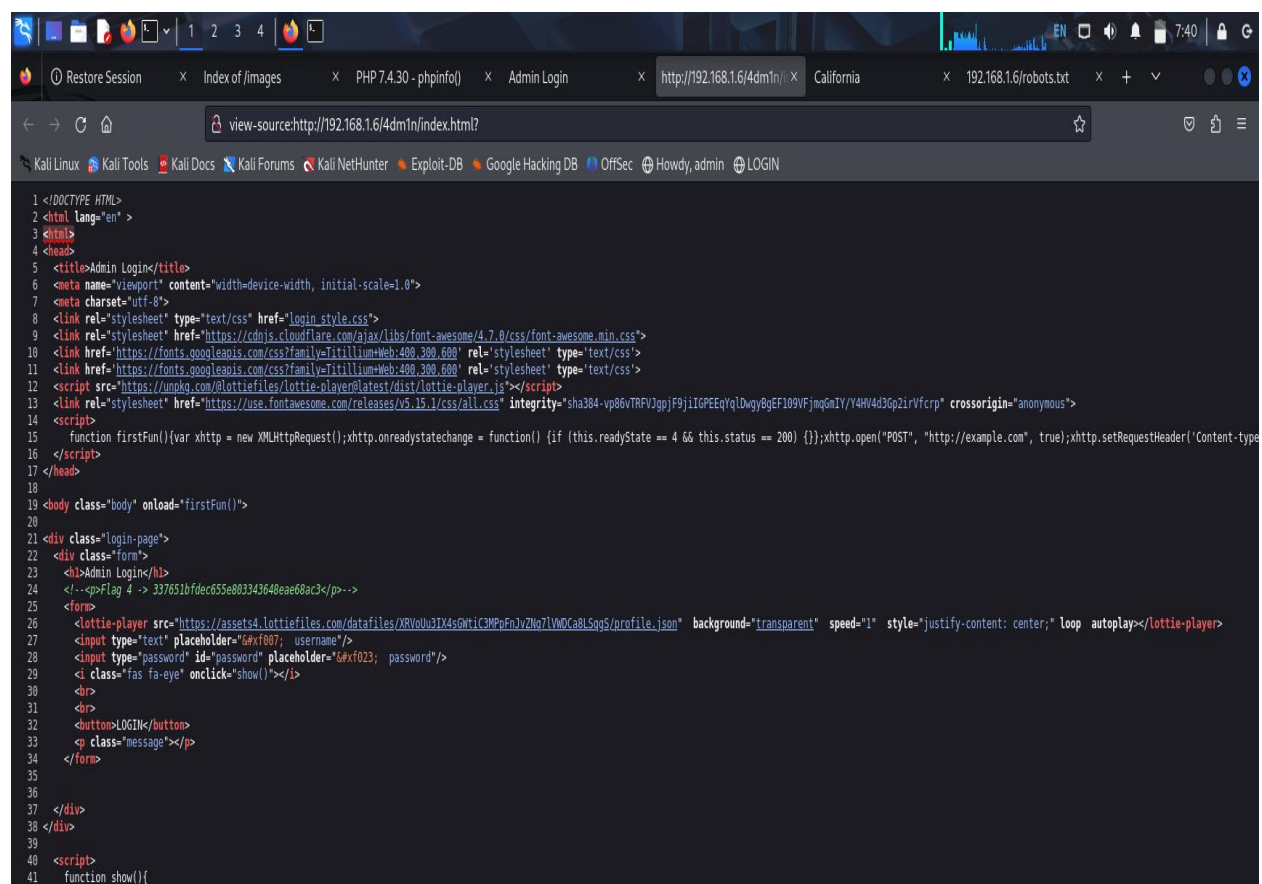
<script src="../../../js/app.js"></script>
</body>
</html>

(kali@kali) ~$
```

There is also a admin page. Index.html here when we click view source code we can easily

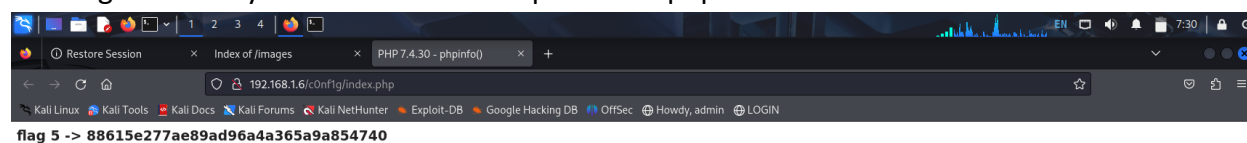


Find flag4 which is shown below.



```
1 <!DOCTYPE HTML>
2 <html lang="en" >
3 <html>
4 <head>
5 <title>Admin Login</title>
6 <meta name="viewport" content="width=device-width, initial-scale=1.0">
7 <meta charset="utf-8">
8 <link rel="stylesheet" type="text/css" href="login_style.css">
9 <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.min.css">
10 <link href="https://fonts.googleapis.com/css?family=TitilliumWeb:400,300,600" rel="stylesheet" type="text/css">
11 <link href="https://fonts.googleapis.com/css?family=TitilliumWeb:400,300,600" rel="stylesheet" type="text/css">
12 <script src="https://unpkg.com/@lottiefiles/lottie-player@latest/dist/lottie-player.js"></script>
13 <link rel="stylesheet" href="https://use.fontawesome.com/releases/v5.15.1/css/all.css" integrity="sha384-vp86vTRFVJgpjF9jIGPEEQqDwgYB9GEFJ99VFjmqGmIVY4H4V43p2irVfcrp" crossorigin="anonymous">
14 <script>
15     function firstFun(){var xhttp = new XMLHttpRequest();xhttp.onreadystatechange = function() {if (this.readyState == 4 && this.status == 200) {}};xhttp.open("POST", "http://example.com", true);xhttp.setRequestHeader('Content-type
16 </script>
17 </head>
18
19 <body class="body" onload="firstFun()">
20
21 <div class="login-page">
22 <div class="form">
23 <h1>Admin Login</h1>
24 <!--<Flag 4 --> 337651b6dec655e803343640eae8ac3</p-->
25 <form>
26 <lottie-player src="https://assets4.lottiefiles.com/datafiles/XRv0u31X4sGiti(3MPpFn)/2No7LVMDCa8LSqgS/profile.json" background="transparent" speed="1" style="justify-content: center;" loop autoplay></lottie-player>
27 <input type="text" placeholder="Username" />
28 <input type="password" id="password" placeholder="Password" />
29 <i class="fas fa-eye" onclick="show()"></i>
30 <br>
31 <br>
32 <button>LOGIN</button>
33 <p class="message"></p>
34 </form>
35
36 </div>
37 </div>
38 </div>
39
40 <script>
41     function show(){
```

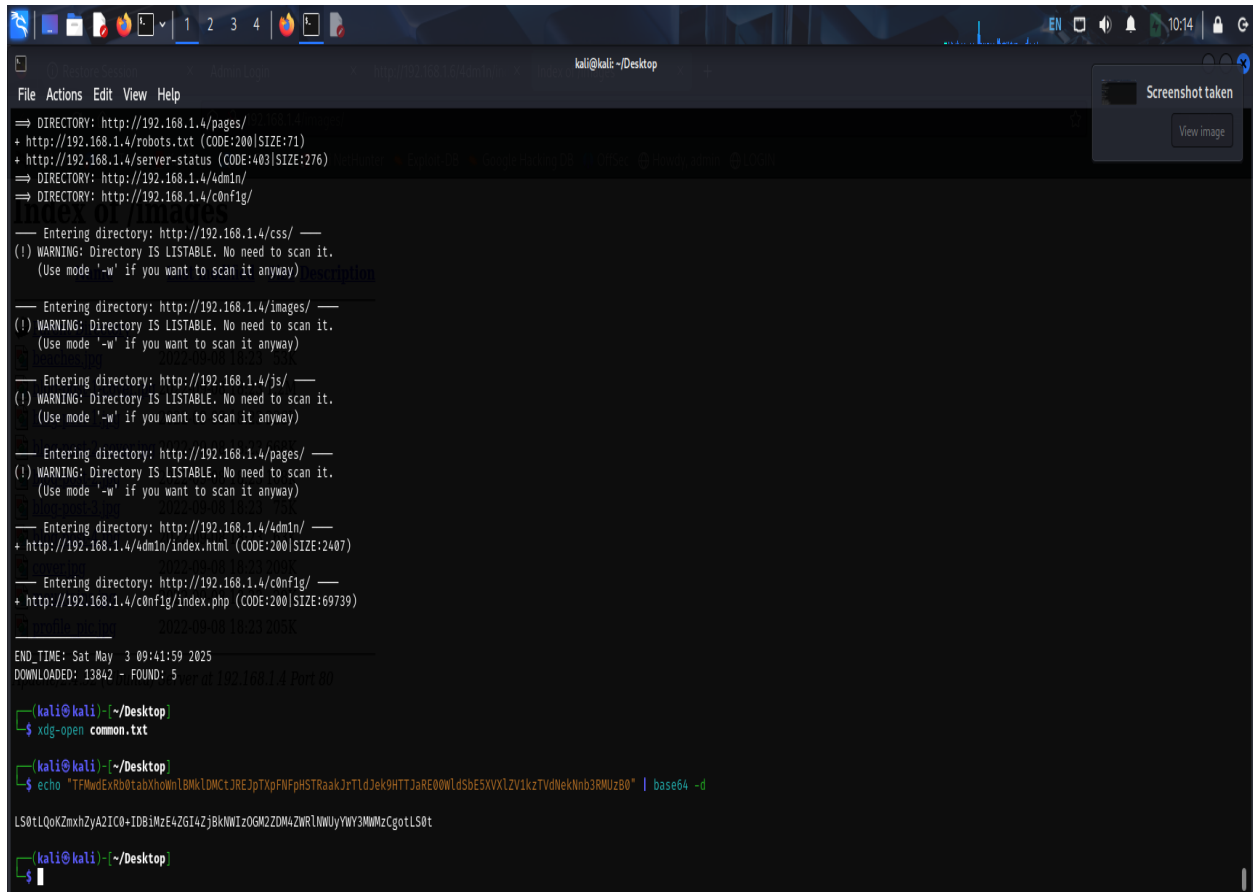
The flag5 is directly available when we open index.php file



```
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

Now the last flag is double hashed and it is found in config file



```
⇒ DIRECTORY: http://192.168.1.4/pages/
+ http://192.168.1.4/robots.txt (CODE:200|SIZE:71)
+ http://192.168.1.4/server-status (CODE:403|SIZE:276)
⇒ DIRECTORY: http://192.168.1.4/4admin/
⇒ DIRECTORY: http://192.168.1.4/c0nf1g/

— Entering directory: http://192.168.1.4/css/ —
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

— Entering directory: http://192.168.1.4/images/ —
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

— Entering directory: http://192.168.1.4/js/ —
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

— Entering directory: http://192.168.1.4/pages/ —
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

— Entering directory: http://192.168.1.4/4admin/ —
+ http://192.168.1.4/4admin/index.html (CODE:200|SIZE:2407)

— Entering directory: http://192.168.1.4/c0nf1g/ —
+ http://192.168.1.4/c0nf1g/index.php (CODE:200|SIZE:69739)

END TIME: Sat May 3 09:41:59 2025
DOWNLOADED: 13842 ~ FOUND: 5

kali@kali: ~/Desktop
$ xdg-open common.txt

kali@kali: ~/Desktop
$ echo "TFMudExRb0tabXhoNn1BMK1DMctJREJpTXpFNfphSTRaakJrTldJek9HTTJaRE00WldSbE5XVX1ZV1kzTVdNekNnb3RMUz80" | base64 -d

LS0tLQoKZmxhZyA2IC0=IDB1MzE4ZGI4ZjBkNW1zOGM2ZDM4ZWRLNWUyYWY3MmMzCgotLS0t

kali@kali: ~/Desktop
$
```

We use base64 to decrypt it and again we get a hash so we should decrypt it using base64

Command is: echo “nycwekkkkkkkkkk3456” | base64 -d

We found all the flags .

```
File Actions Edit View Help
(1) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
--- Entering directory: http://192.168.1.4/pages/ ---
(1) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
--- Entering directory: http://192.168.1.4/admin/ ---
+ http://192.168.1.4/admin/index.html (CODE:200|SIZE:2407) 100%
--- Entering directory: http://192.168.1.4/cnfig/ ---
+ http://192.168.1.4/cnfig/index.php (CODE:200|SIZE:69739) 100%
-----
2023-09-08 18:23 50K
END_TIME: Sat May 3 09:41:59 2025 18:23 1.23K
DOWNLOADED: 13842 - FOUND: 5
2023-09-08 18:23 200K
kali@kali: ~/Desktop
$ xdg-open common.txt 18:23 600K
2023-09-08 18:23 100K
kali@kali: ~/Desktop
$ echo "TFMwExB0tabXh0wn1BMkLDMc1JREjPjTXpFNfPhSTRaakJrTldJek9HTTJaRE00WldSbE5XXV1ZV1kzTVdNekNnb3RMUzB0" | base64 -d
LS0tLQoKZmxhZyA2IC0+IDBiMzE4ZGI4ZjBKNWZiOGM2ZDM4ZWRLNWJyYWY3MmMzCgotLS0t
2023-09-08 18:23 100K
kali@kali: ~/Desktop
$ echo "LS0tLQoKZmxhZyA2IC0+IDBiMzE4ZGI4ZjBKNWZiOGM2ZDM4ZWRLNWJyYWY3MmMzCgotLS0t" | base64 -d
TFMwExB0tabXh0wn1BMkLDMc1JREjPjTXpFNfPhSTRaakJrTldJek9HTTJaRE00WldSbE5XXV1ZV1kzTVdNekNnb3RMUzB0
2023-09-08 18:23 200K
base64: invalid input
Server at 192.168.1.4 Port 80
kali@kali: ~/Desktop
$ echo "LS0tLQoKZmxhZyA2IC0+IDBiMzE4ZGI4ZjBKNWZiOGM2ZDM4ZWRLNWJyYWY3MmMzCgotLS0t" | base64 -d
TFMwExB0tabXh0wn1BMkLDMc1JREjPjTXpFNfPhSTRaakJrTldJek9HTTJaRE00WldSbE5XXV1ZV1kzTVdNekNnb3RMUzB0
Flag 6 -> 0b318dbf0d5b38cd38ede5e2af71c3
kali@kali: ~/Desktop
$
```