



---

# ***Cloud SEK Challenge2020***

---

## ***Walkthrough***



NAME- VISHAL KUMAR SINGH

EMAIL- VISHALBIT99@GMAIL.COM

# Cloud SEK Challenge2020

1. We were given an ip to a login page.

## [Challenge #2] - Cyber Security Analyst - EWYL Program

Challenge Corner

 **CloudSEK** Verified Team 5 2d

Welcome to the second step of **EWYL** 120 Cyber Security Analyst challenge #2. All the updates about this challenge will be posted here.

The second phase of the program would be a **CTF Challenge**. Information and instructions will be added as soon as it is available.

The challenge is live now 🕒

▼ Enter the challenge

### CTF Challenge

- Server URL : <http://54.244.19.42/> 196


Huh, this looks like a simple login page, it isn't 😊


Not secure | 54.244.19.42

n.org Latest News Help

Try harder!

🔒 Login

 jared

 .....

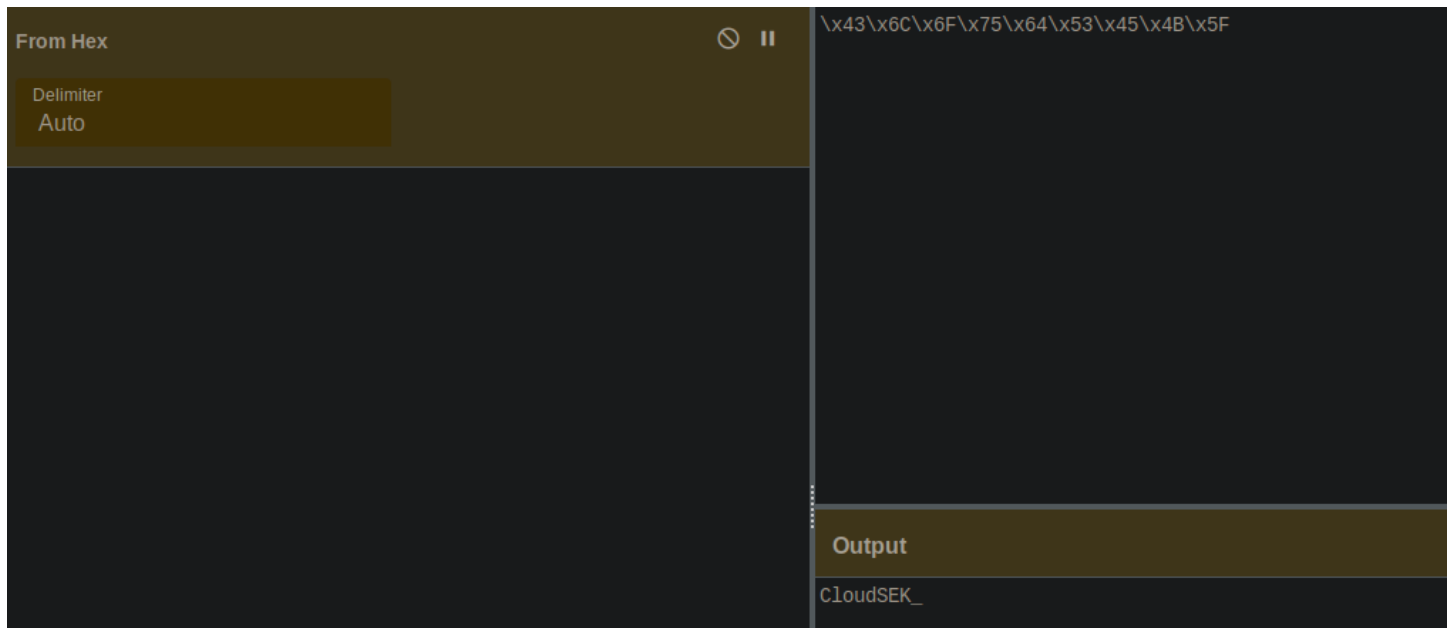
☐ Remember Me

Log in


On inspecting the source code . I found a script that tells us the password.

```
<script src="./md5.min.js"></script>
<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>
```

The first part gives us the first 9 letters of the password and the 2<sup>nd</sup> part the rest of it.



06a3cccaafedc5b09b10b4b26f02a9e1

☐ I'm not a robot 

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1\_bin), QubesV3.1BackupDefaults

Hash	Type	Result
06a3cccaafedc5b09b10b4b26f02a9e1	md5	<u>jeniffer</u>

Hence, we get the password **CloudSEK\_jeniffer**

**Obvious isn't it.**

← → ↻ 🏠 ⓘ Not secure | 54.244.19.42/loader.php?p=bWVzc2FnZTFfdG9famFyZWQudHh0Cg%3D%3D&password=CloudSEK\_jeniffer

📱 Apps 🌐 Debian.org 🌐 Latest News 🌐 Help

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 :)

The above message tells us that a secret.TXT file is present in users home directory which has the access\_token.

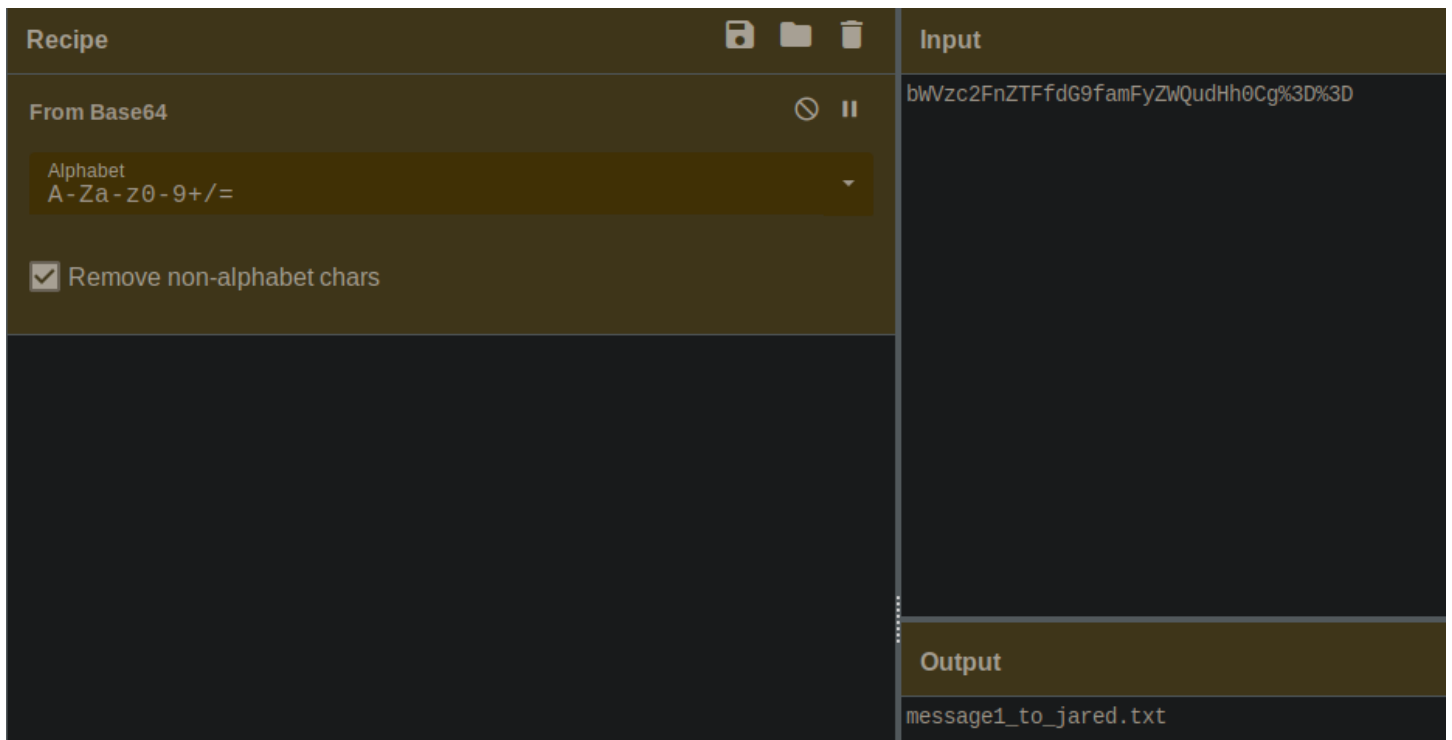
But how to get to the home directory .

← → ↻ 🏠 ⓘ Not secure | 54.244.19.42/loader.php?p=bWVzc2FnZTFfdG9famFyZWQudHh0Cg%3D%3D&password=CloudSEK\_jeniffer

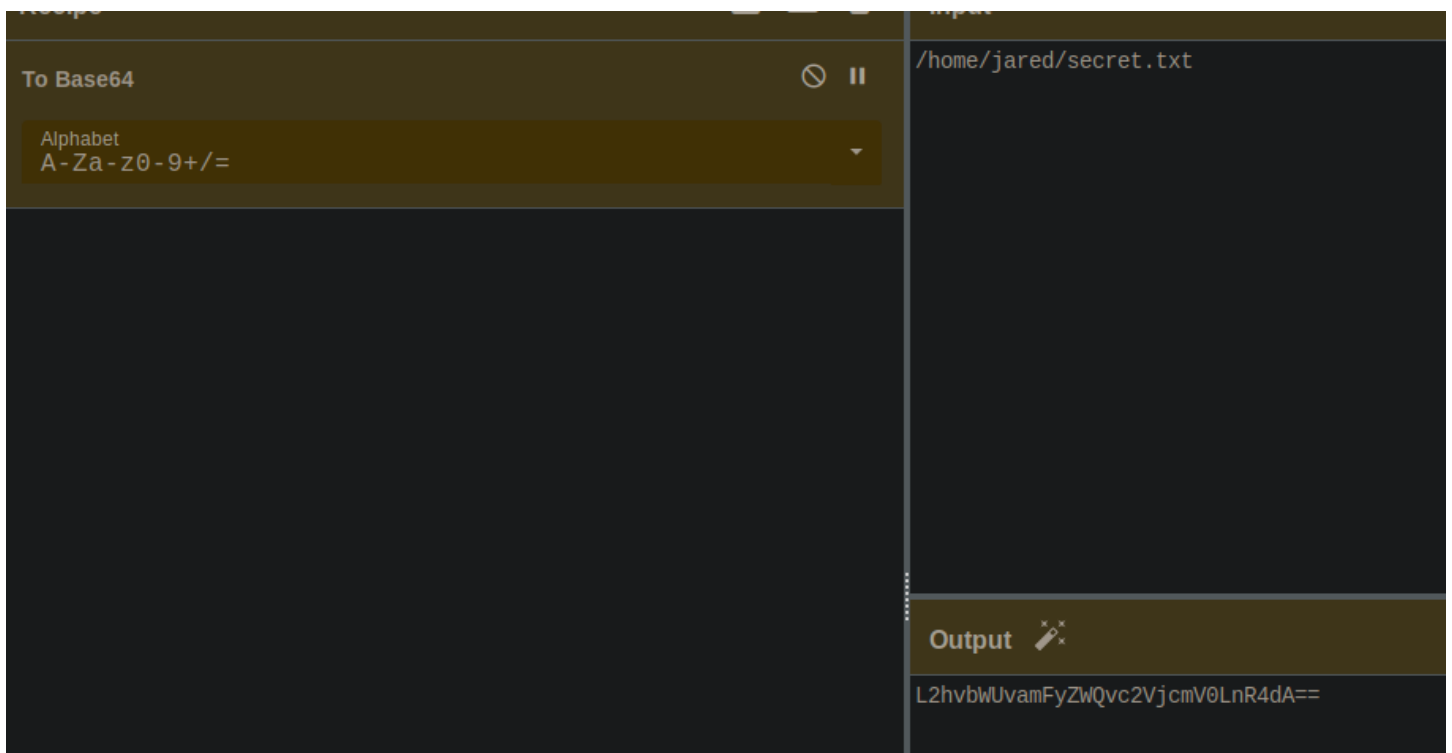
📱 Apps 🌐 Debian.org 🌐 Latest News 🌐 Help

If you noticed above the p parameter has a BASE64 code.

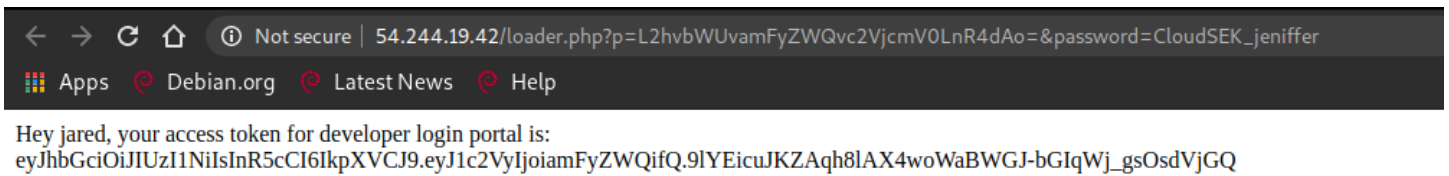
Hmmm,



This tells us how the url is fetching any file from server.

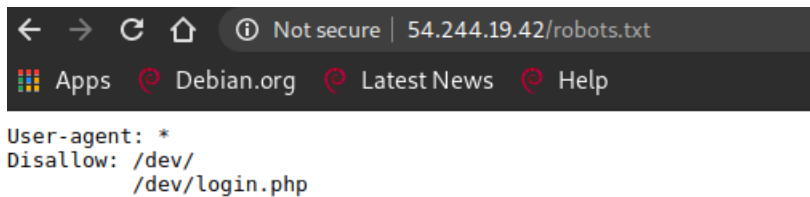


If we use base64 encoded path “/home/jared/secret.txt” in the p parameter like above we get the access\_token

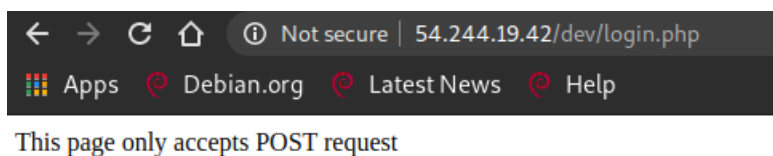


Nice!!

Lets check robots.txt and see if there is anything there for us

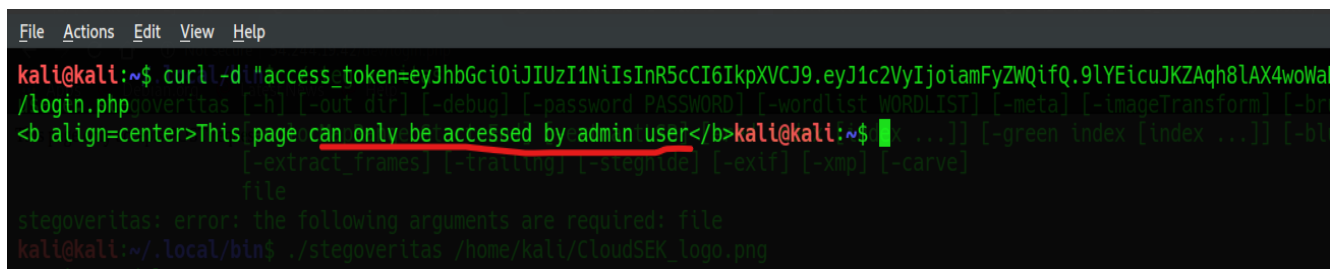


We get the login page url. On going to the login page we see this message



Huh!

Now we have the access token and login page url lets do curl



Hmmm, only looking at the above token I realized that it's a JWT and I know a few ways to bypass it. Let's do it.

## Using jwt.io website

## Encoded

PASTE A TOKEN HERE

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyIjoiamFyZWQifQ.9lYEicuJKZAqh8lAX4woWaBWGJ-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),
  your-256-bit-secret
)
```

We have to edit alg to none and user to admin and we are good to go.

## Encoded

PASTE A TOKEN HERE

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyIjoiamFyZWQifQ.9lYEicuJKZAqh8lAX4woWaBWGJ-bGIqWj_gs0sdVjGQ
```

## Decoded

EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "none",
  "typ": "JWT"
}
```

PAYLOAD: DATA

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

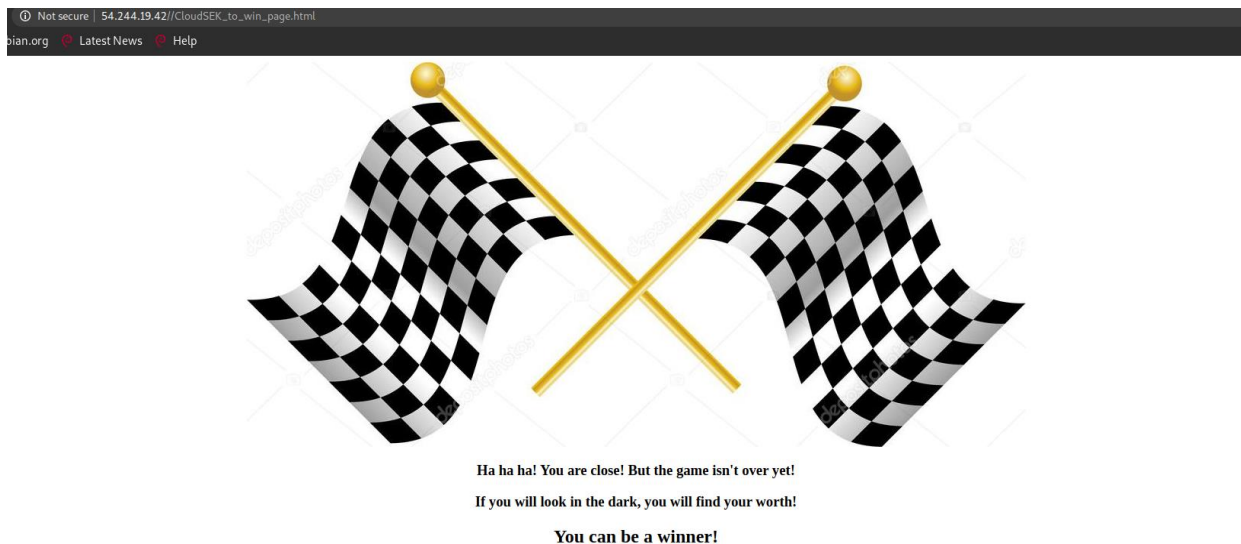
VERIFY SIGNATURE

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  your-256-bit-secret
)
```

Once again curl and we get,

```
kali@kali:~$ curl -d "access_token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyIjoiamFyZWQifQ.9lYEicuJKZAqh8lAX4woWaBWGJ-bGIqWj_gs0sdVjGQ" -X POST http://54.244.19.42/d
<script>window.location.href='../CloudSEK_to_win_page.html';</script>
kali@kali:~$ Error: the following arguments are required: file
kali@kali:~/local/bin$ ./stevenitas /home/kali/CloudSEK/logo.png
```

On visiting the url, we are greeted with an image



I thought the image is hiding something, so I downloaded it and used exiftool to look at its metadata , and did I find something

Oof!

```
kali@kali:~$ exiftool index.jpeg
ExifToolVersion: 11.16
File Name: index.jpeg
Directory: .
File Size: 61 KB
File Modification Date/Time: 2020:09:26 08:36:56-04:00
File Access Date/Time: 2020:09:26 08:36:56-04:00
File Inode Change Date/Time: 2020:09:26 08:36:56-04:00
File Permissions: -rw-r--r--
File Type: JPEG
File Type Extension: .jpeg
MIME Type: image/jpeg
JFIF Version: 1.0
Resolution Unit: None
X Resolution: 1
Y Resolution: 1
Current IPTC Digest: f67d38bf3a447f23b4b5c9fb63c1ee226
Credit: 
Application Record Version: 4
XMP Toolkit: Adobe Photoshop 2020
Creator: 
Comment: 
Images Width: 1023
Image Height: 491
Encoding Process: Baseline DCT, Huffman coding
Bits Per Sample: 8
Color Components: 3
YCbCr Sub Sampling: YCbCr4:2:0 (2 2)
Image Size: 1023x491
MegaPixels: 0.502
```



Lets visit the page.



Hurray!! I found the Flag, but wait it tells us there is still one final step left.

Where is the form link? Hmm!

We see 2 images and a hint that the file containing the link is here somewhere.

So I downloaded both the images did a lot of steganography on them after a while I found this,

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

The password was the Flag.

The text file contained the link.

```
Open ▼ 📎
1 Congratulations on making it to the end!
2 Please submit a detailed walkthrough PDF along with proper steps and screenshots on the link below.
3 We hope to see you in the interview:
4
5 https://forms.gle/CA9vHT6XaisS9HgR6
6
7
8 Happy Hacking!
9
10 ~CloudSEK family
11
```

You can see below the image that compelled me to write this walkthrough 😊

## You Nailed It to the next round!

We are glad that you were able pass the challenge. Please fill the form which help us to contact you for the further rounds of the interview process.

The name and photo associated with your Google account will be recorded when you upload files and submit this form. Not **vishalbit99@gmail.com**? [Switch account](#)

\* Required


**Name \***  
Please enter your full name.

vishal kumar singh

**Email Id \***  
Please enter the correct email address.

vishalbit99@gmail.com

**Report \***  
Upload your final score card here.

 [Add file](#)

⚠ This is a required question