Writeup CTF CHRIST (Deemed to be University)

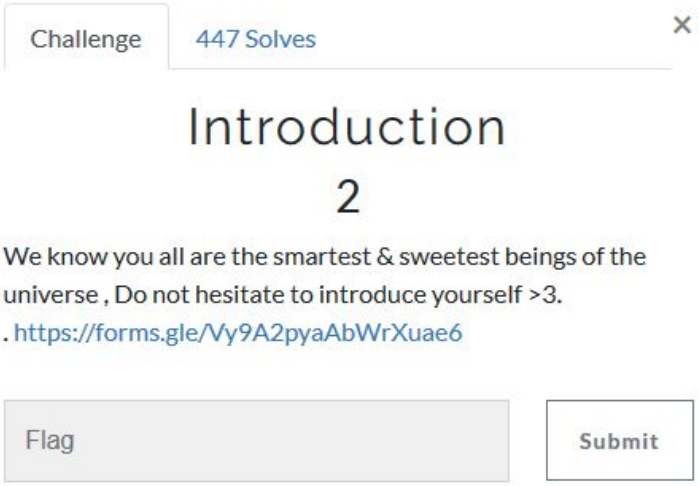
[Hightech - KKN Back To Isekai]

Daftar Isi

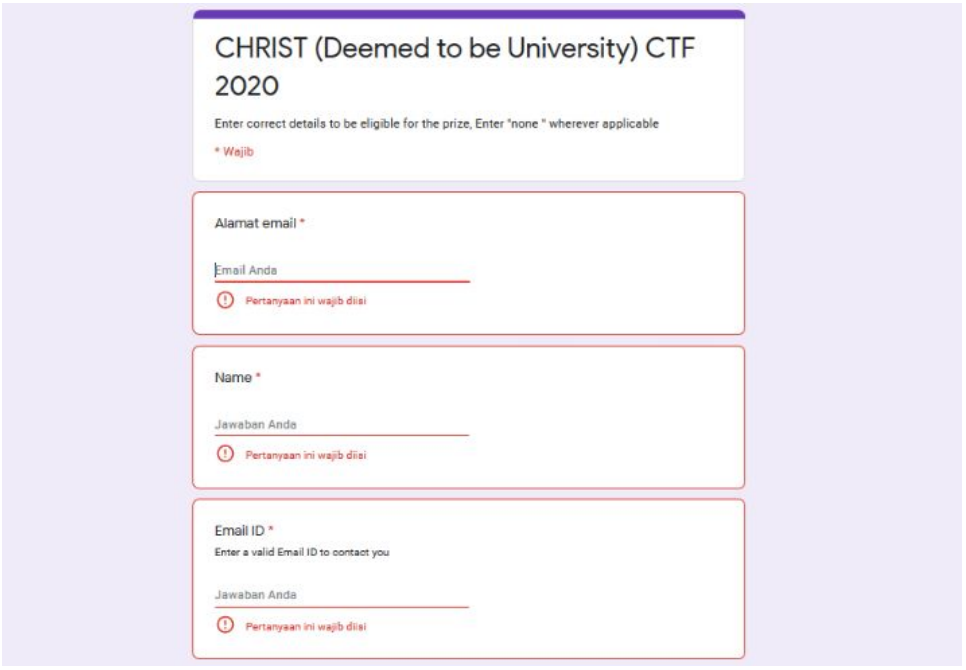
Write Up

From Isekai, With Love

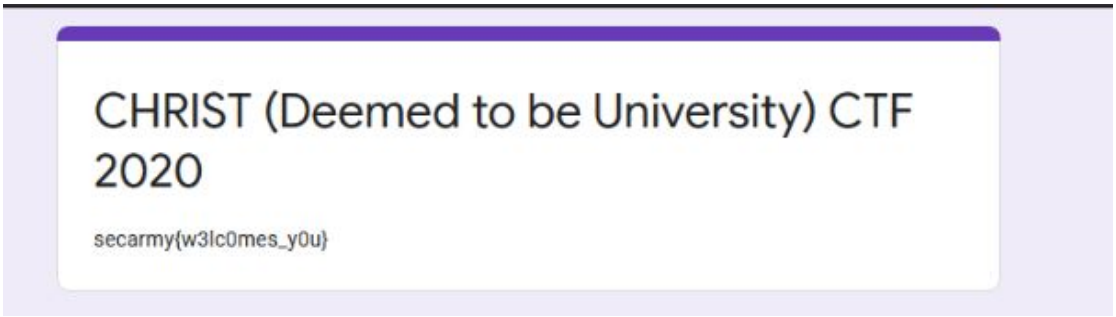
1. [Welcome] - Introductions [10]



Diberikan sebuah Challenge sebagai berikut, dimana flagnya akan muncul setelah melengkapi data didalam google forms tersebut.



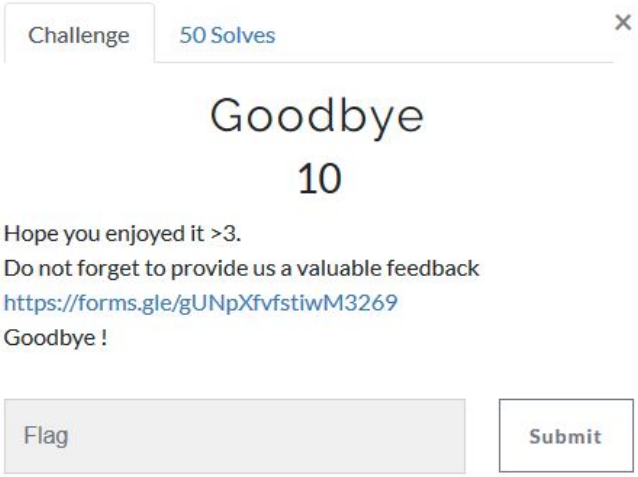
Setelah saya mengisi form dengan lengkap, maka flagnya pun akan muncul.



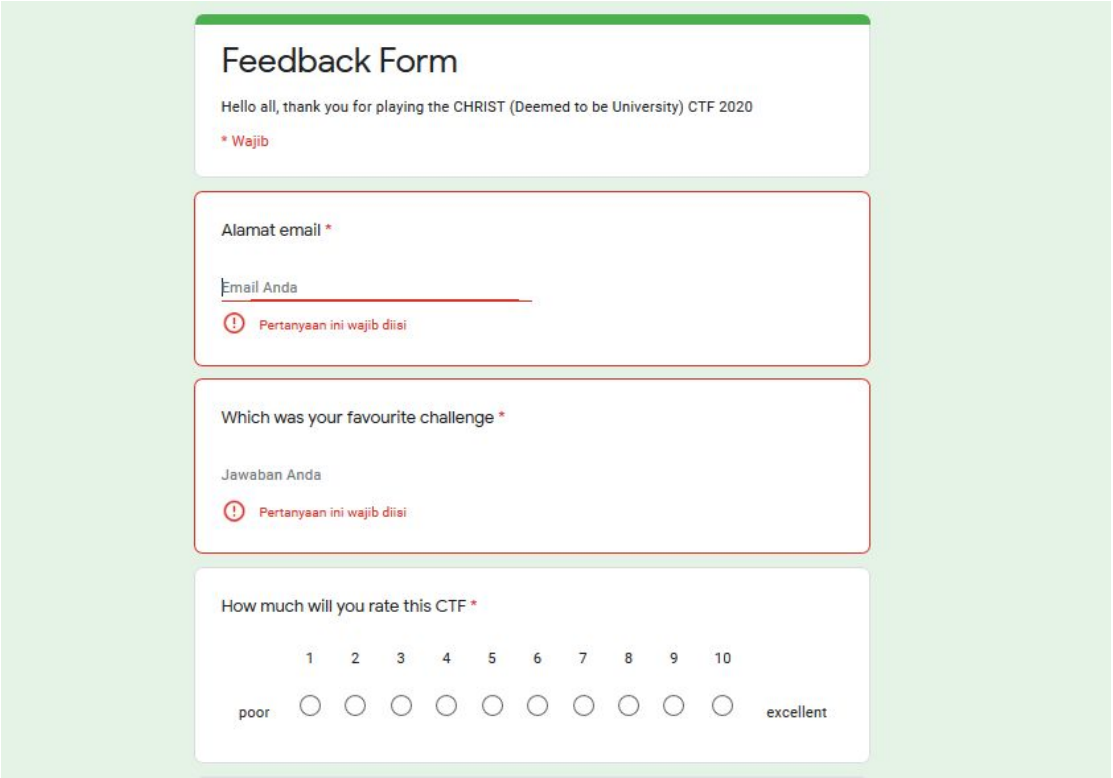
Flag:

secarmy{w3lc0mes_y0u}

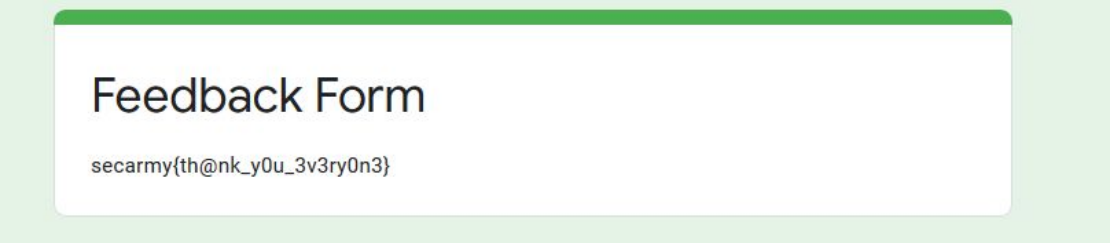
2. [Goodbye] - Goodbye [10]



Diberikan sebuah Challenge sebagai berikut, dimana flagnya akan muncul setelah melengkapi data didalam google forms tersebut.



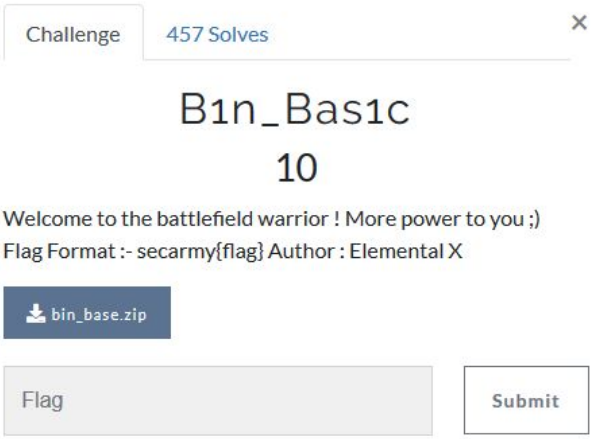
Setelah saya mengisi form dengan lengkap, maka flagnya pun akan muncul.



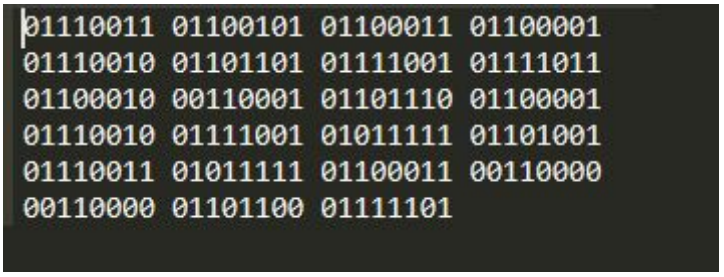
Flag:

secarmy{th@nk_y0u_3v3ry0n3}

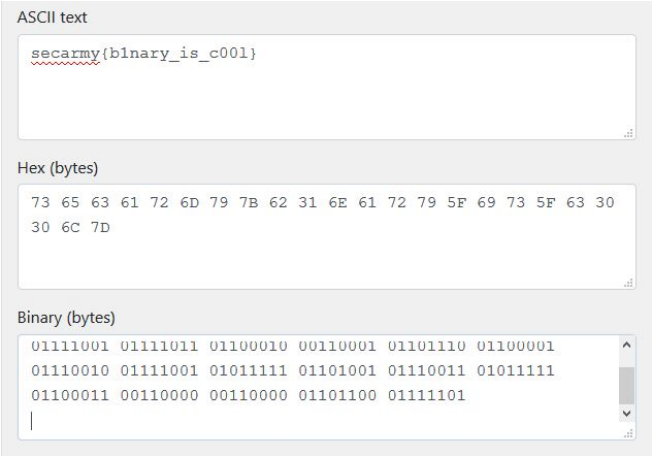
3. [Starters] - B1n_B4s1c [10]



Diberikan sebuah Challenge sebagai berikut, file zip tersebut berisikan file **"flag.txt"**



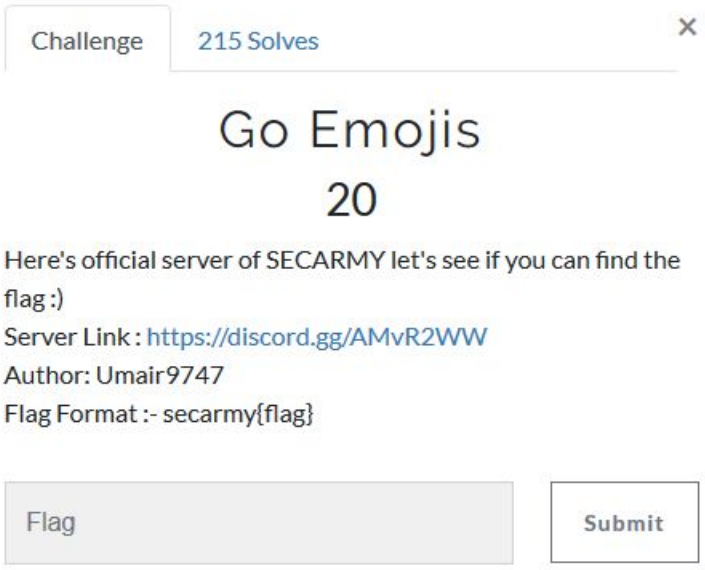
isi dari **"flag.txt"** adalah sebuah bilangan biner, maka saya pun mencoba untuk melakukan convert dari biner ke text



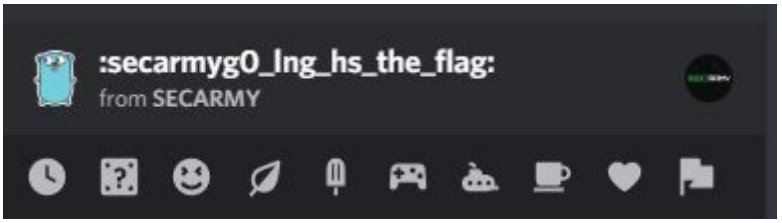
Flag:

secarmy{b1nary_is_c00l}

4. [Starters] - Go Emoji [200]



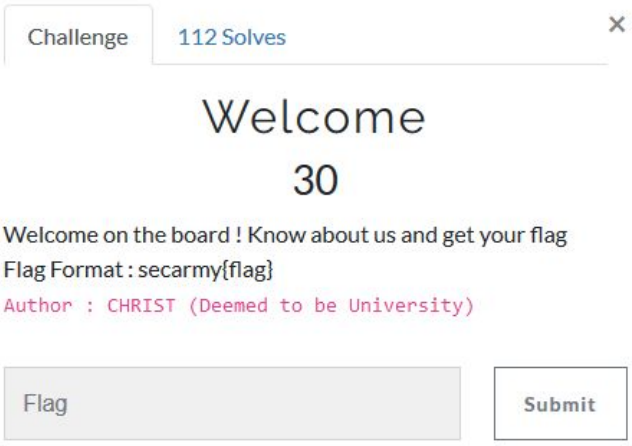
Disini saya membuka link discord tersebut dan mencari emoji dari Go sesuai dr Clue yang ada dan ternyata ketemu.



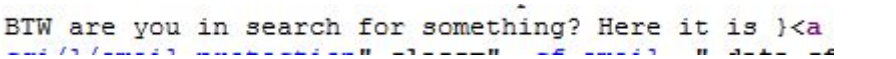
Flag:

secarmy{g0_ln_hs_the_flag}

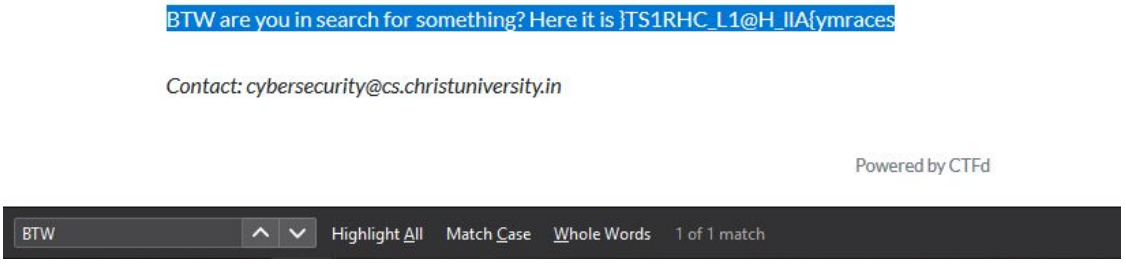
5. [Starters] - Welcome [30]



Dari Challenge ini, perhatian saya tertuju pada page About, lalu saya mengexplore page about tersebut.



Berdasarkan clue diatas, saya mencoba melakukan search di halaman About tadi menggunakan keyword **"BTW"**.



Dan ternyata ketemu, namun ternyata flagnya itu masih harus dibalik sehingga menjadi seperti ini

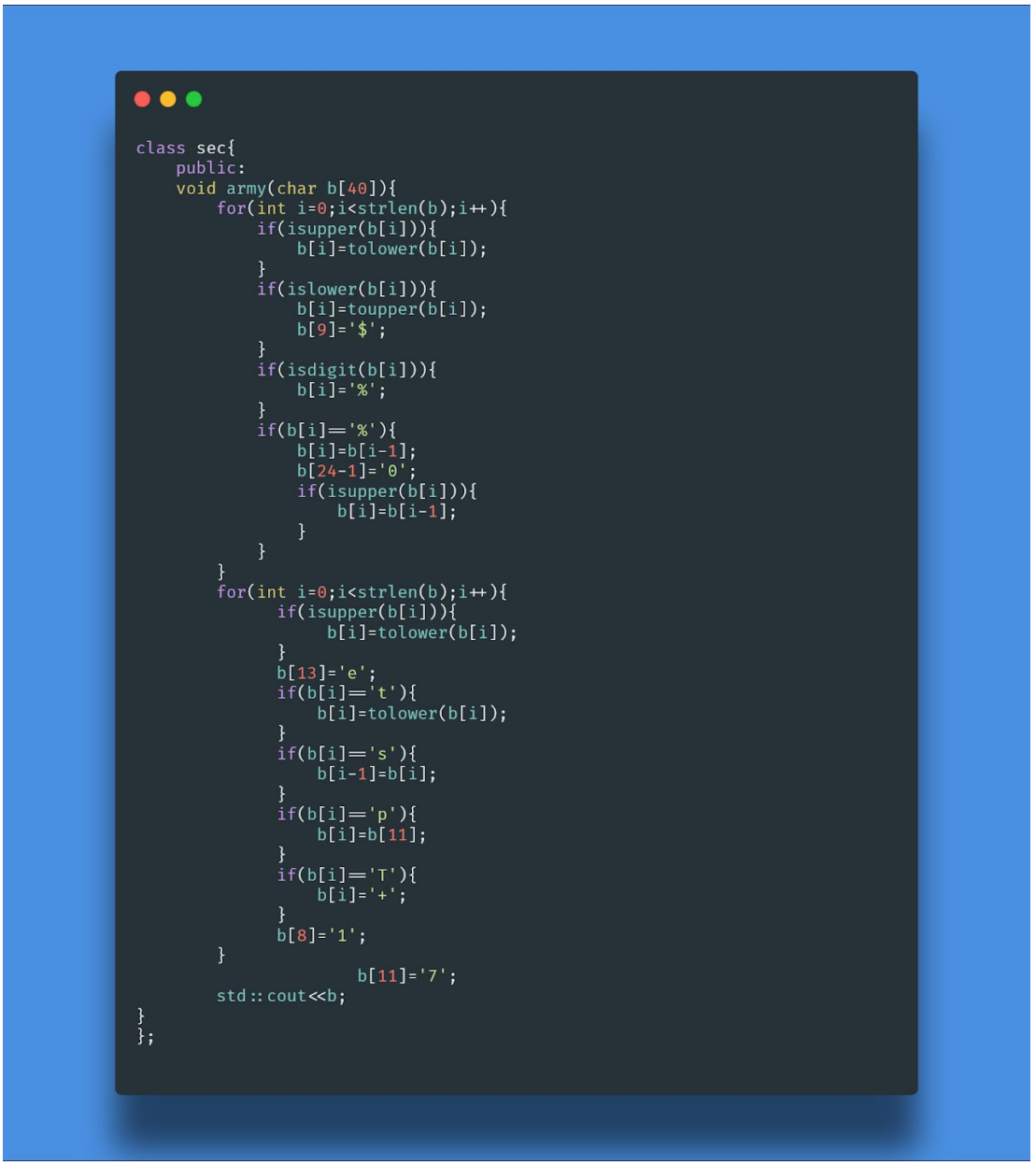
Flag:

secarmy{All_H@1L_CHR1ST}

6. [Programming] - SEC++ [30]

Diberikan sebuah challenge seperti ini, isi dari file zipnya adalah sebuah script **C++** namun masih belum sempurna,

Isi dari scriptnya bisa dilihat dibawah ini.



```
class sec{
    public:
    void army(char b[40]){
        for(int i=0;i<strlen(b);i++){
            if(isupper(b[i])){
                b[i]=tolower(b[i]);
            }
            if(islower(b[i])){
                b[i]=toupper(b[i]);
                b[9]='$';
            }
            if(isdigit(b[i])){
                b[i]='%';
            }
            if(b[i]=='%'){
                b[i]=b[i-1];
                b[24-1]='0';
                if(isupper(b[i])){
                    b[i]=b[i-1];
                }
            }
        }
        for(int i=0;i<strlen(b);i++){
              if(isupper(b[i])){
                  b[i]=tolower(b[i]);
              }
              b[13]='e';
              if(b[i]=='t'){
                  b[i]=tolower(b[i]);
              }
              if(b[i]=='s'){
                  b[i-1]=b[i];
              }
              if(b[i]=='p'){
                  b[i]=b[11];
              }
              if(b[i]=='T'){
                  b[i]='+';
              }
              b[8]='1';
        }
                    b[11]='7';
        std::cout<<b;
}
};
```

Dari script diatas, saya pun melakukan perubahan serta perbaikan agar script bisa dieksekusi dengan

sempurna. Script yang sudah dirubah bisa dilihat dibawah ini.

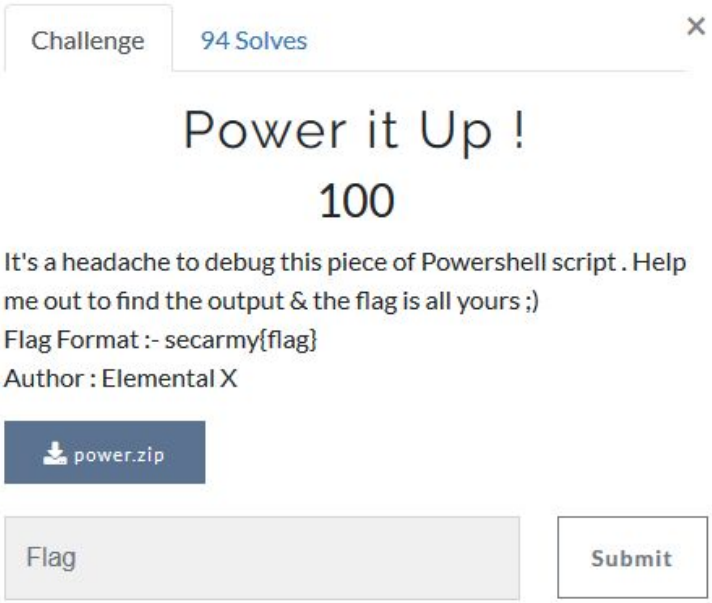
```cpp
#include <iostream>
#include <string.h>

class sec{
    public:
    void army(char b[40]){
        for(int i=0;i<strlen(b);i++){
            if(isupper(b[i])){
                b[i]=tolower(b[i]);
            }
            if(islower(b[i])){
                b[i]=toupper(b[i]);
                b[9]='$';
            }
            if(isdigit(b[i])){
                b[i]='%';
            }
            if(b[i]=='%'){
                b[i]=b[i-1];
                b[24-1]='0';
                if(isupper(b[i])){
                    b[i]=b[i-1];
                }
            }
        }
        for(int i=0;i<strlen(b);i++){
              if(isupper(b[i])){
                  b[i]=tolower(b[i]);
              }
              b[13]='e';
              if(b[i]=='t'){
                  b[i]=tolower(b[i]);
              }
              if(b[i]=='s'){
                  b[i-1]=b[i];
              }
              if(b[i]=='p'){
                  b[i]=b[11];
              }
              if(b[i]=='T'){
                  b[i]='+';
              }
              b[8]='1';
        }
                      b[11]='7';
        std::cout<<b;
}
};
int main(){
    sec gaskeun;
    char b[] = "SECARMY{cpp_1s_TH3_W@Y_T0_G0}";
    gaskeun.army(b);
    return 0;
}
```

Dan setelah melakukan perbaikan, saya pun melakukan compile dan running terhadap script yang sudah dirubah sehingga hasilnya menjadi seperti ini

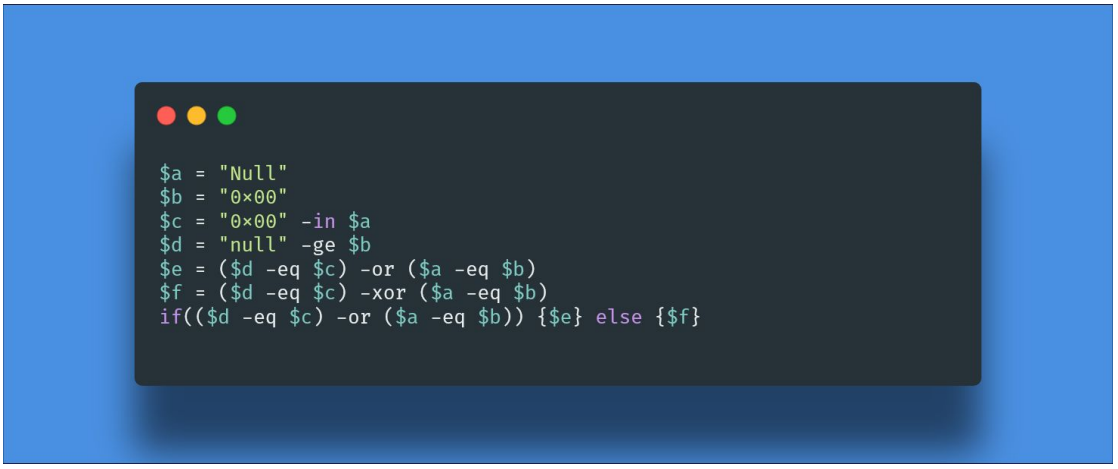
Flag:

secarmy{1$_7_e_thh_w@y_00_gg}

7. [Programming] - Power it Up! [100]

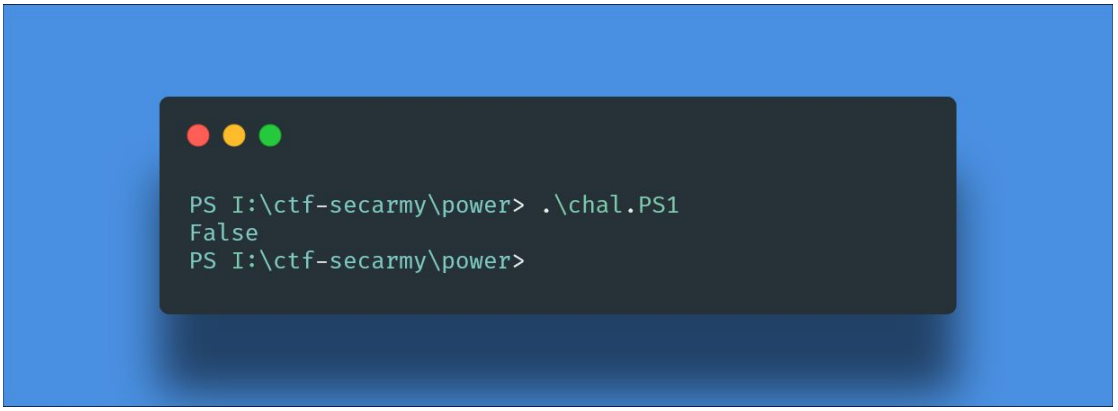


Diberikan sebuah Challenge sebagai berikut, Isi file zip tersebut adalah sebuah powershell script yang berisikan seperti dibawah ini.



```
$a = "Null"
$b = "0×00"
$c = "0×00" -in $a
$d = "null" -ge $b
$e = ($d -eq $c) -or ($a -eq $b)
$f = ($d -eq $c) -xor ($a -eq $b)
if(($d -eq $c) -or ($a -eq $b)) {$e} else {$f}
```

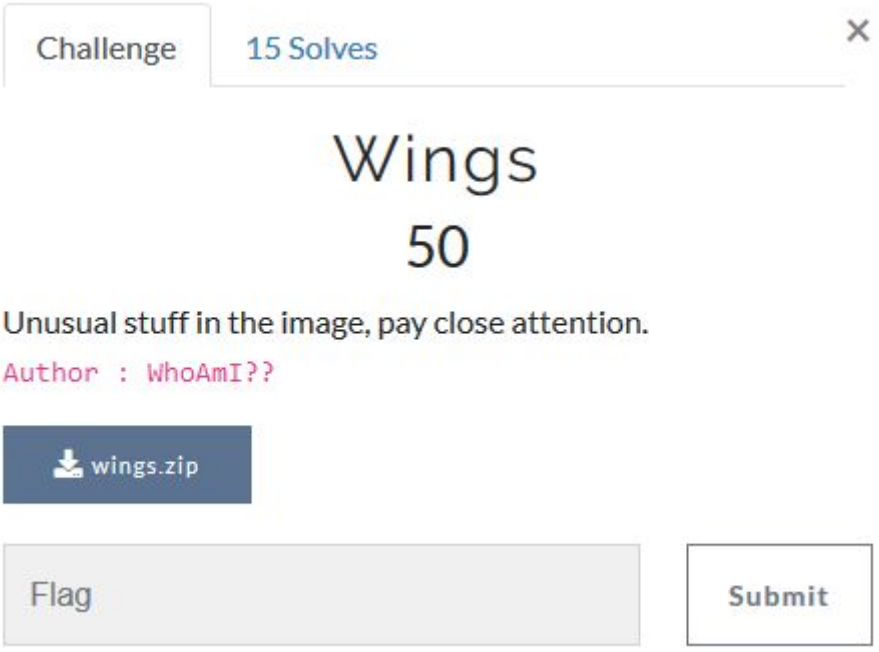
Tugas kita adalah mengetahui apa output dari script tersebut, lalu saya mencoba running script tersebut di powershell saya. dan hasilnya adalah seperti ini, awalnya saya sempat terkecoh karna hasilnya adalah "**False**" namun berhubung kita diminta mengetahui outputnya maka saya mencoba submit flag tsb dan sukses.



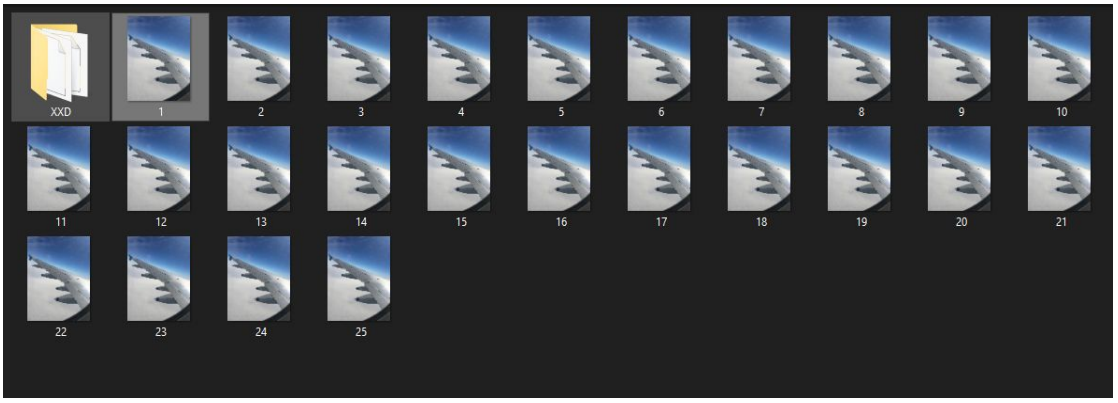
Flag:

secarmy{False}

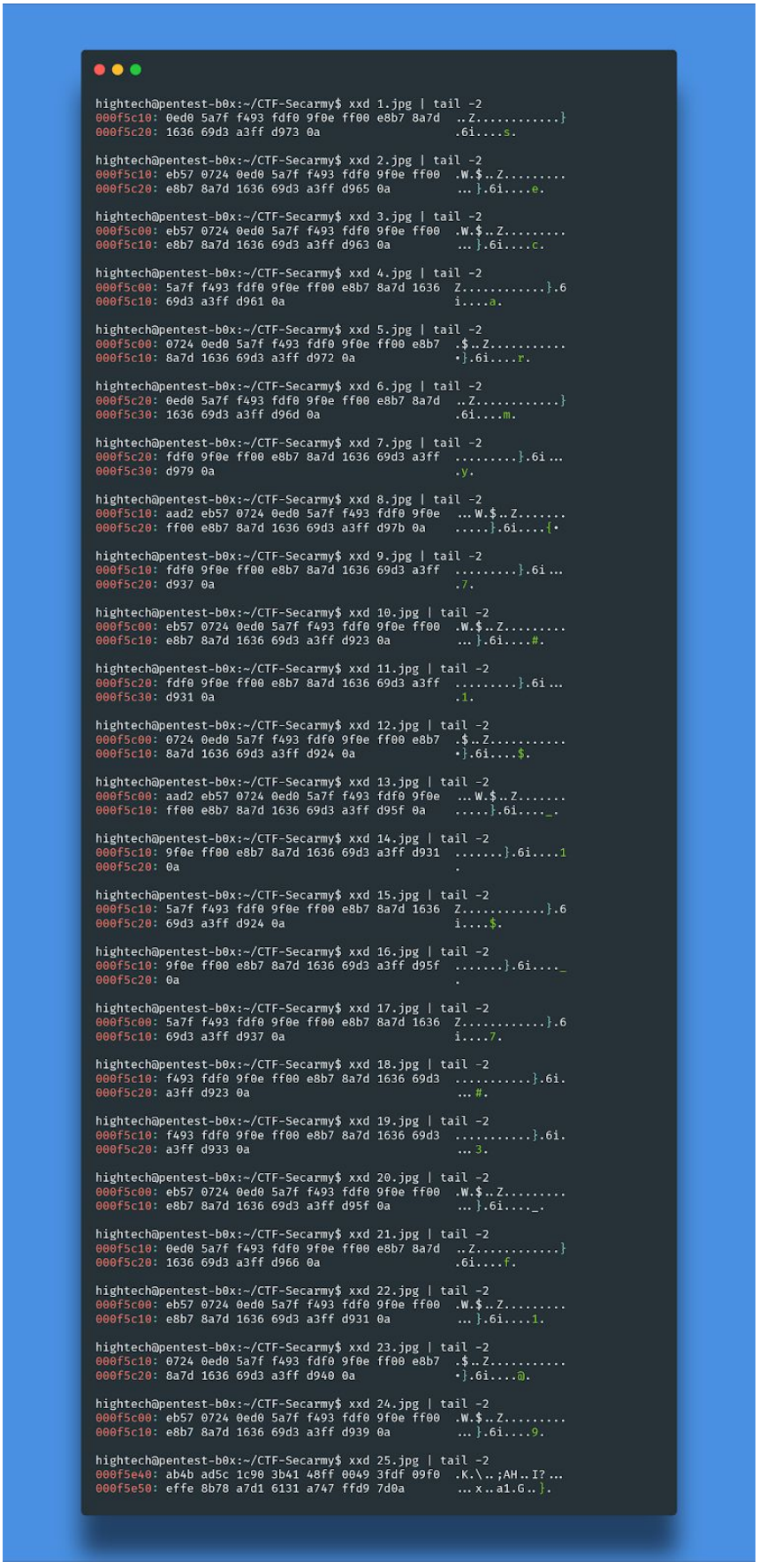
8. [Steganography] - Wings [50]



Diberikan challenge sebagai berikut, Isi dari file zipnya adalah 25 Gambar JPG yang terlihat sama.



Saya mencoba berbagai cara steganography untuk mendapatkan flag namun gagal. Hingga akhirnya saya mencoba bermain menggunakan **XXD dan Tails** menemukan sebuah perbedaan berdasarkan clue dari Challenge yang mengharuskan teliti.

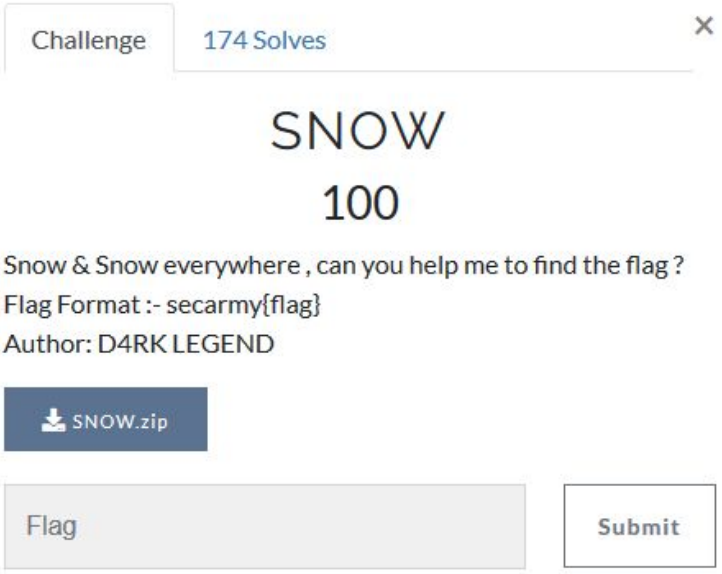

hightech@pentest-b0x:~/CTF-Secarmy$ xxd 1.jpg | tail -2
000f5c10: 0ed0 5a7f f493 fdf0 9f0e ff00 e8b7 8a7d ..Z............}
000f5c20: 1636 69d3 a3ff d973 0a   .6i....s.
hightech@pentest-b0x:~/CTF-Secarmy$ xxd 2.jpg | tail -2
000f5c10: eb57 0724 0ed0 5a7f f493 fdf0 9f0e ff00 .W.$..Z.........
000f5c20: e8b7 8a7d 1636 69d3 a3ff d965 0a   ...}.6i....e.
hightech@pentest-b0x:~/CTF-Secarmy$ xxd 3.jpg | tail -2
000f5c00: eb57 0724 0ed0 5a7f f493 fdf0 9f0e ff00 .W.$..Z.........
000f5c10: e8b7 8a7d 1636 69d3 a3ff d963 0a   ...}.6i....c.
hightech@pentest-b0x:~/CTF-Secarmy$ xxd 4.jpg | tail -2
000f5c00: 5a7f f493 fdf0 9f0e ff00 e8b7 8a7d 1636 Z............}.6
000f5c10: 69d3 a3ff d961 0a   i....a.
hightech@pentest-b0x:~/CTF-Secarmy$ xxd 5.jpg | tail -2
000f5c00: 0724 0ed0 5a7f f493 fdf0 9f0e ff00 e8b7 .$..Z...........
000f5c10: 8a7d 1636 69d3 a3ff d972 0a   .}.6i....r.
hightech@pentest-b0x:~/CTF-Secarmy$ xxd 6.jpg | tail -2
000f5c20: 0ed0 5a7f f493 fdf0 9f0e ff00 e8b7 8a7d ..Z............}
000f5c30: 1636 69d3 a3ff d96d 0a   .6i....m.
hightech@pentest-b0x:~/CTF-Secarmy$ xxd 7.jpg | tail -2
000f5c20: fdf0 9f0e ff00 e8b7 8a7d 1636 69d3 a3ff ....}.6i...
000f5c30: d979 0a   .y.
hightech@pentest-b0x:~/CTF-Secarmy$ xxd 8.jpg | tail -2
000f5c10: aad2 eb57 0724 0ed0 5a7f f493 fdf0 9f0e ...W.$..Z.......
000f5c20: ff00 e8b7 8a7d 1636 69d3 a3ff d97b 0a   .....}.6i....{.
hightech@pentest-b0x:~/CTF-Secarmy$ xxd 9.jpg | tail -2
000f5c10: fdf0 9f0e ff00 e8b7 8a7d 1636 69d3 a3ff ....}.6i...
000f5c20: d937 0a   .7.
hightech@pentest-b0x:~/CTF-Secarmy$ xxd 10.jpg | tail -2
000f5c00: eb57 0724 0ed0 5a7f f493 fdf0 9f0e ff00 .W.$..Z.........
000f5c10: e8b7 8a7d 1636 69d3 a3ff d923 0a   ...}.6i....#.
hightech@pentest-b0x:~/CTF-Secarmy$ xxd 11.jpg | tail -2
000f5c20: fdf0 9f0e ff00 e8b7 8a7d 1636 69d3 a3ff ....}.6i...
000f5c30: d931 0a   .1.
hightech@pentest-b0x:~/CTF-Secarmy$ xxd 12.jpg | tail -2
000f5c00: 0724 0ed0 5a7f f493 fdf0 9f0e ff00 e8b7 .$..Z...........
000f5c10: 8a7d 1636 69d3 a3ff d924 0a   .}.6i....$.
hightech@pentest-b0x:~/CTF-Secarmy$ xxd 13.jpg | tail -2
000f5c00: aad2 eb57 0724 0ed0 5a7f f493 fdf0 9f0e ...W.$..Z.......
000f5c10: ff00 e8b7 8a7d 1636 69d3 a3ff d95f 0a   .....}.6i...._.
hightech@pentest-b0x:~/CTF-Secarmy$ xxd 14.jpg | tail -2
000f5c10: 9f0e ff00 e8b7 8a7d 1636 69d3 a3ff d931 ....}.6i....1
000f5c20: 0a   .
hightech@pentest-b0x:~/CTF-Secarmy$ xxd 15.jpg | tail -2
000f5c10: 5a7f f493 fdf0 9f0e ff00 e8b7 8a7d 1636 Z............}.6
000f5c20: 69d3 a3ff d924 0a   i....$.
hightech@pentest-b0x:~/CTF-Secarmy$ xxd 16.jpg | tail -2
000f5c10: 9f0e ff00 e8b7 8a7d 1636 69d3 a3ff d95f ....}.6i...._
000f5c20: 0a   .
hightech@pentest-b0x:~/CTF-Secarmy$ xxd 17.jpg | tail -2
000f5c00: 5a7f f493 fdf0 9f0e ff00 e8b7 8a7d 1636 Z............}.6
000f5c10: 69d3 a3ff d937 0a   i....7.
hightech@pentest-b0x:~/CTF-Secarmy$ xxd 18.jpg | tail -2
000f5c10: f493 fdf0 9f0e ff00 e8b7 8a7d 1636 69d3 ....}.6i.
000f5c20: a3ff d923 0a   ...#.
hightech@pentest-b0x:~/CTF-Secarmy$ xxd 19.jpg | tail -2
000f5c10: f493 fdf0 9f0e ff00 e8b7 8a7d 1636 69d3 ....}.6i.
000f5c20: a3ff d933 0a   ...3.
hightech@pentest-b0x:~/CTF-Secarmy$ xxd 20.jpg | tail -2
000f5c00: eb57 0724 0ed0 5a7f f493 fdf0 9f0e ff00 .W.$..Z.........
000f5c10: e8b7 8a7d 1636 69d3 a3ff d95f 0a   ...}.6i...._.
hightech@pentest-b0x:~/CTF-Secarmy$ xxd 21.jpg | tail -2
000f5c10: 0ed0 5a7f f493 fdf0 9f0e ff00 e8b7 8a7d ..Z............}
000f5c20: 1636 69d3 a3ff d966 0a   .6i....f.
hightech@pentest-b0x:~/CTF-Secarmy$ xxd 22.jpg | tail -2
000f5c00: eb57 0724 0ed0 5a7f f493 fdf0 9f0e ff00 .W.$..Z.........
000f5c10: e8b7 8a7d 1636 69d3 a3ff d931 0a   ...}.6i....1.
hightech@pentest-b0x:~/CTF-Secarmy$ xxd 23.jpg | tail -2
000f5c10: 0724 0ed0 5a7f f493 fdf0 9f0e ff00 e8b7 .$..Z...........
000f5c20: 8a7d 1636 69d3 a3ff d940 0a   .}.6i....@.
hightech@pentest-b0x:~/CTF-Secarmy$ xxd 24.jpg | tail -2
000f5c00: eb57 0724 0ed0 5a7f f493 fdf0 9f0e ff00 .W.$..Z.........
000f5c10: e8b7 8a7d 1636 69d3 a3ff d939 0a   ...}.6i....9.
hightech@pentest-b0x:~/CTF-Secarmy$ xxd 25.jpg | tail -2
000f5e40: ab4b ad5c 1c90 3b41 48ff 0049 3fdf 09f0 .K.\..;AH..I?...
000f5e50: effe 8b78 a7d1 6131 a747 ffd9 7d0a   ...x..a1.G..}.

Perhatikan strings yang dengan warna hijau, masing2 dari strings tersebut jika disatukan akan menjadi flagnya. Maka cara diatas adalah penyelesaiannya

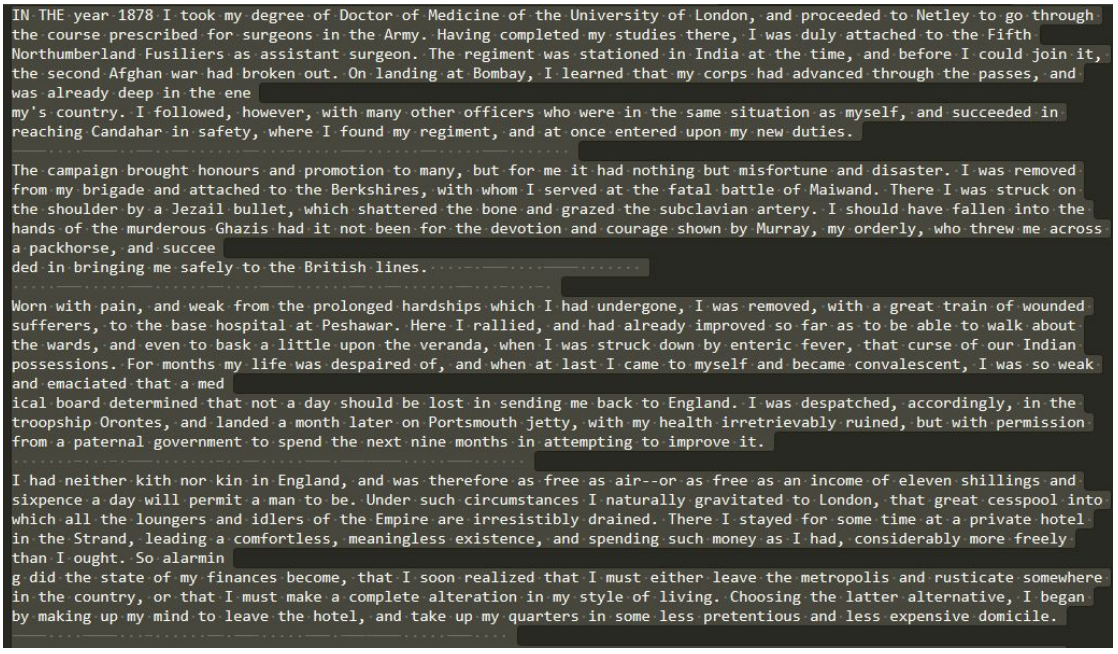
Flag:

secarmy{7#1$_1$_7#3_f1@9}

9. [Steganography] - SNOW [100]



Diberikan sebuah challenge sebagai berikut, file tersebut berisikan sebuah file text seperti ini.



IN THE year 1878 I took my degree of Doctor of Medicine of the University of London, and proceeded to Netley to go through the course prescribed for surgeons in the Army. Having completed my studies there, I was duly attached to the Fifth Northumberland Fusiliers as assistant surgeon. The regiment was stationed in India at the time, and before I could join it, the second Afghan war had broken out. On landing at Bombay, I learned that my corps had advanced through the passes, and was already deep in the ene
my's country. I followed, however, with many other officers who were in the same situation as myself, and succeeded in reaching Candahar in safety, where I found my regiment, and at once entered upon my new duties.

The campaign brought honours and promotion to many, but for me it had nothing but misfortune and disaster. I was removed from my brigade and attached to the Berkshires, with whom I served at the fatal battle of Maiwand. There I was struck on the shoulder by a Jezail bullet, which shattered the bone and grazed the subclavian artery. I should have fallen into the hands of the murderous Ghazis had it not been for the devotion and courage shown by Murray, my orderly, who threw me across a packhorse, and succee
ded in bringing me safely to the British lines.

Worn with pain, and weak from the prolonged hardships which I had undergone, I was removed, with a great train of wounded sufferers, to the base hospital at Peshawar. Here I rallied, and had already improved so far as to be able to walk about the wards, and even to bask a little upon the veranda, when I was struck down by enteric fever, that curse of our Indian possessions. For months my life was despaired of, and when at last I came to myself and became convalescent, I was so weak and emaciated that a med
ical board determined that not a day should be lost in sending me back to England. I was despatched, accordingly, in the troopship Orontes, and landed a month later on Portsmouth jetty, with my health irretrievably ruined, but with permission from a paternal government to spend the next nine months in attempting to improve it.

I had neither kith nor kin in England, and was therefore as free as air--or as free as an income of eleven shillings and sixpence a day will permit a man to be. Under such circumstances I naturally gravitated to London, that great cesspool into which all the loungers and idlers of the Empire are irresistibly drained. There I stayed for some time at a private hotel in the Strand, leading a comfortless, meaningless existence, and spending such money as I had, considerably more freely than I ought. So alarmin
g did the state of my finances become, that I soon realized that I must either leave the metropolis and rusticate somewhere in the country, or that I must make a complete alteration in my style of living. Choosing the latter alternative, I began by making up my mind to leave the hotel, and take up my quarters in some less pretentious and less expensive domicile.

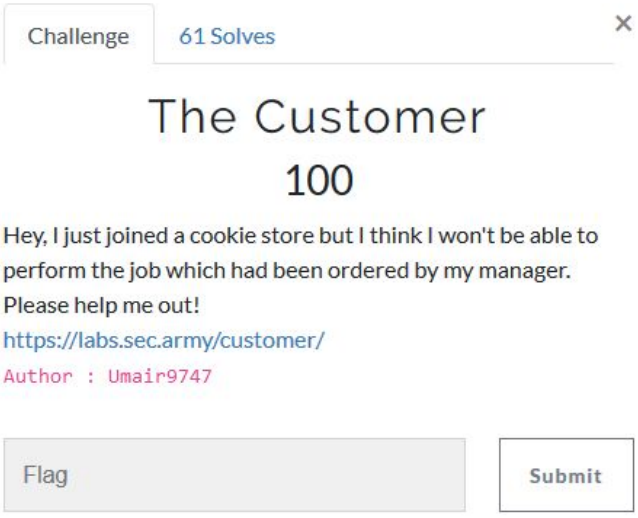
Saya pun fokus kepada strings ". **dan -**", dr analisa saya bahwa ini adalah Stegsnow, maka saya pun mencoba melakukan dekripsi file tsb menggunakan Stegsnow.

Dan hasilnya sukses, ternyata flagnya juga di encode lagi ke dalam **Base64 Encoding** sehingga saya sukses mendecode flag dari snow dan juga base64 tersebut.

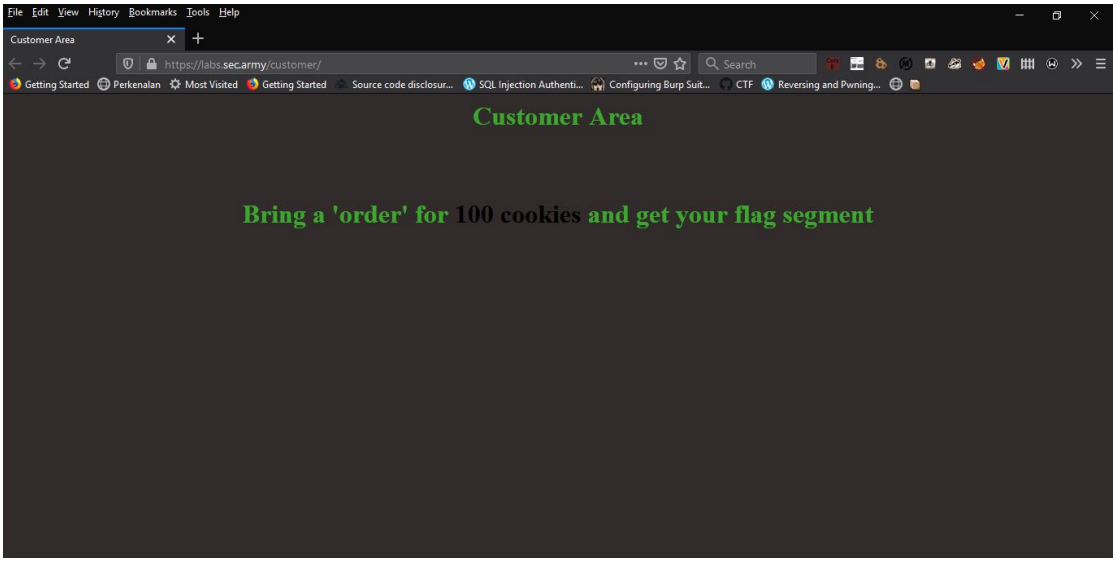
Flag:

secarmy{Clear_The_Snow}

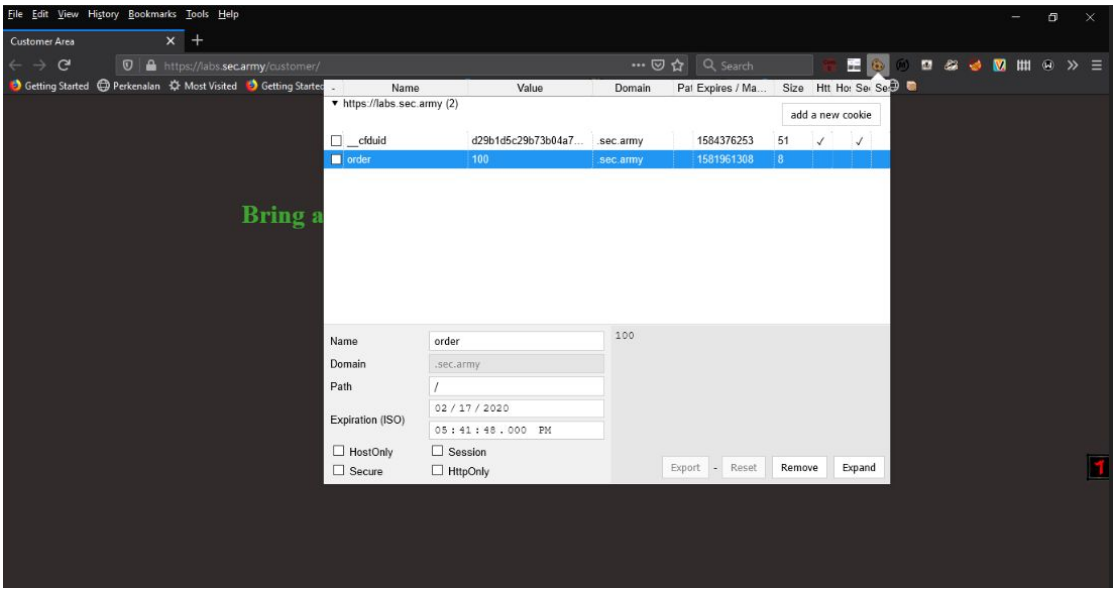
10. [Web] - The Customer [100]



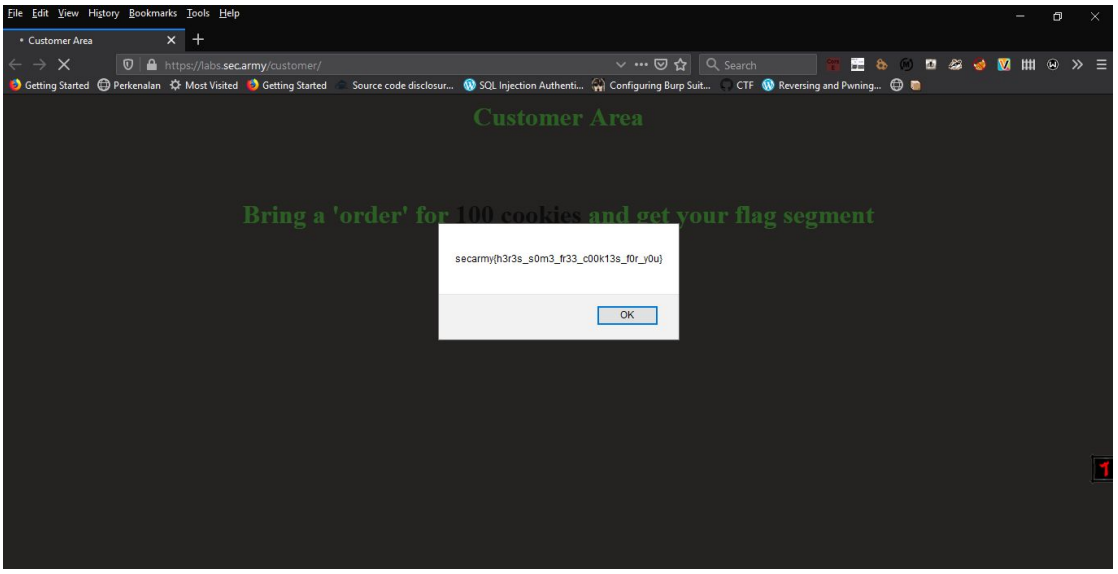
Diberikan sebuah challenge sebagai berikut, ketika saya buka linknya berisikan sebuah web seperti ini.



Dari clue yang ada, saya tahu bahwa disini saya harus melakukan perubahan pada value cookie sesuai dengan petunjuk seperti dibawah ini



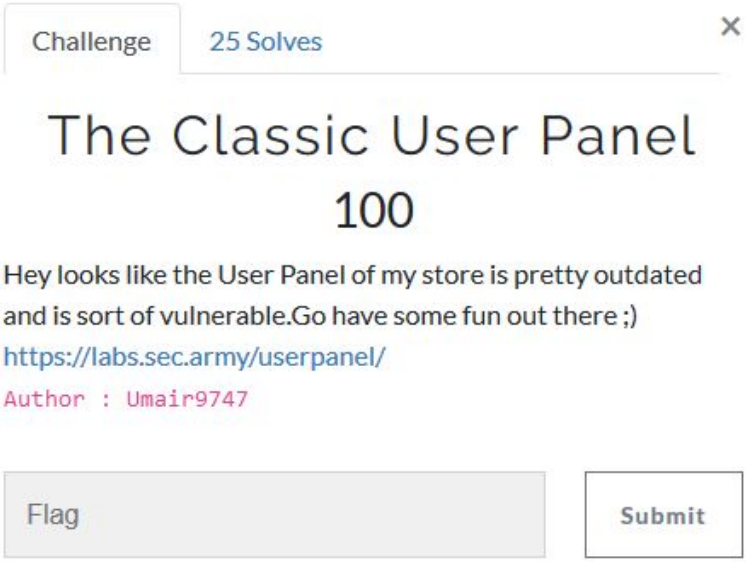
Dan hasilnya sukses, flag yang kita perlukan pun muncul seperti yang bisa dilihat pada gambar dibawah ini



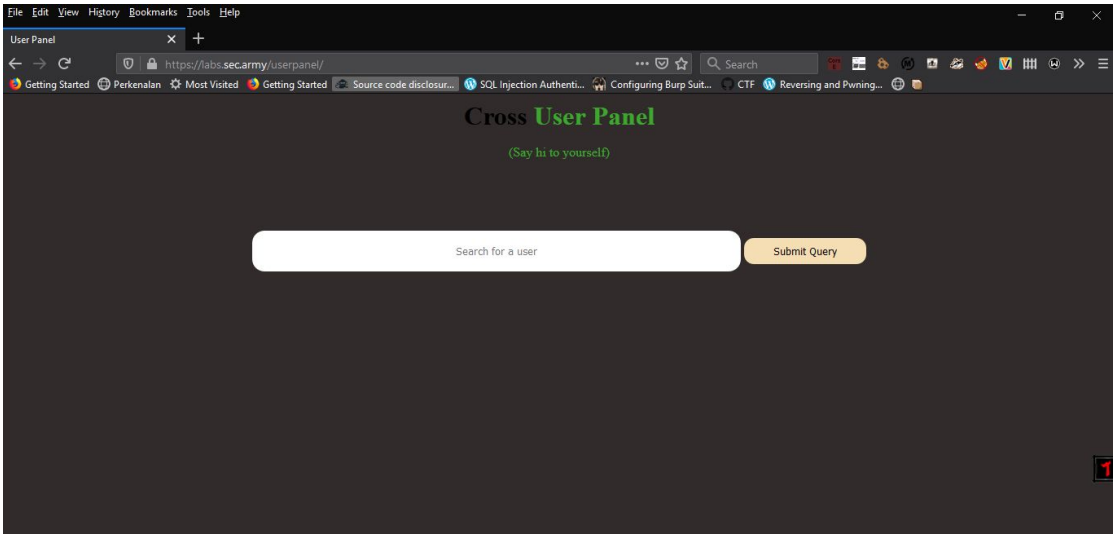
Flag:

secarmy{h3r3s_s0m3_fr33_c00k13s_f0r_y0u}

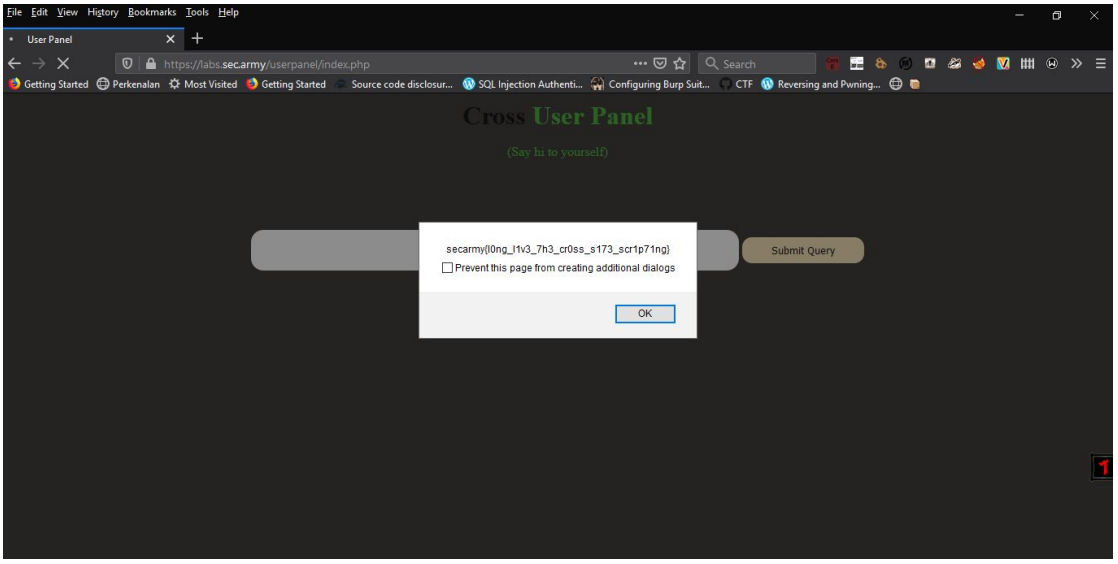
11. [Web] - The Classic User Panel [100]



Diberikan sebuah challenge sebagai berikut, ketika saya buka linknya berisikan sebuah web seperti ini.



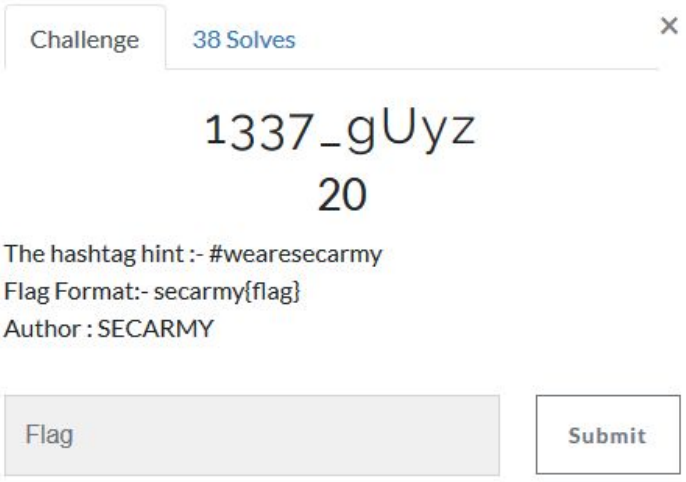
Berdasarkan clue yang ada, saya mencoba melakukan sql injection namun ternyata bukan itu maksud dr challenge ini. Saya mencoba melakukan **XSS** dengan payload "**hi**" sesuai dengan clue yg ada pada web tsb dan setelah XSS sudah di trigger flagnya ternyata muncul



Flag:

secarmy{l0ng_l1v3_7h3_cr0ss_s173_scr1p71ng}

12. [OSINT] - 1337_gUyz [20]

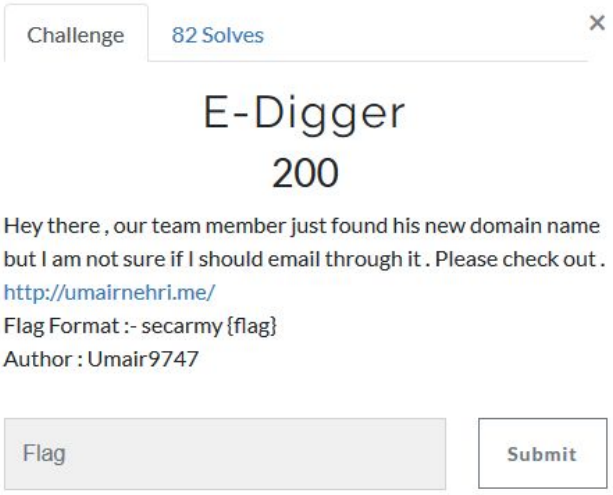


Diberikan sebuah challenge sebagai berikut, disini saya harus melakukan recon bermodalkan "**#wearesecarmy**". Maka saya pun melakukan recon di dua media sosial yang terkenal dengan Hashtag, yakni **Instagram** dan **Twitter**. Setelah berjam2 melakukan pengumpulan informasi di twitter, saya memutuskan bahwa flag tidak ada di twitter. Untuk di instagram, saya menggukana tools Instagram Crawler dengan payload "python3 crawler.py hashtag -t wearesecarmy -u sec_army -o output" Lalu saya menemukan flagnya pada salah satu post, flag nya berada pada Bagian Caption.

Flag:

secarmy{w3_actUalLy_n0t_1337s}

13. [OSINT] - E-Digger [200]



Diberikan sebuah challenge sebagai berikut, disini saya melakukan analisa dari clue yg ada.

Dan akhirnya saya menggunakan tools dig pada linux untuk mengecheck SPF record pada domain tersebut dan ternyata sukses. flagnya tersimpan di SPF Record.

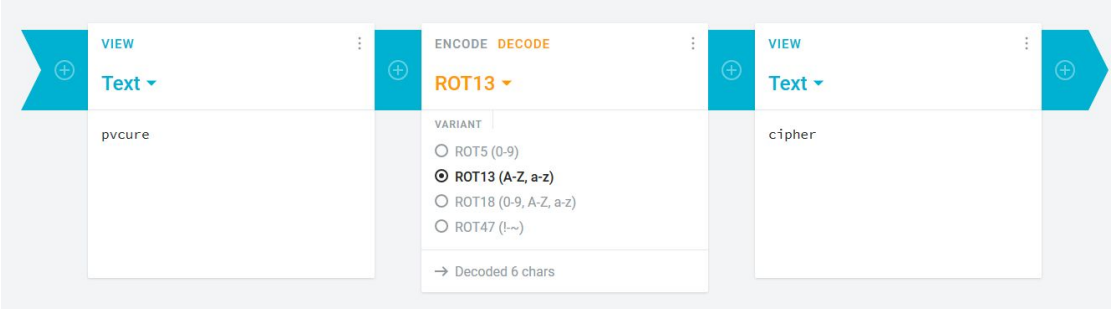
Flag:

secarmy{pf_r3c0rd_@1n7_b0r1ng_r1gh7?}

14. [Crypto] - SUM_IT_UP [70]

Diberikan sebuah challenge sebagai berikut, isi dari file zip tsb adalah sebuah ciphertext seperti ini **"if(D642C>JL#__E6? -eq pvcure) {"flag"}"**, bagian pertama ciphertext tsb adalah ROT-47, Saya melakukan dekripsi ROT-47 [disini](#).

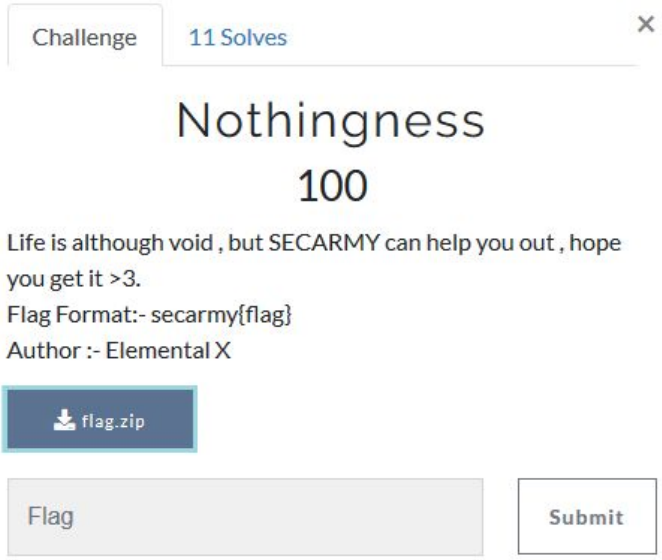
Dan bagian terakhirnya adalah ROT-13



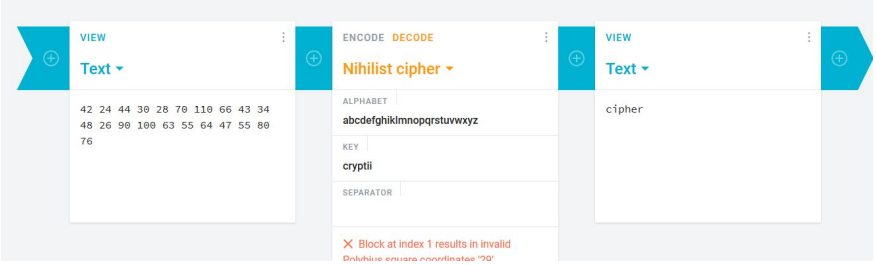
Flag:

secarmy{R00tencipher}

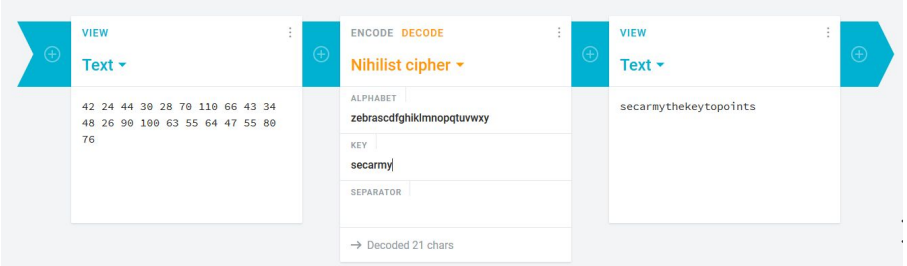
15. [Crypto] - Nothingness [100]



Diberikan sebuah challenge sebagai berikut, isi dari file zip tsb adalah sebuah ciphertext seperti ini "**42 ds24 ds44 ds30 ds28 ds70 ds110 ds66 ds43 ds34 ds48 ds26 ds90 ds100 ds63 ds55 ds64 ds47 ds55 ds80 ds76**", disini saya mencoba menghapus "**ds**" sehingga tersisa angka saja, awalnya saya mencoba mendecode sebagai hex namun gagal. Saya teringat dengan [Nihilist Cipher](). Namun gagal karna offset dan key yg salah



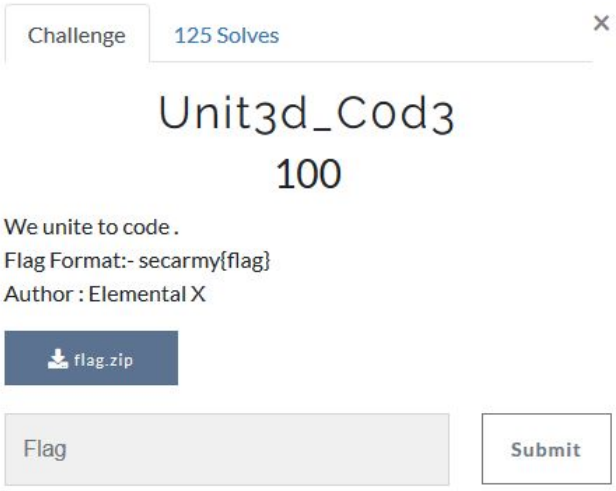
Setelah bermain2 dengan offset dan key, akhirnya flag ditemukan.



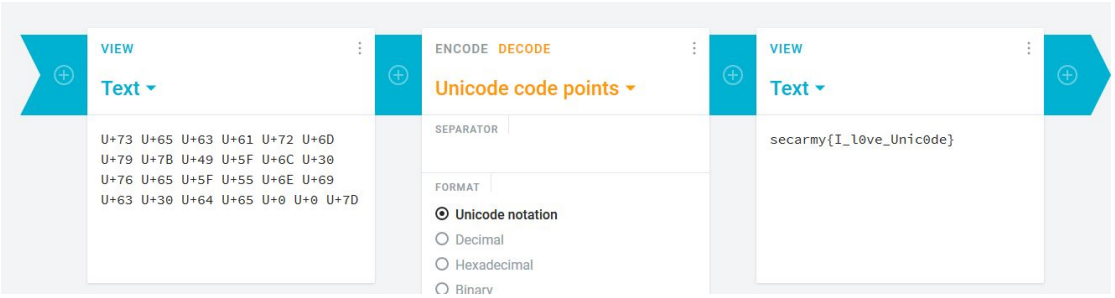
Flag:

secarmy{thekeytopoints}

16. [Crypto] - Unit3d_COd3 [100]



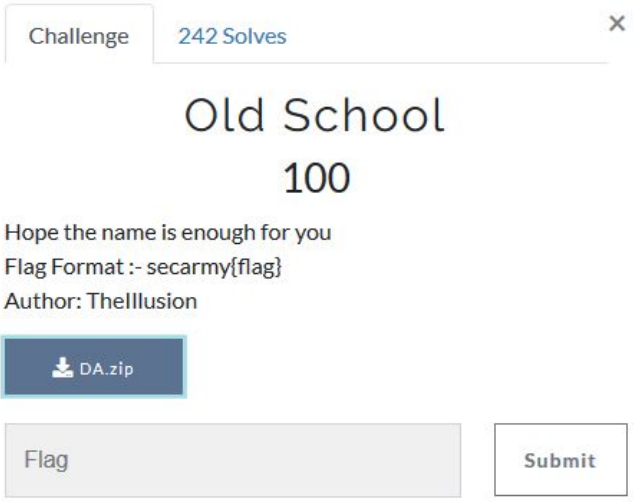
Diberikan sebuah challenge sebagai berikut, isi dari file zip tsb adalah sebuah ciphertext seperti ini "**s e c a r m y { I _ l 0 v e _ U n i c 0 d e &#x0; }**", disini saya mencoba menganti "**&#x**" menjadi "**U+**" lalu saya mencoba mendecode sebagai [Unicode Code Points](#) dan sukses.



Flag:

secarmy{I_l0ve_Unic0de}

17. [Crypto] - Old School [100]



Diberikan sebuah challenge sebagai berikut, isi dari file zip tsb adalah sebuah ciphertext seperti ini

```
01001101 01010100 01000001 01110111 01001001 01000100 01000101 01111000 01001101 01010011 01000001 01111000 01001101
01010100 01100011 01100111 01001111 01010100 01100111 01100111 01001101 01010100 01000001 00110100 01001001 01000100
01000101 01110111 01001101 01010011 01000001 00110101 01001110 01111001 01000001 01111000 01001101 01000100 01100111
01100111 01001101 01010100 01000001 01111010 01001001 01000100 01000101 01111000 01001101 01010011 01000001 01111000
01001101 01010100 01010001 01100111 01001101 01010100 01000001 00110001 01001001 01000100 01000101 01111000 01001110
01101001 01000001 01111000 01001101 01000100 01010001 01100111 01001101 01010100 01000001 00110101 01001001 01000100
01000101 01111000 01001110 01010001 00111101 00111101
```

disini saya pun mencoba untuk melakukan convert dari biner ke text, ternyata setelah di decode dari biner menghasilkan encoding base64

ASCII text

```
MTAwIDExMSAxMTcgOTggMTA4IDEwMSA5NyAxMDggMTAzIDExMSAxMTQgMTA1IDEx
NiAxMDQgMTA5IDExNQ==
```

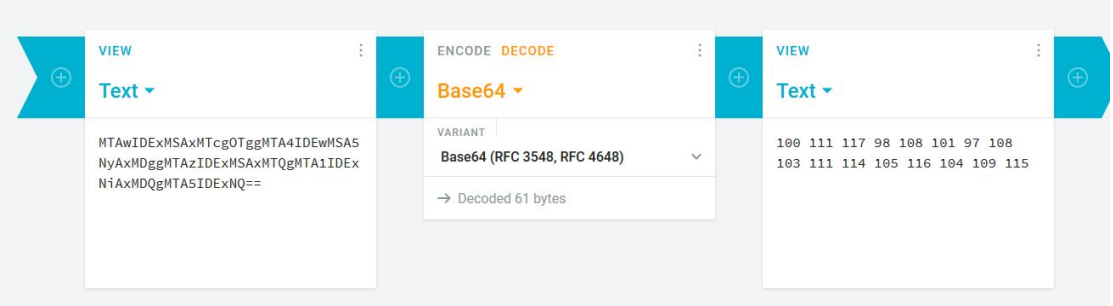
Hex (bytes)

```
4D 54 41 77 49 44 45 78 4D 53 41 78 4D 54 63 67 4F 54 67 67 4D
54 41 34 49 44 45 77 4D 53 41 35 4E 79 41 78 4D 44 67 67 4D 54
41 7A 49 44 45 78 4D 53 41 78 4D 54 51 67 4D 54 41 31 49 44 45
78 4E 69 41 78 4D 44 51 67 4D 54 41 35 49 44 45 78 4E 51 3D 3D
```

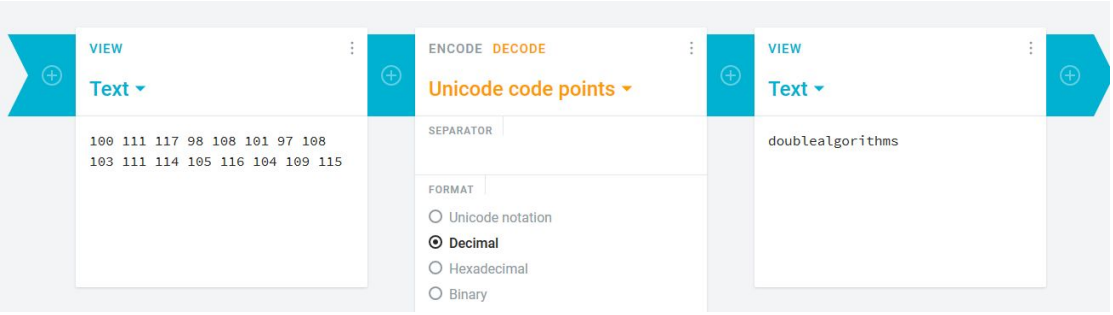
Binary (bytes)

```
01001101 01010100 01000001 00110001 01001001 01000100 01000101
01111000 01001110 01101001 01000001 01111000 01001101 01000100
01010001 01100111 01001101 01010100 01000001 00110101 01001001
01000100 01000101 01111000 01001110 01010001 00111101 00111101
```

lalu saya mencoba melakukan decoding lagi dr base64 ke text yang ternyata menghasilkan bilangan desimal.



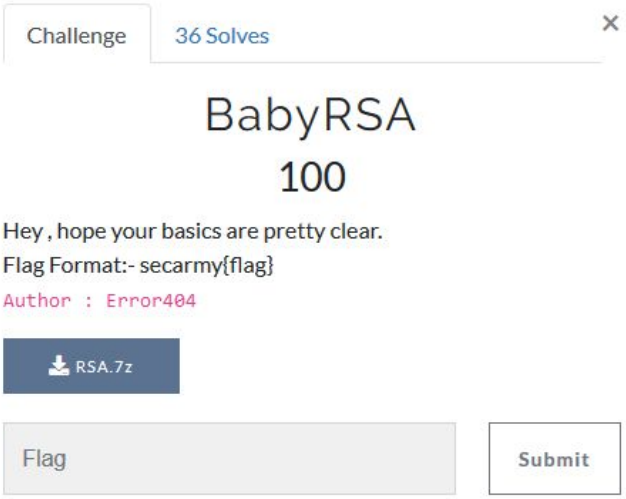
lalu saya mencoba melakukan decoding lagi dr desimal ke text yang ternyata menghasilkan flag.



Flag:

secarmy{doublealgorithms}

18. [Crypto] - BabyRSA [100]

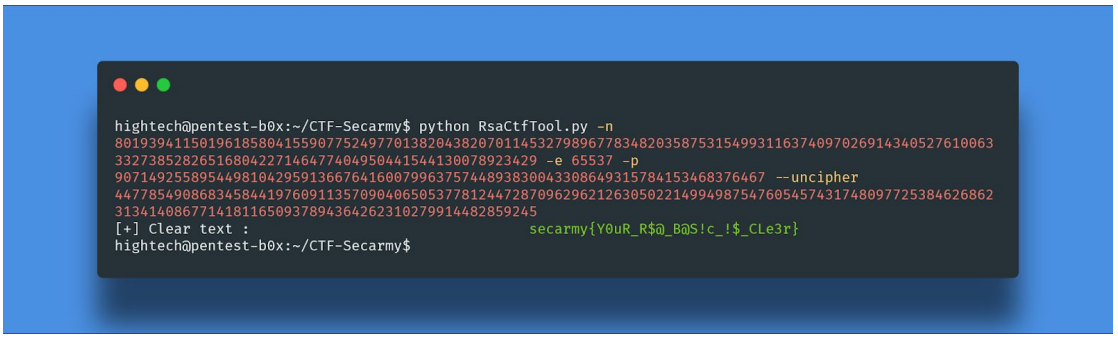


Diberikan sebuah challenge sebagai berikut, isi dari file zip tsb adalah sebuah script python seperti dibawah ini dan p,n,dan cipher text

```python
from Crypto.Util.number import *


def make_key():
    p = getPrime(256)
    q = getPrime(256)
    n = p*q
    e = 65537
    phin = (p-1)*(q-1)
    d = inverse(e,phin)
    return n,e,d,p,q

n,e,d,p,q = make_key()
flag = "Screat Flag Here !!!"
print("n=",n,"p=", p)
print("ct=", pow(bytes_to_long(flag.encode()), e, n))
```

```
n= 80193941150196185804155907752497701382043820701145327989677834820358753154993116374097026914340527610063332738528265168042271464774049504415441300789234290
p= 907149255895449810429591366764160079963757448938300433086493157841534683764670
ct= 44778549086834584419760911357090406505377812447287096296212630502214994987547605457431748097725384626862313414086771418116509378943642623102799144828592450
```

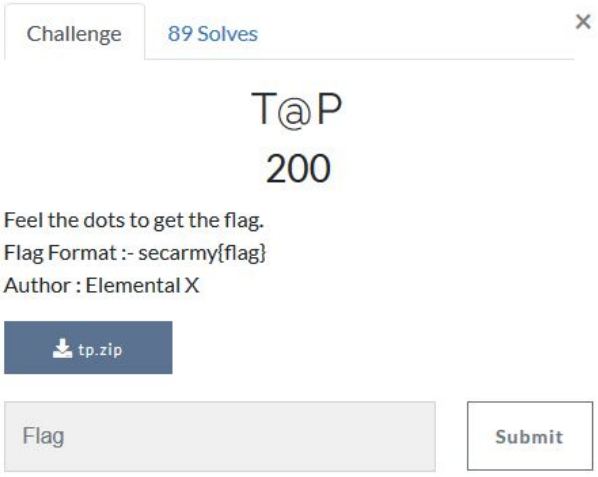
disini saya pun mencoba untuk melakukan Uncipher menggunakan RSACtfTool dan hasilnya sukses. Flagnya berhasil saya uncipher



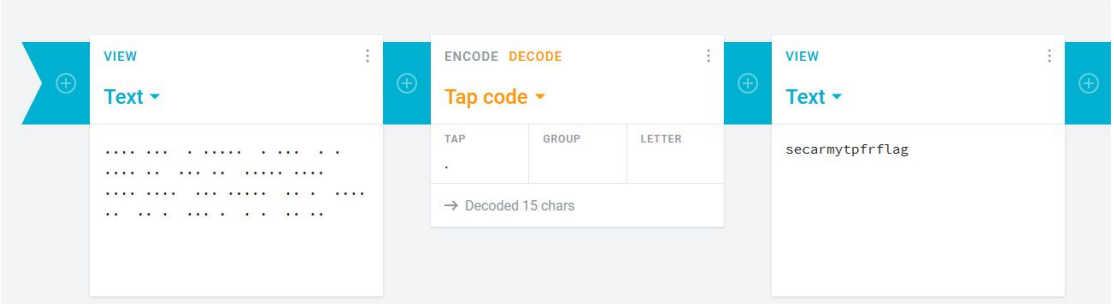
Flag:

secarmy{Y0uR_R$@_B@S!c_!$_CLe3r}

19. [Crypto] - T@P [200]



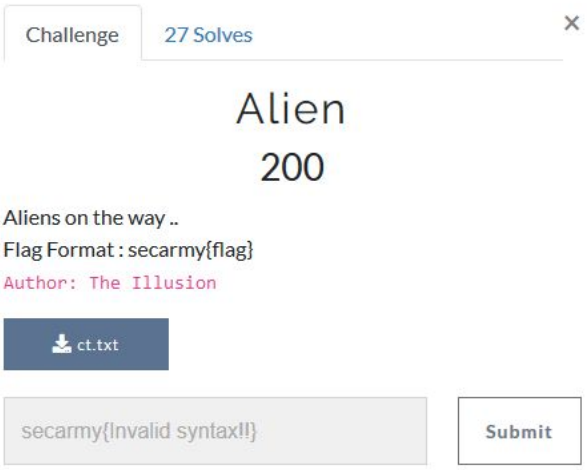
Diberikan sebuah challenge sebagai berikut, isi dari file zip tsb adalah sebuah ciphertext seperti ini ".... ... .", disini saya mencoba melakukan decode sebagai Tap Code. Dan ternyata hasilnya sukses



Flag:

secarmy{tpfrflag}

20. [Crypto] - Alien [200]



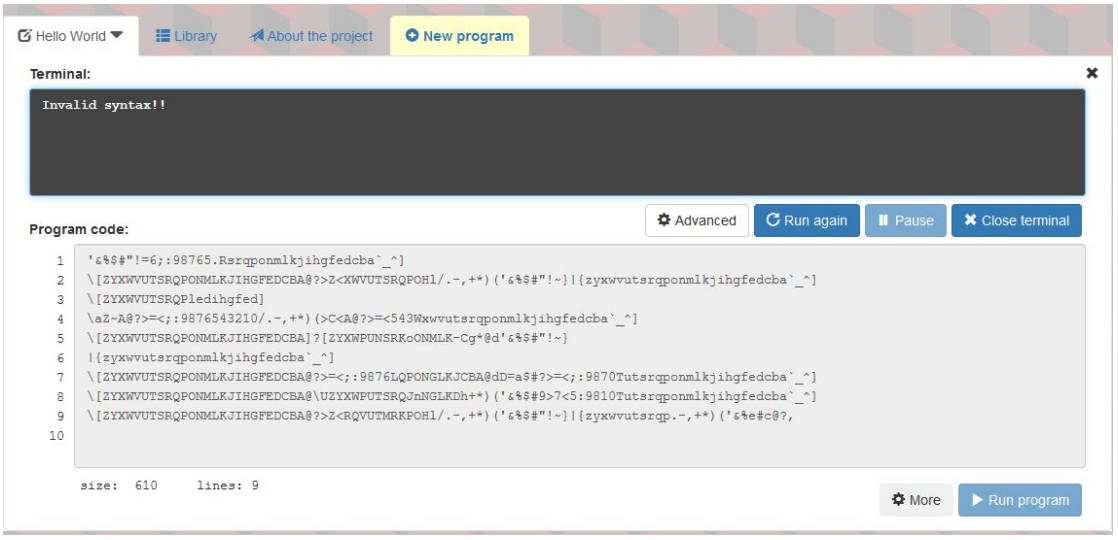
Diberikan sebuah challenge sebagai berikut, isi dari file zip tsb adalah sebuah ciphertext seperti ini, disini saya pun mencoba untuk merapihkan cipher terlebih dahulu.

```
'&%$#"!=6;:98765.Rsrqponmlkjihgfedcba`_^]\[ZYXWVUTSRQPONMLKJIHGFEDCBA@?>Z<XW
VUTSRQPOHl/.-,+*)('&%$#"!~}|{zyxwvutsrqponmlkjihgfedcba`_^]\[ZYXWVUTSRQPledi
hgfed]\aZ~A@?>=<;:9876543210/.-,+*)(>C<A@?>=<543Wxwvutsrqponmlkjihgfedcba`_^
]\[ZYXWVUTSRQPONMLKJIHGFEDCBA]?[ZYXWPUNSRKoONMLK-Cg*@d'&%$#"!~}|{zyxwvutsrqp
onmlkjihgfedcba`_^]\[ZYXWVUTSRQPONMLKJIHGFEDCBA@?>=<;:9876LQPONGLKJCBA@dD=a$
#?>=<;:9870Tutsrqponmlkjihgfedcba`_^]\[ZYXWVUTSRQPONMLKJIHGFEDCBA@\UZYXWPUTS
RQJnNGLKDh+*)('&%$#9>7<5:9810Tutsrqponmlkjihgfedcba`_^]\[ZYXWVUTSRQPONMLKJIH
GFEDCBA@?>Z<RQVUTMRKPOHl/.-,+*)('&%$#"!~}|{zyxwvutsrqp.-,+*)('&%e#c@?,
```

Hasil setelah dirapihkan seperti dibawah ini

```
'&%$#"!=6;:98765.Rsrqponmlkjihgfedcba`_^]
\[ZYXWVUTSRQPONMLKJIHGFEDCBA@?>Z<XWVUTSRQPOHl/.-,+*)('&%$#"!~}|{zyxwvutsrqponmlkjihgfedcba`_^]
\[ZYXWVUTSRQPledihgfed]
\aZ~A@?>=<;:9876543210/.-,+*)(>C<A@?>=<543Wxwvutsrqponmlkjihgfedcba`_^]
\[ZYXWVUTSRQPONMLKJIHGFEDCBA]?[ZYXWPUNSRKoONMLK-Cg*@d'&%$#"!~}
|{zyxwvutsrqponmlkjihgfedcba`_^]
\[ZYXWVUTSRQPONMLKJIHGFEDCBA@?>=<;:9876LQPONGLKJCBA@dD=a$#?>=<;:9870Tutsrqponmlkjihgfedcba`_^]
\[ZYXWVUTSRQPONMLKJIHGFEDCBA@\UZYXWPUTSRQJnNGLKDh+*)('&%$#9>7<5:9810Tutsrqponmlkjihgfedcba`_^]
\[ZYXWVUTSRQPONMLKJIHGFEDCBA@?>Z<RQVUTMRKPOHl/.-,+*)('&%$#"!~}|{zyxwvutsrqp.-,+*)('&%e#c@?,
```

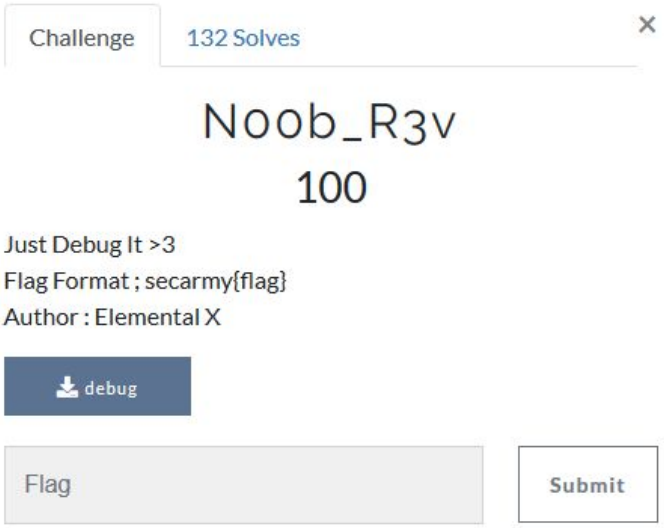
Lalu saya mencoba merunning cipher text yg sudah saya analisa sebagai Malbolge dan resultnya seperti ini. Awalnya saya mengira bahwa ciphernya salah dirapihin atau lainnya. Tapi ternyata pihak Secarmy melakukan "**Trolling**" terhadap peserta. Saya mencoba submit Result nya sebagai flag dan sukses



Flag:

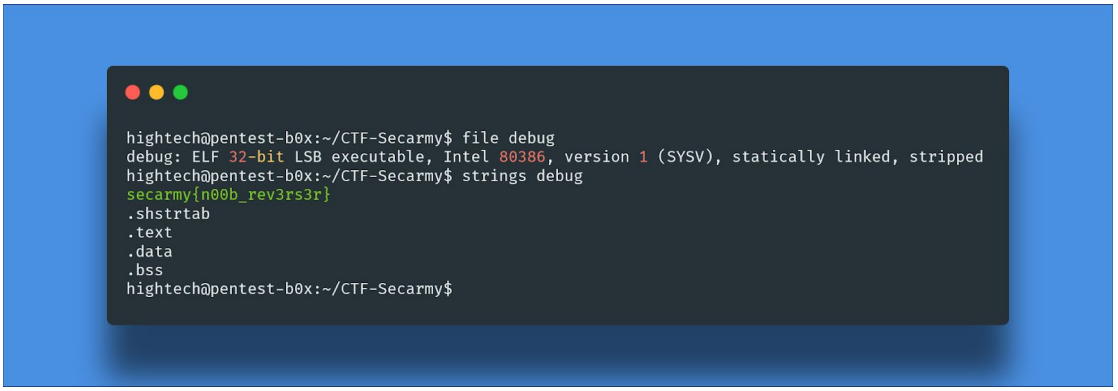
secarmy{Invalid syntax!!}

21. [Reversing] - N00b_R3v [100]



Diberikan sebuah challenge sebagai berikut, isi dari file tersebut adalah sebuah file binary

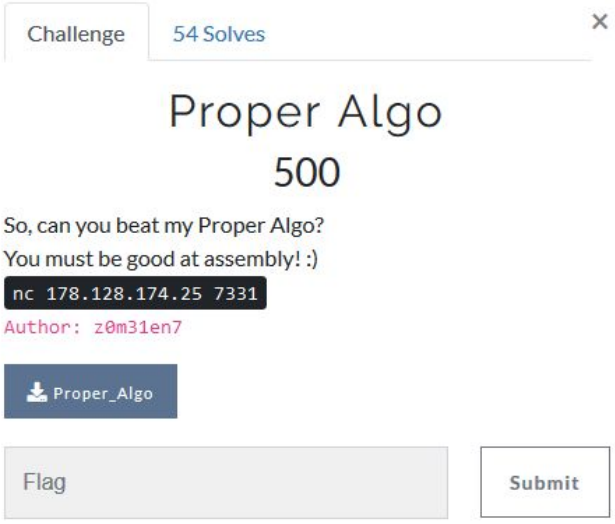
disini saya pun mencoba untuk melakukan strings terhadap file debug tersebut dan ternyata flagnya pun kelihatan.



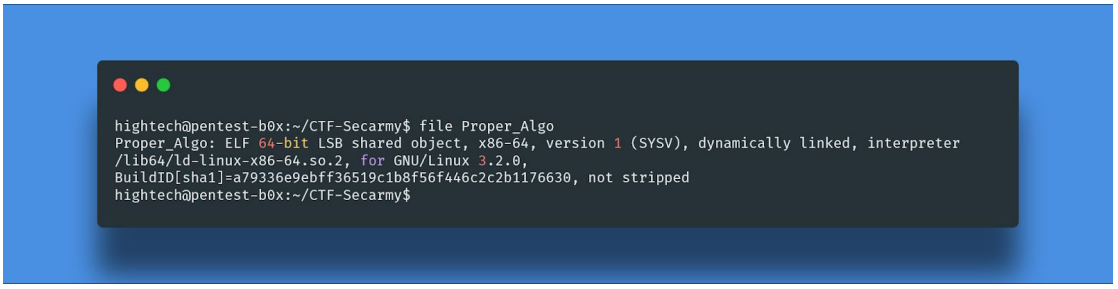
Flag:

secarmy{n00b_rev3rs3r}

22. [Reversing] - Proper Algo [500]



Diberikan sebuah challenge sebagai berikut, isi dari file tersebut adalah sebuah file binary

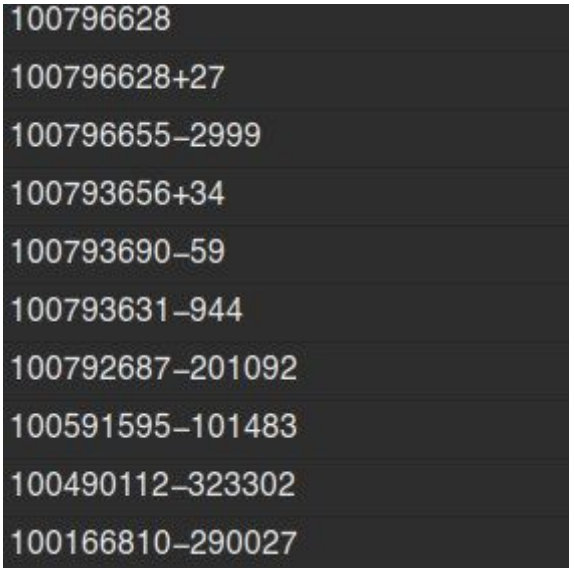


disini saya pun mencoba untuk melakukan reversing menggunakan IDA, Pada fungsi main terlihat bahwa **"V7"** akan membandingkan inputan kita apakah sama atau tidak.

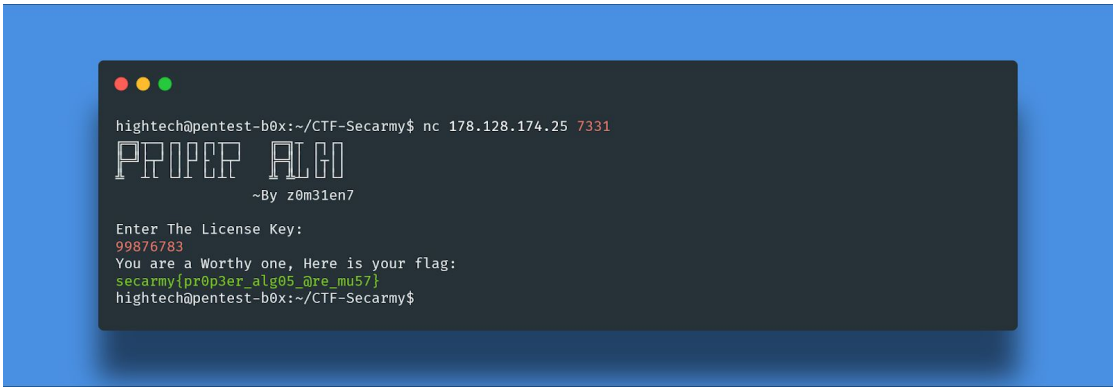
```
strcpy(filename, "flag.txt");
puts("GòöGòÉGòùGö¼GöÇGöÉGöîGöÉGöîGöÉGöîGöÉGö¼GöÇGöÉ   GòöGòÉGòùGö¼ GöîGöÉGöîGöÉ");
puts("GòáGòÉGò¥Gö£Gö¼GöÿGöéGöéGö£GöÿGö£ Gö£Gö¼Göÿ   GòáGòÉGòúGöé GöéGö¼GöéGöé");
puts("Gò¬  Gö¦Göö GööGöÿGö¦ GööGöÿGö¦Göö    Gò¬ Gò¬Gö¦GöÿGööGöÿGööGöÿ");
puts("\t\t˜By z0m31en7\n");
puts("Enter The License Key:");
fflush(_bss_start);
__isoc99_scanf("%lld", &v4);
v7 = start(v4);
if ( v7 == 100796628 )
{
  puts("You are a Worthy one, Here is your flag:");
  stream = fopen(filename, "r");
  if ( !stream )
  {
    puts("Cannot open flag.txt, are you entering the key on the server? ");
    exit(0);
  }
  for ( i = fgetc(stream); i != -1; i = fgetc(stream) )
    putchar(i);
  fclose(stream);
```

Sedangkan pada Fungsi "ZOMBIENT" dibawah2 ini tugasnya adalah melakukan pengecekan dengan operasi pertambahan dan pengurangan terhadap inputan kita yg lalu akan di oper untuk dicocokan dengan value "**v7**" pada fungsi main sebelumnya.

Disini saya memutar algoritma nya dengan melakukan pengurangan dan pertambahan terhadap value "**v7**" seperti dibawah ini.



Lalu hasil operasi matematika sebelumnya didapatkan value "**99876783**" sebagai hasil akhir, lalu saya mencoba untuk memvalidasinya di server dan hasilnya sukses.

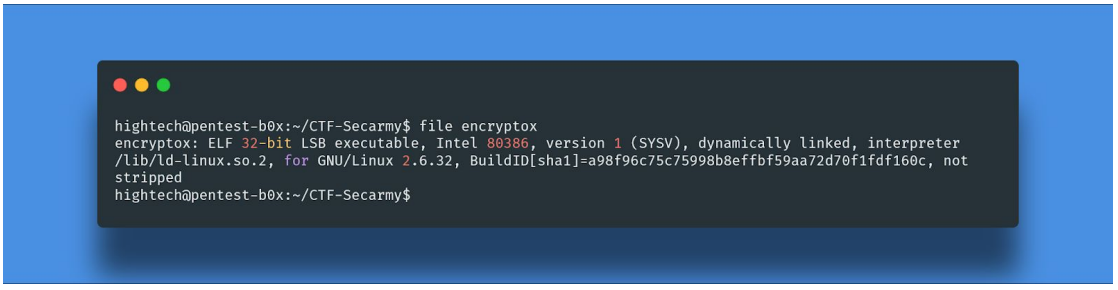


Flag:

secarmy{pr0p3er_alg05_@re_mu57}

23. [Miscellaneous] - ENCRYPTO X [60]

Diberikan sebuah challenge sebagai berikut, isi dari file tersebut adalah sebuah file binary



disini saya pun mencoba untuk melakukan reversing menggunakan IDA, Pada fungsi main Perhatian saya tertuju kepada Beberapa Value decimal dan hex (Gambar Kiri). Lalu saya mencoba melakukan Decode dr Value Hex dan Desimal ke Char (Gambar Kanan).

```
v82 = *MK_FP(__GS__, 20);
*(_DWORD *)s2 = 1329811013;
v53 = 17732;
v54 = 0;
*(_DWORD *)v55 = 1329808708;
v56 = 17732;
v57 = 0;
v70 = 65;
v71 = 45;
v72 = 43;
v73 = 33;
v74 = 64;
v75 = 36;
v76 = 98;
v77 = 52;
v78 = 48;
v79 = 57;
v80 = 88;
v81 = 68;
v60 = 101;
v61 = 110;
v62 = 99;
v63 = 111;
v64 = 100;
v65 = 101;
v66 = 98;
v67 = 105;
v68 = 116;
v69 = 115;
```

c

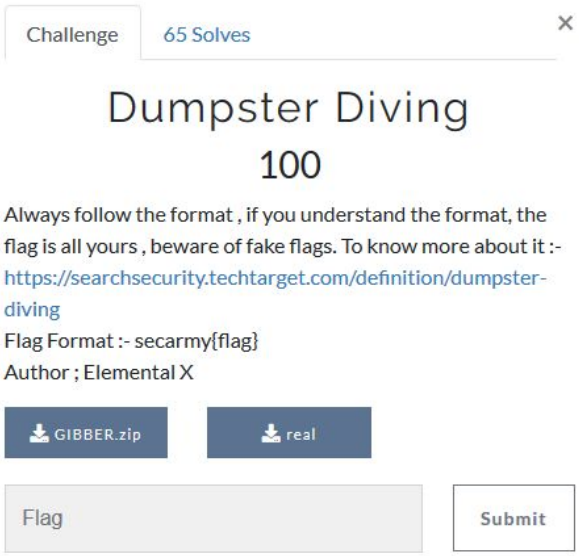
```
v82 = *MK_FP(__GS__, 20);
*(_DWORD *)s2 = 'OCNE';
v53 = 'ED';
v54 = 0;
*(_DWORD *)v55 = 'OCED';
v56 = 'ED';
v57 = 0;
v70 = 'A';
v71 = '-';
v72 = '+';
v73 = '!';
v74 = '@';
v75 = '$';
v76 = 'b';
v77 = '4';
v78 = '0';
v79 = '9';
v80 = 'X';
v81 = 'D';
v60 = 'e';
v61 = 'n';
v62 = 'c';
v63 = 'o';
v64 = 'd';
v65 = 'e';
v66 = 'b';
v67 = 'i';
v68 = 't';
v69 = 's';
```

Hasil dari decode char tsb adalah "**A-+!@$b409XDencodebits**" namun setelah saya analisa lagi ternyata flag nya adalah "**encodedbits**"

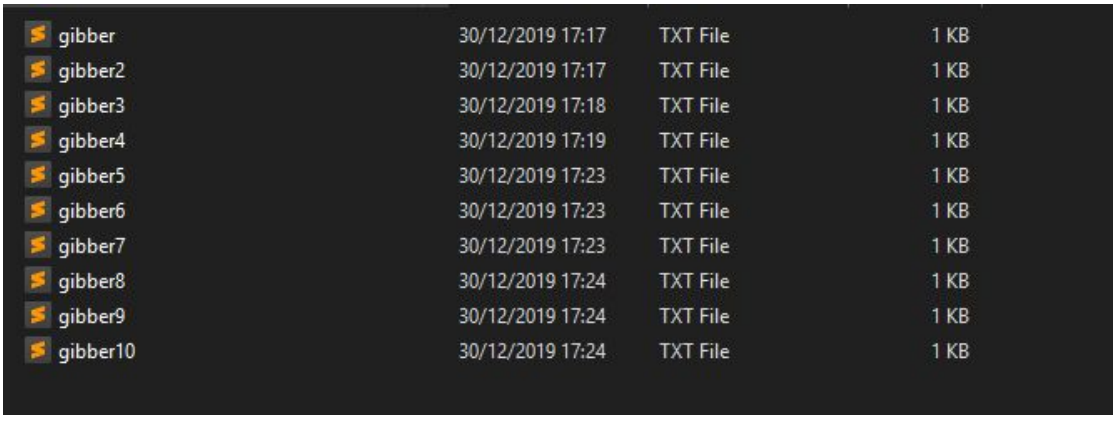
Flag:

secarmy{encodedbits}

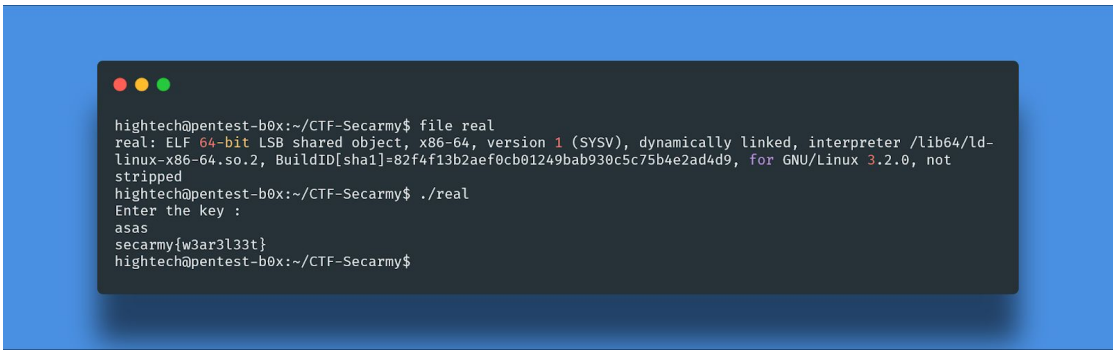
24. [Miscellaneous] - Dumpster Diving [100]



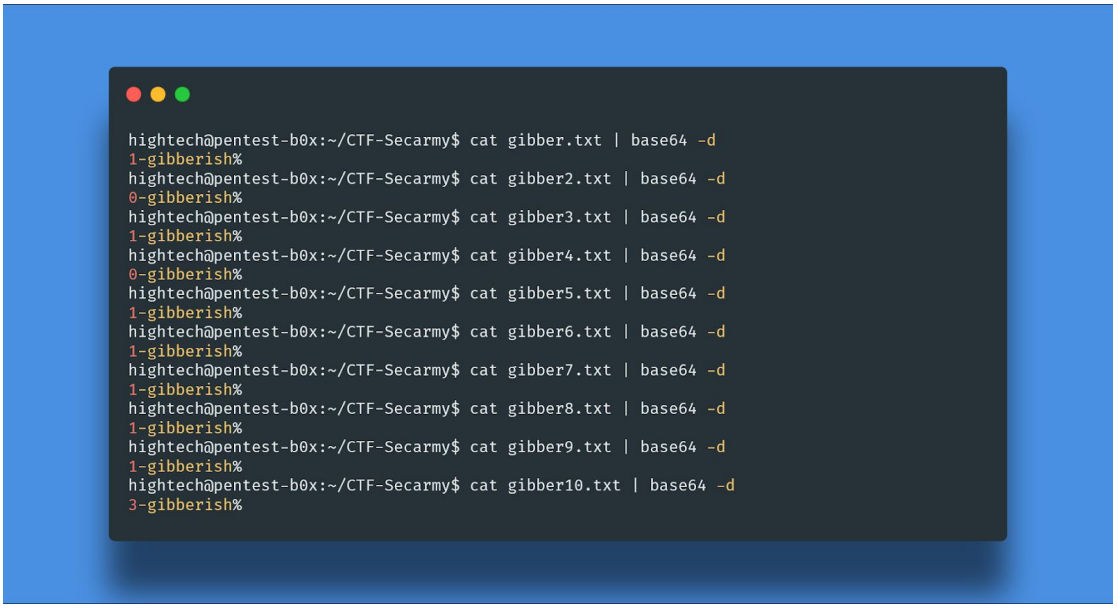
Diberikan sebuah challenge sebagai berikut, isi dari file tersebut adalah sebuah file binary dan file zip yg berisikan encoding base64



disini saya pun mencoba untuk melakukan eksekusi terhadap file binary tadi dan mendapatkan sebuah flag palsu.



Saya mencoba melakukan decoding terhadap file2 tersebut secara berurutan dan membentuk urutan dibawah seperti ini. Fokus saya tertuju pada nomor-nomor yang ada. Lalu saya coba ambil nomor-nomor tersebut dan menyusunnya hingga menjadi **"1010111113"**



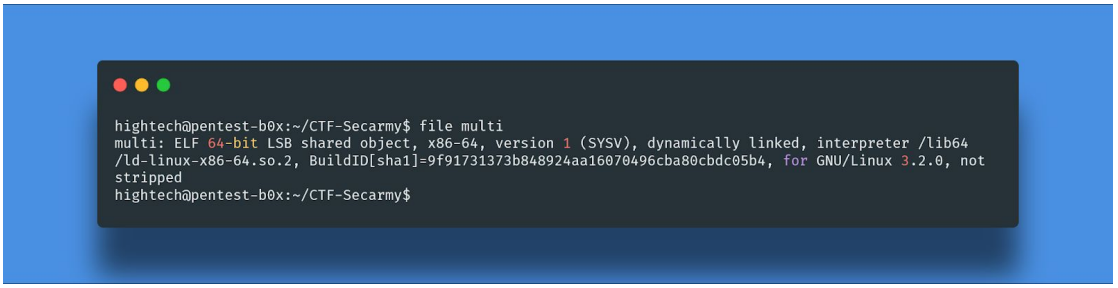
Lalu saya mencoba running lagi file binary sebelumnya dan memasukan nomor yg sebelumnya saya dapatkan dr file-file gibber.txt, dan ternyata hasilnya adalah sukses.

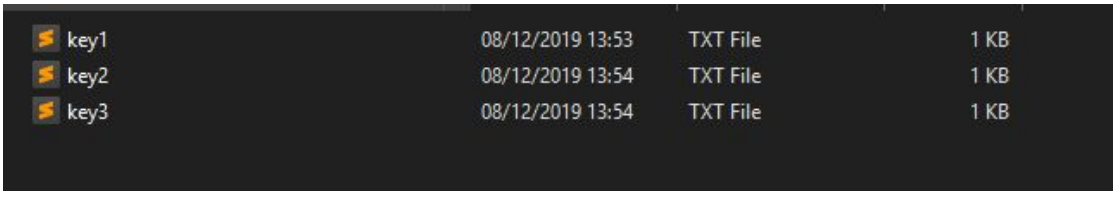
Flag:

secarmy{5656575656259}

25. [Miscellaneous] - Multiple Ways [200]

Diberikan sebuah challenge sebagai berikut, isi dari file tersebut adalah sebuah file binary dan file zip yg berisikan beberapa key

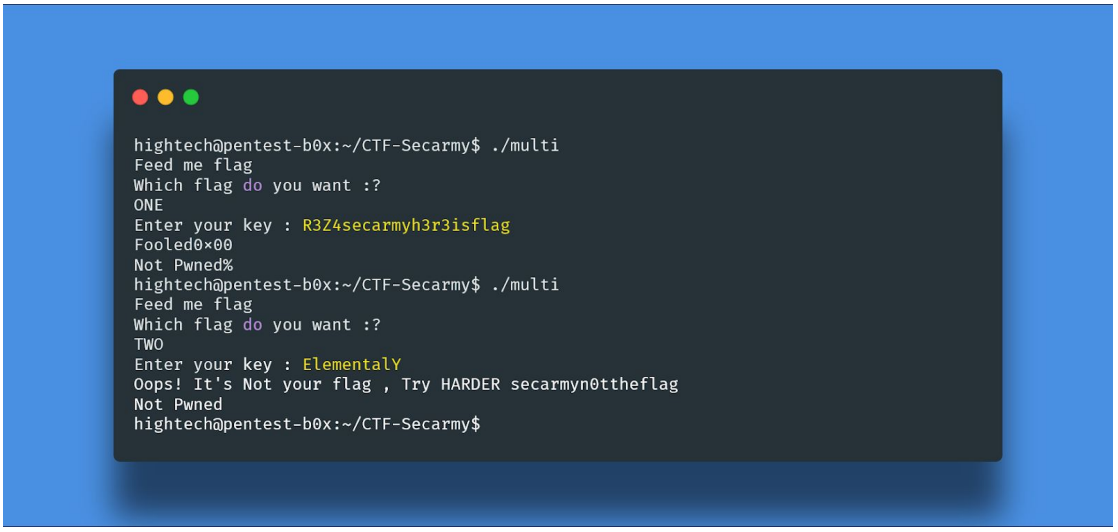




disini saya melakukan analisa dan ternyata file key tersebut hanya sebuah pengecoh. Saya coba melakukan ltrace dan melihat pada strcmp bahwa file binary tsb dapat menerima 3 Inputan, yakni "**ONE, TWO, THREE**". Masing-masing pilihan ternyata berbeda.

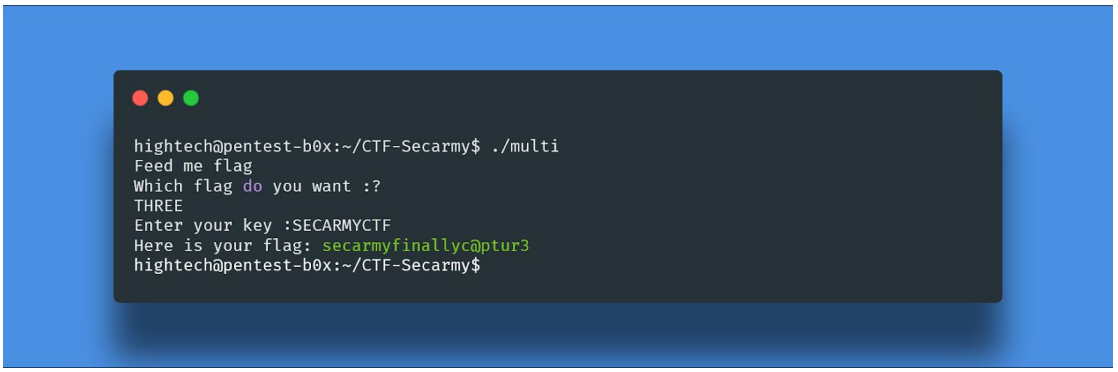
```
hightech@pentest-b0x:~/CTF-Secarmy$ ltrace ./multi
_ZNSt8ios_base4InitC1Ev(0x7fefb9b082d9, 0xffff, 0x7fffc213e328, 128)
 = 0
__cxa_atexit(0x7fefb95139e0, 0x7fefb9b082d9, 0x7fefb9b08088, 6)
= 0
_ZStlsISt11char_traitsIcEERSt13basic_ostreamIcT_ES5_PKc(0x7fefb9b080a0, 0x7fefb9b06083, 0x7fffc213e328,
160) = 0x7fefb9b080a0
_ZNSolsEPFRSoS_E(0x7fefb9b080a0, 0x7fefb9583990, 0x7fefb9b080a0, 0x7fefb9b0608fFeed me flag
)                         = 0x7fefb9b080a0
_ZStlsISt11char_traitsIcEERSt13basic_ostreamIcT_ES5_PKc(0x7fefb9b080a0, 0x7fefb9b06090, 0, 2880)
 = 0x7fefb9b080a0
_ZNSolsEPFRSoS_E(0x7fefb9b080a0, 0x7fefb9583990, 0x7fefb9b080a0, 0x7fefb9b060a9Which flag do you want :?
)                         = 0x7fefb9b080a0
_ZStrsIcSt11char_traitsIcEERSt13basic_istreamIT_T0_ES6_PS3_(0x7fefb9b081c0, 0x7fffc213e210, 0, 2880TEST
)    = 0x7fefb9b081c0
strcmp("ONE", "TEST")
= -5
strcmp("TWO", "TEST")
= 18
strcmp("THREE", "TEST")
= 3
_ZStlsISt11char_traitsIcEERSt13basic_ostreamIcT_ES5_PKc(0x7fefb9b080a0, 0x7fefb9b060aa, 69,
0x7fffba257e85) = 0x7fefb9b080a0
Not a favourable option+++ exited (status 0) +++

hightech@pentest-b0x:~/CTF-Secarmy$
```

Hasil dari Flag "**ONE** dan **TWO**" adalah seperti dibawah ini, tidak lain sebagai pengecoh lagi.



```
hightech@pentest-b0x:~/CTF-Secarmy$ ./multi
Feed me flag
Which flag do you want :?
ONE
Enter your key : R3Z4secarmyh3r3isflag
Fooled0x00
Not Pwned%
hightech@pentest-b0x:~/CTF-Secarmy$ ./multi
Feed me flag
Which flag do you want :?
TWO
Enter your key : ElementalY
Oops! It's Not your flag , Try HARDER secarmyn0ttheflag
Not Pwned
hightech@pentest-b0x:~/CTF-Secarmy$
```

Lalu saya mendapatkan key untuk Flag ketiga setelah sebelumnya menjalankan ltrace. Key yg saya gunakan adalah "**SECARMYCTF**" dan flag pun muncul.



Flag:

secarmy{finallyc@ptur3}

26. [Miscellaneous] - CrackOut [200]

Diberikan sebuah challenge sebagai berikut, isi dari file tersebut adalah sebuah file txt dan file zip yg lainnya berisikan sebuah gambar namun terkunci. Isi dari pass.txt tersebut adalah kumpulan text seperti di bawah ini.

curabitur vitae nunc sed velit dignissim sodales ut eu sem integer vitae justo eget magna fermentum iaculis eu non diam phasellus vestibulum lorem sed risus ultricies tristique nulla aliquet enim tortor at auctor urna nunc id cursus metus aliquam eleifend mi in nulla posuere sollicitudin aliquam ultrices sagittis orci a scelerisque purus semper eget duis at tellus at urna condimentum mattis pellentesque id nibh tortor id aliquet lectus proin nibh nisl condimentum id venenatis a condimentum vitae sapien pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas sed tempus urna et pharetra pharetra massa massa ultricies mi quis hendrerit dolor magna eget est lorem ipsum dolor sit amet consectetur adipiscing elit pellentesque habitant morbi tristique senectus ornare lectus sit amet est placerat in egestas erat imperdiet sed euismod nisi porta lorem mollis aliquam ut porttitor leo a diam sollicitudin tempor id eu nisl nunc mi ipsum faucibus vitae aliquet nec ullamcorper sit amet risus nullam eget felis eget nunc lobortis mattis aliquam faucibus purus in massa tempor nec feugiat nisl pretium fusce id velit ut tortor pretium viverra suspendisse potenti nullam ac tortor vitae purus faucibus ornare suspendisse sed nisi lacus sed viverra tellus in hac habitasse platea dictumst vestibulum rhoncus est pellentesque elit ullamcorper dignissim cras tincidunt lobortis feugiat vivamus at augue eget arcu dictum varius duis at consectetur lorem donec massa sapien faucibus et molestie ac feugiat sed lectus vestibulum mattis ullamcorper velit sed ullamcorper morbi tincidunt ornare massa eget egestas purus viverra accumsan in nisl nisi scelerisque eu ultrices vitae auctor eu augue ut lectus arcu bibendum at varius vel pharetra vel turpis nunc eget lorem dolor sed viverra ipsum nunc aliquet bibendum enim facilisis gravida neque convallis a cras semper auctor neque vitae tempus quam pellentesque nec nam aliquam sem et tortor consequat id porta nibh venenatis cras sed felis eget velit aliquet sagittis id consectetur purus ut faucibus pulvinar elementum integer enim neque volutpat ac tincidunt vitae semper quis lectus nulla at volutpat diam ut venenatis tellus in metus vulputate eu scelerisque felis imperdiet proin fermentum leo vel orci porta non pulvinar neque laoreet suspendisse interdum consectetur libero id faucibus nisl nec dui nunc mattis enim ut tellus elementum sagittis vitae et leo duis ut diam quam nulla porttitor massa id neque aliquam vestibulum morbi blandit cursus risus at ultrices mi tempus imperdiet nulla malesuada pellentesque elit eget gravida cum sociis natoque penatibus et magnis dis parturient montes nascetur ridiculus mus mauris vitae ultricies leo integer malesuada nunc vel risus commodo viverra maecenas accumsan lacus vel facilisis volutpat est velit egestas dui id ornare arcu odio ut sem nulla pharetra diam sit amet nisl suscipit adipiscing bibendum est ultricies integer quis auctor elit sed vulputate mi sit amet mauris commodo quis imperdiet massa tincidunt nunc pulvinar sapien et ligula ullamcorper malesuada proin libero nunc consequat interdum varius sit amet mattis vulputate enim nulla aliquet porttitor lacus luctus accumsan tortor posuere ac ut consequat semper viverra nam libero justo laoreet sit amet cursus sit amet dictum sit amet justo donec enim diam vulputate ut pharetra sit amet aliquam id diam maecenas ultricies mi eget mauris pharetra et ultrices neque ornare aenean euismod elementum nisi quis eleifend quam adipiscing vitae proin sagittis nisl rhoncus mattis rhoncus urna neque viverra justo nec ultrices dui sapien eget mi proin sed libero enim sed faucibus turpis in eu mi bibendum neque egestas congue quisque egestas diam in arcu cursus euismod quis viverra nibh cras pulvinar mattis nunc sed blandit libero volutpat sed cras ornare arcu dui vivamus arcu felis bibendum ut tristique et egestas quis ipsum suspendisse ultrices gravida dictum fusce ut placerat orci nulla pellentesque dignissim enim sit amet venenatis urna cursus eget nunc scelerisque viverra mauris in aliquam sem fringilla ut morbi tincidunt augue interdum velit euismod in pellentesque massa placerat duis ultricies lacus sed turpis tincidunt id

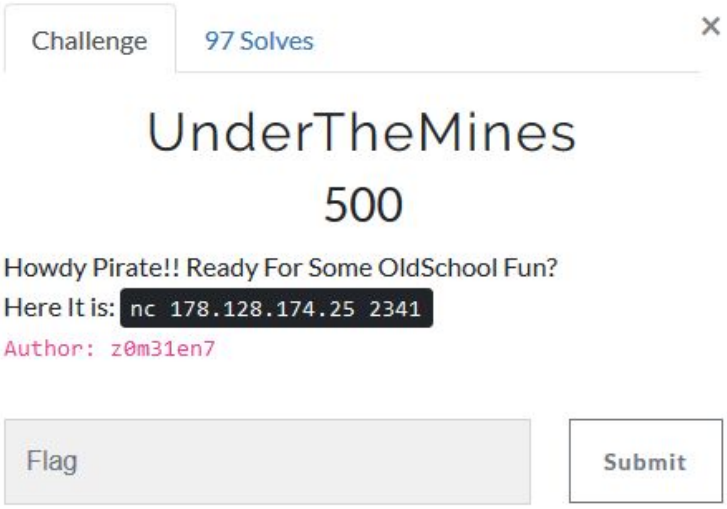
Berdasarkan clue yg di dapat yakni bahwa flag adalah password dr zip yg terkunci. Maka saya merapihkan teks pass.txt sehingga menjadi seperti dibawah ini.

disini saya melakukan bruteforce password terhadap file zip yg terkunci dengan wordlist pass.txt yg sebelumnya saya rapihkan. Saya menggunakan tools fcrack zip dengan payload "**fcrackzip -u -D -p pass.txt wearesecarmy.zip**", dan seperti yg bisa dilihat bahwa tahapan bruteforce sukses dan ditemukan password sekaligus flag kita yakni "**vestibulumi**"

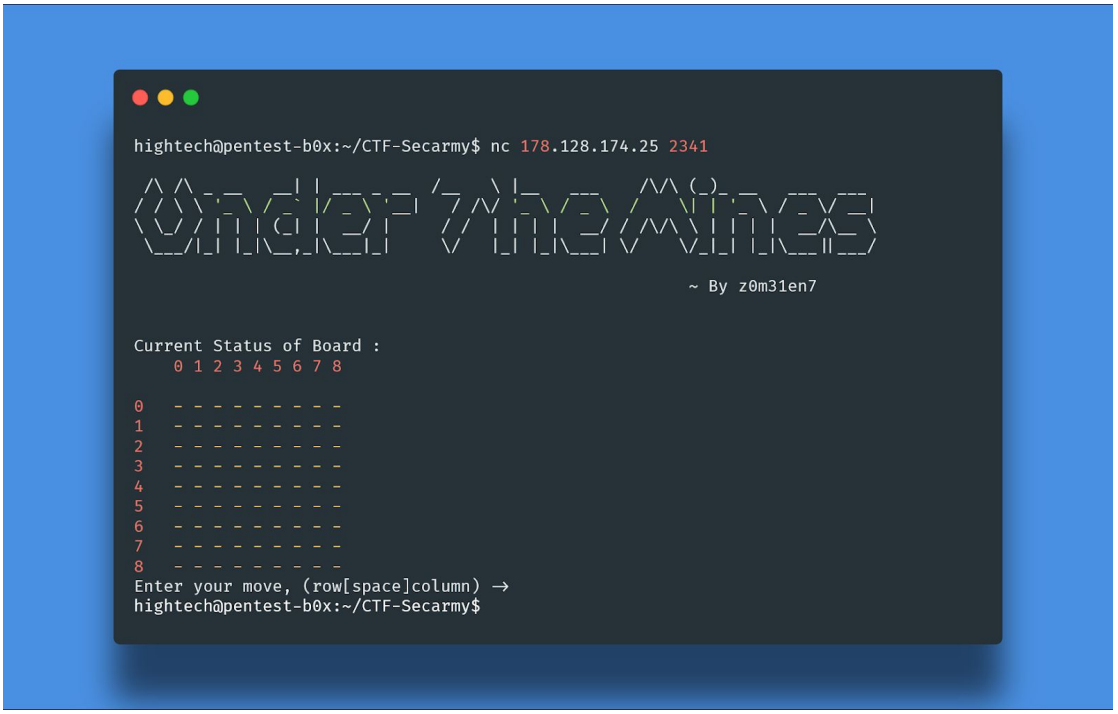
Flag:

secarmy{vestibulumi}

27. [Miscellaneous] - UnderTheMines [500]



Diberikan sebuah challenge sebagai berikut, kita harus connect ke service di servernya menggunakan command "nc 178.128.174.25 2341", setelah saya connect ternyata servicenya itu menjalankan game minesweeper. Pada tahapan ini cukup dimainin saja gamenya, tidak harus di exploitasi atau hal sejenis lainnya.

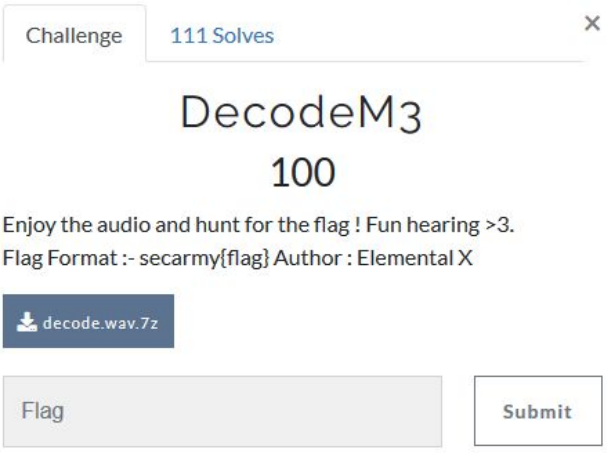


setelah banyak percobaan, akhirnya saya sukses memenangkan permainan minesweeper ini.

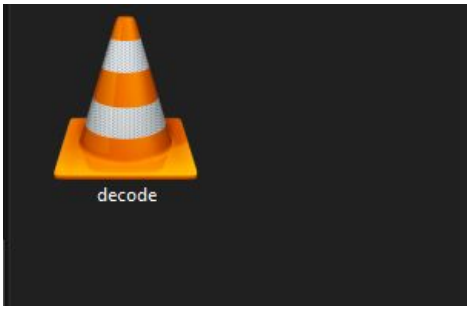
Flag:

secarmy{th3_cl@551c_m1n3sw33per}

28. [Forensics] - DecodeM3 [100]



Diberikan sebuah challenge sebagai berikut, isi dari file tersebut adalah sebuah file wav yg ternyata berisikan kode morse



disini saya pun mencoba untuk melakukan decoding morsecode dengan mengupload file tadi ke situs [Morse Translator](). Dan hasilnya adalah seperti ini

Flag:

secarmy{m0rsedec0ded}