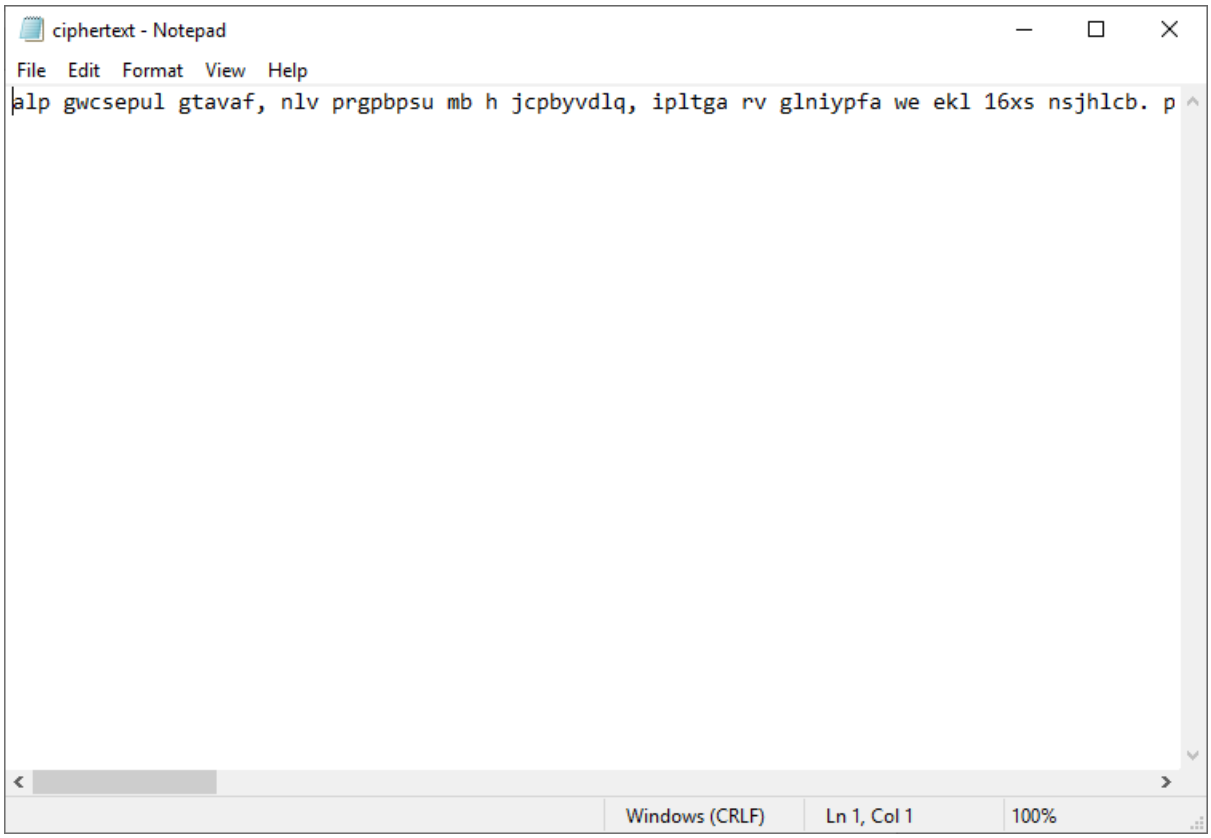
Teng Wei Xian B031610131 3BITZ

1.0 Classic, yet complicated!

1. Download the Zip file and open the cipertext.txt. It contains some cipertext, using Caesar cipher doesn't show the result, so I use classic vigenere.



2. Search classic vigenere decode on Google and choose https://www.guballa.de/vigenere-solver. Copy the ciphertext and click break cipher.

3. Then the result will be shown. Answer is ***HTB{helloworld}.***

Result

Clear text [hide]

Clear text using key "helloworld":

```
the vigenere cipher, was invented by a frenchman, blaise de
vigenere in the 16th century. it is a polyalphabetic cipher
because it uses two or more cipher alphabets to encrypt the data.
in other words, the letters in the vigenere cipher are shifted by
different amounts, normally done using a word or phrase as the
encryption key . unlike the monoalphabetic ciphers, polyalphabetic
ciphers are not susceptible to frequency analysis, as more than
one letter in the plaintext can be represented by a single letter
in the encryption. the key is the flag.
```

Details [show]

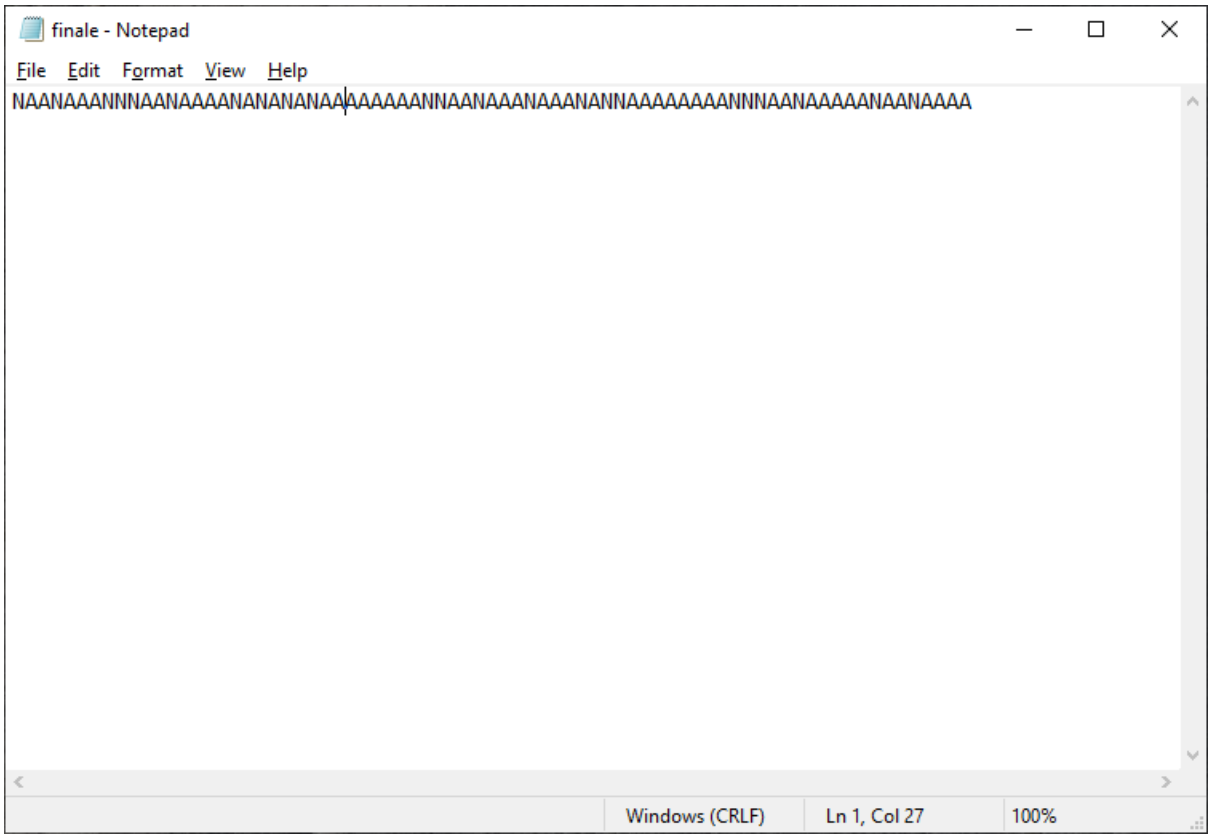
Key length statistics [show]

Histogram [show]

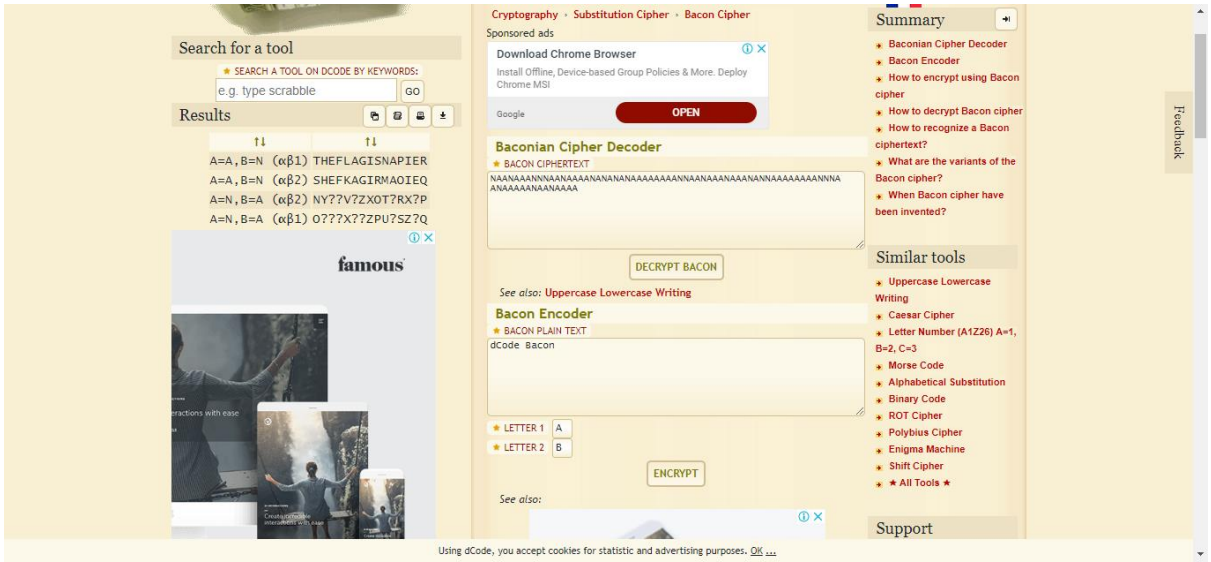
Runtime: 0.010 seconds

2.0 Deceitful Batman

1. From the cipher text we could guess is baconian cipher because it contains two repeated character.

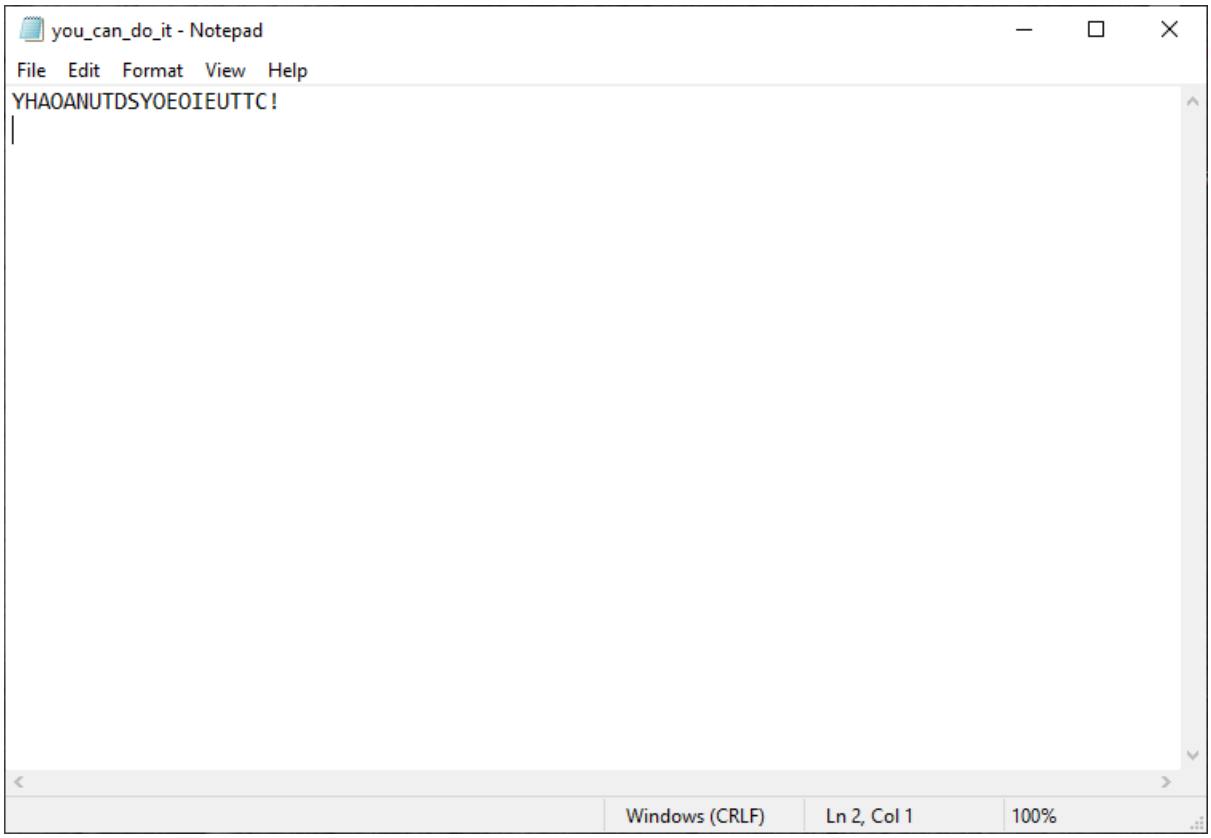


2. Using online tools https://www.dcode.fr/bacon-cipher, we enter the code. We can see the there is THEFLAGISNAPIER. So the flag will be ***HTB{NAPIER}.***



3.0 You Can Do It!

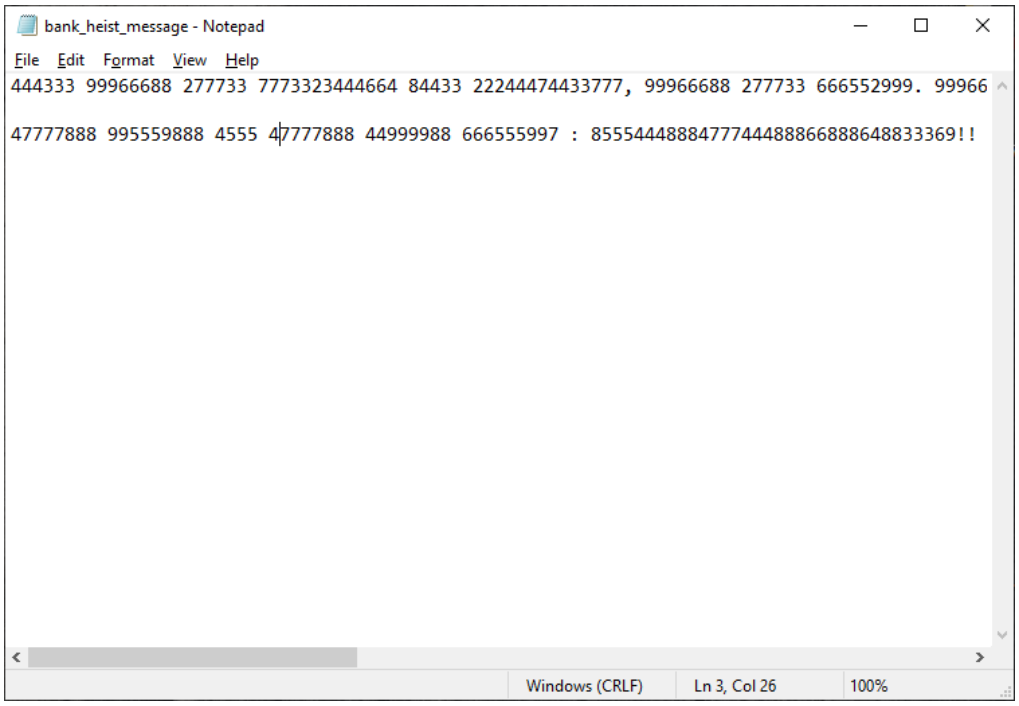
1. From the ciphertext below, we can conclude that it actually quite related to the title, so I think it just a scrambled of letters in sentence.



2. By using Caesar Box Cipher, we can rearrange the letter. Hence the answer will be ***HTB{YOUSEETHATYOUCANDOIT!}***

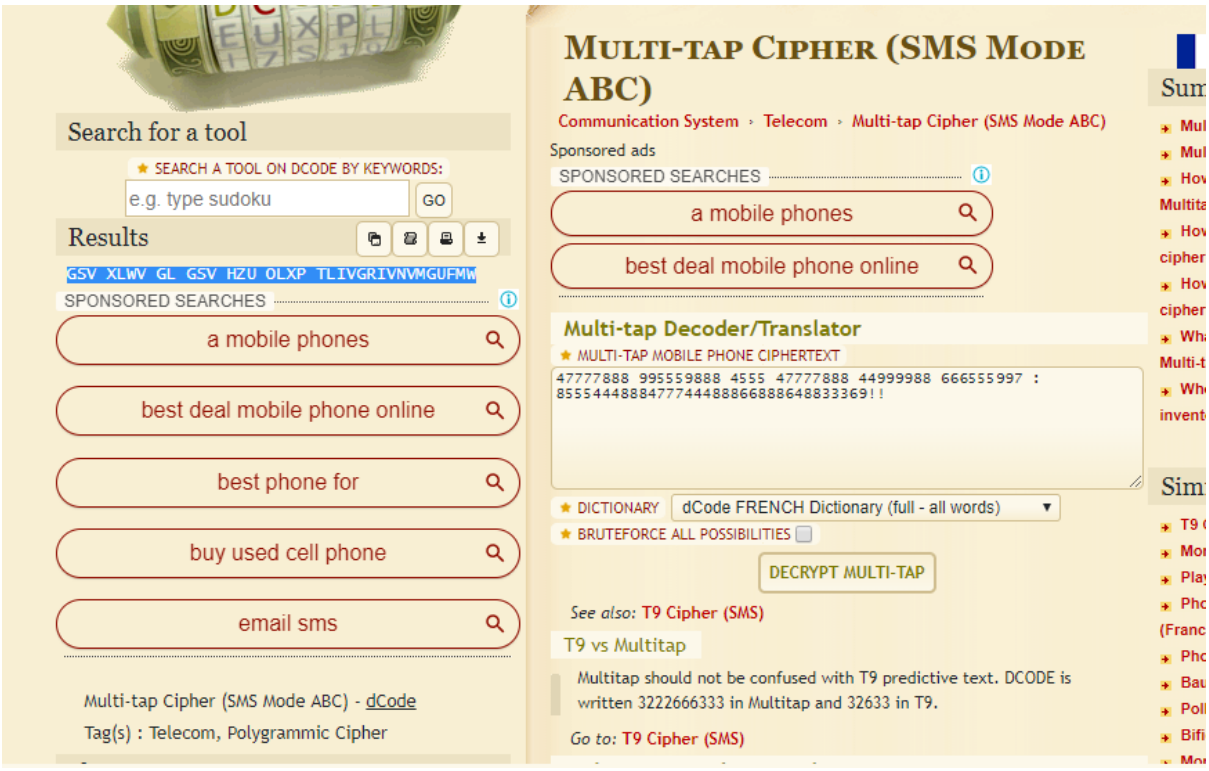
4.0 Bank Heist

1. As from the description show that it is using a phone. So, we can conclude that using a multi-tap cipher.



2. Using online tools multi-tap cipher sms mode, the message decoded are [IIGF YOU ARE READING THE CIPHER YOU ARE OKAY YOUR SHARE OF THE HEIST IS IN YOUR HOUSE THE KEY TO THE LOCK IS BELOW GO TO PARIS]

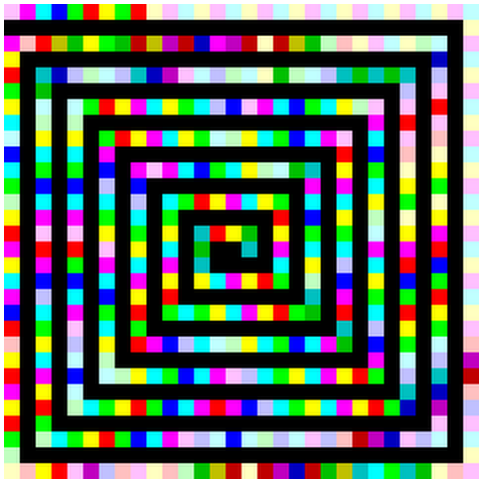
3. The second line of ciphertext will be using FRENCH Dictionary to decode. And it gives out [GSV XLWV GL GSV HZU OLXP TLIVGRIVNVMGUFMW].



4. Take the cipher and user Atbash Mirror Decoder. As we can see the flag will be ***HTB{GORETIREMENTFUND!!}***

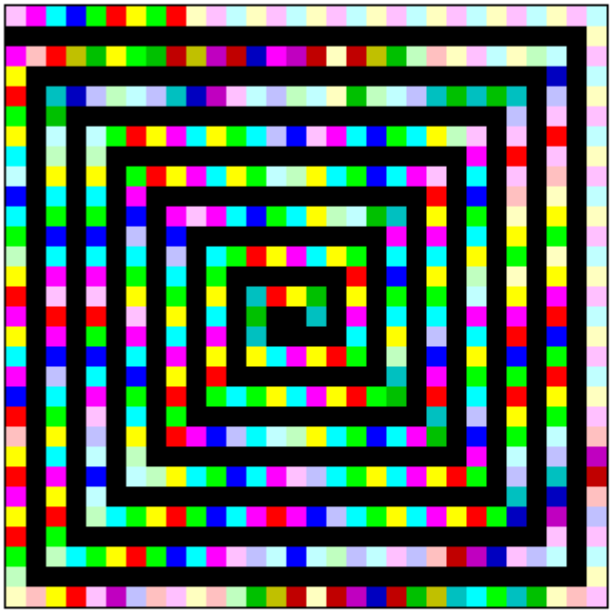
5.0 Art

1. Download the image, is look like a portable pixmap. Use npiet online to decode.



2. Therefore the flag is ***HTB{p137_m0ndr14n}***

Info: upload status: Ok
Info: found picture width=300 height=300 and codel size=10
Uploaded picture (shown with a small border): **art.png**

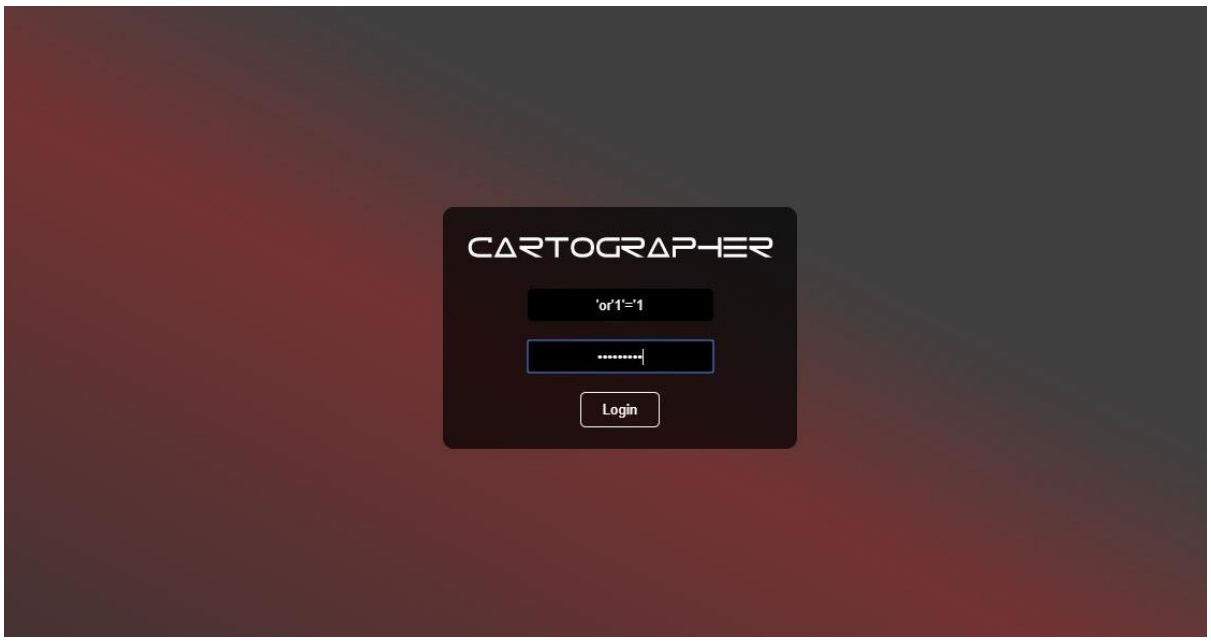


Info: executing: npiet -e 1000000 art.png

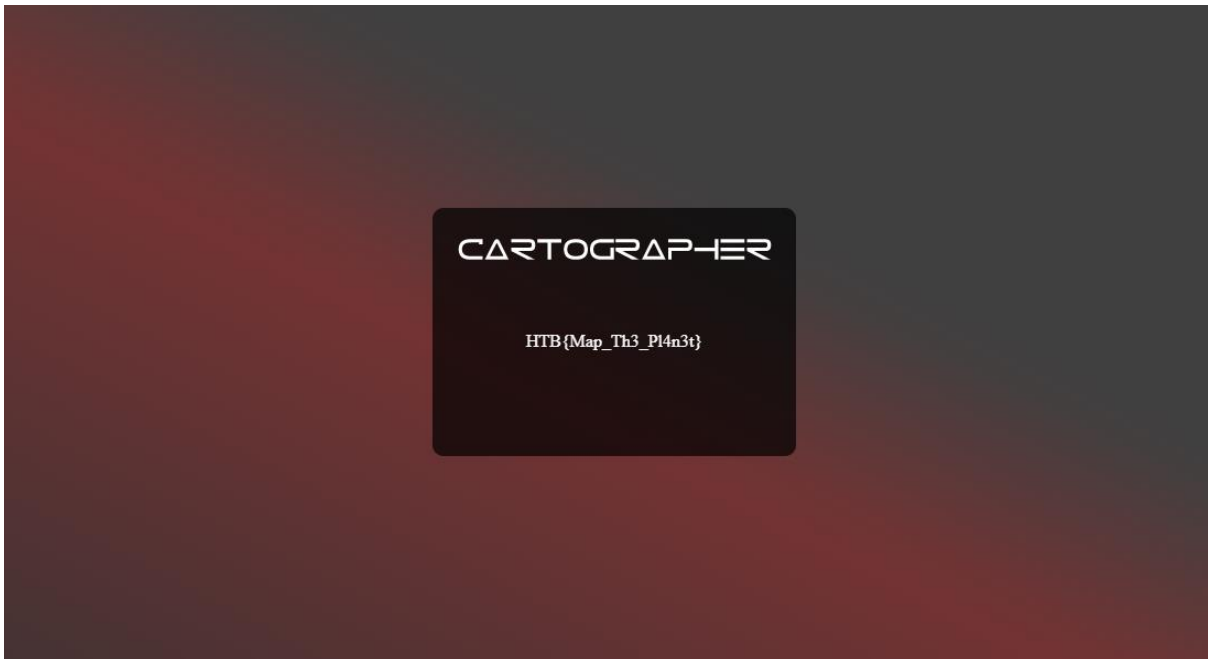
```
HTB{p137_m0ndr14n}? ? $□? ? □□18? 32464? ? ? 8? ? ?
```

6.0 Cartographer

1. Login using 'or'1'='1 by SQL injection.

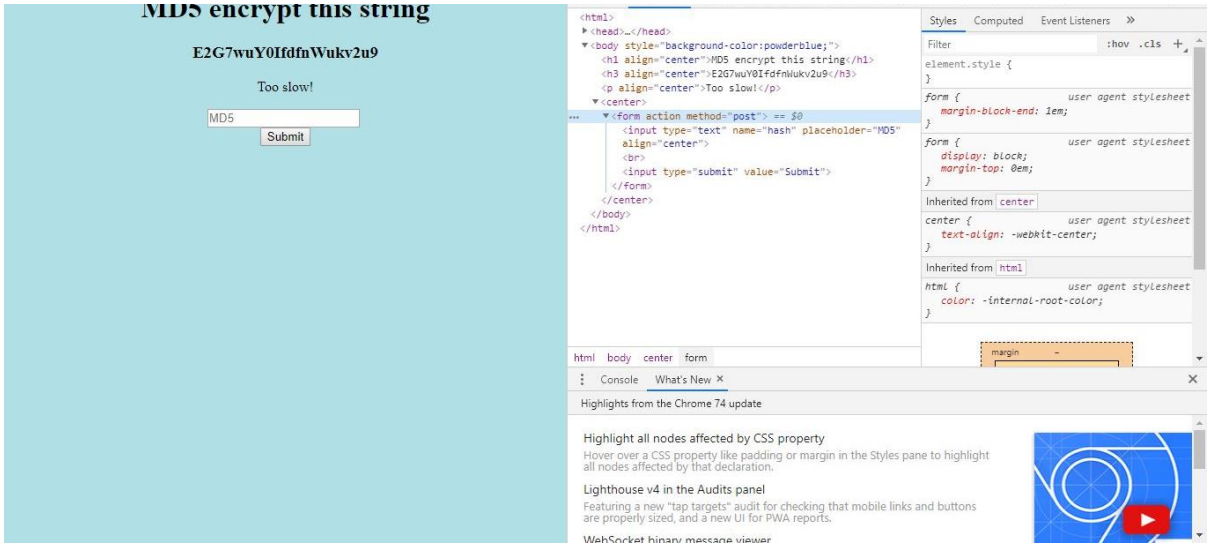


2. At the URL inject info=flag. Flag=***HTB{Map_Th3_Pl4n3t}.***

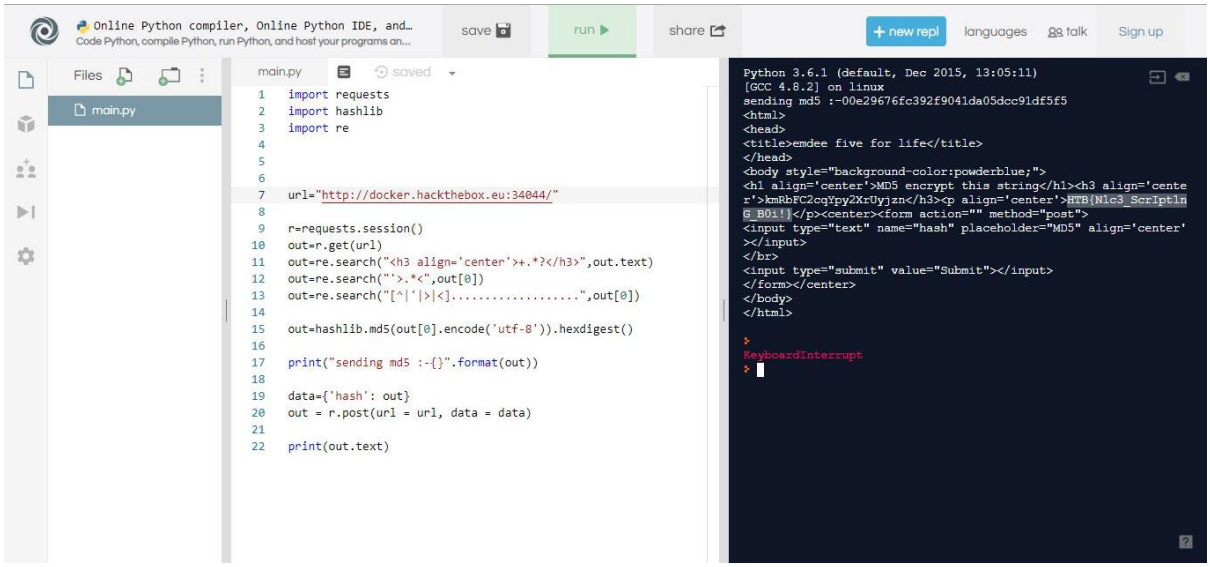


7.0 HDC

1. First inspect the code.

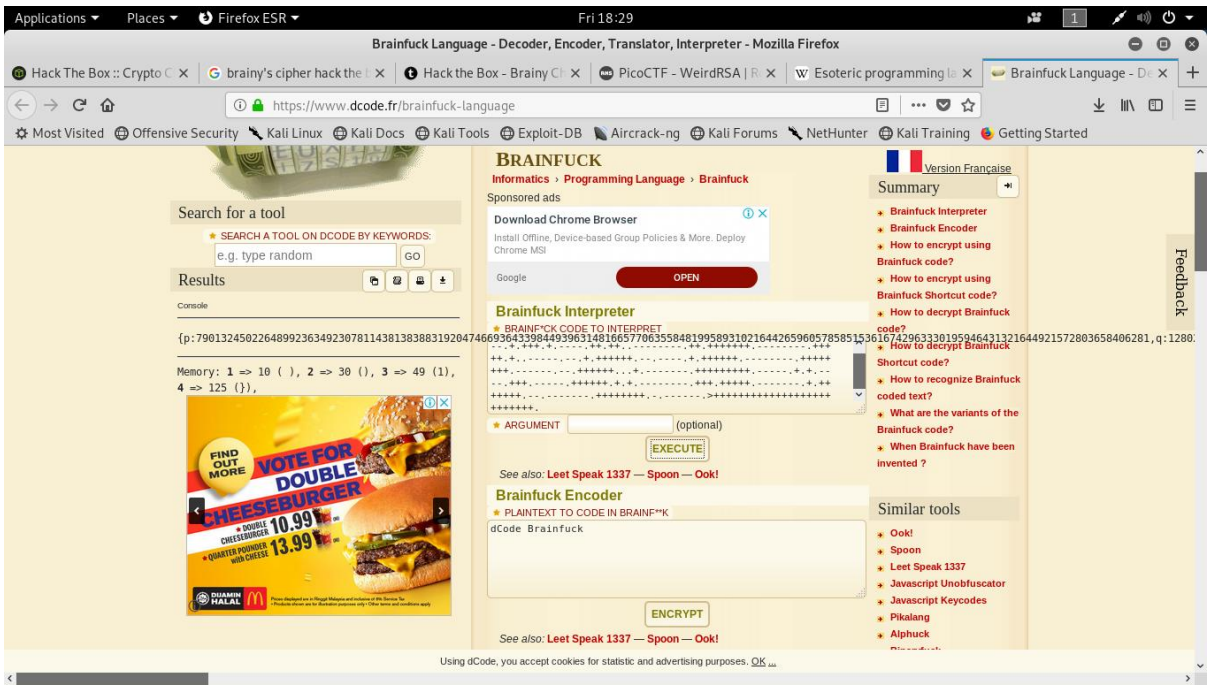


2. Write a python code and run so that can extract the flag. The flag is ***HTB{N1c3_ScrIpt1nG_B0i!}.***

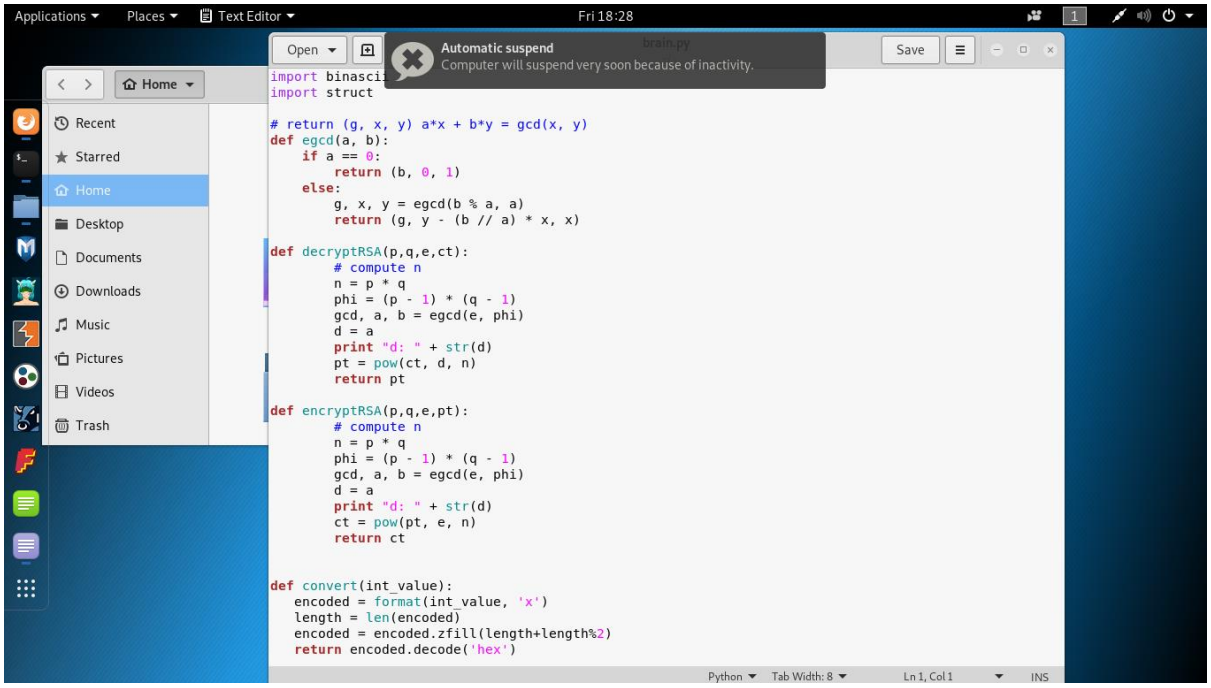


8.0 Brainy's Cipher

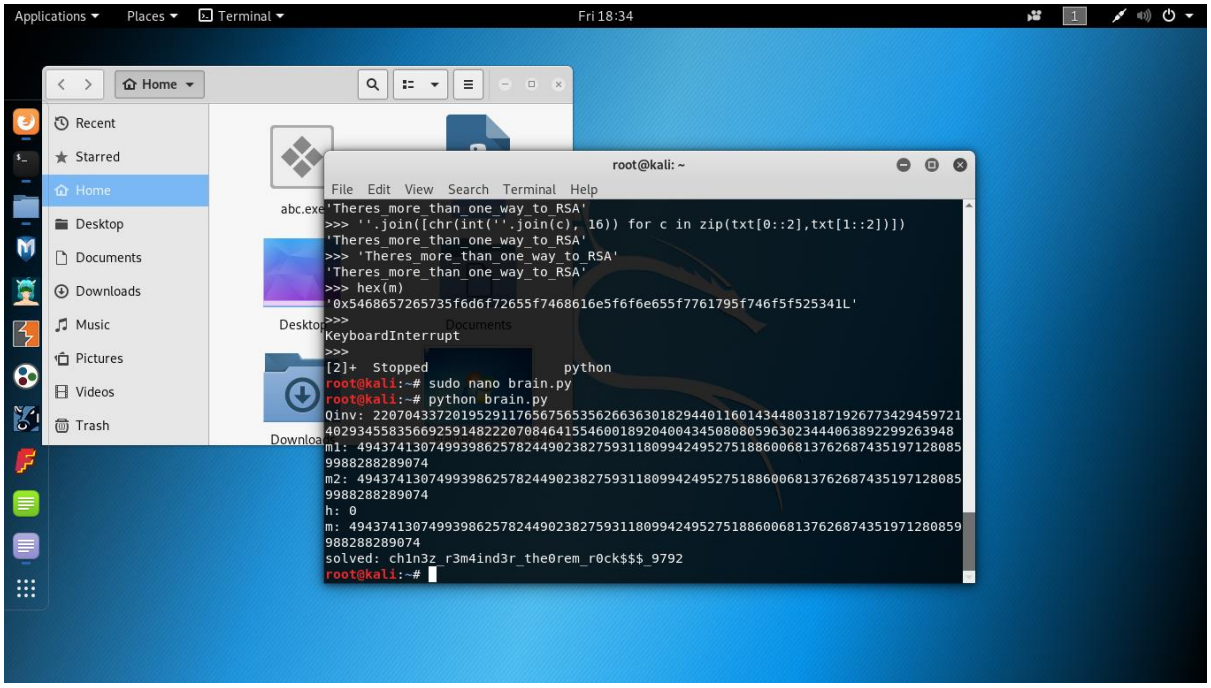
1. Using BrainFuck algorithms to decode the ciphertext.



2. Using the coding below to decode.



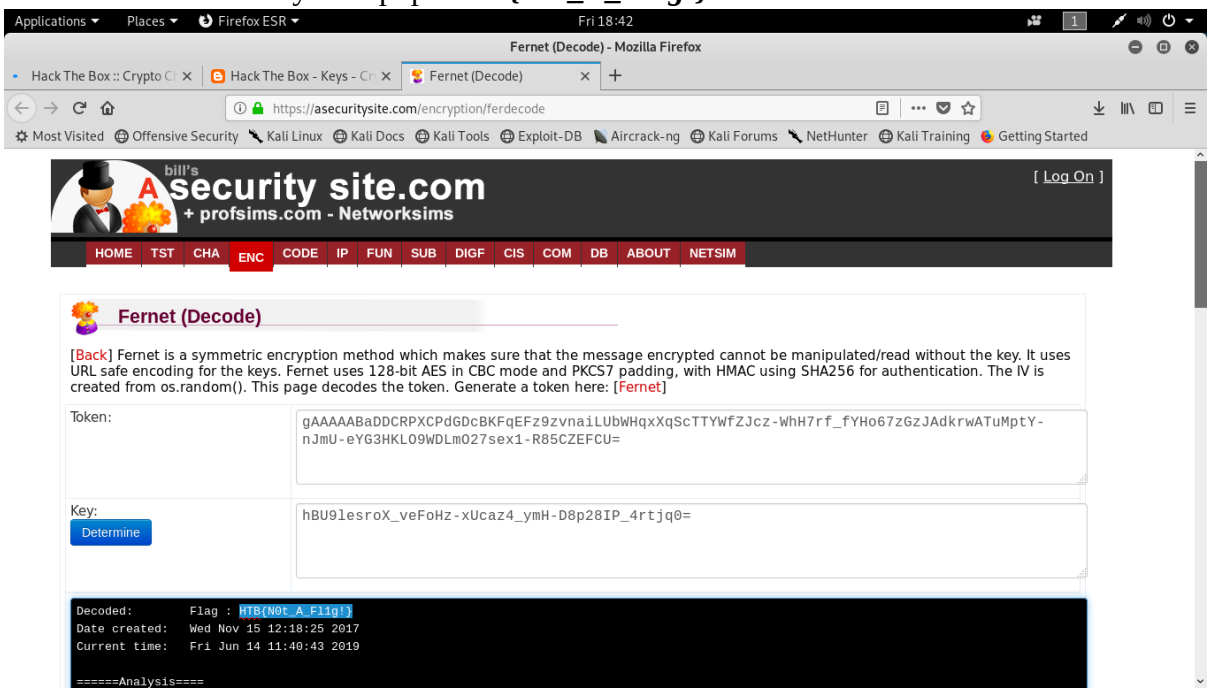
3. Then we get the flag. ***HTB{ch1n3z_r3n4indir_the0rem_rock$$$_9792}***.



9.0 Keys

1. From the ciphertext, we could guess it is a Fernet algorithms.

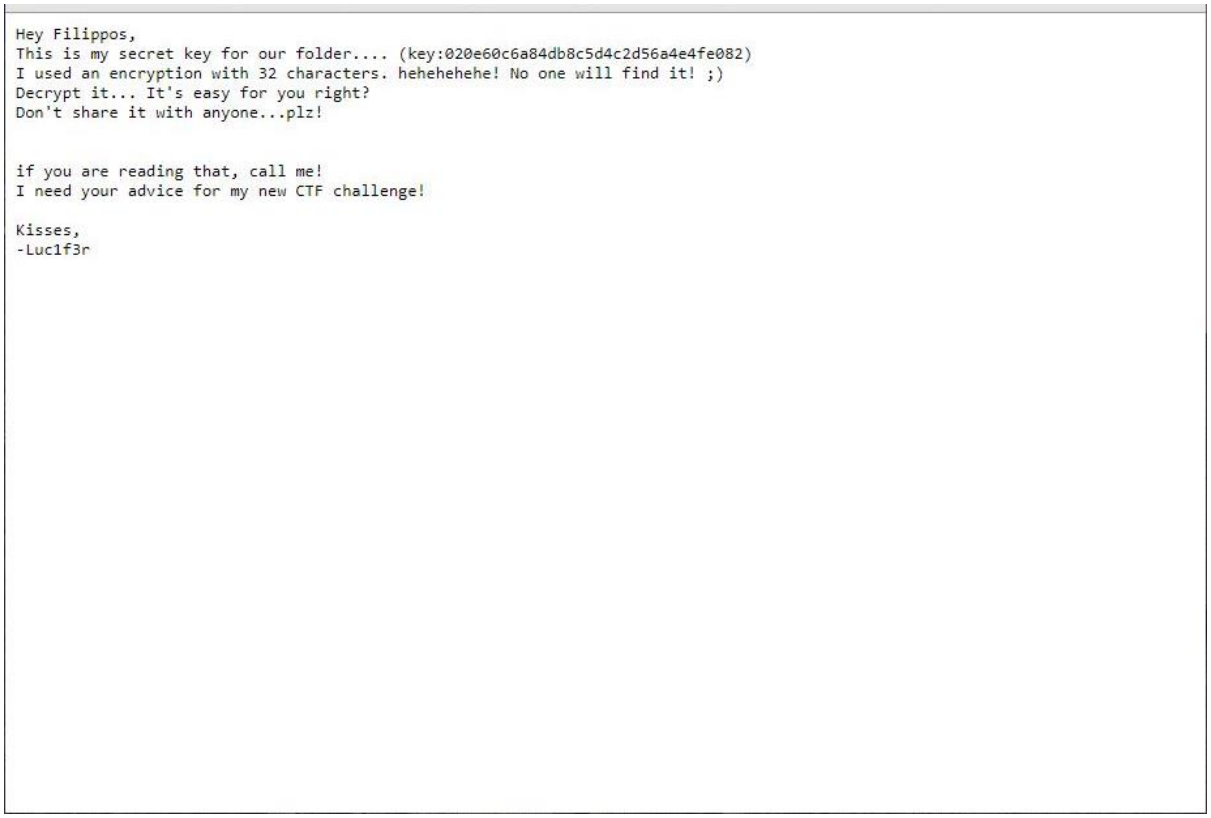
Enter the token and key then pop: ***HTB{N0t_A_Fl1g!}***



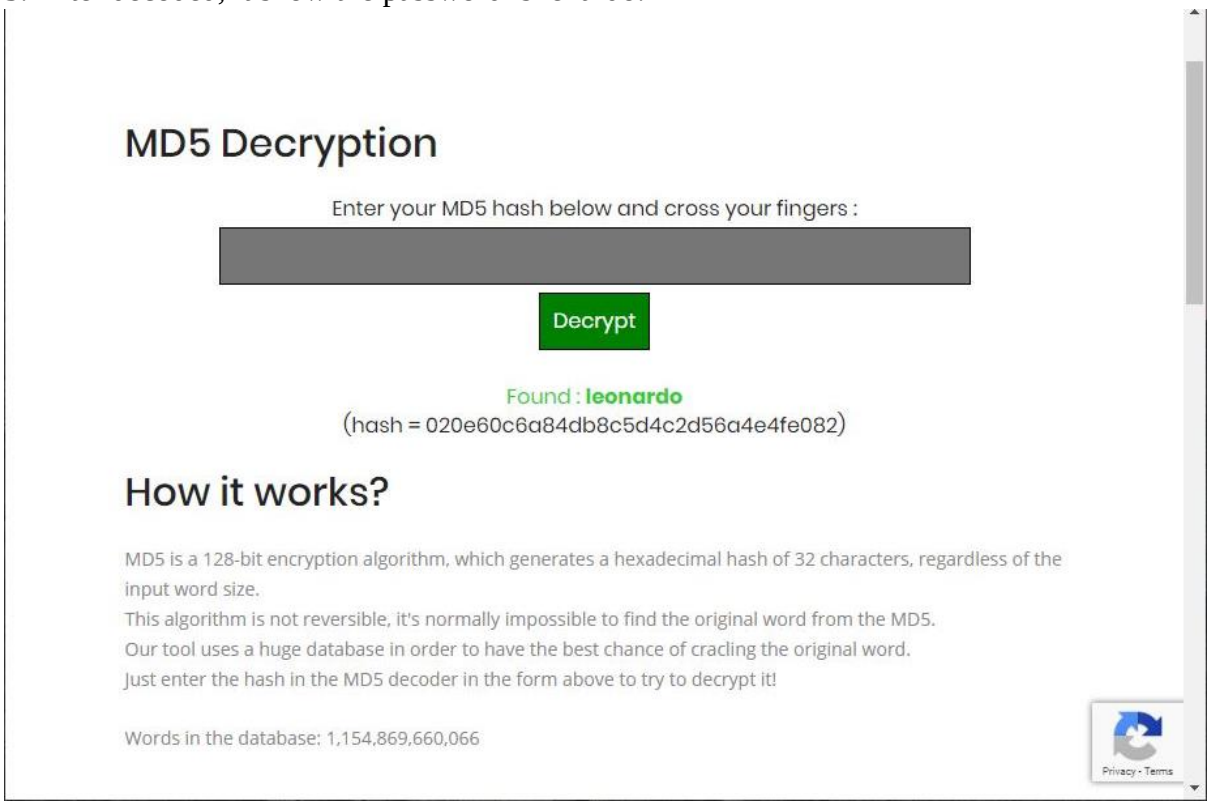
10.0 Da Vinci

1. Download the file, It has 3 image. First we take the picture with paraphrase which is TOM.

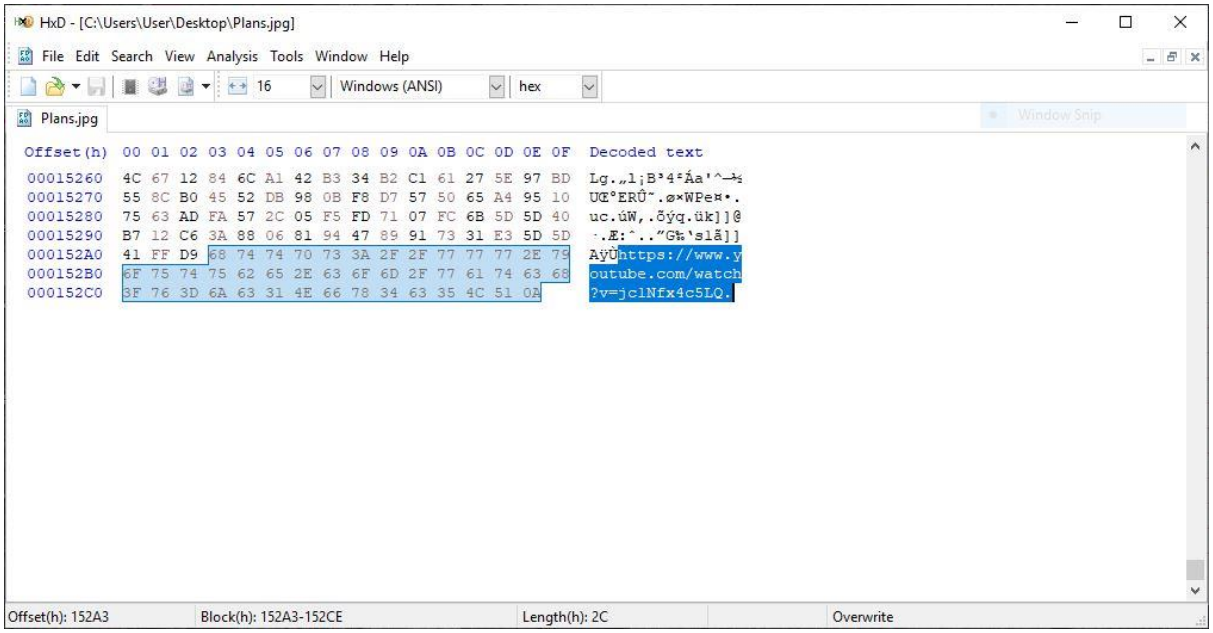
2. It give the key with md5 encoded.



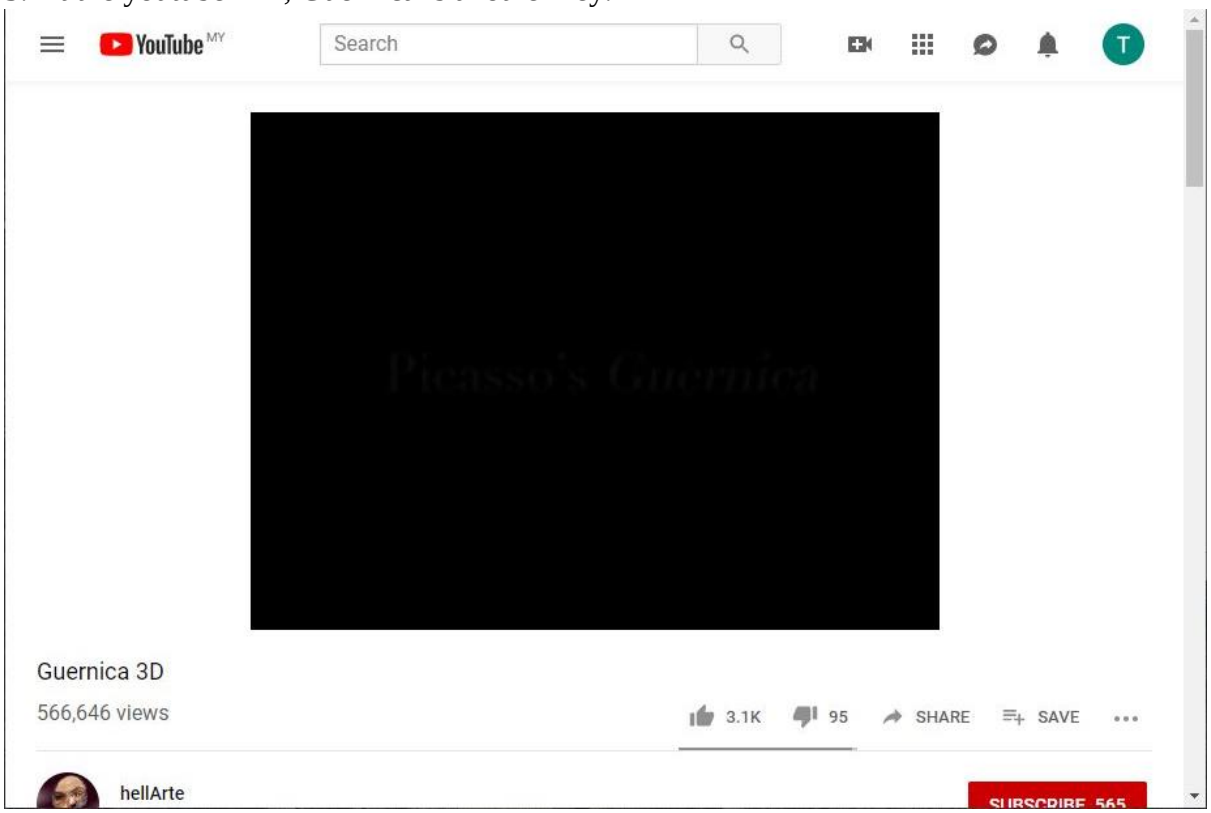
3. After decoded, it show the password is lenardo.



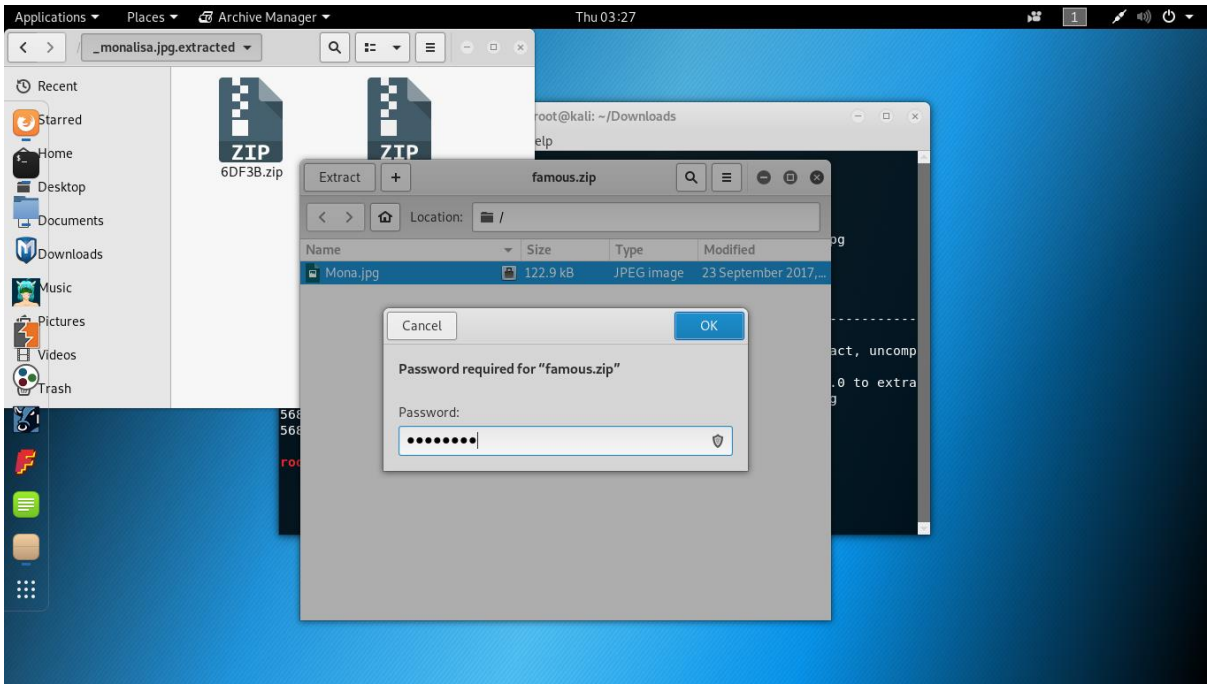
4. For the Plan image, drop to HXD and there is a youtube link.



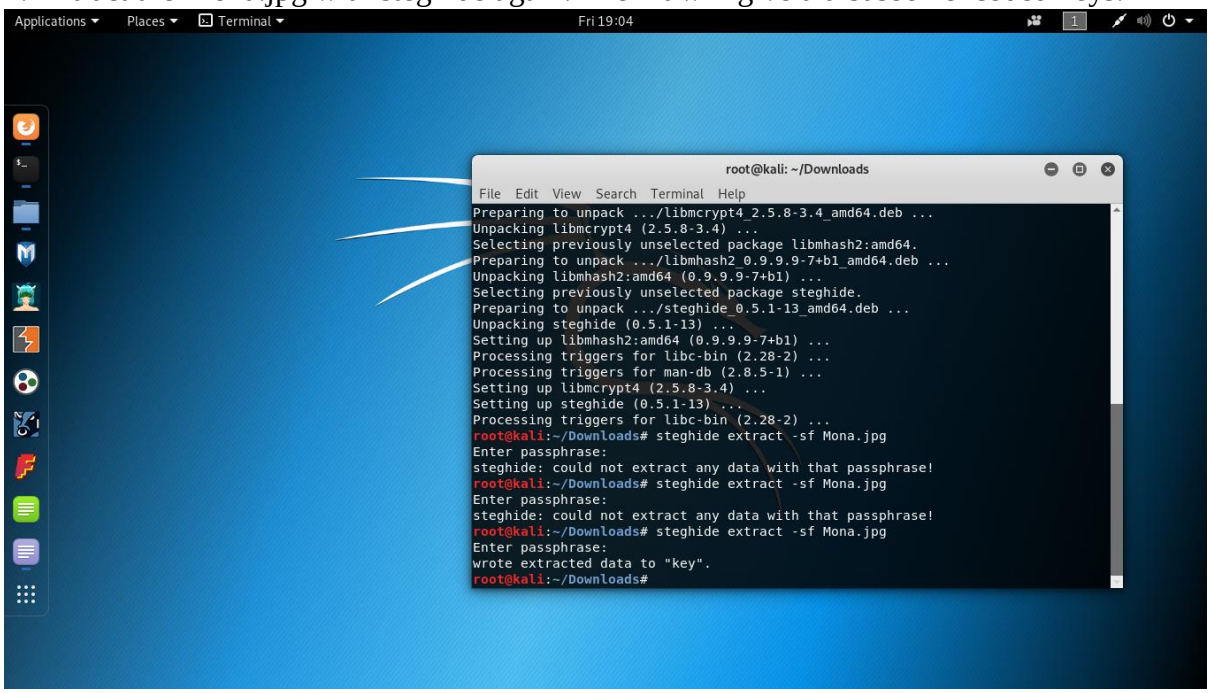
5. At the youtube link, Guernica is another key.



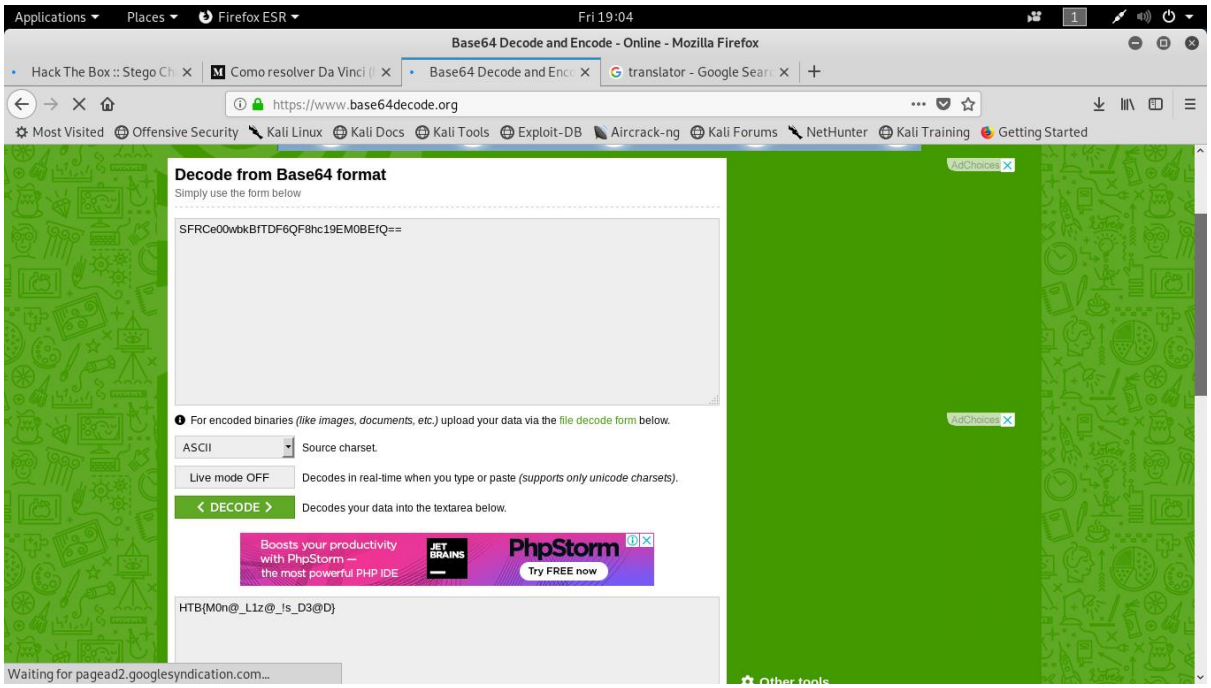
6. After steghide the monalisa, it has 2 zip files in it. Extract the famous.zip using leonardo. Output is Mona.jpg.



7. Extract the Mona.jpg with steghide again. Then it will give u a base64 encoded keys.

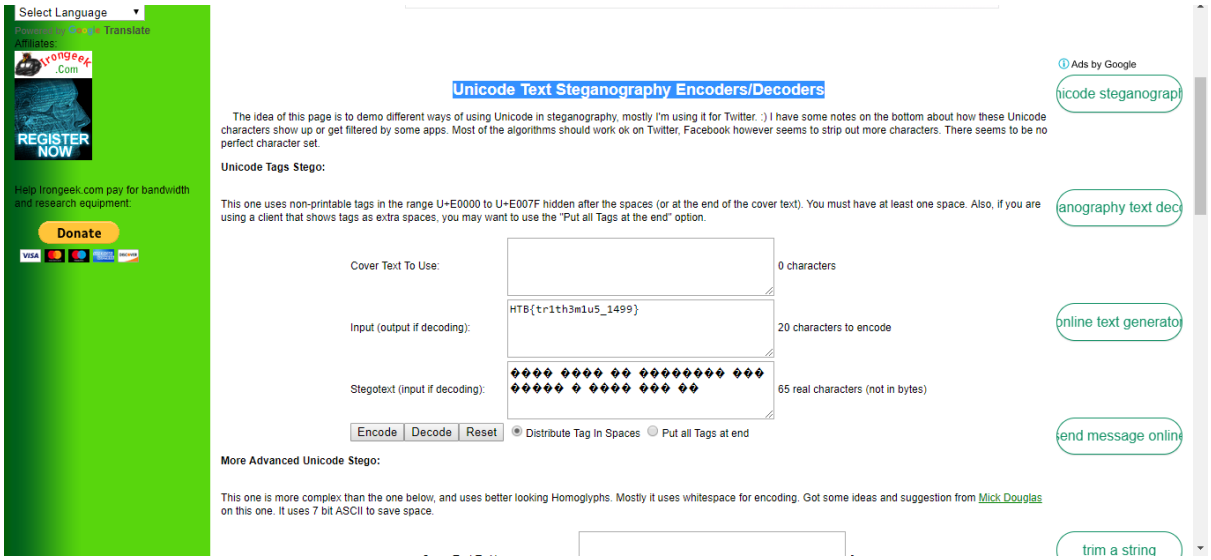


8. Take the key and decoded 3 times. ***HTB{M0n@_L1z@_!sD3@D}***



11.0 Unified

1. The code is using Unicode Text Steganography Encoders/Decoders. So decode the unknow character to get flag ***HTB{tr1th3m1u5_1499}.***

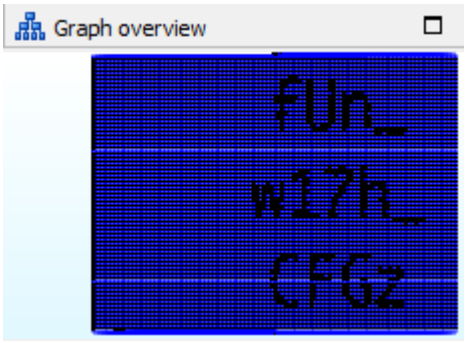


12.0 Pusheen Loves Graphs

1. Since it mention only IDA can read, so open with IDA.

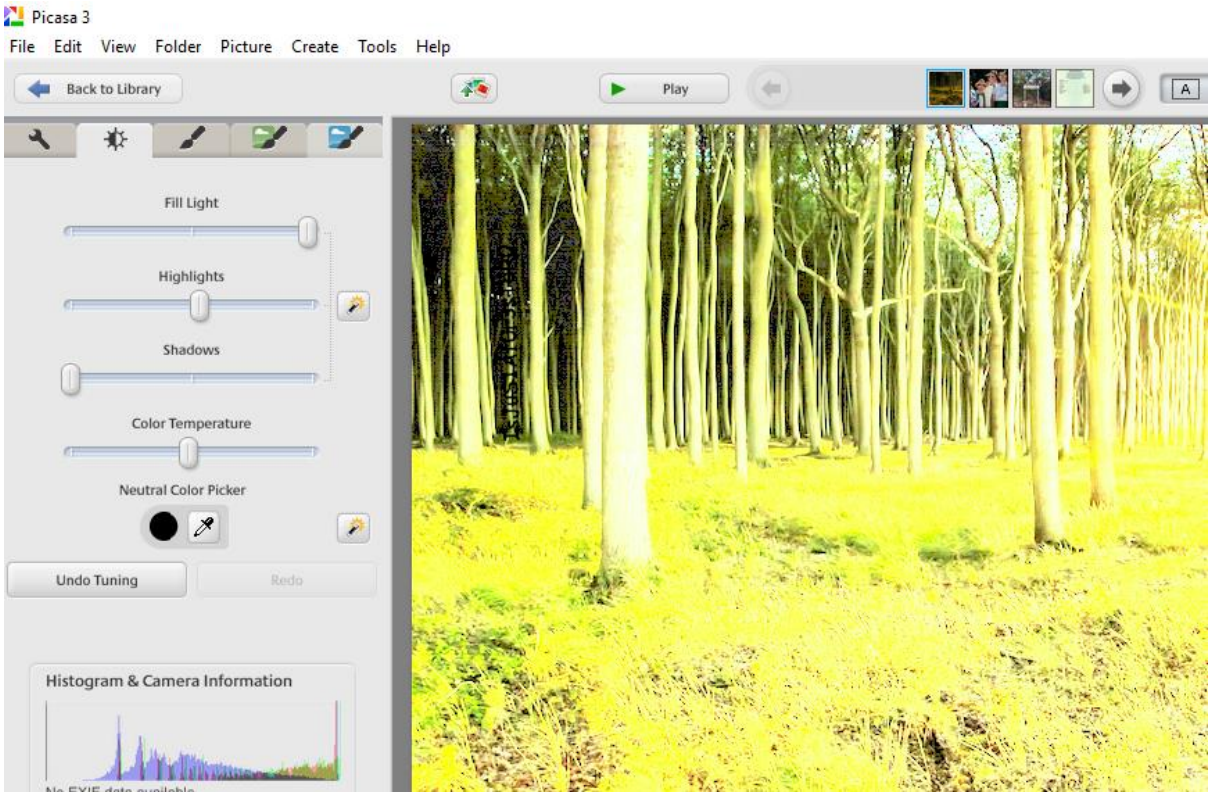
When loading the executable file in IDA it will throw an error on the maximum amount of nodes (in my case they were 1,000), then I raised it to 2,000 and then to 20,000 given that 2,000 was not enough.

Then it show the result below. ***HTB{fUn_w17h_CFGz***}.

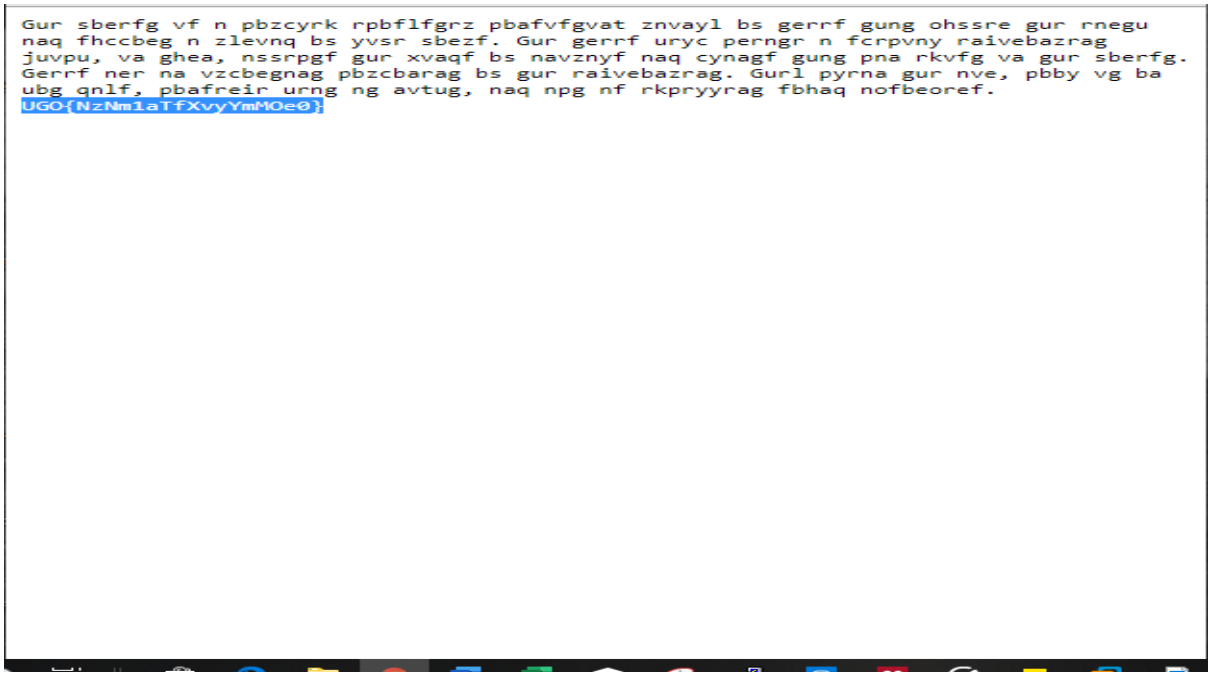


13.0 Forest

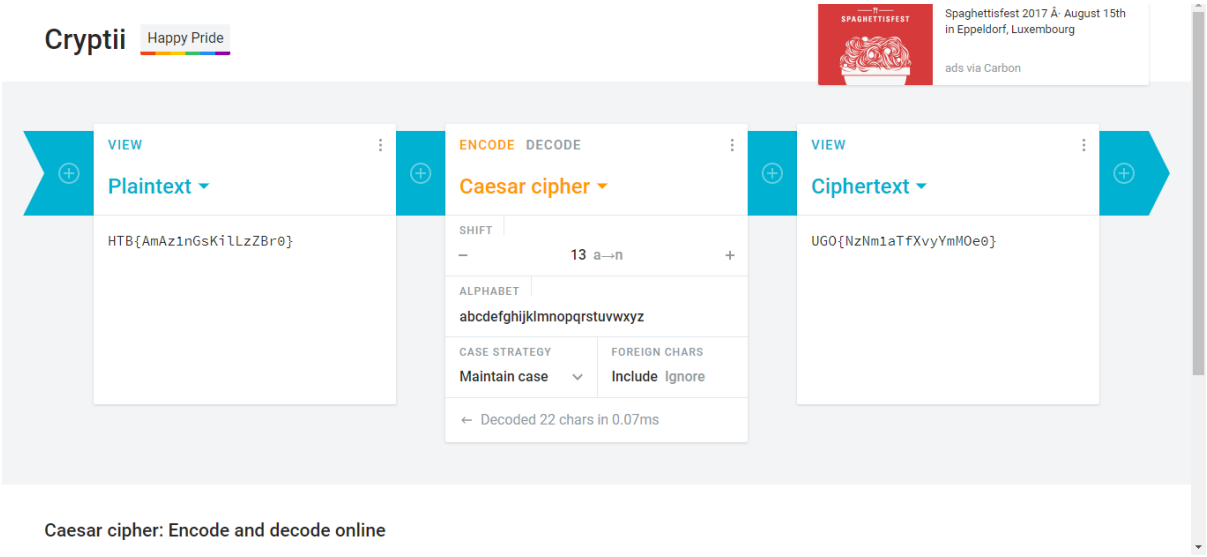
1. Using Picasa 3, adjust the light to highest, we can view some word on the pic. which is IsJuS1Af0r3sTbR0.



2. Use the phrase above to decode the forest.jpg.

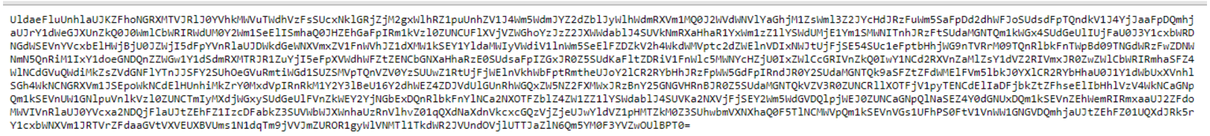


3. Use Caesar cipher to decode the flag: ***HTB{AmAz1nGsKilLzZBr0}.***

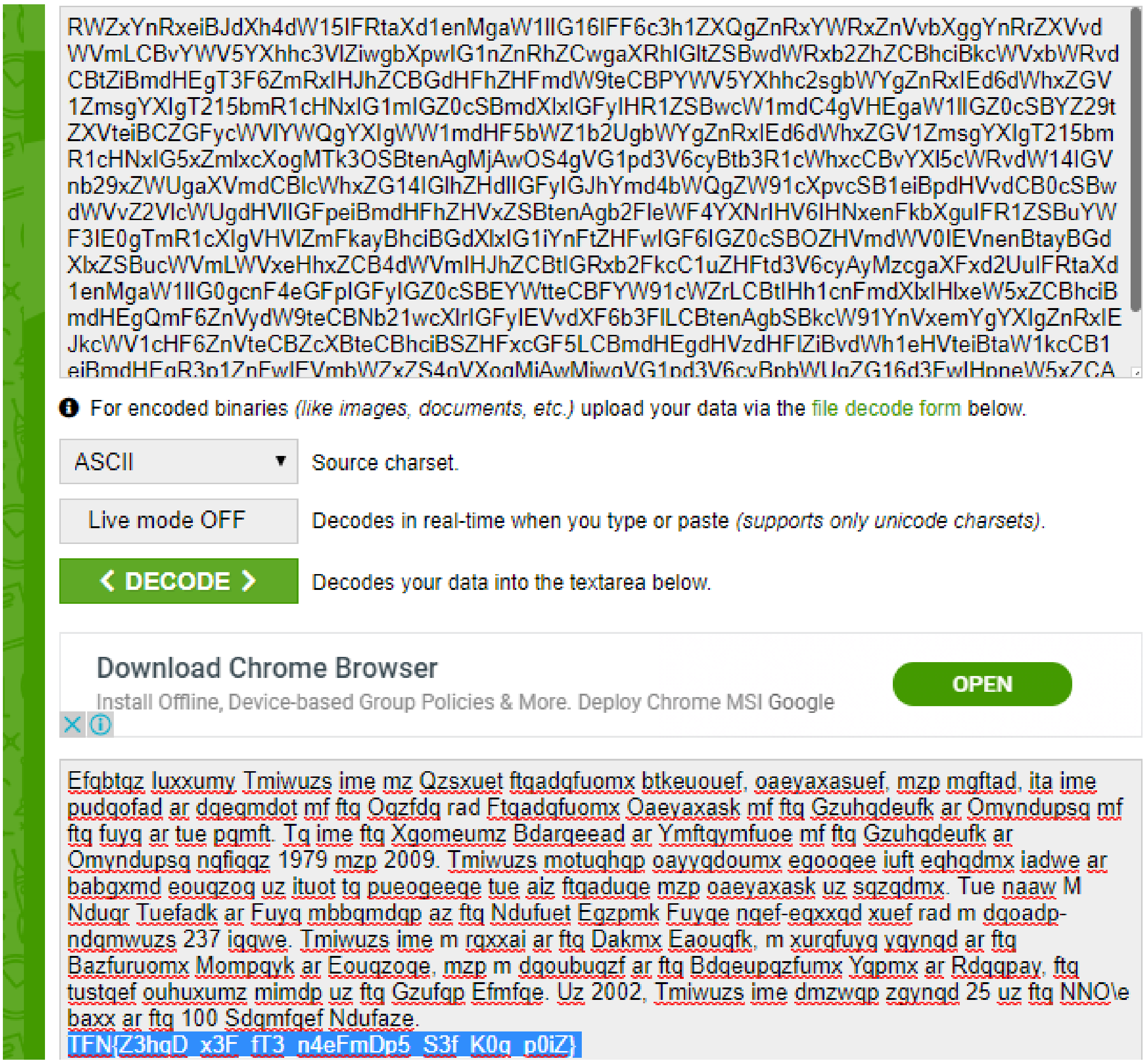


14.0 Blackhole

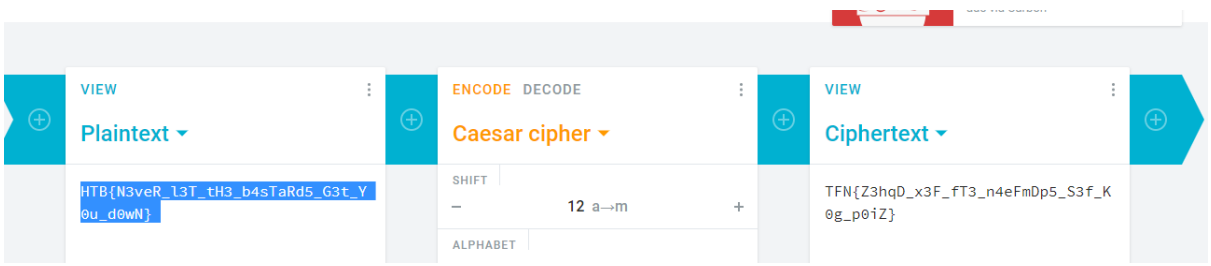
1. Download the file, unzip it. It will show a hawking file. Using HxD we could know it is a JIFF file which will using steganography. Upload the file to decoder using phrase hawking.



2. Decode it twice using base64 decoder to get a {}.

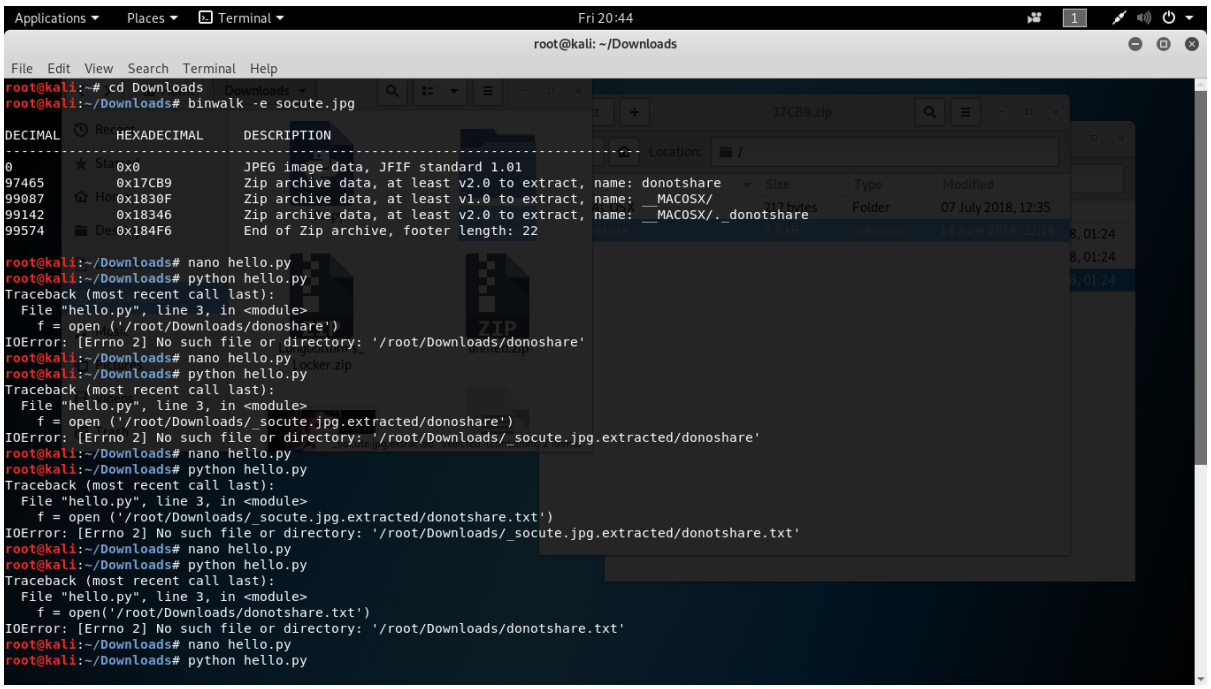

For encoded binaries (like images, documents, etc.) upload your data via the file decode form below.
ASCII
Source charset.
Live mode OFF
Decodes in real-time when you type or paste (supports only unicode charsets).
DECODE
Decodes your data into the textarea below.
Download Chrome Browser
Install Offline, Device-based Group Policies & More. Deploy Chrome MSI Google
OPEN
Efqbtqz luxxumy Tmiwuzs ime mz Qzsxuet ftqadqfuomx btkeuouef, oaeyaxasuef, mzp mqftad, ita ime pudqofad ar dqeqmdot mf ftq Oqzfdq rad Ftqadqfuomx Oaeyaxask mf ftq Gzuhqdeufk ar Omyndupsq mf ftq fuyq ar tue pqmft. Tq ime ftq Xgomeumz Bdarqeead ar Ymftqymfuoe mf ftq Gzuhqdeufk ar Omyndupsq nqfiqqz 1979 mzp 2009. Tmiwuzs motuqhqp oayyqdoumx egoogee iuft eqhqdmx iadwe ar babgxmd eougzoq uz ituot tq pueogeege tue aiz ftqaduqe mzp oaeyaxask uz sqzqdmx. Tue naaw M Nduqr Tuefadk ar Fuyq mbbqmdqp az ftq Ndufuet Egzpmk Fuyqe nqef-eqxxqd xuef rad m dqoadp-ndqmwuzs 237 iqqwe. Tmiwuzs ime m rqxxai ar ftq Dakmx Eaouqfk, m xurqfuyq yqynqd ar ftq Bazfuruomx Mompqyk ar Eougzoqe, mzp m dqoubuqzf ar ftq Bdqeupqzfumx Yqpmx ar Rdqqpay, ftq tustqef ouhuxumz mimdp uz ftq Gzufqp Efmfqe. Uz 2002, Tmiwuzs ime dmzwqp zgynqd 25 uz ftq NNO'e baxx ar ftq 100 Sdqmfqef Ndufaze.
TFN{Z3hqD_x3F_fT3_n4eFmDp5_S3f_K0q_p0iZ}

3. Caesar cipher will do the rest. The flag is:
HTB{N3veR_l3T_tH3_b4sTaRd5_G3t_Y0u_d0wN}.

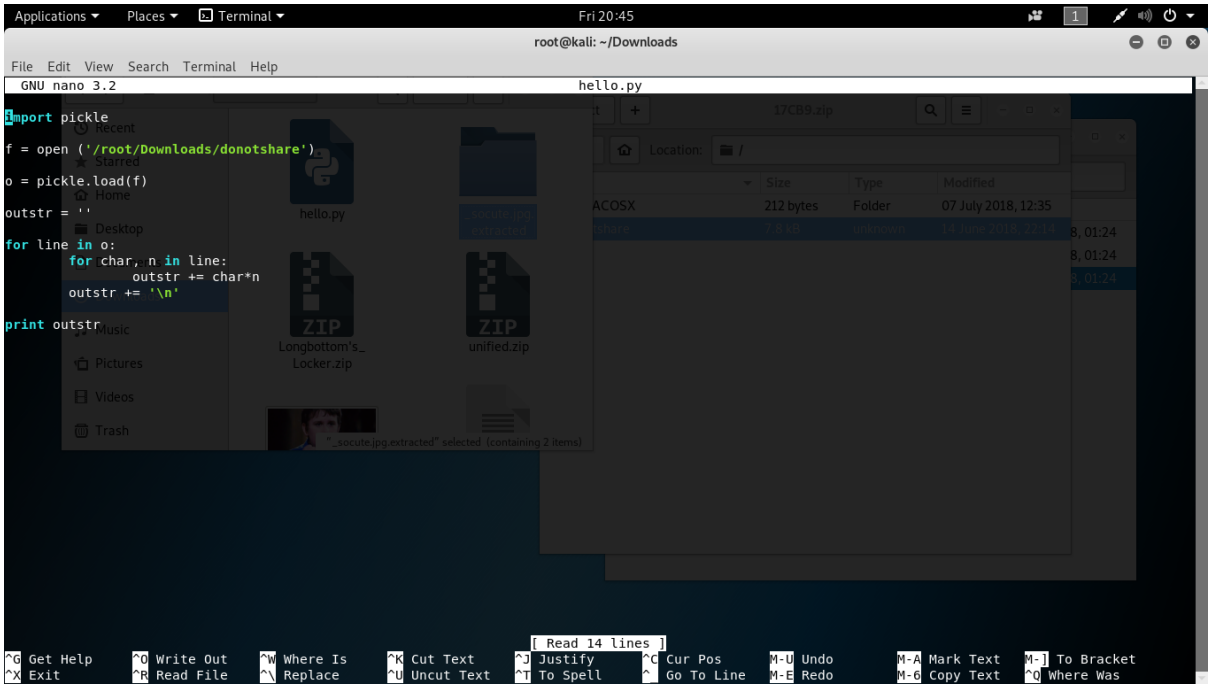


15.0 Longbottom's Locker

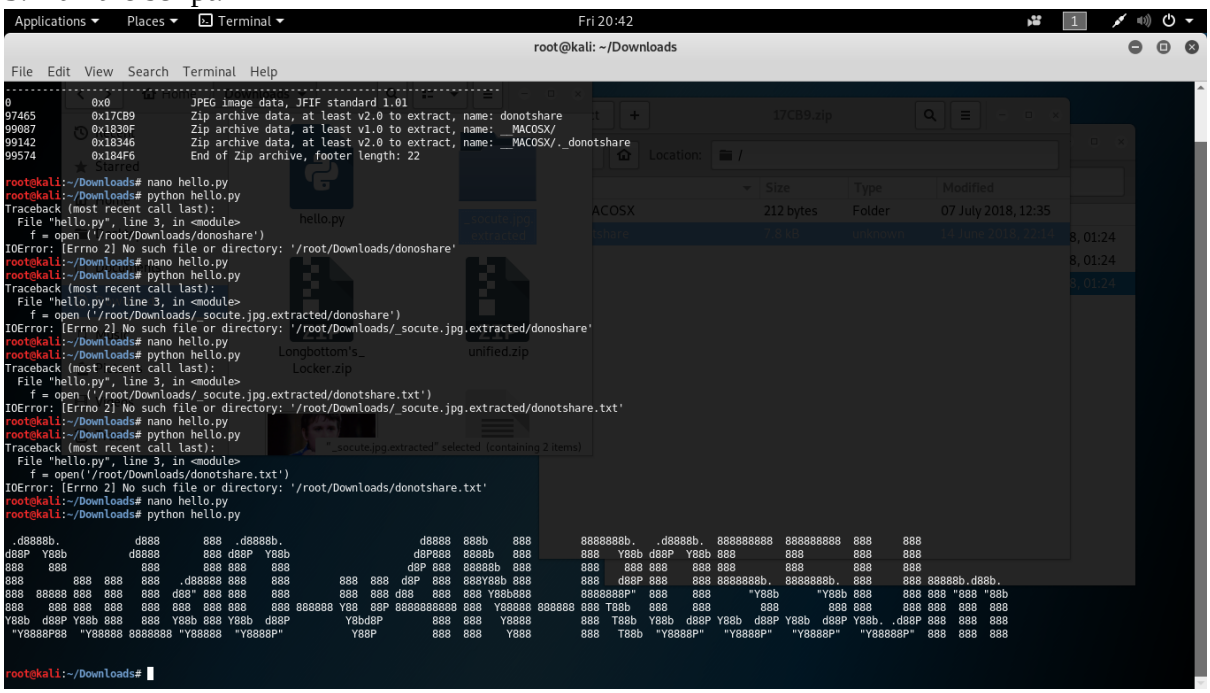
1. Extract the three file. Extract the file in the socute.jpg.



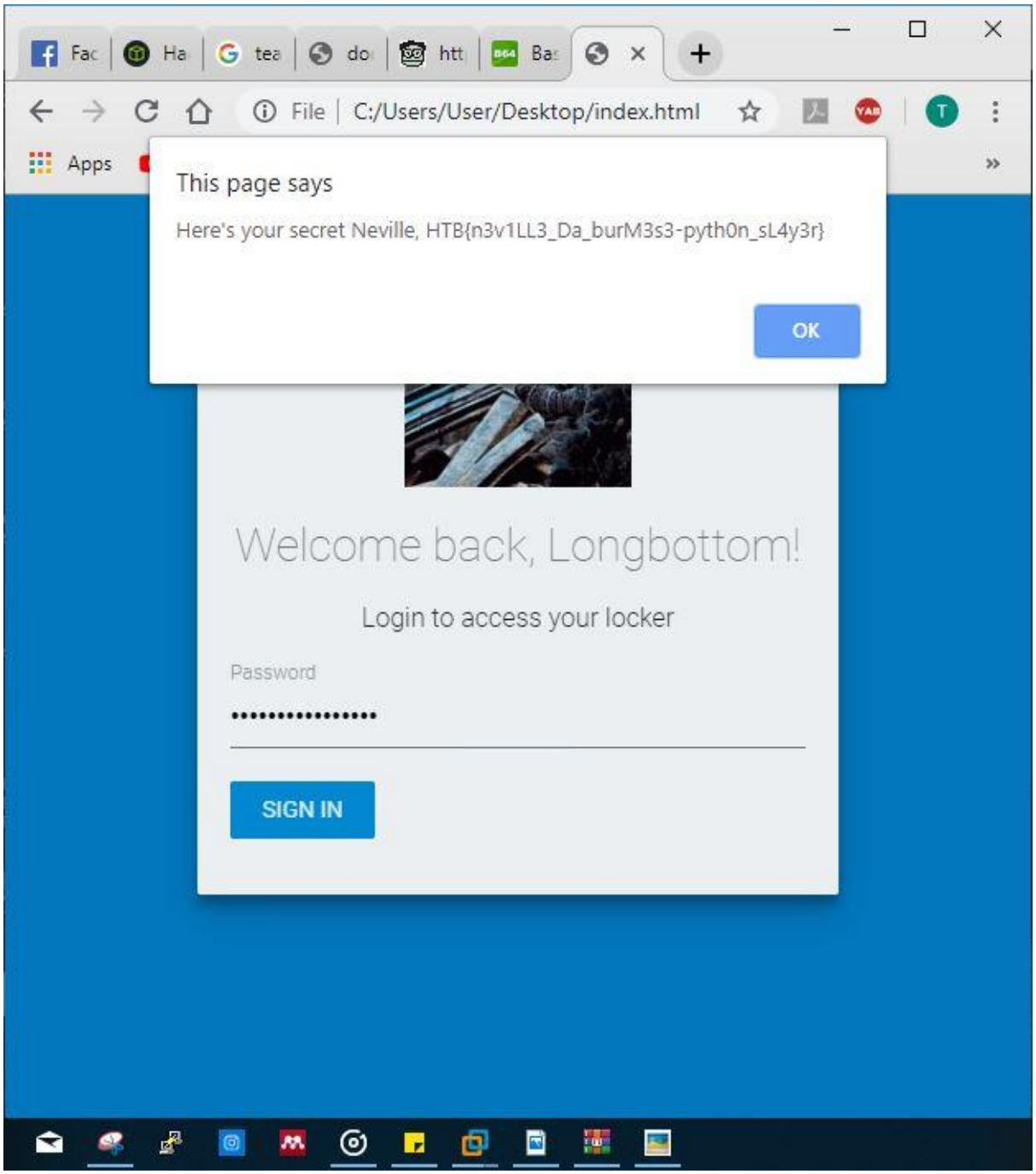
2. Write a python script to extract.



3. Run the script.

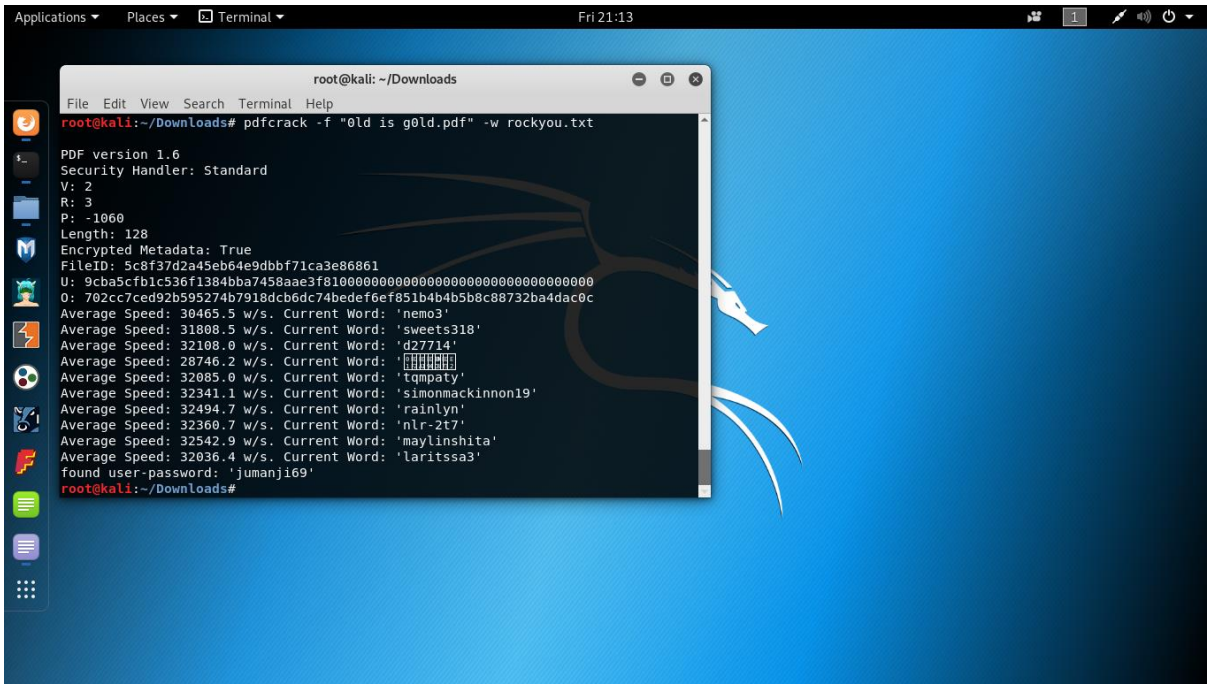


4. Use the key below and enter to the index.html. The flag is: ***HTB{n3v1LL3_Da_burM3s3-pyth0n_sL4y3r}.***

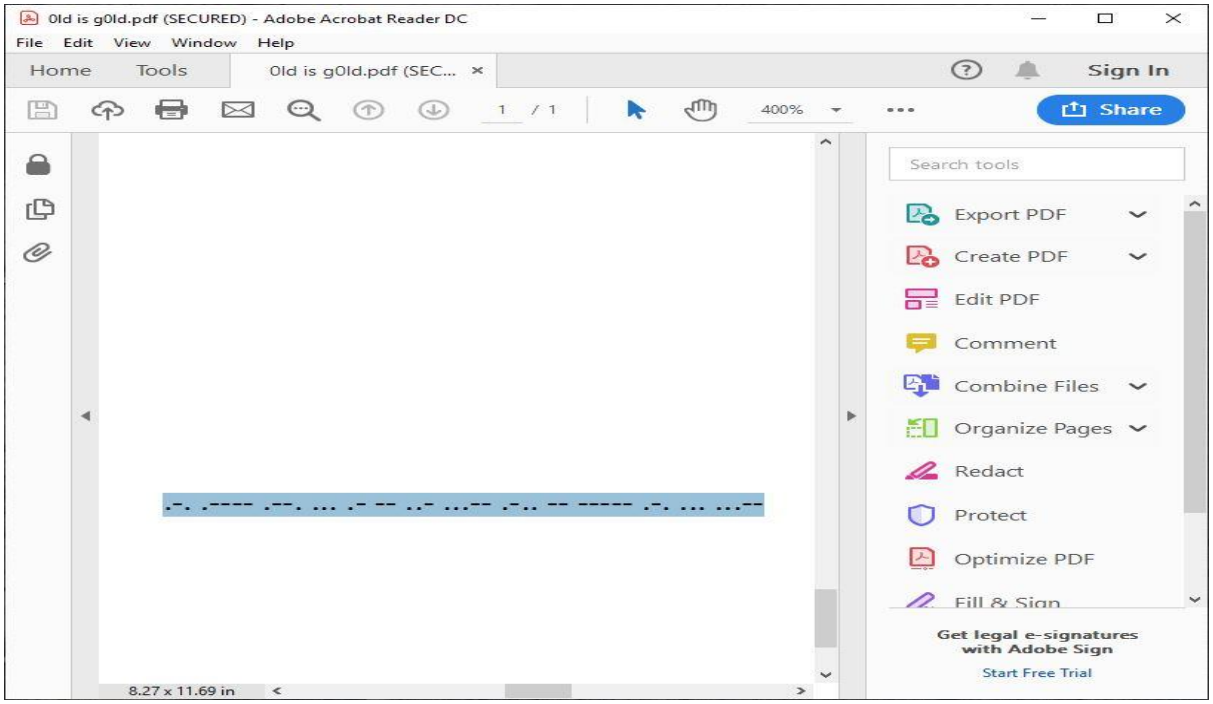


16.0 0ld_is_g0ld

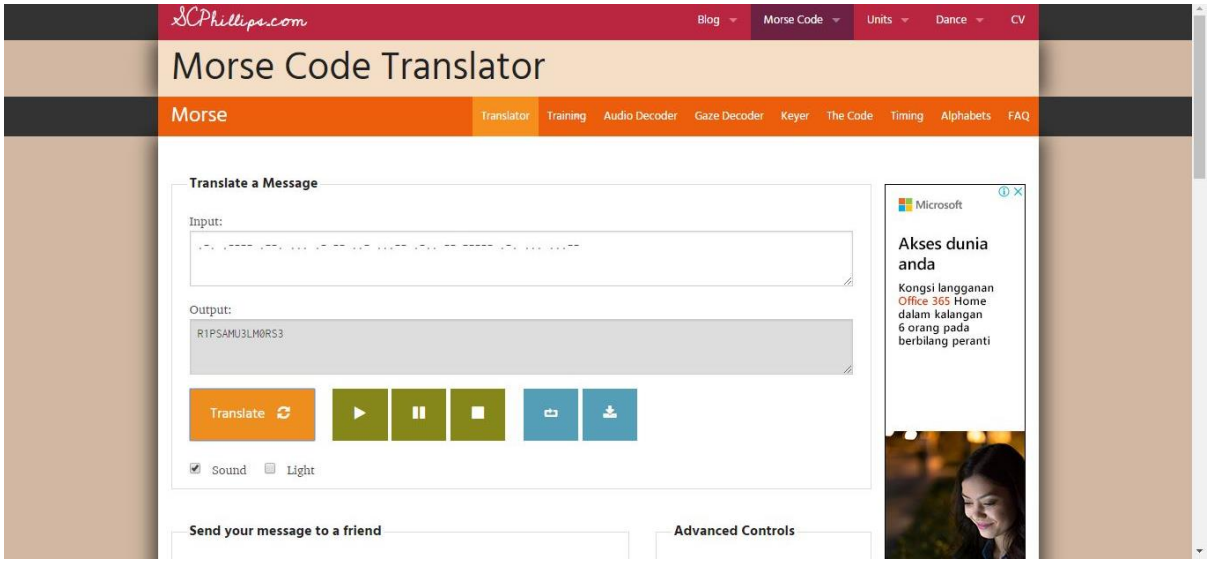
1. Extract it. It requires password to unlock pdf file. Use pdfcrack in kali and get password jumanji69.



2. Unlock the pdf then we can see tiny morse code on below.

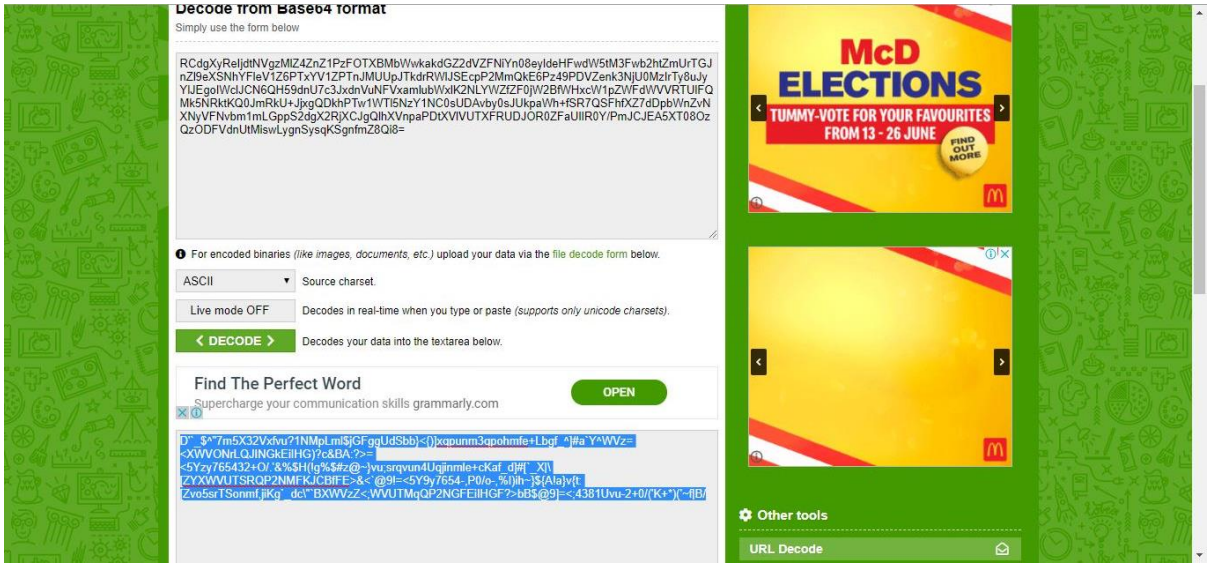


3. Decode the morse code. The flag is: ***HTB{R1PSAMU3LM0RS3}.***

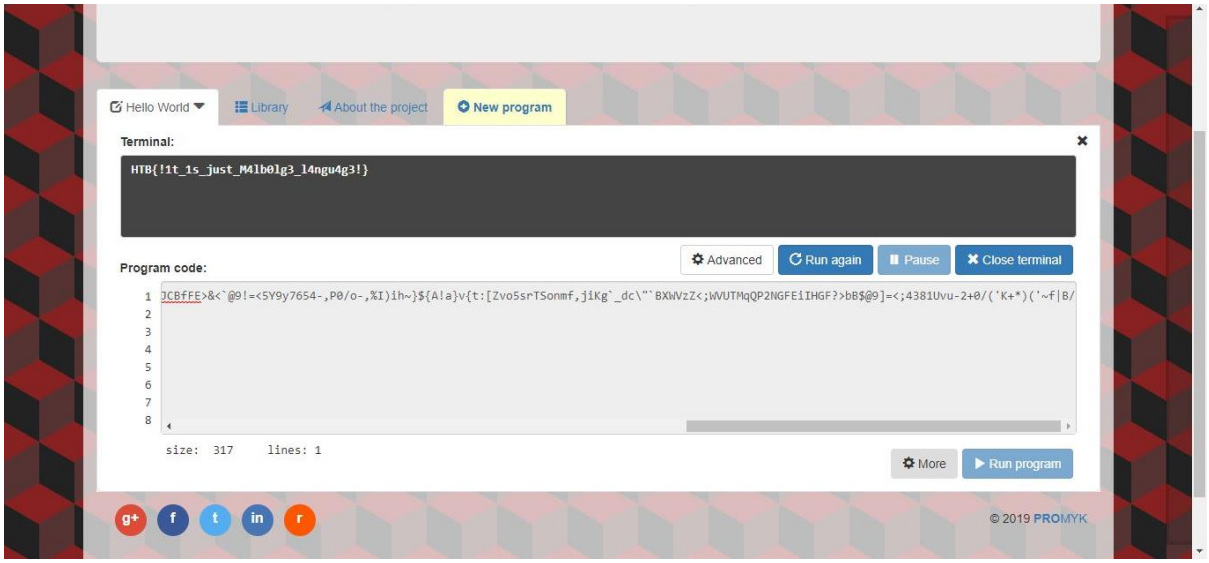


17.0 Inferno

1. Extract the content. Decode with base64.

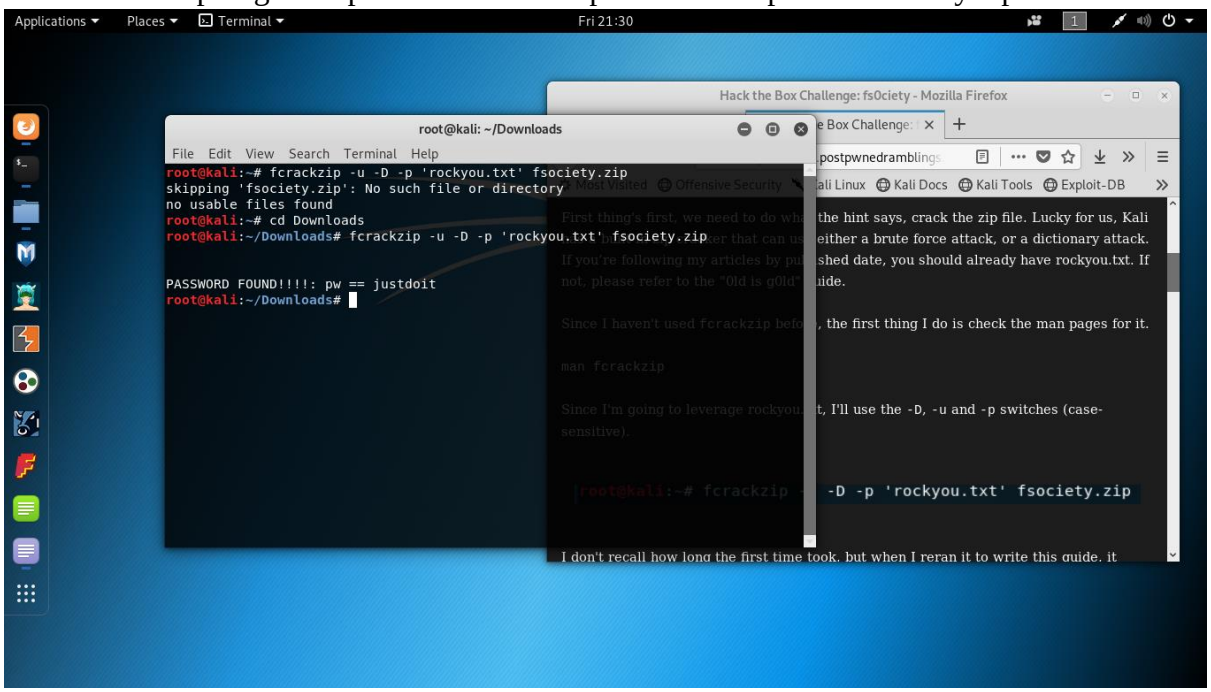


2. Decode again with Malbolge decoder. The flag is ***HTB{!1t_1s_just_M4lb0lg3_l4ngu4g3!}.***

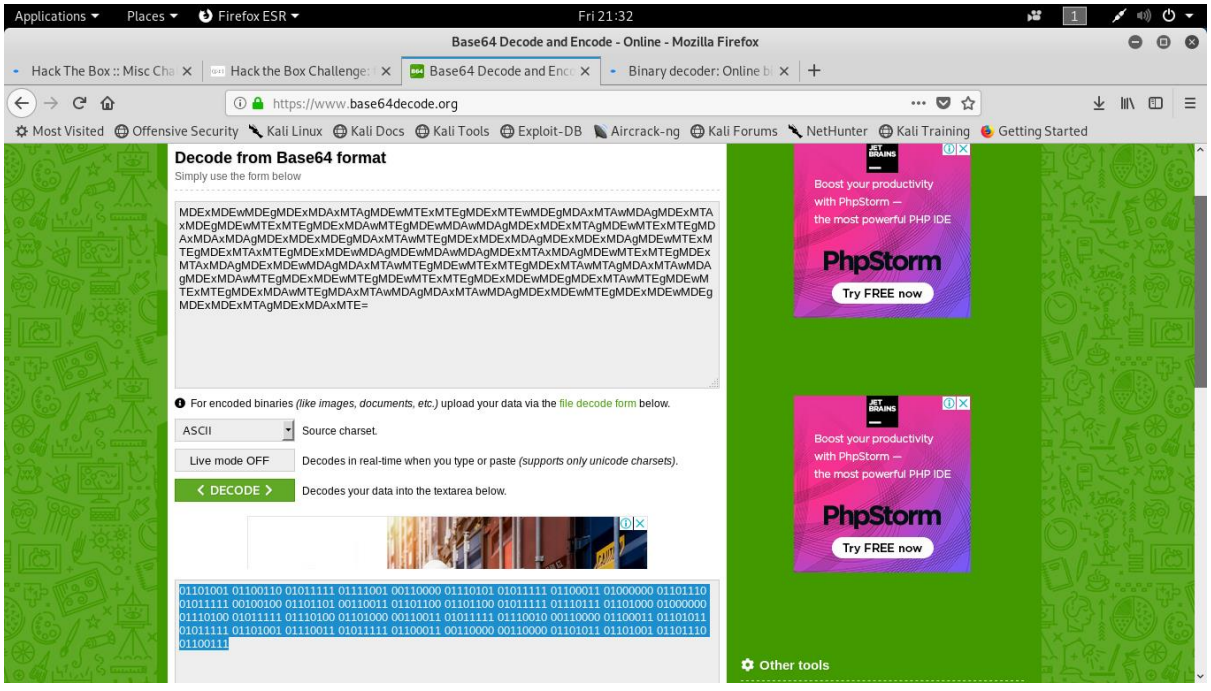


18.0 fs0ciety

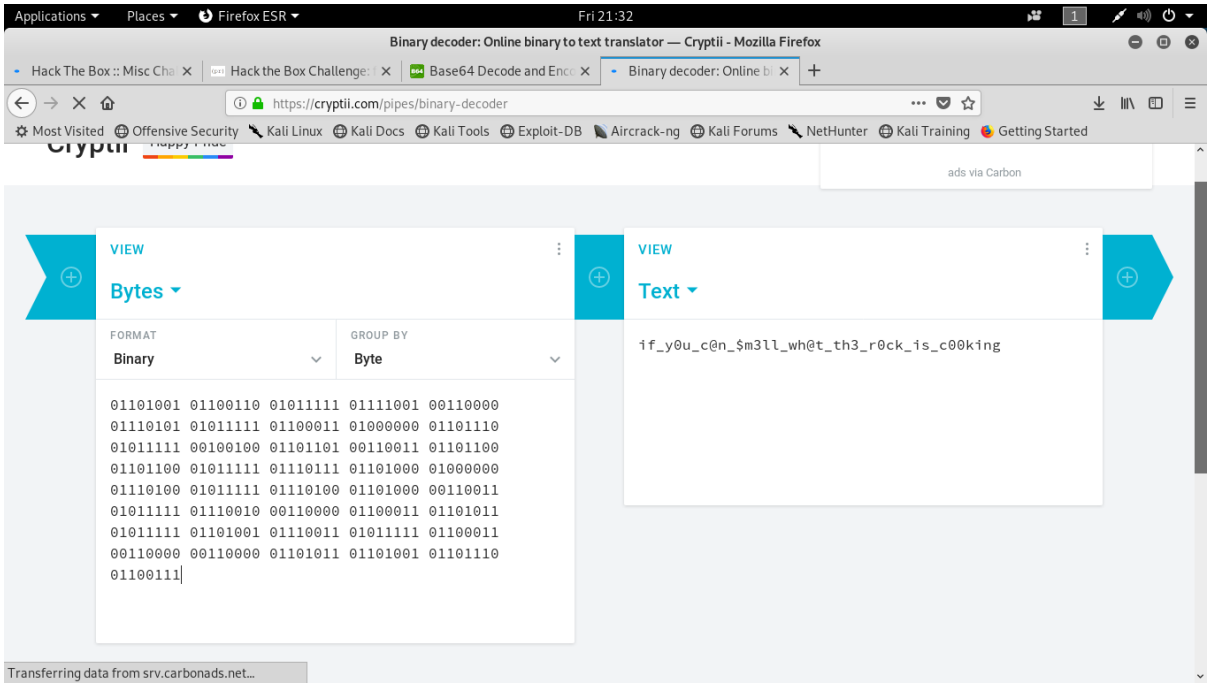
1. Use fcrackzip to get the password. Use the password to open the fsociety.zip



2. In the ssh text file, there is base64 encoded text. So, decode it. It shows all the binary number.



3. Use binary translate to text. The flag is: HTB{if_y0u_$m3ll_wh@t_th3_r0ck_is_c00king}

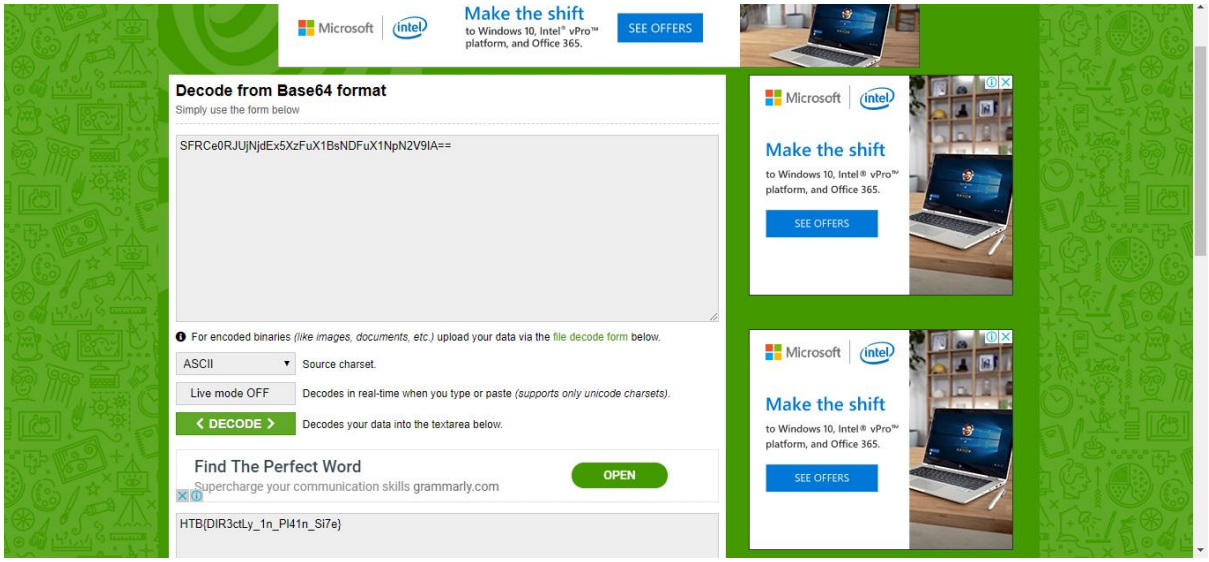


19. misDIRection

1. Download the file. Follow the number and arrange the folder accordingly.

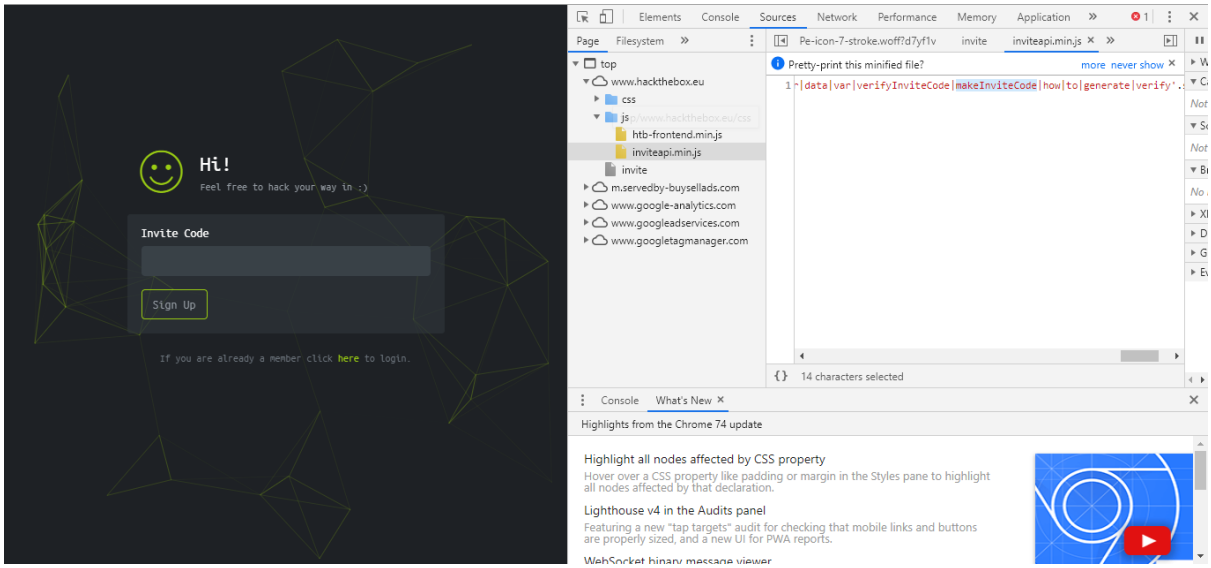
SFRCe0RJUjNjdEx5XzFuX1BsNDFuX1NpN2V9IA==

2. Decode by base64. The flag is: ***HTB{DIR3ctLy_1n_Pl41n_Si7e}***

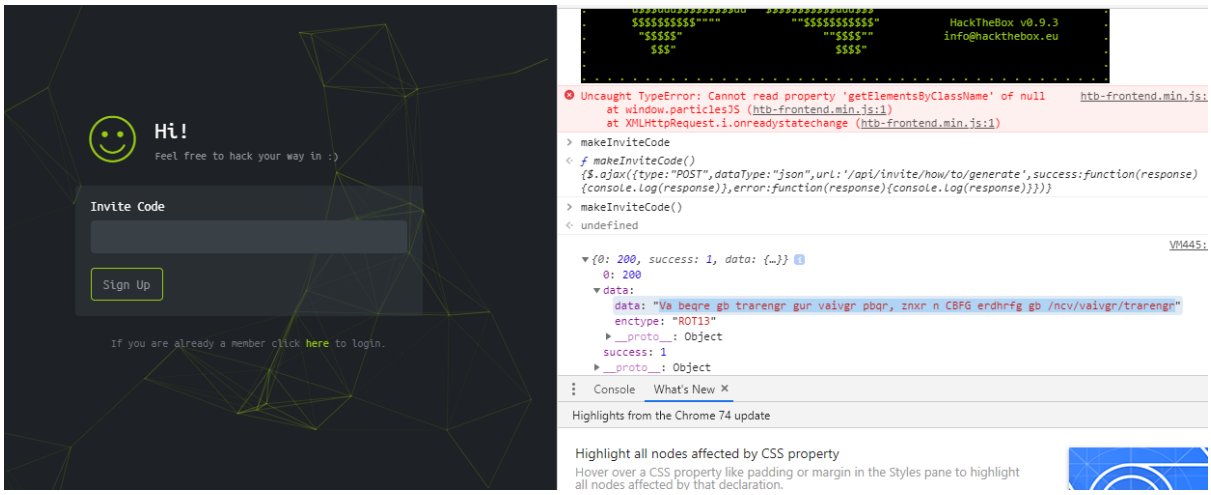


20.0 Hack for Invitation Code.

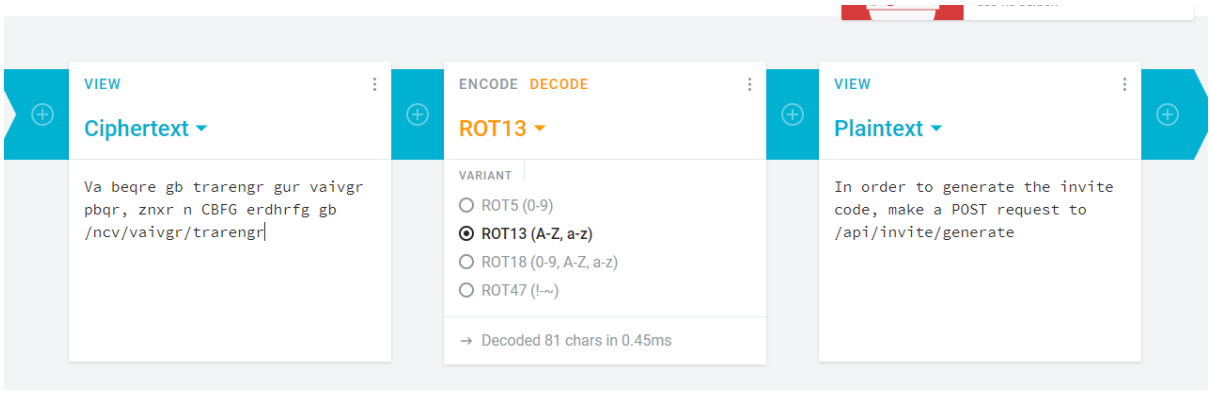
1. View the invite.js, we can see there is makeInviteCode.



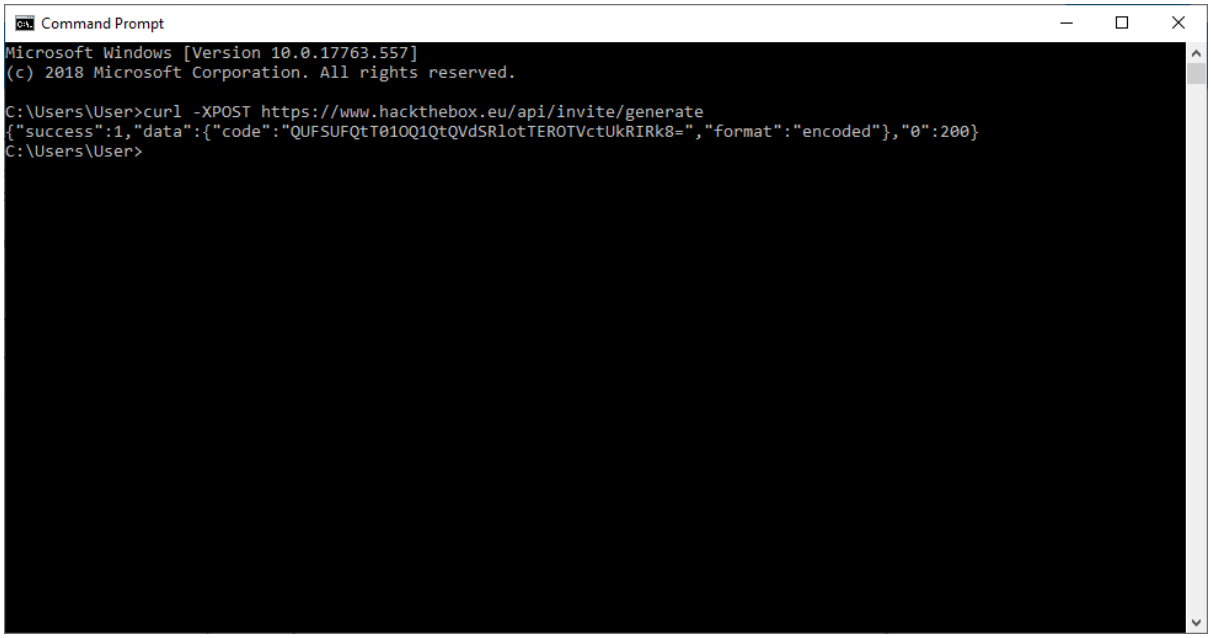
2. At the console, run makeInviteCode(). It will show a message with rot13 encoded.



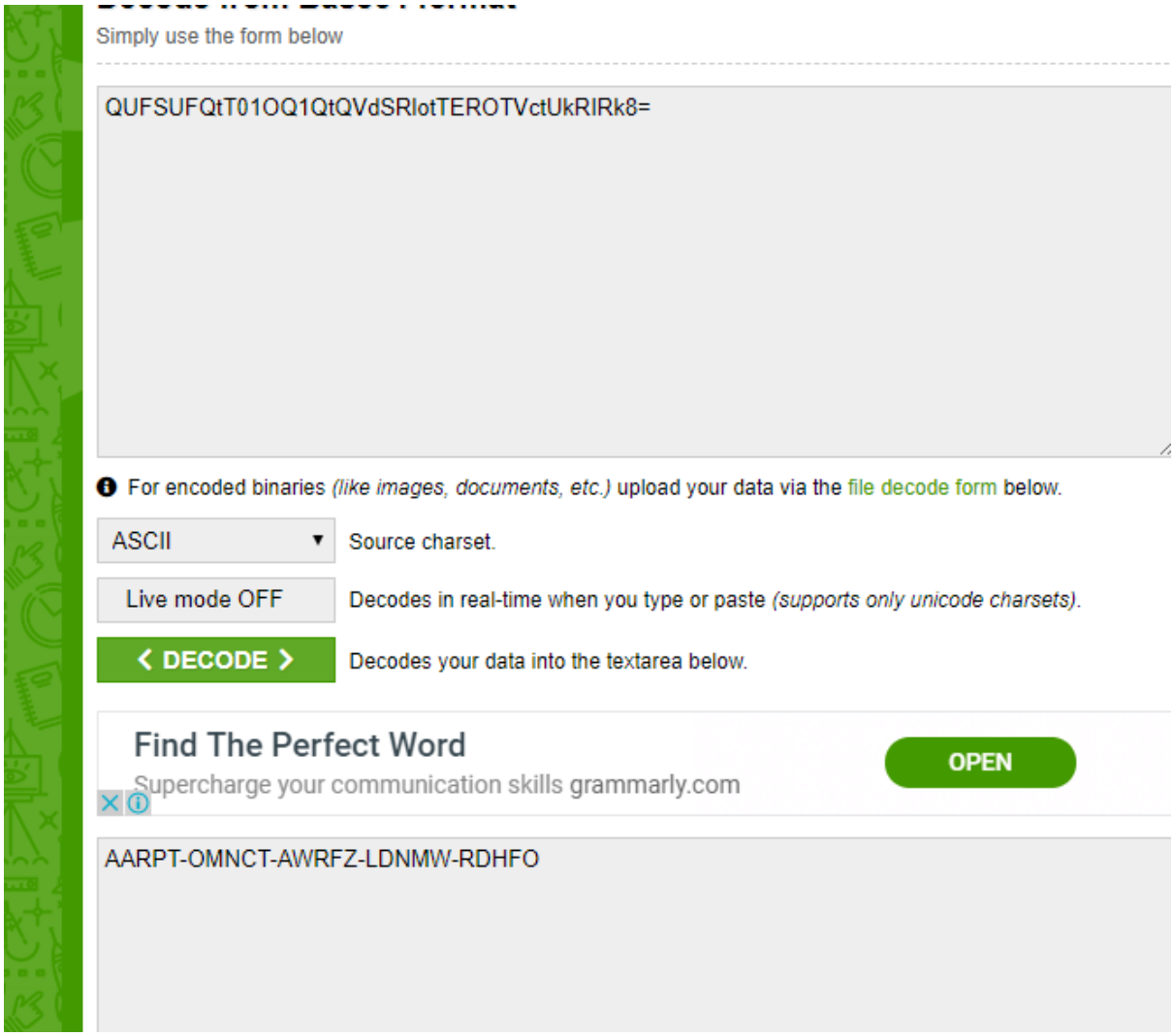
3. Decode and get the message.



4. Use terminal to make a POST request.



5. Decode the message and get the invitation code.



6. Successful.