



**Writeup CTF CHRIST (Deemed to be  
University)**

**[Hightech - KKN Back To Isekai]**

## **Daftar Isi**

[Welcome] - Introductions [10]	4
[Goodbye] - Goodbye [10]	6
[Starters] - Bln_B4sic [10]	8
[Starters] - Go Emoji [200]	9
[Starters] - Welcome [30]	10
[Programming] - SEC++ [30]	11
[Programming] - Power it Up! [100]	15
[Steganography] - Wings [50]	17
[Steganography] - SNOW [100]	20
[Web] - The Customer [100]	22
[Web] - The Classic User Panel [100]	24
[OSINT] - 1337_gUyz [20]	26
[OSINT] - E-Digger [200]	27
[Crypto] - SUM_IT_UP [70]	28
[Crypto] - Nothingness [100]	29
[Crypto] - Unit3d_COD3 [100]	30
[Crypto] - Old School [100]	31
[Crypto] - BabyRSA [100]	33
[Crypto] - T@P [200]	35
[Crypto] - Alien [200]	36
[Reversing] - N00b_R3v [100]	38
[Reversing] - Proper Algo [500]	39
[Miscellaneous] - ENCRYPTO X [60]	41
[Miscellaneous] - Dumpster Diving [100]	43
[Miscellaneous] - Multiple Ways [200]	45
[Miscellaneous] - CrackOut [200]	48
[Miscellaneous] - UnderTheMines [500]	50

## Write Up

*From Isekai, With Love*

### 1. [Welcome] - Introductions [10]

Challenge      447 Solves      X

## Introduction 2

We know you all are the smartest & sweetest beings of the universe , Do not hesitate to introduce yourself >3.

.<https://forms.gle/Vy9A2pyaAbWrXuae6>

Flag

Submit

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

**CHRIST (Deemed to be University) CTF  
2020**

Enter correct details to be eligible for the prize, Enter "none" wherever applicable

\* Wajib

Alamat email \*

Email Anda \_\_\_\_\_  
ⓘ Pertanyaan ini wajib diisi

Name \*

Jawaban Anda \_\_\_\_\_  
ⓘ Pertanyaan ini wajib diisi

Email ID \*

Enter a valid Email ID to contact you

Jawaban Anda \_\_\_\_\_  
ⓘ Pertanyaan ini wajib diisi

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

**CHRIST (Deemed to be University) CTF  
2020**

secarmy{w3lc0mes\_y0u}

**Flag:**

**secarmy{w3lc0mes\_y0u}**

## 2. [Goodbye] - Goodbye [10]

Challenge	50 Solves	X
<h1>Goodbye</h1> <p>10</p> <p>Hope you enjoyed it &gt;3.</p> <p>Do not forget to provide us a valuable feedback</p> <p><a href="https://forms.gle/gUNpXfvfstiwM3269">https://forms.gle/gUNpXfvfstiwM3269</a></p> <p>Goodbye !</p>		
Flag		Submit

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.

## Feedback Form

secarmy{th@nk\_y0u\_3v3ry0n3}

**Flag:**

**secarmy{th@nk\_y0u\_3v3ry0n3}**

### 3. [Starters] - B1n\_B4s1c [10]

Challenge      457 Solves      X

## B1n\_Bas1c

10

Welcome to the battlefield warrior ! More power to you ;)

Flag Format :- secarmy{flag} Author : Elemental X

[bin\\_base.zip](#)

Flag      Submit

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

```
01110011 01100101 01100011 01100001  
01110010 01101101 01111001 01111011  
01100010 00110001 01101110 01100001  
01110010 01111001 01011111 01101001  
01110011 01011111 01100011 00110000  
00110000 01101100 01111101
```

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

ASCII text

```
secarmy{binary_is_c001}
```

Hex (bytes)

```
73 65 63 61 72 6D 79 7B 62 31 6E 61 72 79 5F 69 73 5F 63 30  
30 6C 7D
```

Binary (bytes)

```
01110011 01100101 01100011 01100001  
01110010 01101101 01111001 01111011  
01100010 00110001 01101110 01100001  
01110010 01111001 01011111 01101001  
01110011 01011111 01100011 00110000  
00110000 01101100 01111101
```

Flag:

**secarmy{b1nary\_is\_c001}**

4. [Starters] - Go Emoji [200]

Challenge    215 Solves    X

## Go Emojis

20

Here's official server of SECARMY let's see if you can find the flag :)

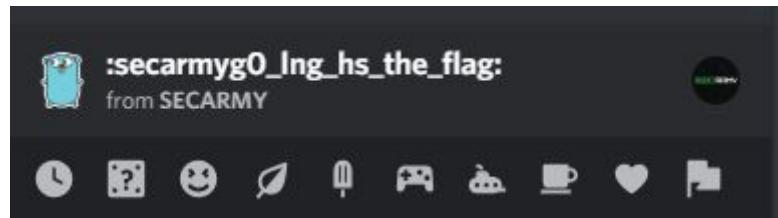
Server Link: <https://discord.gg/AMvR2WW>

Author: Umair9747

Flag Format :- secarmy{flag}

Flag    Submit

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]

Challenge	112 Solves
<h1>Welcome</h1> <h2>30</h2> <p>Welcome on the board ! Know about us and get your flag Flag Format : secarmy{flag} Author : CHRIST (Deemed to be University)</p>	
Flag	Submit

Dari Challenge ini, perhatian saya tertuju pada page [About](#), lalu saya mengexplore page about tersebut.

BTW are you in search for something? Here it is )<a href="https://www.google.com/search?q=site%3A%2F%2Fwww.google.com+site%3A%2F%2Fwww.google.com">https://www.google.com/search?q=site%3A%2F%2Fwww.google.com+site%3A%2F%2Fwww.google.com

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

BTW are you in search for something? Here it is ]TS1RHC\_L1@H\_IIA{ymraces

Contact: [cybersecurity@cs.christuniversity.in](mailto:cybersecurity@cs.christuniversity.in)

Powered by CTFd

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

```
hightech@pentest-b0x:~/CTF-Secarmy$ echo "}TS1RHC_L1@H_llA{ymraces" | rev  
secarmy{All_H@1L_CHR1ST}  
hightech@pentest-b0x:~/CTF-Secarmy$
```

**Flag:**

**secarmy{All H@1L CHR1ST}**

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

Challenge      169 Solves      X

SEC++;  
90

Oi! h0p3 y0u \$t1ll r3m3mb3r C++! d0n't y@?;)

Author : Umair9747

SECARMY{cpp\_1s\_TH3\_W@Y\_T0\_G0}

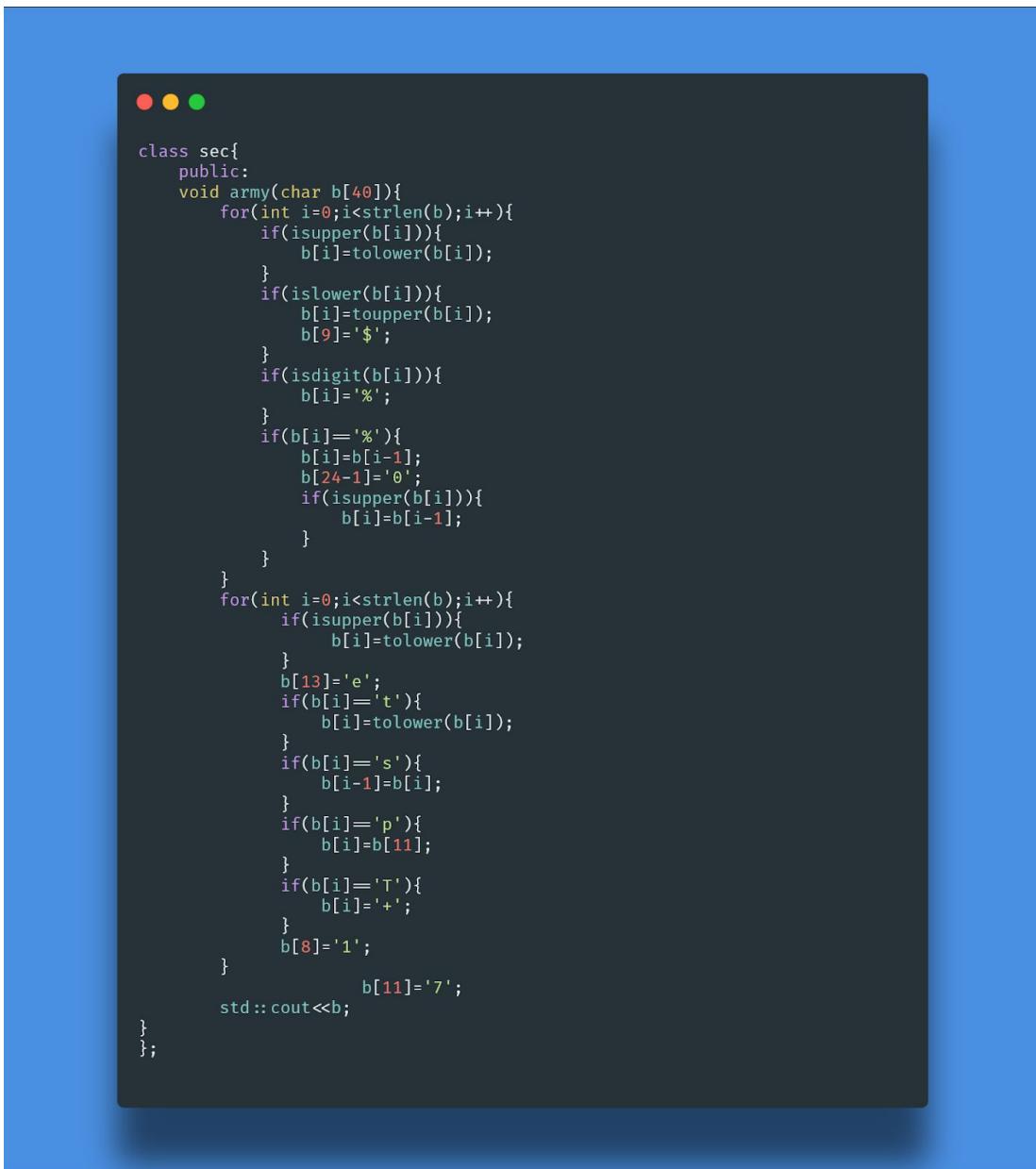
Flag format :- secarmy{flag}

 structOr.zip

Flag      Submit

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.

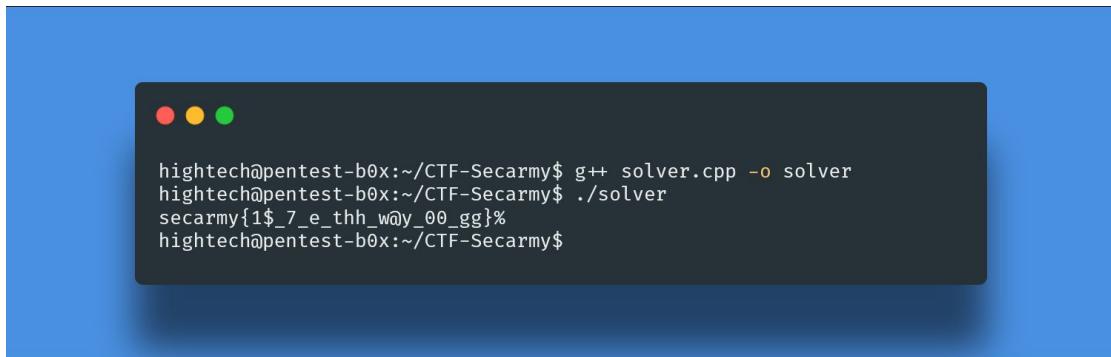


```
#include <iostream>
#include <string.h>

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_Way_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



```
hightech@pentest-b0x:~/CTF-Secarmy$ g++ solver.cpp -o solver
hightech@pentest-b0x:~/CTF-Secarmy$ ./solver
secarmy{1$_7_e_thh_w@y_00_gg}%
hightech@pentest-b0x:~/CTF-Secarmy$
```

**Flag:**

**secarmy{1\$\_7\_e\_thh\_w@y\_00\_gg}**

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

Challenge    94 Solves    X

# Power it Up !

## 100

It's a headache to debug this piece of Powershell script . Help me out to find the output & the flag is all yours ;)

Flag Format :- secarmy{flag}

Author : Elemental X

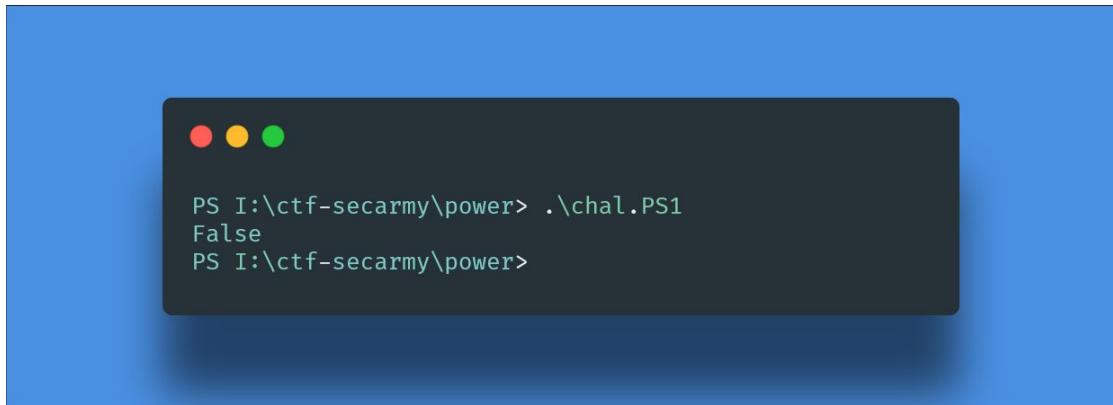
[power.zip](#)

Flag    Submit

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

```
$a = "Null"
$b = "0x00"
$c = "0x00" -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.



```
PS I:\ctf-secarmy\power> .\chal.ps1
False
PS I:\ctf-secarmy\power>
```

**Flag:**

**secarmy{False}**

8. [Steganography] - Wings [50]

Challenge      15 Solves      X

# Wings

## 50

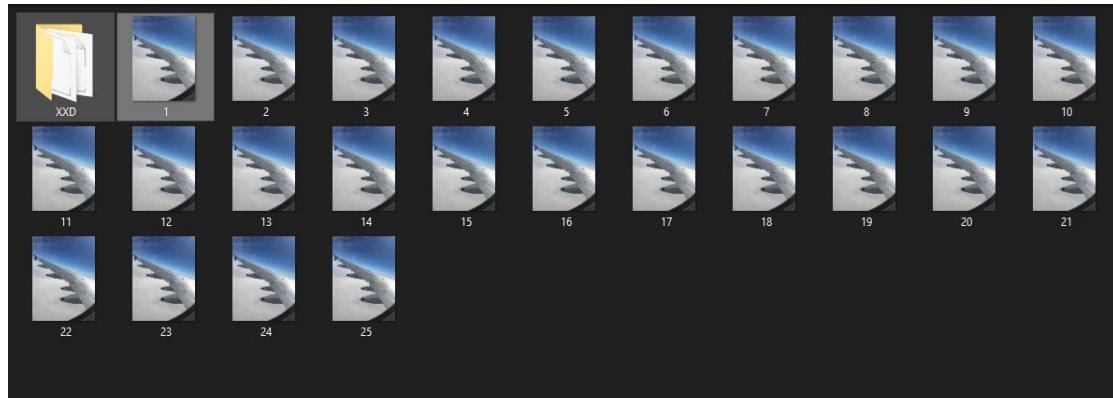
Unusual stuff in the image, pay close attention.

Author : WhoAmI??

 wings.zip

Flag      Submit

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 fdff 9f0e ff00 e8b7 8a7d ..Z....}
000f5c20: 1636 69d3 a3ff d973 0a .61....s.

hightech@pentest-b0x:~/CTF-Secarmy$ xxd 2.jpg | tail -2
000f5c10: eb57 0724 0ed0 5a7f f493 fdff 9f0e ff00 .W.$..Z....}
000f5c20: e8b7 8a7d 1636 69d3 a3ff d965 0a ...}.61....e.

hightech@pentest-b0x:~/CTF-Secarmy$ xxd 3.jpg | tail -2
000f5c00: eb57 0724 0ed0 5a7f f493 fdff 9f0e ff00 .W.$..Z....}
000f5c10: e8b7 8a7d 1636 69d3 a3ff d963 0a ...}.61....c.

hightech@pentest-b0x:~/CTF-Secarmy$ xxd 4.jpg | tail -2
000f5c00: 5a7f f493 fdff 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 fdff 9f0e ff00 e8b7 .$.Z....}
000f5c10: 8a7d 1636 69d3 a3ff d972 0a .}.61....r.

hightech@pentest-b0x:~/CTF-Secarmy$ xxd 6.jpg | tail -2
000f5c20: 0ed0 5a7f f493 fdff 9f0e ff00 e8b7 8a7d ..Z....}
000f5c30: 1636 69d3 a3ff d96d 0a .61....m.

hightech@pentest-b0x:~/CTF-Secarmy$ xxd 7.jpg | tail -2
000f5c20: fdff 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 fdff 9f0e ...W.$..Z....}
000f5c20: ff00 e8b7 8a7d 1636 69d3 a3ff d97b 0a .....}.61....{.

hightech@pentest-b0x:~/CTF-Secarmy$ xxd 9.jpg | tail -2
000f5c10: fdff 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 fdff 9f0e ff00 .W.$..Z....}
000f5c10: e8b7 8a7d 1636 69d3 a3ff d923 0a ...}.61....#.

hightech@pentest-b0x:~/CTF-Secarmy$ xxd 11.jpg | tail -2
000f5c20: fdff 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 fdff 9f0e ff00 e8b7 .$.Z....}
000f5c10: 8a7d 1636 69d3 a3ff d924 0a .}.61....$.

hightech@pentest-b0x:~/CTF-Secarmy$ xxd 13.jpg | tail -2
000f5c20: aad2 eb57 0724 0ed0 5a7f f493 fdff 9f0e ...W.$..Z....}
000f5c30: d931 0a .6i...._.

hightech@pentest-b0x:~/CTF-Secarmy$ xxd 14.jpg | tail -2
000f5c10: 9f0e ff00 e8b7 8a7d 1636 69d3 a3ff d931 .....}.6i...
000f5c20: 0a .

hightech@pentest-b0x:~/CTF-Secarmy$ xxd 15.jpg | tail -2
000f5c10: 5a7f f493 fdff 9f0e ff00 e8b7 8a7d 1636 Z....}.6
000f5c20: 69d3 a3ff d924 0a i....$.

hightech@pentest-b0x:~/CTF-Secarmy$ xxd 16.jpg | tail -2
000f5c00: 5a7f f493 fdff 9f0e ff00 e8b7 8a7d 1636 Z....}.6i...
000f5c20: 0a .

hightech@pentest-b0x:~/CTF-Secarmy$ xxd 17.jpg | tail -2
000f5c10: 69d3 a3ff d937 0a i....7.

hightech@pentest-b0x:~/CTF-Secarmy$ xxd 18.jpg | tail -2
000f5c10: f493 fdff 9f0e ff00 e8b7 8a7d 1636 69d3 .....}.6i.
000f5c20: a3ff d923 0a ...#.

hightech@pentest-b0x:~/CTF-Secarmy$ xxd 19.jpg | tail -2
000f5c10: f493 fdff 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 fdff 9f0e ff00 .W.$..Z....}
000f5c10: e8b7 8a7d 1636 69d3 a3ff d95f 0a ...}.61...._.

hightech@pentest-b0x:~/CTF-Secarmy$ xxd 21.jpg | tail -2
000f5c10: 0ed0 5a7f f493 fdff 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 fdff 9f0e ff00 .W.$..Z....}
000f5c10: e8b7 8a7d 1636 69d3 a3ff d931 0a ...}.61....1.

hightech@pentest-b0x:~/CTF-Secarmy$ xxd 23.jpg | tail -2
000f5c10: 0724 0ed0 5a7f f493 fdff 9f0e ff00 e8b7 .$.Z....}.
000f5c20: 8a7d 1636 69d3 a3ff d940 0a .}.61....@.

hightech@pentest-b0x:~/CTF-Secarmy$ xxd 24.jpg | tail -2
000f5c00: eb57 0724 0ed0 5a7f f493 fdff 9f0e ff00 .W.$..Z....}
000f5c10: e8b7 8a7d 1636 69d3 a3ff d939 0a ...}.61....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]

Challenge      174 Solves      X

# SNOW

## 100

Snow & Snow everywhere , can you help me to find the flag ?  
Flag Format :- secarmy{flag}  
Author: D4RK LEGEND

 SNOW.zip

[Flag](#)      [Submit](#)

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 enemy'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 succeeded 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 medical board determined that not a day should be lost in sending me back to England. I was despatched, accordingly, in the troopship Oronites, 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 alarming 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.



```
hightech@pentest-b0x:~/CTF-Secarmy$ ./snow -C decode.txt
Flag is c2VjYXJteXtDbGVhcl9UaGVfU25vd30=%
hightech@pentest-b0x:~/CTF-Secarmy$ base64 -d <<< c2VjYXJteXtDbGVhcl9UaGVfU25vd30=
secarmy{Clear_The_Snow}%
hightech@pentest-b0x:~/CTF-Secarmy$
```

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

**Flag:**

**secarmy{Clear\_The\_Snow}**

## 10. [Web] - The Customer [100]

Challenge    61 Solves    X

# The Customer

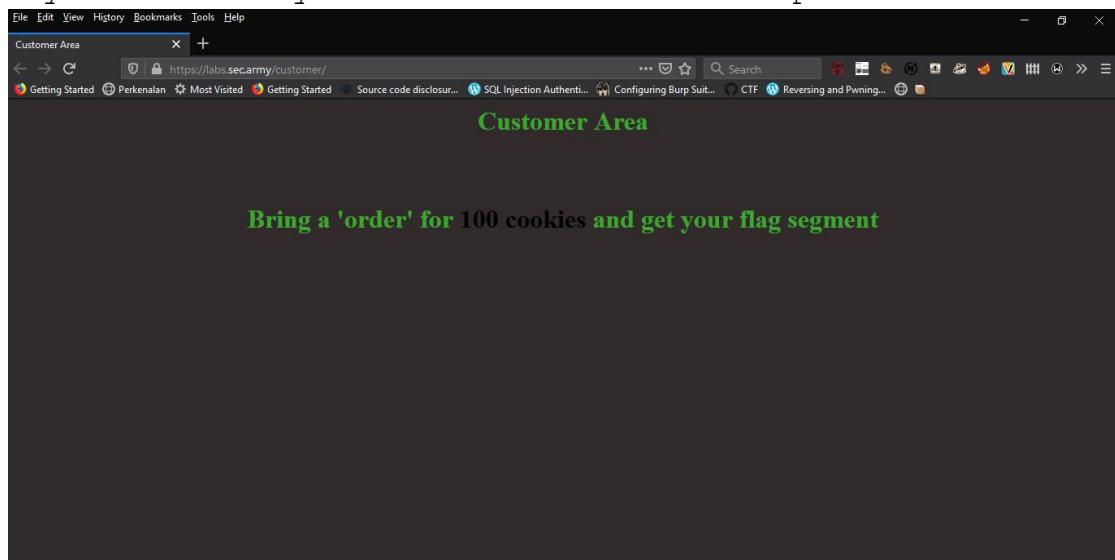
## 100

Hey, I just joined a cookie store but I think I won't be able to perform the job which had been ordered by my manager.  
Please help me out!

<https://labs.sec.army/customer/>

Author : Umair9747

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

A screenshot of a Firefox browser window. The address bar shows 'https://labs.secarmy/customer/'. The main content area displays a message: 'Bring a 'order' for 100 cookies and get your flag segment'. A cookie list table is shown, with one row selected:

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure
clduid	d29b1d5c29b73b04a7...	sec.army		1584376253	51	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<b>order</b>	<b>100</b>	<b>.sec.army</b>	<b>/</b>	<b>02 / 17 / 2020</b>	<b>8</b>	<input type="checkbox"/>	<input type="checkbox"/>

A modal dialog box is open, showing the details for the 'order' cookie:

Name	order
Domain	.sec.army
Path	/
Expiration (ISO)	02 / 17 / 2020 05:41:48 .000 PM
<input type="checkbox"/> HostOnly	<input type="checkbox"/> Session
<input type="checkbox"/> Secure	<input type="checkbox"/> HttpOnly

Buttons at the bottom of the modal include 'Export', 'Reset', 'Remove', and 'Expand'.

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

A screenshot of a Firefox browser window. The address bar shows 'https://labs.secarmy/customer/'. The main content area displays a message: 'Customer Area' and 'Bring a 'order' for 100 cookies and get your flag segment'. A modal dialog box is open, displaying the flag:

secarmy{h3r3s\_s0m3\_fr33\_c00k13s\_f0r\_y0u}

A button labeled 'OK' is visible at the bottom of the modal.

Flag:

**secarmy{h3r3s\_s0m3\_fr33\_c00k13s\_f0r\_y0u}**

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

Challenge    25 Solves    X

# The Classic User Panel

## 100

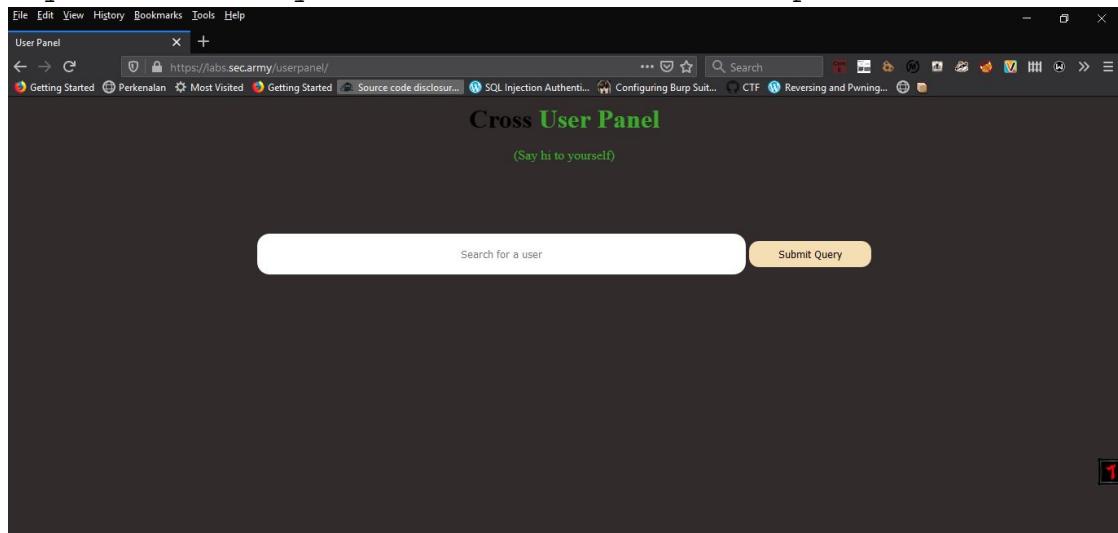
Hey looks like the User Panel of my store is pretty outdated and is sort of vulnerable. Go have some fun out there ;)

<https://labs.sec.army/userpanel/>

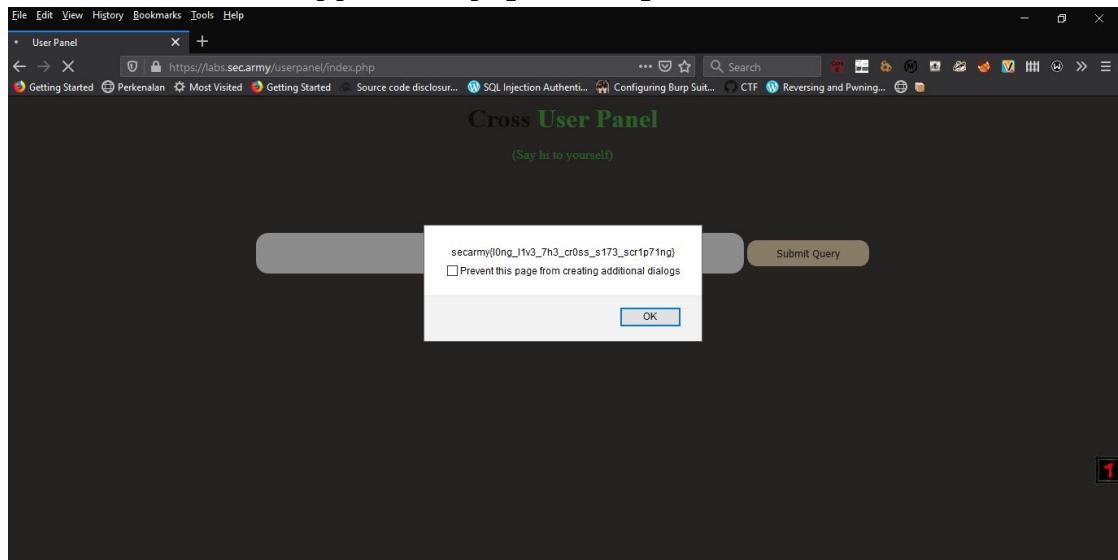
Author : Umair9747

Flag    Submit

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}**

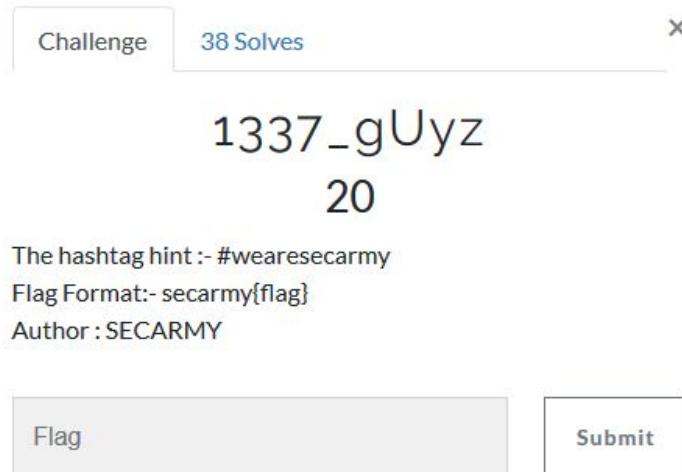
## 12. [OSINT] - 1337\_gUyz [20]

Challenge      38 Solves      X

1337\_gUyz  
20

The hashtag hint :- #wearesecarmy  
Flag Format:- secarmy{flag}  
Author :SECARMY

Flag      Submit



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 mengguna 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]

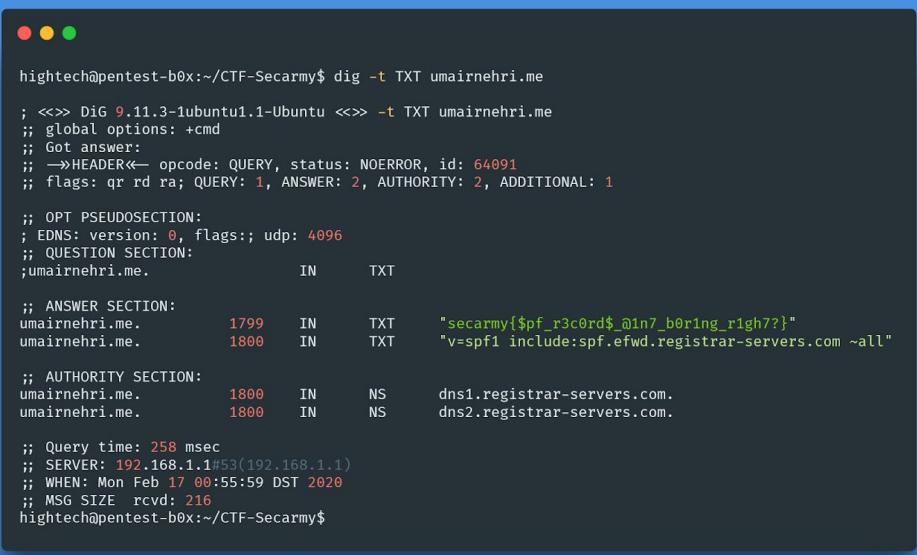
Challenge    82 Solves    X

## E-Digger 200

Hey there , our team member just found his new domain name but I am not sure if I should email through it . Please check out .  
<http://umairnehri.me/>

Flag Format :- secarmy {flag}  
Author : Umair9747

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



```
hightech@pentest-b0x:~/CTF-Secarmy$ dig -t TXT umairnehri.me
; <>> DiG 9.11.3-1ubuntu1.1-Ubuntu <>> -t TXT umairnehri.me
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 64091
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 1
;
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;umairnehri.me.           IN      TXT
;
;; ANSWER SECTION:
umairnehri.me.        1799    IN      TXT    "secarmy{$pf_r3c0rd$_@in7_b0r1ng_r1gh7?}"
umairnehri.me.        1800    IN      TXT    "v=spf1 include:spf.efwd.registrar-servers.com ~all"
;
;; AUTHORITY SECTION:
umairnehri.me.        1800    IN      NS     dns1.registrar-servers.com.
umairnehri.me.        1800    IN      NS     dns2.registrar-servers.com.
;
;; Query time: 258 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Mon Feb 17 00:55:59 DST 2020
;; MSG SIZE rcvd: 216
hightech@pentest-b0x:~/CTF-Secarmy$
```

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\$\_@in7\_b0r1ng\_r1gh7?}**

## 14. [Crypto] - SUM\_IT\_UP [70]

Challenge    67 Solves    X

# SUM\_IT\_UP

70

My newbie scripting friend just got fooled by one of his friend and the message has been hidden using Powershell , if you help him to understand, I hope he will provide you the flag.

Warning: You might be fooled !

Flag Format:- secarmy{flag}

Author: Elemental X

[flag.zip](#)

Flag    Submit

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](#).

The screenshot shows a web-based cipher tool interface. On the left, there is a text input field containing "D642C>JL#\_E6?". In the center, there is a "ROT13" dropdown menu with a "VARIANT" section containing options: ROT5 (0-9), ROT13 (A-Z, a-z), ROT18 (0-9, A-Z, a-z), and ROT47 (!~). The "ROT47 (!~)" option is selected. Below the dropdown, it says "Decoded 14 chars". On the right, the output text is "secarmy{R00ten".

Dan bagian terakhirnya adalah ROT-13

The screenshot shows the same web-based cipher tool interface. On the left, there is a text input field containing "pvcure". In the center, there is a "ROT13" dropdown menu with a "VARIANT" section containing options: ROT5 (0-9), ROT13 (A-Z, a-z), ROT18 (0-9, A-Z, a-z), and ROT47 (!~). The "ROT13 (A-Z, a-z)" option is selected. Below the dropdown, it says "Decoded 6 chars". On the right, the output text is "cipher".

Flag:

**secarmy{R00tencipher}**

## 15. [Crypto] - Nothingness [100]

Challenge    11 Solves    X

# Nothingness

## 100

Life is although void , but SECARMY can help you out , hope you get it >3.

Flag Format:- secarmy{flag}

Author :- Elemental X

[Download flag.zip](#)

Flag    Submit

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]

Challenge    125 Solves    X

# Unit3d\_COD3

## 100

We unite to code.  
Flag Format:- secarmy{flag}  
Author : Elemental X

[Flag.zip](#)

Flag    Submit

Diberikan sebuah challenge sebagai berikut, isi dari file zip tsb adalah sebuah ciphertext seperti ini "73; 65; 63; 61; 72; 6d; 79; 7b; 49; 5f; 6c; 30; 76; 65; 5f; 55; 6e; 69; 63; 30; 64; 65; 0; 7d;", disini saya mencoba menganti "&x" menjadi "U+" lalu saya mencoba mendecode sebagai [Unicode Code Points](#) dan sukses.

The screenshot shows a three-panel interface for converting between Unicode code points and text. The left panel displays a list of hex values: U+73 U+65 U+63 U+61 U+72 U+6D U+79 U+7B U+49 U+5F U+6C U+30 U+76 U+65 U+5F U+55 U+6E U+69 U+63 U+30 U+64 U+65 U+0 U+0 U+7D. The middle panel has dropdown menus for 'VIEW' (set to 'Text'), 'ENCODE' (disabled), 'DECODE' (set to 'Unicode code points'), 'SEPARATOR' (set to a blank line), and 'FORMAT' (set to 'Unicode notation'). The right panel shows the resulting text: secarmy{I\_love\_Unic0de}.

Flag:

**secarmy{I\_10ve\_Unic0de}**

## 17. [Crypto] - Old School [100]

Challenge    242 Solves    X

# Old School

## 100

Hope the name is enough for you  
Flag Format :- secarmy{flag}  
Author: Thellusion

 DA.zip

[Flag](#)    [Submit](#)

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 01000011 01100111 01001111 01010100 01000111 01100111 01001101 01010100 01000001 00110100 01001001 01000100  
01000101 01110111 01001101 01010011 01000001 00110101 01001110 01111001 01000001 01111000 01001101 01000100 01100111  
01000111 01001101 01010100 01000001 01111010 01001001 01000100 01111000 01001101 01000100 01111000 01000001 01111000  
01001101 01001001 01100111 01001101 01010100 01000001 00110001 01001001 01000101 01111000 01001101 01000001 01111000  
01001101 01010100 01000001 01100111 01001101 01010100 01000001 00110001 01001001 01000101 01111000 01001101 01000001 01111000  
01001001 01111000 01001101 01000100 01010001 01001111 01001101 01010100 01000001 00110101 01010100 01000001 00110101 01001001 01000100
```

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

ASCII text

```
MTAwIDEyMSAxMTcgOTggMTA4IDEwMSA5NyAxMDggMTAzIDEyMSAxMTQgMTA1IDEy  
NiAxMDQgMTA5IDEyNQ==
```

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.

The screenshot shows a three-panel interface for decoding Base64. The left panel contains the Base64 encoded string: 'MTAwIDEExMSAxHTcgOTggMTA4IDEwMSA5NyAxMDggMTAzIDExMSAxMTQgMTA1IDEExNiAxMDQgMTA5IDEExNQ=='. The middle panel has 'Base64' selected under 'DECODE' and 'Base64 (RFC 3548, RFC 4648)' under 'VARIANT'. The right panel displays the decoded output as a series of decimal numbers: '100 111 117 98 108 101 97 108 103 111 114 105 116 104 109 115'. A message at the bottom indicates '→ Decoded 61 bytes'.

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

The screenshot shows a three-panel interface for decoding decimal numbers to text. The left panel contains the decimal numbers: '100 111 117 98 108 101 97 108 103 111 114 105 116 104 109 115'. The middle panel has 'Unicode code points' selected under 'DECODE' and 'Decimal' selected under 'FORMAT'. The right panel displays the resulting text: 'doublealgorithms'.

**Flag:**

**secarmy{doublealgorithms}**

## 18. [Crypto] - BabyRSA [100]

Challenge    36 Solves    X

# BabyRSA

## 100

Hey , hope your basics are pretty clear.

Flag Format:- secarmy{flag}

Author : Error404

 RSA.7z

Flag    Submit

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

```
● ● ●

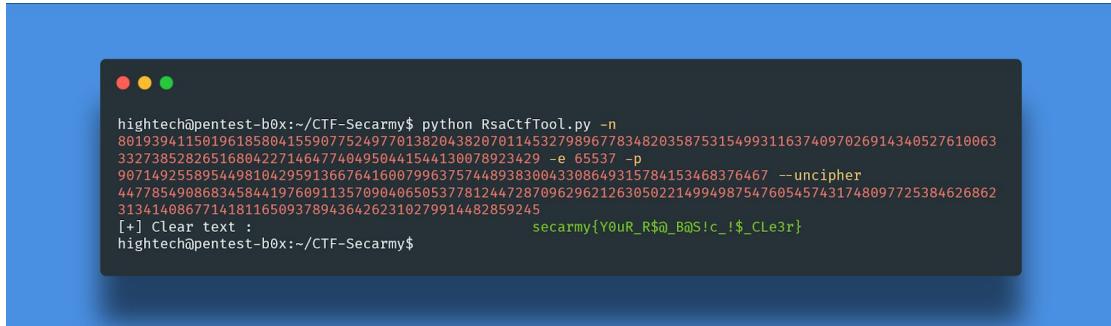
from Crypto.Util.number import *

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= 8019394115019618580415590775249770138204382070114532798967783482035875315499311637409702691434052761006333273852826516804
227146477404950441544130078923429
p= 90714925589544981042959136676416007996375744893830043308649315784153468376467
ct= 447785490868345844197609113570904065053778124472870962962126305022149949875476054574317480977253846268623134140867714181
1650937894364262310279914482859245

disini saya pun mencoba untuk melakukan Uncipher menggunakan [RSACTfTool](#) dan hasilnya sukses. Flagnya berhasil saya uncipher



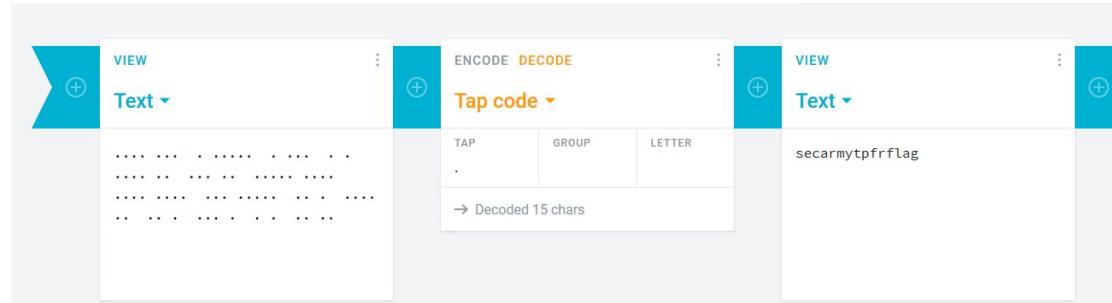
```
hightech@pentest-b0x:~/CTF-Secarmy$ python RsaCtfTool.py -n
80193941158196185804155907752497701382043820701145327989677834820358753154993116374097026914340527610063
33273852826516894227146477484950441544130078923429 -e 65537 -p
90714925589544981042959136676416007996375744893830043308649315784153468376467 --uncipher
44778549086834584419760911357090406505377812447287096296212630502214994987547605457431748097725384626862
31341408677141811650937894364262310279914482859245
[+] Clear text : secarmy{Y0uR_R$@_B@S!c_!$_CLe3r}
hightech@pentest-b0x:~/CTF-Secarmy$
```

**Flag:**

**secarmy{Y0uR\_R\$@\_B@S!c\_!\$\_CLe3r}**

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

Challenge	89 Solves
X	
<p>T@P 200</p> <p>Feel the dots to get the flag. Flag Format :- secarmy{flag} Author : Elemental X</p> <p> tp.zip</p>	
Flag	Submit



**Flag:**

**secarmy{tpfrflag}**

## 20. [Crypto] - Alien [200]

Challenge    27 Solves    X

# Alien

200

Aliens on the way ..

Flag Format : secarmy{flag}

Author: The Illusion

 ct.txt

secarmy{[invalid syntax!]}

Submit

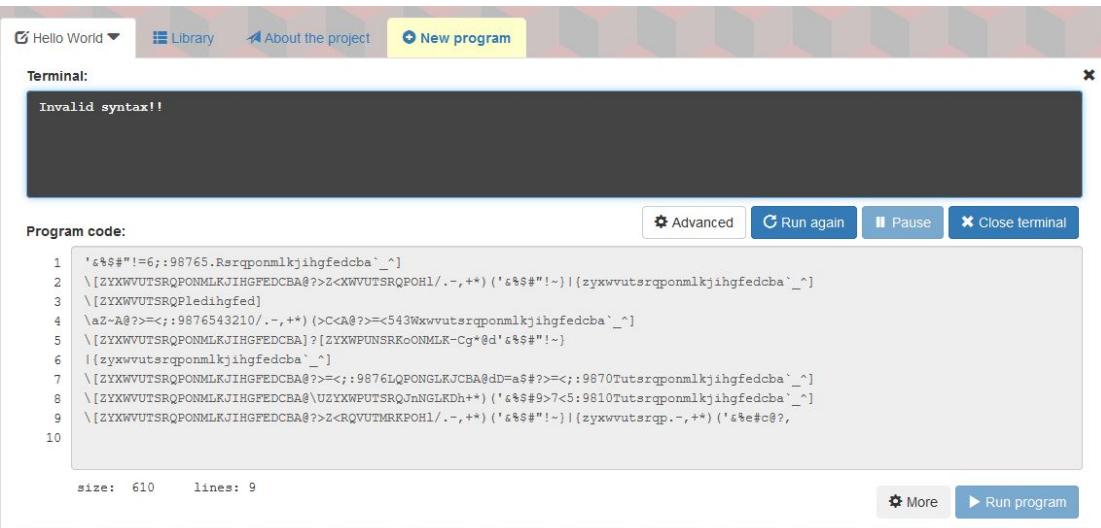
Diberikan sebuah challenge sebagai berikut, isi dari file zip tsb adalah sebuah ciphertext seperti ini, disini saya pun mencoba untuk merapihkan cipher terlebih dahulu.

```
'&%$#!=6;:98765.Rsrqponmlkjihgfedcba`_^\[[ZYXWVUTSRQPONMLKJIHGFE DCBA@?>Z<XW VUTSRQPOH1/..,+*)(`&%$#!~}\{|zyxwvutsrqponmlkjihgfedcba`_^\[[ZYXWVUTSRQPledihg fed]\|aZ~A@?>=<;:9876543210/..,+*)(>C<A@?>=<543Wxwvutsrqponmlkjihgfedcba`_^\[[ZYXWVUTSRQPONMLKJIHGFE DCBA]?[ZYXWPUNS RKOONMLK-Cg*@d'&%$#!~}\{|zyxwvutsrqponmlkjihgfedcba`_^\[[ZYXWVUTSRQPONMLKJIHGFE DCBA@?>=<;:9876LQ PONGLKJCBA@dD=a$#?>=<;:9870Tutsrqponmlkjihgfedcba`_^\[[ZYXWVUTSRQPONMLKJIHGFE DCBA@?\UZYXWPUTSR QJnNGLKDh+*)(`&%$#9>7<5:9810Tutsrqponmlkjihgfedcba`_^\[[ZYXWVUTSRQPONMLKJIHGFE DCBA@?>Z<RQVUTMRKPOH1/..,+*)(`&%$#!~}\{|zyxwvutsrqp.-,+*)(`&%e#c@?,
```

Hasil setelah dirapihkan seperti dibawah ini

```
'&%$#!=6;:98765.Rsrqponmlkjihgfedcba`_^\[[ZYXWVUTSRQPONMLKJIHGFE DCBA@?>Z<XW VUTSRQPOH1/..,+*)(`&%$#!~}\{|zyxwvutsrqponmlkjihgfedcba`_^\[[ZYXWVUTSRQPledihg fed]\|aZ~A@?>=<;:9876543210/..,+*)(>C<A@?>=<543Wxwvutsrqponmlkjihgfedcba`_^\[[ZYXWVUTSRQPONMLKJIHGFE DCBA]?[ZYXWPUNS RKOONMLK-Cg*@d'&%$#!~}\{|zyxwvutsrqponmlkjihgfedcba`_^\[[ZYXWVUTSRQPONMLKJIHGFE DCBA@?>=<;:9876LQ PONGLKJCBA@dD=a$#?>=<;:9870Tutsrqponmlkjihgfedcba`_^\[[ZYXWVUTSRQPONMLKJIHGFE DCBA@?\UZYXWPUTSR QJnNGLKDh+*)(`&%$#9>7<5:9810Tutsrqponmlkjihgfedcba`_^\[[ZYXWVUTSRQPONMLKJIHGFE DCBA@?>Z<RQVUTMRKPOH1/..,+*)(`&%$#!~}\{|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



The screenshot shows a terminal window titled "Terminal" with the message "Invalid syntax!!". Below the terminal is a code editor window titled "Program code:" containing a multi-line string of characters. The code editor has buttons for "Advanced", "Run again", "Pause", and "Close terminal". At the bottom, it shows "size: 610 lines: 9".

```
1 '¢$#!=6;:98765.Rsrqponmlkjihgfedcba`_~]
2 \[ZXWVUTSRQPONMLKJIHGFEDECBA@?>Z<XWVUTSRQPQH1/.-,+*) ('¢$#!~) | {zyxwvutsrqponmlkjihgfedcba`_~]
3 \[ZYXWVUTSRQPledihgfed]
4 \az~@?>=<c;; 9876543210/.-,+*) (>C<@?>=<543Wxwvutsrqponmlkjihgfedcba`_~]
5 \[ZYXWVUTSRQPONMLKJJIHGFEDECBA]?[ZYXWPUNSRRKoONMLK-Cg*@d'¢$#!~]
6 \|{zyxwvutsrqponmlkjihgfedcba`_~]
7 \[ZYXWVUTSRQPONMLKJIHGFEDECBA@?>=<; 9876LQPONGLKJCBA@dD=a$#?>=<; 9870Tutsrqponmlkjihgfedcba`_~]
8 \[ZYXWVUTSRQPONMLKJIHGFEDECBA@\UZYXWPUNSRQJnNGLKDh++*) ('¢$#!~7<5: 9810Tutsrqponmlkjihgfedcba`_~]
9 \[ZYXWVUTSRQPONMLKJIHGFEDECBA@?>Z<RQVUTMRKPQH1/.-,+*) ('¢$#!~) | {zyxwvutsrqp.-,+*) ('¢e#c@?,
```

**Flag:**

**secarmy{Invalid syntax!!}**

## 21. [Reversing] - N00b\_R3v [100]

Challenge    132 Solves    X

# Noob\_R3v

100

Just Debug It >3  
Flag Format : secarmy{flag}  
Author : Elemental X

[debug](#)

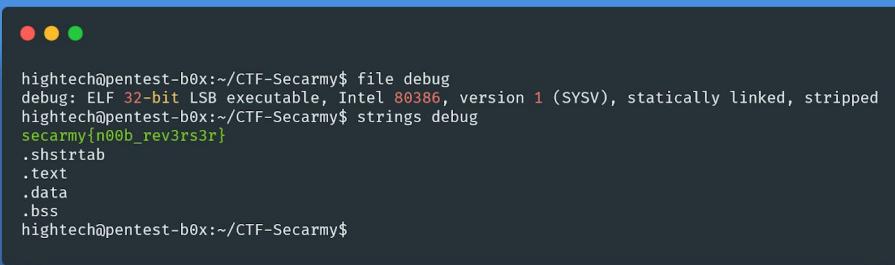
Flag    Submit

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



```
hightech@pentest-b0x:~/CTF-Secarmy$ file debug
debug: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, stripped
hightech@pentest-b0x:~/CTF-Secarmy$
```

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

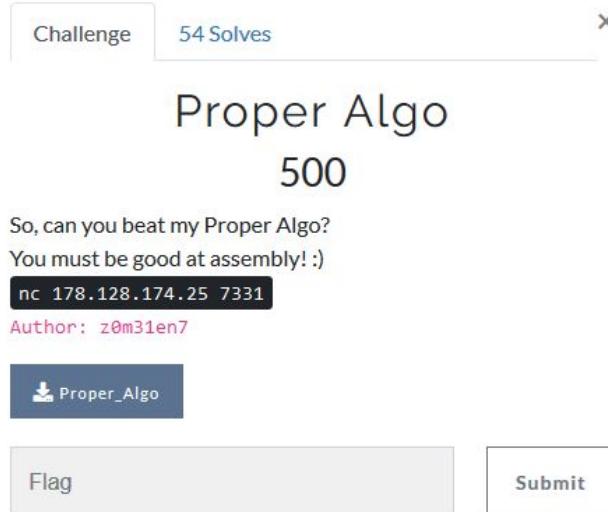


```
hightech@pentest-b0x:~/CTF-Secarmy$ file debug
debug: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, stripped
hightech@pentest-b0x:~/CTF-Secarmy$ strings debug
secarmy{n00b_rev3rs3r}
.shstrtab
.text
.data
.bss
hightech@pentest-b0x:~/CTF-Secarmy$
```

**Flag:**

**secarmy{n00b\_rev3rs3r}**

## 22. [Reversing] - Proper Algo [500]



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

```
hightech@pentest-b0x:~/CTF-Secarmy$ file Proper_Algo
Proper_Algo: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, interpreter
/lib64/ld-linux-x86-64.so.2, for GNU/Linux 3.2.0,
BuildID[sha1]=a79336e9ebff36519c1b8f56f446c2c2b1176630, not stripped
hightech@pentest-b0x:~/CTF-Secarmy$
```

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("GööGöÉGöùGö%GöçGöÉGöíGöÉGöíGöÉGöùGö%GöçGöÉ GööGöÉGöùGö% GöíGöÉGöíGöÉ");
puts("GöáGöùGö%GöéGöùGöéGöéGöùGöýGöü GöéGöùGöé GöéGö%GöéGöé");
puts("Gö~ Gö|Göö GööGöýGö| GööGöýGö|Göö Gö~ Gö~Gö|GöýGööGöýGööGöý");
puts("\t\tBy 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.

```
100796628
100796628+27
100796655-2999
100793656+34
100793690-59
100793631-944
100792687-201092
100591595-101483
100490112-323302
100166810-290027
```

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

```
hightech@pentest-b0x:~/CTF-Secarmy$ nc 178.128.174.25 7331
PROPER ALG
~By z0m31en7

Enter The License Key:
99876783
You are a Worthy one, Here is your flag:
secarmy{proper_alg05_were_mu57}
hightech@pentest-b0x:~/CTF-Secarmy$
```

**Flag:**

**secarmy{pr0p3r\_alg05\_@re\_mu57}**

**23. [Miscellaneous] - ENCRYPTO X [60]**

Challenge    70 Solves    X

## ENCRYPTO X

60

One of my friend sent me this binary with two keys "ENCODE" & "DECODE" and told me the keys are case-sensitive . I am unable to find the hidden message inside , can you help me out ?:(

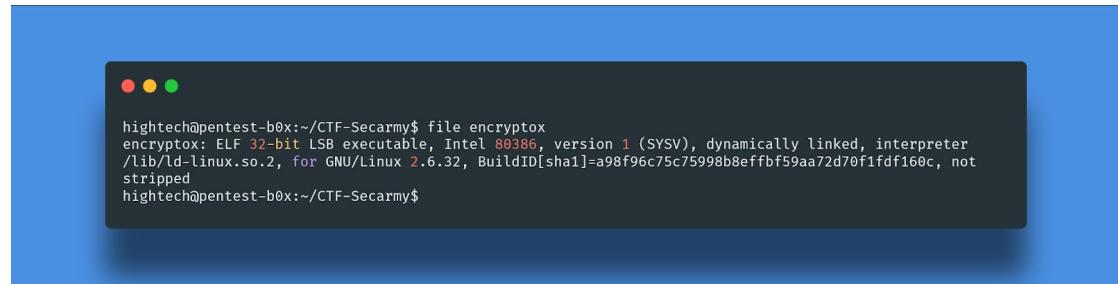
Flag Format :- secarmy{flag}

Author : Elemental X

[encryptox](#)

[Flag](#)    [Submit](#)

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



```
hightech@pentest-b0x:~/CTF-Secarmy$ file encryptox
encryptox: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked, interpreter
/lib/ld-linux.so.2, for GNU/Linux 2.6.32, BuildID[sha1]=a98f96c75c75998b8effbf59aa72d70f1fdf160c, not
stripped
hightech@pentest-b0x:~/CTF-Secarmy$
```

disini saya pun mencoba untuk melakukan reversing menggunakan IDA, Pada fungsii 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;          v82 = *MK_FP(__GS__, 20);
*v53 = 'OCNE';
v54 = 'ED';
*(DWORD *)v55 = 'OCED';
v56 = 'ED';
v57 = '@';
v70 = 'A';
v71 = '-';
v72 = '+';
v73 = '?';
v74 = '@';
v75 = '$';
v76 = 'b';
v77 = '4';
v78 = '8';
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';
```

C

Hasil dari decode char tsb adalah “**A-+!@\$b409XDencodedbits**” namun setelah saya analisa lagi ternyata flag nya adalah “**encodedbits**”

**Flag:**

**secarmy{encodedbits}**

## 24. [Miscellaneous] - Dumpster Diving [100]

Challenge    65 Solves    X

# Dumpster Diving

## 100

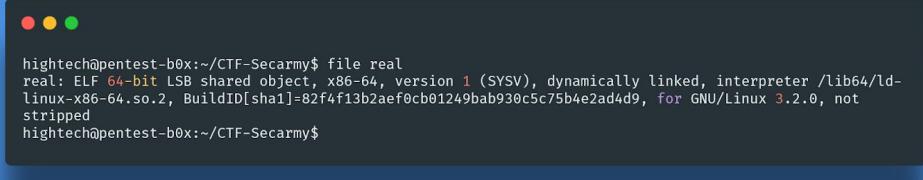
Always follow the format , if you understand the format, the flag is all yours , beware of fake flags. To know more about it :-  
<https://searchsecurity.techtarget.com/definition/dumpster-diving>

Flag Format :- secarmy{flag}  
Author ; Elemental X

[GIBBER.zip](#)     [real](#)

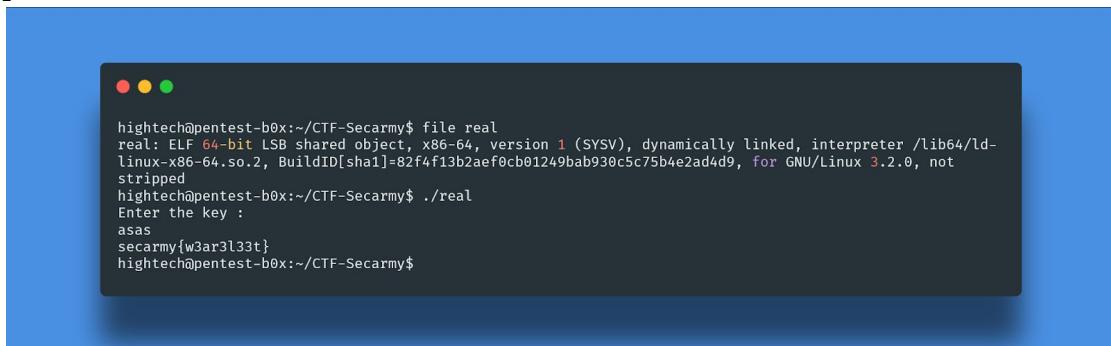
Diberikan sebuah challenge sebagai berikut, isi dari file tersebut adalah sebuah file binary dan file zip yg berisikan encoding base64



hightech@pentest-b0x:~/CTF-Secarmy\$ file real  
real: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, BuildID[sha1]=82f4f13b2aef0cb01249bab930c5c75b4e2ad4d9, for GNU/Linux 3.2.0, not stripped  
hightech@pentest-b0x:~/CTF-Secarmy\$

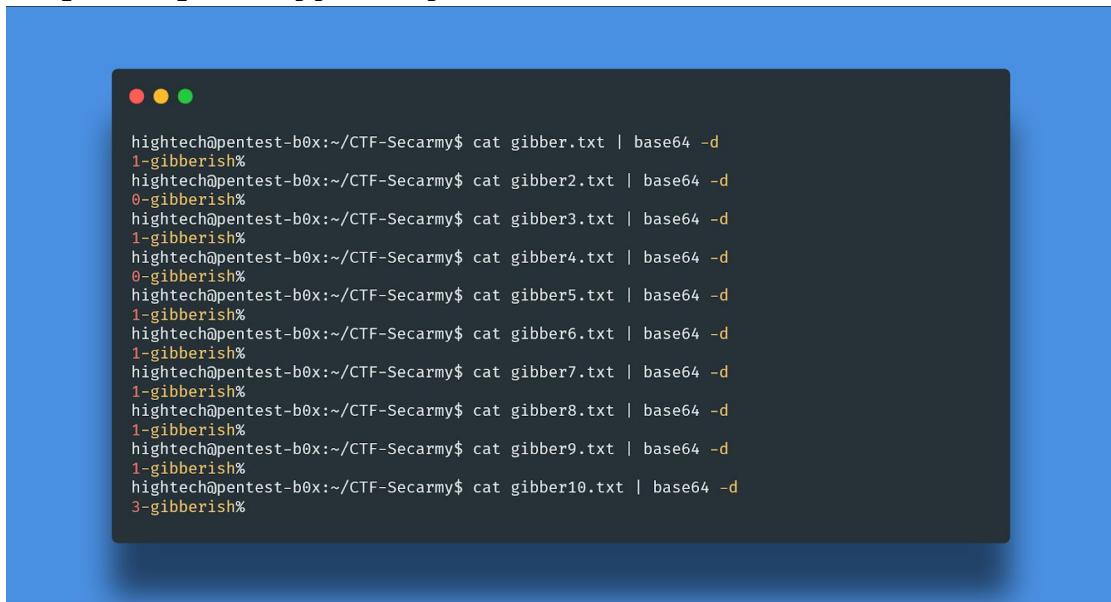
File	Last Modified	Type	Size
gibber	30/12/2019 17:17	TXT File	1 KB
gibber2	30/12/2019 17:17	TXT File	1 KB
gibber3	30/12/2019 17:18	TXT File	1 KB
gibber4	30/12/2019 17:19	TXT File	1 KB
gibber5	30/12/2019 17:23	TXT File	1 KB
gibber6	30/12/2019 17:23	TXT File	1 KB
gibber7	30/12/2019 17:23	TXT File	1 KB
gibber8	30/12/2019 17:24	TXT File	1 KB
gibber9	30/12/2019 17:24	TXT File	1 KB
gibber10	30/12/2019 17:24	TXT File	1 KB

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



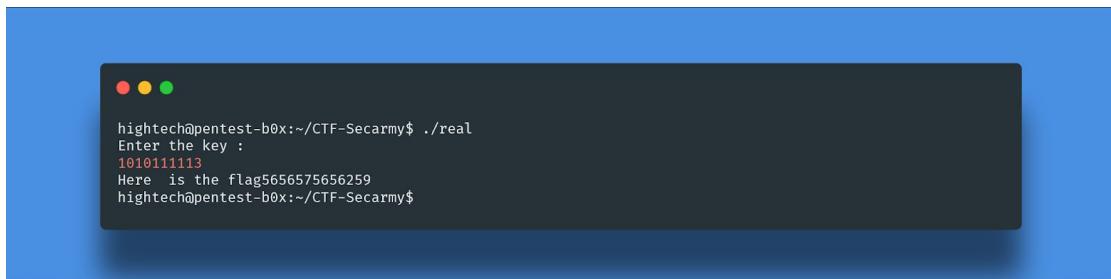
```
hightech@pentest-b0x:~/CTF-Secarmy$ file real
real: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, BuildID[sha1]=82f4f13b2aef0cb01249bab930c5c75b4e2ad4d9, for GNU/Linux 3.2.0, not stripped
hightech@pentest-b0x:~/CTF-Secarmy$ ./real
Enter the key :
asas
secarmy{w3ar3l33t}
hightech@pentest-b0x:~/CTF-Secarmy$
```

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"



```
hightech@pentest-b0x:~/CTF-Secarmy$ cat gibber.txt | base64 -d
1-gibberish%
hightech@pentest-b0x:~/CTF-Secarmy$ cat gibber2.txt | base64 -d
0-gibberish%
hightech@pentest-b0x:~/CTF-Secarmy$ cat gibber3.txt | base64 -d
1-gibberish%
hightech@pentest-b0x:~/CTF-Secarmy$ cat gibber4.txt | base64 -d
0-gibberish%
hightech@pentest-b0x:~/CTF-Secarmy$ cat gibber5.txt | base64 -d
1-gibberish%
hightech@pentest-b0x:~/CTF-Secarmy$ cat gibber6.txt | base64 -d
1-gibberish%
hightech@pentest-b0x:~/CTF-Secarmy$ cat gibber7.txt | base64 -d
1-gibberish%
hightech@pentest-b0x:~/CTF-Secarmy$ cat gibber8.txt | base64 -d
1-gibberish%
hightech@pentest-b0x:~/CTF-Secarmy$ cat gibber9.txt | base64 -d
1-gibberish%
hightech@pentest-b0x:~/CTF-Secarmy$ cat gibber10.txt | base64 -d
3-gibberish%
```

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.



```
hightech@pentest-b0x:~/CTF-Secarmy$ ./real
Enter the key :
1010111113
Here is the flag5656575656259
hightech@pentest-b0x:~/CTF-Secarmy$
```

**Flag:**

**secarmy{5656575656259}**

**25. [Miscellaneous] - Multiple Ways [200]**

Challenge    41 Solves    X

## Multiple Ways

200

I love various encoding schema like Enigma and what not , also I feel encoding my keys are safe . Can you crack them ?

Flag Format :- secarmy{flag}

Author : Elemental X

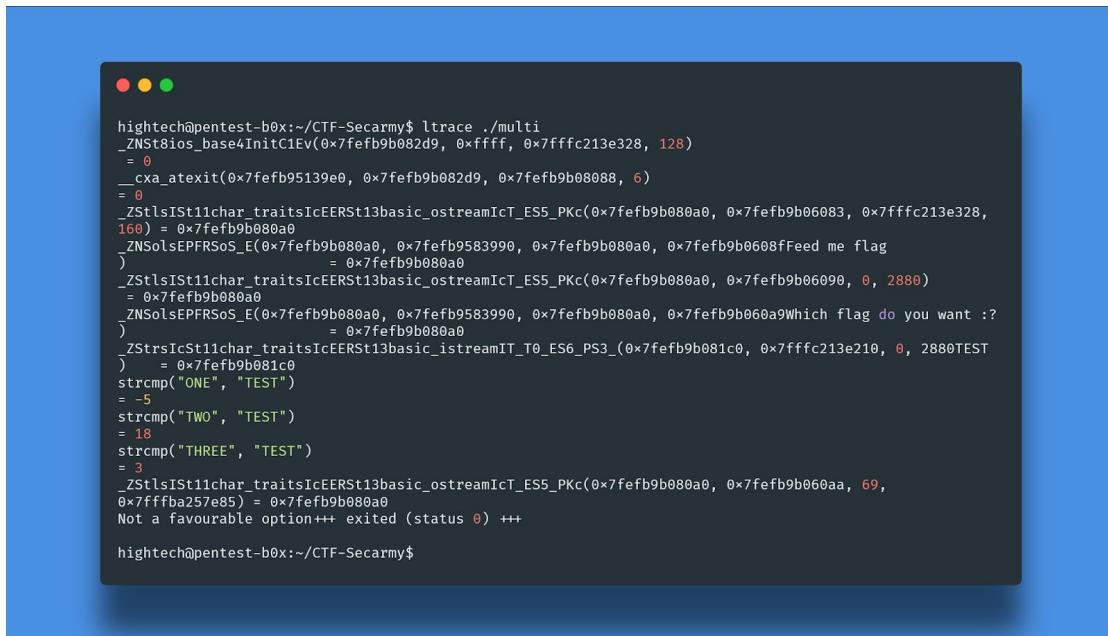
[multi](#)     [keys.zip](#)

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

```
hightech@pentest-b0x:~/CTF-Secarmy$ file multi
multi: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, BuildID[sha1]=9f91731373b848924aa16070496cba80cbdc05b4, for GNU/Linux 3.2.0, not
stripped
hightech@pentest-b0x:~/CTF-Secarmy$
```

File	Modified	Type	Size
key1	08/12/2019 13:53	TXT File	1 KB
key2	08/12/2019 13:54	TXT File	1 KB
key3	08/12/2019 13:54	TXT File	1 KB

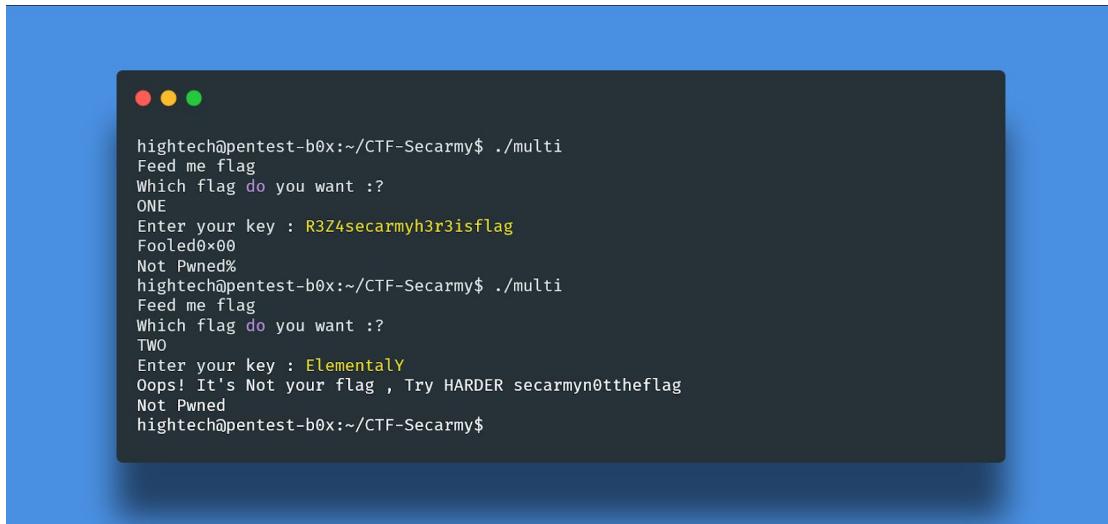
disini saya melakukan analisa dan ternyata file key tersebut hanya sebuah pengecoh. Saya coba melakukan ltrace dan melihat pada strcmp bahwa file binary tsb dapat menerima 3 Inputan, yakni **“ONE, TWO, THREE”**. Masing-masing pilihan ternyata berbeda.



```
hightech@pentest-b0x:~/CTF-Secarmy$ ltrace ./multi
_ZNst8ios_base4InitC1Ev(0x7fefb9b082d9, 0xffff, 0x7ffc213e328, 128)
= 0
__cxa_atexit(0x7fefb95139e0, 0x7fefb9b082d9, 0x7fefb9b08088, 6)
= 0
_ZStlsISt11char_traitsIcEERSt13basic_ostreamIcT_ES5_PKc(0x7fefb9b080a0, 0x7fefb9b06083, 0x7ffc213e328,
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
_ZStlsIcSt11char_traitsIcEERSt13basic_istreamIT_T0_ES6_PS3_(0x7fefb9b081c0, 0x7ffc213e210, 0, 2880TEST
) = 0x7fefb9b081c0
strcmp("ONE", "TEST")
= -5
strcmp("TWO", "TEST")
= 18
strcmp("THREE", "TEST")
= 3
_ZStlsISt11char_traitsIcEERSt13basic_ostreamIcT_ES5_PKc(0x7fefb9b080a0, 0x7fefb9b060aa, 69,
0x7fffb257e85) = 0x7fefb9b080a0
Not a favourable option++ exited (status 0) +++

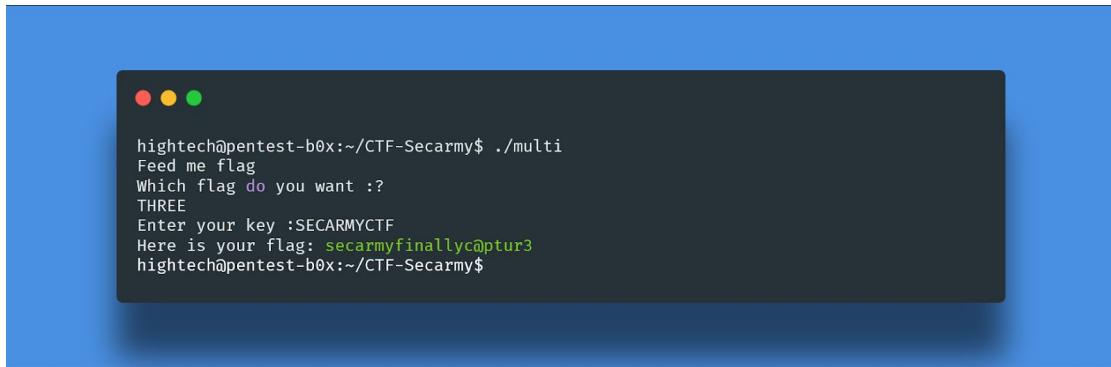
hightech@pentest-b0x:~/CTF-Secarmy$
```

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.



A terminal window with a blue header bar containing three colored dots (red, yellow, green). The main area shows the following text:

```
hightech@pentest-b0x:~/CTF-Secarmy$ ./multi
Feed me flag
Which flag do you want :?
THREE
Enter your key :SECARMYCTF
Here is your flag: secarmyfinallyc@ptur3
hightech@pentest-b0x:~/CTF-Secarmy$
```

**Flag:**

**secarmy{finallyc@ptur3}**

## 26. [Miscellaneous] - CrackOut [200]

Challenge      33 Solves      X

# CrackOut

## 200

Check out each & every letter :) , key itself is the flag  
Flag Format:- secarmy{flag}  
Author : Logan47

[pass.zip](#)      [wearesecarm...](#)

Flag      Submit

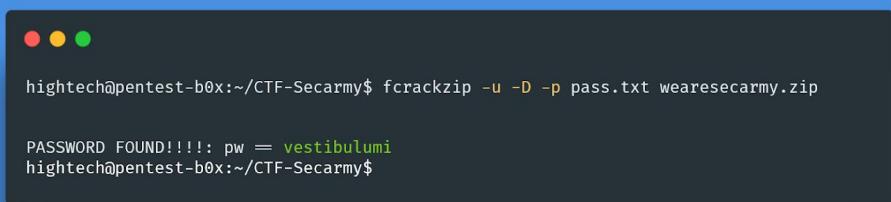
Diberikan sebuah challenge sebagai berikut, isi dari file tersebut adalah sebuah file txt dan file zip yg lainnya berisikan sebuah gambar namun terkunci. Isi dari pass.txt tersebut adalah kumpulan text seperti di bawah ini.

```
curabitur vitae hunc 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 duis 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 duis 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 duis sapien
egestas 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 vulputate sed cras ornare arcu duis 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.

```
1 curabitur
2 |vitae
3 nunc
4 sed
5 velit
6 dignissim
7 sodales
8 ut
9 eu
10 sem
11 integer
12 vitae
13 justo
14 eget
15 magna
```

disini saya melakukan bruteforce password terhadap file zip yg terkunci dengan wordlist pass.txt yg sebelumnya saya rapihkan. Saya menggunakan tools fcrackzip 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**"



```
hightech@pentest-b0x:~/CTF-Secarmy$ fcrackzip -u -D -p pass.txt wearesecarmy.zip

PASSWORD FOUND!!!!: pw = vestibulumi
hightech@pentest-b0x:~/CTF-Secarmy$
```

**Flag:**

**secarmy{vestibulumi}**

27. [Miscellaneous] - UnderTheMines [500]

Challenge

97 Solves

X

# UnderTheMines

## 500

Howdy Pirate!! Ready For Some OldSchool Fun?

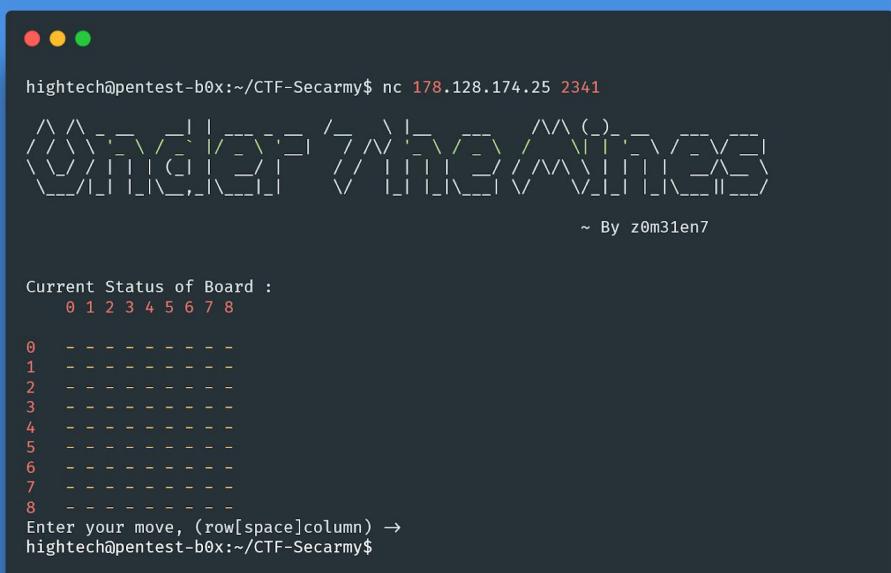
Here It is: nc 178.128.174.25 2341

Author: z0m3ien7

Flag

Submit

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.



```
hightech@pentest-b0x:~/CTF-Secarmy$ nc 178.128.174.25 2341

~ By z0m3ien7

Current Status of Board :
 0 1 2 3 4 5 6 7 8

0  - - - - - -
1  - - - - - -
2  - - - - - -
3  - - - - - -
4  - - - - - -
5  - - - - - -
6  - - - - - -
7  - - - - - -
8  - - - - - -
Enter your move, (row[space]column) →
hightech@pentest-b0x:~/CTF-Secarmy$
```

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

```
hightech@pentest-b0x:~/CTF-Secarmy$ nc 178.128.174.25 2341

$$\begin{array}{ccccccccc} / & \backslash & - & \_ & \backslash & / & | & / & \_ \\ \backslash & \backslash & / & | & | & | & ( & | & \_ \\ \_ & \_ & / & | & | & | & \_ & / & \_ \end{array}$$


$$\begin{array}{ccccccccc} / & \backslash & \backslash & ( & ) & - & \_ & \backslash & \_ \\ \backslash & \backslash & / & | & | & | & \_ & / & \_ \\ \_ & \_ & / & | & | & | & \_ & \_ & \_ \end{array}$$


$$\begin{array}{ccccccccc} \_ & \_ & \_ & \_ & \_ & \_ & \_ & \_ & \_ \end{array}$$

~ By z0m31en7

0 1 2 3 4 5 6 7 8

0 0 1 1 0 0 0 0 1 -
1 2 - 2 0 0 1 1 2 1
2 2 - 2 - 1 3 - 2 1
3 1 2 2 2 - 3 - 2 1
4 0 0 0 1 1 2 2 1 1
5 0 0 0 0 0 0 0 0 1
6 0 0 0 0 0 0 0 0 1 -
7 0 0 1 1 0 0 0 1 1
8 1 1 - 1 0 0 0 0 0

Enter your move, (row[space]column) → 8 0

0 1 2 3 4 5 6 7 8

0 0 1 1 0 0 0 0 1 -
1 2 - 2 0 0 1 1 2 1
2 2 - 2 - 1 3 - 2 1
3 1 2 2 2 - 3 - 2 1
4 0 0 0 1 1 2 2 1 1
5 0 0 0 0 0 0 0 0 1
6 0 0 0 0 0 0 0 0 1 -
7 0 0 1 1 0 0 0 1 1
8 1 1 - 1 0 0 0 0 0

Enter your move, (row[space]column) → 7 3

You Won Pirate!! here, take the flag: secarmy{th3_c10551c_m1n3sw33per}
hightech@pentest-b0x:~/CTF-Secarmy$
```

**Flag:**

**secarmy{th3 cl@551c m1n3sw33per}**

## 28. [Forensics] - DecodeM3 [100]

Challenge      111 Solves      X

# DecodeM3

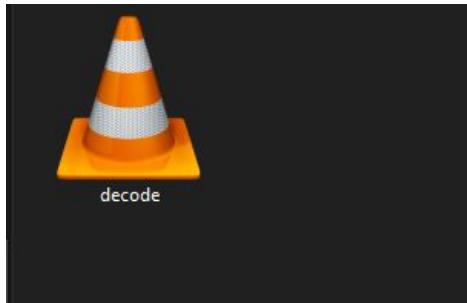
100

Enjoy the audio and hunt for the flag ! Fun hearing >3.  
Flag Format :- secarmy{flag} Author : Elemental X

 decode.wav.7z

Flag      Submit

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

Or analyse an audio file containing Morse code:

Upload  Play  Stop  Filename: "decode.wav"

SECARMYMORSEDECODED



**Flag:**

**secarmy{m0rsedec0ded}**