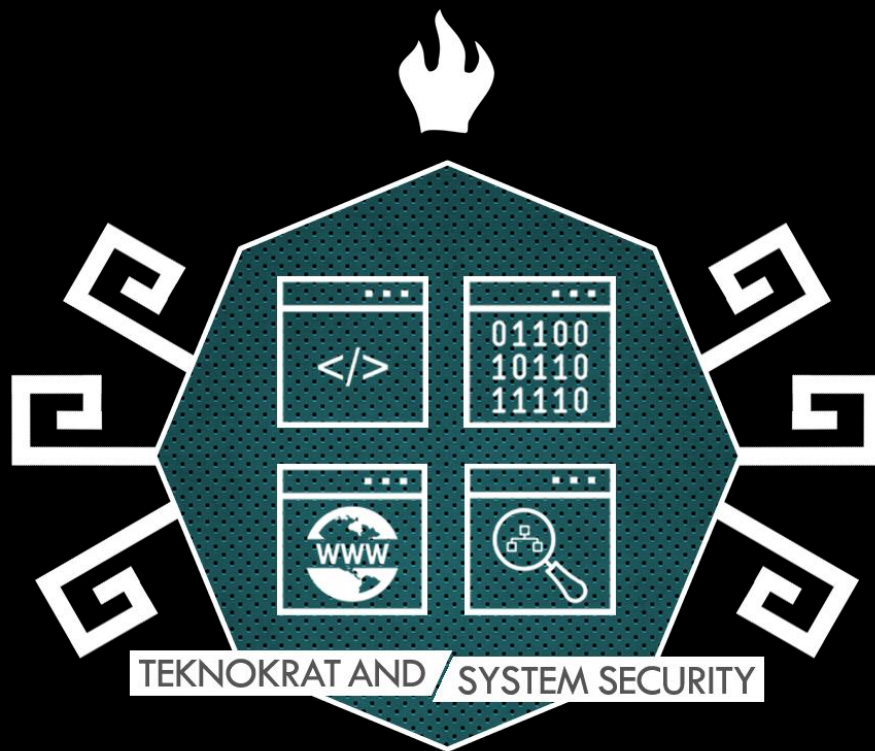


Write Up SECARMY CTF 2.0



Welcome

Welcome All

Welcome All

20

The flag format for the challenges are:
secarmy{your_fl4g_h3r3}

For this particular challenge, flag is:
secarmy{w3lc0me_y0u_all}

Just copy and paste it.

Flag

secarmy{w3lc0me_y0u_all}

Netcat ' (^.^) '

diberikan link nc 68.183.44.136 2200

```
[flintz@shadow]~[~/Downloads/sec-army]
$nc 68.183.44.136 2200

Welcome To SecArmyCTF!!
Here, Take your flag:
secarmy{W3lc0m3_T0_S3c4RmyC7F0x02}
```

Ethical Hacking ▢ Pentesting ▢ CTF ▢
▢
#wearesecarmy
academy.sec.army

Flag

secarmy{W3lc0m3_T0_S3c4RmyC7F0x02}

InstaFamous

Cara Pengerjaan

cek post pertama di ig https://www.instagram.com/sec_army/

How we ranked 4th in SHELL-CTF 0x01 (Writeup)



sec-army 12 February · 10 min read



sec_army • Follow

...



sec_army How we ranked 4th in SHELL-CTF 0x01 (Writeup) Link: link.medium.com/eIXJPf1LfU

secarmy{w3lc0me_1n\$t@_f@m1ly}

#shell #ctf #hackers #cybersecurity
#mrrobot #challenges #winner
#wearesecarmy

24w



venkatesh.k_ 🤔

24w Reply



pro_memer0161 I love this series. Mr.Robot

17w Reply



234 likes

FEBRUARY 22

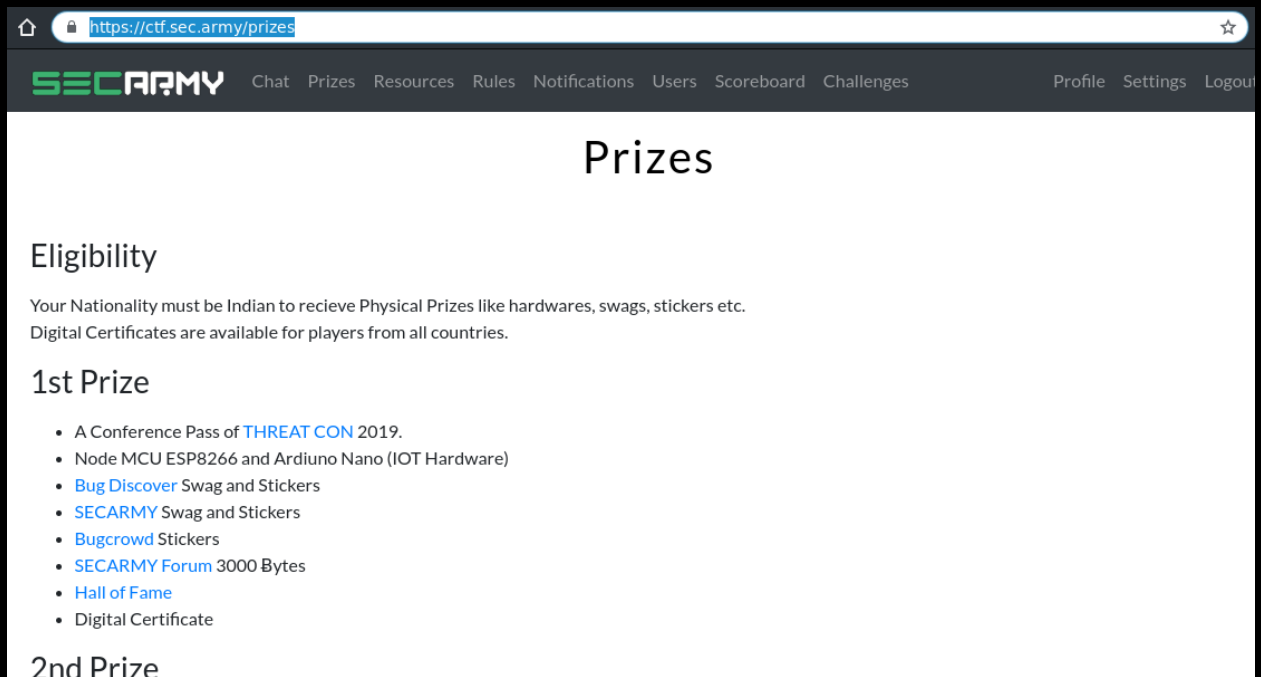
Flag

secarmy{w3lc0me_1n\$t@_f@m1ly}

Web

Prizes

diberikan link hadiah untuk pemenang di secarmy



cek source code web tersebut, terdapat base64, decode aja

```
168 </p>
169 <h3>4th - 10th Prize</h3>
170 <p>
171 <ul>
172 <li>Digital Certificate</li>
173 </ul>
174 <!--One step closer to prizes: c2VjYXJteXtzMHVyYzNfaTVfbjNjZXM1YXJ5fQo= -->
175 </p>
176 </div>
177
178 </main>
179
180 <footer class="footer">
```


Flag

secarmy{s0urc3_i5_n3ces5ary}

web_salad

diberikan link dengan tampilan sebuah form login

https://sec-army.ml/web_salad/login.php



Login

Username

Password

cek pada source code tersebut, didapat sebuah username dan password yang sudah dihash dalam md5

```
94 </form>
95 </body>
96 <!--username: ee11cbb19052e40b07aac0ca060c23ee-->
97 <!--password: bdc87b9c894da5168059e00ebffb9077-->
98 </html>
```

decode dan didapat username=user and password=password1234, dan coba login
cek lagi source codenya didapat sebuah base64 yang merupakan flagnya

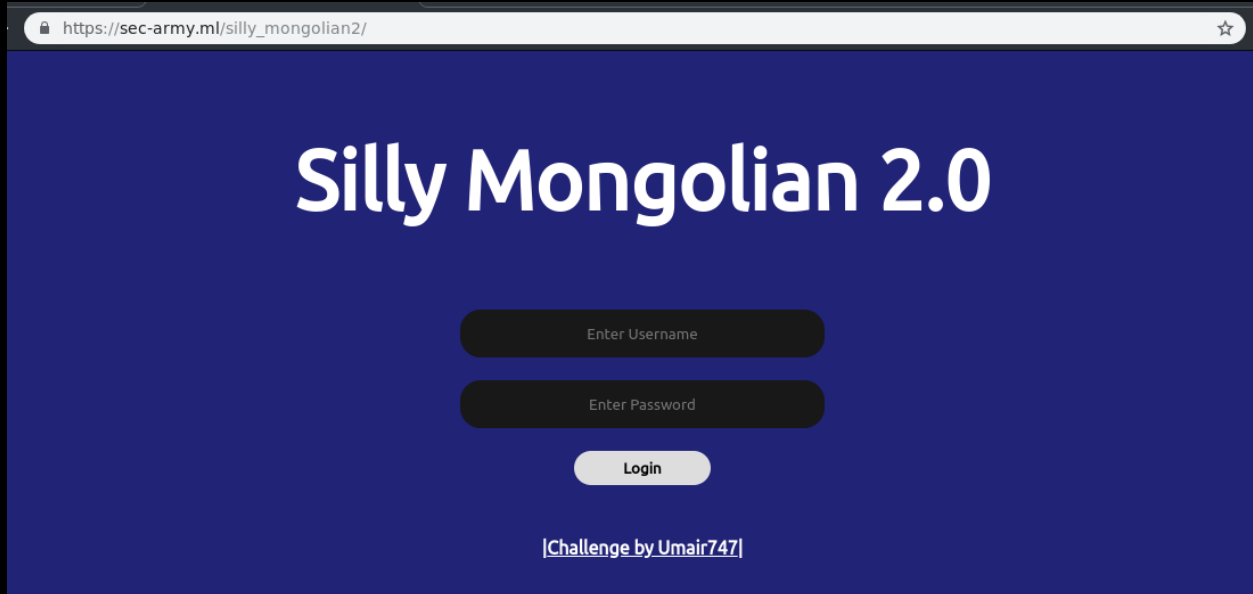
```
flintz@shadow:~/Downloads/sec-army$ echo oc2VjYXJteXt3M2JfYnVjazN0XzNuYzB1bjdlcjNkfQo= | base64 -d
secarmy{w3b_buck3t_3nc0un7er3d}
```

Flag

secarmy{w3b_buck3t_3nc0un7er3d}

Silly Mongolian 2.0

diberikan link dengan tampilan sebuah form login lagi



https://sec-army.ml/silly_mongolian2/

Silly Mongolian 2.0

Enter Username

Enter Password

Login

[Challenge by Umair747](#)

cek kembali source codenya, didapat potongan flag yang terpecah, cari dan gabung menjadi flag utuh.

```
18 <nav>
19 <p><b>|<u>Challenge by Umair747</u>|</p>
20 <!--Here's the first part of flag :
21 secarmy{why
22 -->
23 </nav>
```

```
return new Uint8Array(array);
console.log(flag);
/*Here's the second part of flag :
_ls_thls_
*/
```

```
function login() {
  window.open("error404.html");
  /*Here's the third part of flag :
  m0ng0li@n_$uch
  */
}
```

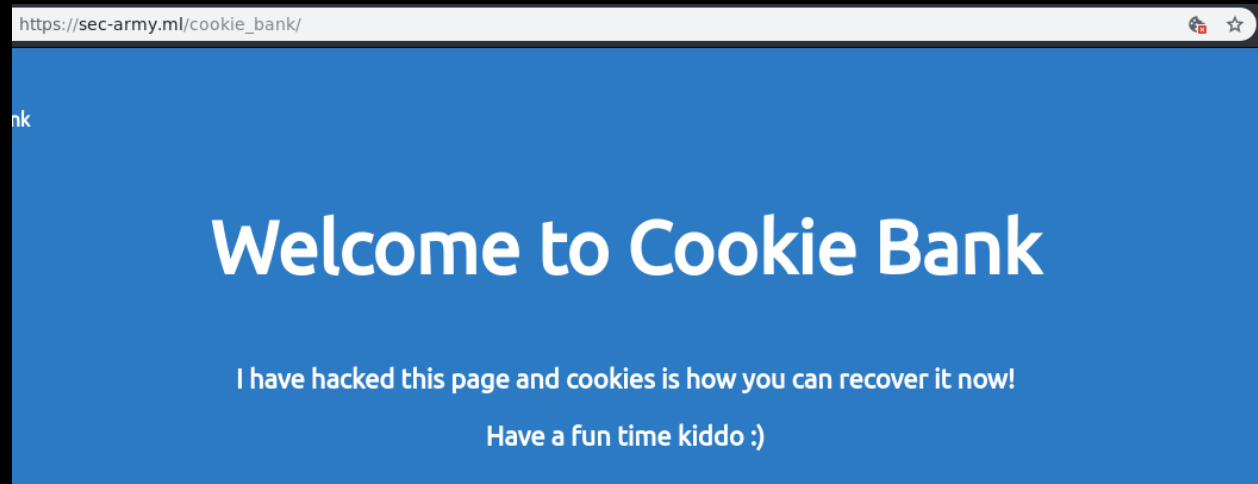
```
.pass{
  margin-top: 20px;
}
/*Here's the fourth part of flag :
@_f00l}
*/
```

Flag

secarmy{why_1s_th1s_m0ng0li@n_\$uch_@_f00l}

Cookie Bank

diberikan tampilan web yang memberikan sebuah hint yaitu cookie



coba cek cookienya, tapi pada sourcecode nya juga ada -_-



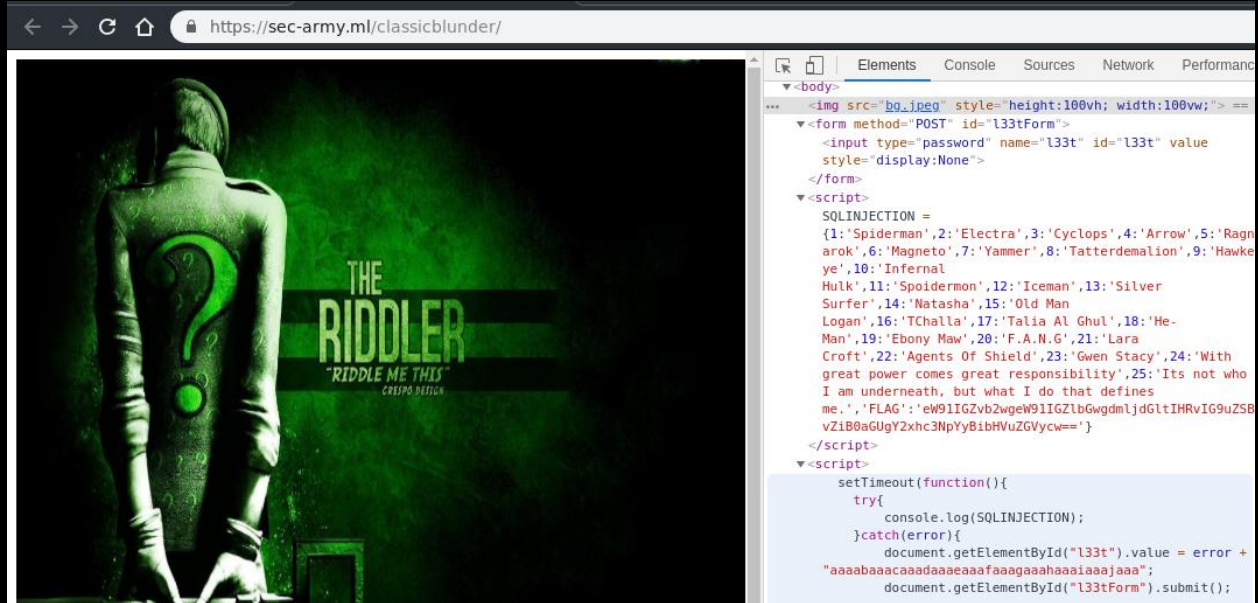
decode dan temukan :v

Flag

secarmy{the_\$hy_c00kie_w1th1n}

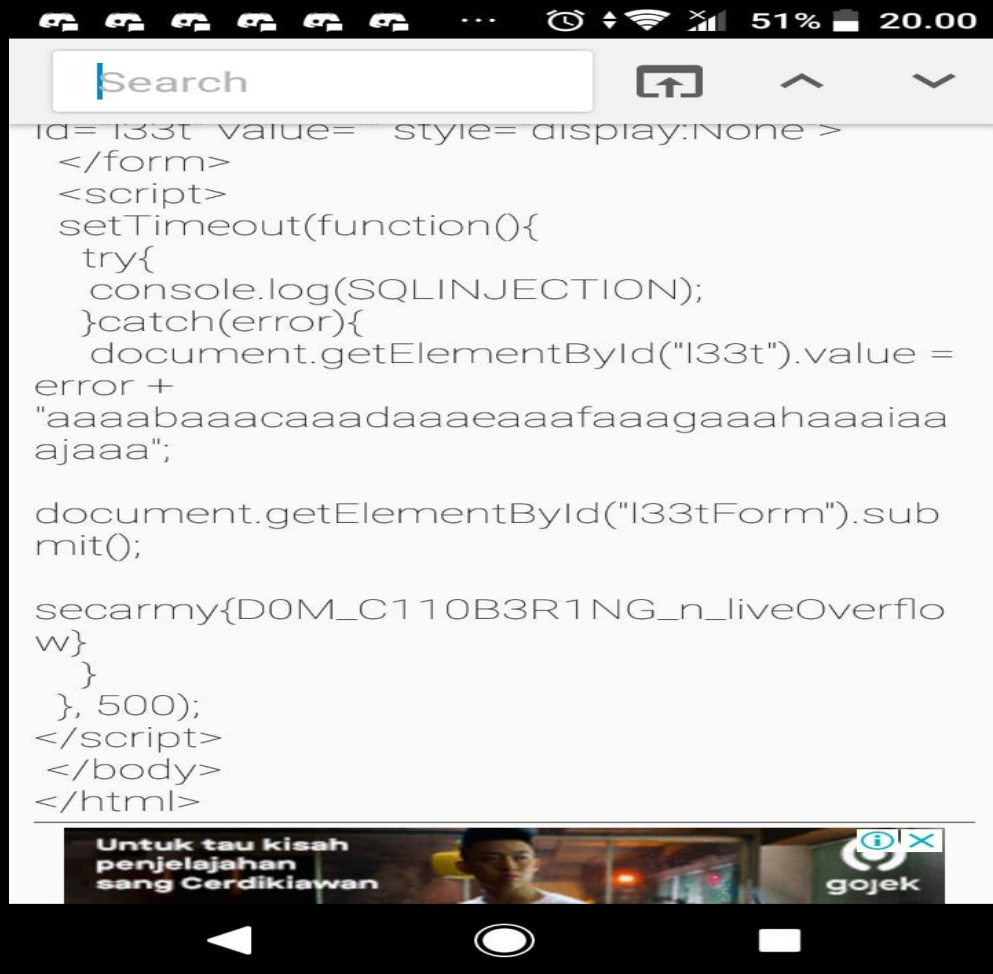
Classic Blunder

diberikan web dengan sebuah object JSON



analisa kemungkinan yang ada seperti sql dkk tapi bukan, juga disana terdapat sebuah flag palsu -_-

disini saya menggunakan html tool pada android untuk mendapatkan flagnya, cek pada sourcecode nya



Flag

`secarmy{DOM_C110B3R1NG_n_liveOverflow}`

Starters

"16+8"

didapat 2 file zip, extract dan didapat file1.txt, file2.txt, dimana file tersebut terdapat hex dan octal code

```
$cat file1.txt.txt
73
65
63
61
72
6d
79
7b
Best of luck :P [flintz@shadow]~[~/Downloads]
```

World's simplest oct to text converter. Just paste octal value and press Convert button, and you get plain text. Press button to see nonsense or garbage.

Like 52K

Announcement: We just launched [math tools for developers](#). It out!

Num3er_sys73m}

decode dan gabungkan menjadi sebuah valid flag

Flag

secarmy{Num3er_sys73m}

Easy Capture

didapat sebuah file flagmain.zip, yang diextract terdapat sebuah biner code, coba untuk decode

```

01110011 01100101 01100011 01100001 01110010 01101101
01111001 01111011 01101000 00110011 01110010 00110011
01011111 01111001 00110000 01110101 01011111 01100011
01000000 01110000 01110100 01110101 01110010 00110011
01111101

```

Character encoding:

ASCII

Convert

Reset

Swap

secarmy{h3r3_y0u_c@ptur3}

Flag

secarmy{h3r3_y0u_c@ptur3}

Die Basis

didapat file zip berisi file1.txt dan file2.txt

```

$ cat file2.txt
*****L52GQM27MJAHG35*****
Th3_G1F7
50

''GMZA===='' [flintz@shadow]~/Downloads
$ cat file1.txt
*****c2VjYXJteXtmEBNzFzXw==***** [flintz@shadow]~/Downloads

```

yang pertama adalah base64 dan kedua merupakan base32, decode dan combine saja

```

$ echo c2VjYXJteXtmEBNzFzXw== | base64 -d
secarmy{fl@g_ls_ [flintz@shadow]~/Downloads
$ echo L52GQM27MJAHG35GMZA==== | base32 -d
th3_b@s3}32 [flintz@shadow]~/Downloads
$

```

secarmy{fl@g_1s_th3_b@s3}

didapat sebuah gambar



```
$zsteg Image3.png
b1,rgb,lsb,xy  .. text:0          secarmy{th3_im@ge_s4ys_i7_all}"50
b1,bgr,msb,xy  .. file: shared library
b2,r,msb,xy     .. text: "TTTTTTTTTTTTTTTTTTTTTTTTTTTTUUU"
b2,g,msb,xy     .. file: PGP\011Secret Key
b2,b,msb,xy     .. text: "TTTTTTTTTTTTTTTTTTTTTTTTUUU"
The image says it all.
```

```
$zsteg Image3.png
b1,rgb,lsb,xy  .. text:0          secarmy{th3_im@g3_s4ys_i7_all}"50
b1,bgr,msb,xy  .. file: shared library
b2,r,msb,xy     .. text: "TTTTTTTTTTTTTTTTTTTTTTTTTTTTUUU"
b2,g,msb,xy     .. file: PGP\011Secret Key
b2,b,msb,xy     .. text: "TTTTTTTTTTTTTTTTTTTTTTTTUUU"
The image says it all.
```

secarmy{th3_im@ge_s4ys_i7_a11}

diberikan sebuah PNG image, penyelesaiannya sama seperti dengan soal IMAGE

[illegible]

secarmy{h3re_1s_th3_g1ft}

Misc

Directories

Directories

100

Linux Basic

It is a type of illusionary filesystem. It does not exist on a disk. Can U name it ? Flag Format :- secarmy{/flag}
Author:Elemental X

Submit

The /proc filesystem adalah jenis illusionary filesystem. ada, tapi tidak tampil pada disk.

Flag

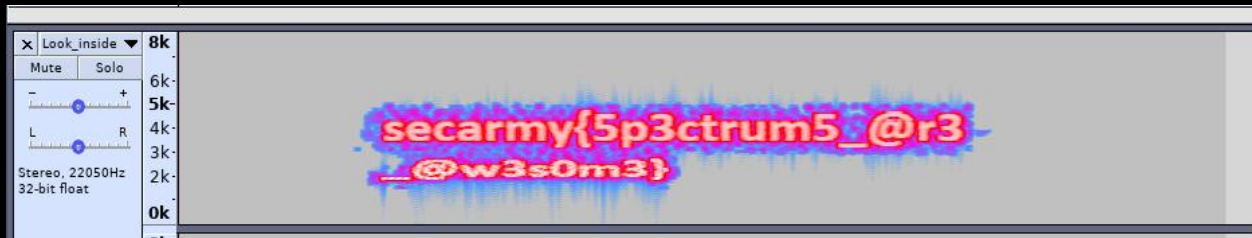
secarmy{/proc}

Look Inside

diberikan sebuah file audio wav

```
[x]-[flintz@shadow]-[~/Downloads]  
$file Look_inside.wav  
Look_inside.wav: RIFF (little-endian) data, WAVE audio, Microsoft PCM, 16 bit, s  
tereo 22050 Hz
```

coba analisa file tersebut dengan audacity, dan cek pada spectrogram



Flag

`secarmy{5p3ctrum5_@r3_@w3s0m3}`

Bruteforce

diberikan file zip yang berisi sebuah image

`lolyouneedtoencryptthistoosolangbrain`



coba dengan binwalk untuk mengekstrak data didalamnya, dan didapat sebuah file zip.

Travel

Travel

100

Basic Networking

Well , I need to discover the path the packet takes . ,
Author : ElementalX

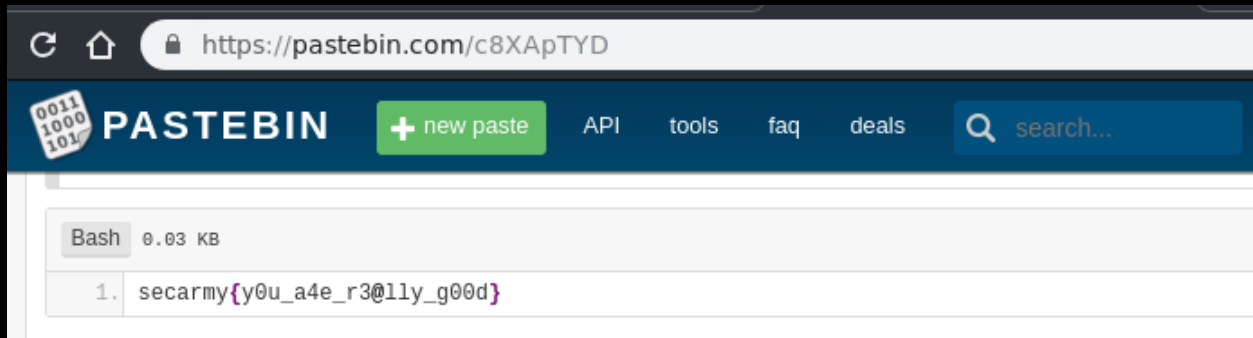
Traceroute adalah perintah untuk menunjukkan rute yang dilewati paket untuk mencapai tujuan

Flag

secarmy{traceroute}

Get_Me

diberikan sebuah file zip yang berisi sebuah base 32

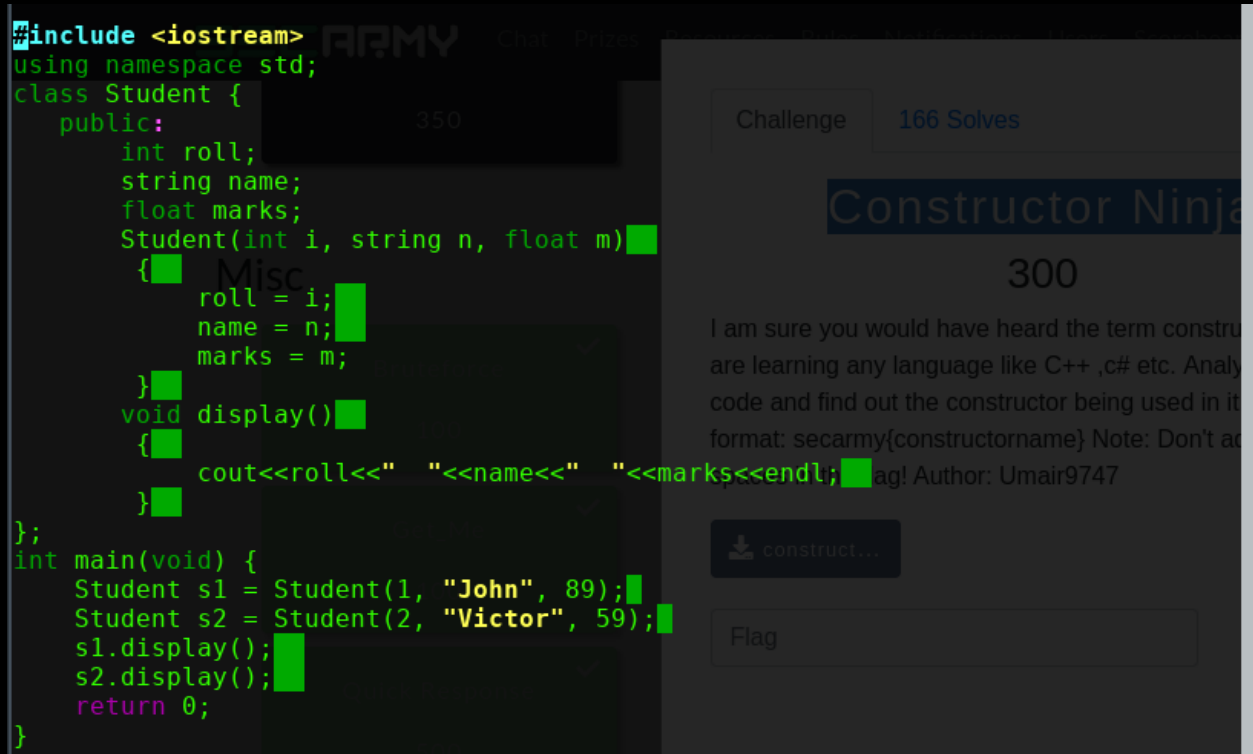


Flag

secarmy{y0u_a4e_r3@lly_g00d}

Constructor Ninja

diberikan sebuah code C++ seperti berikut yang disuruh mencari nama constructor



analisa dan mencoba untuk submit student dan employee, ternyata bukan.

sampai ada hint pada discord, yang menunjukan flag adalah jenis constructor yang dipakai

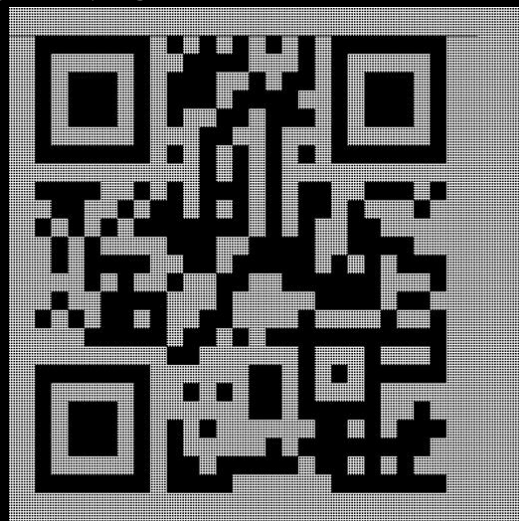
```
secarmy{parameterizedconstructor}
```

Quick Response

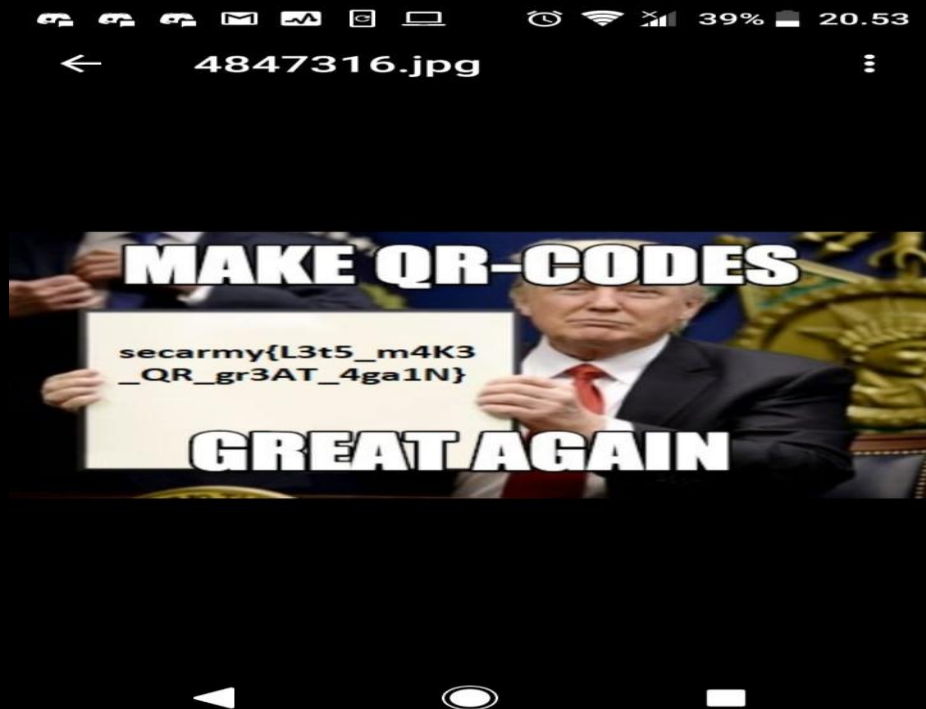
diberikan koneksi nc 68.183.44.136 8282 yang menghasilkan banyak string seperti ini

```
[x]-[flintz@shadow]([~/Downloads])  
$nc 68.183.44.136 8282  
Enjoy:  
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB  
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB  
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB  
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB  
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB  
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB  
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB  
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB  
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB  
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB  
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB  
Do you like different representations of Data?
```

jika dizoom out dilihat seperti sebuah qr code, coba dengan copy dan pastekan di excel dan lakukan manual untuk mengubah warna tiap blok , setelah kerja lembur bagai kuda yang cukup keras akhirnya didapat qr yang utuh :D



scan dan didapat sebuah gambar



Flag

secarmy{L3t5_m4K3_QR_gr3AT_4ga1N}

Poor prisoner

diberikan sebuah file radio_capture.txt yang berisi seperti ini

```
[flintz@shadow]--[~/Downloads]
$cat radio_capture.txt
57,95
43,91
33,96
31,107
41,116
57,124
58,135
49,139
34,140
83,119
92,118
101,114
103,106
```

Poor prisoner

550

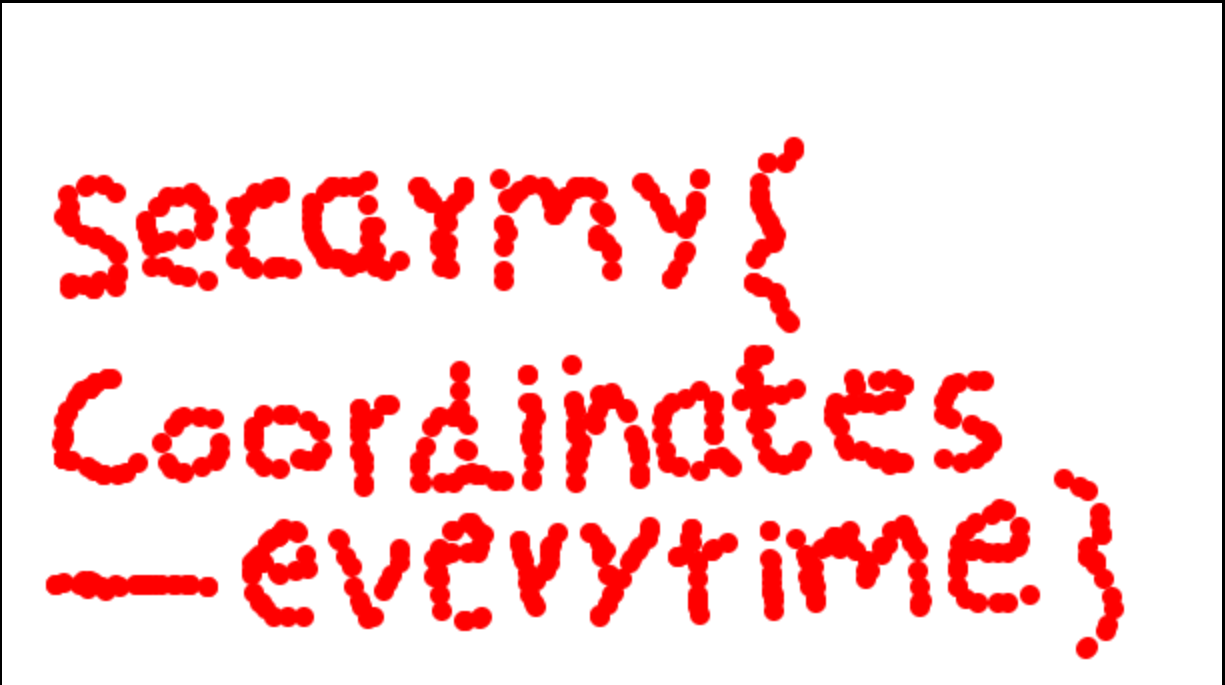
I was playing with my SDR, I saw that someone is communicate through radio, He was captured by s terrorists and needed my help, he told me that he flag for this challenge....and gave me these number me get my flag, he risked his life for same, don't d him :)

Note- The flag is all lowercase

diketahui itu merupakan sebuah coordinate image, coba dengan online tools pada

https://www.mobilefish.com/services/record_mouse_coordinates/record_mouse_coordinates.php

masukan sebuah gambar dan input kordinatnya juga dan flag pun didapat



Flag

secarmy{coordinates-everytime}

Forensics

Its all in your head

```
[flintz@shadow]--[~/Downloads]  
$file its_all_in_your_head.png  
its_all_in_your_head.png: data
```

diberikan sebuah file png dan analisa dengan hex editor didapat kesalahan pada file header gambar tersebut.

00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F	Decoded text
89 5E 4C 74 0D 0A 1A 0A 00 00 00 0D 49 48 44 52	89Lt.....IHDR
00 00 02 3B 00 00 01 53 08 02 00 00 00 50 FB 5A	...;...S....PUZ
A6 00 00 00 01 73 52 47 42 00 AE CE 1C E9 00 00	!....sRGB.0.é..
00 04 67 41 4D 41 00 00 B1 8F 0B FC 61 05 00 00	..gAMA..±..üa...
00 09 70 48 59 73 00 00 12 74 00 00 12 74 01 DE	..pHYs...t...t..b
66 1F 78 00 00 1A 6D 49 44 41 54 78 5E ED DD ED	f.x...m DATx^iYi

Ubah file signature tersebut dengan referensi

https://en.wikipedia.org/wiki/List_of_file_signatures didapat sebuah gambar yang berisi flag



Flag

secarmy{h3ad3rs_t3ll_a_l0t}

secret

Diberikan sebuah file Pdf.

hanya dengan Ctrl+A, dan flag nya terlihat

Here is your credentials, try logging in using the same and keep it on any safe place
For example- Desktop/password.txt

Username- admin

Password- *****secarmy{ain't_visible?}

Flag

secarmy{ain't_visible?}

The_B1N

didapat sebuah file zip yang berisi sebuah gambar bin1.jpg dan b1n.png



coba cek file png tersebut dengan zsteg.

```

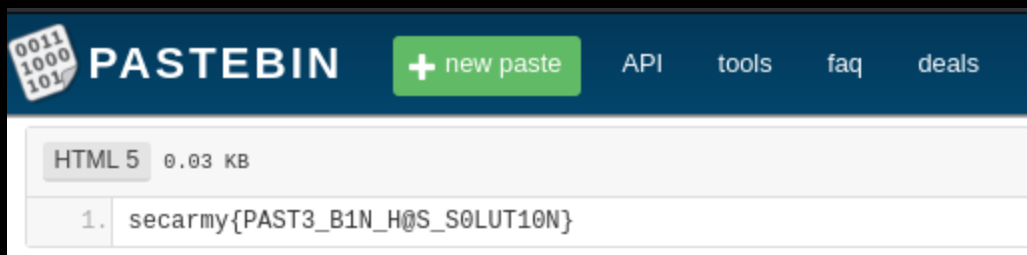
[flintz@shadow]--[~/Downloads]
$zsteg bln.png
b1,r,lsb,xy .. text: "nfJBbfJRbVnnfNJVbVFVbbnfvbbbbBFbfffFBfbFr sfJBbfJRbV
nnfNJVbVFVbbnfvbbbbFrBfBvjRFbFr"
b1,r,msb,xy .. text: "hvfRBFfRJFjvvfrRjFbjFFvfnFFFFBbFffbBfFbN"
b1,g,lsb,xy .. file: PEX Binary Archive
b1,b,msb,xy .. file: PDP-11 UNIX/RT_ldp
b1,rgb,lsb,xy .. text: " here you have the flag :- 61 48 52 30 63 48
4d 36 4c 79 39 77 59 58 4e 30 5a 57 4a 70 62 69 35 6a 62 32 30 76 54 45 30 35 6
3 57 56 33 64 57 6b 3d|61 48 52 30 63 48 4d 36 4c 79 39 77 59 58 4e 30 5a 57 4a
70 62 69 35 6a 62 32 30 76 57 6d 52 71 54 6a 6"

```

didapat sebuah hex code dengan menggunakan zsteg tapi hex code tersebut ttidak lengkap, coba dengan online di <https://stylesuxx.github.io/steganography/> untuk mendapatkan full hex codenya, decode dan didapat sebuah base64

aHR0cHM6Ly9wYXN0ZWJpbi5jb20vTE05cWV3dWk=aHR0cHM6Ly9wYXN0ZWJpbi5jb2OvWmRqTjj

decode kembali, didapat 2 buah link yang pertama berisi flag palsu dan kedua merupakan flag yang benar



Flag

secarmy{PAST3_B1N_H@S_S0LUT10N}

The Confusion

Diberikan sebuah 4 gambar lalu di decode satu persatu dengan

<https://stylesuxx.github.io/steganography/>

Didapatkan gambar flag1_rebuilt



Choose File flag1_Rebuilt.png

Hidden message

frpnezlfJN3_V7_f [empty boxes]

Lalu didecode dengan caesar cipher dan didapatkan = secarmy{WA3_I7_s

Cek gambar yang ternyata ada 2 gambar dengan fake flag

Dan ketika mencoba decode gambar flag3 dan didapatkan ROT 47



Choose File FLAG3.png

Hidden message

04?7Fb:?
8N [empty boxes]

Lalu didecode didapatkan 0_cOnfu3ing}

Flag

secarmy{WA3_I7_s0_cOnfu3ing}

Save Them

diberikan sebuah file zip berisi gambar nekovoi



coba dengan binwalk didapat file text menuju pastebin yang keduanya adalah flag palsu --
coba lihat kembali dengan ls -al

```
$ls -al
total 68
drwxr-xr-x 2 flintz flintz 4096 Aug  8 16:49 .
drwxr-xr-x 3 flintz flintz 4096 Aug 17 23:08 ..
-rw-r--r-- 1 flintz flintz   83 Aug  8 16:44 flags
-rw-r--r-- 1 flintz flintz 55852 Aug  8 16:49 .sauce
```

terdapat file .sauce yang berisi sebuah jsfuck, lakukan decode pada
<http://codertab.com/JsUnFuck>

JSUnFuck

secarmy{c0ng4atulat10ns_y0u_h@v3_th3_fl@g}

Binary / Reversing

Stringy

diberikan sebuah file ELF 64

analisa awal dengan melakukan strings dahulu

```
_ITM_registerTMCloneTable
u/UH
c2VjYXJtH
eXtsMDBrH
X2E3X3RoH
M19zdHIxH
bmc1ISF9H
[]A\A]A^A_
arghhh!! ok enter your string!!!
Did you missed it? look elsewhere...
```

terdapat sebuah base64 yang terpecah jika sudah dicompile

susun dan decode akan menghasilkan sebuah flag

```
$echo c2VjYXJteXtsMDBrX2E3X3RoM19zdHIxbmc1ISF9|base64 -d
secarmy{l00k_a7_th3_str1ng5!!} [flintz@shadow] - [~/Downloads]
```

Flag

secarmy{l00k_a7_th3_str1ng5!!}

Smash it!

diberikan sebuah file ELF 64 , buka dengan IDA pro

```

v23 = 't';
v24 = '@';
v25 = 'c';
v26 char v24; // [sp+23h] [bp-40h]@1
v27 = '.';
v28 = '1';
v29 = 's';
v30 = '.';
v31 = 't';
v32 = '0';
v33 = '0';
v34 = '.';
v35 = 'm';
v36 = 'u';
v37 = 'c';
v38 = 'h';
v39 = '.';
v40 = 'f';
v41 = 'u';
v42 = 'n';
v43 = '}'';
s1 = 1380013139;
v46 = 84;
while ( !v47 )
{
    puts("hahaha, you are locked in the loop of eternity! ");
    printf("smash me:)", v4);
    gets(&s2);
}

```

dilihat bahwa setiap variabelnya sudah terdapat flag

doba dengan menggunakan gdb-peda dan lakukan break pada main agar dapat melihat utuh pada stack nya.

```

0000| 0x7fffffffef0c0 --> 0x7fffffffef210 --> 0x7fffffffef504 ("/home/flintz/Downlo
ads/smash")
0008| 0x7fffffffef0c8 --> 0x10000ffc2 = 'f';
0016| 0x7fffffffef0d0 ("secarmy{sm@sh1ng_st@ck_1s_t00_much_fun}")
0024| 0x7fffffffef0d8 ("sm@sh1ng_st@ck_1s_t00_much_fun")
0032| 0x7fffffffef0e0 ("_st@ck_1s_t00_much_fun")
0040| 0x7fffffffef0e8 ("s_t00_much_fun")
0048| 0x7fffffffef0f0 --> 0x7d6e75665f6863 ("ch fun") v4);
0056| 0x7fffffffef0f8 --> 0x555555555345 (<__libc_csu_init+69>: add    rbx,0x1)
Legend: in:code, data, rodata, value
0x0000555555555227 in main ()
gdb-peda$

```

Flag

secarmy{sm@sh1ng_st@ck_1s_t00_much_fun}

F-L-A-S-H

diberikan sebuah file ELF 64 , buka dengan IDA pro

[illegible]

diilihat lagi bahwa variabel sudah terdapat flag

coba dengan ltrace untuk melihat panjang dan isi dari flag nya

```
[flintz@shadow ~/Downloads]$ ltrace ./F-L-A-S-H
strlen("secarmy{7h1s_w45_345y_p34zy}") = 28
puts("_____")
_____ = 65
```

Flag

secarmy{7h1s_w45_345y_p34zy}

Backyard COWs

diberikan sebuah file ELF 64 , buka dengan IDA pro


```

"1. English\n2. My Native Language\n\nYour choice: ",
argv,
7074925467663627368LL,
3489497484834534505LL,
v6,
*(_QWORD *)&v7);
__isoc99_scanf("%d", &v9);
if ( v9 == 1 )
{
    puts("give me a number");
    __isoc99_scanf("%li", &v8);
    if ( v8 == 13337 )
    {
        puts("moo moo moo!!");
        for ( i = 0; i <= 20; ++i )
            putchar(*((_BYTE *)&v4 + i));
        putchar(10);
    }
    else if ( v8 > 999998 )
    {
        puts("-----");
        puts("< many Cows ,no flag >");
        puts("-----");
        puts("      ^ ^");
        puts("      (oo)\\");
        puts("      ( )\\");
        puts("      ||----w ||");
    }
}

```

diketahui terdapat kondisi pertama untuk memilih 1 dan kedua 13337 untuk mencetak variabel v4. Selain itu bukan hal penting :v
coba jalankan.

```

$ ./moo
< moo! select your language! >
-----
      ^ ^
      (oo)\\
      ( )\\
      ||----w ||

1. English
2. My Native Language

Your choice: 1
give me a number
13337
moo moo moo!!
http://bit.ly/m00_m00

```

I asked for the flag and she gave me this binary!
can you help me get my flag?

Author: z0m31en7

Download moo

Flag

Didapat sebuah link menuju googledrive berisi enkripsi sapi -_-
decode online pada <http://www.frank-buss.de/cow.html>

Program:

```
000Mo0Mo0Mo0Mo0Mo0Mo0Mo0Mo0MMmo0MMMMMMmo0MMMM00Mo0oMo0mo0moom0o
MMmo0MMMMMMmo0MMMM00Mo0oMo0mo0moom0oMMmo0MMMMMMmo0MMMM00Mo0o
Mo0mo0mo000mo0000m0om0oMMmo0MMMM00Mo0oMo0mo0moom0om0oMMmo0mo0
MMMM00Mo0mo0Mo0mo0moom0om0om0oMMmo0mo0mo0MMMM00Mo0oMo0mo0moom0o
Mo0Mo0Mo0Mo0mo0o000mo0000m0om0oMMmo0MMMM00Mo0oMo0mo0moom0om0oMM
mo0mo0MMMM00Mo0mo0Mo0mo0moom0om0Mo0Mo0Mo0Mo0Mo0mo0o000mo0000m0om0o
MMmo0MMMM00Mo0mo0Mo0mo0moom0om0oMMmo0mo0MMMM00Mo0oMo0mo0moom0o
Mo0Mo0Mo0Mo0mo0o000mo0000m0om0oMMmo0MMMM00Mo0oMo0mo0moom0om0oMM
mo0mo0MMMM00Mo0mo0Mo0mo0moom0om0Mo0Mo0mo0o000mo0000m0om0oMMmo0MMMM00
```

Click this button to execute the program:

Execute

Click this button to generate a COW program from the text in the result area below:

Generate

Result:

```
secarmy{d0_y0u_l1k3_c0w_languag3____?}
Done.
```

Flag

secarmy{d0_y0u_l1k3_c0w_languag3____?}

Cryptography

OTAN

diberikan sebuah text yang berisi sebuah enkripsi

```
[flintz@shadow] (~/.Downloads/hint)
$cat hint.txt
==UNIFORM GOLF ECHO CHARLIE TANGO OSCAR ALPHA PAPA CHARLIE VICTOR QUEBEK ROMEO J
ULIETT QUEBEK PAPA GOLF VICTOR KILO ECHO UNIFORM==
```

analisa dan didapat menggunakan enkripsi codegolf yang mengambil tiap huruf didepannya.

Coba decode pada <https://cryptii.com/pipes/nato-phonetic-alphabet>

ubah sedikit penulisan pada ALPHA menjadi alfa, dan QUEBEK menjadi quebec

VIEW	+	ENCODE DECODE	+	VIEW
Text ▾		Spelling alphabet ▾		Text ▾
UNIFORM GOLF ECHO CHARLIE TANGO OSCAR ALFA PAPA CHARLIE VICTOR QUEBEC ROMEO JULIETT QUEBEC PAPA GOLF VICTOR KILO ECHO UNIFORM		ALPHABET <input checked="" type="radio"/> NATO/ICAO phonetic alphabet <input type="radio"/> Dutch spelling alphabet <input type="radio"/> German spelling alphabet <input type="radio"/> Swedish Armed Forces' radio alphabet		ugectoapcvqrjqpgvkeu

hmm ini mungkin sebuah caesar chiper, coba saja

N:

ugectoapcvqrjqpgvkeu

This is your encoded or decoded text:

Flag

secarmy{natophonetics}

Exchange

diberikan sebuah file text

```
[flintz@shadow]--[~/Downloads]
$cat imp_file
Well I only know this :-TRCSUED{C3HH_TDET010D034}
```

setelah melalui perjalanan panjang diketahui bahwa itu adalah substitusi chipper
coba pada <https://quipqiup.com/> . Dan coba berbagai cara dengan mengacu pada flag awal
SECARMY dan juga mengubah angka sementara seperti 3=E, 1=I agar didapat flag yang
mudah dibaca

TRC SUED{CEHH_TDET010D0EA}

Clues: For example G=R QVW=THE

T=S R=E S=A U=R E=M E=E I=I

0 -2.716 SE CARED{ CELL_S DESTITD TEN}

1 -2.718 SEW AREU{WELL_SUESTITUTED}

Flag

secarmy{w3ll_subst1tut34}

SQUARE

didapat sebuah gambar qr code



decode dan didapat sebuah string

43 15 13 11 42 32 54 { 41 42 _ 25 33 0 52 3_ 44 23 3_ 52 @ 54 }

diketahui enkripsi menggunakan polybius square, decode dengan online pada

<https://cryptii.com/pipes/polybius-square>

VIEW	ENCODE DECODE	VIEW
Ciphertext ▾	Polybius square ▾	Plaintext ▾
43 15 13 11 42 32 54 { 41 42 _ 25 33 0 52 3_ 44 23 3_ 52 @ 54 }	ALPHABET abcdefghijklmnopqrstuvwxyz	secarmy{qr_kn0w_orn_w@y}
	ROWS 12345	COLUMNS 12345
	SEPARATOR	

Flag

secarmy{qr kn0w orn w@y}

Flag Basket

Ch wigjonyl mywolcns, u buweyl cm migyihy qbi ziwomym ih mywolcns gywbuhcmgm iz wigjonyl uhx jfuszof{hyn_qile_msm_nygm}. Qbcfy chwfoxcha nbimy qbi yhxypul ni mnlyhanbyh mowbaln{gywb_u_hcmg}, cn cm gily iznyh omyx vs nby gumm gyxcu uhx jijoful alyunij{wof_noly} ni lyzyl ni nbimy qbi myye uwwymm xymjcnv nbymy mywolcns gyumolym. Nbn cm, nby gyxcu jilnlusm nby 'buweyl' um u pcffuch. xisioeg{Hypyl_nby_fymm}, julnm iz nby movwofnoly myy nbycl ucg ch willywncha mywolcns hinbyly{jli_vfy_gm} uhx omy nby qilx ch u jimncpy myhmy. Qbcny bun cm nby hugy acpyh ni ynbcwuf wigjonyl buweylm, qbi oncfcty buwecha ch u eyimnvs{byfj_zof} qus. Qbcny bunm uly vywigcha u hywymms juln iz nby chzilguncih mywolcns zcyfx. Gimn cgjilnuhnfs, byly cm siol zfua mywulgs{IWL_c5_fcn} Nbys ijyluny ohxyl u wixy, qbcwb uwehiqfyxaym nbn vlyuecha chni inbyl jyijfy'm wigjonylm cm vux, von nbn xcmwipylcha uhx fifzfua{yrj_ficn_cha} mywolcns gywbuhcmgm uhx vlyuecha chni wigjonylm cm mncff uh bylyoai{chnylymn_cha} uwnpcns nbn wuh vy xihy ynbcwuffs uhx fyauffs. Uwwilxchafs, nby nylg vyulm mnlia ulgsymw{wihh_inun_cihm} nbn uly zupiluvfy il jydiluncpy, xyjyhxcha ih nby wihnyrn.

didapat sebuah gambar dengan text seperti caesar chipper , coba geser pada rumkin

N: 6 ▼

Ch wigjonyl mywolcns, u buweyl cm migyihy qbi ziwomym ih mywolcns gywbuhcmgm iz wigjonyl uhx jfuszof{hyn_qile_msm_nygm}. Qbcfy chwfoxcha nbimy qbi yhxypul ni mnlyhanbyh mowbaln{gywb_u_hcmg}, cn cm gily iznyh omyx vs nby gumm gyxcu uhx jijoful alyunij{wof_noly} ni lyzyl ni nbimy qbi myye uwwymm xymjcnv nbymy mywolcns

This is your encoded or decoded text:

In computer security, a hacker is someone who focuses on security mechanisms of computer and playful{net_work_sys_tems}. While including those who endeavor to strengthen suchgrt{mech_a_nism}, it is more often used by the mass media and popular greatop{cul_ture} to refer to those who seek access despite these security measures That is, the media portrays the 'hacke!' as a villain. doyoukm{Never_the_less}. parts of the subculture see their aim in correcting security nothere{oro_ble_ms} and use the word in a positive sense. White hat is the name given to ethical computer hackers, who utilize hacking in a keostby{help_ful} way. White hats are becoming a necessary part of the information sebcurity field. Most importantly, here is your flag secarmy{OCR_i5_lit} They perate under a code, which acknowledges that breaking into other people's computers is bad but that discovering and lolflag{exp_loit_ing} security mechanisms and breaking into computers is still an hereugo{interest_ing} activity that can be done ethically and legally. Accordingly, the term bears strong armiesclconn_otat_ions that are favorable or pejorative, deoending on the context.

flag ada diantara kalimat tersebut

Flag

secarmy{OCR_i5_lit}

Exclusive OR Non-Exclusive

didapat sebuah file text berisi hex code

190f090b18071311125a1835035f35080b5f0309350c5a183559040918131a1e035a045f17

sesuai dengan hint yang ada, coba dilakukan bruteforce XOR didapat flag

```
102 10m~auwt<~se9Snm9e0sJ<~s?d0~u|x<b9q
103 ~hnl`tvu=Rd8Rol8dnRk=R>cnt}yd=c8p
104 qgacpo{yz2p]k7]}c7ka]d2p]llap{rvk2l7
105 pf`bqnzx{3q\j6\ab6j`\e3q\0m`qzswj3m6~
106 secarmy{x0r_i5_ba5ic_f0r_3ncrypti0n5}
107 rdb`slxzyls^h4^c^4hb^gls^2obsxquh1o4|
```

Flag

```
secarmy{x0r_i5_ba5ic_f0r_3ncrypti0n5}
```

The 3ASY

diberikan file zip yang diextract berisi sebuah text

[illegible]

diketahui plaint text tersebut menggunakan 3 enkripsi.

pertama merupakan polybius square, kedua adalah trifid chiper, dan terakhir pastinya adalah morse code

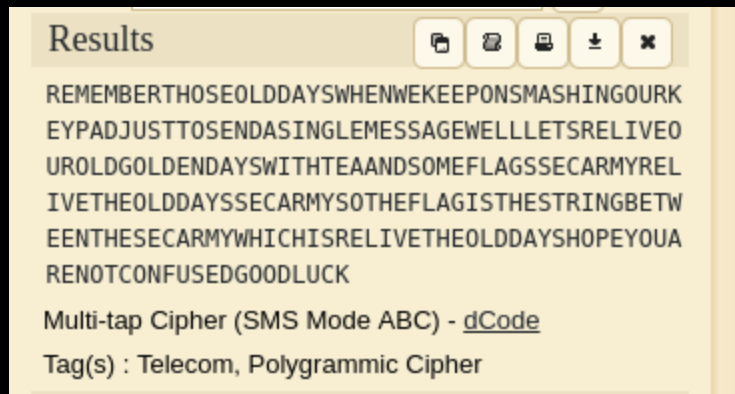
decode semuanya dan akan menghasilkan string

kaaaakaaaaaaakaaaaakakkkakkaaaaaaakaaaaaaaaakaakkaakakaaaakakaakakaakakaaaaaa
aakk

jika diperhatikan chipper tersebut adalah baconian

*

diketahui enkripsi menggunakan Multi-tap Cipher, decode online pada <https://www.dcode.fr/multitap-abc-cipher>






Flag

secarmy{relivetheolddays}

Rivest Shamir Adelman

Diberikan sebuah encrypt.py , encrypt_flag.png dan private key

 encrypt.py	16/08/2019 13:12	Python File	1 KB
 encrypted_flag.png	16/08/2019 13:12	PNG image	19 KB
 private_key.pem	16/08/2019 13:12	PEM File	4 KB

Berikut encrypt :

```
from Crypto.PublicKey import RSA
from Crypto.Cipher import PKCS1_OAEP
import zlib
import base64

def encrypt_blob(blob, public_key):
    rsa_key = RSA.importKey(public_key)
    rsa_cipher = PKCS1_OAEP.new(rsa_key)
    blob = zlib.compress(blob)
    chunk_size = 470
    offset = 0
```

```

end_loop = False
encrypted = ""
while not end_loop:
    chunk = blob[offset:offset + chunk_size]
    if len(chunk) % chunk_size != 0:
        end_loop = True
        chunk += " " * (chunk_size - len(chunk))
    encrypted += rsa_key.encrypt(chunk)
    offset += chunk_size
return base64.b64encode(encrypted)

fd = open("public_key.pem", "rb")
public_key = fd.read()
fd.close()
fd = open("flag.png", "rb")
unencrypted_blob = fd.read()
fd.close()
encrypted_blob = encrypt_blob(unencrypted_blob, public_key)
fd = open("encrypted_flag.png", "wb")
fd.write(encrypted_blob)
fd.close()

```

Berikut private key

```

-----BEGIN RSA PRIVATE KEY-----
MIIJKAIBAAKCAgEAoOIJQ2VsT4Im6LJHA4n9kox/AH75Q3i7bUQO44N5rKKIO6kU
a9HoBfwZ+Zo9gp4bsrNdpD4LKRh44sTABZK5CqhUHYFiJfcqC5rzPwwF5zzTMKq/
fVswuZvK480QtrMFYUV3o+WtFhscLHDbDfMiZVyf1ks7ILBayFNmVPs7L6M+IKJi
cq6pZ/qEMKNvQf37JRofPspoPQE2be6A7KfckFy0XIsZnDVQf3Lz1Qlcw1ulRyo5
Liruo0vEY7IUSrbU0PWYowN1z+kmHOk6+zpcfQod4xkAPbs1hymYWgXflu0fmw7a
ZToMgD+7M1B1SKeNq3Pa0GleAVSNGGW1A5xEcfkAmu4ZIEhHqNWwG8caoP3mtuw+
yU7GhHJV81jNz5qZru4F8gEGWR3ngyGfCCiNeQt/B103m1pWayW29rAkUqKmyKL3
VesmQwoJBeT7xUbs3Z/iGfj5x6CkgI7YVR7qWmfO3e5OMmn5h0ZHKFgTUsanb6+S
1JRDTpT/XtYO7ha44PEHwgi/VVXVs50fzE5CN/wFmmm3A4hPGA/QyeNOsDcNbwdn
RRo7NX2W/EibCfQMX/e3m/TqcF9EmQnqCEA4WhcOtYWSUU6+b1xXM9kmK8B4Fa1h
/vZasOkE0XYgS2HHDrrBBml+v1qwy/HAK5a+MuqcW8wJRcJaGnpCfZQHDn1ECAwEA
AQKCAgBZluXPqRgSgojGRhiziNEzHZfPn+WQxBejNiYQXfOQxgWVK4earw5E3ulc
DJ86MG9+KNH5ly9B2EXhCe1gbR8sJyalM7eDKss4ITZZomW3ajC0xjDSTsioY3At
QNGQ28ogK73+//RN/hUBOINTIiROG7FKdSSdnUNAkOjIzArGcWIObBjkgg0GQQQB
zdEz74o+U/iYT8CSUC2ONCWJl8T4gxdQ/YjqauoDwvC3anC3/T3hjq/QdsYBiY7
2jvgi0Whg1JXXKLrf4rgyKQ2qH4/bt4ry41N0wVw2iHj56dl9XAHOdM2UYgKlvLZ
FXHqXpvOoTp1lI3dlceWe4y8kPWvm7zAxfl43ZIQgtl3AczOsjv5CMIApgyLJHMA
KoR/N3CTMaSTY2pMtn/SUu+csNptRXenY5uKnQ8JjzvYEypK+CFae4UK5QEhrieV
dS1QiEcDaXmKhdzXlrIB497v2cRJGNL9QMvkUIYepPt/8PHOu2nPW8KPyEBnecAq
m0E+0S9m98zrmBIIT05l16wJrsXIQWrAzriSC0Qm82noWerfLnRDC5r9r0cnGk8K

```

```
qQYJHSLck0JG8KnWy/YspmzhSi16dBvgD+3y7aMWZVjg8K0WXzpYz2PioPsavtRT
7pwd3SyysEbAr/acOchglDn/BV6wnofp0kEm2NA6VwceGI0o3QKCAQEAwDZoGJrF
a3o4BlpcwwjrGuxCgmoTwZJ4cB91uy6NRRtIQf2Ubc0rkjx26+mulqCBFvzcbzwf8
vVNrcKwSU15Y1UED6o7M9mXCWKE+HyWpebHiprwWN0FpuLOWwtjClbuSXsNGwKDe
kLoSS1XIVz7e1KnwV7xQha8Uz3JvHHKLYBZ0OAAE3LISB0yYYUrOwQQueDtulm3p
xjNyFKb+3+ANRxHenAK+VruLwklXupjb2GwwpJ262IQI1I9zaoD1zDJale48FX7M
4uSkTzMPjNjPshmGwM6QR5P3Stwrx7/4vC3DlrTmf6inixld52kvLxCqyjNPtjZi
LiDsgHXXA7s4pwKCAQEA1kX/KLlsgt+Q1nKuwQnUXXMZFY/QrqJCiJzbuk6yIVOB
/kFKJFFGBFRAobDvjmKJh6kaLEo3tgkTg8MA7tuqB1Ybf+UB2KwOo775rUBnXdAO
3tKjcU7QZt39maCU83QxQSQSN5EUJxDCWemzUaBipxAWf34M2BhHTxNQUiqvOe7u
uVqLU2Wopk/jAr9eZ4QffjhT7MDM6CISgD1GPbylmFhtfpPYZDEPoyv+Yk1j7FVD
aCAECY9LrfX08ZrAflxBFJDQHL+/y9ikfRt0o9vlquHmiDSNS66ag+jO9n5ezR2O
t+3ZUkRHzBXf7ZNZE2uuzKka5y+byBAJ2YzMFNXvRwKCAQEAkVMRVTj/dolLfpIn
fFzr20kx6ARnt30UjkFa9BD4Q8ljK863+G1xbTtfOSLWds0frjrtz5QMZOCDZQbU
PDAjHekwGtGo6cp6LCSNIWOKRTZXVRTz/wb39eviWqMkS60rt3YRMmbun6HvXwls
idBBDa0GyG7auphrNYUhuPJPqlaPvB9Xjb0coGQq+bRjqdR3oPpEYuHrVC1IXXP9
VCrEHy3Fj1MLsevOeTCWocAcx/7UsEGJGVagfPph+u5R6PdRQfaDewUJx6pzCGZk
pWrvbYqbNX932oZm/DSG7VmZqD05Qi5f77kGI8Go1mPSfcKGPqaY5/0qMhI2fdGa
pXmSFQKCAQA22jpkqXse0a6ZR0h3QFXuCk3smCFa40zW/hi9y/GpinQnq30zClc9
Cnh1K/9XWuBMKzz5A5LZdd9aBqyReQhA0ok9p1lep0Ukl/p0oJ0VhfKYliGjGwL8
om2OS252GFOXkm1bbjdTfNXUAKCYD8/RZqvrU/6bdSral1SS30J/qF8L7KICcwv
rxm1FVpMc6VAQZkybXTHJBnKXGVD3qS1I0X8dkqZ83IGUzfO4HLpCDa2TCPccqN0
CBfJVc1a1OjAJAYypd+qhm4tXL7yR5O2uBe03lcjTbJefFWnAliwd5WWfjv49GPQ
2fS2M9dEwndACzZl4oYlo/1xhLqlxtJ3AoIBAEzteqoh2a5YiUOcMq4vNOymwJh1
2+u8+YN/0Xjb+q10IJ2nHJ19zD2D+/R0+KySTYtZmVcsoToTkGJjWQiBB615RF9S
veLkL7TJsG2tLldz0V7uS+vR/u9gaFoGt5tvLzrpzuqdaqxmFO+tn0ueevxyavBT
ewQQLiSbxBR/FICchg7q0a3VTLHCBCdJCnj7XYkaazZEKrhmw2itghN0wilBHVjm
Sm/uJI095w3pW4KQNPav69ygvfcL3bk2XHbn6Fa+zoWpMWlu3EN1PaNrQfSVKEfg
vXUe9t6MuTVJP6Jj9iER0/h+5kMFNP5A8IEsQGJh6s/jrSICC3RP3SveDWA=
-----END RSA PRIVATE KEY-----
```

Jalankan script berikut :

```
from Crypto.PublicKey import RSA
from Crypto.Cipher import PKCS1_OAEP
import base64
import zlib

def decrypt_blob(encrypted_blob, private_key):

    rsakey = RSA.importKey(private_key)
    rsakey = PKCS1_OAEP.new(rsakey)

    encrypted_blob = base64.b64decode(encrypted_blob)
```

```

chunk_size = 512
offset = 0
decrypted = ""

while offset < len(encrypted_blob):
    chunk = encrypted_blob[offset: offset + chunk_size]
    decrypted += rsakey.decrypt(chunk)
    offset += chunk_size

return zlib.decompress(decrypted)

fd = open("private_key.pem", "rb")
private_key = fd.read()
fd.close()

fd = open("encrypted_flag.png", "rb")
encrypted_blob = fd.read()
fd.close()

fd = open("hasil.jpg", "wb")
fd.write(decrypt_blob(encrypted_blob, private_key))
fd.close()

```

Dan didapatkan :



Flag

Secarmy{RSA_ba51c5_to_be_l3arn7}

NB:

Terima Kasih untuk Akinari, ZheeK, Flintz, Noid3a, Nesc udah berpartisipasi dengan teamnya masing masing