

# WU CYBER STRIKE ID CTF 2024

By : Sironcy (Rafi)

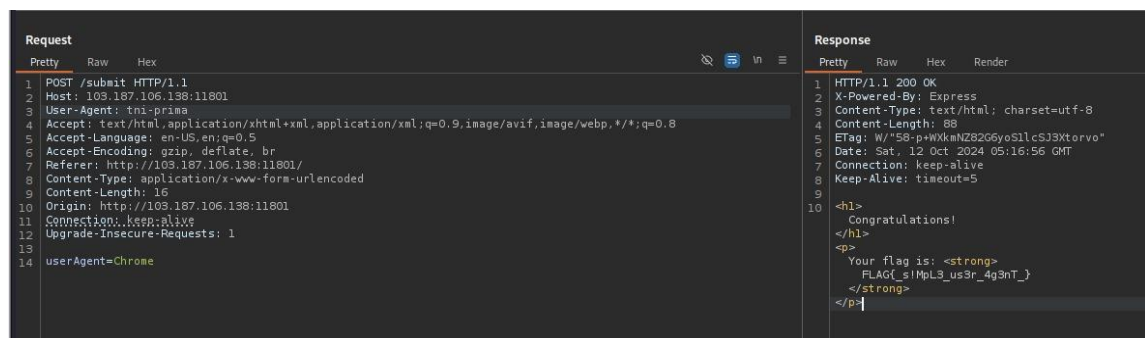
## 1. Hacker wanna be

Diberikan sebuah website dengan sebuah input berupa user agent

Enter Your User Agent:

Setelah membaca hint **Hacker wanna be "tni-prima"** saya berpikir mungkin ada kaitannya user agent dengan tni-prima, lalu saya memodifikasi request saya menggunakan Burpsuite untuk mengganti user agent menjadi tni-prima dan berhasil mendapatkan Flagnya.



FLAG : FLAG{\_s!MpL3\_us3r\_4g3nT\_}

## 2. Log yang Tersembunyi

Diberikan sebuah file zip bernama forensic\_challenge.zip, ketika kita mengekstraknya, kita hanya memperoleh sebuah text file yang isinya tidak berguna.

```
(sironcy@Cause)-[~/Downloads]
$ cat important.txt
Ini adalah file penting.
```

Kemudian saya mencoba untuk menggunakan command cat pada file zipnya untuk mengecek saja, dan ternyata mengandung Flagnya.

```
(sironcy@Cause)-[~/Downloads]
$ cat forensic_challenge.zip
User login attempt failed: 2024-10-03 12:45:23
User login successful: 2024-10-03 12:46:10
File downloaded: suspicious_file.zip
User logged out: 2024-10-03 12:50:45
CTF{askdjaskjd123280912}
PK
important.txtUT ***f***fux
                                **Ini adalah file penting.
PK
***important.txtUT***fux
                                **PKS`
```

FLAG : CTF{askdjaskjd123280912}

### 3. Eksplorasi Gambar Terenkripsi

Kita diberi sebuah file png, dengan nama ctf.png. Ketika saya cek image tersebut saya tidak menemukan informasi apapun, lalu saya berpikiran untuk mengecek metadata file tersebut menggunakan exiftool dan exiv2 tetapi tidak ada juga, lalu berlanjut ke binwalk, hexdump, xxd, saya juga tidak menemukan apapun. Kemudian saya mencoba tool **zsteg** dan akhirnya berhasil menemukan hidden Flagnya.

```
(sironcy@Cause)-[~/Downloads]
$ zsteg ctf.png
b1,r,lsb,xy      .. text: "CTF{hidden_flag}"
b4,bgr,msb,xy   .. file: MPEG ADTS, layer I, v2, Monaural
```

FLAG : CTF{hidden\_flag}

### 4. Eksplorasi File Terenkripsi

Kita diberikan sebuah file zip dengan nama secret\_data.zip, setelah diekstrak kita mendapatkan sebuah file yang mengandung file berisi teks yang diencode menggunakan base64. Kita coba decode dan mendapatkan teks enkripsi yang belum diketahui menggunakan metode apa.

```
(sironcy@Cause)-[~/Downloads/cry1]
$ cat secret_data.txt
aX5sUV5CQ1l1Q1l1XkJPdVlPSVhPXnVMRktNVw==

(sironcy@Cause)-[~/Downloads/cry1]
$ echo "aX5sUV5CQ1l1Q1l1XkJPdVlPSVhPXnVMRktNVw==" | base64 -d
i~lQ^BCYuCYu^B0uY0IX0^uLFKMW
```

Saya mencoba semua metode dekripsi yang ada pada situs cyberchef untuk menemukan Flagnya, dan akhirnya berhasil ditemukan pada enkripsi metode XOR dengan key = 2a.

Recipe

XOR Brute Force

Key length: 1, Sample length: 100, Sample offset: 0, Scheme: Standard

☐ Null preserving, ☒ Print key, ☐ Output as hex

Crib (known plaintext string)

Input: i~lQ^BCYuCYu^BouYOIX0^uLFKMW

Output:

Key = 20: I^Lq~bcyUcyU~boUyoixo~Ulfkmw  
Key = 21: H\_Mp~cbxTbxT~cnTxnhyn~Tmgjlv  
Key = 22: K\Ns|`a{wa{w|`mw{mkzm|wndiou  
Key = 23: J|Or}a`zV`zV}aLvzlj{l}Voeht  
Key = 24: MZHuzfg}Qg}QzfkQ}km|kzQhbois  
Key = 25: L[It{gf|Pf|P{gjP|j}j{Picnhr  
Key = 26: OXJwxde~Se~SxdiS~io~ixSj`mkq  
Key = 27: NYKvyed~Rd~RyehR~hn~hyRkaljp  
Key = 28: AVDyvjkk]kq]vjg]qgapgv]dnce~  
Key = 29: @wExwkjp\jp\wkf\pf`qfwleobd~  
Key = 2a: CTF{this\_is\_the\_secret\_flag}  
Key = 2b: BUGzuihr^hr^uid^rdbdsdu^gm`f|  
Key = 2c: ER@}rnouYouYrncYucetcrY`jga{  
Key = 2d: DSA|sontXntXsobXtbdubsXakf`z

STEP: BAKE! Auto Bake

FLAG : CTF{this\_is\_the\_secret\_flag}

## 5. Tersembunyi

Diberikan sebuah zip file dengan nama forensic\_challenge2.zip, setelah diekstrak kita mendapat dua file, terdapat string menarik pada file secret\_message.txt yang tampaknya seperti encoding base64, lalu saya coba mendecodenya dan mendapatkan Flagnya.

```
(sironcy@Cause)~/Downloads/fc2
$ ls
forensic_challenge2.zip  random_info.txt  secret_message.txt

(sironcy@Cause)~/Downloads/fc2
$ cat random_info.txt
File ini berisi pesan rahasia.

(sironcy@Cause)~/Downloads/fc2
$ cat secret_message.txt
Pesan penting: 101101010110001
Flag terenkripsi: Q1RGezEyM1NyeXB0b30=

(sironcy@Cause)~/Downloads/fc2
$ echo "Q1RGezEyM1NyeXB0b30=" | base64 -d
CTF{123Srypto}
```

FLAG : CTF{123Srypto}

## 6. Mystery in the Files

Diberikan file zip bernama barangbukti.zip ketika diekstrak kita mendapatkan sebuah directory dengan 50 file, saya coba untuk menampilkan semua file dengan perintah **ls -lah** yang akan menampilkan semua file termasuk hidden files dengan format list, serta ukurannya. Setelah dicermati terdapat satu file dengan ukuran yang berbeda dari file lain, yaitu file **file\_025.txt**.

```
(sironcy@Cause)-[~/Downloads/bb/forensic_files]
$ ls -lah
total 208K
drwxrwxr-x 2 sironcy sironcy 4.0K Oct 10 23:21 .
drwxrwxr-x 3 sironcy sironcy 4.0K Oct 12 09:59 ..
-rw-rw-r-- 1 sironcy sironcy 1.0K Oct 10 23:21 file_000.txt
-rw-rw-r-- 1 sironcy sironcy 1.0K Oct 10 23:21 file_001.txt
-rw-rw-r-- 1 sironcy sironcy 1.0K Oct 10 23:21 file_002.txt
-rw-rw-r-- 1 sironcy sironcy 1.0K Oct 10 23:21 file_003.txt
-rw-rw-r-- 1 sironcy sironcy 1.0K Oct 10 23:21 file_004.txt
-rw-rw-r-- 1 sironcy sironcy 1.0K Oct 10 23:21 file_005.txt
-rw-rw-r-- 1 sironcy sironcy 1.0K Oct 10 23:21 file_006.txt
-rw-rw-r-- 1 sironcy sironcy 1.0K Oct 10 23:21 file_007.txt
-rw-rw-r-- 1 sironcy sironcy 1.0K Oct 10 23:21 file_008.txt
-rw-rw-r-- 1 sironcy sironcy 1.0K Oct 10 23:21 file_009.txt
-rw-rw-r-- 1 sironcy sironcy 1.0K Oct 10 23:21 file_010.txt
-rw-rw-r-- 1 sironcy sironcy 1.0K Oct 10 23:21 file_011.txt
-rw-rw-r-- 1 sironcy sironcy 1.0K Oct 10 23:21 file_012.txt
-rw-rw-r-- 1 sironcy sironcy 1.0K Oct 10 23:21 file_013.txt
-rw-rw-r-- 1 sironcy sironcy 1.0K Oct 10 23:21 file_014.txt
-rw-rw-r-- 1 sironcy sironcy 1.0K Oct 10 23:21 file_015.txt
-rw-rw-r-- 1 sironcy sironcy 1.0K Oct 10 23:21 file_016.txt
-rw-rw-r-- 1 sironcy sironcy 1.0K Oct 10 23:21 file_017.txt
-rw-rw-r-- 1 sironcy sironcy 1.0K Oct 10 23:21 file_018.txt
-rw-rw-r-- 1 sironcy sironcy 1.0K Oct 10 23:21 file_019.txt
-rw-rw-r-- 1 sironcy sironcy 1.0K Oct 10 23:21 file_020.txt
-rw-rw-r-- 1 sironcy sironcy 1.0K Oct 10 23:21 file_021.txt
-rw-rw-r-- 1 sironcy sironcy 1.0K Oct 10 23:21 file_022.txt
-rw-rw-r-- 1 sironcy sironcy 1.0K Oct 10 23:21 file_023.txt
-rw-rw-r-- 1 sironcy sironcy 1.0K Oct 10 23:21 file_024.txt
-rw-rw-r-- 1 sironcy sironcy 1.1K Oct 10 23:21 file_025.txt
-rw-rw-r-- 1 sironcy sironcy 1.0K Oct 10 23:21 file_026.txt
-rw-rw-r-- 1 sironcy sironcy 1.0K Oct 10 23:21 file_027.txt
-rw-rw-r-- 1 sironcy sironcy 1.0K Oct 10 23:21 file_028.txt
-rw-rw-r-- 1 sironcy sironcy 1.0K Oct 10 23:21 file_029.txt
-rw-rw-r-- 1 sironcy sironcy 1.0K Oct 10 23:21 file_030.txt
-rw-rw-r-- 1 sironcy sironcy 1.0K Oct 10 23:21 file_031.txt
-rw-rw-r-- 1 sironcy sironcy 1.0K Oct 10 23:21 file_032.txt
-rw-rw-r-- 1 sironcy sironcy 1.0K Oct 10 23:21 file_033.txt
-rw-rw-r-- 1 sironcy sironcy 1.0K Oct 10 23:21 file_034.txt
-rw-rw-r-- 1 sironcy sironcy 1.0K Oct 10 23:21 file_035.txt
-rw-rw-r-- 1 sironcy sironcy 1.0K Oct 10 23:21 file_036.txt
-rw-rw-r-- 1 sironcy sironcy 1.0K Oct 10 23:21 file_037.txt
-rw-rw-r-- 1 sironcy sironcy 1.0K Oct 10 23:21 file_038.txt
-rw-rw-r-- 1 sironcy sironcy 1.0K Oct 10 23:21 file_039.txt
-rw-rw-r-- 1 sironcy sironcy 1.0K Oct 10 23:21 file_040.txt
-rw-rw-r-- 1 sironcy sironcy 1.0K Oct 10 23:21 file_041.txt
-rw-rw-r-- 1 sironcy sironcy 1.0K Oct 10 23:21 file_042.txt
```

Setelah dilihat isi file tersebut mengandung Flag yang kita cari.

```
0uEojZZbijzAUghI5RmPLS4bczBnICrgc4VAMV
l2vF3bNd80FY01br8RgIf7osB8Gj2YbkaikvDXU
QQdLIOctwBFLAG{Forensic_Expert_123}
```

FLAG : FLAG{Forensic\_Expert\_123}

## 7. Pengacak Kode Python

Diberikan sebuah program python yang berfungsi mendecode string dari base64 lalu mendekompresinya dari zlib, ternyata setelah dijalankan program tidak berfungsi.

```
GNU nano 8.0 mystery_key_obf.py
import zlib, base64
exec(zlib.decompress(base64.b64decode('eJwtjEEKgzAQRfc5xTSrCD1BIBsLgpTu3A9The0QnYrRSim9eyN09+G/9zruoXaR34U3ZZgX0dVQEJ231cAe7MIvXhIj6yD
# Created by pyminifier (https://github.com/liftoff/pyminifier)
```

Dengan bantuan internet saya membuat program yang serupa, ketika dijalankan berfungsi dengan baik dan mereveal Flagnya.

```
(sironcy@Cause)-[~/Downloads]
$ cat obs.py
import zlib
import base64

compressed_data = 'eJwtjEEKgzAQRfc5xTSrCD1BIBsLgpTu3A9The0QnYrRSim9eyN09+G/9zruoXaR34U3ZZgX0dVQEJ231cAe7MIvXhIj6yD8o'

def flag(data):
    decoded_data = base64.b64decode(compressed_data)
    decompressed_data = zlib.decompress(decoded_data)
    print(decompressed_data.decode('utf-8'))

if __name__ == '__main__':
    flag(compressed_data)
```

```
(sironcy@Cause)-[~/Downloads]
$ python3 obs.py
def I(key):
B=print
a=input
w="reverse_engineering_rocks"
if key==w:
    B("Flag: CTF{flag_anda_disini}")
else:
    B("Kunci salah, coba lagi!")
if __name__=="__main__":
    T=a("Masukkan kunci: ")
    I(T)
```

FLAG : CTF{flag\_anda\_disini}