**CloudSEK CTF Challenge 2020**

**REPORT**

## **INDEX**

1. **Bypassing Login Page.**
2. **Finding The Access Token.**
3. **Manipulating The Token.**
4. **Extraction of Data from Developer Admin Portal.**
5. **Extraction of MetaData from the Image.**
6. **Extraction of Another File from an Image file by the concept of Steganography.**

## **TOOLS USED:**

* **BURP SUITE**
* **EXIFTOOL**
* **STEGHIDE**

## **OS USED:**

* **Windows 10**
* **Kali Linux**

**INTRODUCTION**

**There were lots of Decoding and Encoding during this CTF. A simple, yet quite Interesting Challenge. Initial Stages were Easy to Do but after few steps you have apply your Brain and Think out of the box.**

**Basic Knowledge of URL Encoding and Steganography will do the Trick For you.**

**Let’s See How I Captured The Flag and then Found the Submission Details For The Same.**

**KEYWORDS :**

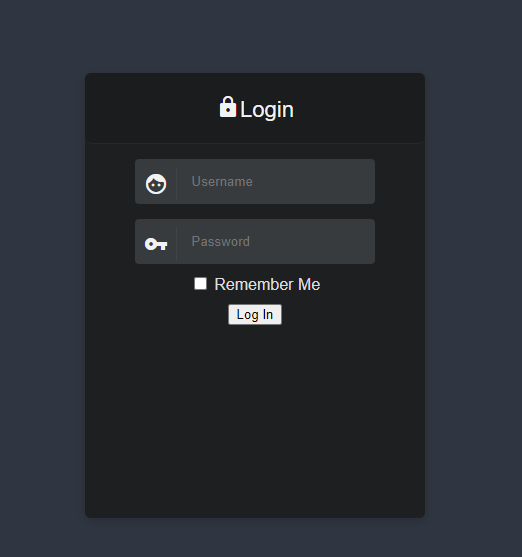
* **Steganography**
* **Access Token**
* **Source Code**
* **Meta-Data**
* **POST Request**
* **Flag**

**Part 1:**

**Bypassing Login Page**

* **So After Going on the Website** [**http://54.244.19.42/**](http://54.244.19.42/)

**You see nothing but a Login Panel on the Homepage.**

****

* **NO username or password were given to login with so the First thing which should be Checked is the Source Code of this Homepage and we can find an interesting Script which was used to validate the Username and Password.**

****

* **In this Script Both the Variables ‘x’ and ‘y’ were Password as it was sliced into 2 parts by slice(); function.**

**The variable ‘x’ is an Encoded Javascript String so Decoding it is pretty easy.**

**The Decoded String is “CloudSEK\_”,**

**So this is only the first part of the password.**

* **By looking at the variable z it is clear that its MD5 encrypted.**

**By decrypting the hash “**06a3cccaafedc5b09b10b4b26f02a9e1” **we get the string “jeniffer”.**

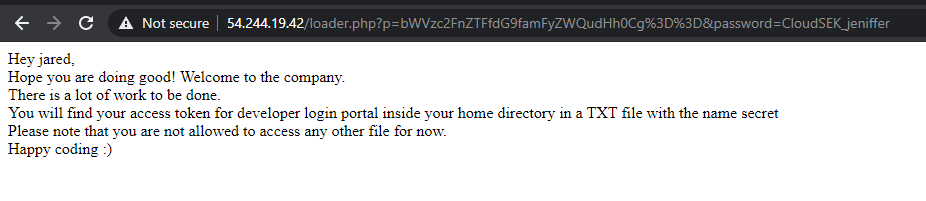
**Which is the second part of the password.**

* **So Now the Final Password is CloudSEK\_jeniffer**
* **By further looking at the script we can figure out that**

**After successful login it is been redirected to this page**

**“**[**http://54.244.19.42/loader.php?p=bWVzc2FnZTFfdG9famFyZWQudHh0Cg%3D%3D&password=**](http://54.244.19.42/loader.php?p=bWVzc2FnZTFfdG9famFyZWQudHh0Cg%3D%3D&password=) **”**

* **By Putting the Password which we Decoded Before We Get to this Page!!**

****

* **We finally get the message With the Instructions for the Next Step.**

**Things to be Noted at this Point:**

* **Username = Jared**
* **File to find = secret.txt**
* **Location = Home Directory Of Jared**
* **The parameter p is Base64 Encoded.**

**The Decoded value of Parameter p is “message1\_to\_jared.txt”**

* **So it’s safe to assume that it can be somehow related to the success.txt file which will give us the Access Token for the Next Step.**

**Part 2:**

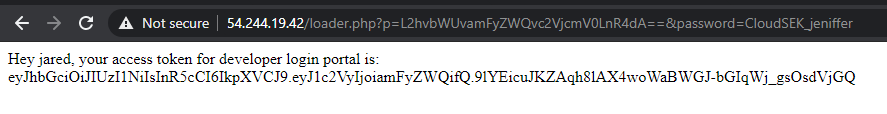
**Finding The Access Token.**

* **So the URL which we have now is** [**http://54.244.19.42/loader.php?p=bWVzc2FnZTFfdG9famFyZWQudHh0Cg%3D%3D&password=CloudSEK\_jeniffer**](http://54.244.19.42/loader.php?p=bWVzc2FnZTFfdG9famFyZWQudHh0Cg%3D%3D&password=CloudSEK_jeniffer)
* **The Hints given on the Page is “**You will find your access token for developer login portal inside your home directory in a TXT file with the name secret”
* **Home Directory of Jared… That would be /home/jared/success.txt and it can be somehow related to the “p=” parameter in the URL.**
* **Let’s Encode This Location to Base64 and put it in the URL at the parameter “p=”**
* **So the encoded value would be : L2hvbWUvamFyZWQvc2VjcmV0LnR4dA==**

**The Final URL is :**

[**http://54.244.19.42/loader.php?p=L2hvbWUvamFyZWQvc2VjcmV0LnR4dA==&password=CloudSEK\_jeniffer**](http://54.244.19.42/loader.php?p=L2hvbWUvamFyZWQvc2VjcmV0LnR4dA==&password=CloudSEK_jeniffer)

**and HIT !!!**

**We have the Access Token Now.**

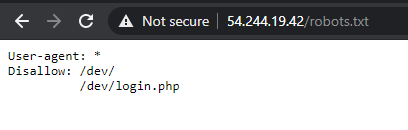
**By Looking at the Access Token Format. It is in JSON Format.**

**PART 3:**

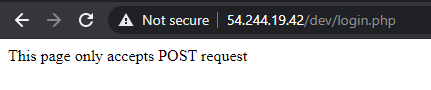
**Extraction of Data from Developer Admin Portal.**

* **Now Time to Find the Developers Login Portal.**
* **By Looking at the Robot.txt of the website.**

**We can easily find the Login Portal Path.**

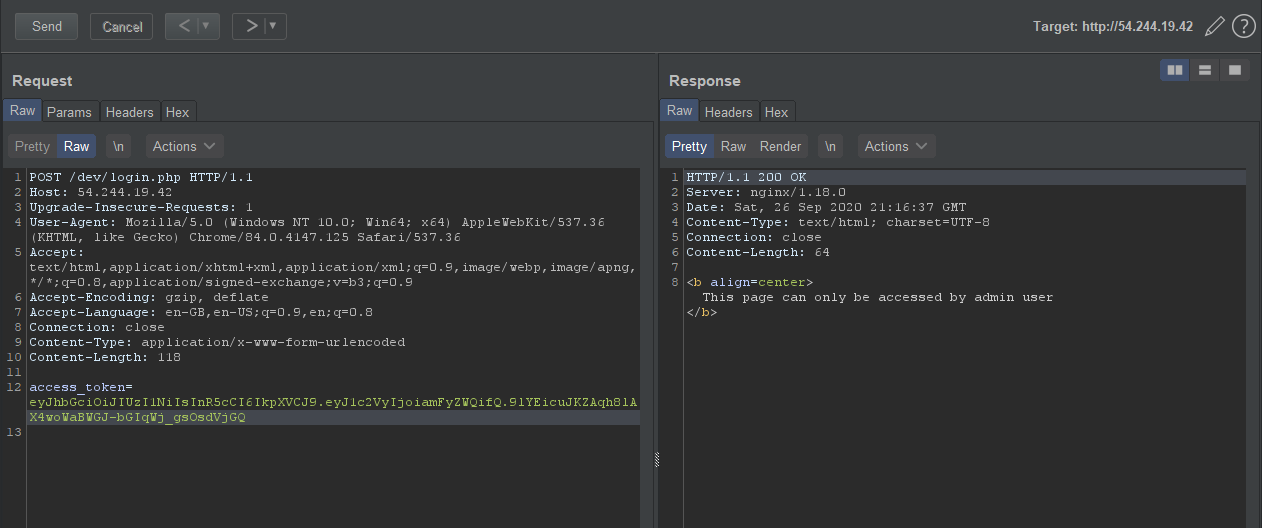
****

**Okay So Let’s Go to “**[**http://54.244.19.42/dev/login.php**](http://54.244.19.42/dev/login.php)**”.**

****

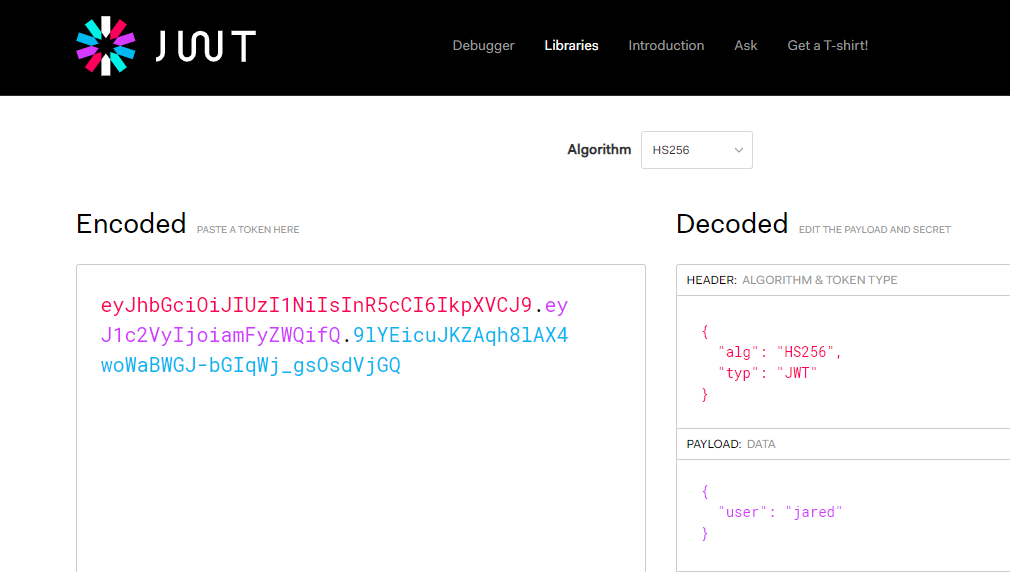
**Hmm. Fair Enough. Let’s Fire Up Burp Suite For sending the POST data Request.**

**After Sending the POST data Request using the access\_token and by changing the content-type to** “application/x-www-form-urlencoded” **we get this message.**

****

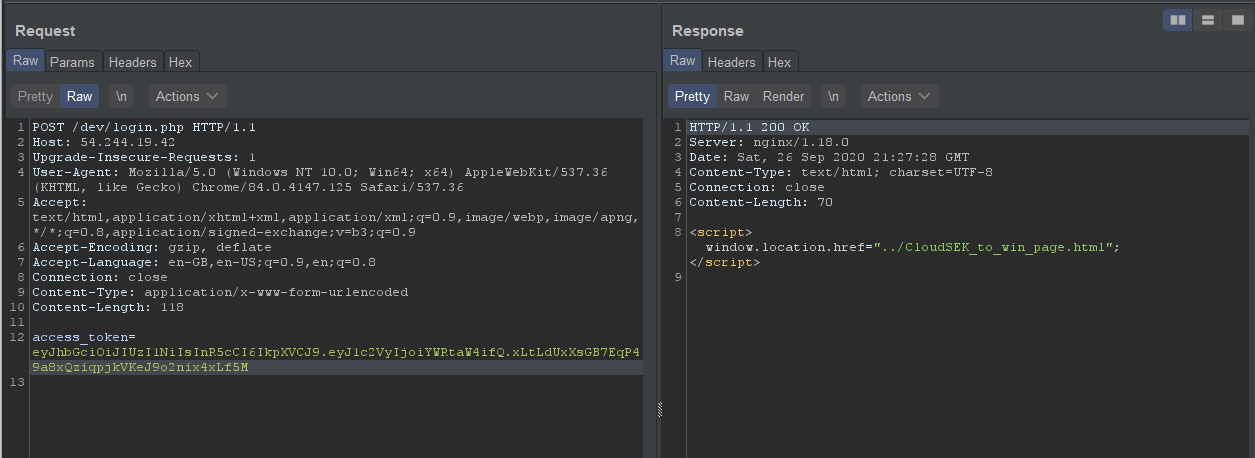
**“This page can only be accessed by admin user”**

* **Let’s Try to Manipulate the JWT Access Token at** [**https://jwt.io/**](https://jwt.io/)

****

* **Change The “user” from “jared” to “admin” and try with the new access\_token**

***eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyIjoiYWRtaW4ifQ.xLtLdUxXsGB7EqP49a8xQziqpjkVKeJ9o2nix4xLf5M***

****

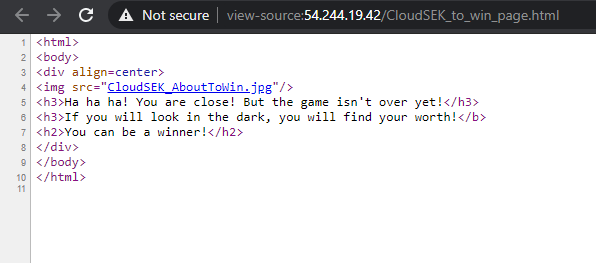
**Another HITT !!!**

**Now Lets Open The Given URL**

[**http://54.244.19.42/CloudSEK\_to\_win\_page.html**](http://54.244.19.42/CloudSEK_to_win_page.html)

****

* **Hmm So Nothing but Texts and a Image.   
  Let’s Check the Source Code !**

****

* **Nope. Nothing Here.**

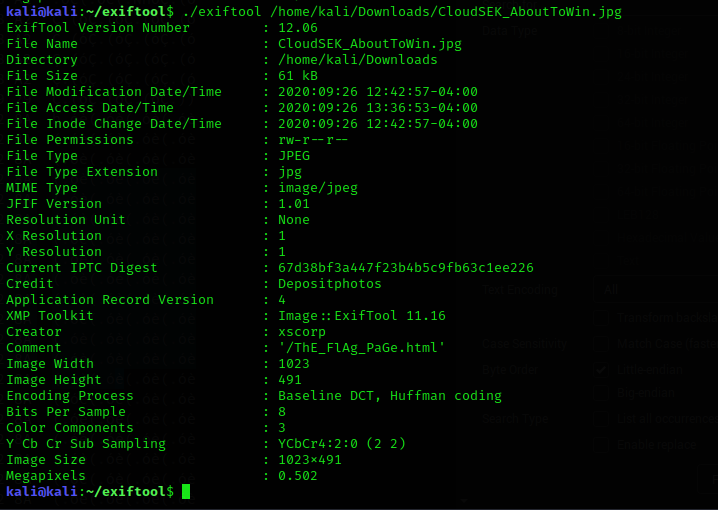
**PART 5:**

**Extraction of MetaData from the Image.**

***If you will look in the dark, you will find your worth.***

**OKAY.**

* **Let’s Look For Something in the Image given on the page Then. As No Other Option is Left.**
* **By using the ExifTool we can Find The Basic Info and meta-data about the Image**

****

* **We Can see a URL path in the Comment Section of the Image :**

“/ThE\_FlAg\_PaGe.html”

* **Lets Go The URL “**[**http://54.244.19.42/ThE\_FlAg\_PaGe.html**](http://54.244.19.42/ThE_FlAg_PaGe.html)**”**

****

**AND IT’S DONE !!!**

* **WE FOUND THE FLAG !** ☺

# CloudSEK\_CTF\_2020{H4cKiNG\_i$\_FuN}

# Okay So Flagging is Done

# Now The Most Important PART

# SUBMITTING IT.

# Hint is given on the Page

# *Wondering where to submit this flag? Well.. that file containing the form link must be somewhere in here.* *The flag is the key to the next door*

# Okay… It must be somewhere in here… and the Flag is the key to the next door.

# Lets Check The Source Code

# 

# Again nothing but the Two Images.

# Lets Check Their Meta Data

# First check the metadata of the “you\_are\_winner\_indeed\_img.jpg”

# 

# Umm… Nothing.

# Lets Check if this File is Hiding Something

# PART 6:

# Extraction of Another File from the Image by the concept

# of Steganography.

# What is Steganography?

# In Simple words it is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination. The use of steganography can be combined with encryption as an extra step for hiding or protecting data.

# Use Steghide Tool

# While trying to extract data from the image it asked for the passphrase and it immediately struck my mind that *The flag is the key to the next door*

# So The Used the Flag “CloudSEK\_CTF\_2020{H4cKiNG\_i$\_FuN}” as the passphrase and…

# C:\Users\wayne\Desktop\CTF Report\Screenshots\Completion Message.png

# Done!!!

# Lets See Whats in the compl3tion\_m3ssag3.txt File.

# C:\Users\wayne\Desktop\CTF Report\Screenshots\The ENd.png

# Just WOW !!

# This CSRF was Really Interesting and I had Fun Doing it

# REFERENCES:

<https://jwt.io/>

<https://www.edureka.co/blog/steganography-tutorial>