

Try Hack Me CTF collection Vol.1

Write Up

About the room:

The CTF collection Vol.1 is designed for beginners and focuses on sharpening up our CTF skill. The room has 20 levels.

Task 1: What does the base said?

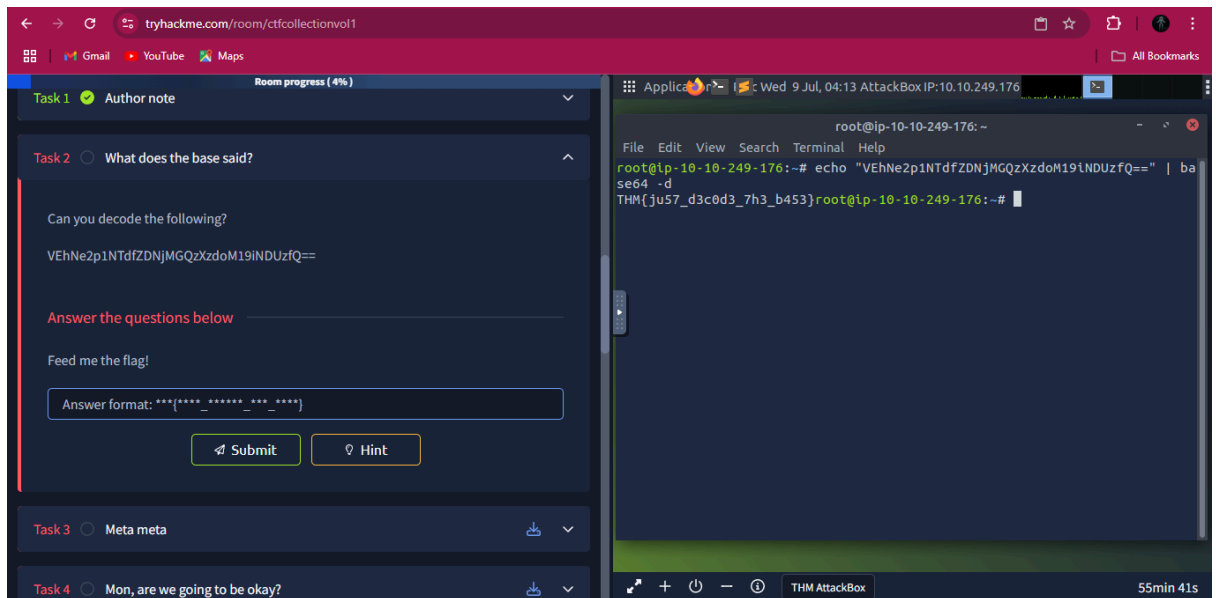
- **Challenge**

Can you decode the following?

VEhNe2p1NTdfZDNjMGQzXzdoM19iNDUzfQ==

- **Solution**

This looks like a base64 encoded message. So I decoded it.



Flag: THM{ju57_d3c0d3_7h3_b453}

Task 2: Meta meta

- **Challenge**

Meta! meta! meta! meta.....

I'm hungry, I need the flag.

Download Task Files: Findme.jpg

- **Solution**

First I downloaded the image. Then to analyse its meta data, I used exiftool.

```
└─$ exiftool Findme.jpg
ExifTool Version Number      : 12.57
File Name                    : Findme.jpg
Directory                    : .
File Size                    : 35 kB
File Modification Date/Time   : 2023:06:17 11:41:01+01:00
File Access Date/Time        : 2023:06:17 11:41:01+01:00
File Inode Change Date/Time   : 2023:06:17 11:42:09+01:00
File Permissions              : -rwxr-xr-x
File Type                    : JPEG
File Type Extension          : jpg
MIME Type                    : image/jpeg
JFIF Version                 : 1.01
X Resolution                  : 96
Y Resolution                  : 96
Exif Byte Order               : Big-endian (Motorola, MM)
Resolution Unit               : inches
Y Cb Cr Positioning           : Centered
Exif Version                  : 0231
Components Configuration      : Y, Cb, Cr, -
Flashpix Version              : 0100
Owner Name                    : THM{3x1f_0r_3x17}
Comment                      : CREATOR: gd-jpeg v1.0 (using IJG JPEG
Image Width                   : 800
Image Height                  : 480
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                    : 800x480
Megapixels                    : 0.384
```

Flag: THM{3x1f_0r_3x17}

Task 3: Mon, are we going to be okay?

- **Challenge**

Something is hiding. That's all you need to know.

It is sad. Feed me the flag.

Download Task Files: Extinction.jpg

- **Solution**

I downloaded the image and used exiftool on it but it revealed nothing. So I used steghide. That revealed an embedded text file named "Final_message.txt". On reading it, it revealed the flag.

```
$ steghide info Extinction.jpg
"Extinction.jpg":
  format: jpeg
  capacity: 1.3 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
  embedded file "Final_message.txt":
    size: 79.0 Byte
    encrypted: rijndael-128, cbc
    compressed: yes
```

```
$ steghide extract -sf Extinction.jpg
Enter passphrase:
wrote extracted data to "Final_message.txt".

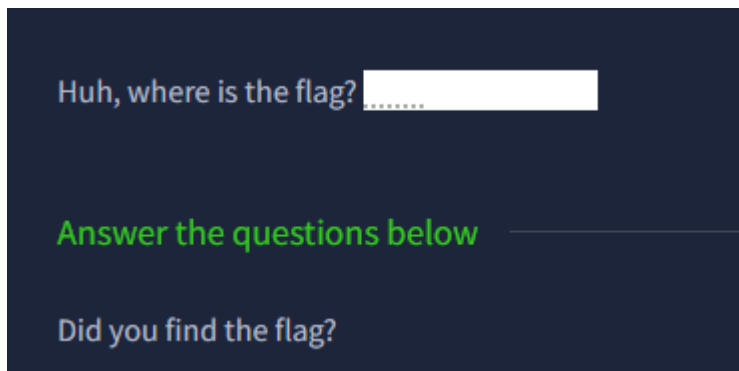
$ cat Final_message.txt
It going to be over soon. Sleep my child.

THM{500n3r_0r_l473r_17_15_0ur_7urn}
```

Flag: THM{500n3r_0r_l473r_17_15_0ur_7urn}

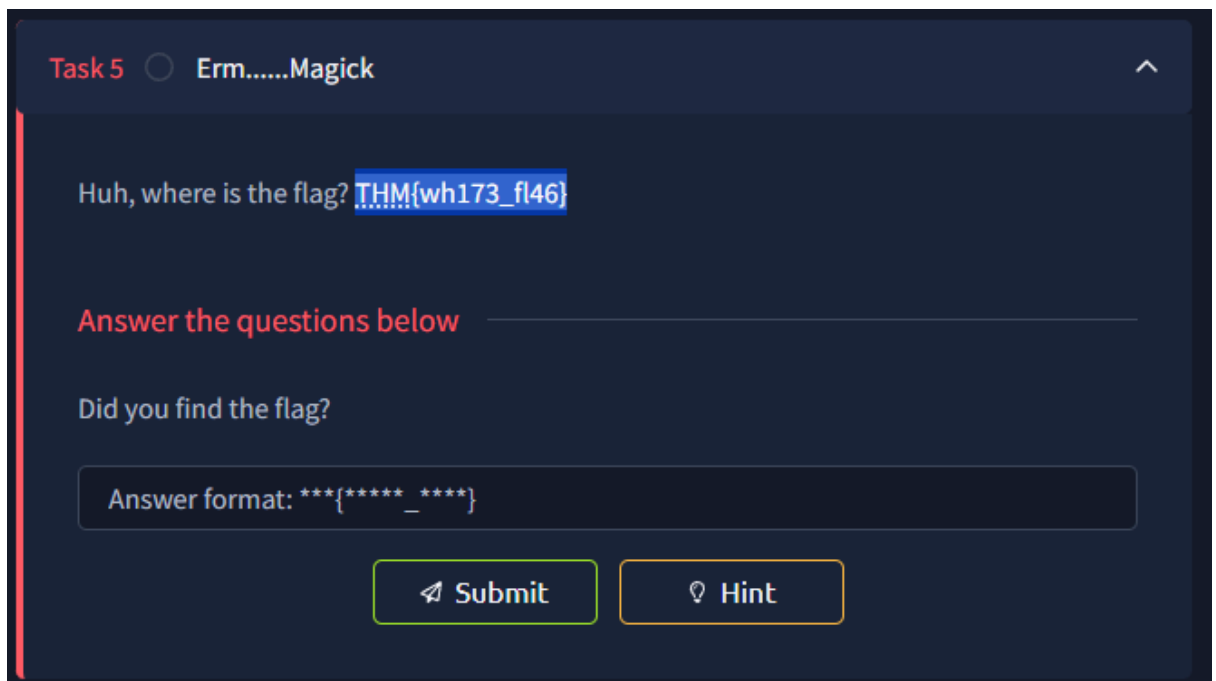
Task 4: Erm.....Magick

- **Challenge**



- **Solution**

For this challenge, I just highlighted the white space and it revealed the next flag.



Flag: THM{wh173_fl46}

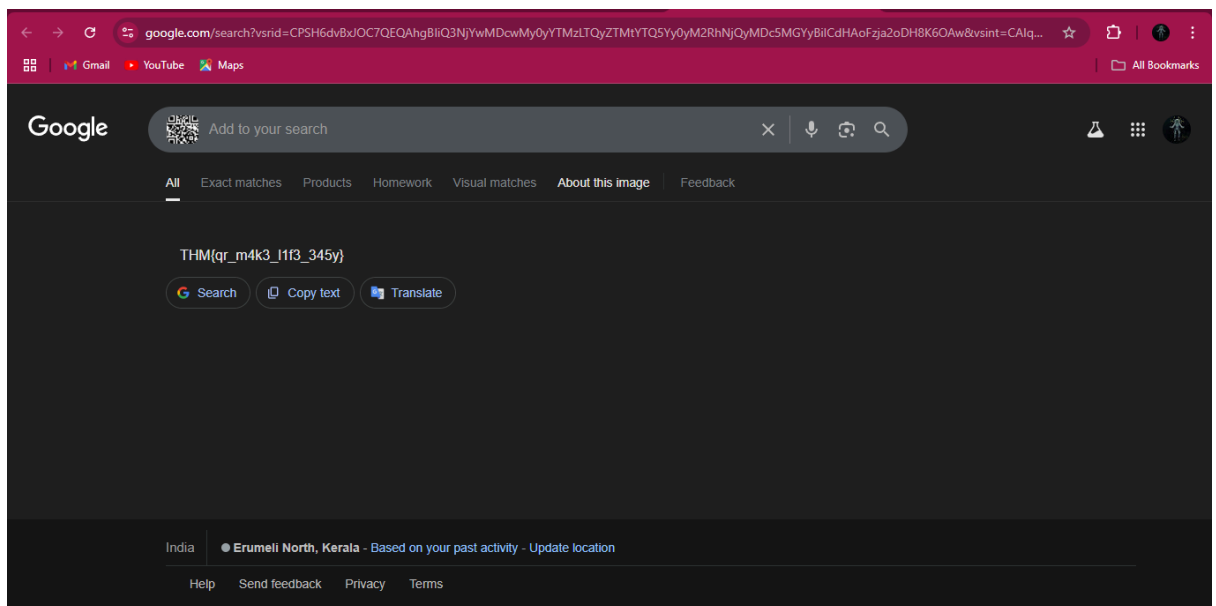
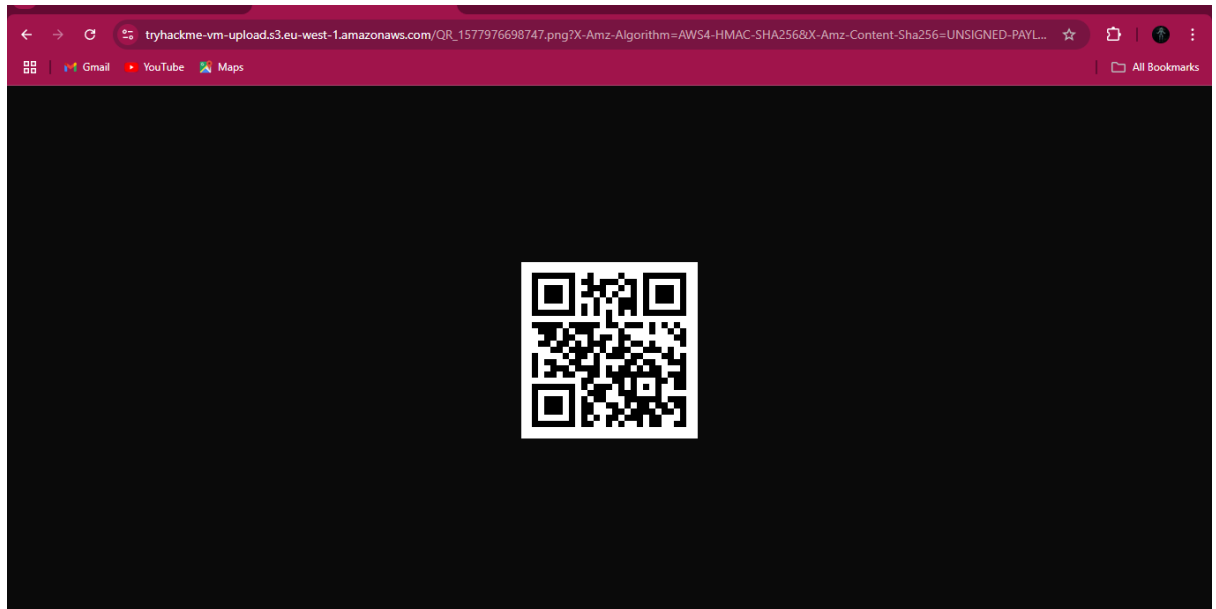
Task 5: Qrrrr

- **Challenge**

Such technology is quite reliable.
More flag, please!
Download Task Files: QR.png

- **Solution**

The image in this challenge turned out to be a QR so I scanned it using google lens which revealed the next flag



Flag: THM{qr_m4k3_l1f3_345y}

Task 6: Reverse it or read it?

- **Challenge**

Both work, it's all up to you.

Found the flag?

Download Task Files: hello.hello

- **Solution**

I took the “read” approach here. So I extracted the strings from the file and sorted it for strings that began with THM (case-insensitive) which gave me the flag.

```
$ strings hello.hello | grep -i thm{  
THM{345y_f1nd_345y_60}
```

Flag: THM{345y_f1nd_345y_60}

Task 7: Another decoding stuff

- **Challenge**

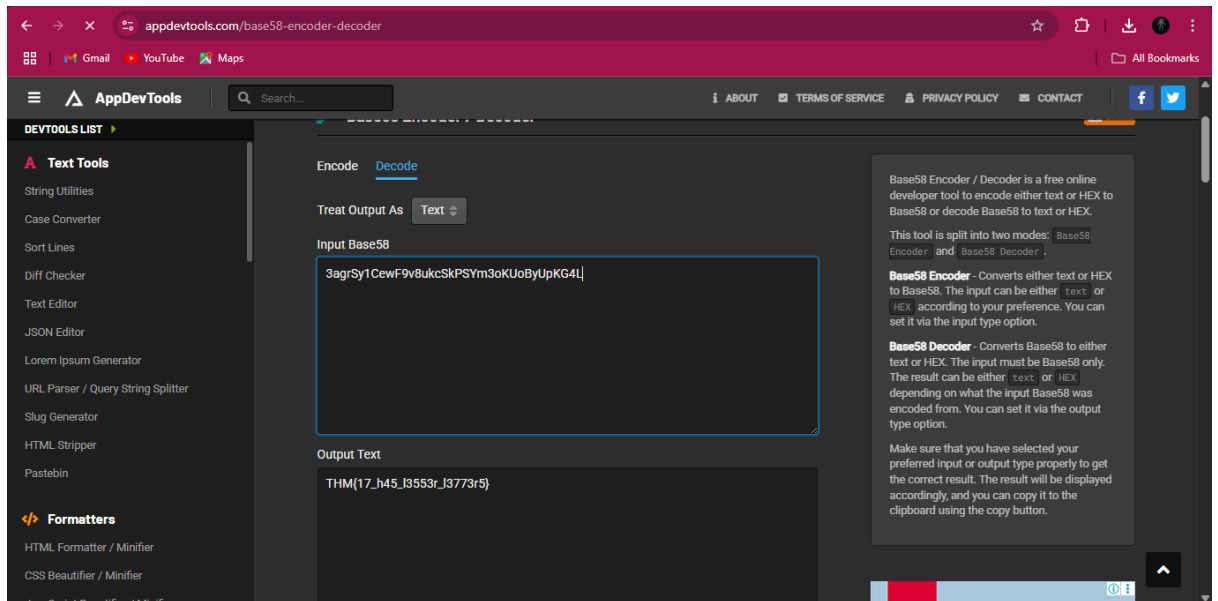
Can you decode it?

3agrSy1CewF9v8ukcSkPSYm3oKUoByUpKG4L

Oh, Oh, Did you get it?

- **Solution**

So at first I thought it was another base64 encoding but it was not. So after using an online base decoder, I discover that it was an base58 encoding and after decoding it I got the flag.



Flag: THM{17_h45_l3553r_l3773r5}

Task 8: Left or right?

- **Challenge**

Left, right, left, right... Rot 13 is too mainstream. Solve this

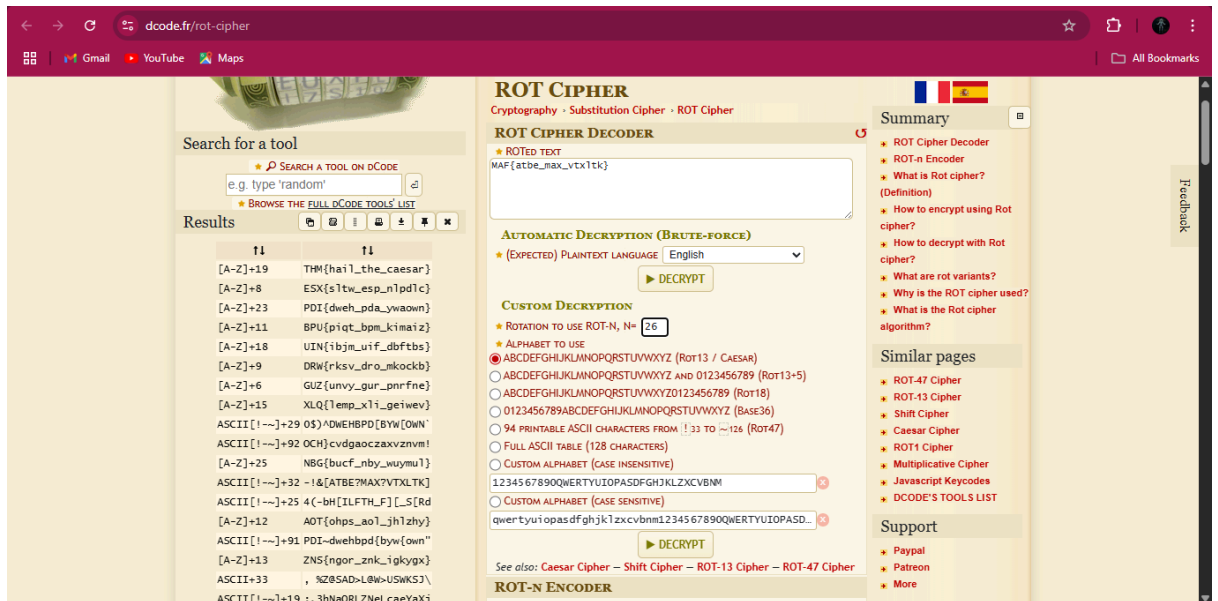
MAF{atbe_max_vtxltk}

What did you get?

- **Solution**

For this challenge, I used an online decoder:

<https://www.dcode.fr/rot-cipher>.



Flag: THM{hail_the_caesar}

Task 9: Make a comment

• Challenge

No downloadable file, no ciphered or encoded text. Huh

I'm hungry now... I need the flag

• Solution

Since we had nothing to go on, I checked the hint which said to check the html. So I checked source code and found the flag.

```
<div class="room-task-desc"> flex
  <div class="room-task-desc-data">
    <p>
      "No downloadable file, no ciphered or encoded text. Huh ....."
    <br>
  </p>
  <p style="display:none;"> THM{4lw4y5_ch3ck_7h3_c0m3mn7} </p>
</div>
```

Flag: THM{4lw4y5_ch3ck_7h3_c0m3mn7}

Task 10: Can you fix it?

- **Challenge**

I accidentally messed up with this PNG file. Can you help me fix it?

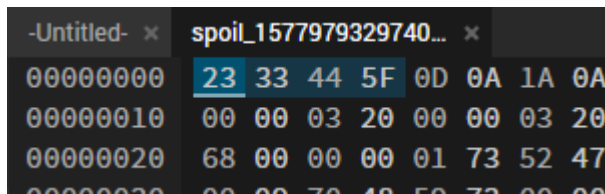
Thanks, ^^

What is the content?

Download Task File: [spoil.png](#)

- **Solution**

When I downloaded it, the image did not open and was giving an error message. Checking its hex, I found the first numbers to be corrupted as for a png it should be 89 50 4e 47.



-Untitled- x	spoil_1577979329740... x
00000000	23 33 44 5F 0D 0A 1A 0A
00000010	00 00 03 20 00 00 03 20
00000020	68 00 00 00 01 73 52 47
00000030	00 00 70 48 59 72 00 00

So I changed it and then tried opening the image.



THM{y35_w3_c4n}

Flag: THM{y35_w3_c4n}

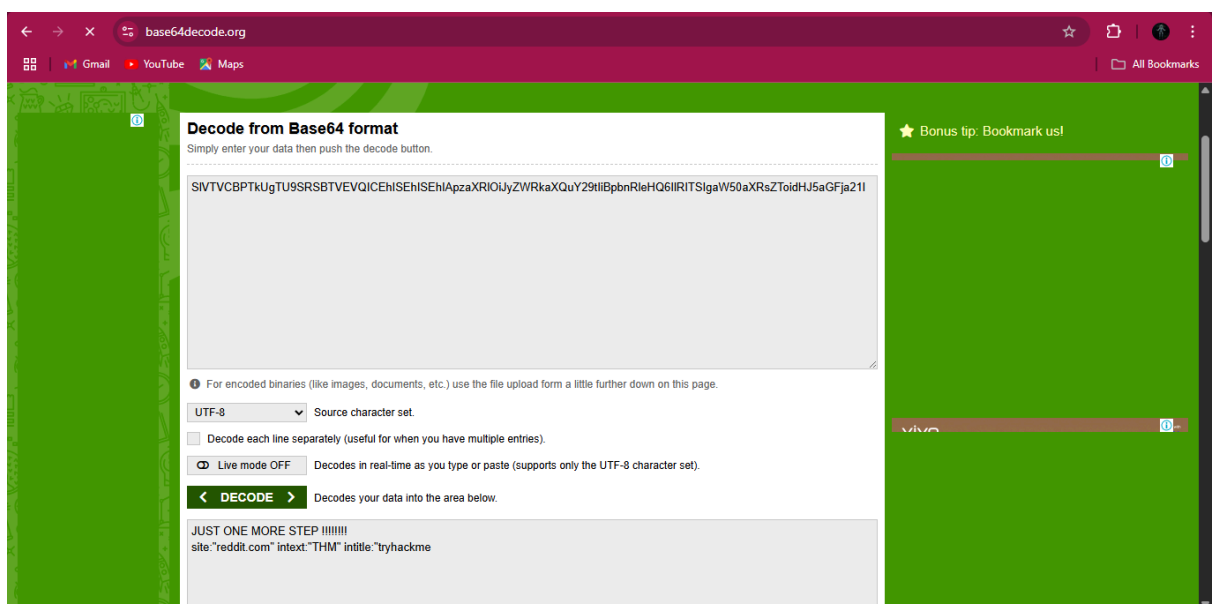
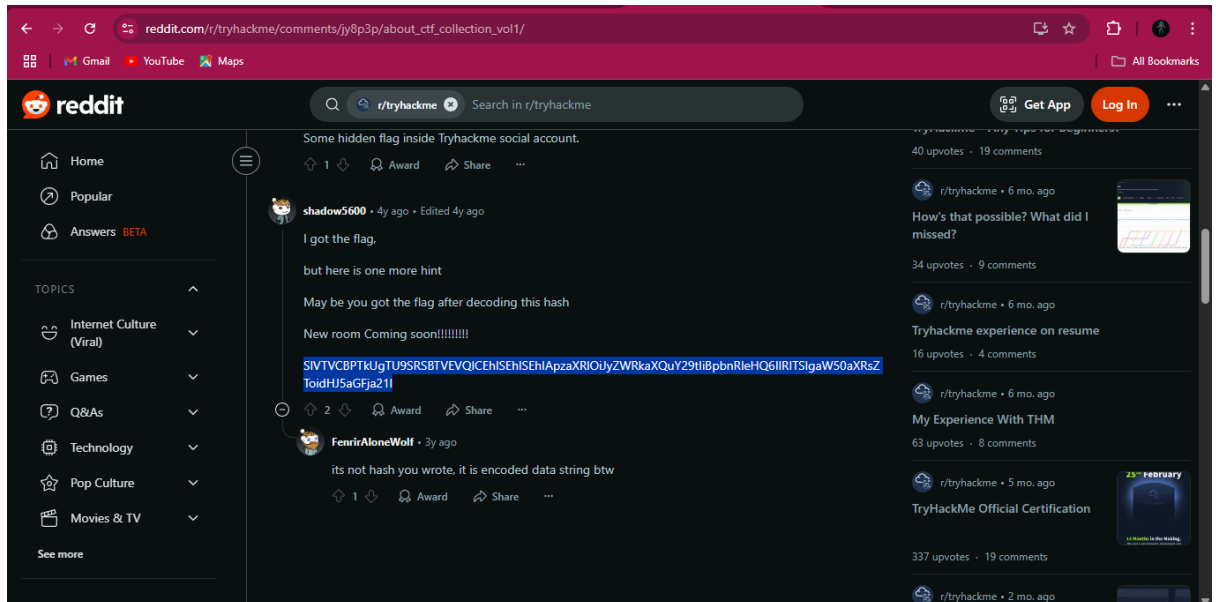
Task 11: Read It

- **Challenge**

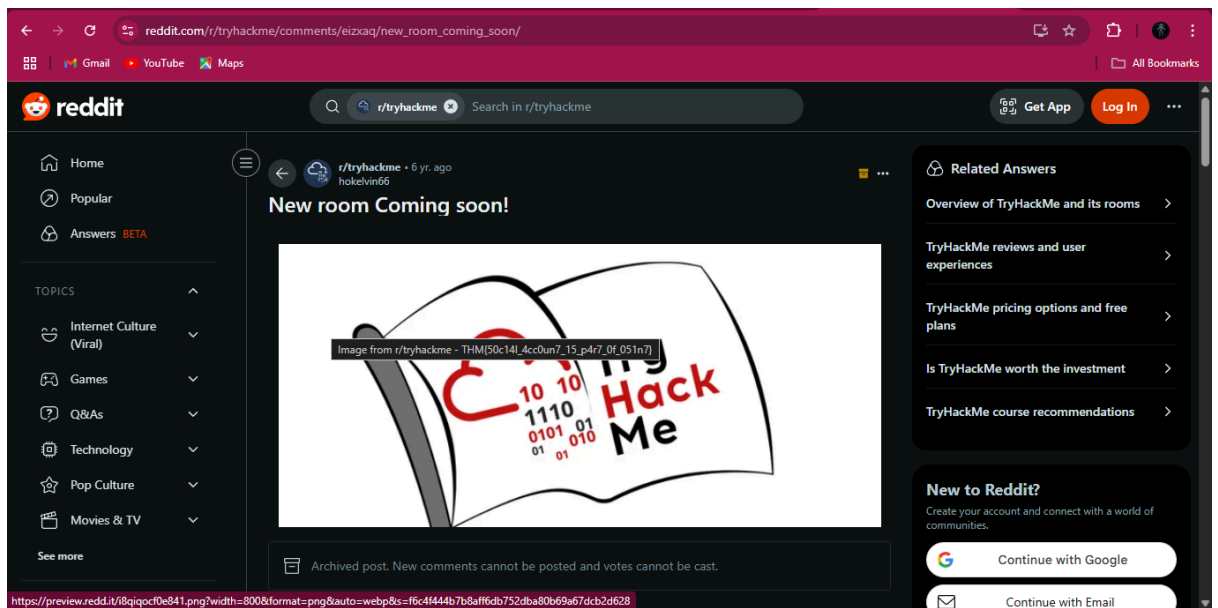
Some hidden flag inside the Tryhackme social account.
Did you find the hidden flag?

- **Solution**

Here also I used a hint. It said to check reddit. So after checking a lot of reddit posts and subreddit I found a clue in one thread which was a base64 encoded.



After pasting the query in Google, I found another reddit which had the flag in an image.



Flag: THM{50c14l_4cc0un7_15_p4r7_of_051n7}

Task 12: Spin my head

● Challenge

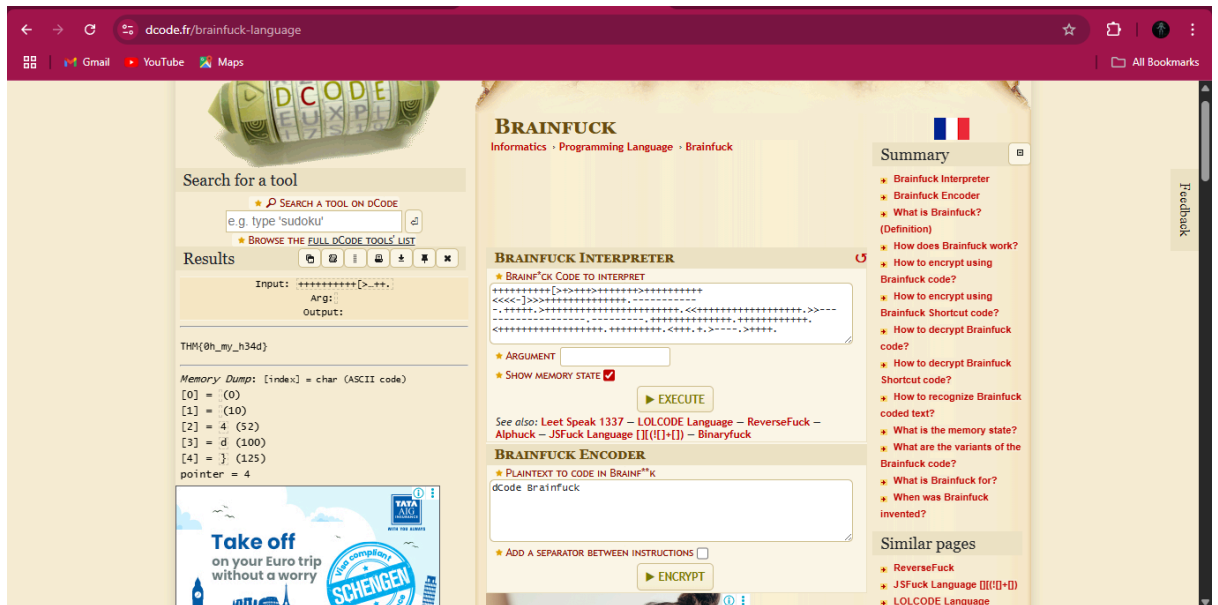
What is this?

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

Can you decode it?

● Solution

I had to use another clue for this challenge. It said it was a brainfuck encryption. So again using the online decoder I decoded the text.



Flag: THM{0h_my_h34d}

Task 13: An exclusive

● Challenge

Exclusive strings for everyone!

S1: 44585d6b2368737c65252166234f20626d

S2: 101010101010101010101010101010101010

Did you crack it? Feed me now!

● Solution

Given the name of the challenge and the two strings given, I calculated the XOR of the strings using an online calculator. The result was the reverse of the flag.

Ascii Result:

```
}r0_3v15ulcx3{MHT
```

The result of XOR operation in Ascii

Flag: THM{3xclu51v3_0r}

Task 14: Binary walk

- **Challenge**

Please exfiltrate my file :)

Flag! Flag! Flag!

Download Task File: hell.jpg

- **Solution**

As the name suggested I used binwalk on the file.

DECIMAL	HEXADECIMAL	DESCRIPTION

0	0x0	JPEG image data, JFIF standard 1.02
30	0x1E	TIFF image data, big-endian, offset of first image directory: 8
265845	0x40E75	Zip archive data, at least v2.0 to extract, uncompressed size: 69, name: hello_there.txt
266099	0x40F73	End of Zip archive, footer length: 22

So to extract the “hello_there.txt” I used binwalk -e hell.jpg. This created a directory with the text file which had the flag.

Flag: THM{y0u_w4lk_m3_0u7}

Task 15: Darkness

- **Challenge**

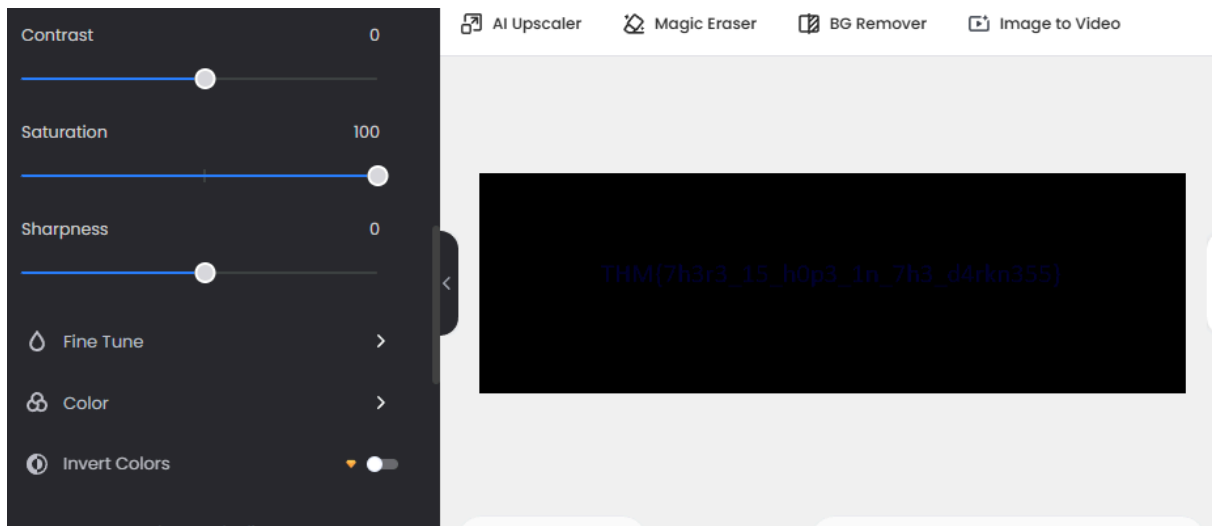
There is something lurking in the dark.

What does the flag said?

Download Task File: dark.png

- **Solution**

The image was a black rectangle. After playing with the saturation, color and contrast for a while I found the flag superimposed in it.



Flag: THM{7h3r3_15_h0p3_1n_7h3_d4rkn355}

Task 16: A sounding QR

- **Challenge**

How good is your listening skill?

P/S: The flag formatted as THM{Listened Flag}, the flag should be in All CAPS

Download Task File: QRCTF.png

- **Solution**

The downloaded image was again a QR. It took me to a soundcloud audio which played the flag.

Flag: THM{SOUNDINGQR}

Task 17: Dig up the past

- **Challenge**

Sometimes we need a 'machine' to dig the past.

Targetted website:

<https://www.embeddedhacker.com/>

Targetted time: 2 January 2020

- **Solution**

As the title suggests we need to go to a previous date of the website. For this I used Internet Archive's WayBack Machine(<https://archive.org/web/>) and opened the page on 2 Jan 2020. Along the contents I found the flag



Flag: THM{ch3ck_th3_h4ckb4ck}

Task 18: Uncrackable!

- Challenge

Can you solve the following? By the way, I lost the key.

Sorry >.<

MYKAHODTQ{RVG_YVGGK_FAL_WXF}

Flag format: TRYHACKME{FLAG IN ALL CAP}

- Solution

After a bit of research, I found out that the given crypt is a Vigenere Cipher. So using an online decoder, I decoded the cipher to give the flag.

Search for a tool

★ [SEARCH A TOOL ON DCODE](#)

★ [BROWSE THE FULL DCODE TOOLS' LIST](#)

Results

Warning Showing most likely results

ABCDEFGHIJKLMNOPQRSTUVWXYZ (26)

↑↓	↑↓
THM	TRYHACKME{YOU_FOUND_THE_KEY}
THMTHM	TRYHACKME{YOU_FOUND_THE_KEY}
THMTHMTHM	TRYHACKME{YOU_FOUND_THE_KEY}
ZYTUGDAXAX	NARENIATT{RYH_ACKME_CAO_WAG}
YFTCAOBJENE	OTRYHACKM{ERI_TCEGW_ERH_JTH}
UURTOXFMQPL	SETHTRYHA{CKM_EENSN_AOV_HML}
YFEIZKDQZSE	OTGSIADR{ZRI_TRYHA_CKM_ETH}
YGRJJHHRGFR	OSTRYHACK{MEI_SEXXD_CJF_RGH}
WMRTDVMVJRT	QMTHETRYH{ACK_MENDP_TFC_FEJ}
EOJCDCKCKSKV	IKBYEMTRY{HAC_KMEDI_VYT_MCB}
YGCPIDFYBKT	OSILZLYVP{HCI_STRYH_ACK_MEH}
BGRNPMYAJML	LSTNSCFTH{FKF_SETRY_HAC_KME}
IRVEWYBAYYE	EHPWLQCTS{TRY_HACKM_EAN_YTX}
AJMLBNPMY	MPYPGBOHS{RMU_NUTRY_HAC_KME}
NHXZGIVOHDE	ZRNBBGIFJ{ORT_RYHAC_KME_TTS}

VIGENERE CIPHER

Cryptography · Poly-Alphabetic Cipher · Vigenere Cipher

VIGENERE DECODER

★ VIGENERE CIPHERTEXT

★ PLAINTEXT LANGUAGE English

★ ALPHABET ABCDEFGHIJKLMNOPQRSTUVWXYZ

▶ AUTOMATIC DECRYPTION

DECRYPTION METHOD

☐ KNOWING THE KEY/PASSWORD: KEY

☐ KNOWING THE KEY-LENGTH/SIZE, NUMBER OF LETTERS: 3

☐ KNOWING ONLY A PARTIAL KEY (JOKER=?): KE?

☒ KNOWING A PLAINTEXT WORD: TRYHACKME

☐ VIGENERE CRYPTANALYSIS (KASISKI'S TEST)

★ SHOW VIGENÈRE'S SQUARE/GRID (TABULA RECTA) ☐

▶ DECRYPT

Flag: TRYHACKME{YOU_FOUND_THE_KEY}

Task 19: Small bases

● Challenge

Decode the following text.

581695969015253365094191591547859387620042736036
246486373595515576333693

● Solution

I had to use a hint for this one. The hint was: dec -> hex
-> ascii. So I used a base converter.

Decimal to Hexadecimal converter

From

Decimal



To

Hexadecimal



Enter decimal number

58169596901525336509419159154785938

10

= Convert

✕ Reset

↕ Swap

Hex number (60 digits)

54484D7B31375F6A7535375F346E5F30726
4316E3472795F62343533357D

16

Hex to ASCII Text String Converter

Enter hex bytes with any prefix / postfix / delimiter and press the *Convert* button
(e.g. 45 78 61 6d 70 6C 65 21):

From: Hexadecimal To: Text

Open File

Paste hex numbers or drop file

54484D7B31375F6A7535375F346E5F307264316E3472795F62343533357D

Character encoding: ASCII

Convert Reset Swap

THM{17_ju57_4n_0rd1n4ry_b4535}

Flag: THM{17_ju57_4n_0rd1n4ry_b4535}

Task 20: Read the packet

- Challenge

I just hacked my neighbor's WiFi and tried to capture some packets.

He must be up to no good. Help me find it.

Download Task Files: flag.pcapng

- Solution

In this scenario, we look for the common protocols that contain data. An assumption is made that our neighbor will be doing some web browsing so I started my analysis by zooming in on HTTP protocol communications. I found a total of 12 HTTP packets (6 requests and 6 responses).

Ignoring the OCSP packets (Online Certificate Status Protocol), we are left with a single HTTP request for /flag.txt and a response that contains our flag.

The image shows a Wireshark packet capture analysis of a file named 'flag.pcapng'. The top toolbar has a red circle '1' next to the 'http' filter. The packet list table below shows several OCSP packets and two HTTP packets. The second HTTP packet (No. 1827) is highlighted with a red box and a red circle '2'. The packet details pane shows the structure of the HTTP response, including headers and a body containing a flag. The flag is highlighted with a yellow box and a red circle '3'.

No.	Time	Source	Destination	Protocol	Length	Info
1186	32.867250827	117.18.237.29	192.168.247.130	OCSP	842	Response
1188	32.869127200	192.168.247.130	117.18.237.29	OCSP	485	Request
1190	33.007430898	117.18.237.29	192.168.247.130	OCSP	842	Response
1194	33.049069644	117.18.237.29	192.168.247.130	OCSP	842	Response
1526	35.030617044	192.168.247.130	117.18.237.29	OCSP	485	Request
1554	35.557862858	192.168.247.130	117.18.237.29	OCSP	485	Request
1557	35.700180599	117.18.237.29	192.168.247.130	OCSP	842	Response
1564	35.722281715	117.18.237.29	192.168.247.130	OCSP	842	Response
1825	52.508233774	192.168.247.130	192.168.247.140	HTTP	506	GET /flag.txt HTTP/1.1
1827	52.509987109	192.168.247.140	192.168.247.130	HTTP	455	HTTP/1.1 200 OK

Content-Type: text/plain\r\n\r\n[HTTP response 1/1]
[Time since request: 0.001753335 seconds]
[\[Request in frame: 1825\]](#)
[Request URI: http://192.168.247.140/flag.txt]
Content-encoded entity body (gzip): 52 bytes -> 32 bytes
File Data: 32 bytes

Line-based text data: text/plain (3 lines)
THM{d0_n07_574lk_m3}\n
Found me!\n

Frame (455 bytes)

Hypertext Transfer Protocol: Protocol | Packets: 2209 | Displayed: 12 (0.5%) | Profile: Default

Flag: THM{d0_n07_574lk_m3}

tryhackme.com/room/ctfcollectionvol1

All Bookmarks

Try Hack Me

Vol. 1

Woop woop! Your answer is correct

Congratulations on completing CTF collection Vol.1!!! 🎉

Points earned

🎯 600

Completed tasks

📋 21

Room type

🚩 Challenge

Difficulty

📶 Easy

Streak

🔥 1

This room counted toward joining the league 🏆