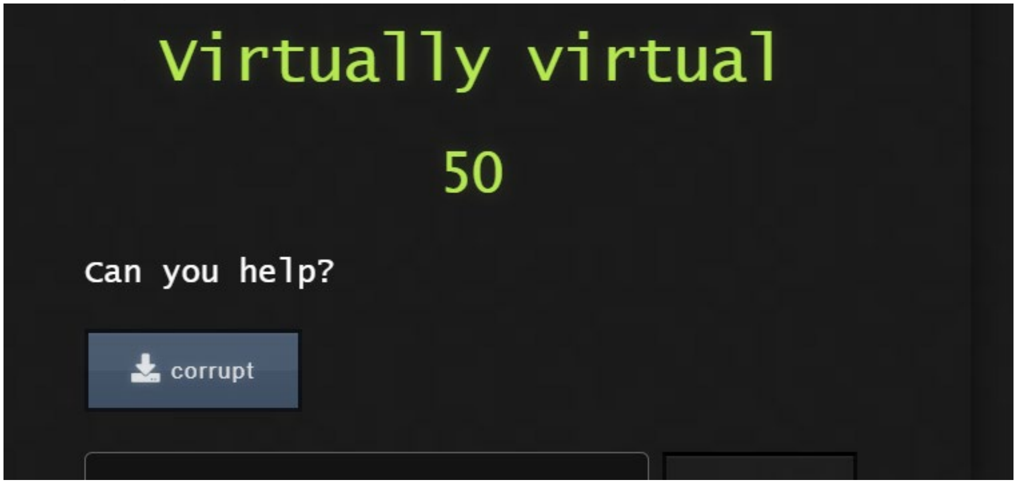
Nexa x MMU CTF 2022 Part2

Author : yialexlee / w9u0l1.l2lvi & My Packet Monkey teammate

***Reverse Engineering and Buffer Overflow Challenge is down by my teammate in this ctf part2**

Forensic

Virtually virtual

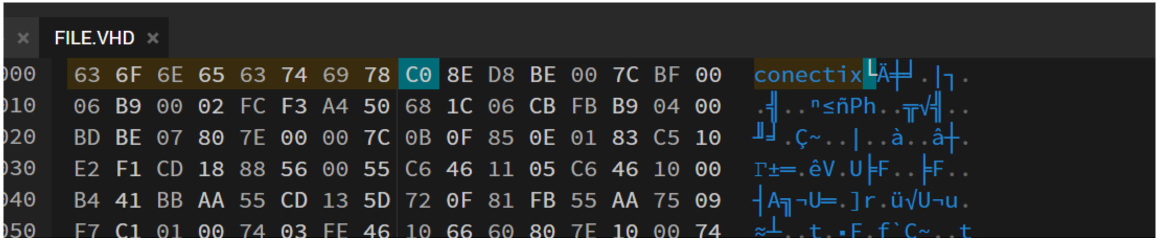


Virtually virtual

50

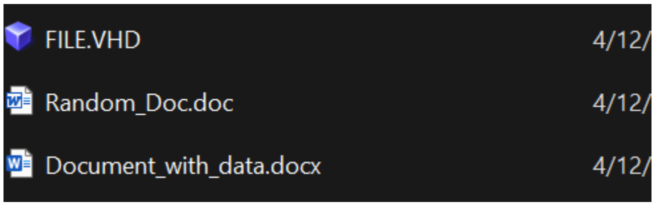
Can you help?

Download the file and change the magic header to VHD file



```
000  63 6F 6E 65 63 74 69 78 C0 8E D8 BE 00 7C BF 00  conectixLÄ╪.|┐.
010  06 B9 00 02 FC F3 A4 50 68 1C 06 CB FB B9 04 00  .╣..ⁿ≤ñPh..╥√╣..
020  BD BE 07 80 7E 00 00 7C 0B 0F 85 0E 01 83 C5 10  ╜╛.Ç~..|..à..â┼.
030  E2 F1 CD 18 88 56 00 55 C6 46 11 05 C6 46 10 00  Γ±═.êV.U╞F..╞F..
040  B4 41 BB AA 55 CD 13 5D 72 0F 81 FB 55 AA 75 09  ┤A╗¬U═.]r.ü√U¬u.
050  F7 C1 01 00 74 03 FE 46 10 66 60 80 7E 10 00 74  ≈┴..t.■F.f`Ç~..t
```

Save as .vhd

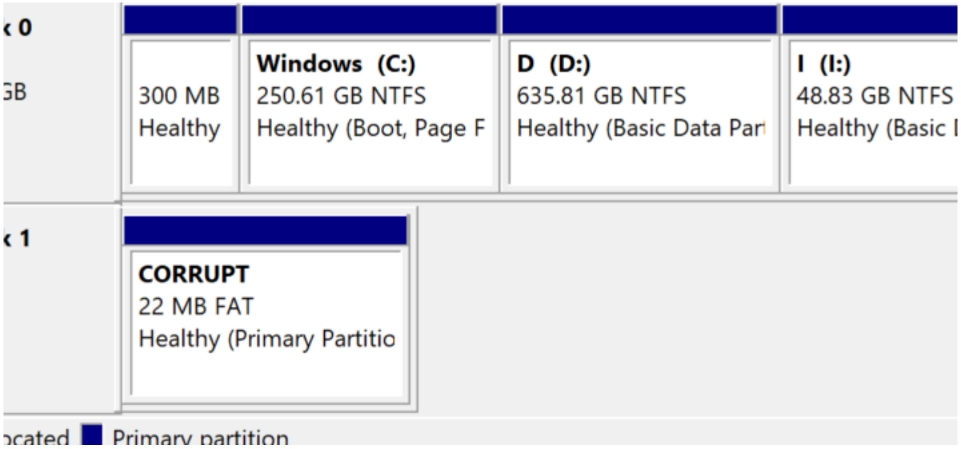


FILE.VHD 4/12/

Random_Doc.doc 4/12/

Document_with_data.docx 4/12/

Use Disk Management tool to open .vhd



k 0

GB

300 MB
Healthy

Windows (C:)
250.61 GB NTFS
Healthy (Boot, Page F

D (D:)
635.81 GB NTFS
Healthy (Basic Data Part

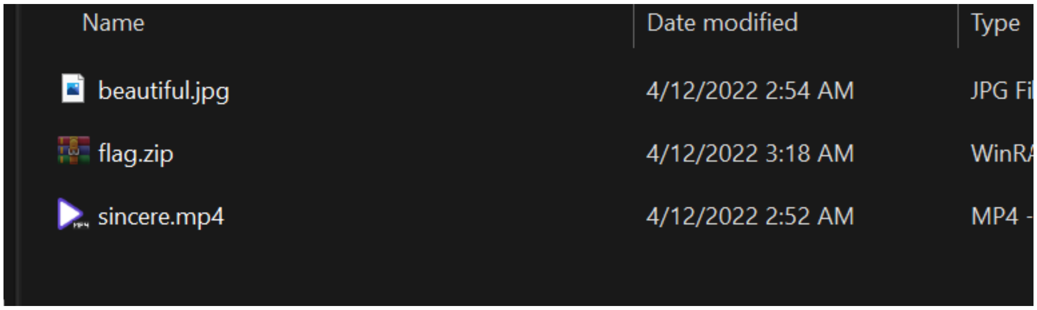
I (I:)
48.83 GB NTFS
Healthy (Basic I

k 1

CORRUPT
22 MB FAT
Healthy (Primary Partitio

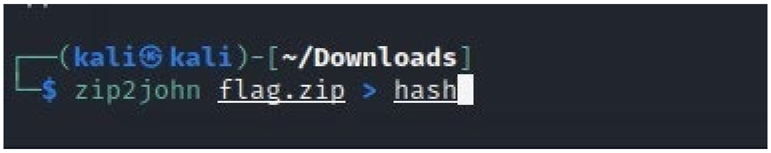
ocated ■ Primary partition

We can see 3 files inside

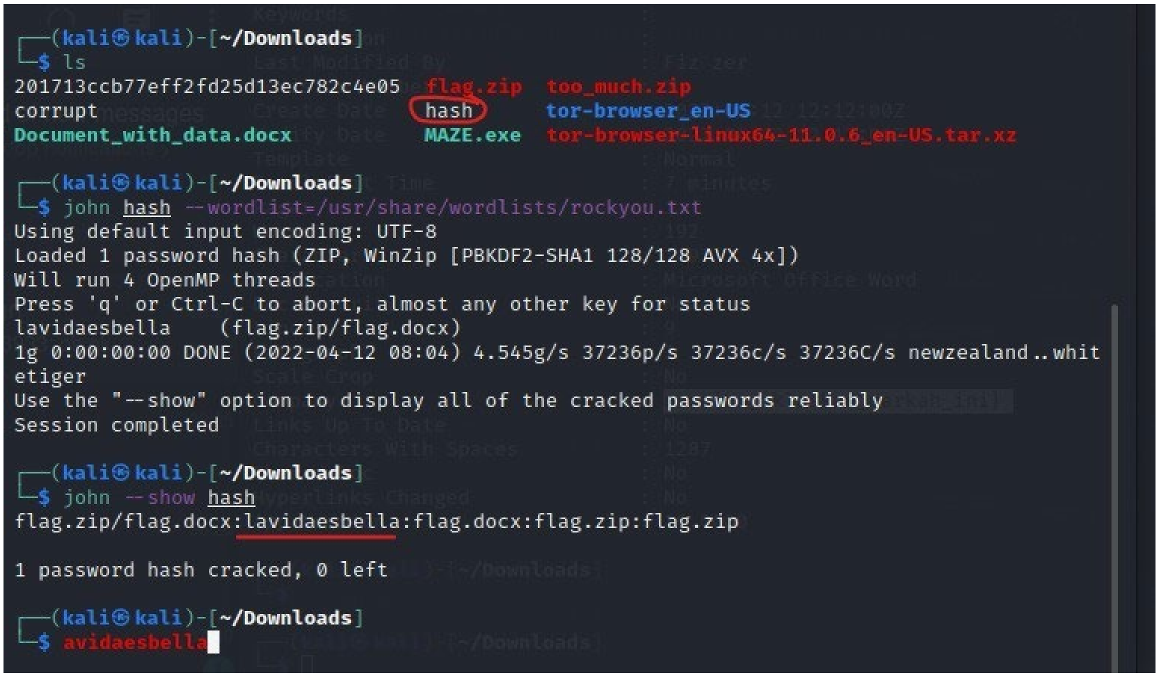


Name	Date modified	Type
beautiful.jpg	4/12/2022 2:54 AM	JPG Fi
flag.zip	4/12/2022 3:18 AM	WinRA
sincere.mp4	4/12/2022 2:52 AM	MP4 -

Send to flag.zip to kali vm and use johntheripper to crack the flag.zip

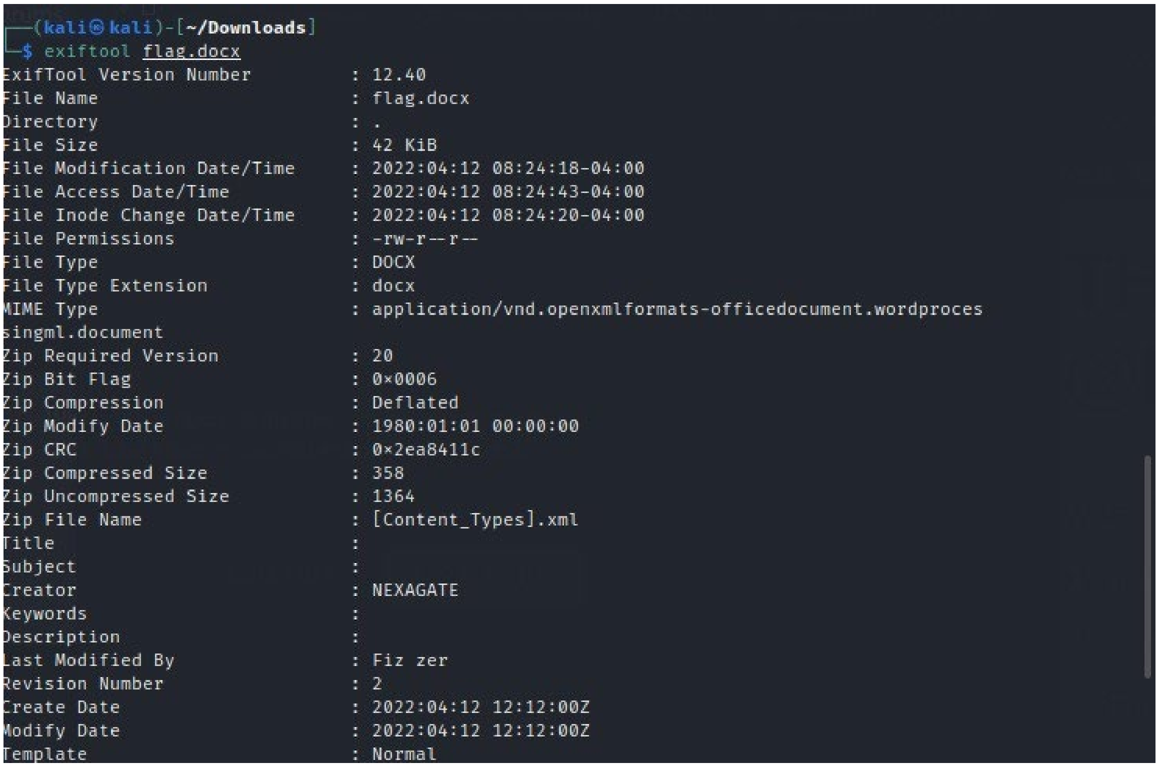


```
┌──(kali㉿kali)-[~/Downloads]
└─$ zip2john flag.zip > hash
```



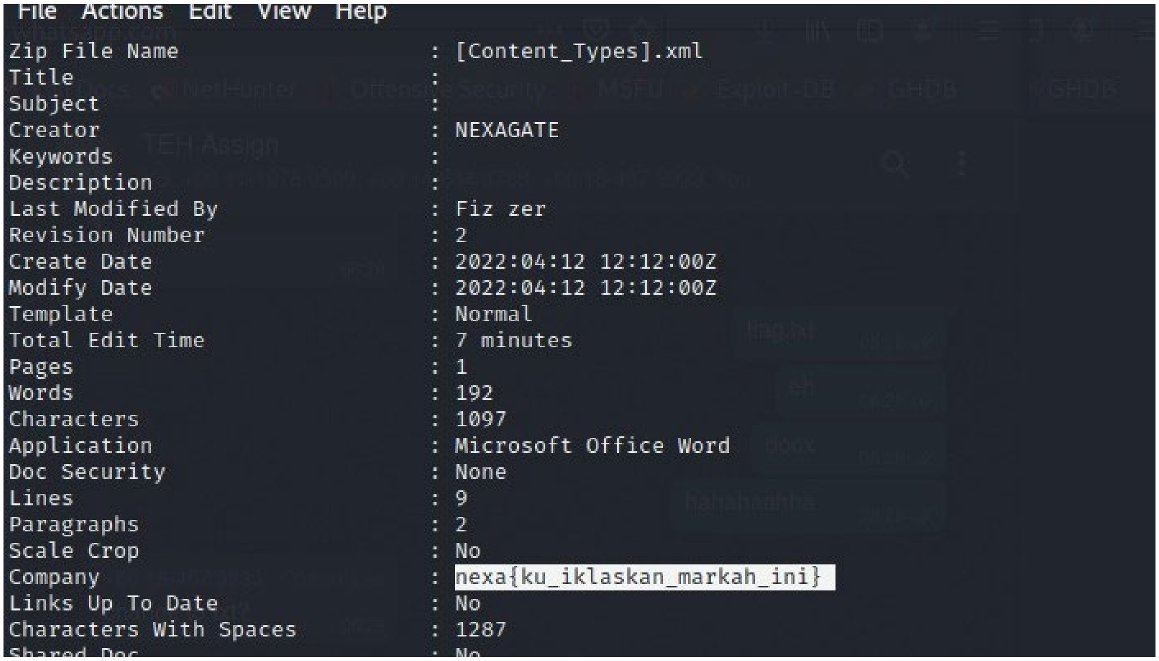
```
┌──(kali㉿kali)-[~/Downloads]
└─$ ls
201713ccb77eff2fd25d13ec782c4e05  flag.zip  too_much.zip
corrupt                           hash      tor-browser_en-US
Document_with_data.docx           MAZE.exe  tor-browser-linux64-11.0.6_en-US.tar.xz

┌──(kali㉿kali)-[~/Downloads]
└─$ john hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 128/128 AVX 4x])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
lavidaesbella    (flag.zip/flag.docx)
1g 0:00:00:00 DONE (2022-04-12 08:04) 4.545g/s 37236p/s 37236c/s 37236C/s newzealand..whit
etiger
Use the "--show" option to display all of the cracked passwords reliably
Session completed

┌──(kali㉿kali)-[~/Downloads]
└─$ john --show hash
flag.zip/flag.docx:lavidaesbella:flag.docx:flag.zip:flag.zip

1 password hash cracked, 0 left

┌──(kali㉿kali)-[~/Downloads]
└─$ avidaesbella
```

Extract with cracked password and use exiftool to open



```
┌──(kali㉿kali)-[~/Downloads]
└─$ exiftool flag.docx
ExifTool Version Number         : 12.40
File Name                       : flag.docx
Directory                       : .
File Size                       : 42 KiB
File Modification Date/Time     : 2022:04:12 08:24:18-04:00
File Access Date/Time           : 2022:04:12 08:24:43-04:00
File Inode Change Date/Time     : 2022:04:12 08:24:20-04:00
File Permissions                : -rw-r--r--
File Type                       : DOCX
File Type Extension             : docx
MIME Type                       : application/vnd.openxmlformats-officedocument.wordproces
singml.document
Zip Required Version            : 20
Zip Bit Flag                    : 0×0006
Zip Compression                 : Deflated
Zip Modify Date                 : 1980:01:01 00:00:00
Zip CRC                         : 0×2ea8411c
Zip Compressed Size             : 358
Zip Uncompressed Size           : 1364
Zip File Name                   : [Content_Types].xml
Title                           :
Subject                         :
Creator                         : NEXAGATE
Keywords                        :
Description                     :
Last Modified By                : Fiz zer
Revision Number                 : 2
Create Date                     : 2022:04:12 12:12:00Z
Modify Date                     : 2022:04:12 12:12:00Z
Template                        : Normal
```

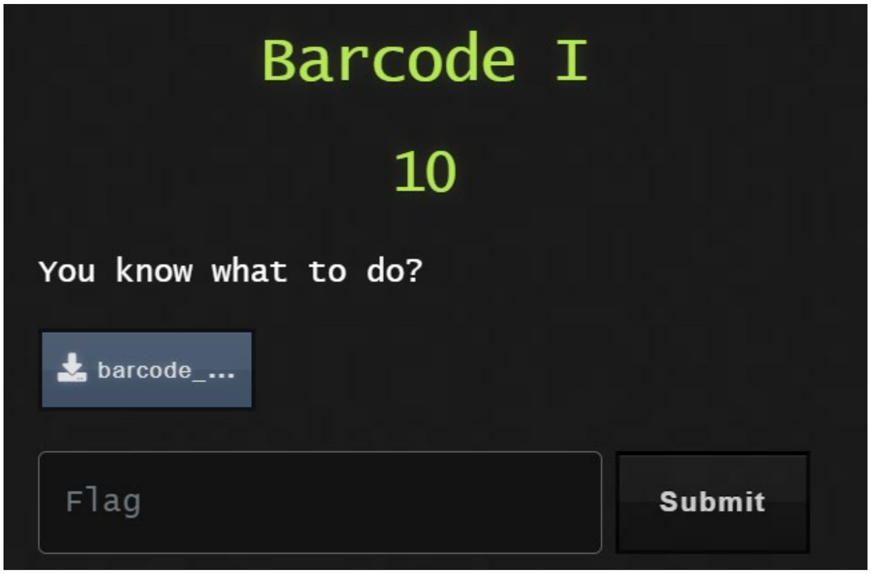
And we get the flag



```
Zip File Name                   : [Content_Types].xml
Title                           :
Subject                         :
Creator                         : NEXAGATE
Keywords                        :
Description                     :
Last Modified By                : Fiz zer
Revision Number                 : 2
Create Date                     : 2022:04:12 12:12:00Z
Modify Date                     : 2022:04:12 12:12:00Z
Template                        : Normal
Total Edit Time                 : 7 minutes
Pages                           : 1
Words                           : 192
Characters                      : 1097
Application                     : Microsoft Office Word
Doc Security                    : None
Lines                           : 9
Paragraphs                      : 2
Scale Crop                      : No
Company                         : nexa{ku_iklaskan_markah_ini}
Links Up To Date                : No
Characters With Spaces          : 1287
Shared Doc                      : No
```

Misc

Barcode I

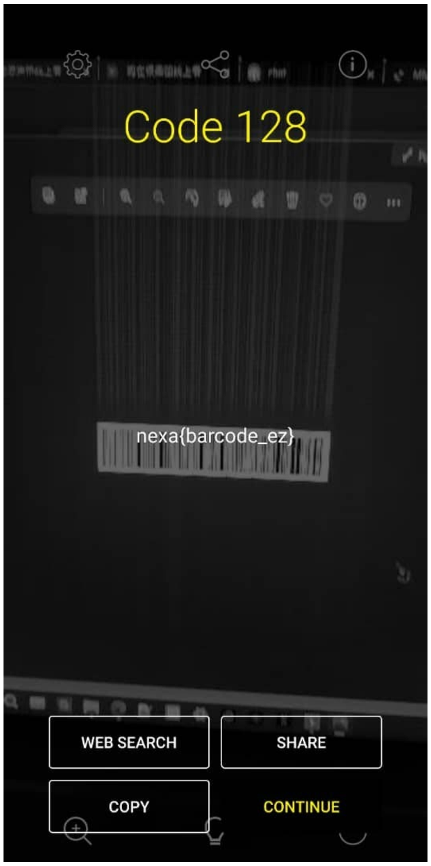


Barcode I

10

You know what to do?

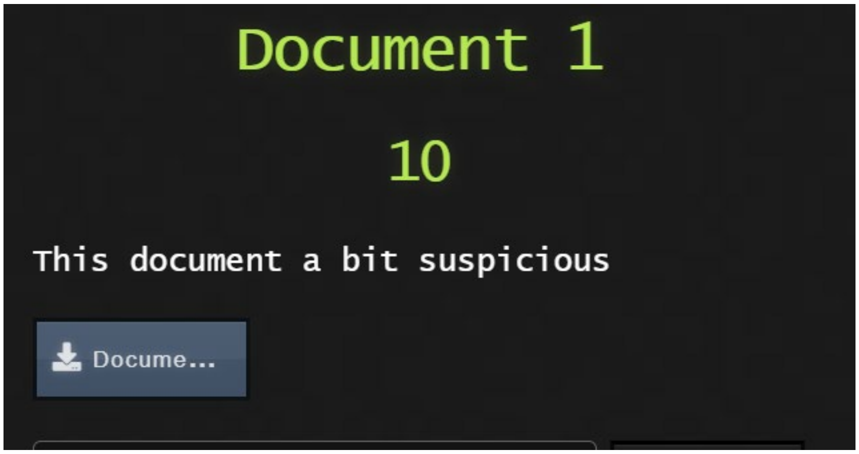
Use phone to scan barcode and get the flag



Code 128

nexa{barcode_ez}

Document I

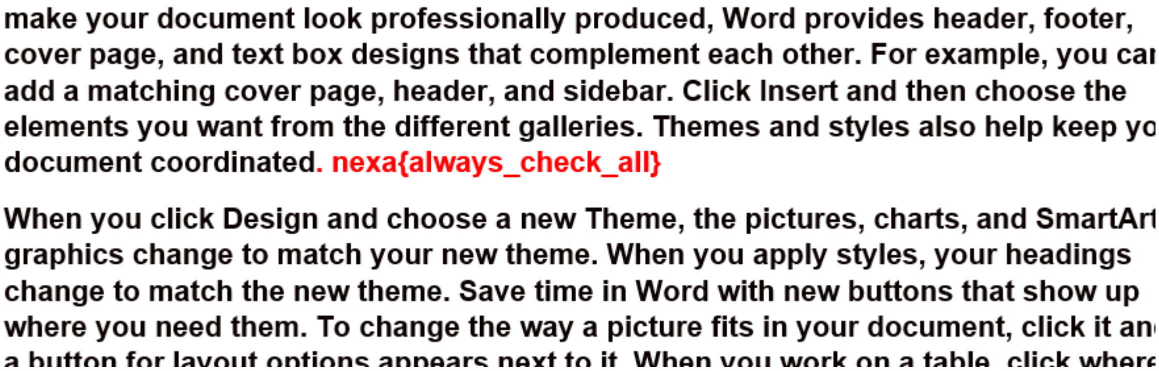


Document 1

10

This document a bit suspicious

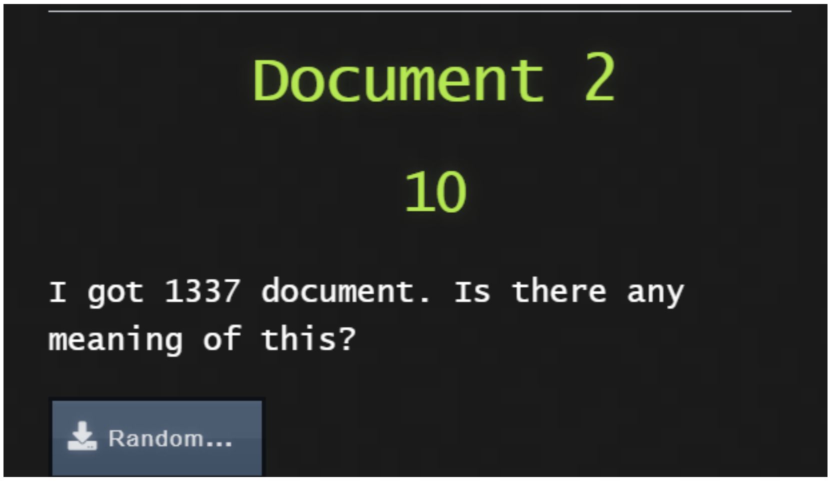
Open the file and ctrl+f search nexa and found, but the flag is hidden. Change to color to see the flag



make your document look professionally produced, Word provides header, footer, cover page, and text box designs that complement each other. For example, you car add a matching cover page, header, and sidebar. Click Insert and then choose the elements you want from the different galleries. Themes and styles also help keep yo document coordinated. nexa{always_check_all}

When you click Design and choose a new Theme, the pictures, charts, and SmartArt graphics change to match your new theme. When you apply styles, your headings change to match the new theme. Save time in Word with new buttons that show up where you need them. To change the way a picture fits in your document, click it an a button for layout options appears next to it. When you work on a table, click where

Document II

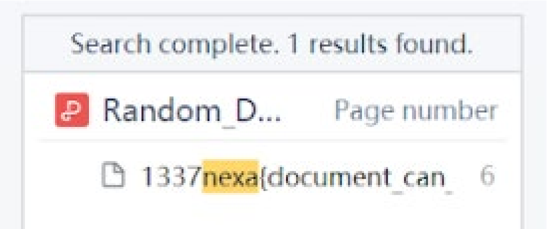


Document 2

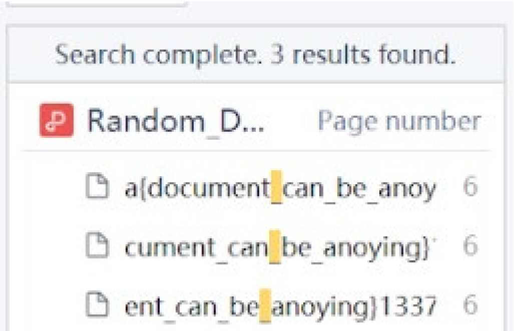
10

I got 1337 document. Is there any meaning of this?

Use WPS Office to open and search for nexa like DocumentI and found. But it is nexa no flag, so search _ for the flag after nexa. And combine them

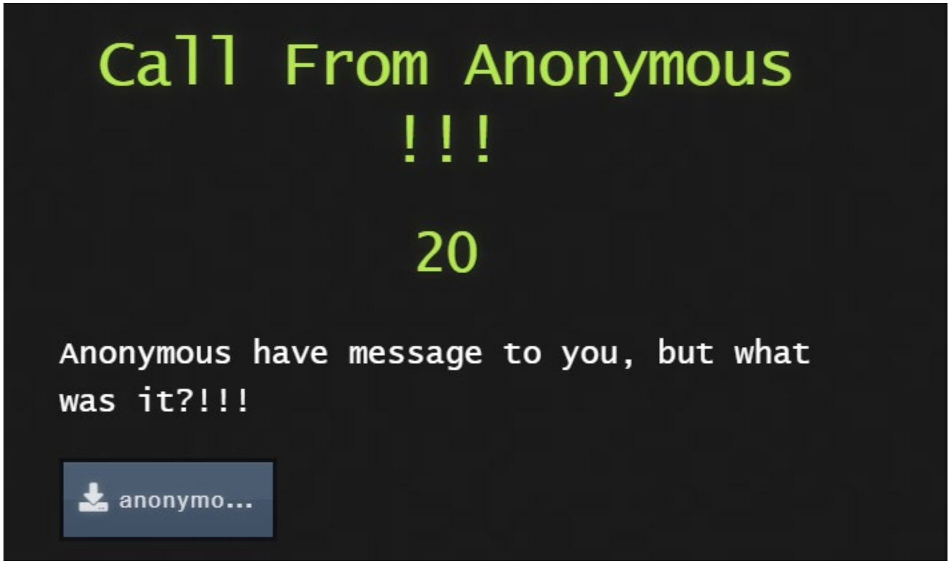


```
Search complete. 1 results found.
Random_D...          Page number
    1337nexa{document_can_    6
```



```
Search complete. 3 results found.
Random_D...          Page number
    a{document_can_be_anoy      6
    cument_can_be_anoying}'     6
    ent_can_be_anoying}1337     6
```

Call From Anonymous !!!

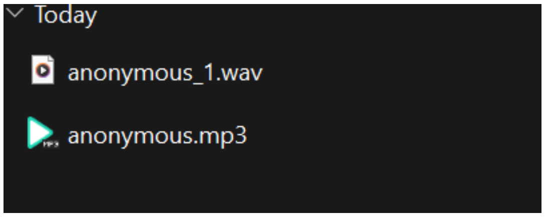


Call From Anonymous !!!

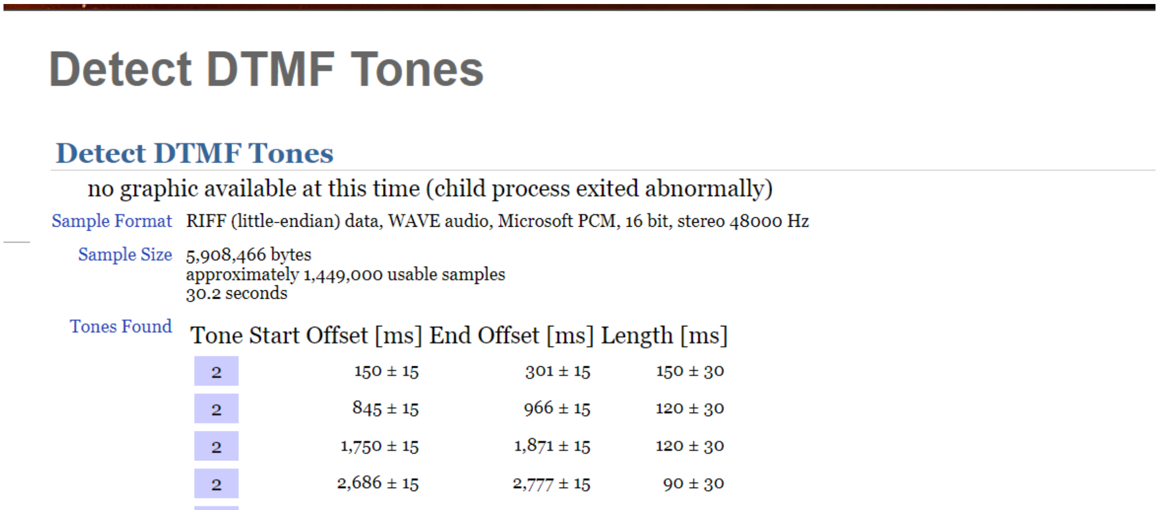
20

Anonymous have message to you, but what was it?!!!

Save the file as wav(cut the front and back)



Use DTMF Tones decode tool to decode



Detect DTMF Tones

Detect DTMF Tones

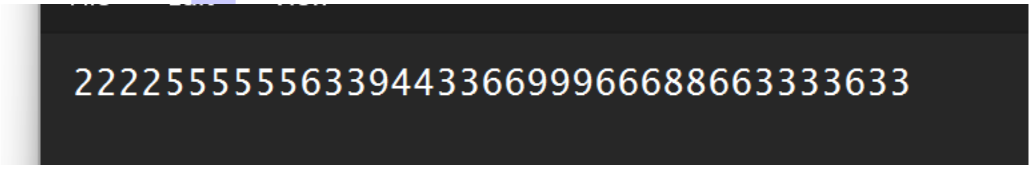
no graphic available at this time (child process exited abnormally)

Sample Format RIFF (little-endian) data, WAVE audio, Microsoft PCM, 16 bit, stereo 48000 Hz

Sample Size 5,908,466 bytes
approximately 1,449,000 usable samples
30.2 seconds

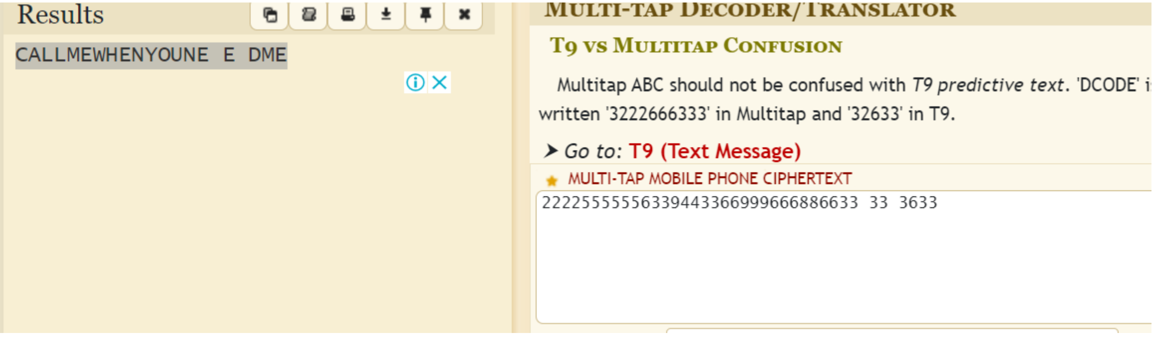
Tones Found

Tone	Start Offset [ms]	End Offset [ms]	Length [ms]
2	150 ± 15	301 ± 15	150 ± 30
2	845 ± 15	966 ± 15	120 ± 30
2	1,750 ± 15	1,871 ± 15	120 ± 30
2	2,686 ± 15	2,777 ± 15	90 ± 30



```
2222555555633944336699966688663333633
```

Decode the number we get and seperrate the 3 at the back, we get the flag.



CALLMEWHENYOUNE E DME

T9 vs Multitap Confusion

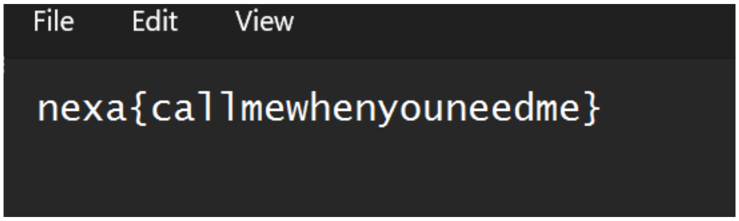
Multitap ABC should not be confused with *T9 predictive text*. 'DCODE' i written '3222666333' in Multitap and '32633' in T9.

➤ *Go to:* T9 (Text Message)

★ MULTI-TAP MOBILE PHONE CIPHERTEXT

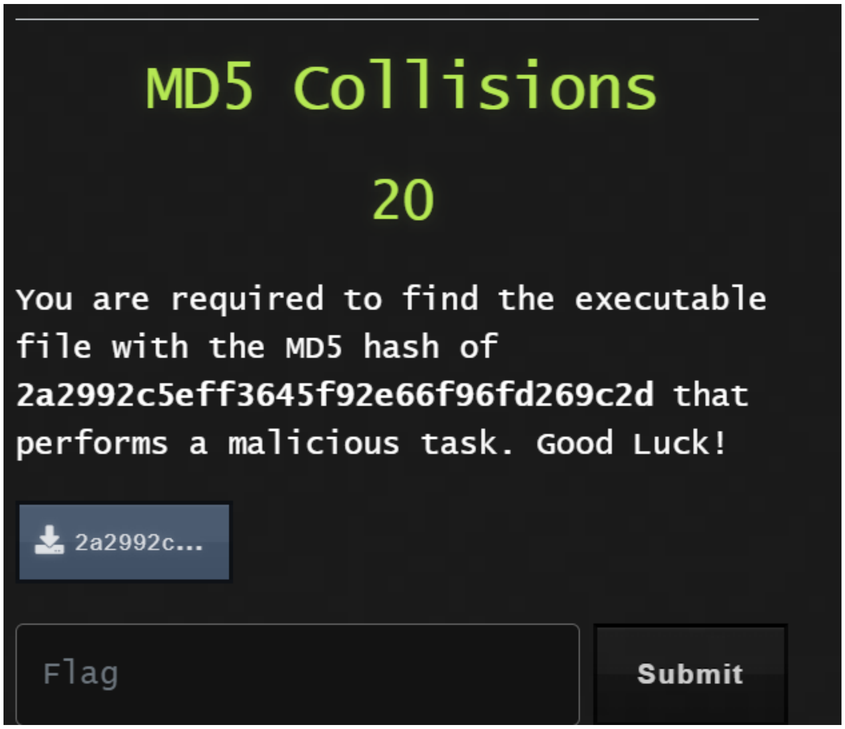
```
22225555556339443366999666886633 33 3633
```

Make the flag lower case



```
nexa{callmewhenyouneedme}
```

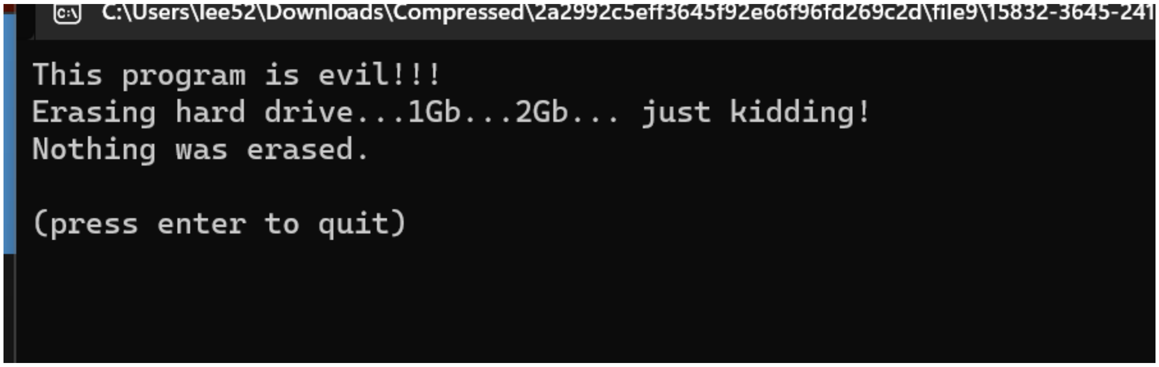
MD5 Collisions


MD5 Collisions

20

You are required to find the executable file with the MD5 hash of 2a2992c5eff3645f92e66f96fd269c2d that performs a malicious task. Good Luck!

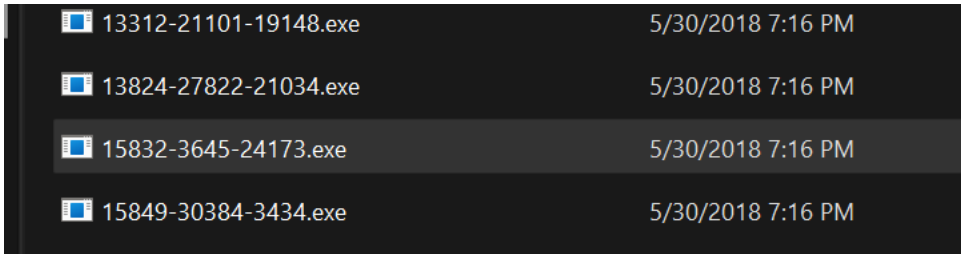
Extract the zip file and one of the exe file out put is difference.



C:\Users\lee52\Downloads\Compressed\2a2992c5eff3645f92e66f96fd269c2d\file9\15832-3645-241

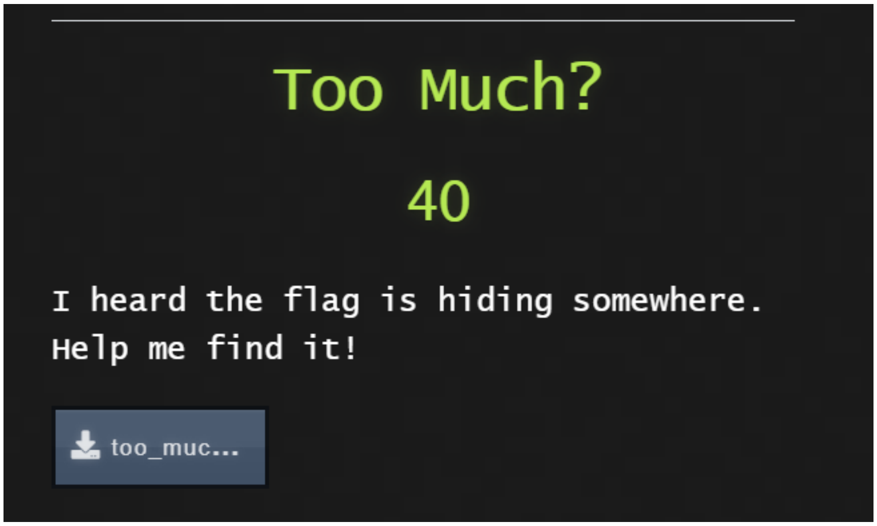
```
This program is evil!!!
Erasing hard drive...1Gb...2Gb... just kidding!
Nothing was erased.

(press enter to quit)
```

Use the file name as flag



```
13312-21101-19148.exe          5/30/2018 7:16 PM
13824-27822-21034.exe          5/30/2018 7:16 PM
15832-3645-24173.exe           5/30/2018 7:16 PM
15849-30384-3434.exe           5/30/2018 7:16 PM
```

Too Much?

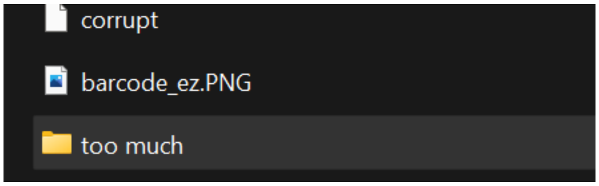


Too Much?

40

I heard the flag is hiding somewhere. Help me find it!

Download the zip file, extract it

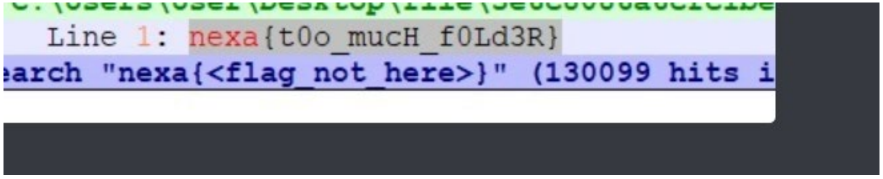


corrupt

barcode_ez.PNG

too much

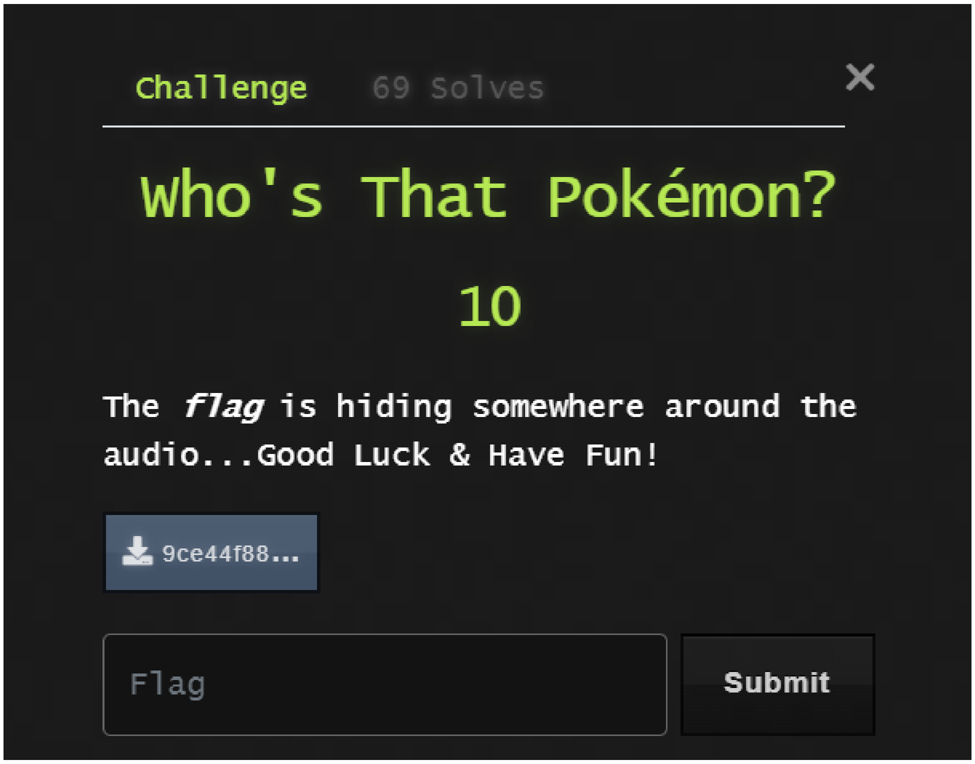
Use Notepad++ to search nexa in folder and we found the flag



```
  Line 1: nexa{t0o_mucH_f0Ld3R}
earch "nexa{<flag_not_here>}" (130099 hits i
```

Stego

Who's That Pokémon?



Challenge 69 Solves

Who's That Pokémon?

10

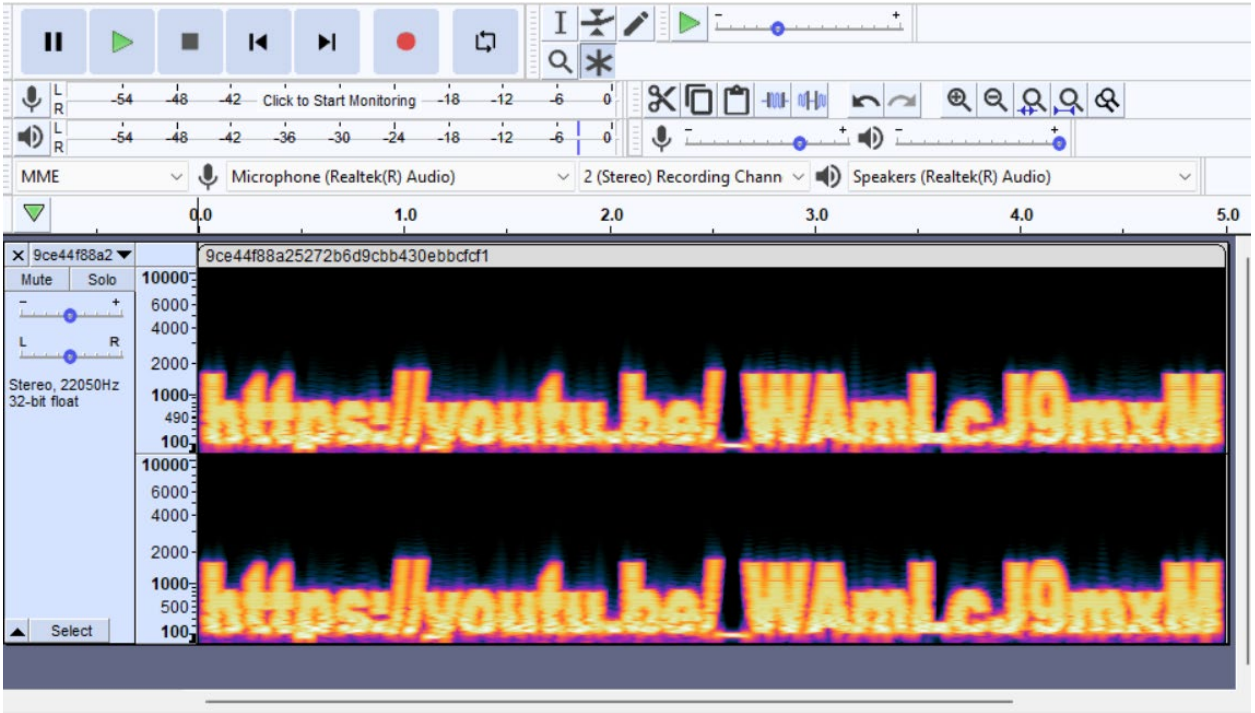
The *flag* is hiding somewhere around the audio...Good Luck & Have Fun!

9ce44f88...

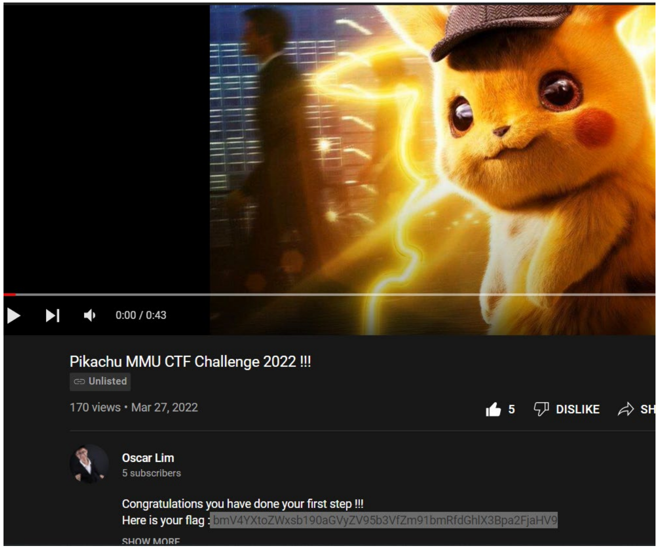
Flag

Submit

Download the audio file given. Open the audio file with an audio editor application. Then change the view from waveform to spectrogram. A link is shown.


Click to Start Monitoring
MME
Microphone (Realtek(R) Audio)
2 (Stereo) Recording Chann
Speakers (Realtek(R) Audio)
0.0
1.0
2.0
3.0
4.0
5.0
9ce44f88a2
Mute
Solo
Stereo, 22050Hz
32-bit float
Select
9ce44f88a25272b6d9cbb430ebbcfcf1
10000
6000
4000
2000
1000
490
500
100
https://youtu.be/_WAmLcJ9mxM

Browse the link and the encoded flag is given in the description box of the youtube videos.



Pikachu MMU CTF Challenge 2022 !!!

Unlisted

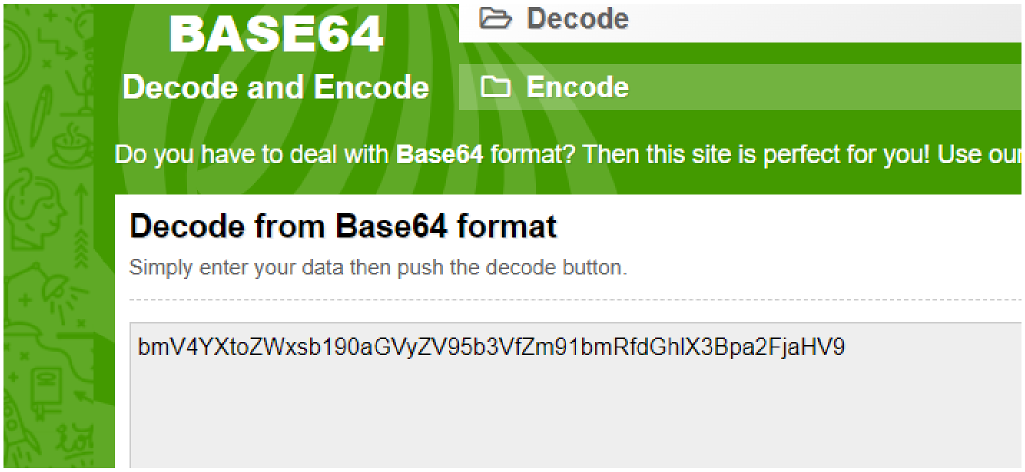
170 views • Mar 27, 2022

Oscar Lim
5 subscribers

Congratulations you have done your first step !!!
Here is your flag : bmV4YXtoZWxsb190aGVyZV95b3VfZm91bmRfdGhlX3Bpa2FjaHV9

SHOW MORE

Decode the Base64 format flag to text and the plain text flag was found.



Do you have to deal with **Base64** format? Then this site is perfect for you! Use our

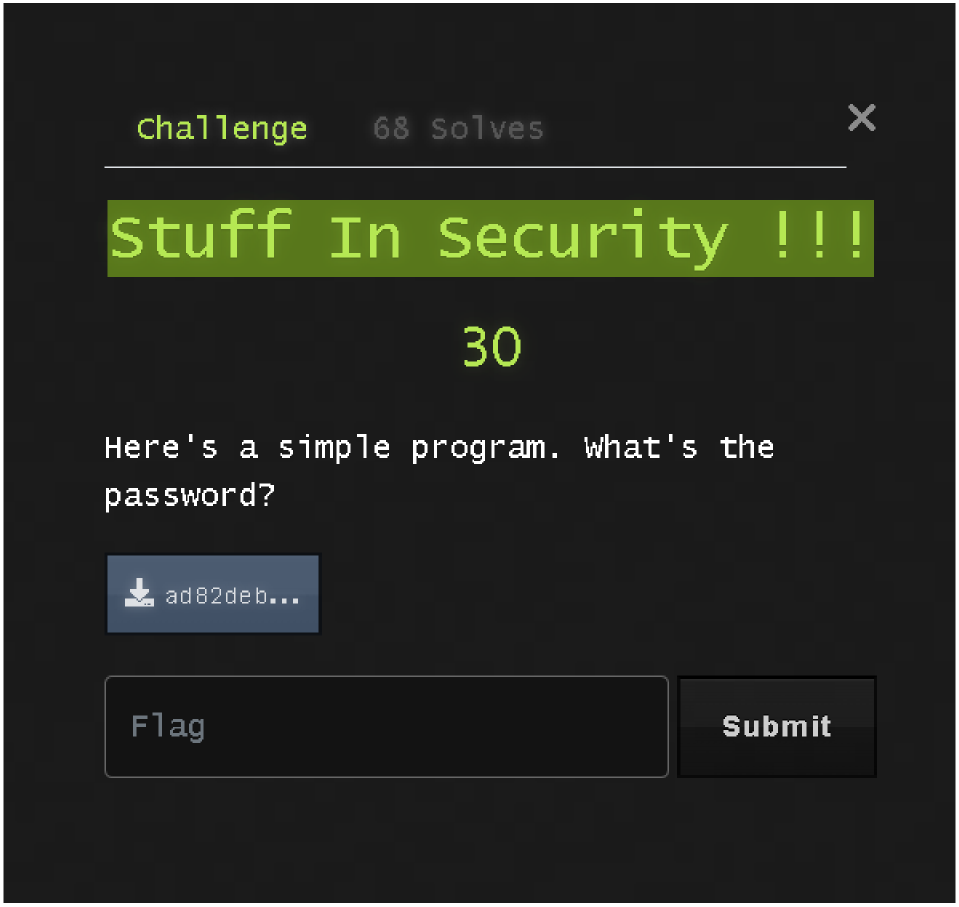
Decode from Base64 format

Simply enter your data then push the decode button.

bmV4YXtoZWxsb190aGVyZV95b3VfZm91bmRfdGhlX3Bpa2FjaHV9

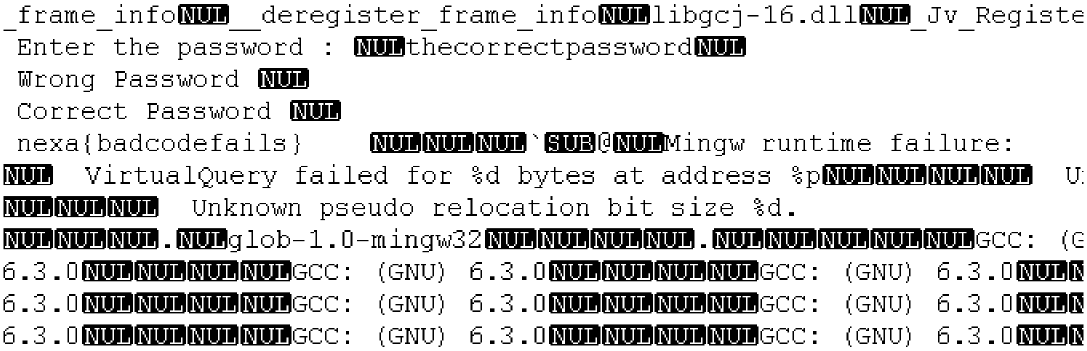
Buffer Overflows

Stuff In Security !!!



Here's a simple program. What's the password?

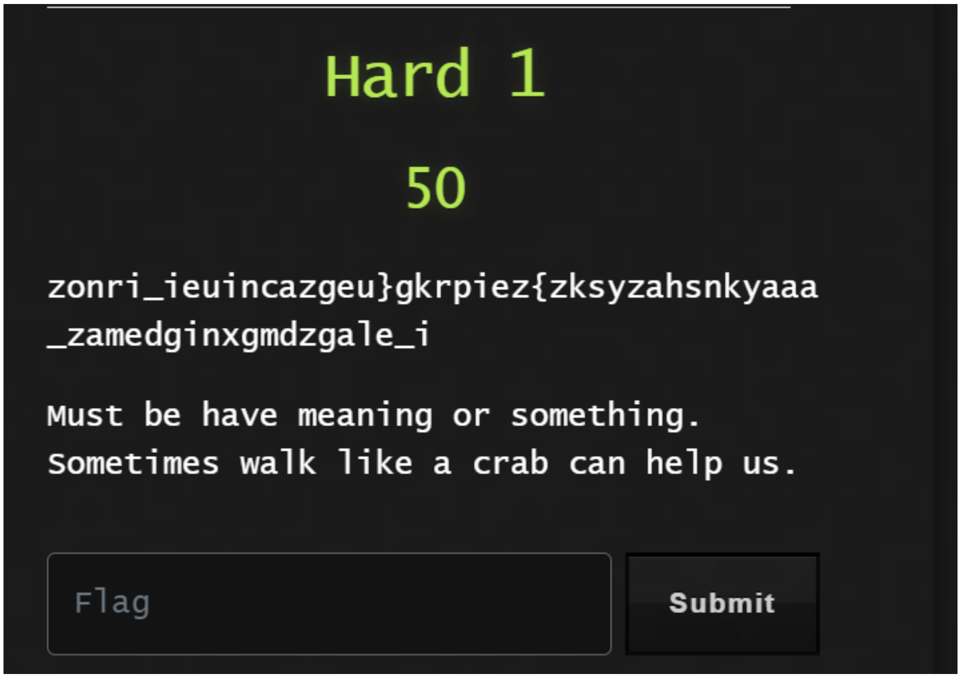
First, download the .exe. Open with Notepad++ and found the flag.



```
_frame_infoNUL__deregister_frame_infoNULlibgcj-16.dllNUL_Jv_Registe
 Enter the password : NULthecorrectpasswordNUL
 Wrong Password NUL
 Correct Password NUL
 nexa{badcodefails}    NULNULNUL`SUB@NULMingw runtime failure:
NUL  VirtualQuery failed for %d bytes at address %pNULNULNULNUL  U:
NULNULNUL  Unknown pseudo relocation bit size %d.
NULNULNUL.NULglob-1.0-mingw32NULNULNULNUL.NULNULNULNULNULGCC: (G
6.3.0NULNULNULNULGCC: (GNU) 6.3.0NULNULNULNULGCC: (GNU) 6.3.0NULN
6.3.0NULNULNULNULGCC: (GNU) 6.3.0NULNULNULNULGCC: (GNU) 6.3.0NULN
6.3.0NULNULNULNULGCC: (GNU) 6.3.0NULNULNULNULGCC: (GNU) 6.3.0NULN
```

Cryptography

Hard 1



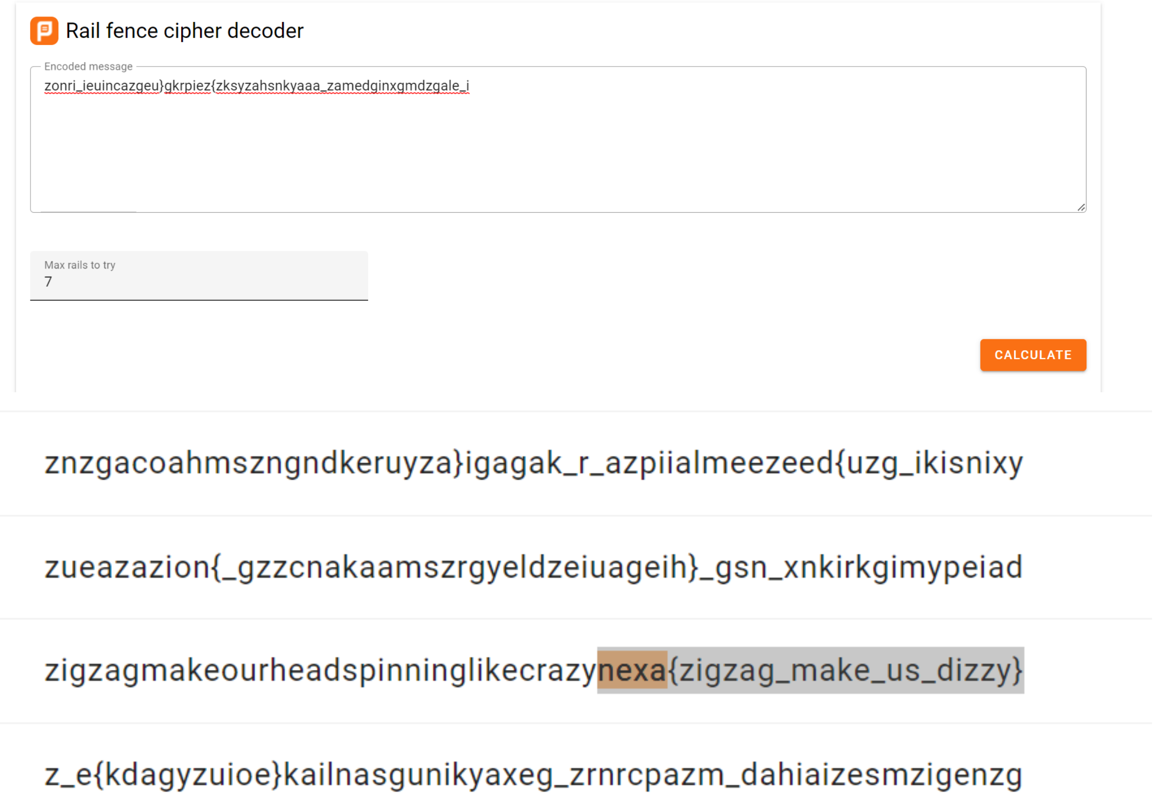
Hard 1

50

zonri_ieuincazgeu}gkrpiez{zksyzahsnkyaaa_zamedginxgmdzgale_i

Must be have meaning or something. Sometimes walk like a crab can help us.

Use rail frence decoder to decode, tried many times finally found flag in max7



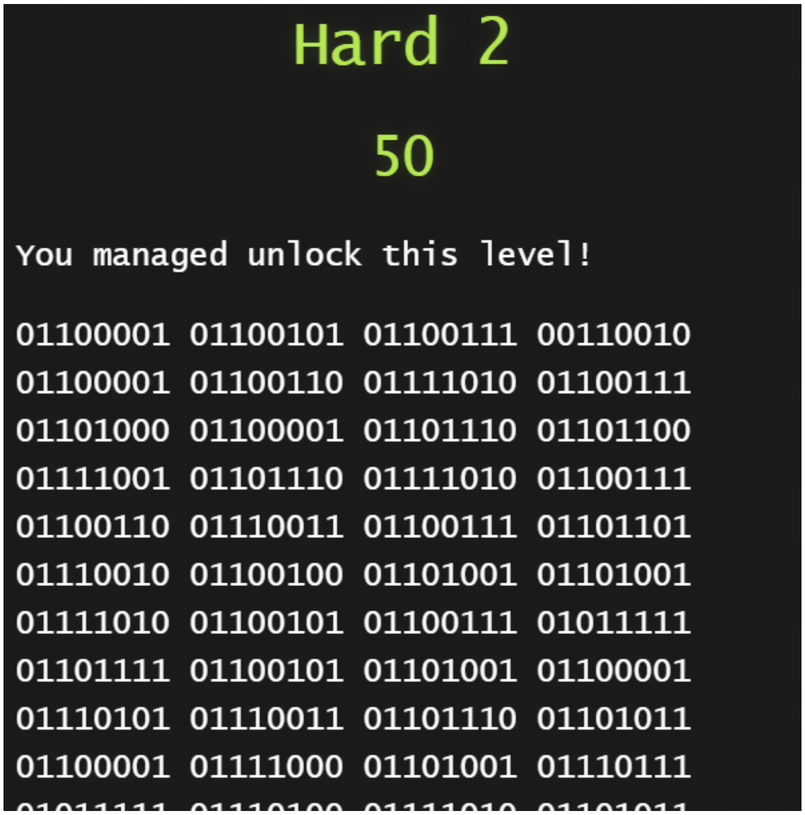
Rail fence cipher decoder

Encoded message: zonri_ieuincazgeu}gkrpiez{zksyzahsnkyaaa_zamedginxgmdzgale_i

Max rails to try: 7

```
znzgacoahmszngndkeruyza}igagak_r_azpiialmeezeed{uzg_ikisnixy

zueazazion{_gzzcnakaamszrgyeldzeiuageih}_gsn_xnkirkgimypeiad

zigzagmakeourheadspinninglikecrazynexa{zigzag_make_us_dizzy}

z_e{kdagyzuioe}kailnasgunikyaxeg_zrnrcpazm_dahiaizesmzigenzg
```

Hard 2

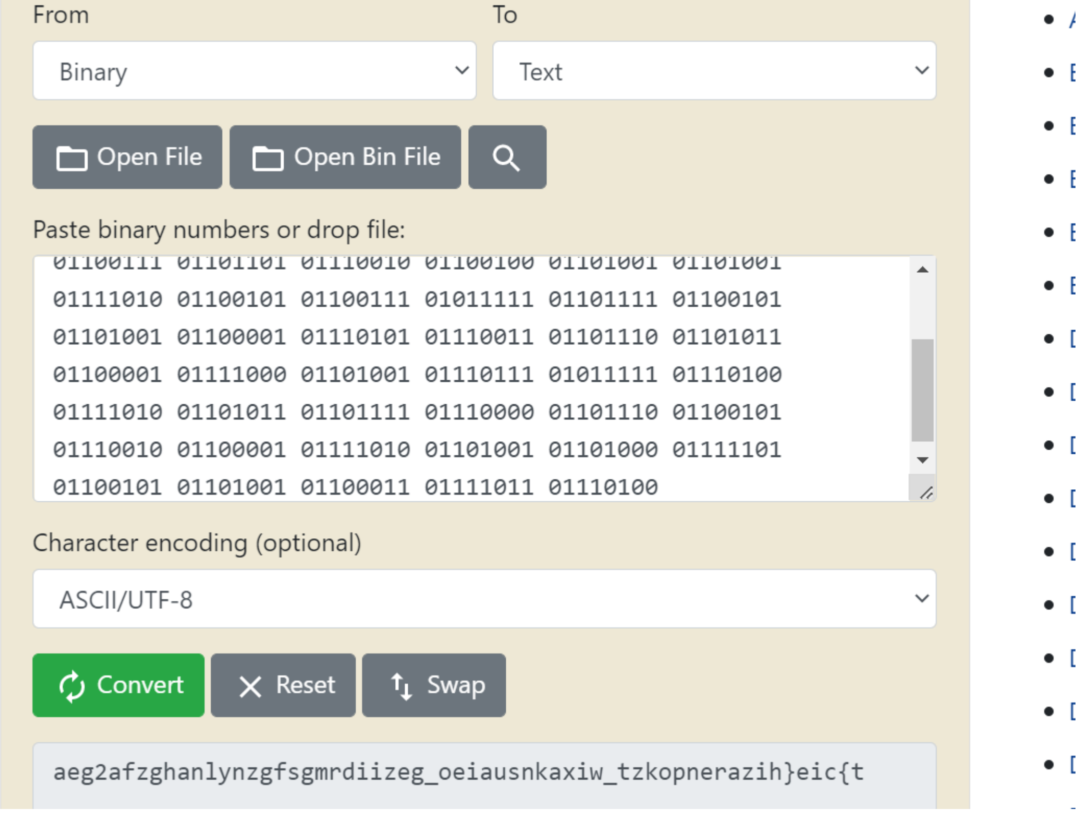


Hard 2

50

```
You managed unlock this level!

01100001 01100101 01100111 00110010
01100001 01100110 01111010 01100111
01101000 01100001 01101110 01101100
01111001 01101110 01111010 01100111
01100110 01110011 01100111 01101101
01110010 01100100 01101001 01101001
01111010 01100101 01100111 01011111
01101111 01100101 01101001 01100001
01110101 01110011 01101110 01101011
01100001 01111000 01101001 01110111
01011111 01110100 01111010 01101011
```

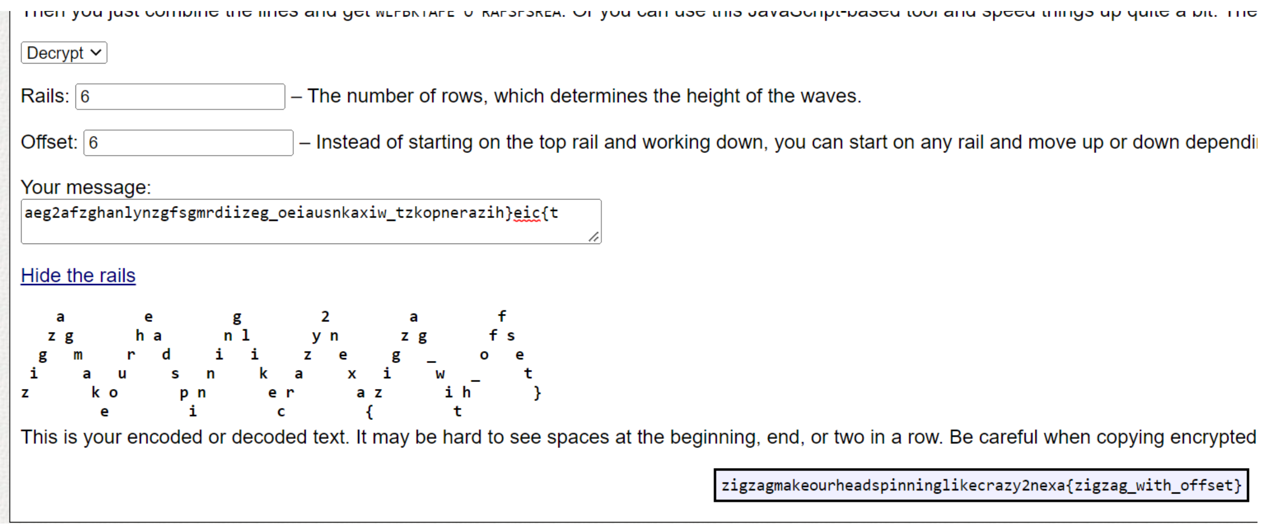
Dedode the binary



```
01100111 01101101 01110010 01100100 01101001 01101001
01111010 01100101 01100111 01011111 01101111 01100101
01101001 01100001 01110101 01110011 01101110 01101011
01100001 01111000 01101001 01110111 01011111 01110100
01111010 01101011 01101111 01110000 01101110 01100101
01110010 01100001 01111010 01101001 01101000 01111101
01100101 01101001 01100011 01111011 01110100
```

```
aeg2afzghanlynzgfsgmrdiizeg_oeiausnkaxiw_tzkopnerazih}eic{t
```

Decrypt the railfence with 6



Then you just combine the lines and get WLFBKTAFE O KAPSPSREA. Or you can use this JavaScript-based tool and speed things up quite a bit. The

Rails: 6 – The number of rows, which determines the height of the waves.

Offset: 6 – Instead of starting on the top rail and working down, you can start on any rail and move up or down dependi

Your message:

```
aeg2afzghanlynzgfsgmrdiizeg_oeiausnkaxiw_tzkopnerazih}eic{t
```

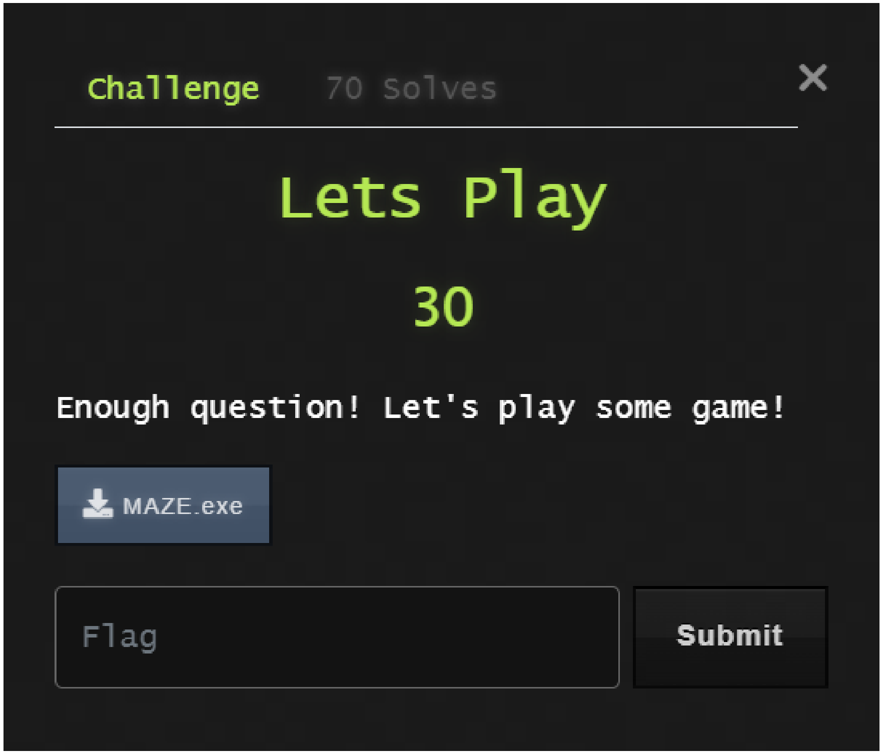
```
    a         e         g         2         a         f
   z g     h a     n l     y n     z g     f s
  g   m     r   d     i   i     z   e     g   _     o   e
 i     a   u     s   n     k   a     x   i     w   _     t
z       k o       p n       e r       a z       i h       }
         e         i         c         {         t
```

This is your encoded or decoded text. It may be hard to see spaces at the beginning, end, or two in a row. Be careful when copying encrypted

```
zigzagmakeourheadspinninglikecrazy2nexa{zigzag_with_offset}
```

Reverse Engineering

Lets Play



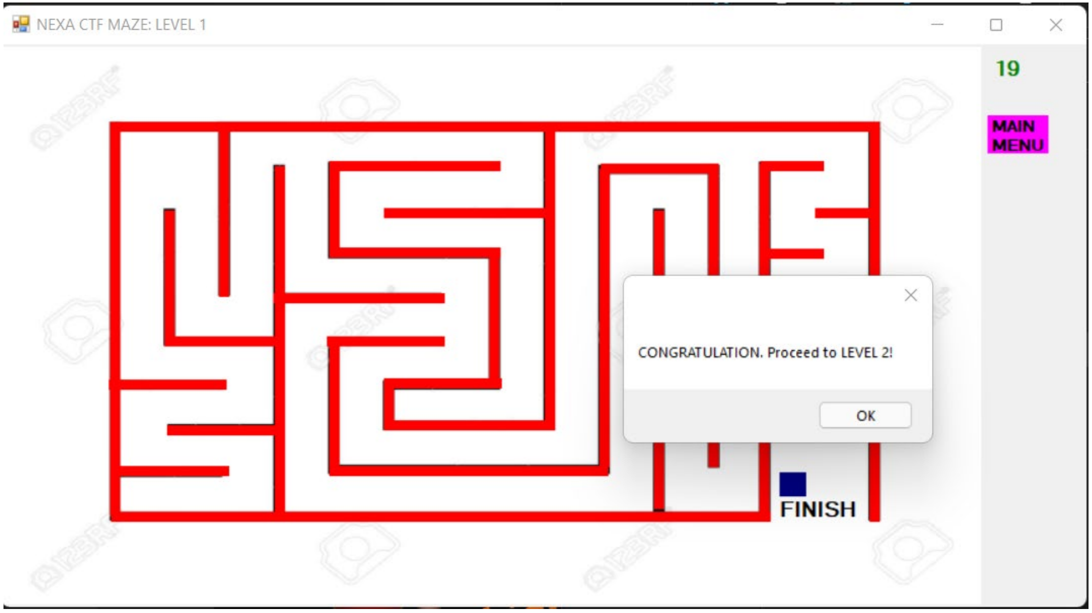
Challenge 70 Solves

Lets Play

30

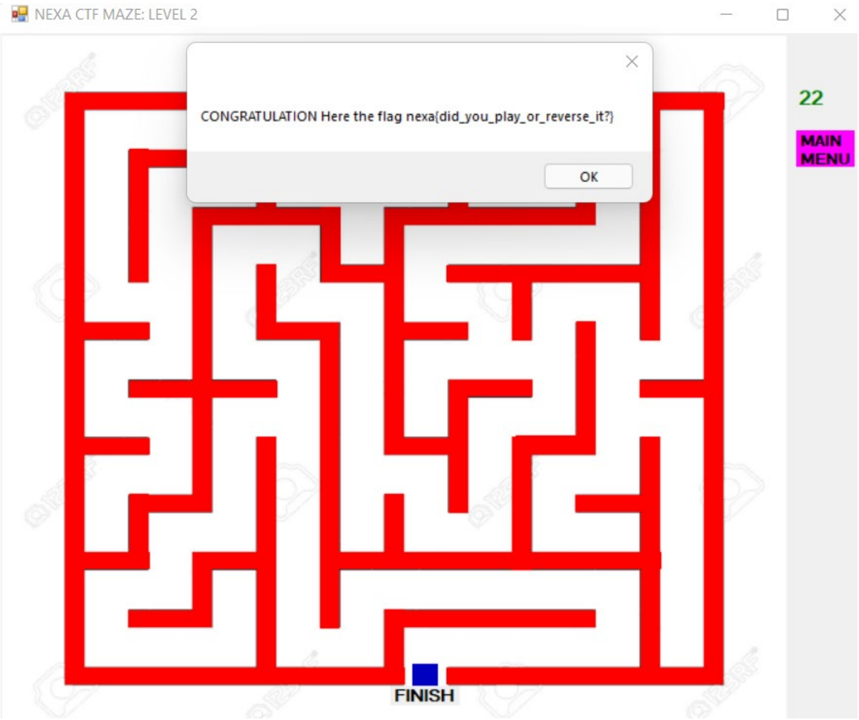
Enough question! Let's play some game!

Download the MAZE.exe, execute it and play the game, first Level has been solved.



CONGRATULATION. Proceed to LEVEL 2!

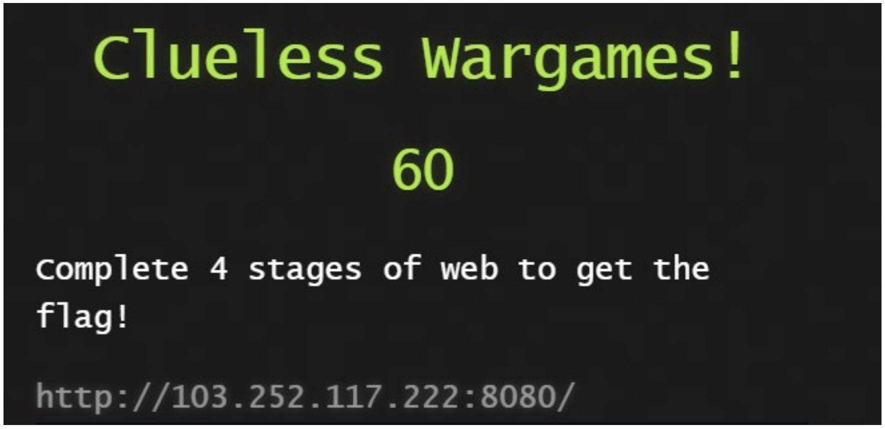
Finish the level 2 and the flag is given. (Even times up , press “yes” to try again ,the blue dot will not go back to the original spawn spot and you can continue play with the remain spot before the times up until go to the finish spot.)



CONGRATULATION Here the flag nexa{did_you_play_or_reverse_it?}

Web

Clueless Wargames!



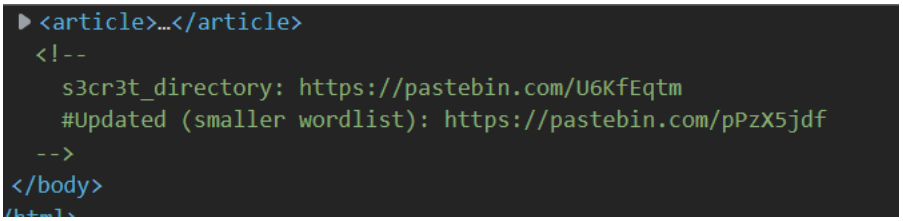
Clueless Wargames!

60

Complete 4 stages of web to get the flag!

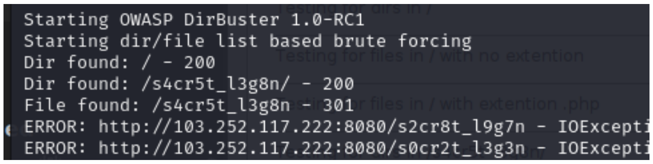
http://103.252.117.222:8080/

In stage1 we found the wordlist provided



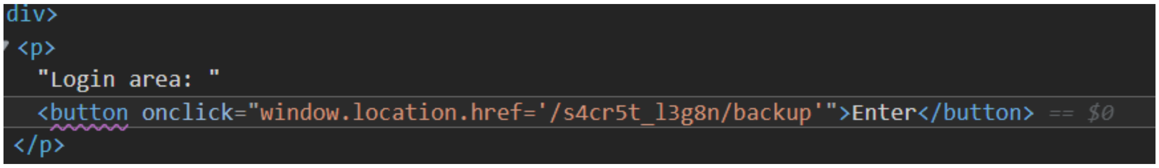
```
▶ <article>…</article>
  <!--
    s3cr3t_directory: https://pastebin.com/U6KfEqtm
    #Updated (smaller wordlist): https://pastebin.com/pPzX5jdf
  -->
</body>
```

Use dirbuster with wordlist given to brute force the directory, and we found.



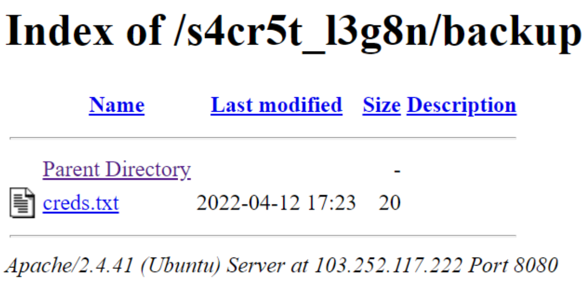
```
Starting OWASP DirBuster 1.0-RC1
Starting dir/file list based brute forcing
Dir found: / - 200
Dir found: /s4cr5t_l3g8n/ - 200
File found: /s4cr5t_l3g8n - 301
ERROR: http://103.252.117.222:8080/s2cr8t_l9g7n - IOExcepti
ERROR: http://103.252.117.222:8080/s0cr2t_l3g3n - IOExcepti
```

In stage 2 edit the button ,the window.location.href dir change with backup dir



```
div>
▾ <p>
   "Login area: "
   <button onclick="window.location.href='/s4cr5t_l3g8n/backup'">Enter</button> == $0
 </p>
```

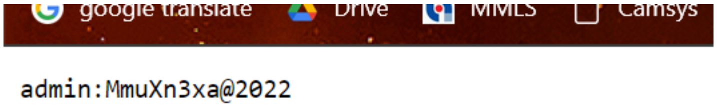
Then click the button and access



Index of /s4cr5t_l3g8n/backup

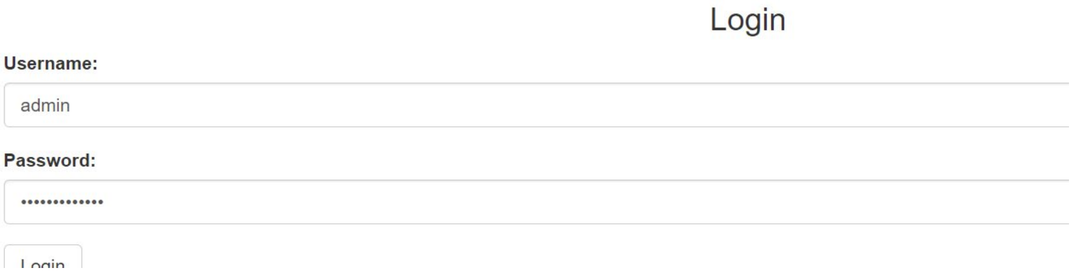
```
      Name          Last modified     Size Description
------------------------------------------------------
  Parent Directory                       -
  creds.txt         2022-04-12 17:23    20
------------------------------------------------------
Apache/2.4.41 (Ubuntu) Server at 103.252.117.222 Port 8080
```

Open creds.txt and get the username and password



```
admin:MmuXn3xa@2022
```

Back to the stage2 page and click the original button to enter the login page. And use the username and password we found to login

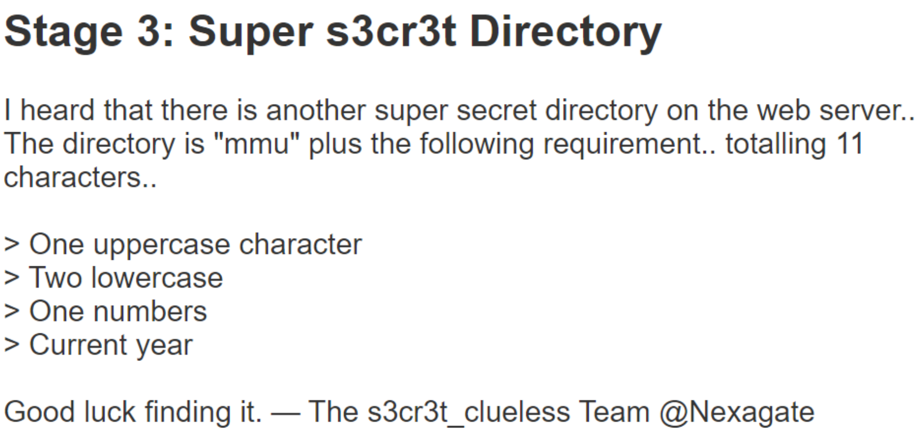


Login

Username: admin

Password: •••••••••••••

Stage3 need to brute force the dir again.



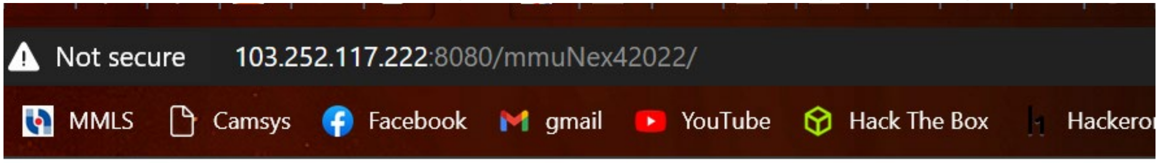
Stage 3: Super s3cr3t Directory

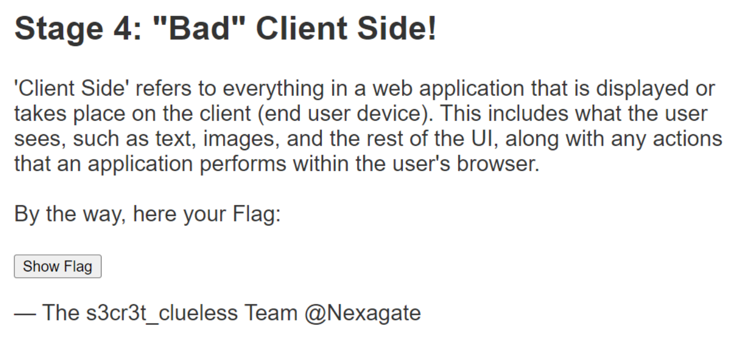
I heard that there is another super secret directory on the web server.. The directory is "mmu" plus the following requirement.. totalling 11 characters..

> One uppercase character
> Two lowercase
> One numbers
> Current year

Good luck finding it. — The s3cr3t_clueless Team @Nexagate

But here I use a short cut. I saw the format is similar with password at stage2 so I guess the password with the format, and bingo. So access to the dir and get into stage4





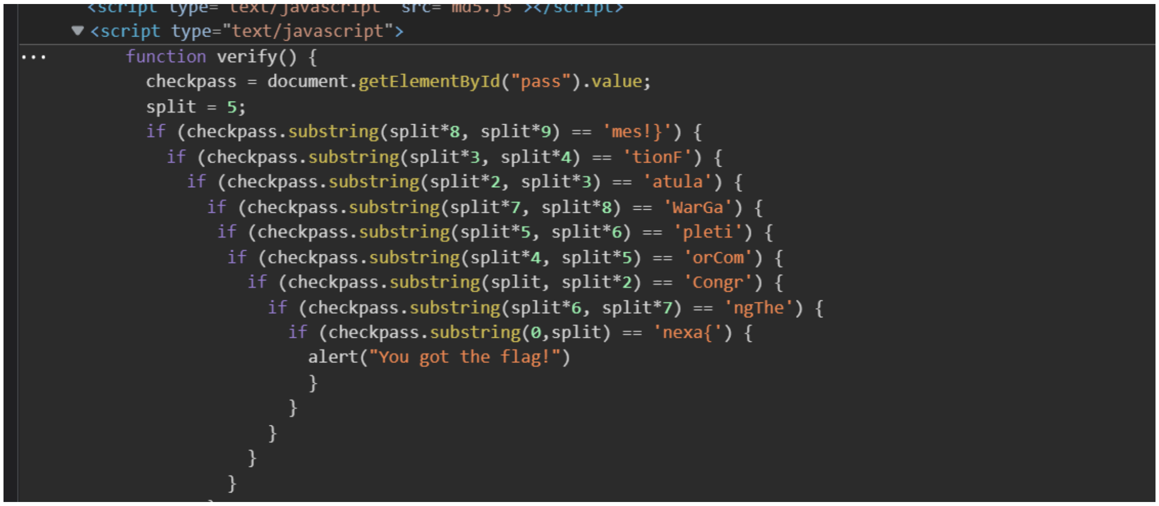
Stage 4: "Bad" Client Side!

'Client Side' refers to everything in a web application that is displayed or takes place on the client (end user device). This includes what the user sees, such as text, images, and the rest of the UI, along with any actions that an application performs within the user's browser.

By the way, here your Flag:

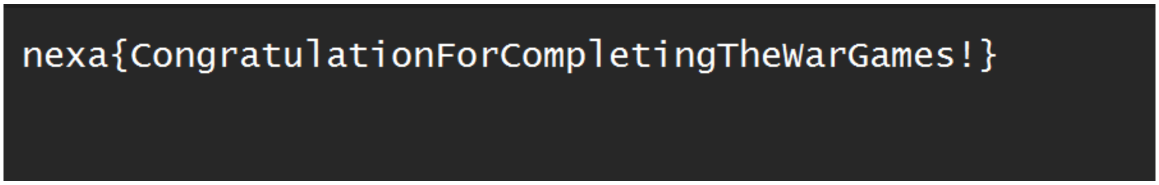
— The s3cr3t_clueless Team @Nexagate

Click the show flag but it’s need password. But we read the network and the source code, we found the flag



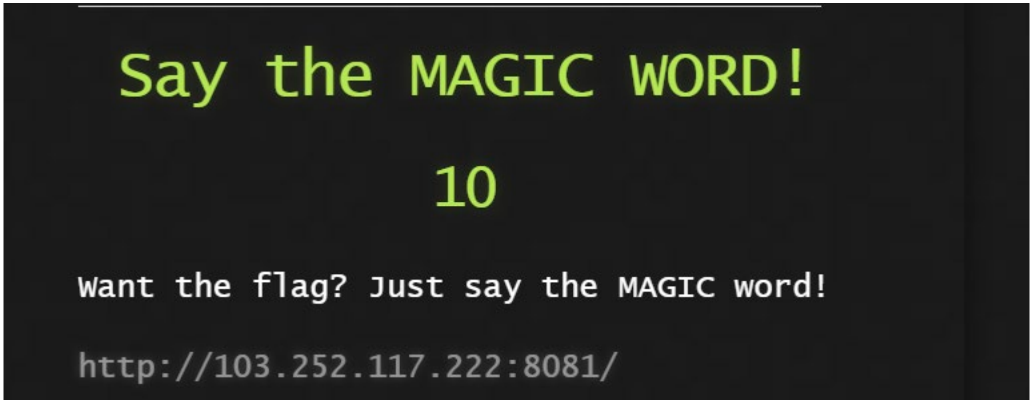
```
    <script type="text/javascript" src="md5.js"></script>
  ▼<script type="text/javascript">
        function verify() {
          checkpass = document.getElementById("pass").value;
          split = 5;
          if (checkpass.substring(split*8, split*9) == 'mes!}') {
            if (checkpass.substring(split*3, split*4) == 'tionF') {
              if (checkpass.substring(split*2, split*3) == 'atula') {
                if (checkpass.substring(split*7, split*8) == 'WarGa') {
                 if (checkpass.substring(split*5, split*6) == 'pleti') {
                  if (checkpass.substring(split*4, split*5) == 'orCom') {
                    if (checkpass.substring(split, split*2) == 'Congr') {
                      if (checkpass.substring(split*6, split*7) == 'ngThe') {
                        if (checkpass.substring(0,split) == 'nexa{') {
                          alert("You got the flag!")
                          }
                        }
                      }
                    }
                  }
```

Combine the flag and we get the full flag



```
nexa{CongratulationForCompletingTheWarGames!}
```

Say the MAGIC WORD!



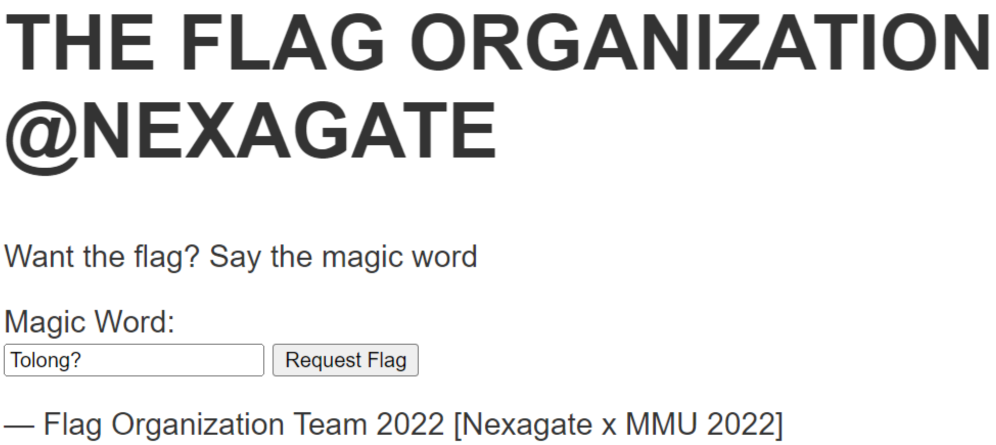
Say the MAGIC WORD!

10

Want the flag? Just say the MAGIC word!

http://103.252.117.222:8081/

We need to use magic word to get the flag



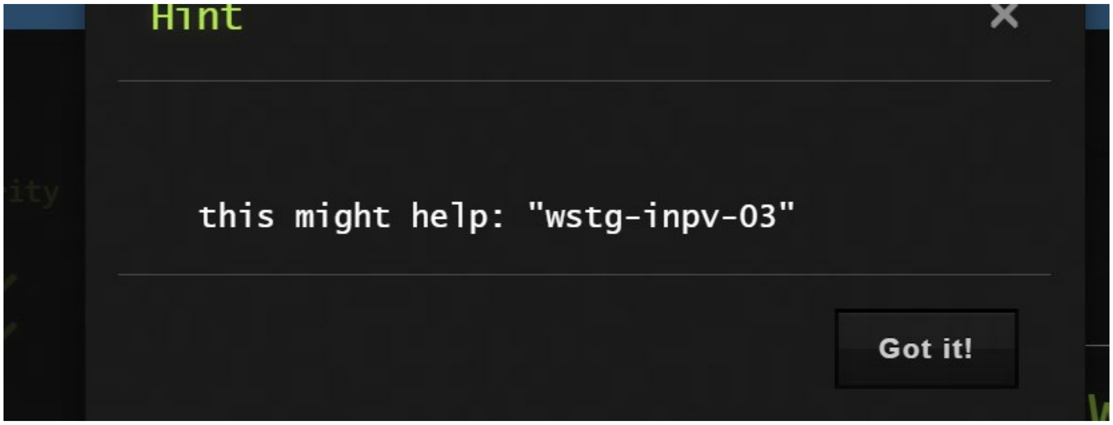
THE FLAG ORGANIZATION @NEXAGATE

Want the flag? Say the magic word

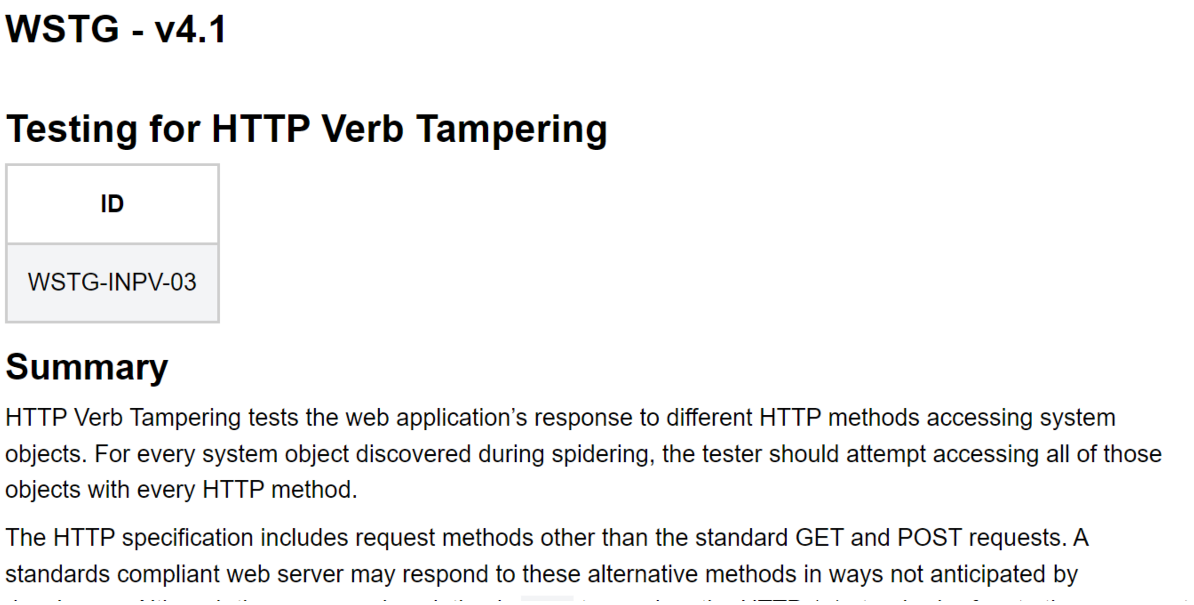
Magic Word: Tolong?

— Flag Organization Team 2022 [Nexagate x MMU 2022]

After view the hint below and have some google search we know that it require to change the http methos



this might help: "wstg-inpv-03"



WSTG - v4.1

Testing for HTTP Verb Tampering

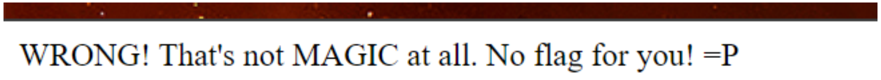
ID
WSTG-INPV-03

Summary

HTTP Verb Tampering tests the web application’s response to different HTTP methods accessing system objects. For every system object discovered during spidering, the tester should attempt accessing all of those objects with every HTTP method.

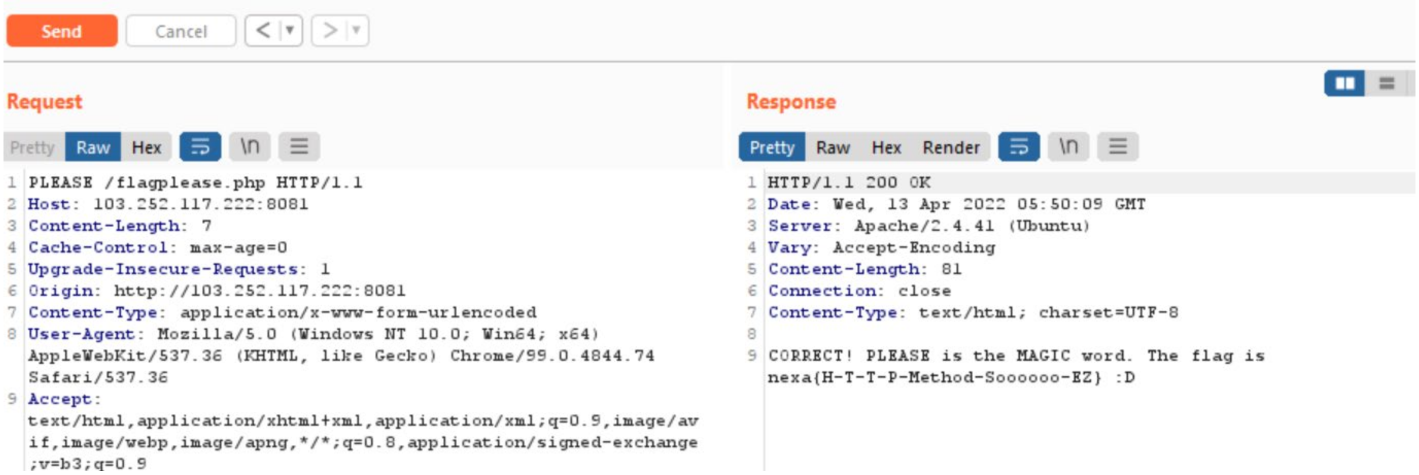
The HTTP specification includes request methods other than the standard GET and POST requests. A standards compliant web server may respond to these alternative methods in ways not anticipated by

After some trying of changing HTTP methos, I realise the =P from the wrong message



WRONG! That's not MAGIC at all. No flag for you! =P

And I remember the weird word tolong? In the form. So I try the PLEASE and it is work.



Request

```
PLEASE /flagplease.php HTTP/1.1
Host: 103.252.117.222:8081
Content-Length: 7
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://103.252.117.222:8081
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/av
if,image/webp,image/apng,*/*;q=0.8,application/signed-exchange
;v=b3;q=0.9
```

Response

```
HTTP/1.1 200 OK
Date: Wed, 13 Apr 2022 05:50:09 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 81
Connection: close
Content-Type: text/html; charset=UTF-8

CORRECT! PLEASE is the MAGIC word. The flag is
nexa{H-T-T-P-Method-Soooooo-EZ} :D
```