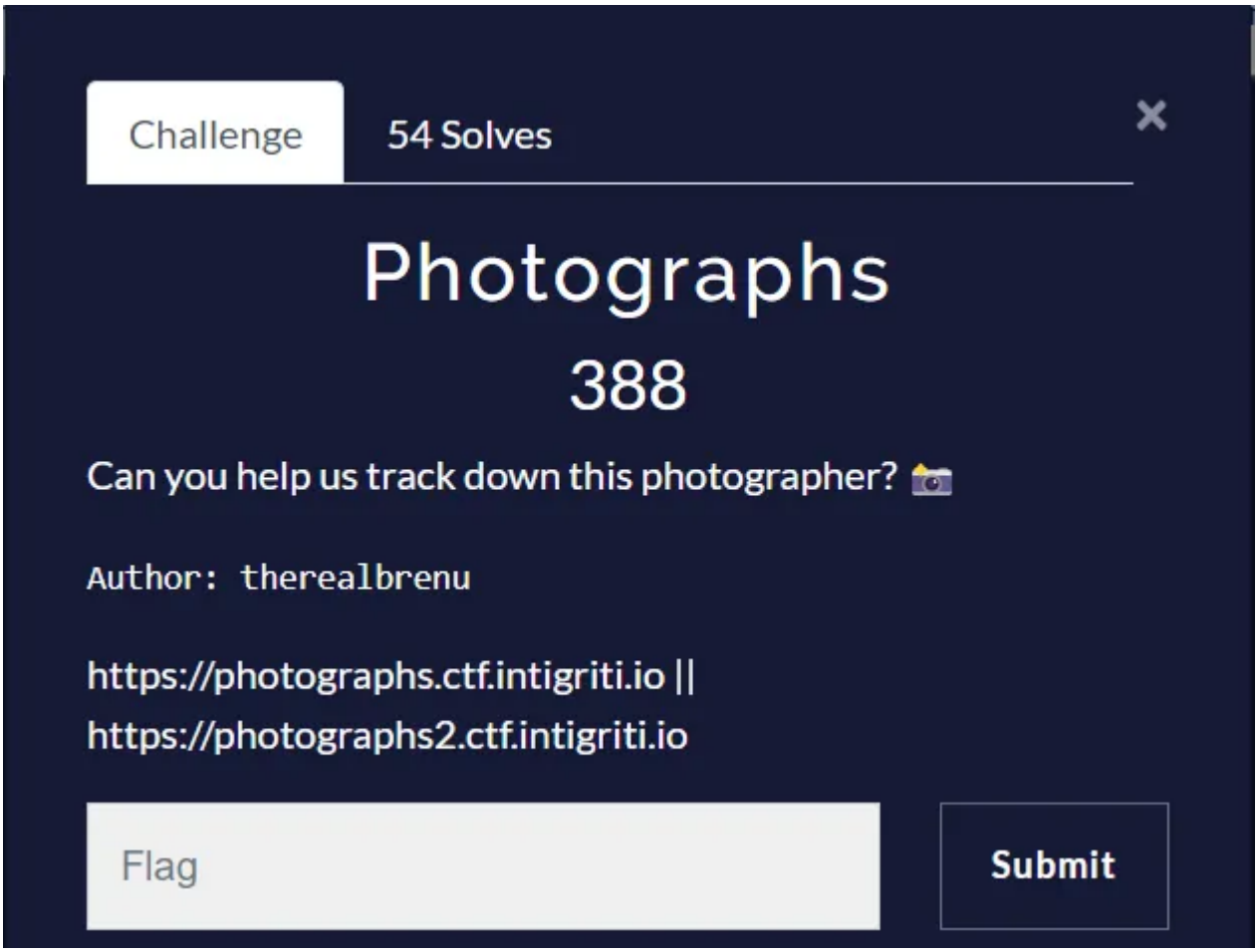
Intigriti CTF write up for OSINT , Cryptography challenges

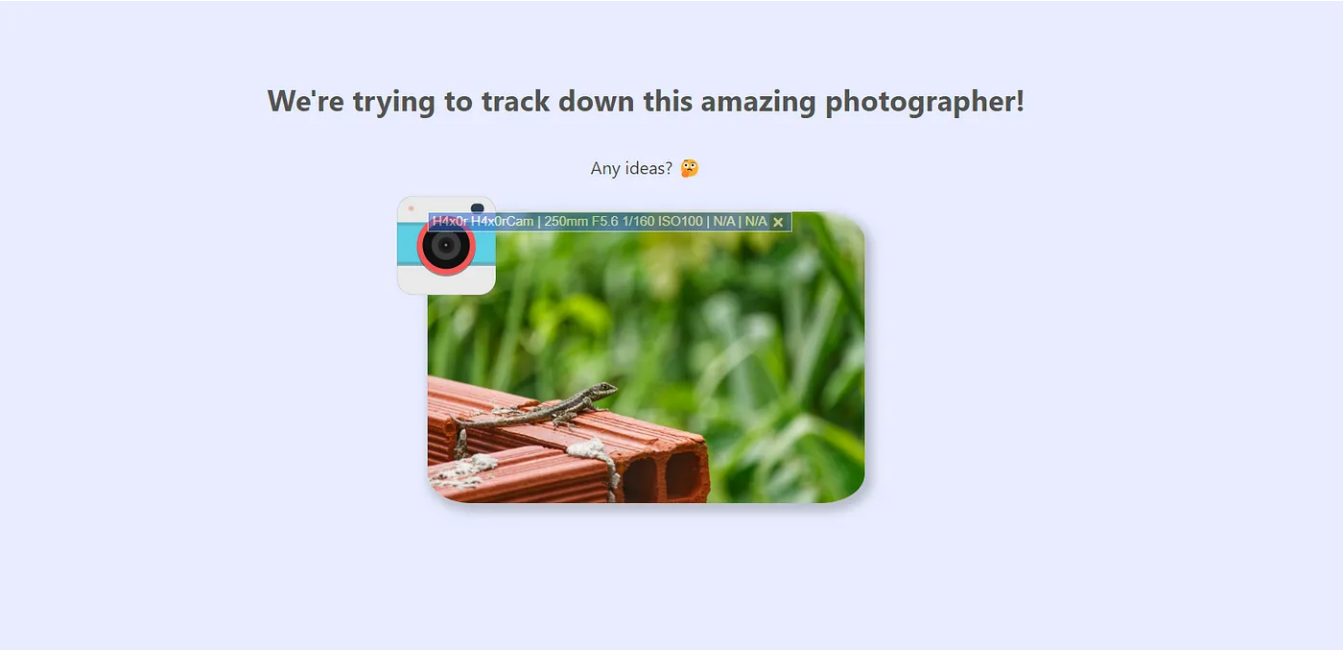
dnelsaka · Follow
5 min read · 1 day ago

Hello It's me youssef a Web/OSINT CTF player and currently learning cryptography

##Challenge 1 : (OSINT) DIfficulty : Medium

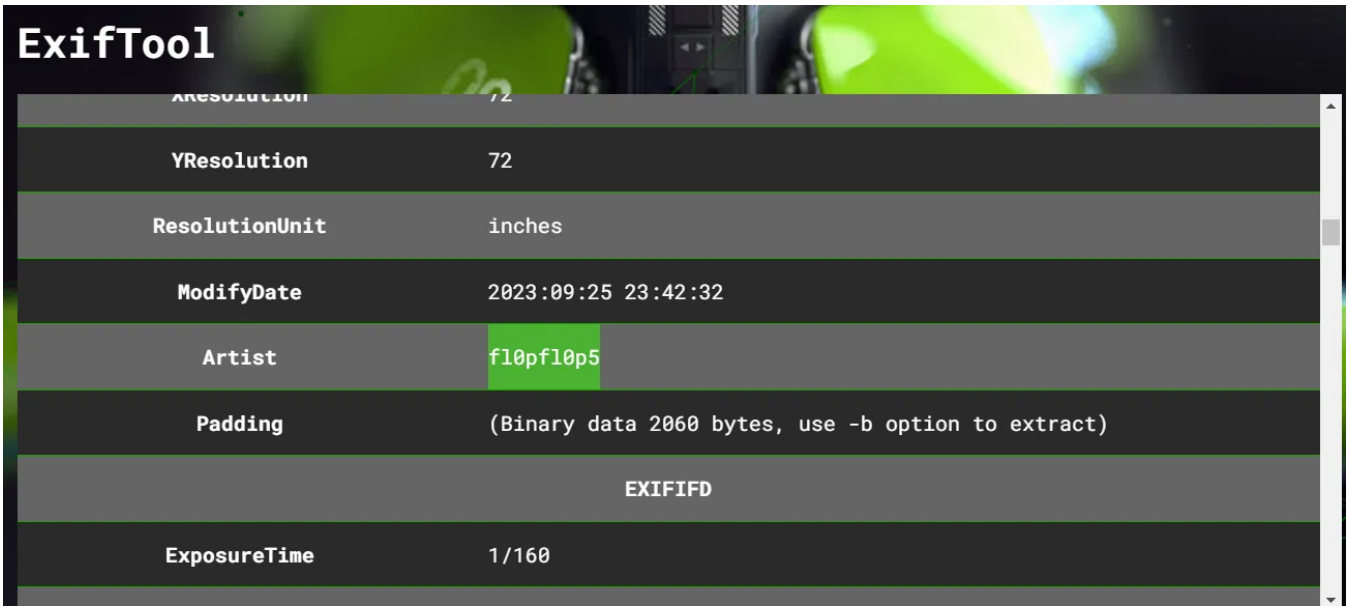


After opening the challenge photo which is a lizard I tried as everyone would do in the first thing to lookup at this image using **Google Index Research** but we found nothing so that it's not about image research it's maybe could be a **METADATA**

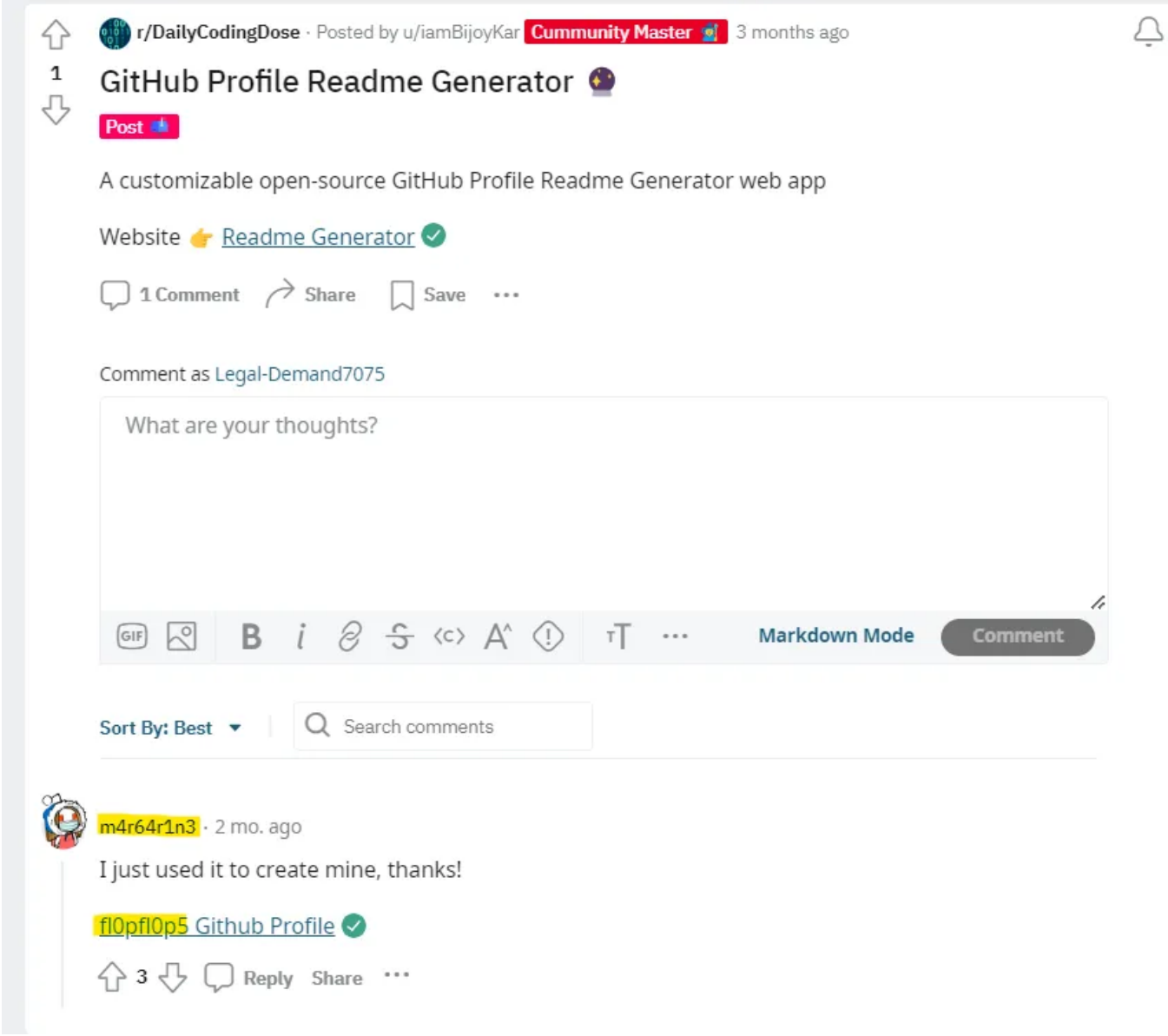


so after downloading the image and opened any tool that may extract photo details I'm always using this website aperisolve

after uploading here we can see the artist name is : **fl0pfl0p5**

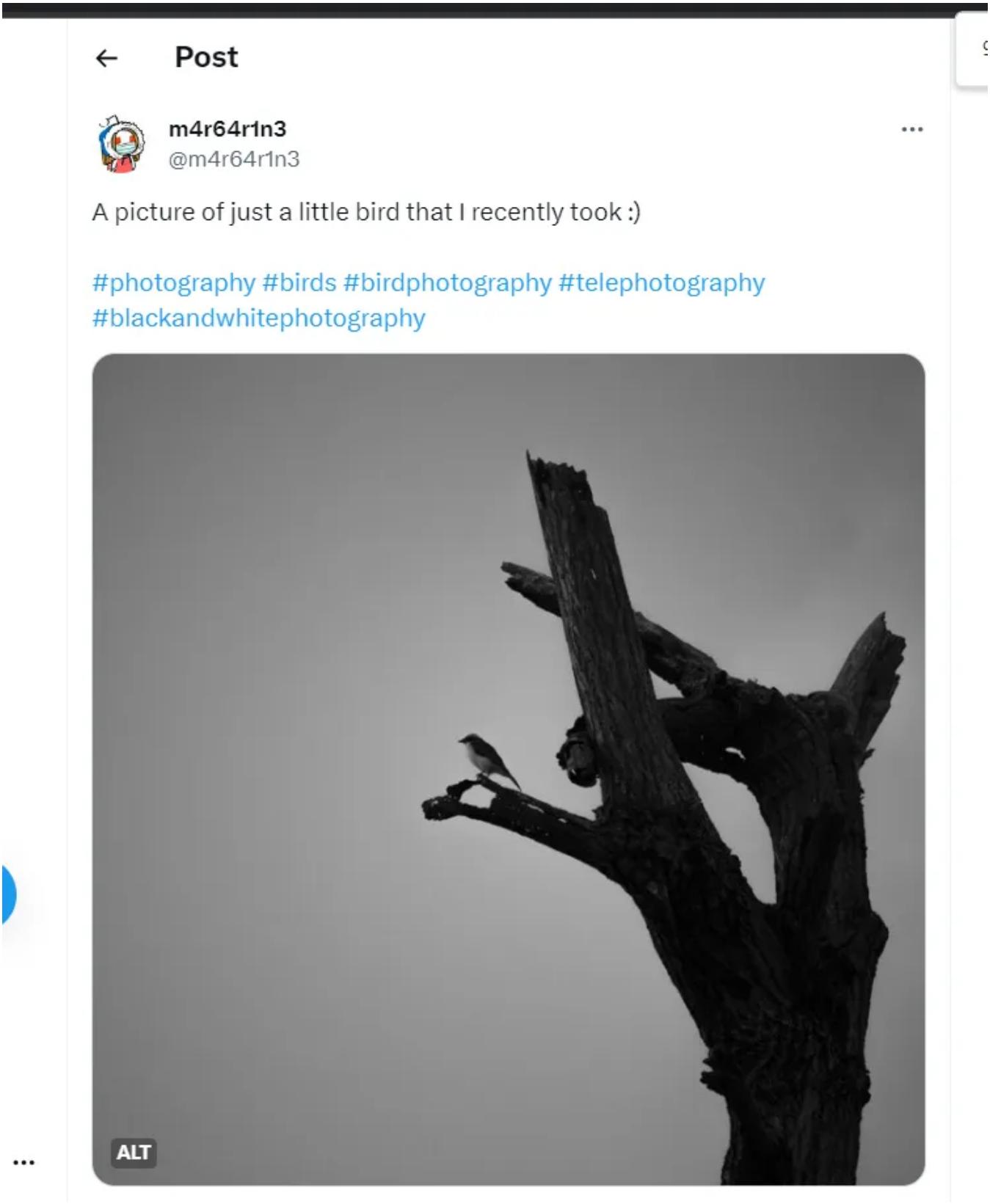


so i thought that is the end of the challenge but it's not they are asking for an actual flag so we need to lookup at this username we didn't find much social media accounts just (reddit and an empty medium account) but after investigating and watching his profile we found that we have another account name !



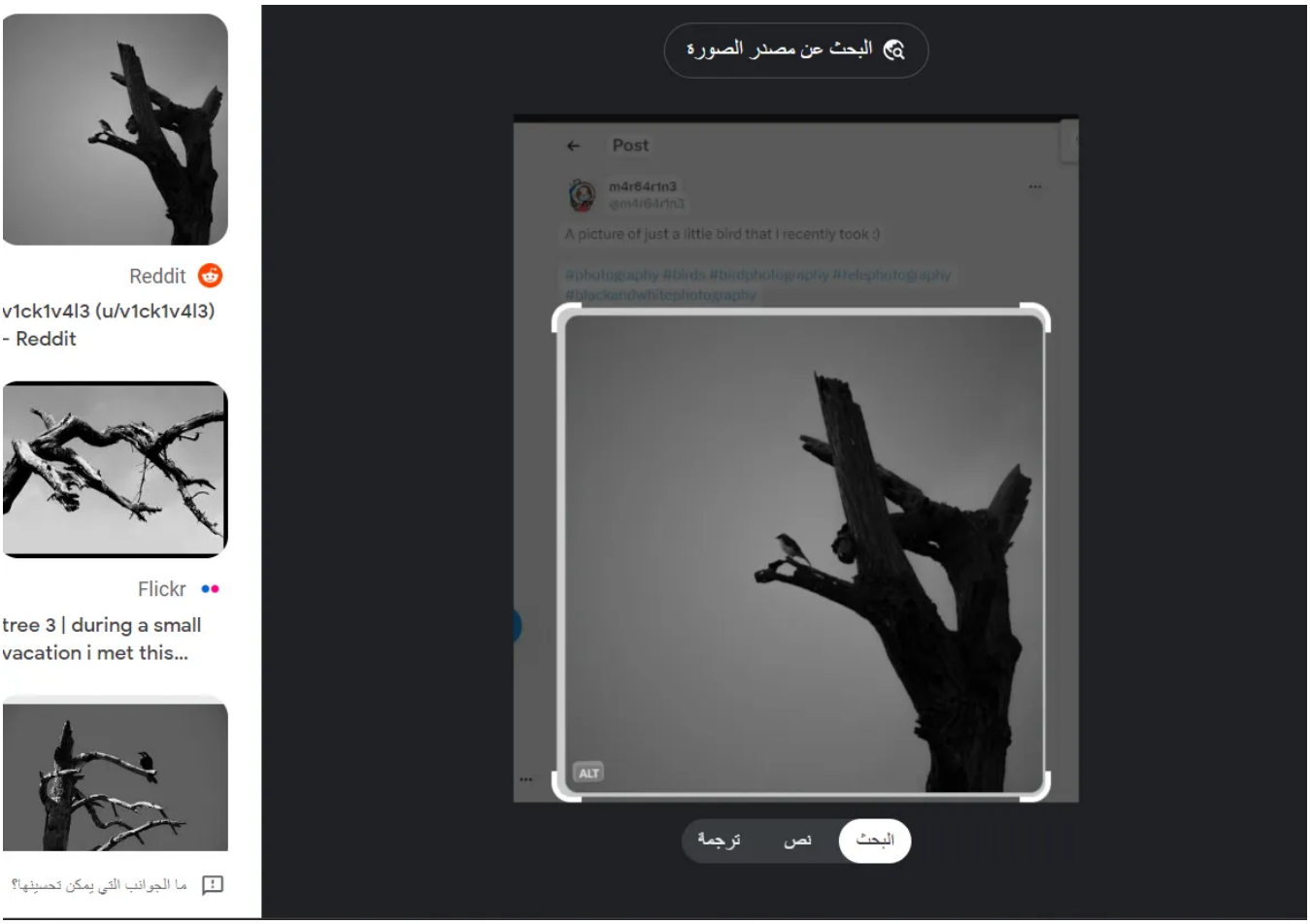
then the artist have another name which is **m4r64r1n3** so after looking up on this name we found a Twitter account using googling

so after opening his Twitter account at the first sight you'll notice nothing same as I but I remembered that this challenge is about a photographer and he have a post said that *"A picture of just a little bird that I recently took :)"* then i started to suspect that this is the challenge completition



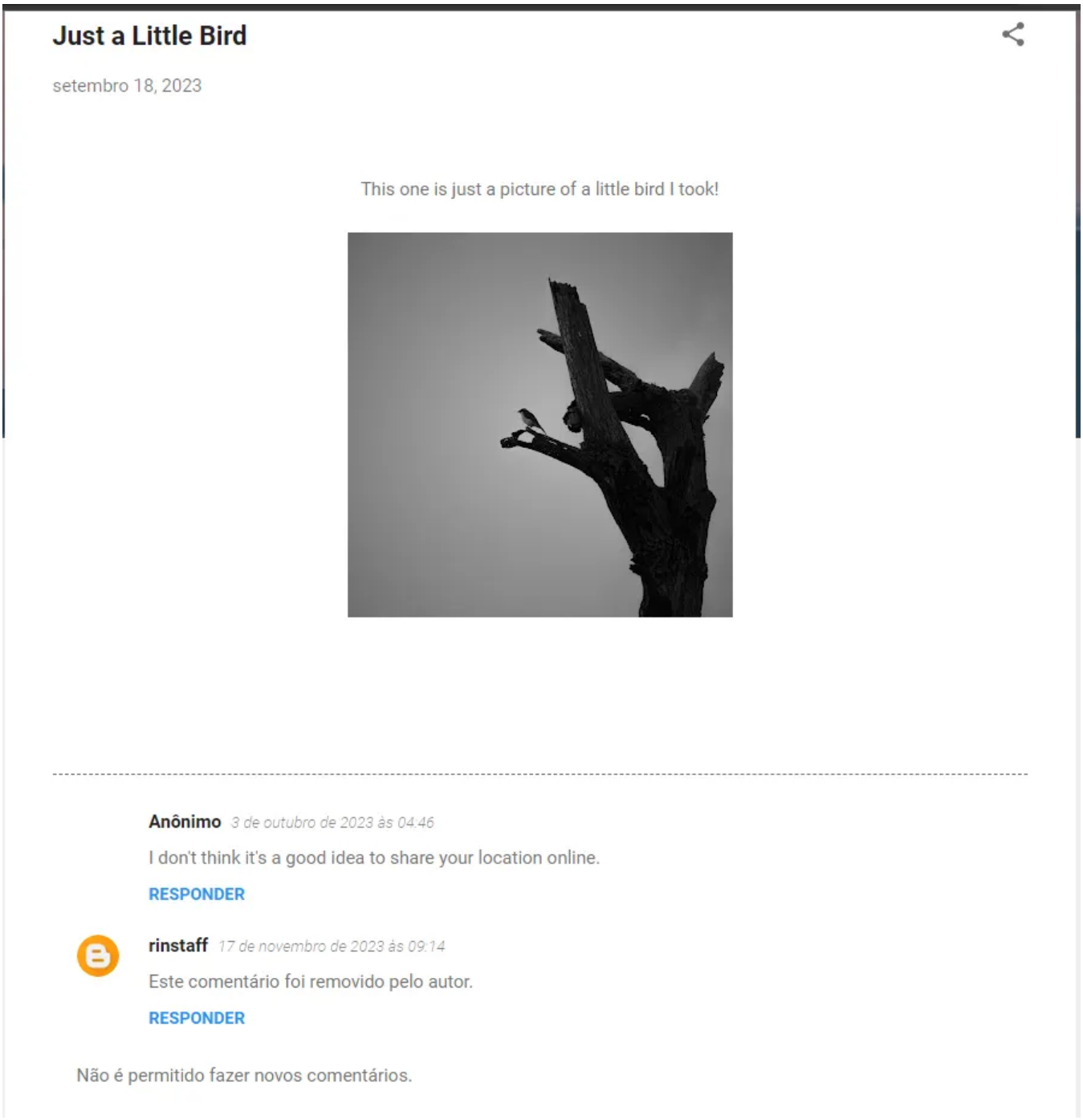
and yeah nothing actually surprising I took the same photo and tried the same process again

1. Image Reverse Using google hell no we got another username called : **v1ck1v4l3**



after looking at his reddit account we found literally nothing so here I started to lose control and started to ignore that challenge but i said there's maybe anything else that related to this image and started again doing the image reverse but we found an Personal blog !!

which is : https://v1ck1pictures.blogspot.com



if we noticed in the comments there's someone telling him that it's not a good idea to share his location ??

but there is no location in the post .... uhhh wayback machine Archive

after looking up on this website we found 1 result in 2 October 2023

and we opened it then ..... finally we got the flag

Just a Little Bird

setembro 18, 2023

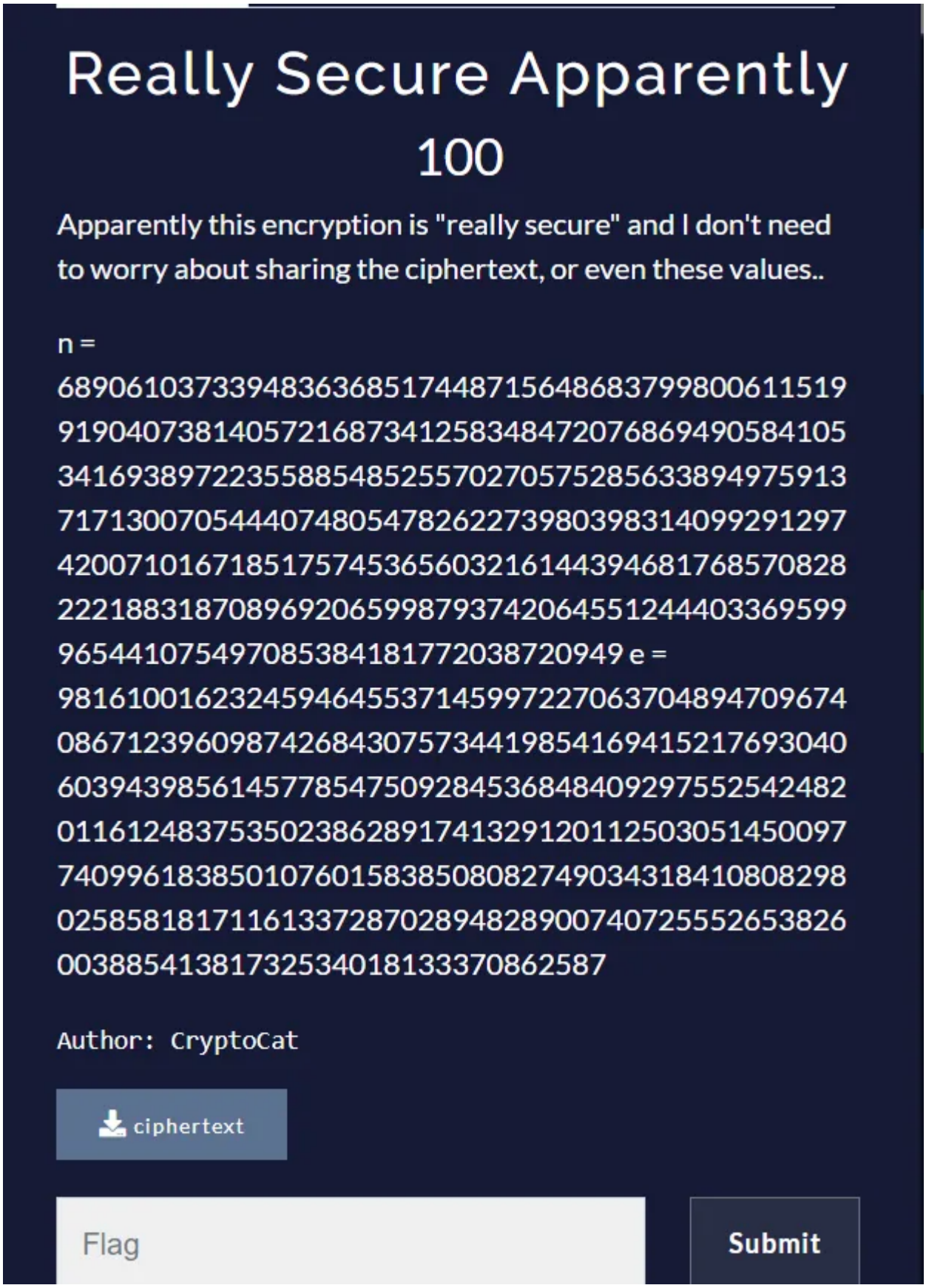
This one is just a picture of a little bird I took when I was in INTIGRITI{D3F1N173LY_N07_60TH4M_C17Y}

##INTIGRITI{D3F1N173LY_N07_60TH4M_C17Y}

==========

Challenge 2 : Cryptography (Really Secure Apparently) Difficulty : Easy

Clearly It’s an Basic RSA but we need to get the d Value First



I solved many RSA Challenges in Cryptohack so I remember that i saw this idea before and this depends on an attack called Wiener Attack by using this tool we can get the D value easy

GitHub - zweisamkeit/RSHack: RSHack - Tool for RSA CTF's challenges

RSHack - Tool for RSA CTF's challenges. Contribute to zweisamkeit/RSHack development by creating an account on...

github.com

```
./RS./rshack.py -n $N Value -e $E Value
```

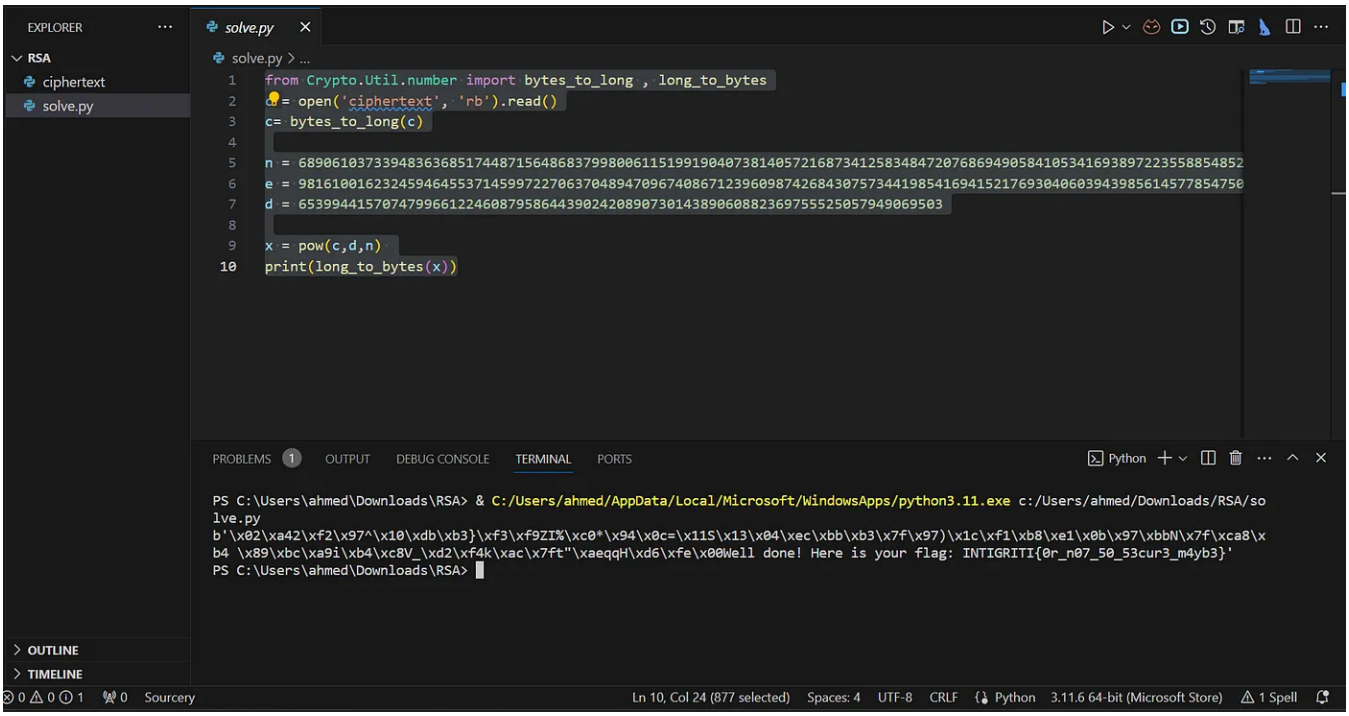
Then after getting the D value which is the private key

we need to get the C value and in the challenge there's a given file called plaintext but as it shown it's an Bytes and we need to convert it into Int


```
from Crypto.Util.number import bytes_to_long , long_to_bytes
c = open('ciphertext', 'rb').read()
c= bytes_to_long(c)

n = 689061037339483636851744871564868379980061151991904073814057216873412583484
e = 981610016232459464553714599722706370489470967408671239609874268430757344198
d = 653994415707479966122460879586443902420890730143890608823697555250579490695

x = pow(c,d,n)
print(long_to_bytes(x))
#FLag: INTIGRITI{0r_n07_50_53cur3_m4yb3}
```



##INTIGRITI{0r_n07_50_53cur3_m4yb3}

==========

Challenge 3 : Keyless (Cryptography) Difficulty : Easy

after downloading the challenge file and unzipped it we got that python file

```
def encrypt(message):
    encrypted_message = ""
    for char in message:
        a = (ord(char) * 2) + 10
        b = (a ^ 42) + 5
        c = (b * 3) - 7
        encrypted_char = c ^ 23
        encrypted_message += chr(encrypted_char)
    return encrypted_message

flag = "INTIGRITI{REDACTED}"
encrypted_flag = encrypt(flag)

with open("flag.txt.enc", "w") as file:
    file.write(encrypted_flag)
```

> *so here the python encrypts the flag and outputting it in the flag.txt.enc*

we can decrypt this file by reversing the process

```
def encrypt(message):
    encrypted_message = ""
    for char in message:
        a = (ord(char) * 2) + 10
        b = (a ^ 42) + 5
        c = (b * 3) - 7
        encrypted_char = c ^ 23
        encrypted_message += chr(encrypted_char)
    return encrypted_message

from string import printable

key = {}
for c in printable:
    key[encrypt(c)] = c

chiphrt = open('flag.txt.enc', 'rb').read().decode()
flag=""
for c in chiphrt:
    flag += key[c]

print(flag) # INTIGRITI{m4yb3_4_k3y_w0uld_b3_b3773r_4f73r_4ll}
```

so here we imported the printable library and then we created the dictionary “Key” and It associates each encrypted character with its corresponding original character from the printable ASCII characters. It uses the `encrypt` function defined earlier to generate the keys.

```
chiphrt = open('flag.txt.enc', 'rb').read().decode()
flag = ""
for c in chiphrt:
    flag += key[c]

print(flag) #INTIGRITI{m4yb3_4_k3y_w0uld_b3_b3773r_4f73r_4ll}
```

Here, the encrypted message is read from the file ‘flag.txt.enc’, and each character is looked up in the `key` dictionary to find its corresponding original character. The resulting characters are concatenated to form the decrypted `flag`, which is then printed.

##INTIGRITI{m4yb3_4_k3y_w0uld_b3_b3773r_4f73r_4ll}

kind regards, Hope you enjoyed this write up <’3

Ctf Writeup | Ctf | Ctf Walkthrough | Intigriti | Cryptography

Follow

Written by dnelsaka

228 Followers

CNSS | eJPT | 18 yrs | engineering student | bughunter