---------- **Contest Name : Root CTF 2021** ----------
---------- **Organizer :Bytersec_Squad** ----------
---------- **Flag Format:Cyberbangla{}** ----------

Challenge: Trivia 4

Category :General Info

a. What is the file **name of john for cracking zip file passwords** ?

b. What is the **format type of the given below hash for John the ripper** ?

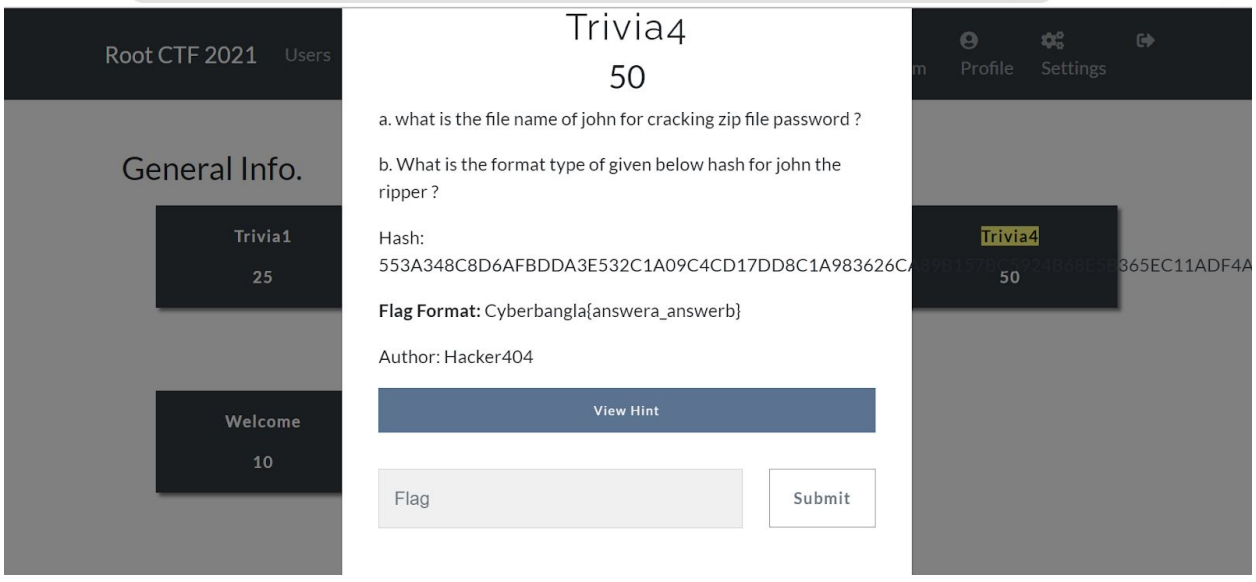
Hash:553A348C8D6AFBDDA3E532C1A09C4CD17DD8C1A983626CA89B157BC5924B68E5B365EC11ADF4A71C331BDC6C3608C917531E434882EC083BC3593753E46E16FE

Flag Format:Cyberbangla{answera_answerb}

Points :50

Author:Hacker404

Flag:Cyberbangla{zip2john_whirlpool}



Step 1:

Use locate command with target strings :

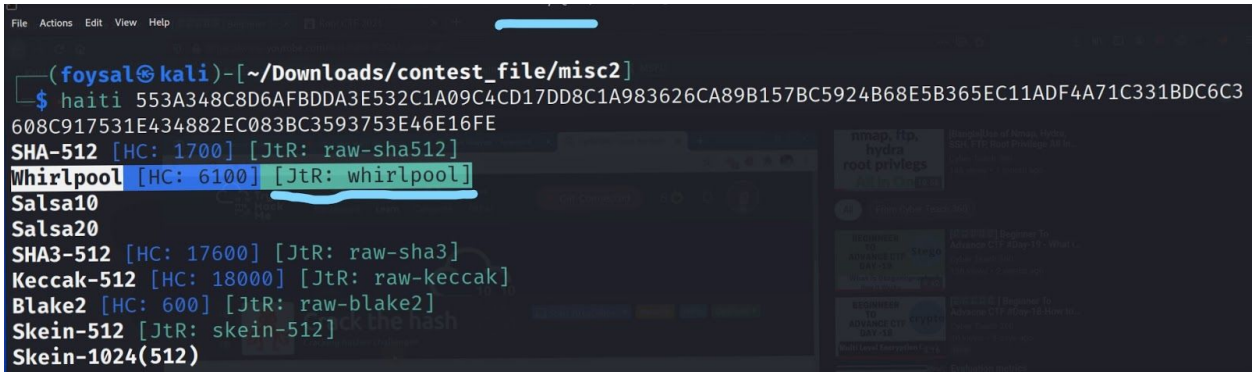
locate john | grep -i zip

Step 2:

Use any hash identifier for detect hash type .Here , I used haiti tools

Command :

haiti target hash



So , According to Flag Format the Flag is :

Cyberbangla{zip2john_whirlpool}

----------**********----------
----------**********----------
----------**********----------

---------- **Contest Name : Root CTF 2021** ----------
---------- **Organizer :Bytersec_Squad** ----------
---------- **Flag Format:Cyberbangla{}** ----------

Challenge: Error 001

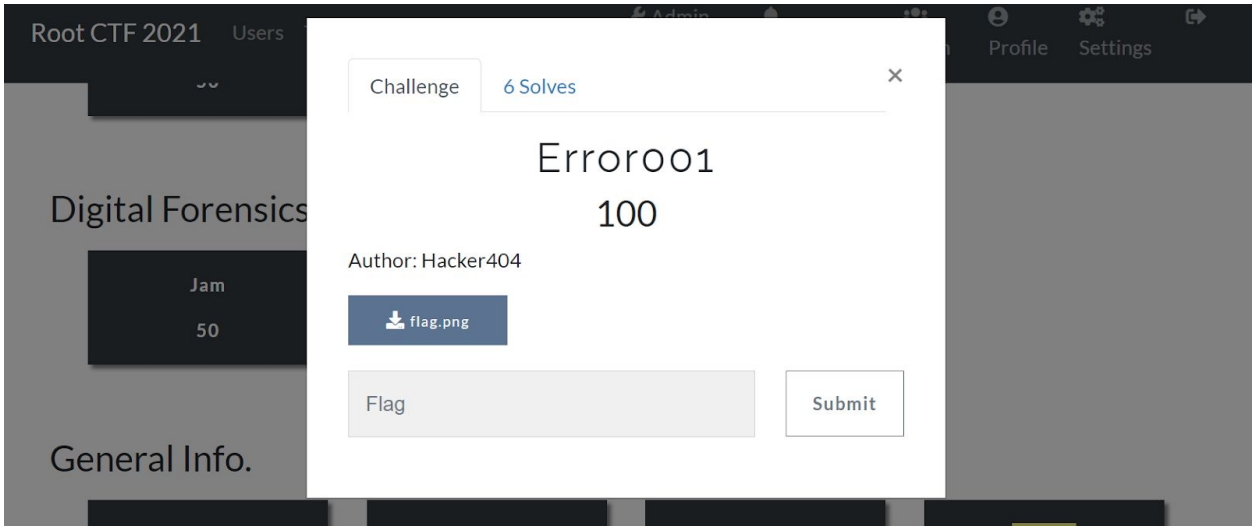
Category :Digital Forensics

Points :100

File:

Link:https://drive.google.com/drive/folders/1MsjnLXgL6chG8ZkYu94RXhqipf7rV0Ah?usp=sharing

Auth :Hacker404



1st Process :

Step1 : Download Target File

Step 2 :Open Target file , but what happens??? Ohhh no , the file doesn't open. Ok ,no problem .

Step 3: We know that , If our target file doesn't open, that means the format of the file is wrong . Now , What can we do ?? well , we open target file **Via HXD or any Hex Editor**

Step 4: Open , target file via HxD editor & analyze **file signature bytes** of target file at the beginning .

Step 5 : Then , compare the magic number or file signature values of the target file with the international file signature list . Ohh no , we got it .The file format of target file must be txt .

Step 6 : Ok , rename the target file with .txt format extensions and open it .

Step 7 : After opening our target file we get a flag but it is cipher . Now , what can we do ??

Step 8 :Well , analyze the Cipher and we understand it is a Substitution cipher . So , Use online tools for decrypting it .

Step 9:Finally , we got the flag .

Flag :Cyberbangla{Allah is Only One}

2nd Process :

Step 1:Use **file command** for checking the real format of the file .

Command:

file flag.png

Step 2: Wow, they contain **ascii value** .Ok that's good.

Step 3: As , file contains **ascii values** now we can easily read the content of the target file using the strings command .

Command :

strings flag.png

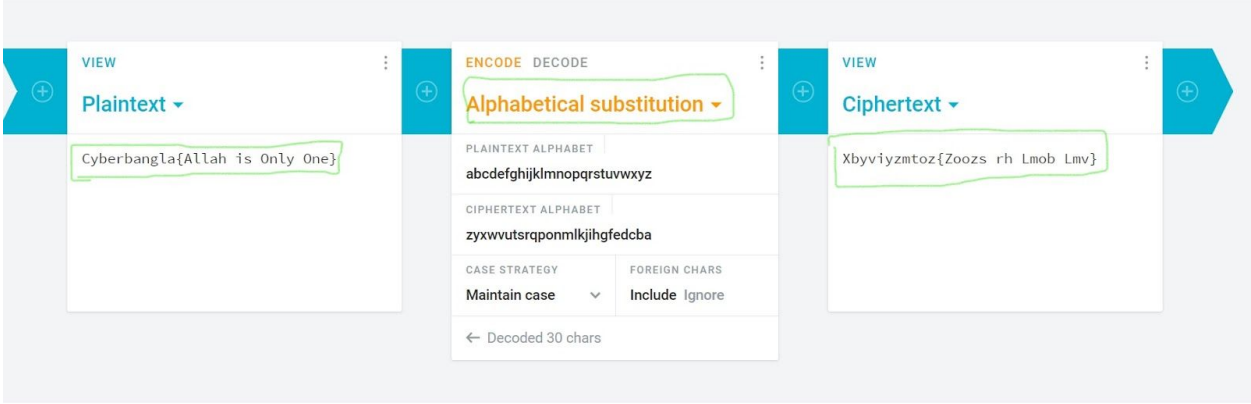
Step 4: We got ,

Xbyviyzmtoz{Zoos rh Lmob Lmv}

Step 5: **Xbyviyzmtoz{Zoozs rh Lmob Lmv} is a cipher** .Well , analyze the Cipher and we understand it is **a Substitution cipher** . So , Use online tools for decrypting it .

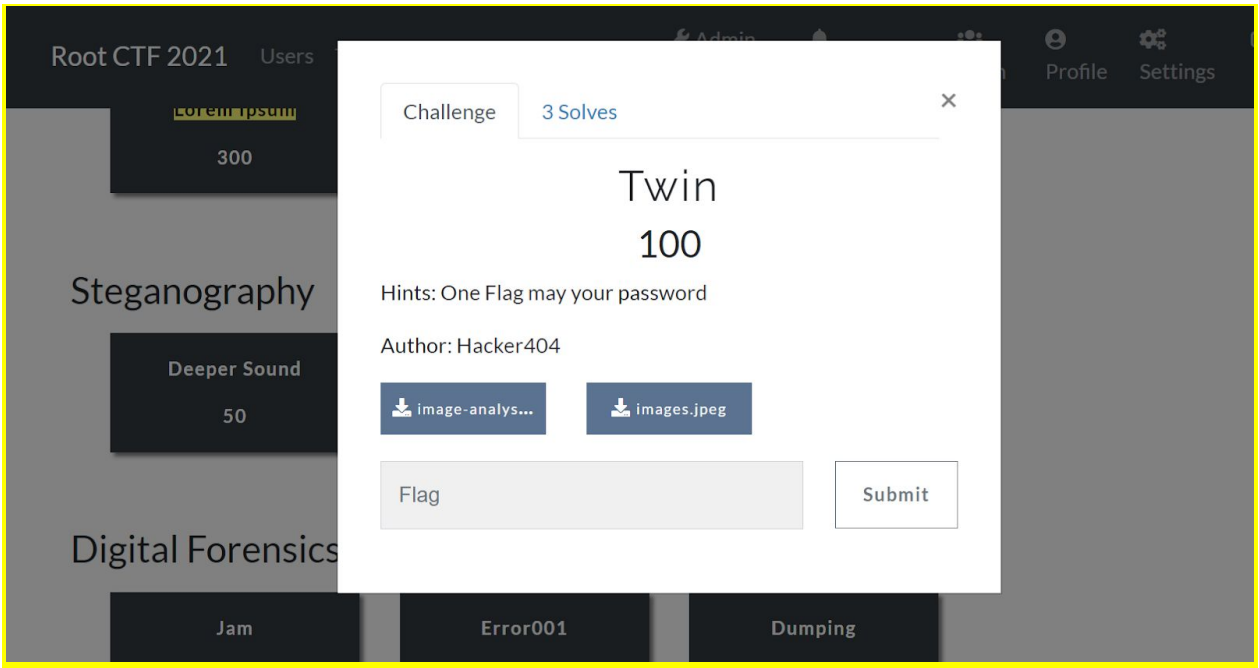
Step :Finally , we got the flag .

Cryptii



Flag :Cyberbangla{Allah is Only One}

---------- **Contest Name : Root CTF 2021** ----------
---------- **Organizer :Bytersec_Squad** ----------
---------- **Flag Format:Cyberbangla{}** ----------



Challenge: Twin

Category :Steganography

Hints: One Flag may your password

Author: Hacker404

POINTS:100

File Link :
https://drive.google.com/drive/folders/117lUrRc-3xlrqgxHPxeQCv4DWdwV64L8?usp=sharing

Step 1:Download target files .See file type using file command

Step 2:Here , We have two files . One is **.png format ,another is .jpeg** formatted files .

Step 3: Open , .png format file via zsteg .
Command :
zsteg image-analysis.png

Step 4: After analyze previous command output , we got **"ShadowCTF{1_t0ld_y0u}"** which is the password for extract images.jpeg file according to challenge hints .(**Hints: One Flag may your password)**

Step 5: Ok , great .We already got our **password**.Now we can easily extract our target file via **steghide** . Command :

steghide extract -sf images.jpeg

Step 6:Enter "ShadowCTF{1_t0ld_y0u}" as a **passphrase** .

Step 7: Finally , we extracted our target file. Now, read content of flag.txt file via cat command

The Flag is :
Cyberbangla{Read_Quran_EveryDay_And_Try_To_Realize_it}

---------- **Contest Name : Root CTF 2021** ----------
---------- **Organizer :Bytersec_Squad** ----------
---------- **Flag Format:Cyberbangla{}** ----------

Challenge: Power of Social Media
Category :Steganography

Hints : Social Media can help to get password

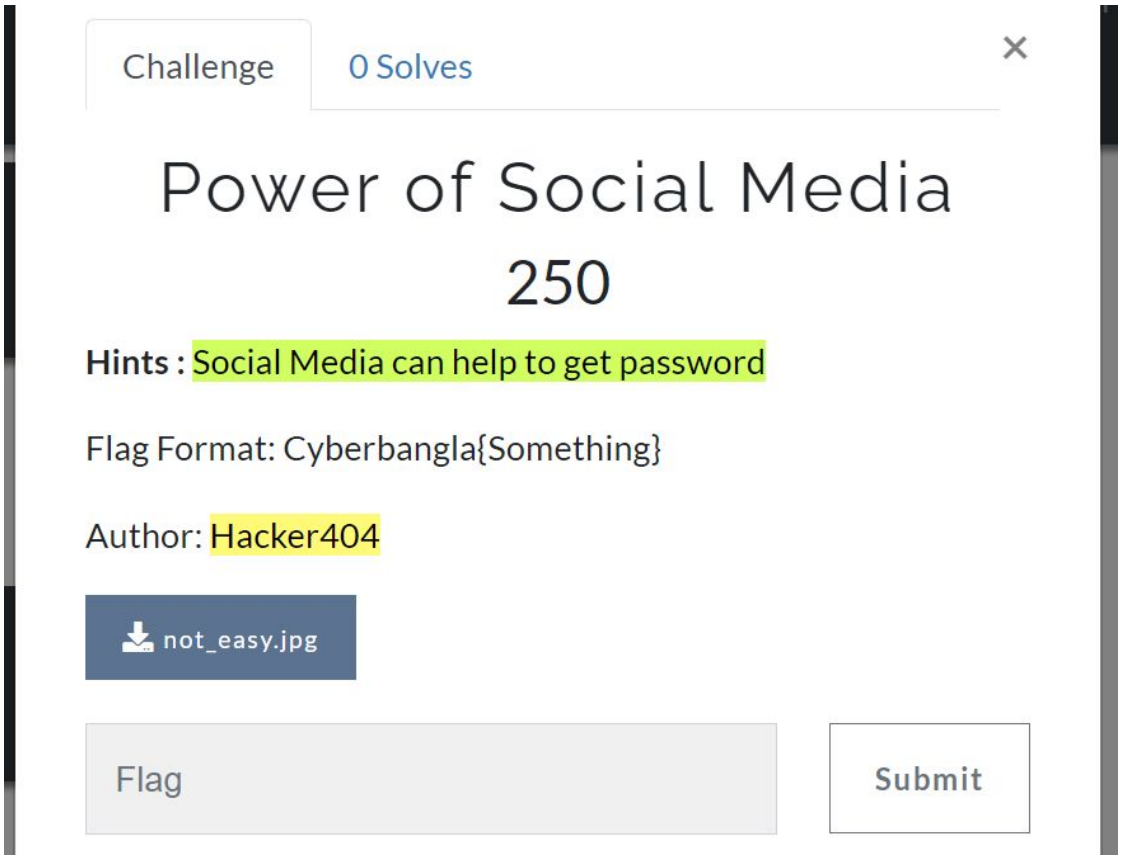
Flag Format: Cyberbangla{Something}

Author: Hacker404

FileLink:

https://drive.google.com/drive/folders/1-Wfaur06ggmteucM_CJvWpPMSqn-tjAQ?usp=sharing

Step 1:Download target file and use file command to know the real format of target file .



Step 2:Target file is **jpg format file .Well, we need a password for extracting our target file .Now , Question is , where is the password or how can we get the password ?? ok ,no problem ,follow given below steps**.

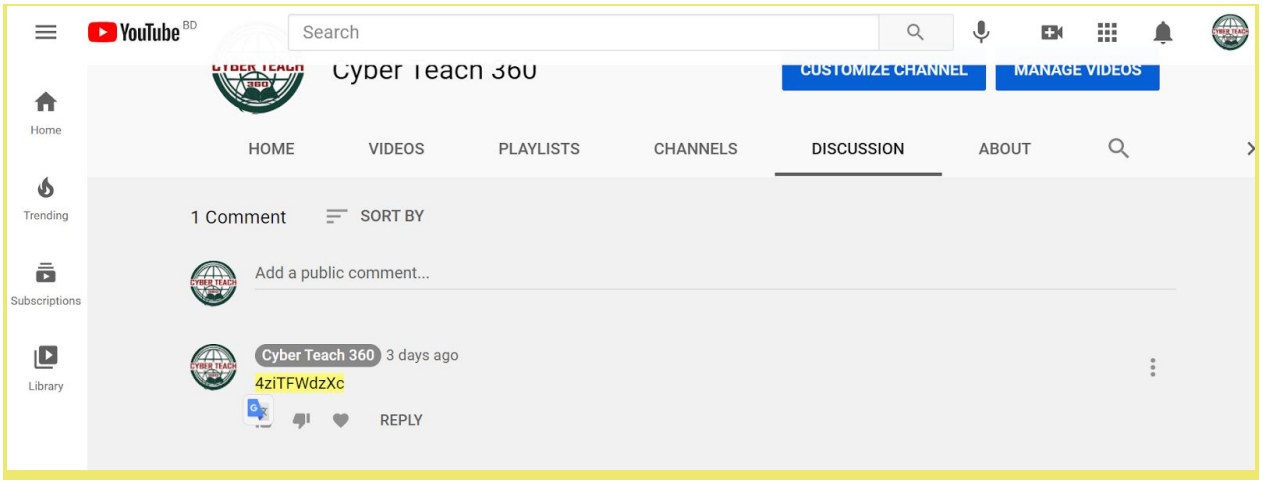
Step 3:According to hints , we will **get a password from the author's social account** . So , we must osint author social media like youtube , facebook, twitter ,github etc.

Step 4:Well , after analyzing author user name we got author social media name:

Twitter :cyberteach360
Youtube:cyberteach360

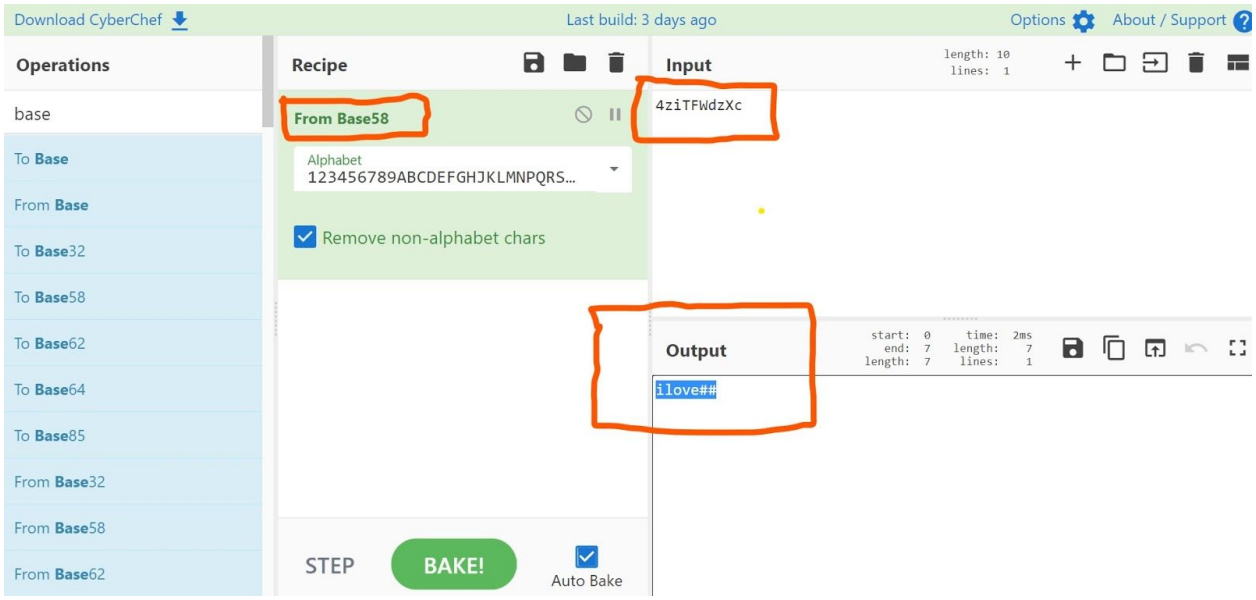
Step 5:Go to author social media and osint carefully .

Step 6: Well , we **got cipher from author youtube channel discussion part like 4ziTFWdzXc**



Step 7:As , 4ziTFWdzXc is cipher we must decrypt it .Here, I was use Cyber Chef online tools and I was decrypt it from **base58 to Plain text (ilove##)**

Step 8:Plain text of 4ziTFWdzXc is ilove## . Ok , now we can extract our target file using steghide tools .



Step 9: I extracted our target file using **steghide extract -sf not_easy.jpg command**

Step 10: **Well , we got flag.txt and after read flag.txt file we saw it was cipher . Ohh!!! no what can we do???? Well , no problem .**

```
┌──(foysal㉿kali)-[~/Downloads/contest_file/steg_1]
└─$ steghide extract -sf not_easy.jpg
Enter passphrase:
wrote extracted data to "flag.txt".

┌──(foysal㉿kali)-[~/Downloads/contest_file/steg_1]
└─$ ls
flag.txt  not_easy.jpg

┌──(foysal㉿kali)-[~/Downloads/contest_file/steg_1]
└─$ cat flag.txt
----------]<-<----<----------<----------»>>+[<<<+++,<----------,++++++++++++++++++++
+,---,----------,++++++++++++++++,+,----------,+++++++,-------,++++++++++,----------
----------,>----------,<++,+++++,++++++++++++,-------,+,»--,<<+++++,----------,>>,<<+++++
++++++++++++,---,----------,-,>>,<<++++,--,+++,++++++++,----------,>----------,<++
+++,++++,-------,>-------,>,<<++,>++++++,<--,>-------,<----------,>++++++,-------,++,<----------,
```

Step 11: After Analyzed , **the cipher , we realized it is reverse fuck cipher as the cipher start with minus ---------- and third bracket "] " open Reversly or Close . Note: Brain fuck or Binary fuck start with Plus +++++ and "[" third bracket open mode**

Step 12 : Now , we can easily decode it using online tools like **dcode.fr** .Here , I was use dcode.fr

Step 13: Finally , we got the flag and the flag is :

Cyberbangla{Python is best programing language}

---------- **Contest Name : Root CTF 2021** ----------
---------- **Organizer :Bytersec_Squad** ----------
---------- **Flag Format:Cyberbangla{}** ----------

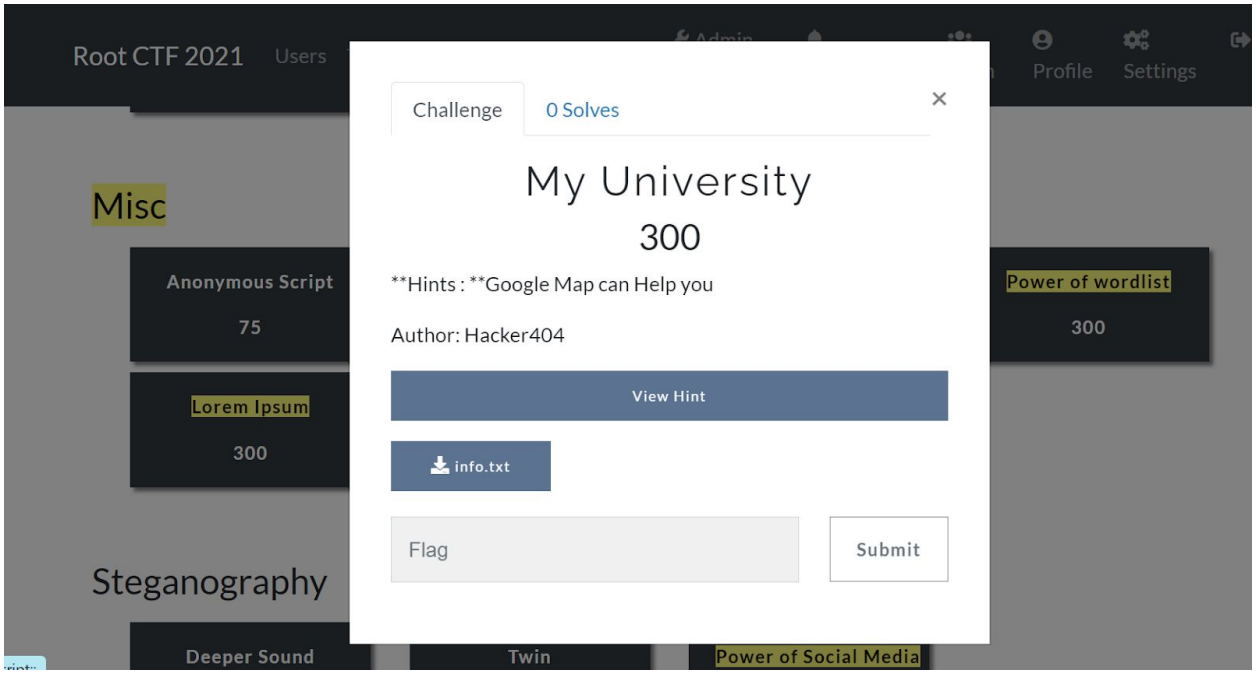
Challenge Name :My University

Category :Misc

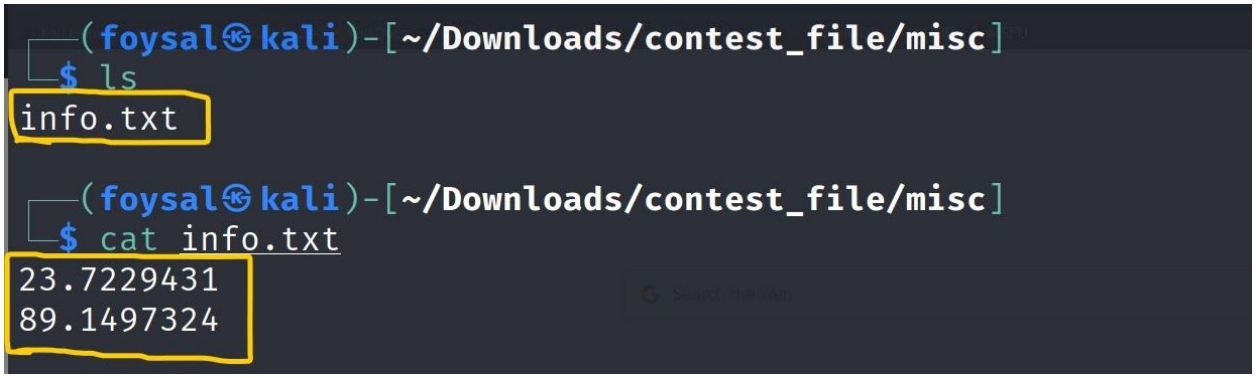
Hints : Google Map can Help you

Points: 300

Auth: Hacker404



Step 1: Download **target file and Read target file using cat command.**

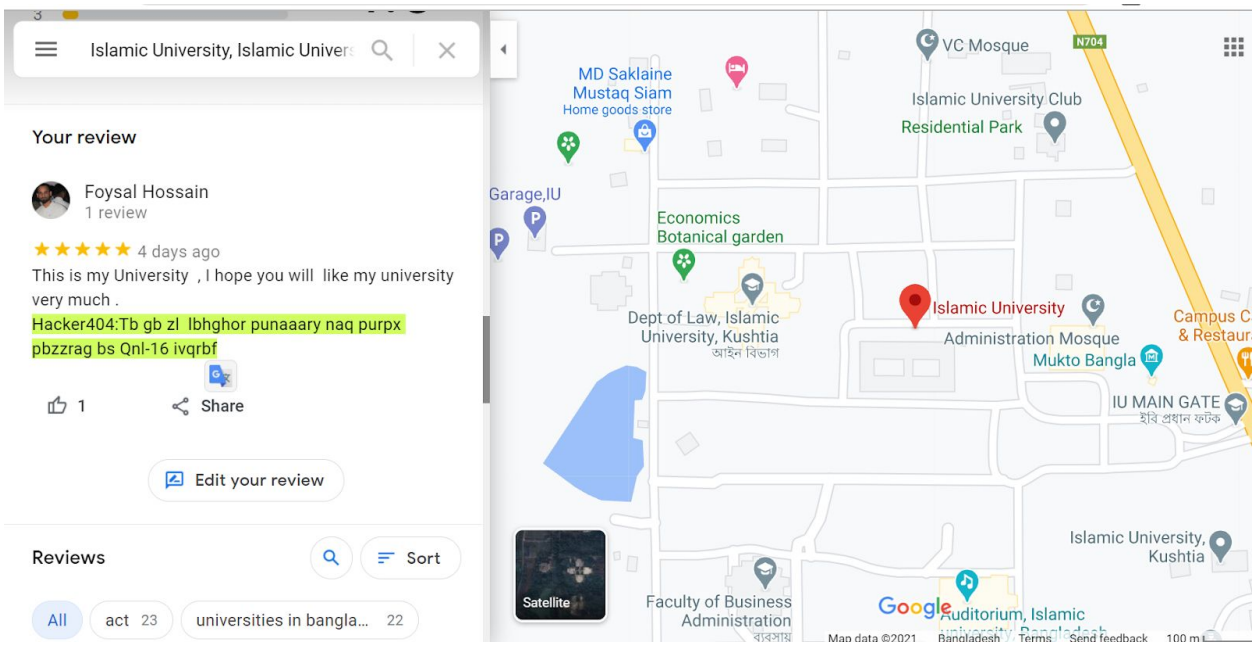


Step 2: We got two values like 23.7229431 , 89.1497324 . I think 23.7229431,89.1497324 are **longitude** , **latitude and they expose the location of Islamic University ,Kushtia .**

Step 3: **According to Challenge name and Challenge hint , we are sure that 23.7229431,89.1497324 expose location and the location will be the university of challenge author . So, our guess is right** .

Step 4 : Go to Author University google map and analyze properly .

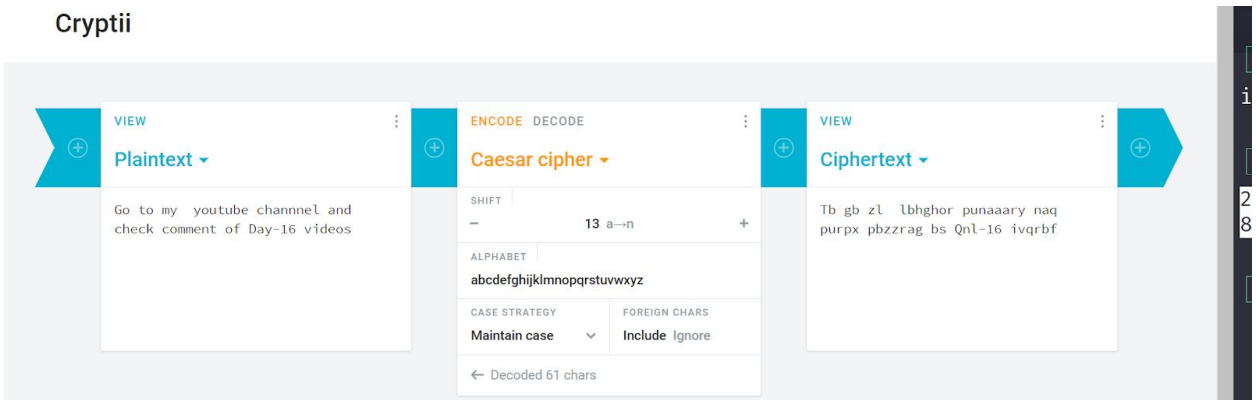
Step 5: After , **analyze author university google map we got author command like that :**



Step 6: Copy the command of Hacker404 and try to decode it as it is cipher

Step 7: After , decode the author cipher we got :

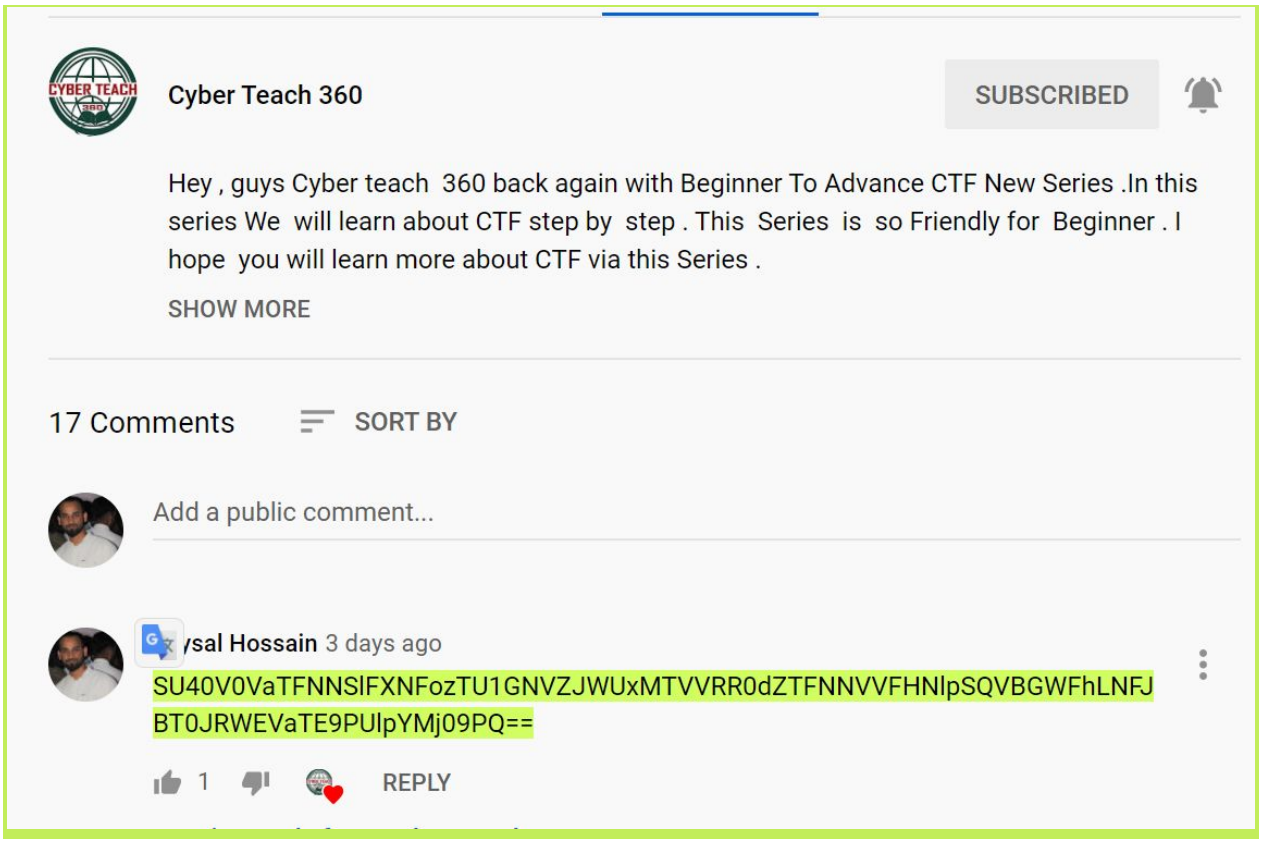
Go to my youtube channel and check comment of Day-16 videos



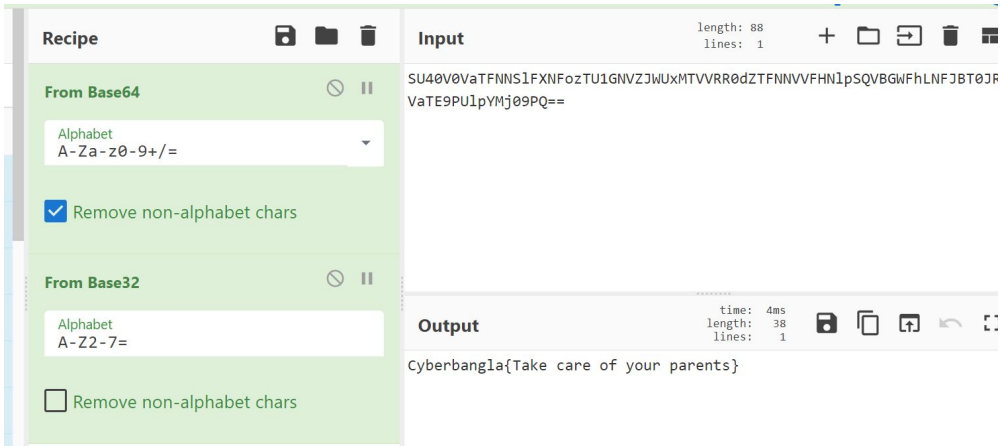
Step 8: **Go to the author youtube channel (cyber teach 360)** and check command of day 16 video .

Step 9: Ohh ….. We don't get flag , What can we do??? Well , no problem .Take your time .

Step 10: Click on sort by and select newest first , then I got author comment like that:
SU40V0VaTFNNSlFXNFozTU1GNVZJWUxMTVVRR0dZTFNNVVFHNlpSQVBGWFhLNFJBT0JRWEVaTE9PUlpYMj09PQ==



Step 11: As , **the comment base64 cipher** , we decode it using cyber chef online tools And the Flag **Cyberbangla{Take care of your parents}**

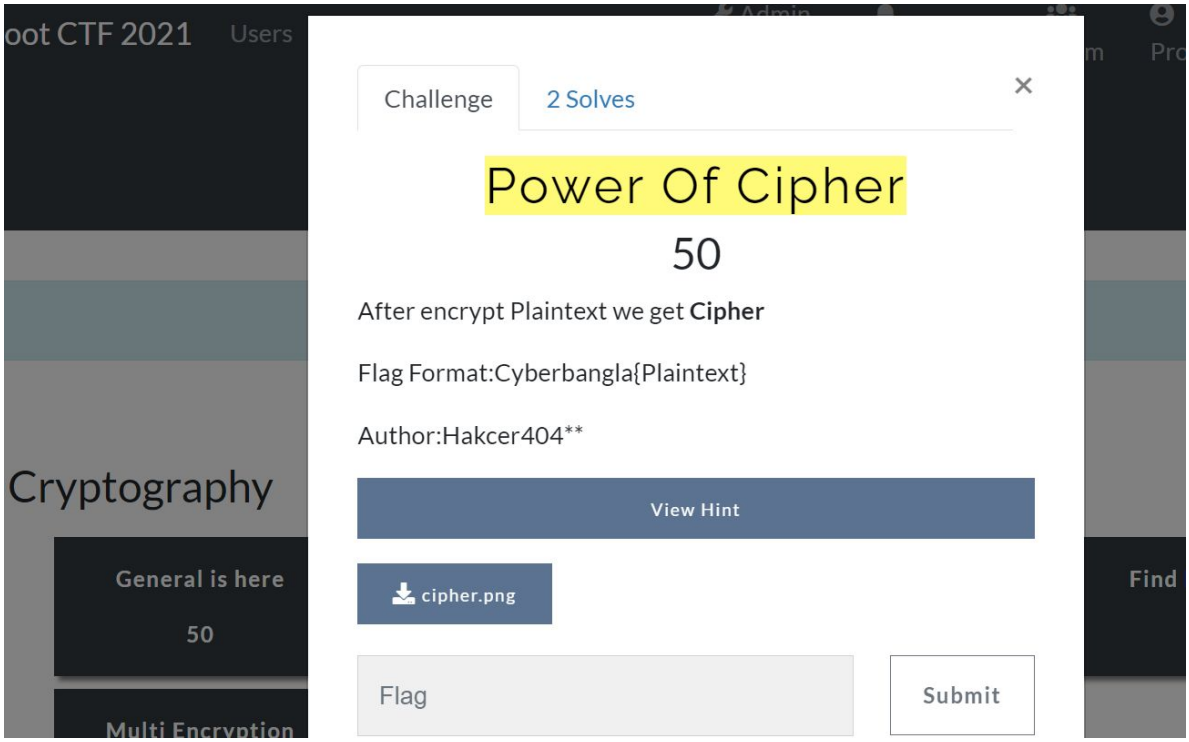


---------- **Contest Name : Root CTF 2021** ----------
---------- **Organizer :Bytersec_Squad** ----------
---------- **Flag Format:Cyberbangla{}** ----------

Challenge Name :Power Of Cipher
Category :Cryptography

Hints : case sensitive

Points: 50
Auth: Hacker404



Step 1: Download Target file and open it .

Step 2: As the challenge category is **cryptograph**y , I think this image expresses cipher .

Step 3: Now , try to find out the type of image cipher and Decode it .

Step 4:Ohh , no . We don't find any cipher type . What can we do ??? well , no problem. **Osint can help you** .

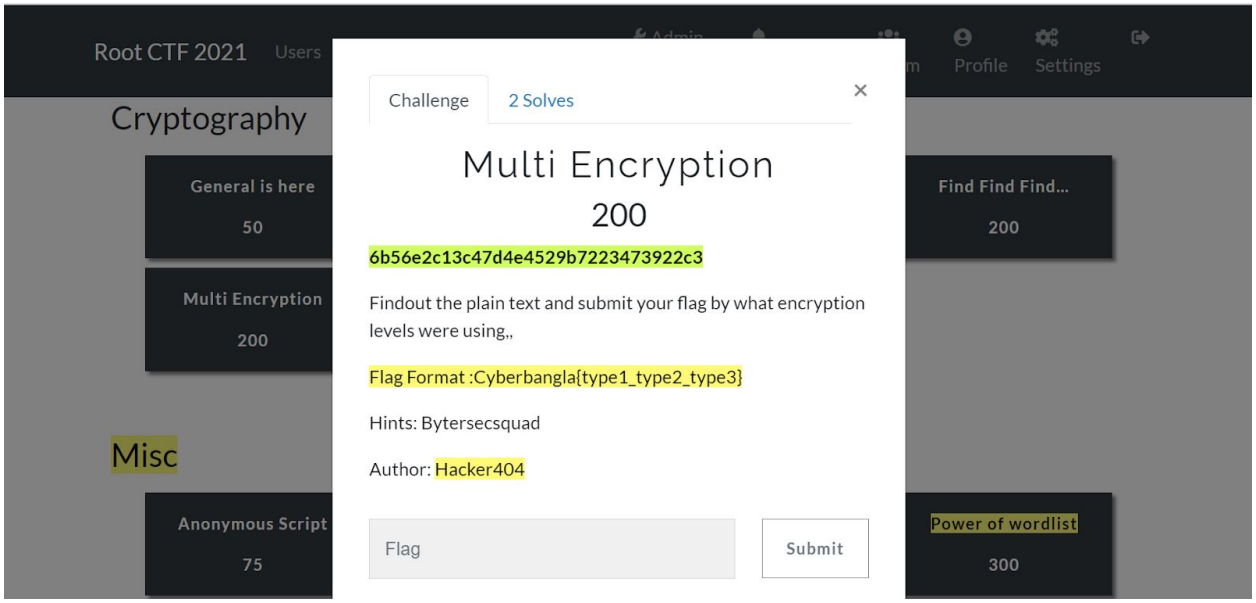
Step 5: Search **google "image search " and upload your target image or reverse image search and upload your target image or use google lense and click on similar image .**

Step 6: After analyzing we got the type of cipher and its **"bacon cipher** " .

Step 7: Use online tools for extracting target cipher :

Step 8: Finally , we got the flag and that is :

Cyberbangla{BCON_CIPHER}



Challenge Name :Multi Encryption

Category : Cryptography

Points: 200

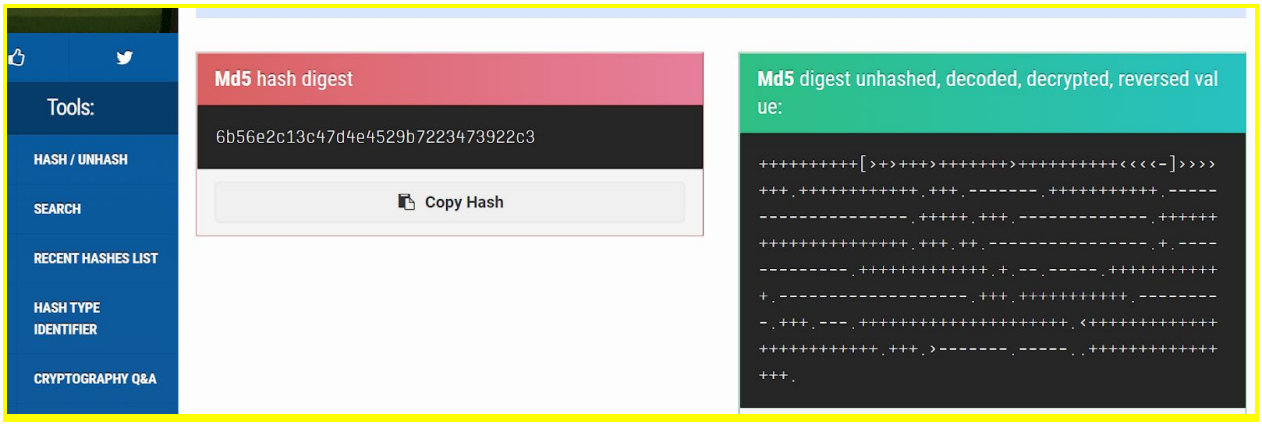
Author: Hacker404

Hints: BytersecSquad

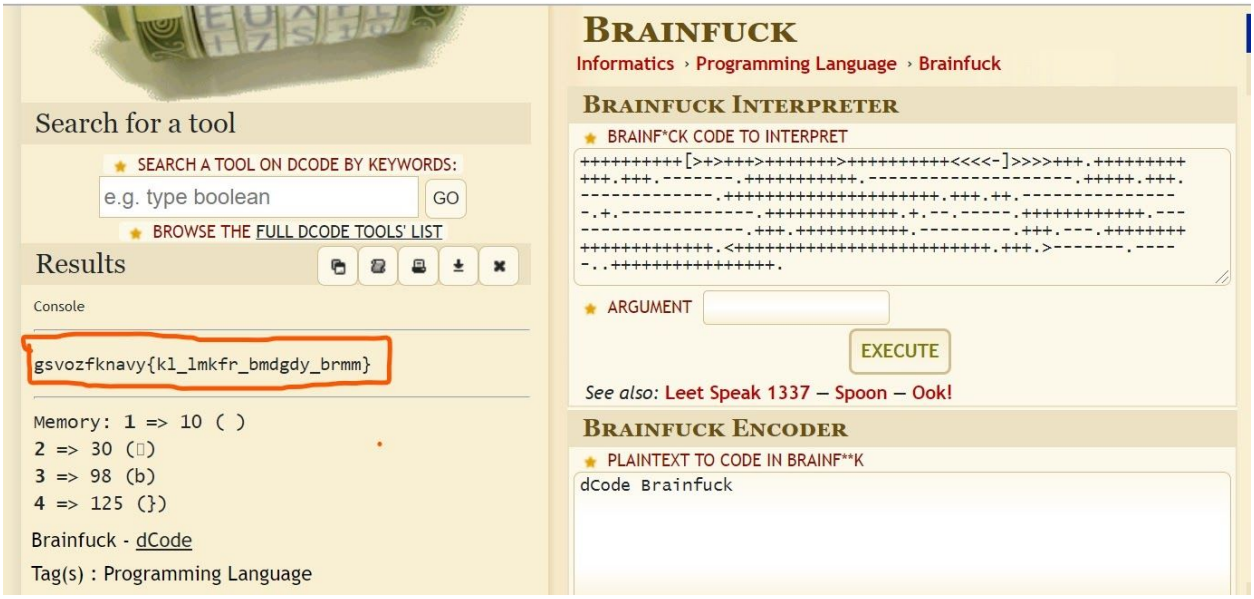
Step 1: Identify the target hash . Here , I used Hash Analyzer online tools

Step 2: The target hash type is **md5** . Now , try to crack the hash . Here , **I used md5hashing.net online hash cracker tools** .

Step 3:We **cracked the md5 hash and result is brain fuck cipher**



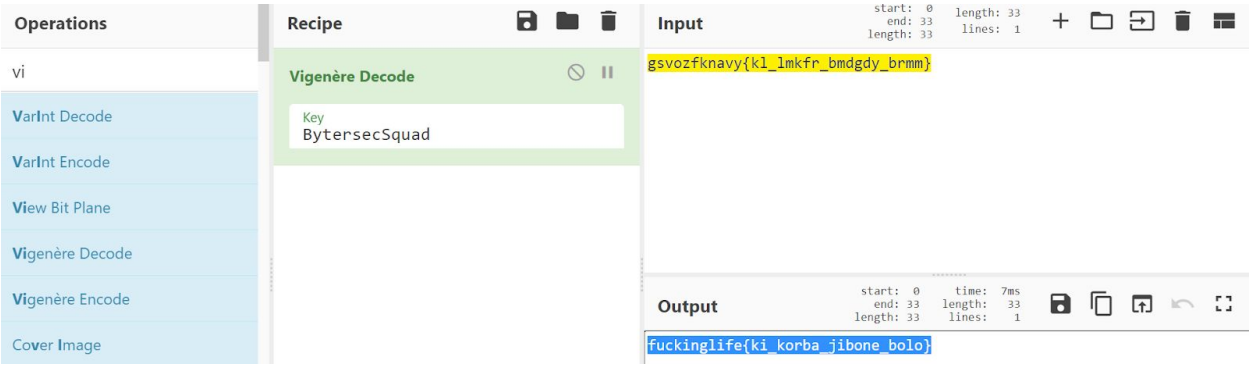
Step 4: Use online tools and decode **target brain fuck cipher** .



Step 5: After Decode we got the cipher again . Ok , no problem, try to decrypt it .

Step 6: Look at the Challenge description , there is a hint: BytersecSquad but we did not use it before . So , it can be key for decrypting a cipher if the target cipher is Vigenere Cipher.

Step 7: Wow, **we decrypt our target cipher using hints .**



Step 8: Finally ,

Type1 cipher ----md5
Type2 cipher -----brainfuck
Type3 cipher -----vigenere

So ,the flag is :

Cyberbangla{md5_brainfuck_vigenere}