Proof Of Concept
Cyber Security Hackathon

NAMA TIM : P4/UI

Minggu, 20 November 2022

Ketua Tim

1. A. Athoillah

Member

1. Ahmad Ryan Faizal
2. Rezka Norhafizah
3. Reja Revaldy F

DIGITAL FORENSIC

[Strs]

Executive Summary

Diberikan file berupa gambar dengan format jpg.

Technical Report

Kami mengunduh file gambar tersebut dan menggunakan tool strings untuk mendapatkan flag kemudian kami grep untuk memudahkan pencarian.

```
yunj1@Yunj1:~/hackathon/forensic$ strings chall.jpg | grep cyber
cyberwarriors{Strings_Strings_Strings_Strings}
```

Conclusion

Mengetahui teks yang tersembunyi dalam sebuah gambar menggunakan tool strings
Flag = cyberwarriors{Strings_Strings_Strings_Strings}

[Stego]

Executive Summary

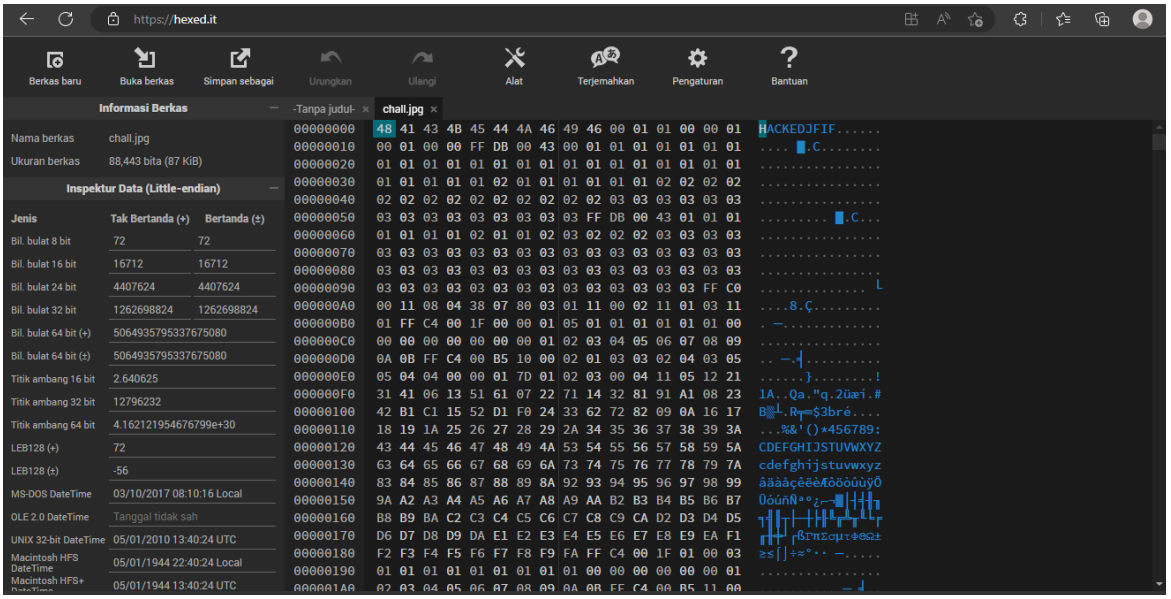
Diberikan sebuah file gambar yang ketika dibuka terdapat pesan error, serta hint bahwa ada pesan tersembunyi pada file tersebut.

Technical Report

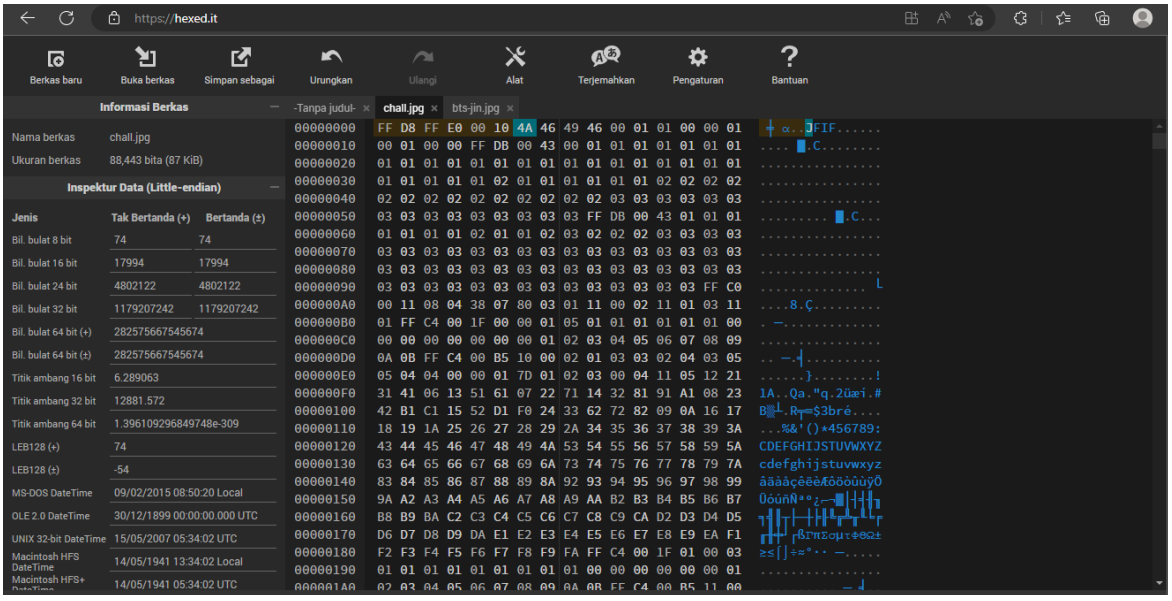
1. Kami mengunduh soal dan ternyata ketika diidentifikasi file tersebut merupakan file corrupt yang tidak dapat dibaca :

```
yunj1@Yunj1:~$ file chall.jpg
chall.jpg: data
```

2. Kemudian kami melihat ke dalam header file tersebut menggunakan hexeditor dan kami mengasumsikan bahwa file tersebut adalah file gambar berformat jpg berdasarkan header nya (JFIF).



3. Untuk memperbaiki file tersebut, kami membandingkannya dengan file jpg yang bisa dibuka, sehingga headernya menjadi seperti berikut :

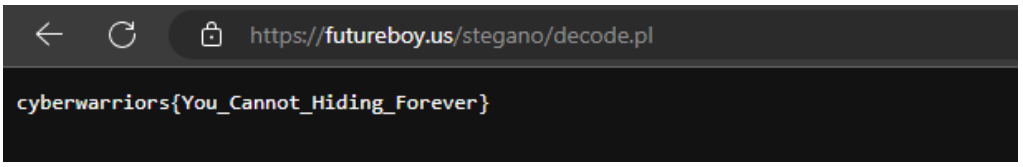


4. Setelah itu, kami coba buka kembali dan ternyata berhasil. Gambar tersebut ternyata hanya berupa gambar kosong berwarna putih dan kami selanjutnya mencoba untuk menganalisisnya menggunakan tools stegsolve dan didapat key nya :

Kamu nanya key nya apa?
Sini biar aku kasih tau yha
Jadi Key nya adalah
"CyberWarriorsHackathon2022"
yha, Rawrrrr

Ya ampun gini banget soal CTF

5. Selanjutnya kami menggunakan tool steghide online di https://futureboy.us/stegano/decinput.html dan kami inputkan passphrasenya menggunakan key tadi, maka didapat flagnya :



Conclusion

Memperbaiki header file yang sudah di-*damage* dan menemukan pesan tersembunyi pada file tersebut.

Flag = cyberwarriors{You_Cannot_Hiding_Forever}

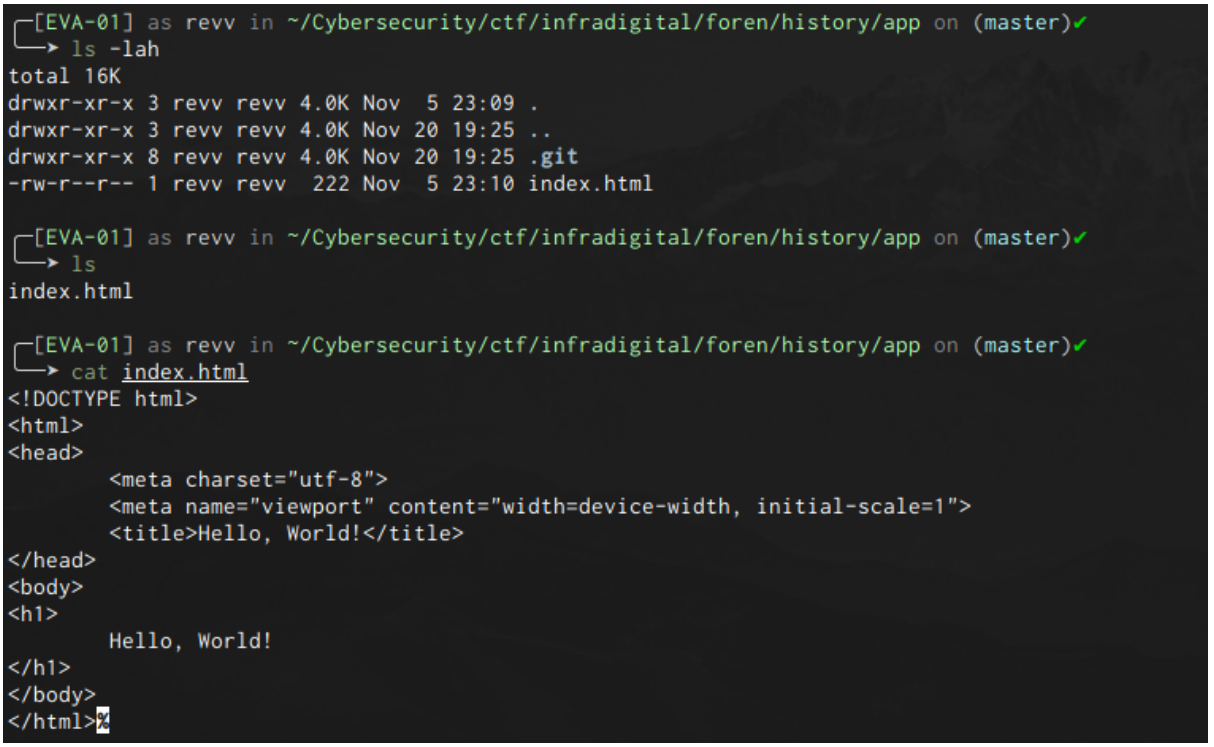
[History]

Executive Summary

Diberikan file zip yang berisikan folder yang berisikan file index.html.

Technical Report

1. Disini kami menemukan bahwa folder tersebut menggunakan git dan saya melakukan pengecekan terlebih dahulu terhadap file index.html



2. Setelah itu kami melakukan pengecekan terhadap log git tersebut dan menemukan beberapa commit sebelumnya

```
┌─[EVA-01] as revv in ~/Cybersecurity/ctf/infradigital/foren/history/app on (master)✔
└─➤ git log
commit e541f933d88c29cb0244e0168d461276186af058 (HEAD -> master)
Author: Cyber Warriors <cyber@warriors.com>
Date:   Sat Nov 5 23:10:50 2022 +0700

    update index.html

commit a383108098a0b8a14cd25f7592f511b2f2f88bba
Author: Cyber Warriors <cyber@warriors.com>
Date:   Sat Nov 5 23:10:16 2022 +0700

    update index.html

commit b5560b5d12cc242ad7350680f4953f561e2a5ffa
Author: Cyber Warriors <cyber@warriors.com>
Date:   Sat Nov 5 23:09:31 2022 +0700

    add index.html

commit b96f3f90db47d1f6844c269057fc8b2862ce151e
Author: Cyber Warriors <cyber@warriors.com>
Date:   Sat Nov 5 23:08:40 2022 +0700

    add index
```

3. Langsung saja kami melakukan pengecekan terhadap commit tersebut satu persatu dan membaca file yang ada di commit tersebut dan menemukan flagnya

```
┌─[EVA-01] as revv in ~/Cybersecurity/ctf/infradigital/foren/history/app on (master)✔
└─➤ git checkout b96f3f90db47d1f6844c269057fc8b2862ce151e
Note: switching to 'b96f3f90db47d1f6844c269057fc8b2862ce151e'.

You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by switching back to a branch.

If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -c with the switch command. Example:

  git switch -c <new-branch-name>

Or undo this operation with:

  git switch -

Turn off this advice by setting config variable advice.detachedHead to false

HEAD is now at b96f3f9 add index

┌─[EVA-01] as revv in ~/Cybersecurity/ctf/infradigital/foren/history/app on (b96f3f9)✔
└─➤ ls
index.php

┌─[EVA-01] as revv in ~/Cybersecurity/ctf/infradigital/foren/history/app on (b96f3f9)✔
└─➤ cat index.php
<?php
$flag = "cyberwarriors{Becareful_with_your_git!}";
?>
```

Conclusion

Melakukan pengecekan terhadap git log
Flag = cyberwarriors{Becareful_with_your_git!}

CRYPTOGRAPHY

[One Xor Away]

Executive Summary

Diberikan dua buah file yang berisikan file encryption menggunakan python dan hasil dari encryption tersebut di file flag.enc

Technical Report

1. Setelah kami coba analisis file python tersebut saya tertarik di baris python ini

```
def main():
        f = open('flag.txt').read()
        k = randint(1, 256)
```

2. Ternyata text di encrypt menggunakan xor dengan angka diantara 1 - 256, disini kami mencoba untuk melakukan bruteforce

```
┌─[EVA-01] as revv in ~/Cybersecurity/ctf/infradigital/crypto/xor
└─➤ cat decrypt.py
#!/usr/bin/env python3

from random import randint
from base64 import *


def decrypt():
    data = "PiQ/OC8qPC8vNDIvLiYzMikCOig4Li40MzoCNyguKQI/LygpODsyLz40MzoCKTU8KQIyMzgCPyQpOCA="
    data = b64decode(data)

    for x in range(1, 256):
        flag = "".join(chr(i ^ x) for i in data)
        if "cyberwarriors{" in flag:
            return f'{x} = {flag}'


def main():
    print(decrypt())


if __name__ == "__main__":
    main()

┌─[EVA-01] as revv in ~/Cybersecurity/ctf/infradigital/crypto/xor
└─➤ python3 decrypt.py
93 = cyberwarriors{not_guessing_just_bruteforcing_that_one_byte}
```

3. Ditemukan flag di encrypt menggunakan xor dengan kunci 93

Conclusion

Bruteforce key dari xor.
Flag = cyberwarriors{not_guessing_just_bruteforcing_that_one_byte}

WEB EXPLOITATION

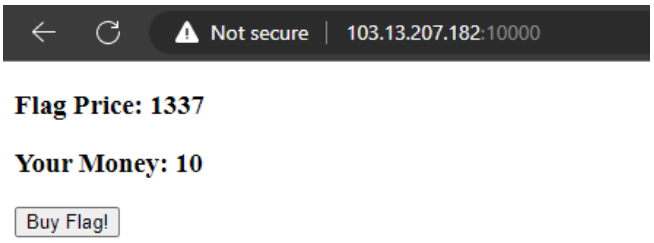
[Tamperer]

Executive Summary

Diberikan sebuah website dengan tampilan berupa form untuk membeli flag.

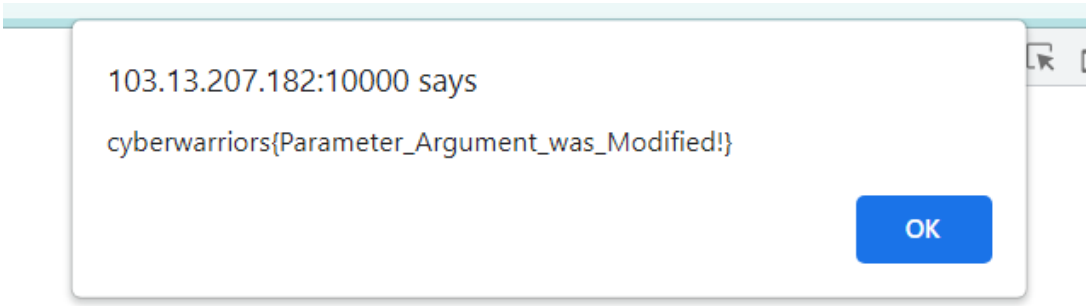
Technical Report

1. Kami membuka web soal dengan tampilan seperti berikut :



2. Setelah itu simpel saja karena uang yang dibutuhkan adalah 1337 untuk membeli flag maka kami ganti valuenya dari 10 menjadi 1337

3. Jadi tinggal disubmit ulang maka didapatkan lah flagnya



Conclusion

Mengubah value yang akan disubmit

Flag= cyberwarriors{Parameter_Argument_was_Modified!}

[PHP Sandbox]

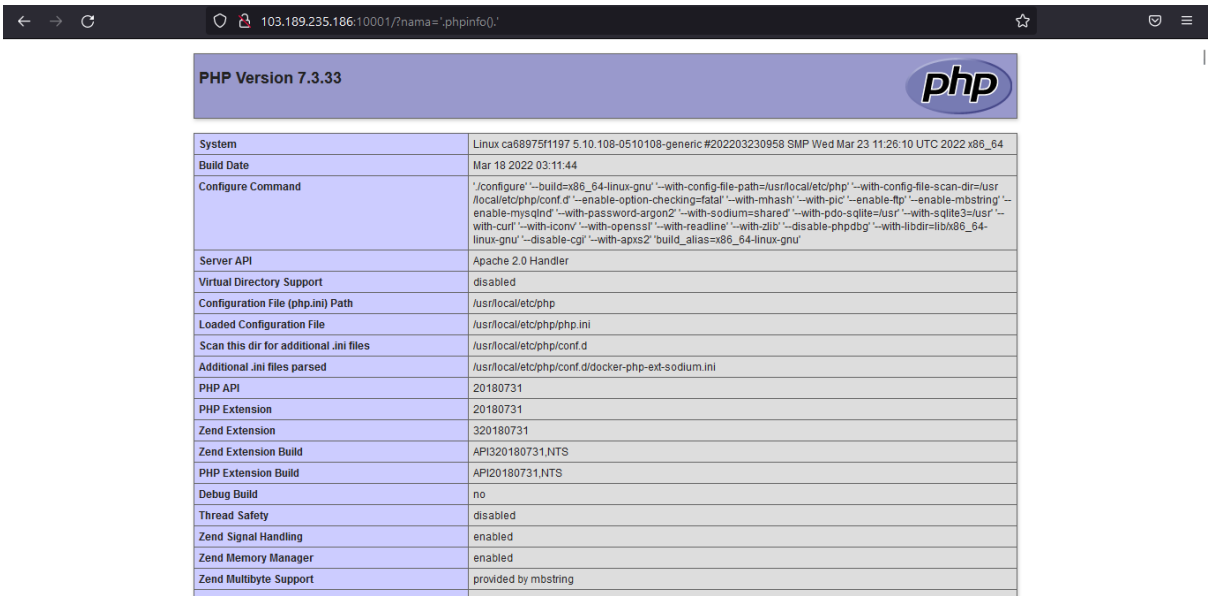
Executive Summary

Diberikan soal berupa web dengan kerentanan fungsi eval php

Technical Report

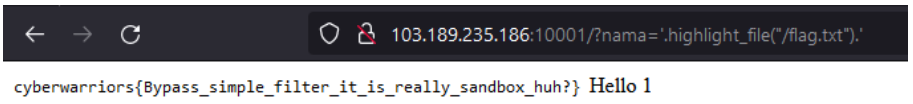
1. Kami membuka link yang diberikan dengan tampilan berikut :

2. Pada website terlihat bahwa web menerima method get dengan variabel nama, kemudian langsung saja kami masukkan payloadnya sebagai berikut :



System	Linux ca68975f1197 5.10.108-0510108-generic #202203230958 SMP Wed Mar 23 11:26:10 UTC 2022 x86_64
Build Date	Mar 18 2022 03:11:44
Configure Command	'./configure' '--build=x86_64-linux-gnu' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--enable-option-checking=fatal' '--with-mhash' '--with-pic' '--enable-ftp' '--enable-mbstring' '--enable-mysqlnd' '--with-password-argon2' '--with-sodium=shared' '--with-pdo-sqlite=/usr' '--with-sqlite3=/usr' '--with-curl' '--with-iconv' '--with-openssl' '--with-readline' '--with-zlib' '--disable-phpdbg' '--with-libdir=lib/x86_64-linux-gnu' '--disable-cgi' '--with-apxs2' 'build_alias=x86_64-linux-gnu'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc/php
Loaded Configuration File	/usr/local/etc/php/php.ini
Scan this dir for additional .ini files	/usr/local/etc/php/conf.d
Additional .ini files parsed	/usr/local/etc/php/conf.d/docker-php-ext-sodium.ini
PHP API	20180731
PHP Extension	20180731
Zend Extension	320180731
Zend Extension Build	API320180731,NTS
PHP Extension Build	API20180731,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring

3. Berdasarkan php info, semua perintah exec di-*disable,* sehingga untuk membypass nya kami menggunakan command script php. Langsung saja kami menggunakan function highlight_file untuk membaca flag pada server :



Conclusion

Vulnerability pada fungsi eval php yang bisa menyebabkan Remote Code Execution (RCE).
Flag = cyberwarriors{Bypass_simple_filter_it_is_really_sandbox_huh?}

REVERSE ENGINEERING

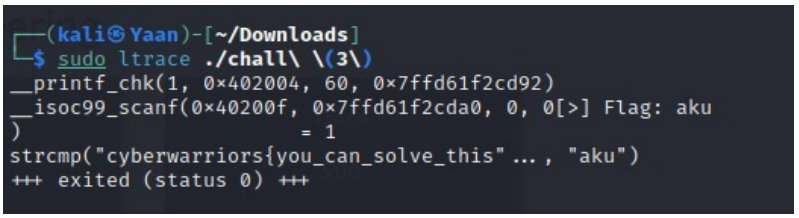
[Trace]

Executive Summary

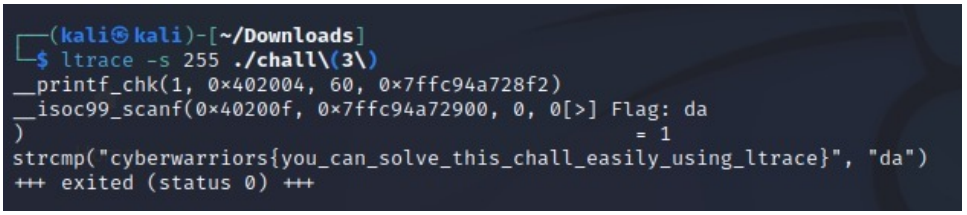
Diberikan sebuah program berupa elf file dan diminta untuk melihat alur dari program tersebut.

Technical Report

1. Kami mengunduh file tersebut dan kami menggunakan tool ltrace untuk melihat alur program tersebut, ternyata didapat potongan flag nya :



2. Karena flag nya tidak lengkap, kami mencoba untuk melihat kembali ke help command ltrace. Selanjutnya, kami menggunakan parameter -s untuk mengatur batasan size string yang ingin ditampilkan, yaitu sebanyak 255.



Conclusion

Mengetahui alur dari sebuah program dan melacak string program.
Flag = cyberwarriors{you_can_solve_this_chall_easily_using_ltrace}