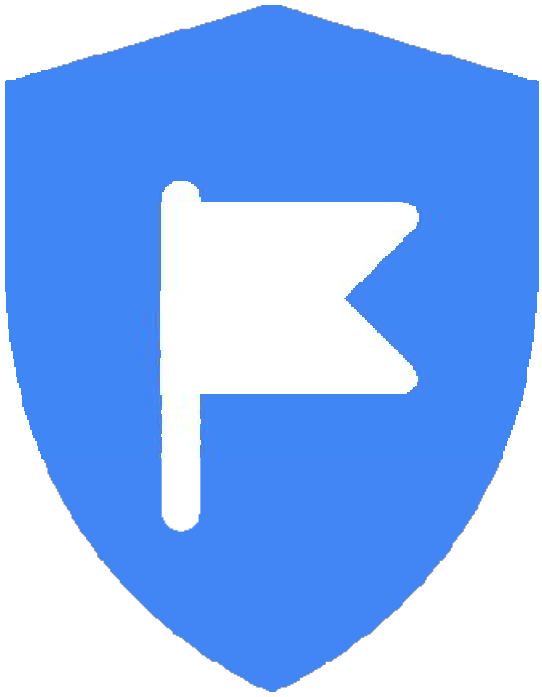
Cyber Security Analyst - EWYL Program



CTF CHALLENGE

Detailed completion report submitted by *Abhinav Ranjan*

Introduction:

CTF Challenge

- Server URL : http://54.244.19.42/

Rules and other information

- General Rules of a CTF Challenge.*
- **Front login page** is a part of CTF, find your way to log in.
- Server will be open for **2 days**.
- **Submissions** are also a part
- **Leaking solutions in the forum may lead to disqualification.**
- **Finding the submission link is a part of CTF**

Hints

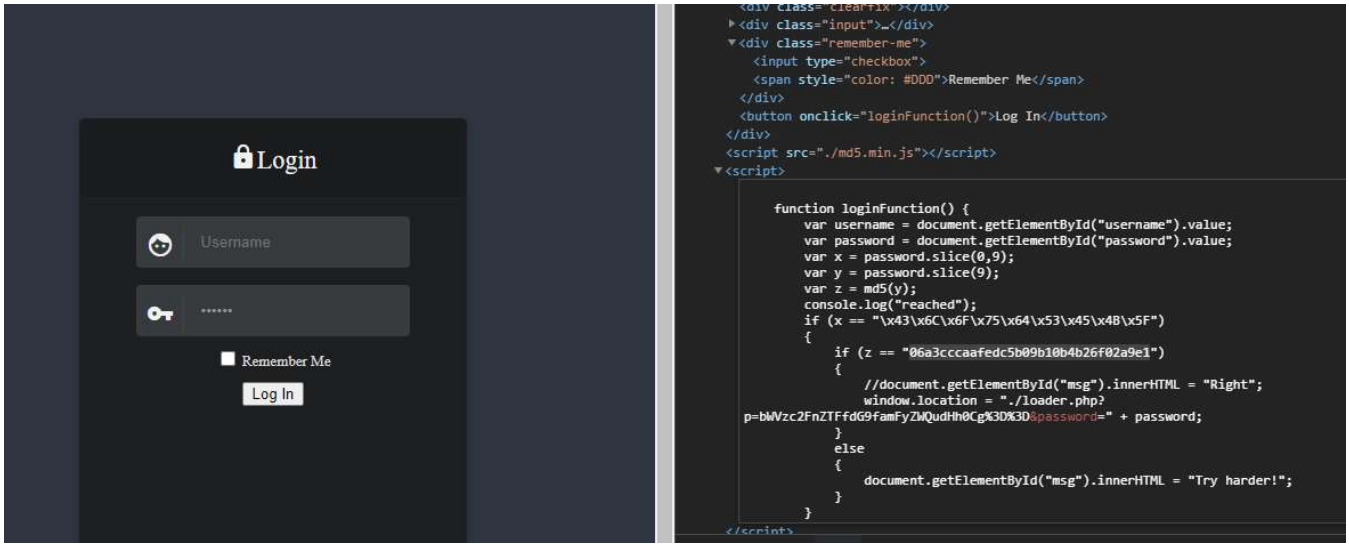
- What is robot.txt?
- It's a completely web-based CTF. You don't need to play with other ports
- One of the fields in login portal is optional. Both strings might be a part of same thing.
- If you are a Linux user, recall how **home** directory of a **user** looks like 150
- What is base64?
- Ask yourself what bug let's you read files inside system?
- Can images hide something? What is "data about data" is called as?
- What is a JWT token? How can you see contents of it?
- Can images hide a file inside them? How can we extract it?

One of the challenging CTF challenges ever faced the steps which lead to capture the flag are:

- Step1: Logging In
- Step2:Robots.txt+ Secret.txt
- Step3: Passing the Access token
- Step4:Steganography Part
- Step5: Steganography Part 2

Step1: Logging In

1. Visiting Server URL
2. Filling the credential was not enough, leading to “Invalid Credential”
3. Hints were given as “One of the fields in login portal is optional and both strings might be part of something”.
4. Looking to the JavaScript of page:
5. X and Y were the password, X was password.slice(0,9) and Y was md5 encryption of Z
6. Decoding the value of Z and removing “\x” from X and decoding it gave a string which was obviously the password: i.e.; CloudSEK_jeniffer
7. So first flag was captured leading to new challenge.



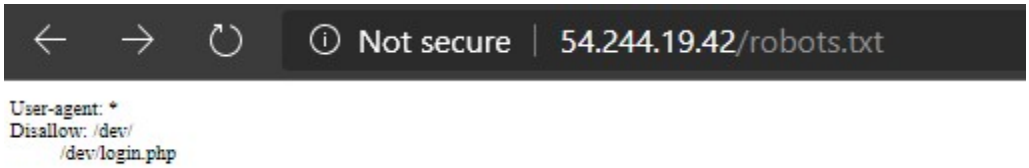
8. So new page appeared http://54.244.19.42/loader.php?p=bWVzc2FnZTFfdG9famFyZWQudHh0Cg%3D%3D&password=CloudSEK_jeniffer
9. Page have some instructions below:

   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 :)

10. So new challenge was to find that secret text file.

Step2: Robots.txt + Secret.txt

1. So, moving to the hint section, it was saying robots.txt could help.
2. Did every possible thing with robots.txt, created a robots.txt file, and tested it and many more things, nothing helped.
3. Tried harder and just searched for robots.txt on server using: "http://54.244.19.42/robots.txt" URL, now got something.



4. It was like directory address.
5. So again moved to directory inside the server as http://54.244.19.42/dev/login.php and now which said : ***"This page only accepts POST request"***
6. This was hardest part to get the secret file using POST request.
7. Tried everything from curl to postman and many more.
8. Using Curl it needed access token, so the access token was stored in secret.txt file.
9. So started finding the location for secret.txt.
10. Tried everything encoding and decoding everything, putting everywhere.
11. Again hints section helped,

    If you are still stuck at that secret.txt, pay attention to URL in loader.php. Do you see any params there? Tried playing with them(decoding them)? Do it! Do you know how the home directory structure of a user looks like? Use all that knowledge to reach secret.txt. There is a visible LFI bug in there

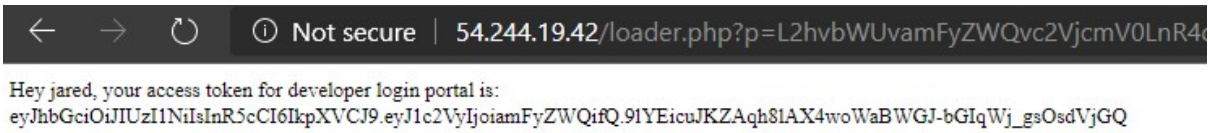
    So everything was in this hint, actually the hint was also like a CTF and working hard on hint lead to URL parameter changing hint.

    - So, first decoded the parameter there using base-64 decoder and found **bWVzc2FnZTFfdG9famFyZWQudHh0Cg is message1_to_jared.txt**
    - Now thinking for the source of secret.txt file started encoding every possible directory format to the file, finally **/home/jared/secret.txt** encoded form = **L2hvbWUvamFyZWQvc2VjcmV0LnR4dA** in URL as

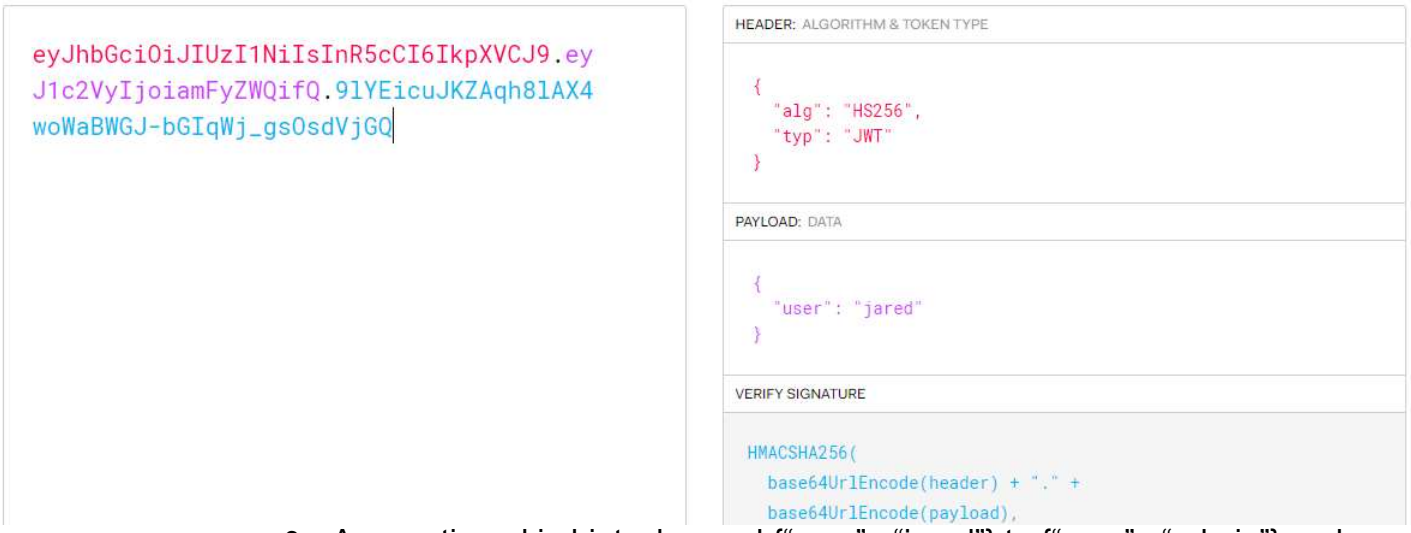
      http://54.244.19.42/loader.php?p=L2hvbWUvamFyZWQvc2VjcmV0LnR4dA&&password=CloudSEK_jeniffer made to the secret.txt and access token.

Step3: Passing the access token.

1. Now after getting the access token.



2. First decoded the access token by using the tool **https://jwt.io/#debugger**



3. As mentioned in hint, changed {“user” : “jared”} to {“user” : “admin”} and again copied the encoded access token.
4. Now using curl command to get the next flag.

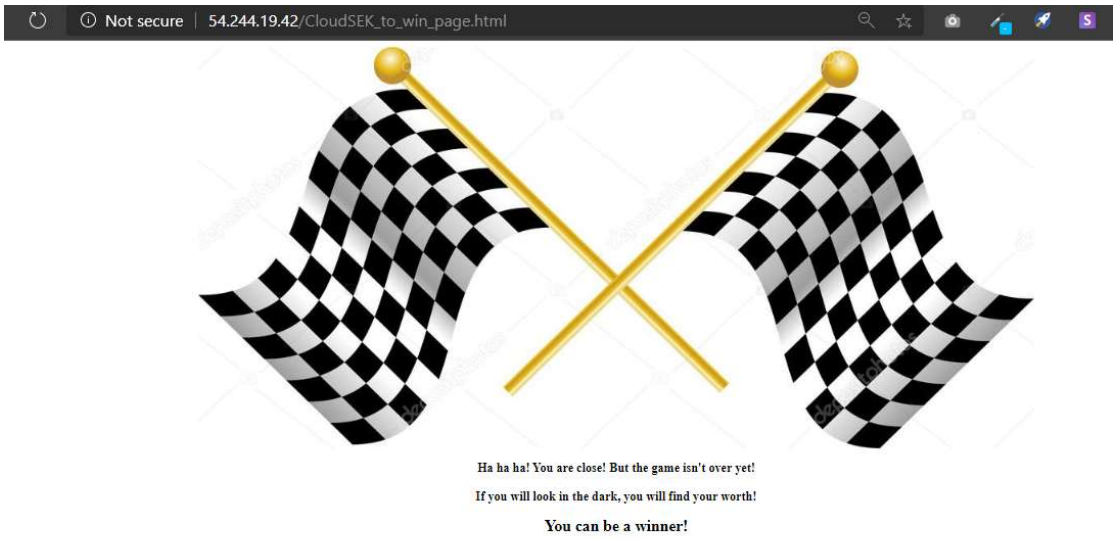
   curl -d "access_token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyIjoiYWRtaW4ifQ.9lYEicuJKZAqh8lAX4woWaBWGJ-bGIqWj_gsOsdVjGQ " -X POST http://54.244.19.42/dev/login.php

5. Got a location **as<script>window.location.href="../CloudSEK_to_win_page.html";</script>**

6. Now using the **../CloudSEK_to_win_page.html** with server as http://54.244.19.42/CloudSEK_to_win_page.html helped found a new flag leading to next step

Step4: Steganography Part

1. So the new flag landed at a new page.



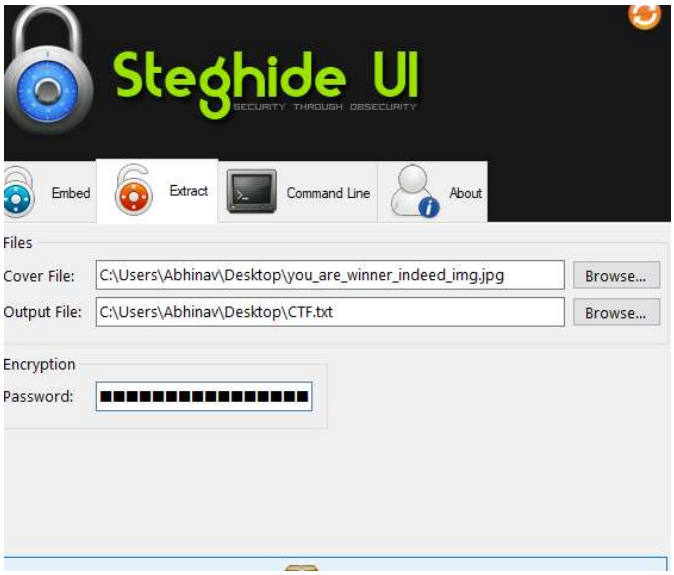
2. As mentioned in the hints it was a Steganography part.
3. Used many tools to find the hidden data, URL, etc.
4. Being windows user searched for online Steganography tool and found https://compress-or-die.com/analyze.
5. Resulting to give the URL in comment section **'/ThE_FlAg_PaGe.html'**

6. Using comment URL with server http://54.244.19.42/ThE_FlAg_PaGe.html
7. Lead to second-last flag.

Step5: Steganography Part-2

1. So the new captured flag lead to new page again a Steganography part.

2. Again used the same tool but didn't get anything.
3. Used multiple tools, as mentioned in hint section suggested to use **steghide** and **exiftool**, but in windows, not inbuilt!
4. So found alternative https://sourceforge.net/projects/steghideui/
5. And using the password as:
   CloudSEK_CTF_2020{H4cKiNG_i$_FuN}



6. Got the final flag and link to the submission.

7. Metadata of last image file:

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

Thank You “CloudSEK” for creating the CTF challenge enjoyed a lot.