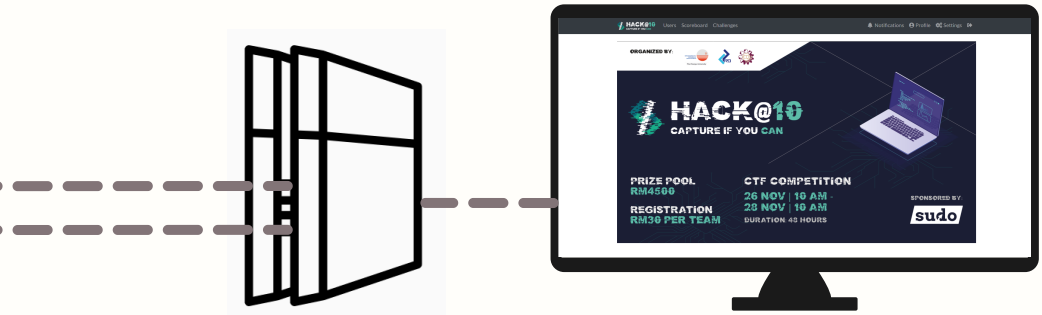
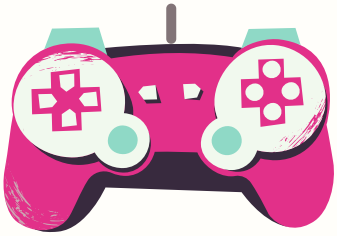
MUSANG✕QWEEN
WRITEUP

↘ MEET THE TEAM



PLAYER 1 : g33exx



PLAYER 2 : 3zm47ch

PLAYER 3 : ph4nt0m

HACK@10 CTF WRITEUP SPONSORED BY sudo

TABLE OF CONTENT

$find 2021/hack10/writeup

↘ PARTICULARS

BROKEN HEART

MISC.

CHALLENGE

300pts
PG 001

We were given a picture of a heart with QR code attached

Scanning the QR gets me a text that I'd never get since I'm a programmer, and good programmers stay single.

Text : I Love You

PROCEDURES

1. TAKE A GOOD WALK IN THE PICTURE

I want to visit inside the heart to see if I can get some love that I've never had during my childhood, I mean get the flag, yep the flag and tried $binwalk -ing to the brokenheart.jpg

```
$ binwalk brokenheart.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
```

And, Ta Da !, looks like the flag's not there, just like my father, that left me.

2. I ALWAYS WANTED A STEGOSAURUS

Since I couldn't get the love, maybe I can get a toy dinosaur from the picture and tried $steghide extract. Of course I need some money, I mean passphrase. Maybe its from the text from the QR code earlier.

```
$ steghide extract -sf brokenheart.jpg -xf out.jpg
Enter passphrase:
wrote extracted data to "out.jpg".
```

After some phrase bargaining, I Love You, 143, iloveyou, we closed the deal and I got my saurus with the phrase ILoveYou.

3. MY SAURUS LOST ITS HEAD !

I got this incomplete QR and the colour's are inverted too.
What a total scam.

The QR is in dark mode cus light attracts bug

POPULATION WIPED HALF .4

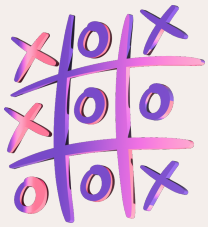
Fine, I'll do it myself - Thanos

I live by this word and fixed the QR by myself and restored humanity

5. HEARTBREAK

Scan the QR and live happily **never** after

flag : hack10{br0k3n_QR_c4n_b3_f1x3d_n0t_br0k3nH34rT}

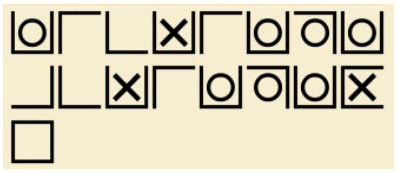


TRIPLE T

CRYPTOGRAPHY

↘ CHALLENGE

50pts
PG 010



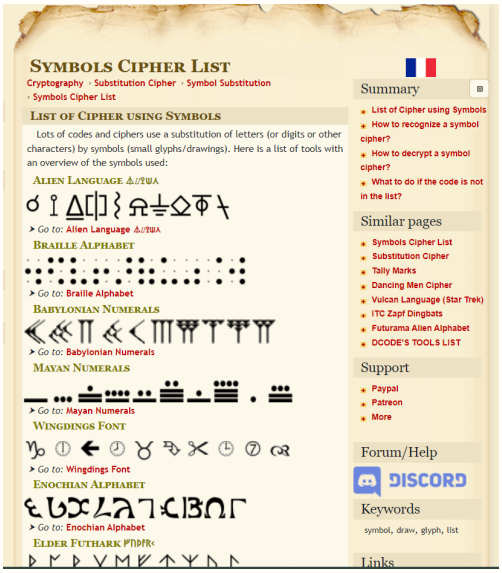
We were given a picture of symbols. It also looks like some laundromat.

First thought : Symbol Cipher

↘ PROCEDURES

1. SEE WHAT WE HAVE IN STORE

I went all the way to **France** to go get myself some cipher tools.



dcode.fr/symbols-cipher

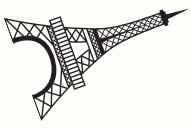
Scrolled through thick layers of baguettes, rioters, and protesters. Oh that's not what I meant.

Well, what do we got here ?

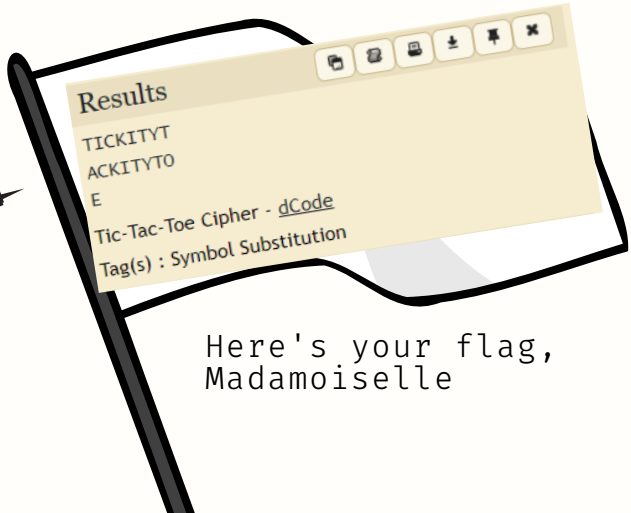
2. VOILA !

Copy the symbol from the picture

Thanks to city Nurhaliza, I mean city of france :D



Annnd, Voila !



Here's your flag, Madamoiselle

flag : hack10{tickitytackitytoe}

DOUBLE P

CRYPTOGRAPHY

↘ CHALLENGE

100pts
PG 011

Another Symbol Cipher !

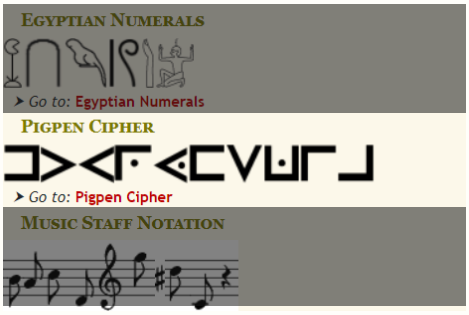
A clue in the description says something about dinosaur that loves to RAR

First thought : France!

↘ PROCEDURES

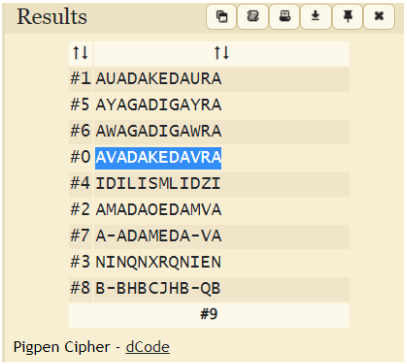
1. WE'RE STILL IN FRANCE ??

CTF's too easy that I lost 3 of them including this one.

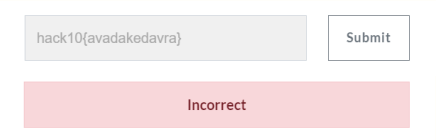


Its PigPen Cipher !

Only one cipher made sense AVADAKEDAVRA !



2. I TRIPPED IN FRANCE, EIFFEL-OVER BACK HOME .3



That's a hard fall. Back to the terminal

I took a deep breath and went for a $binwalk again

Ouiii !!

```
$ binwalk piedPiper.jpg
```

oui

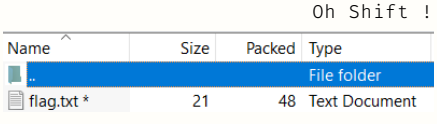
```
DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
7743          0x1E3F          RAR archive data, version 5.x
```

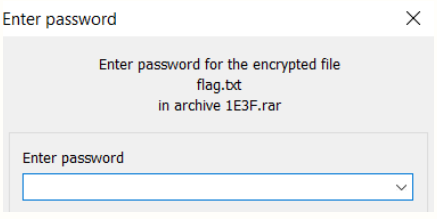
4. ITS RARE TO SEE A RAR IN AN IMAGE

Extract the RAR from picture's binary

```
$ binwalk --dd='.*' piedPiper.jpg
```

Oh Shift !

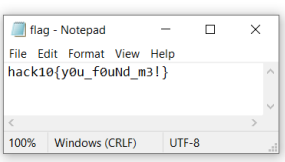




Expelliarmus'd my way in using avadakedavra

I'll keep the flag

But I wonder why my girlfriend doesn't want to keep my baby



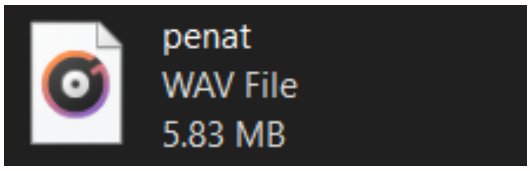
flag : hack10{y0u_f0uNd_m3!}

PENAT

STEGANOGRAPHY

↘ CHALLENGE

150pts
PG 100



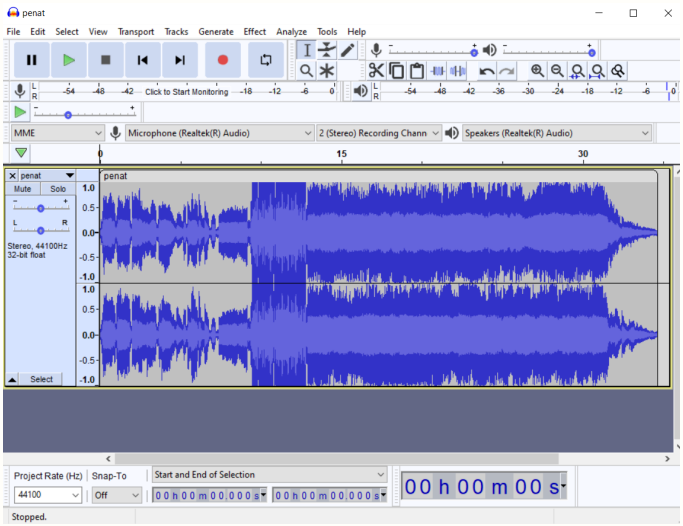
We were given an audio file titled penat.wav

First thought : Audacity

↘ PROCEDURES

1. BLAST TO THE PAST

I loaded the audio to the million years old software, Audacity



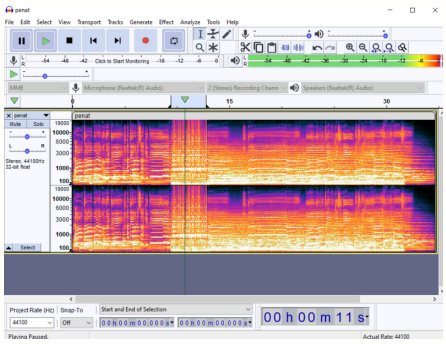
All the sound seems perfectly normal, except from the timeframe

00:09 to 00:13

I figured that the flag is on that part but I never did an audio steganography so I was lost. Just like MH370.

2. I NEEDED TO C#

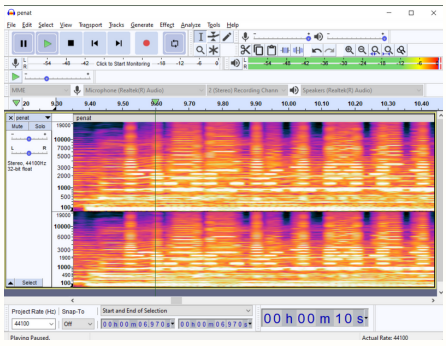
After some time with Audacity and Googling stuffs. I found out we can view the spectogram of the audio to see-sharply.



Nothing here ?
Or there is ?

y r u ask me?

After zooming in on the timeframe



I finally me++ myself by learning new software;

flag : hack10{1M_t1R3d_0f_Mc0_jkjk}

GARY KESSLER

STEGANOGRAPHY

↘ CHALLENGE

150pts
PG 101

We were given an image titled matabatin.jpg which contains Uniten's campus view

First thought : Binwalk

↘ PROCEDURES

1. I LOST MY SON

My son got into UNITEN. Join me $binwalk-ing through his campus.

```
$ binwalk matabatin.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
174253        0x2A8AD         PNG image, 1280 x 720, 8-bit/color RGB, non-interlaced
176218        0x2B05A         Zlib compressed data, default compression
```

2A8AD

See I wasn't lying ! Meet 2A8AD, he's my firstborn.

2. MY SON REQUESTED FOR A SEMESTER EXTENSION

2A8AD failed his final year at UNITEN. I wonder why.

0	11/27/2021 7:14 PM	File	280 KB
2A8AD	11/27/2021 7:14 PM	File	110 KB
2B05A	11/27/2021 7:14 PM	File	2,701 KB
2B05A.zlib	11/27/2021 7:14 PM	ZLIB File	108 KB

Don't tell Elon
2A8AD is not his son.

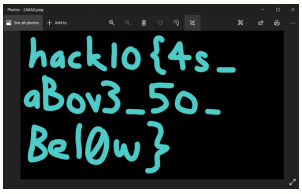
I allowed him to get a PnG extension

```
$ mv 2A8AD 2A8AD.png
```

My son is a certified PnG. Graduate

2A8AD is a reference to X Æ A-Xii Musk

He got me a flag on his graduation



That's my boy !

0	11/27/2021 7:14 PM	File	280 KB
2A8AD	11/27/2021 7:14 PM	PNG File	110 KB
2B05A	11/27/2021 7:14 PM	File	2,701 KB
2B05A.zlib	11/27/2021 7:14 PM	ZLIB File	108 KB

flag : hack10{4s_aBov3_5o_Bel0w}

101

OSINT

20pts
PG 110

CHALLENGE

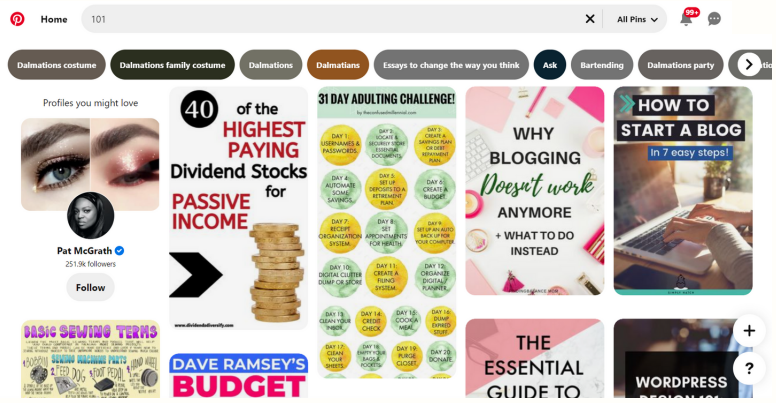
Social media full of images.
Perhaps rotate it 47 times?!

We were given a text.
Well, only text -_-

PROCEDURES

1. WASTE SOME TIME CUS I GOT LOADS

Pinterest got loads of images. Why dont we start with that.

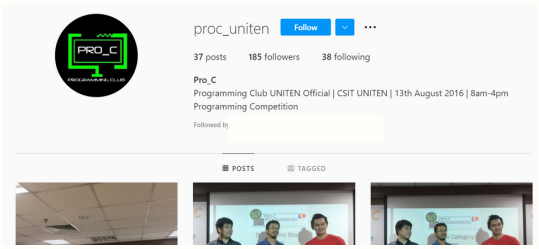


2. GETTING SOMEWHERE, MAYBE

Me realizing Pinterest is not a social media

3. WASTE MORE TIME ON INSTA!

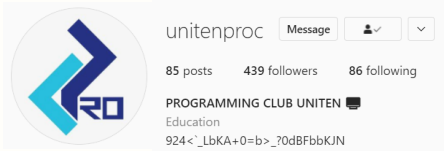
Searched and analyzed all of Pro-C's images and profile



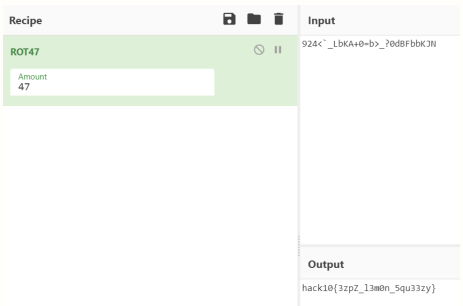
Wrong Insta Account

4. A FRIEND IN NEED

I asked my mates about this. He said he already got it...

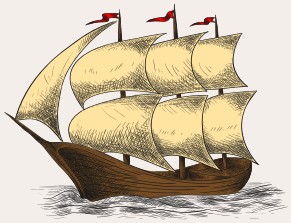


He showed me this...



I didn't get paid enough to do all this...

flag : hack10{3zpZ_l3m0n_5qu33zy}

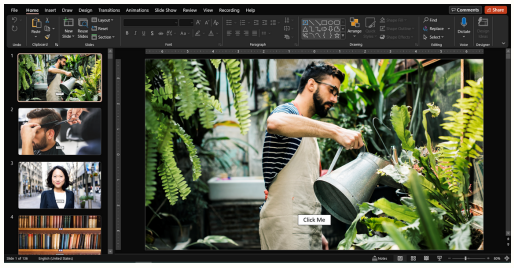


POWER ENOUGH?

MISC.

↘ CHALLENGE

150pts
PG 111

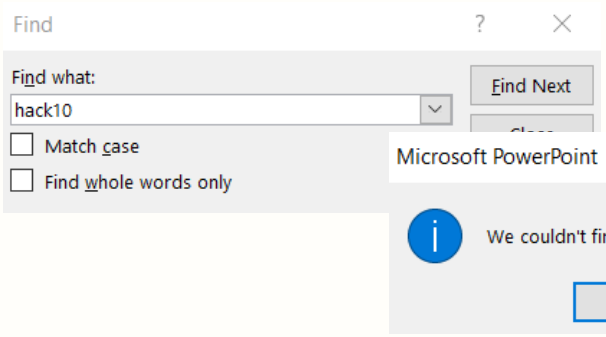


We were given a PowerPoint slides full of HD images with a Click Me button on the middle

↘ PROCEDURES

1. TAKE CONTROL

Why don't we just search for the flag ? CTRL + F

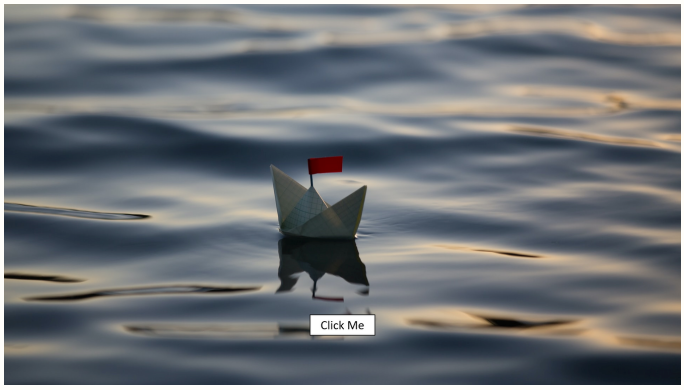


my income before ctf = 0
my income after ctf = 0
i didn't even get arrays.

:(

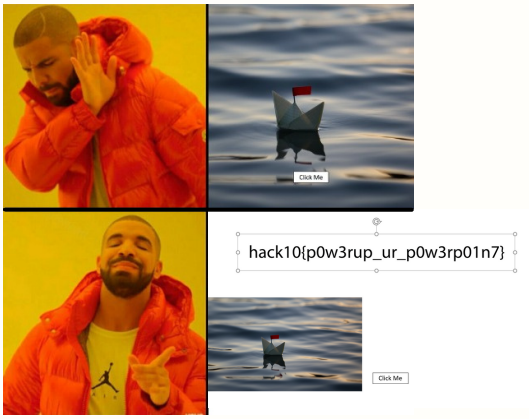
2. MY GAMING MOUSE R.I.P

After clicking the Click Me button with my Asus Rog Strix Impact gaming mouse featuring Aura Sync RGB Lighting with durable 50-million click Omron Switches, I found a flag.



Schmol flag that is

I #include too many <jokes.h>
I'm tired so I'll just put this meme



Put the pic aside and there's our flag
Good thing I joined Pro-C's PowerPoint Workshop

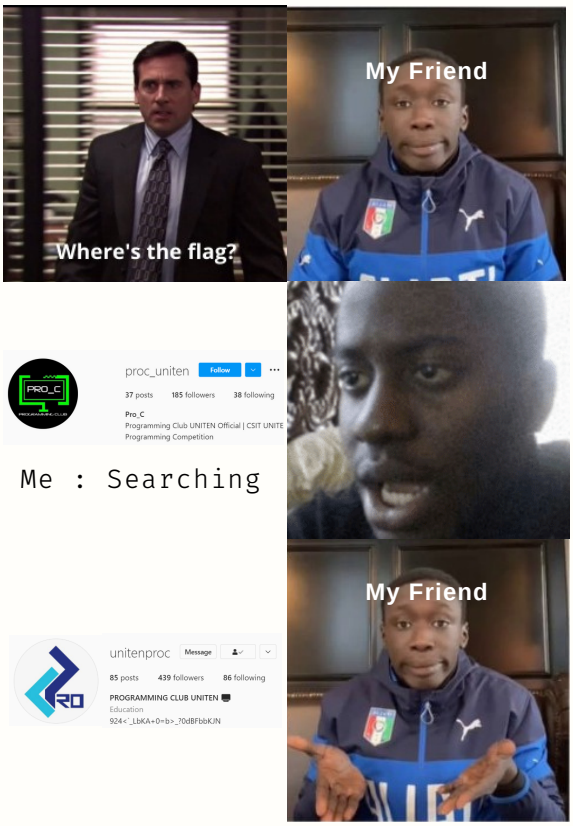
flag : hack10{p0w3rup_ur_p0w3rp01n7}

THANK YOU

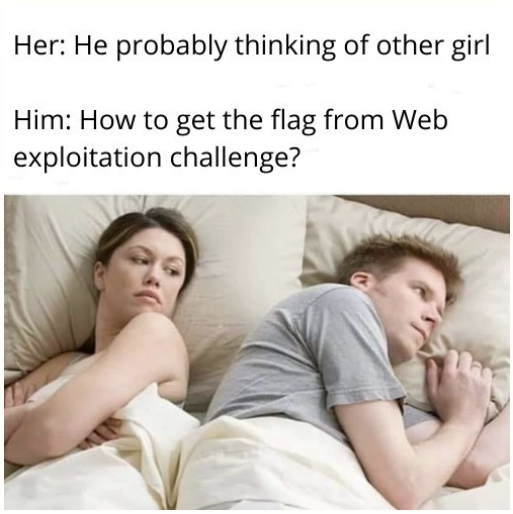
CYA IN NEXT CTF

↘ MEMES

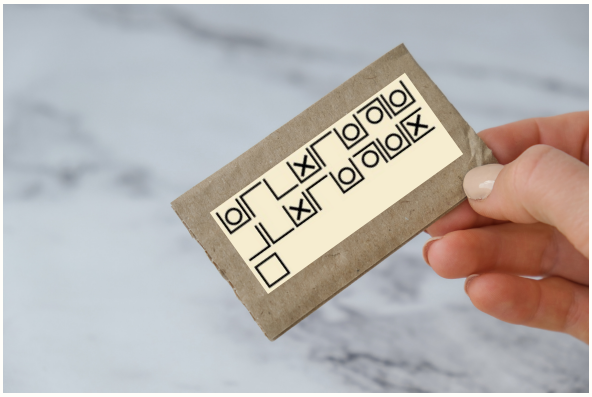
1. ABOUT INSTAGRAM



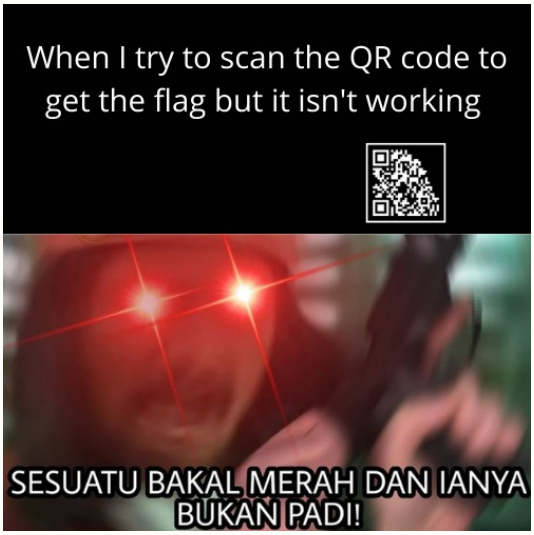
2. ABOUT WEB CHALLENGES



3. ABOUT SQUID GAME



4. ABOUT BROKENHEART



flag : hack10{THANKYOU_FOR_READING_OUR_WRITEUP}