

# MMU X NEXAGATE 2024 CTF WRITEUP

By k3shi

## Contents

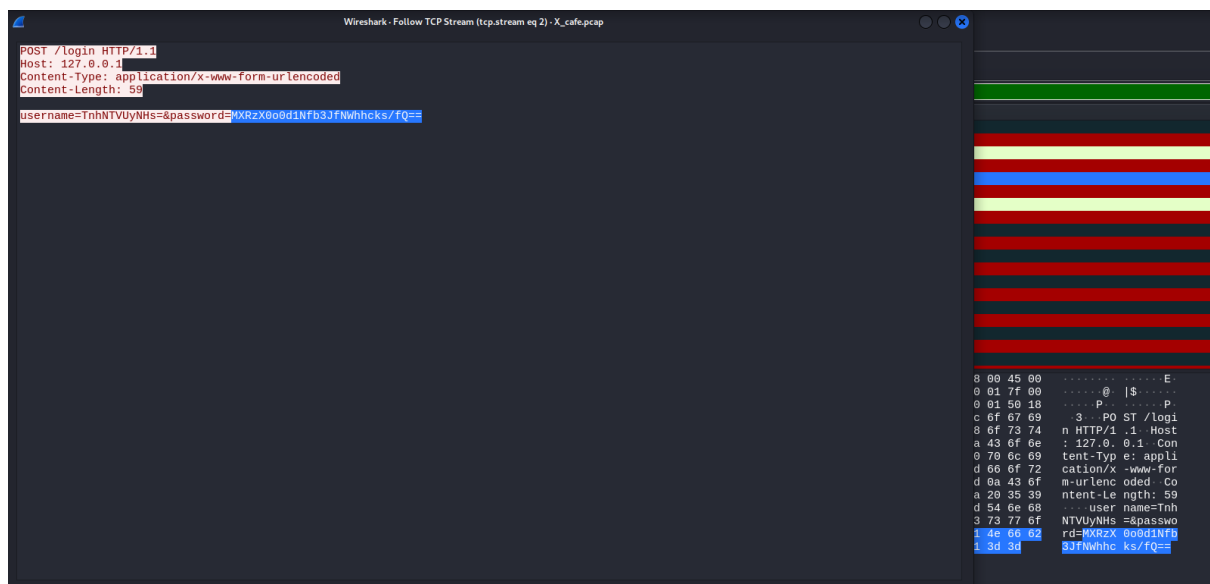
Forensic.....	2
miniJAWS.....	2
Cryptography.....	3
Reaaranged.....	3
Punch Card.....	5
Spam message .....	7
XOR.....	8
Gibberish.....	9
3 encryption .....	11
Reverse engineering.....	13
Drunk Vending Machine.....	13
Drunk Vending Machine 2.....	14
Steganography.....	15
In the Beginning.....	15
Morse Code.....	16
Just a normal cat pic.....	17
Is it cookie?.....	18
Corrupted Audio.....	20
Web.....	23
Just a normal website.....	23
Misc .....	25
Old Nokia.....	25
Nice to meet you!.....	26
Cow breeder.....	28

# Forensic

## miniJAWS



Open .pcap file using wireshark and lookup for login HTTP. After that follow the TCP streamline and will get an encoded password in a base64 format.



Decode using CyberChef to get the flag.

### Input

```
TnhNTVUyNHs=MXRzX0o0d1Nfb3JfNWwhhcks/fQ==
```

### Output

```
NxMMU24{1ts_J4wS_or_5harK?}
```

## Cryptography

### Rearranged

Challenge

# Rearranged

## 50

Do you know what is it?

 rearranged.txt

Flag

Submit

Cat the txt file and encoded messages given bellow. I notice that there is number 1 - 5 inside the messages.

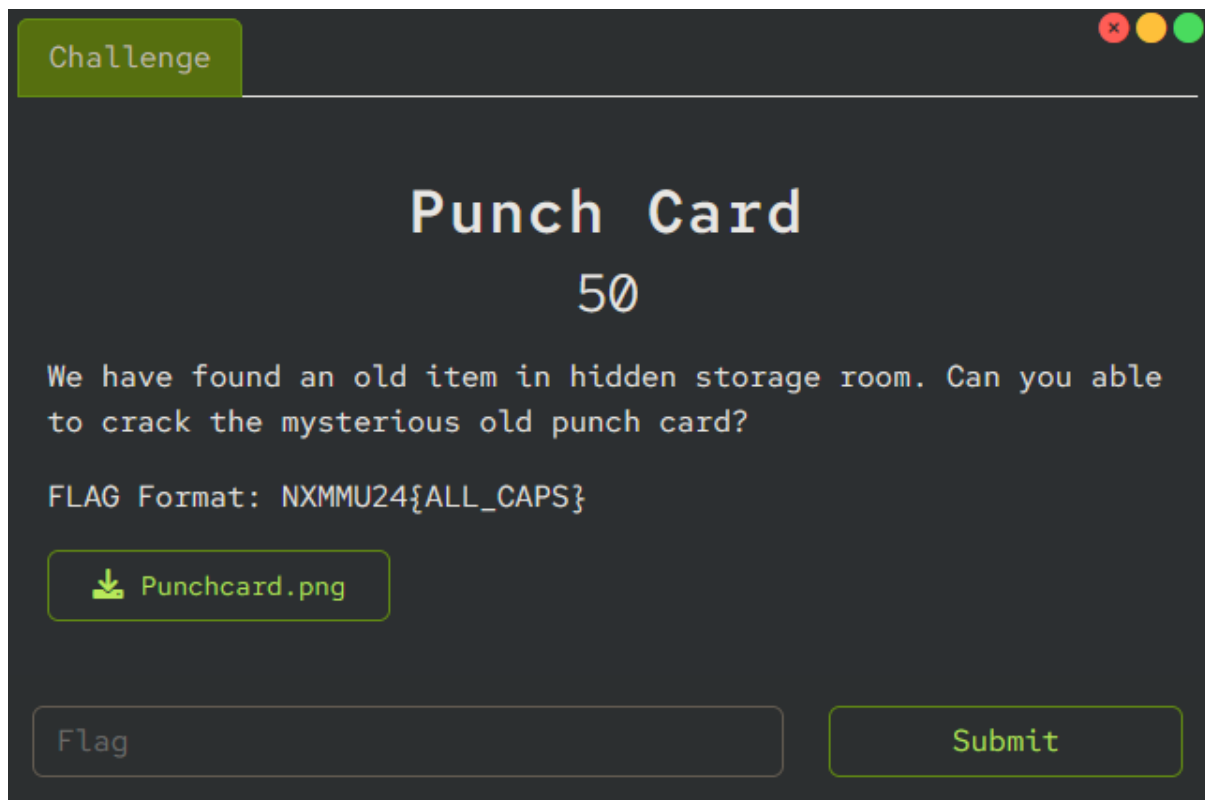
```
tcpw ajmqc
sio uly wfimy
It can't be said I'm an early bird
It's ten o'clock before I say a word
Baby, I can never tell
How do you sleep so well?
You keep telling me to live right
To go to bed before the daylight
But then you wake up for the sunrise
You know you don't gotta pretend
Baby, now and then
4.sw33t_
Don't you just wanna wake up
Dark as a lake
Smelling like a bonfire
Lost in a haze?
If you're drunk on life, babe
I think it's great
1.NxMMU24{
But while in this world
I think I'll take my whiskey neat
My coffee black and my bed at three
You're too sweet for me
You're too sweet for me
I take my whiskey neat
My coffee black and my bed at three
You're too sweet for me
You're too sweet for me
I aim low
I aim true, and the ground's where I go
I work late where I'm free from the phone
And the job gets done
5.4_m3}
But you worry some, I know
But who wants to live forever, babe?
You treat your mouth as if it's Heaven's gate
The rest of you like you're the TSA
I wish I could go along
Babe, don't get me wrong
You know you're bright as the morning
As soft as the rain
Pretty as a vine
As sweet as a grape
You can sit in a barrel
Maybe I'll wait
Until that day
I'd rather take my whiskey neat
My coffee black and my bed at three
You're too sweet for me
You're too sweet for me
I take my whiskey neat
3.t00_
My coffee black and my bed at three
You're too sweet for me
You're too sweet for me
I take my whiskey neat
2.y0ur_
My coffee black and my bed at three
You're too sweet for me
You're too sweet for me
```

Use the cipher identifier to identify which cipher it is and it uses ROT13 for the messages. So, I gathered the 5 messages together and here goes the flag.

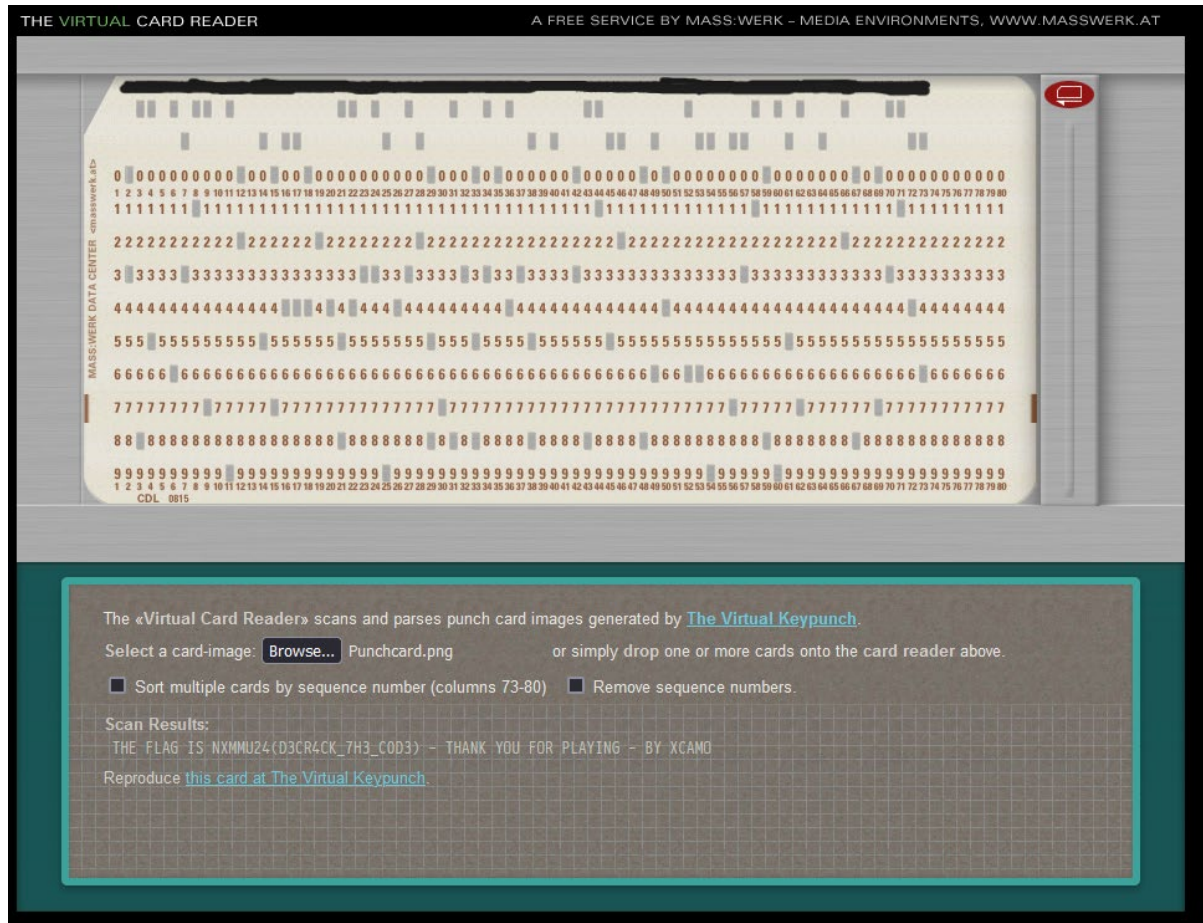


Flag: NxMMU24{y0ur\_t00\_sw33t\_4\_m3}

## Punch Card



Open the jpg file and we'll see a punch card picture is given. So, with the information given I try to search up for Punch Card Decoder and my guessing is correct. Upload the jpg file and decode it to get the flag.



Flag: NXMMU24(D3CR4CK\_7H3\_C0D3)

## Spam message

Challenge

47 Solves

✕ ● ●

# Spam message

## 100

Someone left a spam message in my inbox. I have a feeling that this hides a message within. Can you help me decode it?

 spam.txt

Flag


Submit

Cat spam.txt and copy the messages.

```
1 Dear Friend , This letter was specially selected to
2 be sent to you . This is a one time mailing there is
3 no need to request removal if you won't want any more
4 ! This mail is being sent in compliance with Senate
5 bill 2716 , Title 4 ; Section 304 ! This is not multi-level
6 marketing . Why work for somebody else when you can
7 become rich within 83 weeks ! Have you ever noticed
8 the baby boomers are more demanding than their parents
9 and people will do almost anything to avoid mailing
10 their bills . Well, now is your chance to capitalize
11 on this . WE will help YOU deliver goods right to the
12 customer's doorstep plus deliver goods right to the
13 customer's doorstep ! You can begin at absolutely no
14 cost to you . But don't believe us . Mrs Jones who
15 resides in South Dakota tried us and says "Now I'm
16 rich, Rich, RICH" . We assure you that we operate within
17 all applicable laws ! We BESEECH you - act now . Sign
18 up a friend and your friend will be rich too . Thanks
19 . Dear Cybercitizen ; Thank-you for your interest in
20 our publication ! This is a one time mailing there
21 is no need to request removal if you won't want any
22 more ! This mail is being sent in compliance with Senate
23 bill 2416 ; Title 3 ; Section 304 . THIS IS NOT MULTI-LEVEL
24 MARKETING . Why work for somebody else when you can
25 become rich inside 68 weeks . Have you ever noticed
26 people love convenience and nobody is getting any younger
27 ! Well, now is your chance to capitalize on this !
28 We will help you SELL MORE and use credit cards on
29 your website ! The best thing about our system is that
30 it is absolutely risk free for you . But don't believe
31 us . Ms Jones of Hawaii tried us and says "My only
32 problem now is where to park all my cars" . We are
33 licensed to operate in all states ! Because the Internet
34 operates on "Internet time" you must act now . Sign
35 up a friend and you get half off ! Thanks . |
```



Use spammimic to decode it.



# Decoded

Your spam message **Dear Friend , This letter was specially ...** decodes to:

Look wrong?, try the [old version](#)

Copyright © 2000-2023 spammimic.com, All rights reserved

## XOR

Challenge 35 Solves

# XOR

## 200

My laptop was hit by a ransomware attack. To decode it, I have to input a piece of code inside an input area. The attacker has left me a string of code in a .txt file. What could it possibly mean?

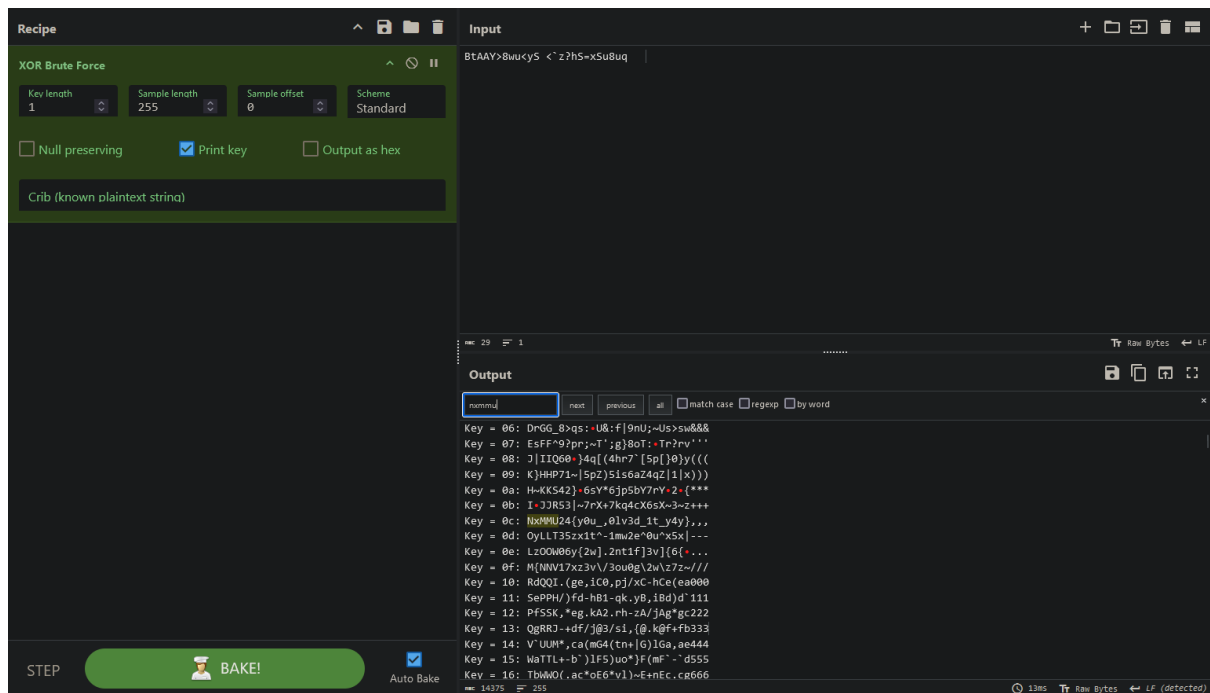
► Unlock Hint for 0 points

📄 note.txt

Flag

Submit

The hint already given at the title where we need to use XOR to decode the messages. Copy the messages and decode it using XOR brute force and lookup for the keyword of the flag - NxMMU.

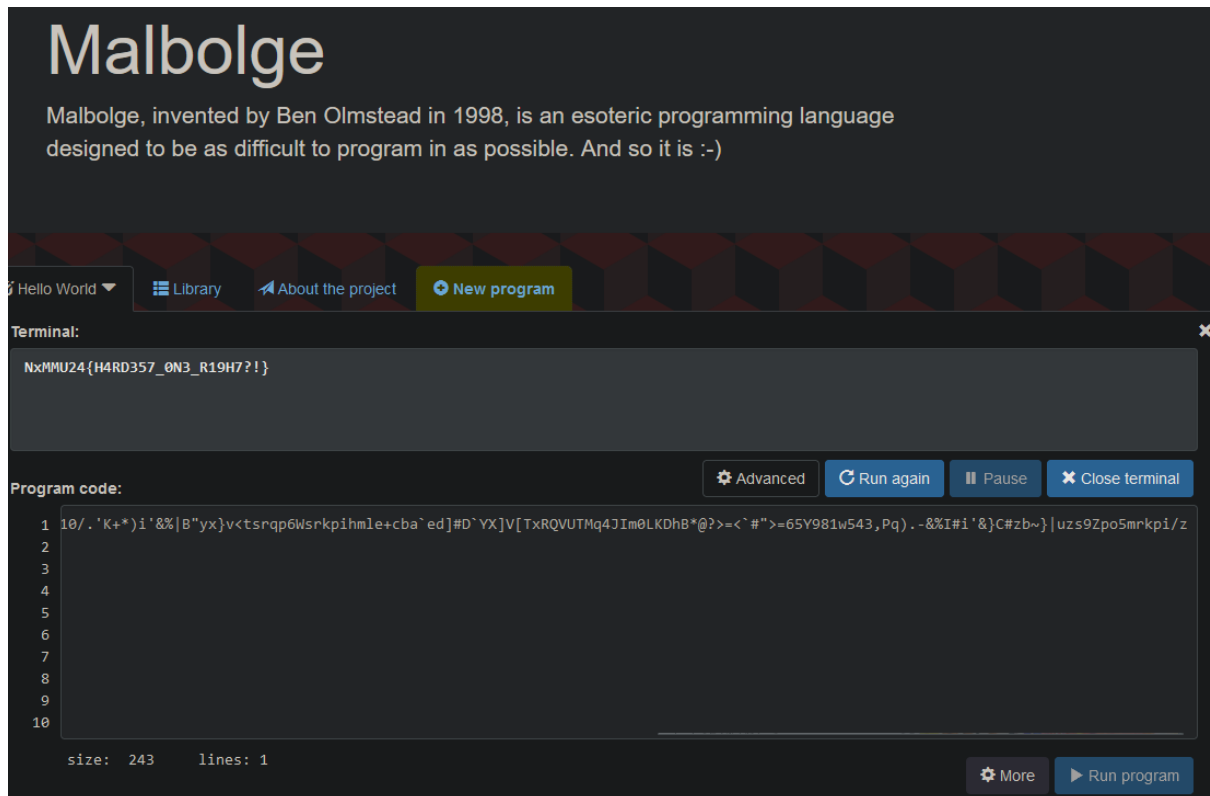


Flag: NxMMU24{y0u\_,01v3d\_1t\_y4y}

## Gibberish



With the hint given try to search for malbolge and I found a malbolge decoder. Copy the messages and decode it.



Flag: NxMMU{H4RD357\_0N3\_R19H7?!}

### 3 encryption

Challenge 57 Solves

## 3 Encryption

### 200

My grandpa left me a key to his will - but it is encrypted with 3 different kinds of encryption! Help me decrypt it so I can get the will.

▼ Unlock Hint for 0 points

Hint: Base 32, Base64, Hex (which order is corect to decrypt this?)

📄 key.txt.txt

Flag Submit

Cat key.txt and copy the text given.

```
(k3shi@kali)-[~/Downloads/ctf/crypto]
$ cat key.txt
GU2CANTFEA3DQIBUMUQDKNBAGU3CANJVEA3TSIBUMUQDIOBAG42CAMZVEA2GIIBUHAQDKNRAGY3CANDEEAZTEIBTGUQDMYJAGYZSANTF
EA3GGIBXG4QDMNBAGQ2CANDFEA3GEIBVHAQDGMRAGMYCAN3BEA3DMIBVGEQDGBAGNSA=====
```

Use cyberchef to decode the text using base32 and we'll get a text in hex.

From Base32

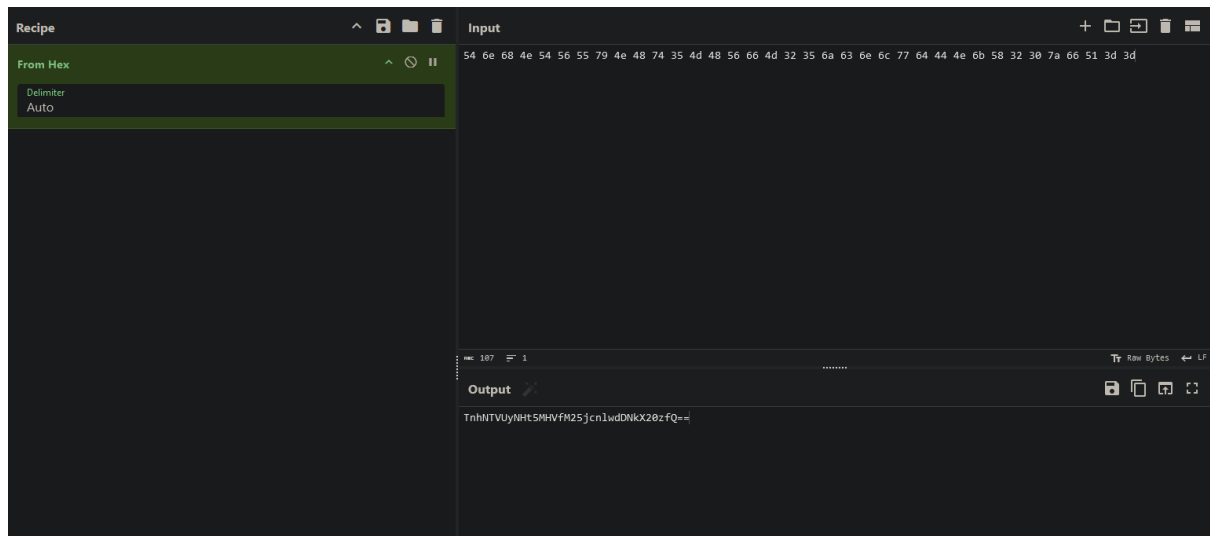
Alphabet A~Z2~7= ☒ Remove non-alphabet chars

GU2CANTFEA3DQIBUMUQDKNBAGU3CANJVEA3TSIBUMUQDIOBAG42CAMZVEA2GIIBUHAQDKNRAGY3CANDEEAZTEIBTGUQDMYJAGYZSANTFEA3GGIBXG4QDMNBAGQ2CANDFEA3GEIBVHAQDGMRAGMYCAN3BEA3DMIBVGEQDGBAGNSA=====

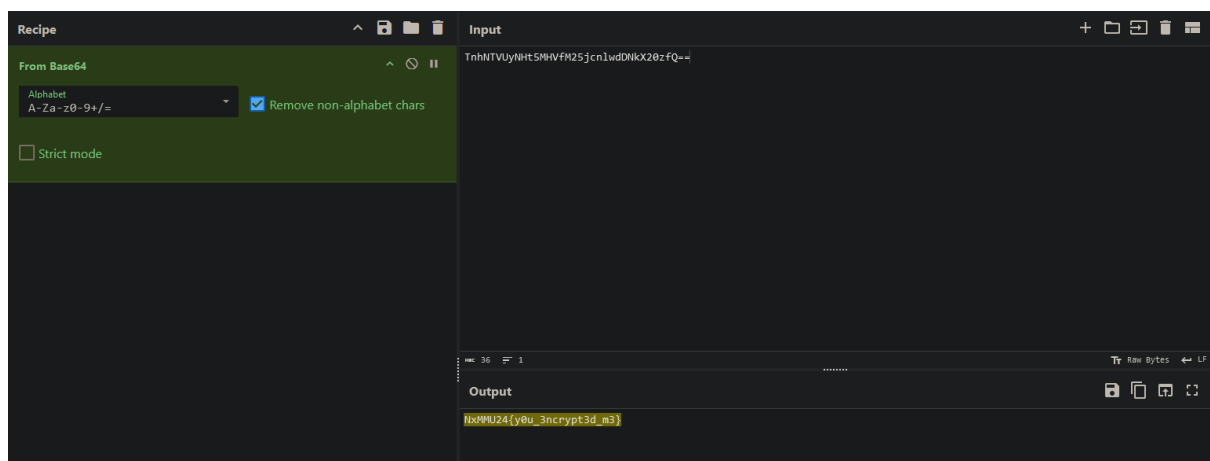
Output

54 6e 68 4e 54 56 55 79 4e 48 74 35 4d 48 56 66 4d 32 35 6a 63 6e 6c 77 64 44 4e 6b 58 32 30 7a 66 51 3d 3d

Decode it using hex.



Lastly, use the base64 to decode the previous output that we got from hexadecimal.



Flag: NxMMU24{y0u\_3ncrypt3d\_m3}

# Reverse engineering

## Drunk Vending Machine



Look into the python source code and modify it.

```
def choose_drink():
    drinkID = [
        "4e78", "4d4d", "5532", "347b",
        "3174", "735f", "3769", "6d33",
        "5f32", "5f63", "7537", "5f35",
        "7547", "3472", "7d"
    ]

    drink_ID = ''.join(drinkID)
    choice = bytes.fromhex(drink_ID).decode('utf-8')
    return choice

def step1():
    special = choose_drink()
    key = 42
    master_drink = xor_encrypt(special, key)
    return master_drink

def step2():
    encrypted_flag = step1()
    encoded = base64.b64encode(encrypted_flag.encode()).decode()
    return encoded

encoded_flag = step2()

def decode_and_decrypt(encoded_flag, key):
    decoded_flag = base64.b64decode(encoded_flag).decode()
    decrypted_flag = xor_encrypt(decoded_flag, key)
    return decrypted_flag

key = 42
flag = decode_and_decrypt(encoded_flag, key)
print("Flag:", flag)
```

Run SOFT\_DRINK.py and get the flag.

```
(k3shi@kali)-[~/Downloads/ctf/reverse]
$ python3 SOFT_DRINK.py
Flag: NxMMU24{1ts_7im3_2_cu7_5uG4r}
```

## Drunk Vending Machine 2

Challenge 56 Solves

# Drunk Vending Machine II

## 100

"you might guess the right function, but I'm gate-crypting the flag from you hehehe"

SOFT\_DRINK-II.py

Flag

Submit

```
(k3shi@kali)-[~/Downloads/ctf/reverse/drunk2]
$ python3 soft_drink_2.py
Welcome to the Vending Machine! Please choose a drink

['Coke', 'Pepsi', 'Sprite', 'Fanta', 'Mountain Dew', 'Dr Pepper', '7 Up', 'Vida', 'F&N', 'Milo', 'Nescafe', 'Wonda', 'Twister', 'Redbull']
Enter your choice (or type 'exit' to quit): test
Dispensing drink...
Here is your test
Thank you for using the Vending Machine. Goodbye!
Encoded: fEp/f2cABklbbVl8AkVtWxkHbVwCBW0BUwdLbQpTUAE=
Decoded: NxMMU24{i_kN0w_i+5_n07_3a5y_8ab3}
fEp/f2cABklbbVl8AkVtWxkHbVwCBW0BUwdLbQpTUAE=
```

# Steganography

## In the Beginning

Challenge

## In the Beginning

### 50

My friend sent me a audio.wav. It looks weird, and looks like he's hiding something in it, because he included a notepad titled "decode.txt!"

audio.wav

decode.txt

Flag

Submit

Decode the passphrase given with cyberchef to decode the audio.wav

Input

dGhpc19pc19hX3Bhc3N3b3Jk

Output

this\_is\_a\_password

Search for audio decoder and upload the audio.wav along with the passphrase.

### Steganographic Decoder

This form decodes the payload that was hidden in a JPEG image or a WAV or AU audio file using the [encoder form](#). When you submit, you will be asked to save the resulting payload file to disk. This form may also help you guess at what the payload is and its file type...

Select a JPEG, WAV, or AU file to decode:

Browse...

audio.wav

Password (may be blank):

this\_is\_a\_password

☒ View raw output as MIME-type `text/plain`

☐ Guess the payload

☐ Prompt to save (you must guess the file type yourself.)

Submit Query

To use this form, you must first [encode a file](#).

These pages use the [steghide](#) program to perform steganography, and the files generated are fully compatible with steghide.

Please send comments or questions to [Alan Eliasen](#).

[Back to Alan's Home Server](#)

NxMMU24{f14w3d\_m4ng035}



## Morse Code


Challenge

# Morse Code

## 50

Whilst listening for radio frequencies on my make-shift radio, I came across this morse code on a random frequency. What does it say?

Flag format: NXMMU24{FL4GH3R3}

 audio\_morse.wav

Submit

Use Morse Decoder to decode audio messages and we got the flag.

## Morse Decoder

This is an experimental tool for listening to, analysing and decoding [International Morse code](#). No information from the microphone is transmitted to the server, but the connection to the server is encrypted nonetheless.

If you cannot produce your own Morse code sounds then try using my [Morse code translator](#) to play or download some.


Alphabet to decode into


Latin


All these alphabets can be sent in Morse using standard timing. The "Latin" alphabet is e.g. "ABC" (and includes accented characters and prosigns).


Use the microphone:


Or analyse an audio file containing Morse code:

Listen 

Stop 


Upload 

Play 

Stop 

Filename: "audio\_morse.wav"

NXMMU24L1ST3NC4R3FU11Y

Clear Message 

## Just a normal cat pic

Challenge

# Just a normal cat pic

## 50

This cat picture looks strangely suspicious...

cat.jpg

decode.txt

Flag

Submit

As the decode.txt is given we knew that we must get the passphrase to decode the cat.jpg. Use CyberChef to decode the hexadecimal messages.

Input

63 7a 4e 6a 64 58 49 7a 58 33 41 30 63 33 4e 33 4d 48 4a 6b

Output

czNjdXIzX3A0c3N3MHJk

I'm lazy with using command so I just simply use the previous online Steganographic Decoder. At the first, I thought it was the passphrase and try to decode it but then it seems like the passphrase is incorrect.

Steganographic Decoder

This form decodes the payload that was hidden in a JPEG image or a WAV or AU audio file using the [encoder form](#). When you submit, you will be asked to save the resulting payload file to disk. This form may also help you guess at what the payload is and its file type...

Select a JPEG, WAV, or AU file to decode:

Browse... cat.jpg

Password (may be blank):

czNjdXIzX3A0c3N3MHJk

☒ View raw output as MIME-type

☐ Guess the payload

☐ Prompt to save (you must guess the file type yourself)

Submit Query

To use this form, you must first [encode a file](#).

These pages use the [steghide](#) program to perform steganography, and the files generated are fully compatible with steghide.

Please send comments or questions to [Alan Fiksen](#).

[Back to Alan's Home Server](#)

Error. This file may not contain steganographic data, or you may have specified an incorrect password.

Decode the previous passphrase again.

<b>Input</b>
czNjdXIzX3A0c3N3MHJk

<b>Output</b>
s3cur3_p4ssw0rd

Try again and we get the flag.

**Steganographic Decoder**

This form decodes the payload that was hidden in a JPEG image or a WAV or AU audio file using the [encoder form](#). When you submit, you will be asked to save the resulting payload file to disk. This form may also help you guess at what the payload is and its file type ...

Select a JPEG, WAV, or AU file to decode:  
 cat.jpg

Password (may be blank):

☒ View raw output as MIME-type   
☐ Guess the payload  
☐ Prompt to save (you must guess the file type yourself)

---

To use this form, you must first [encode a file](#).  
These pages use the [steghide](#) program to perform steganography, and the files generated are fully compatible with steghide.

Please send comments or questions to [Alan Elason](#).  
[Back to Alan's Home Server](#)

NxMMU24{C4T5\_Y4444Y}

## Is it cookie?

Challenge


3 Solves

# Is it cookie?

## 100

What happen to this file?

▼ Unlock Hint for 0 points  
Have you tried stegcracker?

 cookie.txt

Flag

Submit

Use exiftool to check the metadata and the file type is incorrect.

```
(k3shi@kali)-[~/Downloads/ctf/stega/cookie]
$ exiftool cookie.txt
ExifTool Version Number      : 12.76
File Name                    : cookie.txt
Directory                    : .
File Size                    : 231 kB
File Modification Date/Time  : 2024:06:11 16:21:16+08:00
File Access Date/Time       : 2024:06:15 12:40:02+08:00
File Inode Change Date/Time  : 2024:06:15 12:39:58+08:00
File Permissions             : -rw-rw-r--
File Type                    : JPEG
File Type Extension         : jpg
MIME Type                    : image/jpeg
JFIF Version                 : 1.01
Resolution Unit              : None
X Resolution                  : 1
Y Resolution                  : 1
Image Width                  : 1708
Image Height                 : 2100
Encoding Process              : Baseline DCT, Huffman coding
Bits Per Sample              : 8
Color Components              : 3
Y Cb Cr Sub Sampling         : YCbCr4:2:0 (2 2)
Image Size                   : 1708x2100
Megapixels                   : 3.6
```

Change .txt into .jpg extension.

```
(k3shi@kali)-[~/Downloads/ctf/stega/cookie]
$ file cookie.txt
cookie.txt: JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline,
precision 8, 1708x2100, components 3

(k3shi@kali)-[~/Downloads/ctf/stega/cookie]
$ mv cookie.txt cookie.jpg
```

Use stegcraker to brute force and extract the data.

```
(k3shi@kali)-[~/Downloads/ctf/stega/cookie]
$ man stegcracker

(k3shi@kali)-[~/Downloads/ctf/stega/cookie]
$ stegcracker cookie.jpg /usr/share/wordlists/rockyou.txt
StegCracker 2.1.0 - (https://github.com/Paradoxis/StegCracker)
Copyright (c) 2024 - Luke Paris (Paradoxis)

StegCracker has been retired following the release of StegSeek, which
will blast through the rockyou.txt wordlist within 1.9 second as opposed
to StegCracker which takes ~5 hours.

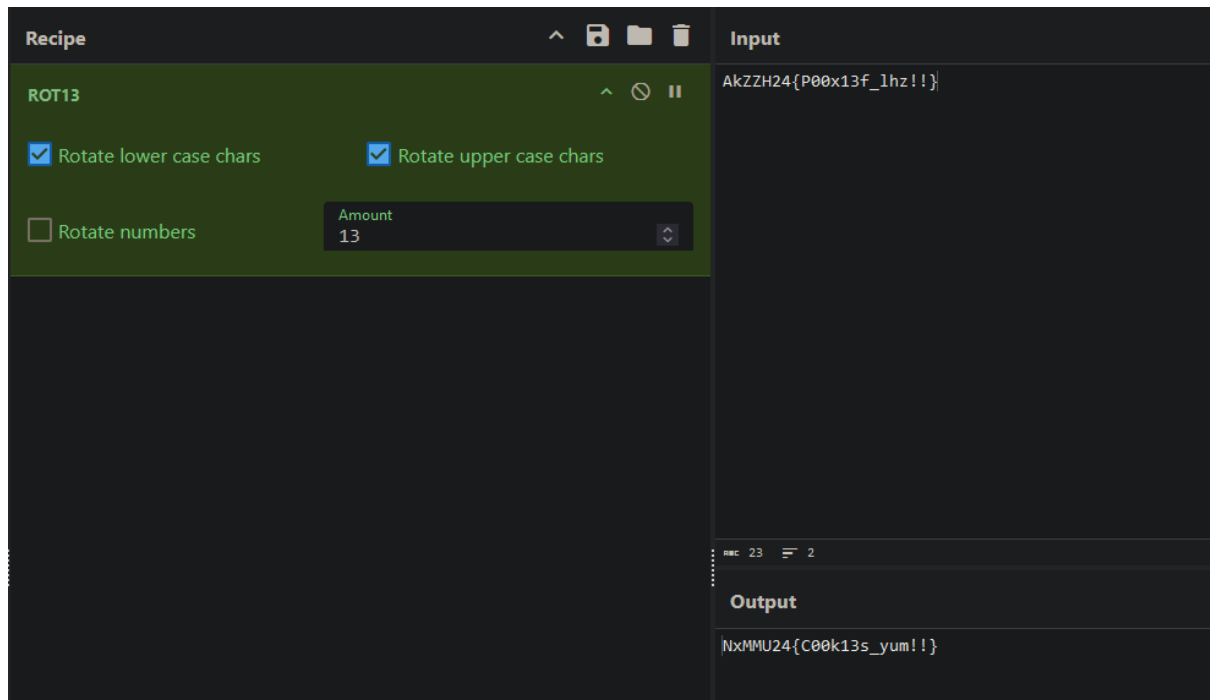
StegSeek can be found at: https://github.com/RickdeJager/stegseek

Counting lines in wordlist..
Attacking file 'cookie.jpg' with wordlist '/usr/share/wordlists/rockyou.txt'..
Successfully cracked file with password: iloveyou
Tried 197 passwords
Your file has been written to: cookie.jpg.out
iloveyou

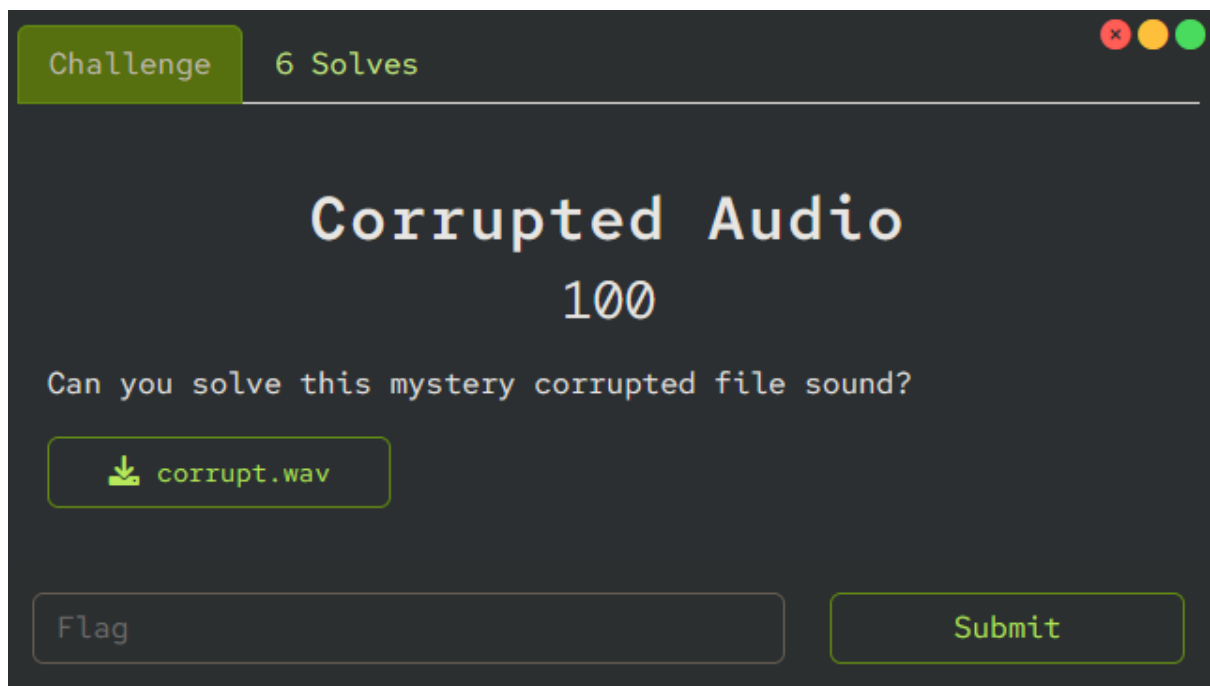
(k3shi@kali)-[~/Downloads/ctf/stega/cookie]
$ ls
cookie.jpg  cookie.jpg.out

(k3shi@kali)-[~/Downloads/ctf/stega/cookie]
$ cat cookie.jpg.out
AkZZH24{P00x13f_lhz !! }
```



Decode the text with ROT13 cipher and get the flag.

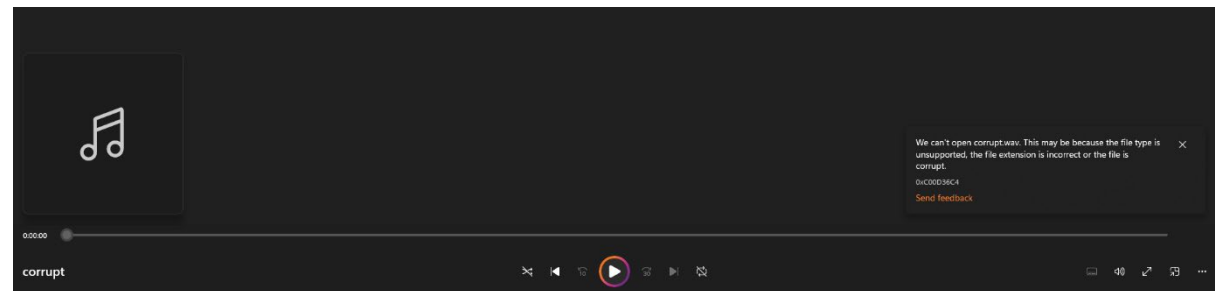


## Corrupted Audio



The corrupt.wav cannot be opened.

Today			
	2024-06-15 12_12_33-MMU CTF 2024 — ...	15/6/2024 12:13 PM	PNG File 16 KB
	corrupt.wav	15/6/2024 12:15 PM	cloudmusic.wav 431 KB



Use hexeditor and we can see that the header file is corrupted.

-Untitled- x corrupt.wav x	
00000000	60 48 B7 A6 20 B9 06 00 50 41 47 45 66 6D 74 20 H a ..PAGEfmt
00000010	14 00 00 00 01 00 02 00 22 56 00 00 88 58 01 00 ..... "V..êX..
00000020	04 00 10 00 00 00 00 00 64 61 74 61 F8 B8 06 00 .....data°..
00000030	00 00 00 00 FA FF FA FF FF FF 00 00 E5 FF E4 FF .... . . .σ Σ
00000040	CE FF C9 FF C8 FF BF FF D0 FF C6 FF E9 FF E0 FF ‡ ℓ γ ℓ † θ α
00000050	E1 FF D4 FF D5 FF C4 FF 9F FF 88 FF 60 FF 43 FF β ℓ γ - f ê ` C
00000060	8B FF 74 FF 82 FF 6A FF 68 FF 4E FF 8D FF 7B FF ï t é j h N i {
00000070	4E FF 35 FF 6F FF 5A FF AB FF A1 FF 24 FF 10 FF N 5 o Z ½ í \$ .
00000080	62 FF 59 FF 83 FF 7E FF 99 FE 79 FE 12 FF 02 FF b Y â ~ Ö.y.. .
00000090	C4 FF C7 FF 06 FF ED FE EA FE C9 FE 4E FF 38 FF - † . φ·Ω·ƒ·N 8
000000A0	1D FF FE FE A7 FE 72 FE AE FE 72 FE B8 FF 9B FF . . .°-r·«-r-γ ¢
000000B0	92 FF 75 FF 1E FE D7 FD DA FD 8B FD AB FD 5D FD Æ u . . ‡² γ² ÿ² ½² ]²
000000C0	E1 FD A0 FD 0A FF E6 FE A5 FE 67 FE A8 FE 64 FE β² á² . μ·Ñ·g·z·d·
000000D0	8A FF 69 FF B6 FE 87 FE F0 FE C8 FE 6D FF 54 FF è i † .ç·≡·ℓ·m T
000000E0	20 FE E5 FD 3D FF 23 FF 00 01 17 01 24 00 1F 00 ·σ²= # ....\$...
000000F0	FC FF F6 FF 9F 00 B2 00 6E 00 7E 00 C5 FF CB FF n ÷ f.■.n.~.† T
00000100	71 FF 87 FF 04 00 47 00 7E FE A4 FE 8E FC 80 FC q ç ..G.~·ñ·ÃⁿÇⁿ

Check the file format which using RIFF and search up for the header.

```
(k3shi@kali)-[~/Downloads/ctf/stega/corrupted_aud]
$ file corrupt.wav
corrupt.wav: RIFF (little-endian) data, WAVE audio, Microsoft PCM, 16 bit, stereo 22050 Hz
```

52 49 46 46 - RIFF

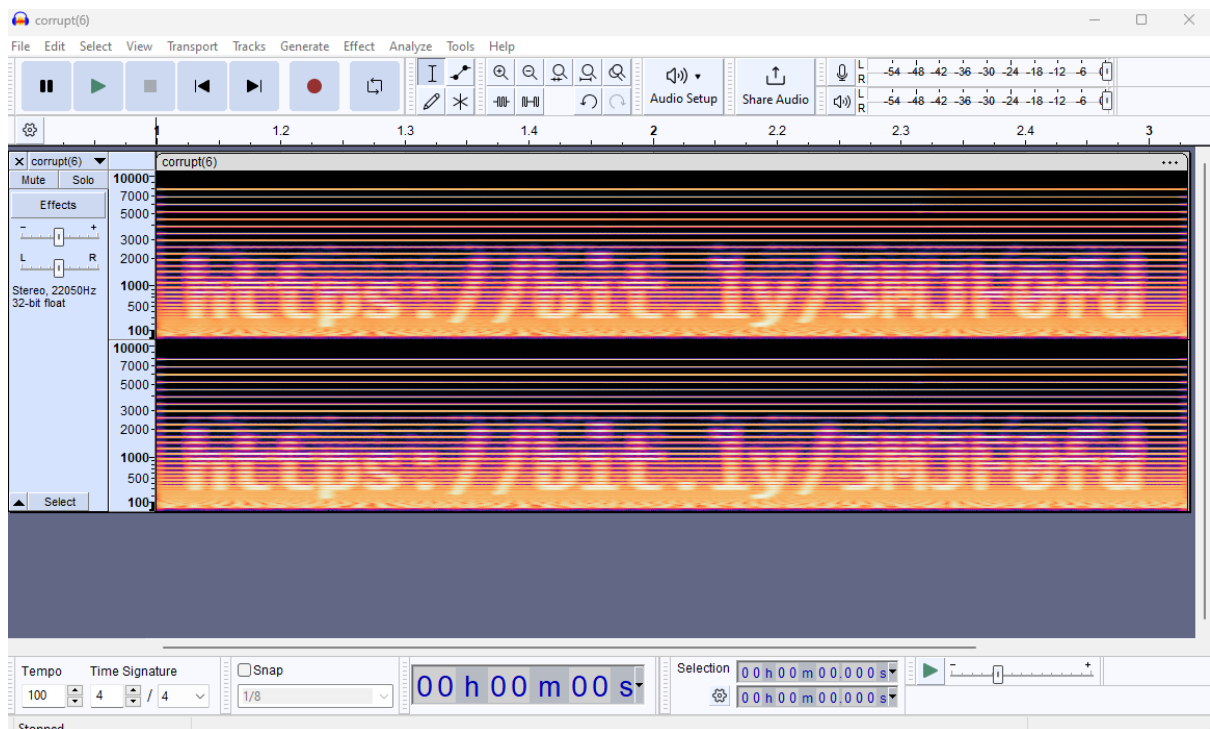
The next 4 bytes represent the chunk size, which is little endian. In your case it is:

e8 57 14 00 - 1333224

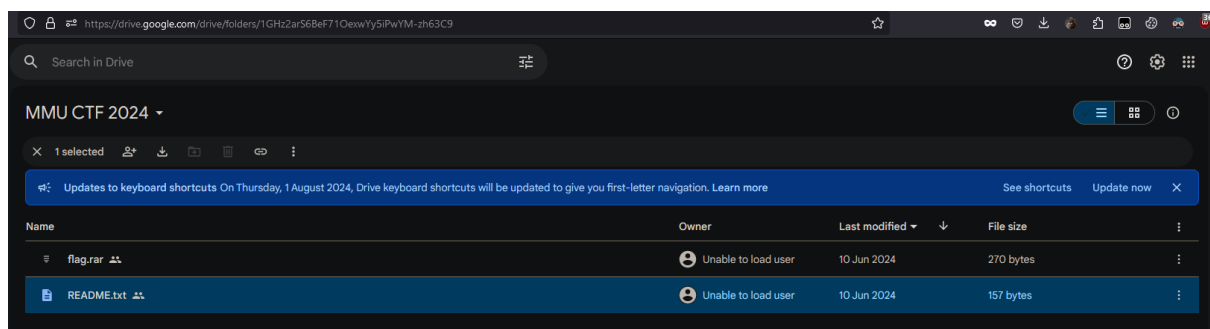
The next 8 bytes represent ASCII characters again. In your case:

57 41 56 45 - WAVE  
66 6d 74 20 - fmt.

After the file can be opened, use Audacity and import the file and show it in the spectrogram form and there's a link given.



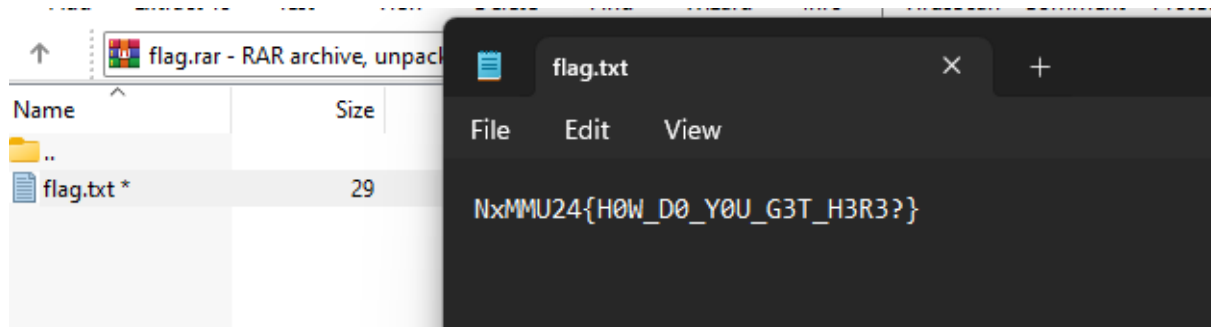
Search the link and download the file.



Unzip the flag.rar with the passphrase given which is -500. I tried to insert the passphrase in previous, but it shows incorrect.

```
A zoo has 1000 sums of rhinoceros and parrots. The total number of animal legs is 2500. How many parrots are there?
```

```
P@55WORD ZIP = rhinoceros - parrots
```



## Web

### Just a normal website





I tried to use gobuster to lookup for any possible file, but it seems nothing.

```
(k3shi@kali)-[~/Downloads/ctf/web]
$ gobuster dir -u https://mmuctf-normalwebsite.chals.io/ -w /usr/share/dirb/wordlists/common.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

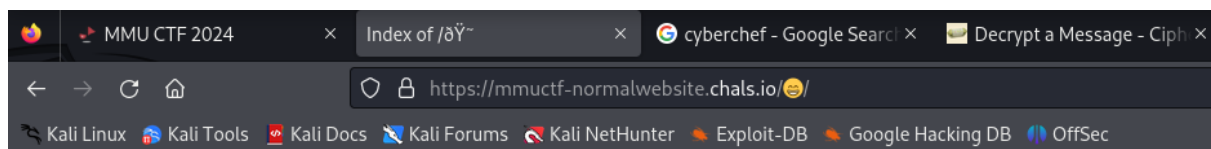
[+] Url: https://mmuctf-normalwebsite.chals.io/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/.hta (Status: 403) [Size: 199]
/.htaccess (Status: 403) [Size: 199]
/.htpasswd (Status: 403) [Size: 199]
/index.html (Status: 200) [Size: 490]
Progress: 4614 / 4615 (99.98%)

Finished
```

With the hint given, I try to insert the emoji behind the url and it navigate to the page where showing flag.html.



## Index of /ðŸ˜~

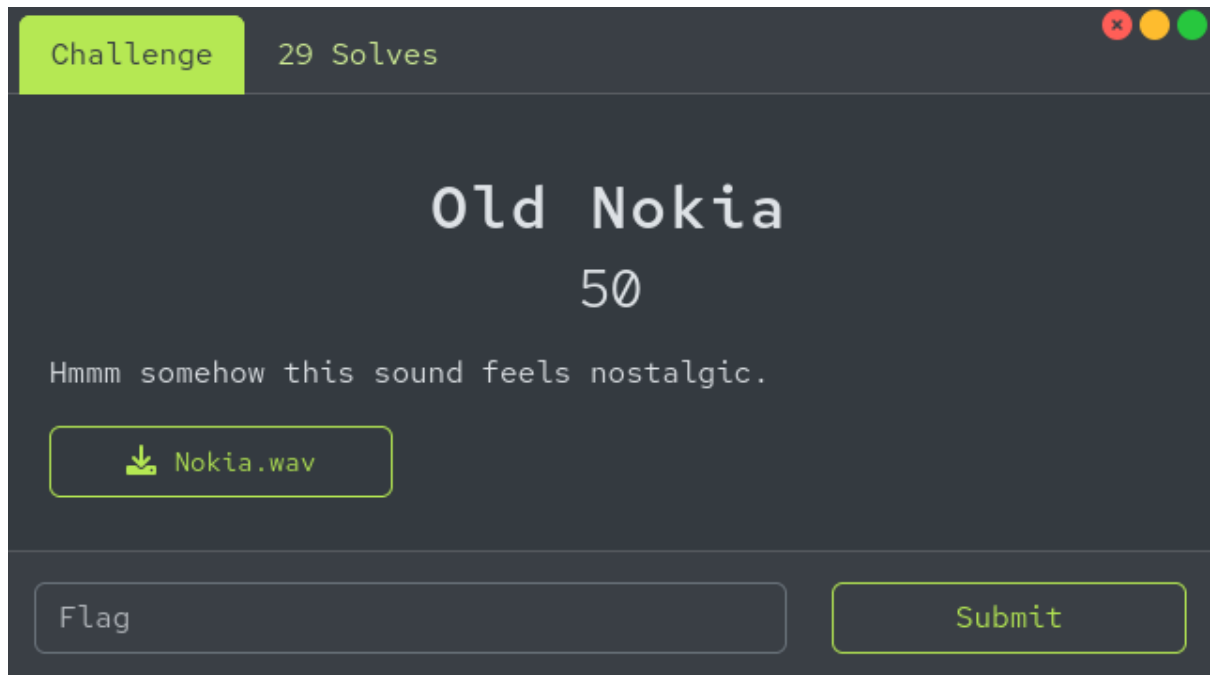
- [Parent Directory](#)
- [flag.html](#)

Click on flag.html and we get the flag.

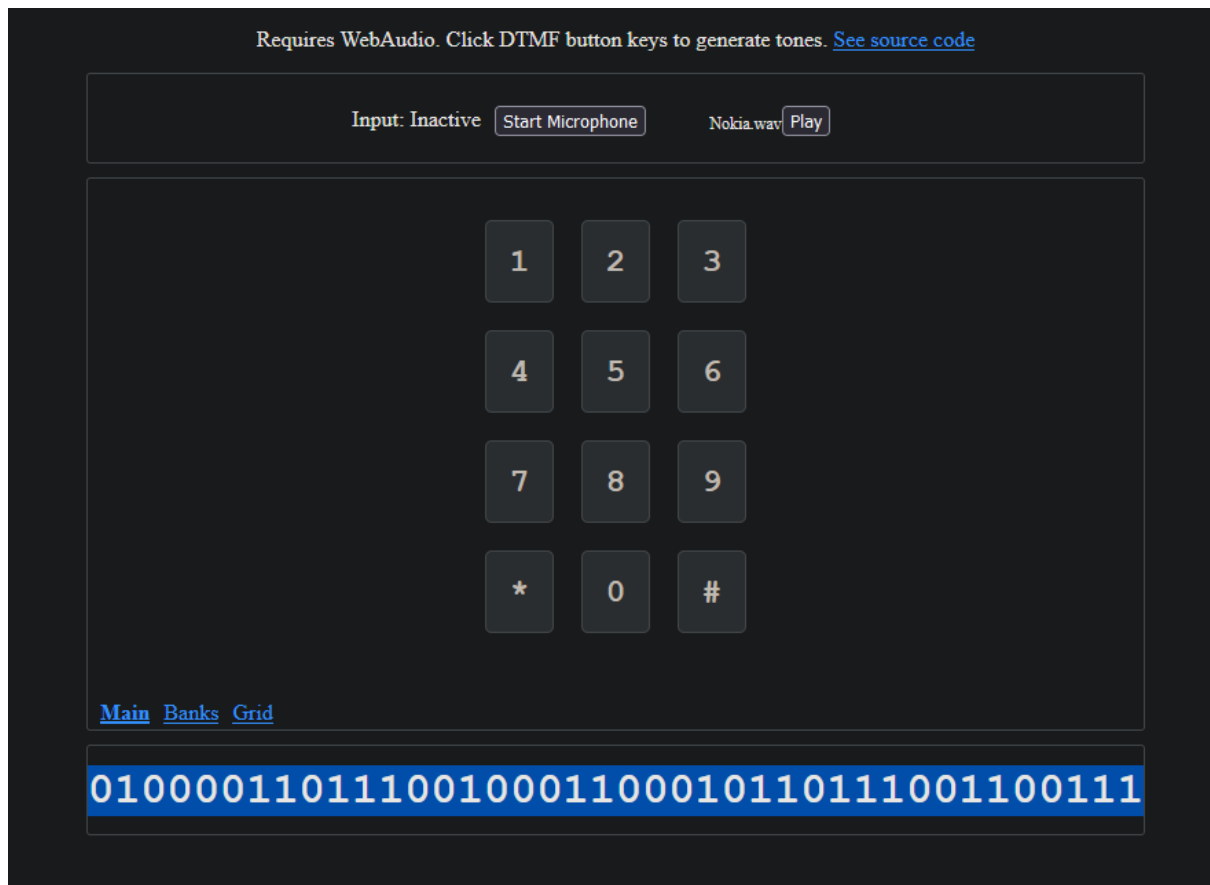
NxMMU24{c0ngr4t5\_it\_w0rks}

## Misc

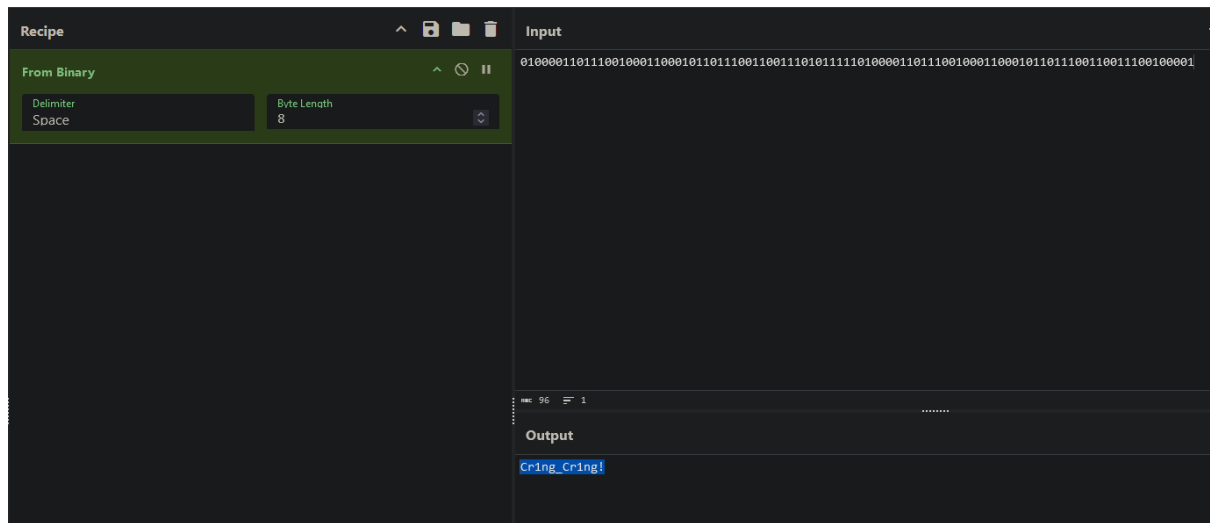
### Old Nokia



I heard a phone dialling sound when I opened the file. So, I try to look up for phone dial audio detector and luckily, I found one.



Copy the binary number and decode using cyberchef and we got the flag.



Flag: NxMMU24{Cr1ng\_Cr1ng!}

Nice to meet you!



I just use an aircrack-ng when I saw the cap file.

```
(k3shi@kali)-[/usr/share/wordlists]
$ aircrack-ng ~/Downloads/ctf/misc/nicotomeetyou/wpa.cap -w /usr/share/wordlists/rockyou.txt
Reading packets, please wait...
Opening /home/k3shi/Downloads/ctf/misc/nicotomeetyou/wpa.cap
Read 13 packets.

# BSSID          ESSID          Encryption
1 00:0D:93:EB:B0:8C test          WPA (1 handshake)
```

And we got the flag.

```
Aircrack-ng 1.7

[00:01:21] 153164/14344392 keys tested (1925.57 k/s)

Time left: 2 hours, 2 minutes, 49 seconds

KEY FOUND! [ biscotte ]

Master Key   : CD D7 9A 5A CF B0 70 C7 E9 D1 02 3B 87 02 85 D6
              39 E4 30 B3 2F 31 AA 37 AC 82 5A 55 B5 55 24 EE

Transient Key : 33 55 0B FC 4F 24 84 F4 9A 38 B3 D0 89 83 D2 49
              73 F9 DE 89 67 A6 6D 2B 8E 46 2C 07 47 6A CE 08
              AD FB 65 D6 13 A9 9F 2C 65 E4 A6 08 F2 5A 67 97
              D9 6F 76 5B 8C D3 DF 13 2F BC DA 6A 6E D9 62 CD

EAPOL HMAC   : 28 A8 C8 95 B7 17 E5 72 27 B6 A7 EE E3 E5 34 45
```

Flag: NxMMU{biscotte}

## Cow breeder

Challenge

30 Solves

# Cow Breeder

## 100

Mr Say is a cow breeder and he's also my uncle, i found this message on his secret drawer. Do you know what is it?

► Unlock Hint for 0 points

 Cow\_Breeder.zip

Flag

Submit

Unzip and cat the file showing a lot of moo moo.

```
(k3shi@kali)-[~/Downloads/ctf/misc/cow]
$ unzip Cow_Breeder.zip
Archive: Cow_Breeder.zip
  inflating: 1.txt
  inflating: 2.txt
  inflating: 3.txt
  inflating: 4.txt
  inflating: 5.txt
  inflating: 6.txt

(k3shi@kali)-[~/Downloads/ctf/misc/cow]
$ cat 1.txt
OOOMoOMoOMoOMoOMoOMoOMoOMoOMMMmoOMMMMMmoOMMMMOOMoOmOomOmoOmoOmO
MMMMmoOMMMMMmoOMMMMOOMoOmOmoOmOmoOmOmmmoOMMMmoOMMMMMmoOMMMMOOMoOmO
MoOmOmoOmOOOmO000mOomOoMMmoOMMMMOOMoOmOmoOmOmoOmOmoOmOmoOmOmoOmO
MoOMoOMoOMoOMoOMoOMoOMoOMoOMoOmOo000mO000mOomOoMMmoOMMMMOOMoO
moOMoOmOomoomOomOoMMmoOMMMMOOMoOmOmoOmOmoOmOmoOmOmoOmOoMMmoOmO
moOMMMMOOMoOmOmoOmOmoOmOmoOmOmoOmOmoOmOmoOmOmoOmOmoOmOmoOmOmoOmO
mOomOoMMmoOMMMMOOMoOmOmoOmOmoOmOmoOmOmoOmOmoOmOmoOmOmoOmOmoOmOmoOmO
```

Use a moo moo decoder to to decode the 1.txt can I saw the flag header starting with Nx and I know that we need to combine all the 5 file.

Moo (Cow) ?

Decrypt

Encrypt

Coordinates:

Nx

Combine all the moo moo messages and we get the flag.

# Moo (Cow) ?

DecryptEncrypt

NxMMU24{W0w\_do\_y0u\_Und3rStaNd\_C0w?}  
Done.

Reverse

to UpperCase

no spaces

Coords

Reset

Reload cipher

Prefill test values

# Moo (Cow) ?

DecryptEncrypt

NxMMU24{W0w\_do\_y0u\_Und3rStaNd\_C0w?}  
Done.

Reverse

to UpperCase

no spaces

Coords

Reset

Reload cipher

Prefill test values

Flag: NxMMU24{W0w\_do\_y0u\_Und3rStaNd\_C0w?}