

CLOUDSEK CTF WALKTHROUGH

MEENAKSHI R

In this report, I have explained in detail about how I solved the CTF (Capture The Flag) Challenge hosted by CloudSEK as a part of the EWYL Program. The target of the CTF is to get to the final page hosted by the team and submit it in a form. But where did the form come from? How did I access the form? This report is all about that!

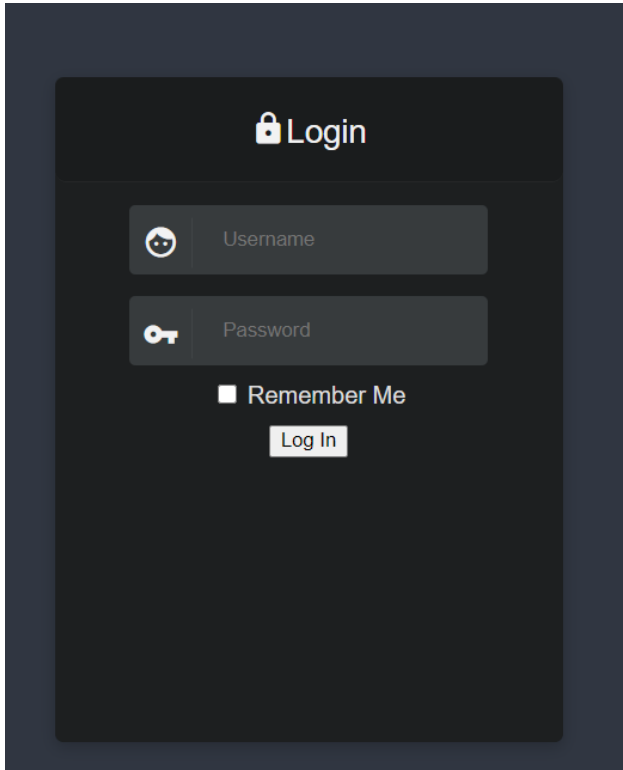
TABLE CONTENT OF THE REPORT

1. Find the credentials for the login page
2. Hello Jared!
3. JWT for developer login
4. Passing the access token in POST data
5. CloudSEK_to_win_page!
6. Captured the Flag! But is the challenge over?
7. Open the Final Door!

1. Find the credentials for the Login page

As the first step of the challenge, I was given a link of a webpage

Link <http://54.244.19.42/>



As anyone would have tried, I first entered my credentials but it didn't work. So I checked the source page. I was able to see that, for verification, the username was not checked, only the password was verified. Moreover, there were 2 parts for the password. The first part was base64 encoded. The next part was md5 hashed. With the help of online tools I was able to decode the passwords using open source online tools.

- **x43\x6C\x6F\x75\x64\x53\x45\x4B\x5F** First part of the password
- **06a3cccaafedc5b09b10b4b26f02a9e1** Second part of the password

CloudSEK_jeniffer is the password!

I was able to login without a username and just with the password!

2. Hello Jared!

After logging in, I got a message for Jared.

```
Hey jared,  
Hope you are doing good! Welcome to the company.  
There is a lot of work to be done.  
You will find your access token for developer login portal inside your home directory in a TXT file with the name secret  
Please note that you are not allowed to access any other file for now.  
Happy coding :)
```

From this page, I was supposed to find the access token for the developer login portal. It was mentioned that the file is in my (Jared's) home directory with the name "Secret". I was sure it was either '`C:\jared\home\secret.txt`' or '`/home/jared/secret.txt`'.

So I encoded the path (base64) using the open source tools available on the internet and replaced it in the link .

Original link

http://54.244.19.42/loader.php?p=bWVzc2FnZTFfdG9famFyZWQudHh0Cg%3D%3D&password=CloudSEK_jeniffer

Link I entered

http://54.244.19.42/loader.php?p=L2hvbWUvamFyZWQvc2VjcmV0LnR4dA==&password=CloudSEK_jeniffer

3. JWT For Developer login portal

Got the Access token! What next?

"Hey jared, your access token for developer login portal is:

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyIjoiamFyZWQifQ.9lYEicuJKZAqh8lAX4woWaBWGJ-bGIqWj_gsOsdVjGQ"

This message was the only message found on the link.

I checked the <http://54.244.19.42/robots.txt> to figure out how to get to the login portal .

```
User-agent: *  
Disallow: /dev/  
          /dev/login.php
```

I checked the first link, but <http://54.244.19.42/dev/> was forbidden. So I check the next link <http://54.244.19.42/dev/login.php> . It was mentioned that the page only accepts POST requests. That cleared my doubt about passing the access token.

4. Passing the access token in POST Data

I tried to use Burpsuite to pass the access token but I constantly faced some issues and got the error : “ No ‘access_token’ specified”. So I decided to use the curl command .

Curl -X POST <http://54.244.19.42/dev/login.php> -d access_token =
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyIjoiamFyZWQifQ.9lYEicuJKZAqh8lAX4woWaBWGJ-bGIqWj_gsOsdVjGQ

I got the message that the page can only be accessed by the admin user. I decided to decode the access token. As the token had two ‘ . ’ in them, it was clear that the access token was a **JSON Web token**. By decoding the access token, I found that, in the payload, the user was mentioned as *jared*.

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

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

If you will look in the dark, you will find your worth!

You can be a winner! “




I was not able to find any data in the source page or the quote. So I was pretty sure that the link for the next task would be hidden inside the above flag image. Using *Jeffrey's Image Metadata Viewer* I was able to find the link of the next task.

Jeffrey's Image Metadata Viewer

URL:

or... No file chosen

☐ I'm not a robot

 [View Image Data](#)

Jeffrey Friedl's Image Metadata Viewer
(How to use)

Some of my other stuff

- [My Blog](#) · [Lightroom plugins](#) · [Pretty Photos](#)
- ["Photo Tech"](#)

This tool remains available so long as I can keep it free and the bandwidth doesn't cost me too much. A gift of thanks is always appreciated, but certainly not required. [Send a gift via PayPal](#), or perhaps an Amazon gift certificate (to: jfriedl@yahoo.com), or perhaps send me some good karma by doing something kind for a stranger.


If you have questions about this tool, please [see the FAQ](#).

Basic Image Information

Target file: CloudSEK_AboutToWin.jpg

Creator:	xscorp
Credit:	Depositphotos
File Comment:	'ThE_FlAg_PaGe.html'
File:	1,023 × 491 JPEG 62,917 bytes (61 kilobytes)
Color Encoding:	WARNING: No color-space metadata and no embedded color profile: Windows and Mac web browsers treat colors randomly. Images for the web are most widely viewable when in the sRGB color space and with an embedded color profile. See my Introduction to Digital-Image Color Spaces for more information.

Main JPG image displayed here at 44% width (19% the area of the original)



[Click image to isolate](#), [click this text to show histogram](#)

6. Captured the Flag! But is the challenge over?

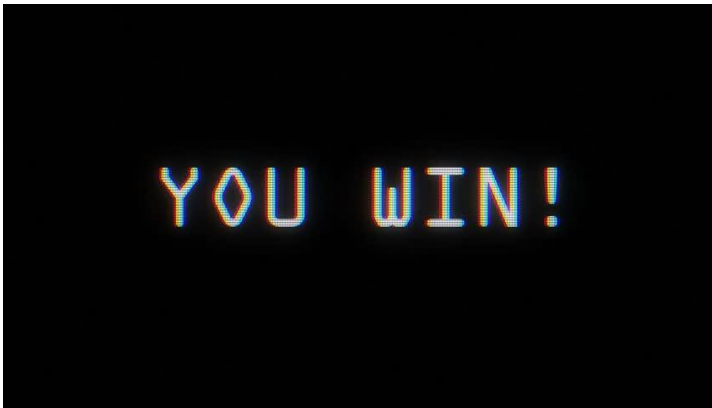
The Link http://54.244.19.42/ThE_FlAg_PaGe.html had the Flag of the CTF Challenge.

CloudSEK_CTF_2020{H4cKiNG_i\$_FuN}

Voila! Got the Flag! But is it over? Where do I submit the flag?

7. Open the Final Door!

I was wondering where to find the link to submit the flag. There were 2 images in the link, but the metadata search didn't fetch any results. I figured out that the link was not just hidden in one of the images, but was inside a file that was hidden in the image.



The above image had a hidden file inside it!

Using Steghide, I was able to retrieve the hidden textfile.

```

root@kali:~/Desktop# steghide --info you_are_winner_indeed_img.jpg
"you_are_winner_indeed_img.jpg":
  format: jpeg
  capacity: 758.0 Byte
Try to get information about embedded data ? (y/n) y
Enter passphrase: yes, try 'apt --fix-broken install' with no packages (0
  embedded file "compl3tion_m3ssag3.txt":
    size: 258.0 Byte
    encrypted: rijndael-128, cbc
    compressed: yes
root@kali:~/Desktop# steghide extract -sf you_are_winner_indeed_img.jpg
Enter passphrase: yes, done
wrote extracted data to "compl3tion_m3ssag3.txt".

```

As the hint given in the flag page, the passphrase was the flag. The ‘compl3tion_m3ssag3.txt’ had the link to the submission form.

```

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

```

And that is how the challenge was completed!