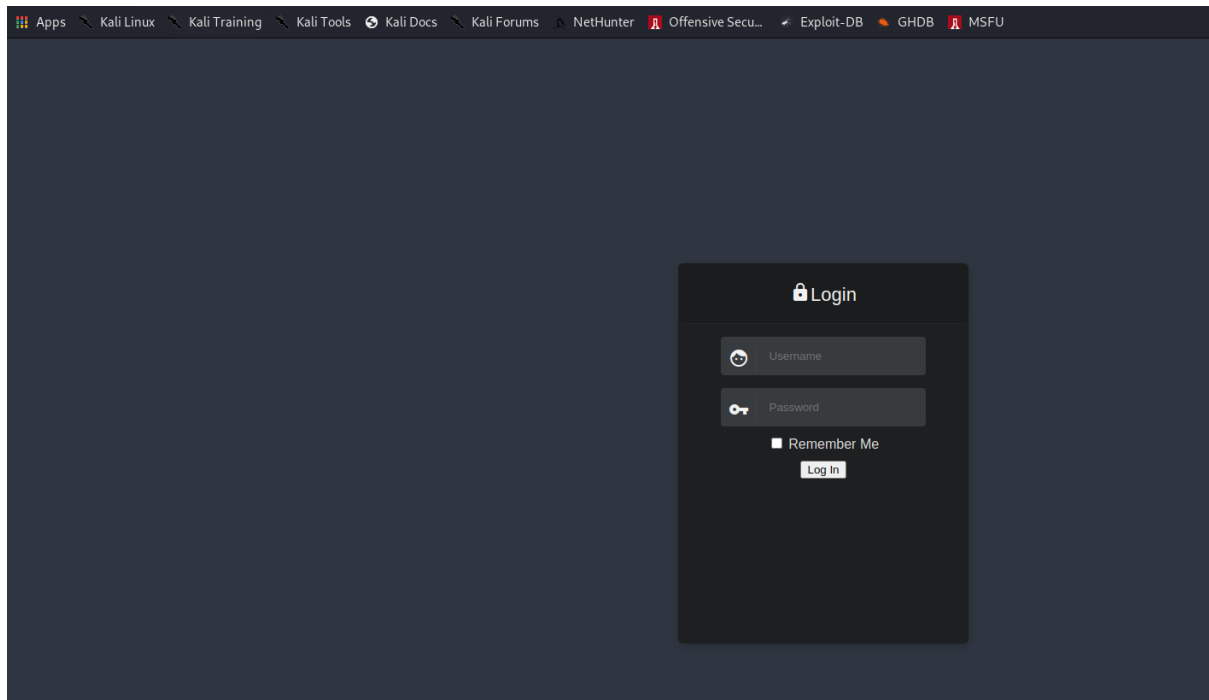
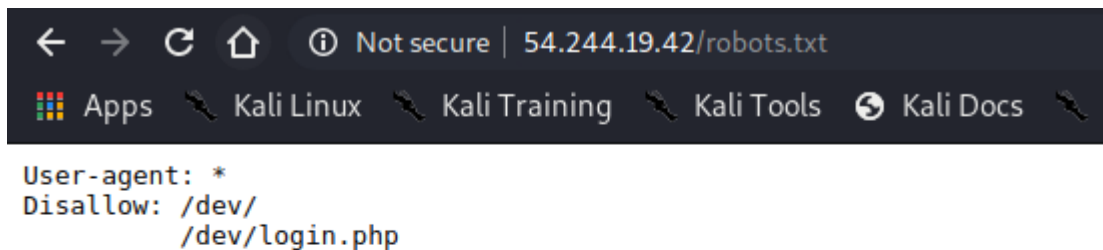


Walkthrough by Sneha Surana

A login page with user name and password we need them to get enter into account



Since we don't have both username and password let check robots.txt that tells about allowed and disallowed path



We got to disallowed But lets check it



This page only accepts POST request



Both the paths were not useful. Let's have look on Source code

```
<script>
function loginFunction() {
  var username = document.getElementById("username").value;
  var password = document.getElementById("password").value;
  var x = password.slice(0,9);
  var y = password.slice(9);
  var z = md5(y);
  console.log("reached");
  if (x == "\x43\x6C\x6F\x75\x64\x53\x45\x4B\x5F")
  {
    if (z == "06a3cccaafedc5b09b10b4b26f02a9e1")
    {
      //document.getElementById("msg").innerHTML = "Right";
      window.location = "./loader.php?p=bWVzc2FnZTFfdG9famFyZWQudHh0Cg%3D%3D&password=" + password;
    }
    else
    {
      document.getElementById("msg").innerHTML = "Try harder!";
    }
  }
  else
  {
    document.getElementById("msg").innerHTML = "Incorrect credentials";
  }
}
</script>
</html>
```

After understanding the code password is been sliced from 0 to 9 and stored in variable x and again password is sliced and stored to variable y and now md5 of the same

We got md5 z==0683..... and X='\x43\...

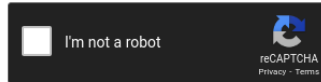
Let's decode it



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

06a3cccaafedc5b09b10b4b26f02a9e1



Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, rpeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1BackupDefaults

Hash	Type	Result
06a3cccaafedc5b09b10b4b26f02a9e1	md5	jeniffer

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

[Download CrackStation's Wordlist](#)

x43\x6C\x6F\x75\x64\x53\x45\x4B\x5F

Decode

Original code:

x43\x6C\x6F\x75\x64\x53\x45\x4B\x5F

Decoded results:

CloudSEK_

Since password is being sliced so that final password is **CloudSEK_jeniffer**

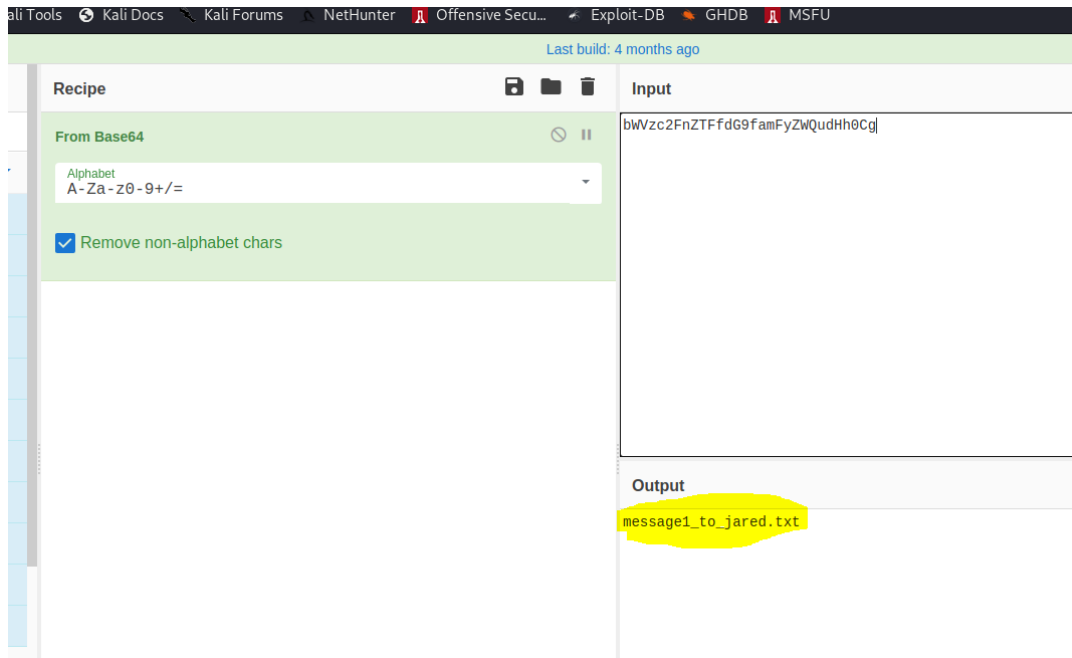
But we don't have user let look again at source code

```

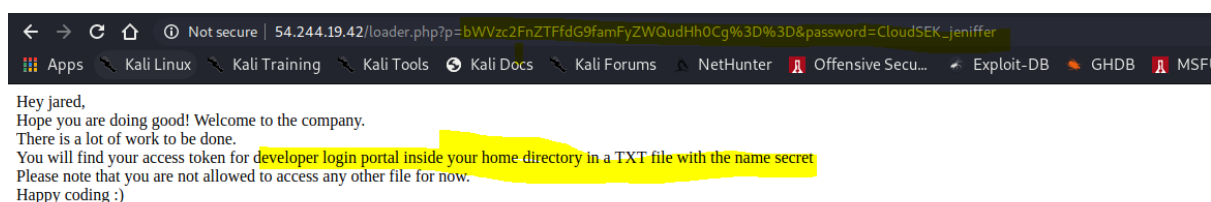
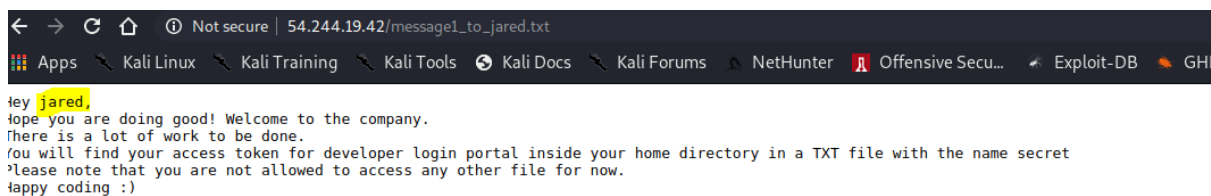
if (x == "\x43\x6C\x6F\x75\x64\x53\x45\x4B\x5F")
{
    if (z == "06a3cccaafedc5b09b10b4b26f02a9e1")
    {
        //document.getElementById("msg").innerHTML = "Right";
        window.location = "./loader.php?p=bWVzc2FnZTFfdG9famFyZWQudHh0Cg%3D%3D&password=" + password;
    }
    else
    {

```

We got base64 code Lets' decode it



After decoding we got a file and got a message



Since we need to find secret file in home directory Let use LDAP injection and try to add
'../../../../home/jared/secret.txt' . But it doesn't work and in the source code it accepting base64
Let convert '../../../../home/jared/secret.txt' to base 64

Last build: 4 months ago

Recipe

To Base64

Alphabet
A-Za-z0-9+/=

Input

../../../../home/jared/secret.txt

Output

Li4vLi4vLi4vLi4vaG9tZS9qYXJlZC9zZWNYZXQudHh0

And put in p= .After that we got access token as in hint it was mention about JWT

← → ↻ ⌂ ⓘ Not secure | 54.244.19.42/loader.php?p=Li4vLi4vLi4vLi4vaG9tZS9qYXJlZC9zZWNYZXQudHh0&password=CloudSEK_jeniffer

Apps Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Secu... Exploit-DB GHDB

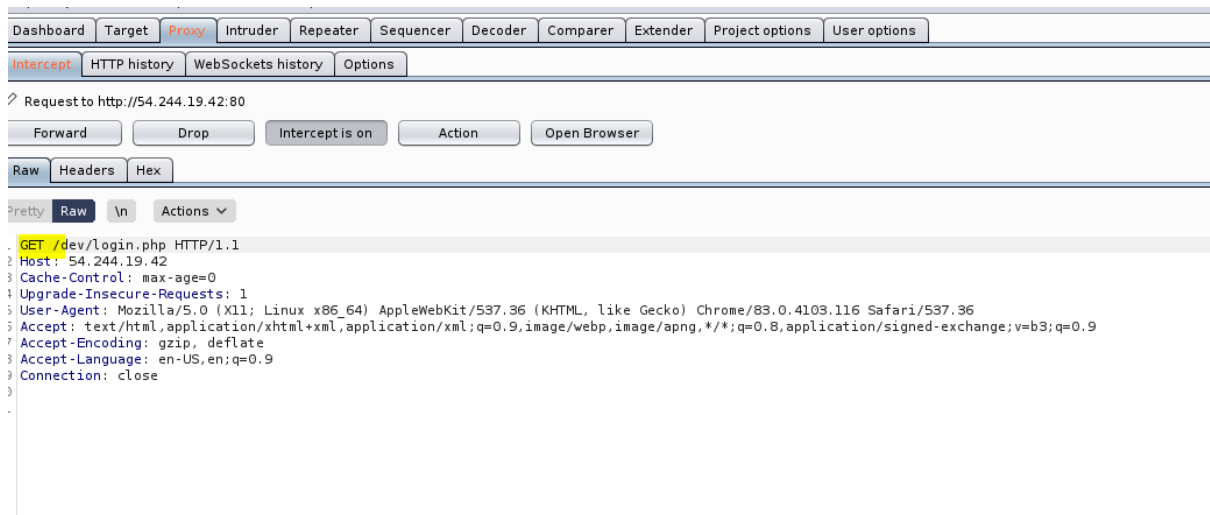
Hey jared, your access token for developer login portal is:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyJjoiamFyZWQifQ.9lYEicuJKZAqh8lAX4woWaBWGJ-bGIqWj_gsOsdVjGQ

← → × ⌂ ⓘ 54.244.19.42/dev/login.php

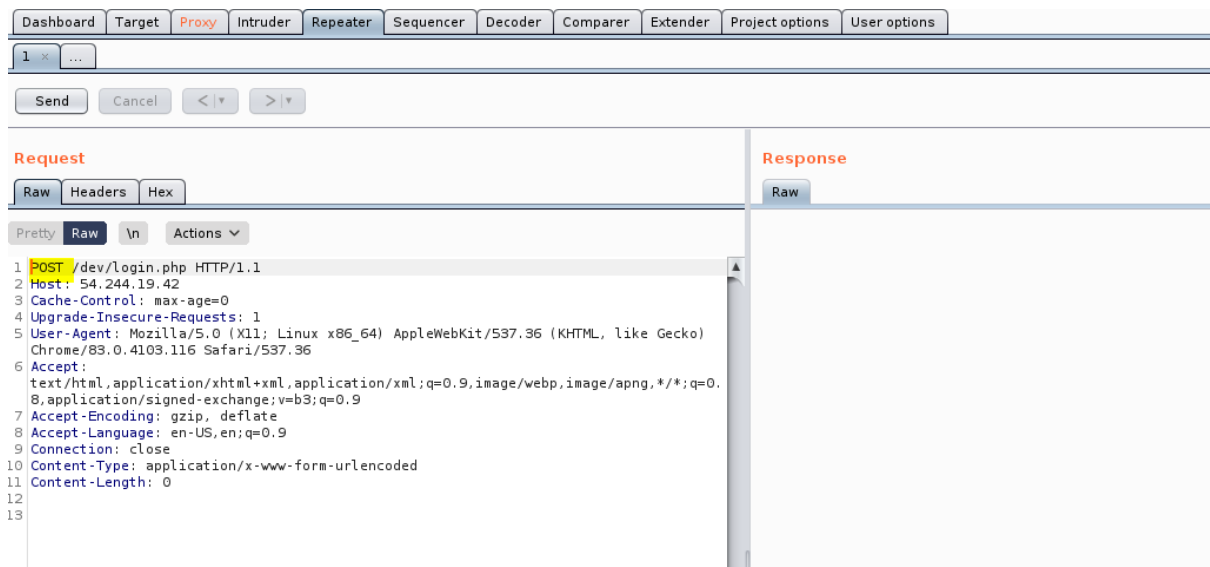
Apps Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Secu... Exploit-DB GHDB MSFU

This page only accepts POST request

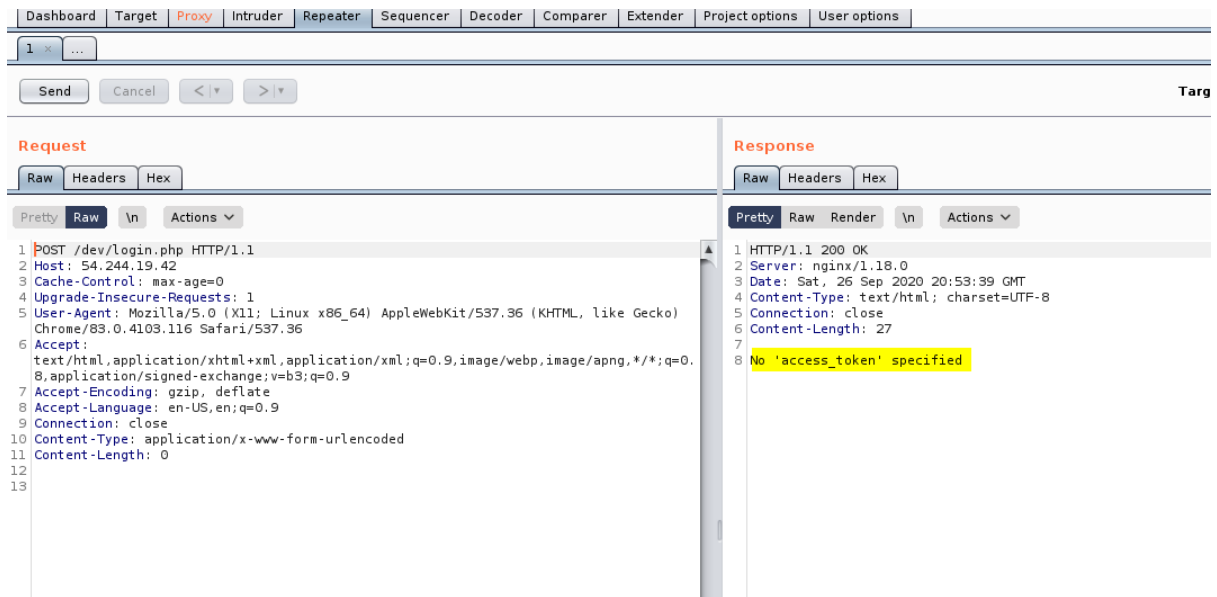
Let get the request normally in burpsuite by enabling foxy -proxy and send the request to repeater



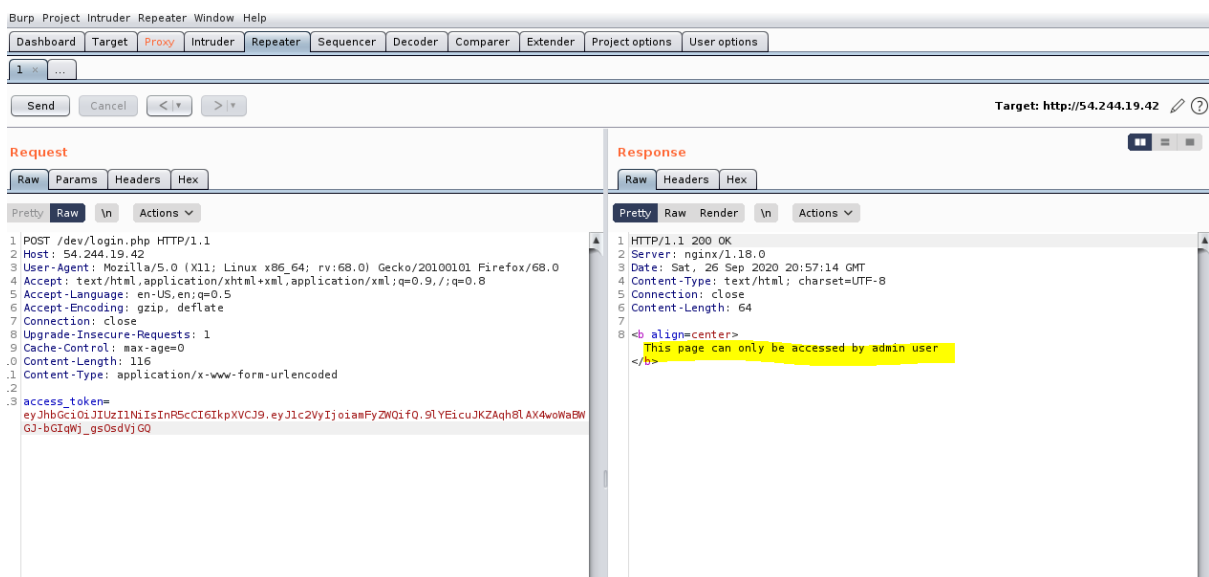
Click On Action button and Send to Repeater to make post request and change the request from GET to POST



Click on Send button



We need to add access_token in the Request .Now specify the access token in the request and post it We need to post request by admin user



Now as in hints JWT was mentioned let analyse access_token in it

Algorithm HS256

Encoded

PASTE A TOKEN HERE

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyIjoiamFyZWQifQ.91YEicuJKZAqh81AX4woWaBWGJ-bGIqWj_gs0sdVjGQ|

Decoded

EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

PAYLOAD: DATA

```
{
  "user": "jared"
}
```

VERIFY SIGNATURE

```
HMACSHA256(
    base64UrlEncode(header) + "." +
    base64UrlEncode(payload),
```

Now change user to admin and new access_token is generated Now let post request using it

Encoded

PASTE A TOKEN HERE

**eYJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.ey
JlcnVyaioiYWRTaW4ifQ.xLtlDUxXSGB7EqP49a
8xQziqpjkVKeJ9o2nix4xLf5M**

Decoded

EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

PAYLOAD: DATA

```
{
  "user": "admin"
}
```

VERIFY SIGNATURE

```

HMACSHA256(
    base64UrlEncode(header) + "." +
    base64UrlEncode(payload),

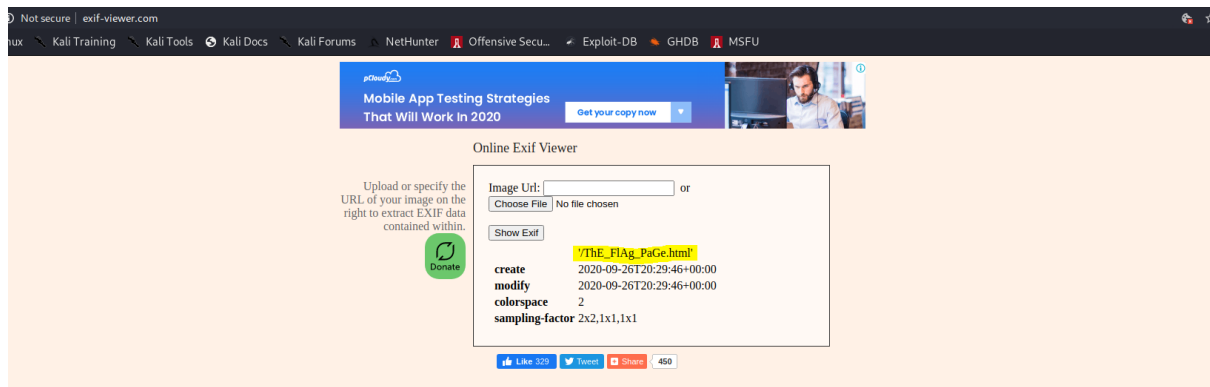
```


We got page and now we have analyse as mentioned in hint

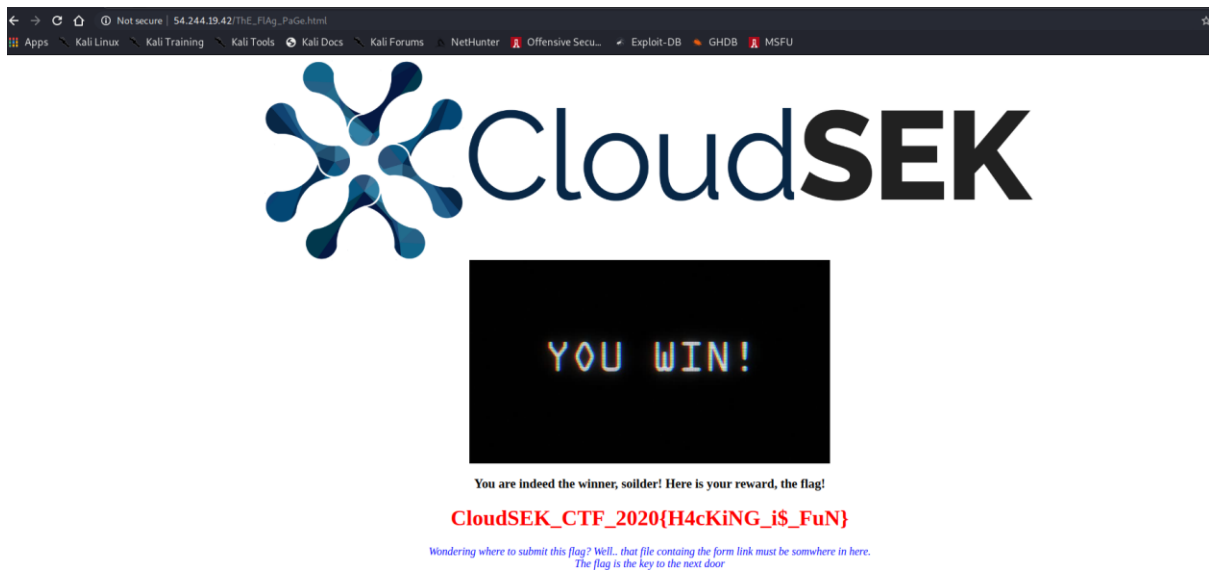


Ha ha ha! You are close! But the game isn't over yet!
If you will look in the dark, you will find your worth!
You can be a winner!

Let analyse this image and After using steghide ,zsteg, foremost and binwalk no result and examin meta data used online tool



We got again a new page and let enter



Again image this time there is flag also Run zsteg foremost binwalk no result now let run steghide and we have flag this can be password let's try

```
sneha@kali:~/Downloads$ steghide extract -sf you_are_winner_indeed_img.jpg
Enter passphrase:
wrote extracted data to "compl3tion_m3ssag3.txt".
```

Extracted the data got a file

```
sneha@kali:~/Downloads$ cat compl3tion_m3ssag3.txt
Congratulations on making it to the end!
Please submit a detailed walkthrough PDF along with proper steps and screenshots on the link below.
We hope to see you in the interview:
https://forms.gle/CA9vHT6XaisS9HgR6

Happy Hacking!

~CloudSEK family
```