1. Free Flag

WRECKIT50{just_ch3cking_f0r_y0ur_sani7y}

2. hum45

Kategory : CRYPTOGRAPHY

```
can you solve this with no clue???

RH95N9U34E+91C9Y34CY8O095IAYX9T6ASNAK*9QY9
S9BT90B9SNABT9.HAK*9YCBE+9*34HY8UY9W34EY8DB8MA85N9$Y9IZAW34MB8CB9W34B
Y8NB88B8 :7W0

format: WRECKIT50{???????}
```

Terdapat teks yang ter enkripsi, gunakan cipher identifier dan ketemu bahwa teks tersebut menggunakan enkripsi base45, lakukan dekripsi dan hasilnya adalah

```
JIKA INGIN MENGIRIM PESAN MELALUI SALURAN YANG RESMI KEPADA KAMPUS KAMI,
KEMANA???
```

Masuk ke website resmi Politeknik Siber dan Sandi Negara yaitu “https://poltekssn.ac.id/”, scroll hingga menemukan email resmi dari Politeknik Siber dan Sandi Negara, masukkan email ke dalam format yang diberikan.
Flag : “WRECKIT50{humas@poltekssn.ac.id}”

3. Babysnake

Kategori : REVERSE ENGINEERING

```
silahkan puh, babyrevnya puh

author: k.eii

chall.pyc
```

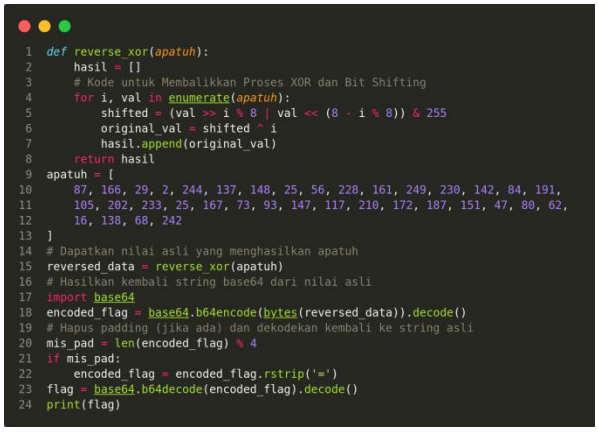
Terdapat sebuah file yang merupakan compiled Python bytecode file, gunakan tools pycdc untuk membaca file tersebut. Hasil nya :

```
# Source Generated with Decompyle++
# File: babysnake.pyc (Python 3.8)

from base64 import b64encode as b64e, b64decode as b64d

def xor(data):
    hasil = []
    for i, val in enumerate(data):
        shifted = (val ^ i) << i % 8 | (val ^ i) >> 8 - i % 8
        hasil.append(shifted & 255)
    return hasil

usr_input = input('>>> ')
usr_input = usr_input.encode()
enc = b64e(usr_input).decode()
mis_pad = len(enc) % 4
if mis_pad:
    enc += '=' * (4 - mis_pad)
dec = b64d(enc)
```

```
apani = xor(dec)
apatuh = [
    87,
    166,
    29,
    2,
    244,
    137,
    148,
    25,
    56,
    228,
    161,
    249,
    230,
    142,
    84,
    191,
    105,
    202,
    233,
    25,
    167,
    73,
    93,
    147,
    117,
    210,
    172,
    187,
    151,
    47,
    80,
    62,
    16,
    138,
    68,
    242]
if apani == apatuh:
    print('Nais!')
else:
    print('Coba lagi!')
```

Kode ini meminta pengguna untuk memasukkan sebuah input, yang kemudian dienkode dalam base64, didekode kembali, dan diproses dengan operasi XOR dan bit shifting. Hasil dari operasi ini kemudian dibandingkan dengan daftar nilai yang telah ditentukan. Jika hasilnya sama, pengguna dinyatakan berhasil ("Nais!"). Jika tidak, pengguna diminta untuk mencoba lagi ("Coba lagi!").

Lakukan reverse engineering untuk mendapatkan flag dengan program :



```python
def reverse_xor(apatuh):
    hasil = []
    # Kode untuk Membalikkan Proses XOR dan Bit Shifting
    for i, val in enumerate(apatuh):
        shifted = (val >> i % 8 | val << (8 - i % 8)) & 255
        original_val = shifted ^ i
        hasil.append(original_val)
    return hasil
apatuh = [
    87, 166, 29, 2, 244, 137, 148, 25, 56, 228, 161, 249, 230, 142, 84, 191,
    105, 202, 233, 25, 167, 73, 93, 147, 117, 210, 172, 187, 151, 47, 80, 62,
    16, 138, 68, 242
]
# Dapatkan nilai asli yang menghasilkan apatuh
reversed_data = reverse_xor(apatuh)
# Hasilkan kembali string base64 dari nilai asli
import base64
encoded_flag = base64.b64encode(bytes(reversed_data)).decode()
# Hapus padding (jika ada) dan dekodekan kembali ke string asli
mis_pad = len(encoded_flag) % 4
if mis_pad:
    encoded_flag = encoded_flag.rstrip('=')
flag = base64.b64decode(encoded_flag).decode()
print(flag)
```

Jalankan program dan flag didapatkan. Flag : “WRECKIT50{b4by_pyth0n_c0mp1led_c0d3}”

4. Lets Go

Kategori : REVERSE ENGINEERING

lets goooo author: k.eii *dist.rar*

Terdapat file rar yang di dalamnya terdapat file flagenc yang terenkripsi dan terdapat program bernama wrek1t, yang kemungkinan besar merupakan program untuk mendekripsi flag nya, jalankan program dan lakukan perintah programnya, flag kemudian di dekripsi. Flag : “WRECKIT50{g0_wrek_1t_ye}”

5. MatPem

Kategori : CRYPTOGRAPHY

SPLXV *chall.py*

Terdapat sebuah program Python yang berisi :

```
import random

FLAG = b"WRECKIT50{????????}"
fint = int(FLAG.hex(),16)
key = [random.getrandbits(4) for _ in range(3)]

pk = [
  [11,14,17,20], [12,15,18,21], [13,16,19,22]
]

result = [sum([key[j]*pk[i][j] for j in range(3)]) for i in range(3)]

var = ['a','b','c','d']
for i in range(len(pk)):
    equation = ''
    for j in range(len(pk[i])):
        equation += str(pk[i][j])+"*"+var[j]+" + "
    equation = equation[:-3] + " = " + str(result[i])
```

```
    print(equation)

key = sum(key)

enc = key*fint
print("Encryted flag:", enc)


"""
Output:
11*a + 14*b + 17*c + 20*d = 263
12*a + 15*b + 18*c + 21*d = 282
13*a + 16*b + 19*c + 22*d = 301
Encryted flag:
232248373780702558559732705634320310324639111824357224567527709756665492
238132012558072443413580231257415
"""
```

Kode program Python ini mengenkripsi sebuah flag menggunakan transformasi dan perkalian linear sederhana.

Program di atas memiliki output berupa 3 persamaan linear yaitu
11*a + 14*b + 17*c + 20*d = 263
12*a + 15*b + 18*c + 21*d = 282
13*a + 16*b + 19*c + 22*d = 301

Dalam konteks ini, a, b, c, dan d biasanya akan merepresentasikan nilai dari key[0], key[1], key[2], dan key[3]. Namun, dalam kode, key hanya memiliki tiga elemen (a, b, dan c), sehingga bisa dianggap bahwa d adalah 0.

-Eliminasi Variabel
Sederhanakan sistem persamaan ini. Diasumsikan bahwa d = 0, sehingga persamaan menjadi:
11a + 14b + 17c = 263
12a + 15b + 18c = 282
13a + 16b + 19c = 301

-Kurangi Persamaan untuk Menghilangkan Variabel
Mengurangi Persamaan 1 dari Persamaan 2:
(12a + 15b + 18c) − (11a + 14b + 17c) = 282 − 263
a + b + c = 19 (Persamaan 4)

Mengurangi Persamaan 2 dari Persamaan 3:
(13a + 16b + 19c) − (12a + 15b + 18c) = 301 − 282
a + b + c = 19 (Persamaan 5)

Ditemukan bahwa Persamaan 4 dan 5 adalah identik. Ini berarti sistem persamaan ini memiliki solusi yang tak terbatas (tidak unik) karena ada ketergantungan linier antara persamaan. Sehingga bisa memilih salah satu variabel secara bebas dan kemudian menghitung dua variabel lainnya.

Misalnya, kita asumsikan bahwa c = 0, Maka:
a + b + 0 = 19
a + b = 19

Sekarang, kita bisa memilih nilai untuk a dan b yang memenuhi persamaan ini. Misalnya:
 a = 10 dan b = 9

Dengan demikian, telah ditemukan nilai untuk a, b, dan c.

Kemudian gunakan nilai ini untuk mendekripsi flag:

```python
key_sum = 10 + 9 + 0
print("Sum of key elements (key):", key_sum)
enc = 232248373780702558559732705634320310324639111824357224567527709756665492238132012558072443413580231257415
fint = enc // key_sum
flag = bytes.fromhex(hex(fint)[2:]).decode('utf-8')
print("Decrypted Flag:", flag)
```

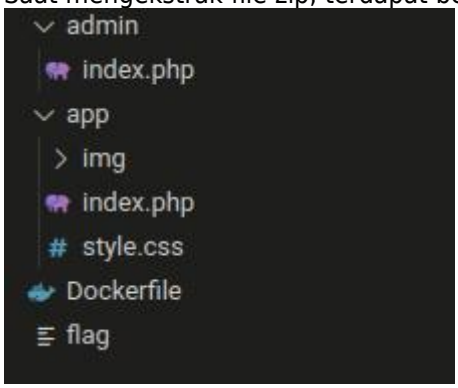
Jalankan program dan flag ditemukan. Flag :
“WRECKIT50{5ist3m_PrSm44n_l1n13r_4_vaRiabEL}”

6. Cheemsweb

Kategori : WEB EXPLOITATION

cheems belajar membuat sebuah web, keamanannya ntar aja, gampang itu katanya http://137.184.250.54:10001/ alt http://13.212.238.29:10001/ author: k.eii *dist-cheemsweb.zip*

Saat mengekstrak file zip, terdapat beberapa folder dan file.



Di dalam folder app terdapat index.php yang berisi

```php
<?php
$images = [
    '1.png',
    '2.png',
    '3.png',
    '4.png',
    '5.png'
];

if (isset($_GET['url'])) {
    $url = $_GET['url'];

    $curl = curl_init();

    curl_setopt($curl, CURLOPT_URL, $url);
    curl_setopt($curl, CURLOPT_RETURNTRANSFER, true);
    curl_setopt($curl, CURLOPT_FOLLOWLOCATION, true);
    curl_setopt($curl, CURLOPT_CONNECTTIMEOUT, 10);
    curl_setopt($curl, CURLOPT_TIMEOUT, 30);

    $content = curl_exec($curl);

    if ($content === false) {
        echo "Error fetching content: " . curl_error($curl);
    } else {
        echo $content;
    }

    curl_close($curl);

    exit;
}
?>

<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>cheems</title>
    <style>
        img {
            margin: 10px;
            width: 200px;
            height: 200px;
            object-fit: cover;
            cursor: pointer;
        }
    </style>
</head>
<body>
    <h1>cheems hold the flag</h1>
    <div>
        <?php foreach ($images as $image): ?>
            <a href="?image=<?php echo urlencode($image); ?>">
                <img src="img/<?php echo htmlspecialchars($image); ?>" alt="flag">
            </a>
        <?php endforeach; ?>
    </div>
</body>
</html>
```

Di dalam folder admin terdapat index.php yang berisi

```php
<?php
error_reporting(E_ALL);
ini_set('display_errors', 1);

if (isset($_GET['url'])) {
    $url = $_GET['url'];
    $content = file_get_contents($url);
    echo $content;
    exit;
}

if (isset($_GET['search'])) {
    $search = $_GET['search'];
    eval($search);
    exit;
}
?>

<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Admin Page</title>
</head>
<body>
    <h1>Admin Page</h1>
    <form method="GET" action="">
        <input type="text" name="search" placeholder="Search Image">
        <button type="submit">Search</button>
    </form>
</body>
</html>

```

Dan file flag yang berisi “WRECKIT50{redacted}”

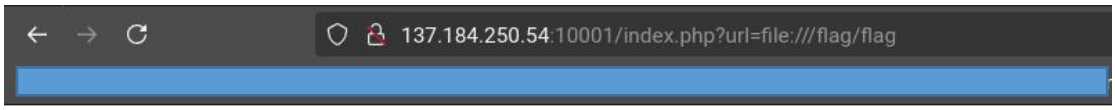
Website ini memiliki beberapa kerentanan keamanan seperti Local File Inclusion (LFI) pada bagian ‘admin/index.php’ :

```
if (isset($_GET['url'])) {
    $url = $_GET['url'];
```

```
$curl = curl_init();

curl_setopt($curl, CURLOPT_URL, $url);
curl_setopt($curl, CURLOPT_RETURNTRANSFER, true);
curl_setopt($curl, CURLOPT_FOLLOWLOCATION, true);
curl_setopt($curl, CURLOPT_CONNECTTIMEOUT, 10);
curl_setopt($curl, CURLOPT_TIMEOUT, 30);

$content = curl_exec($curl);
```

‘curl_setopt($curl, CURLOPT_URL, $url);’ Di sini, URL yang diset oleh pengguna ($_GET['url']) digunakan langsung tanpa validasi atau sanitasi. Ini memungkinkan pengguna untuk mengarahkan curl ke URL mana pun, termasuk file:// yang bisa digunakan untuk mengakses file lokal di server.

Untuk mendapatkan flag yang berupa file, kita bisa memanfaatkan kerentanan tersebut menggunakan parameter url untuk mengakses file flag,
‘http://137.184.250.54:10001//index.php?url=file:///flag/flag’



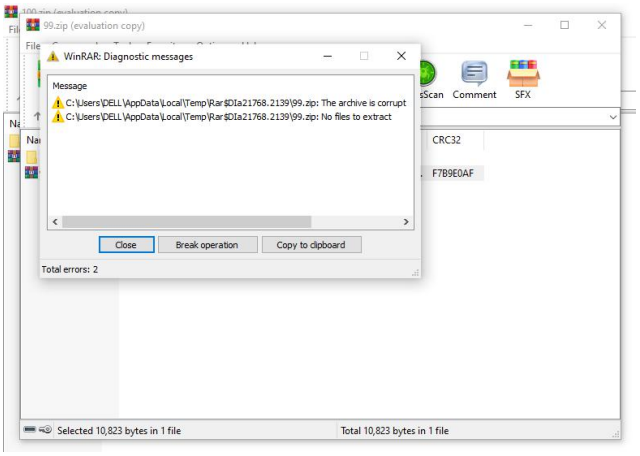
WRECKIT50{server_side_rem0te_f0rgeryyyy}

Flag : ‘WRECKIT50{server_side_rem0te_f0rgeryyyy}’

7. BROKEN

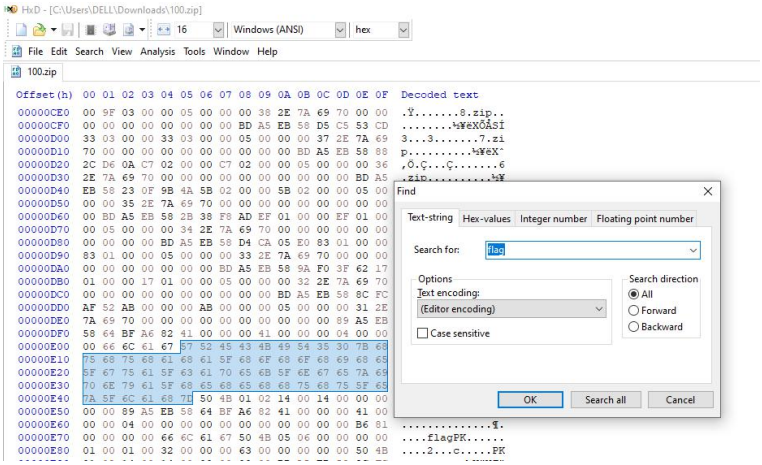
```
rusak rusak rusakkkkk
author: k.eii
 100.zip
```

Mari kita lihat isi file 100.zip

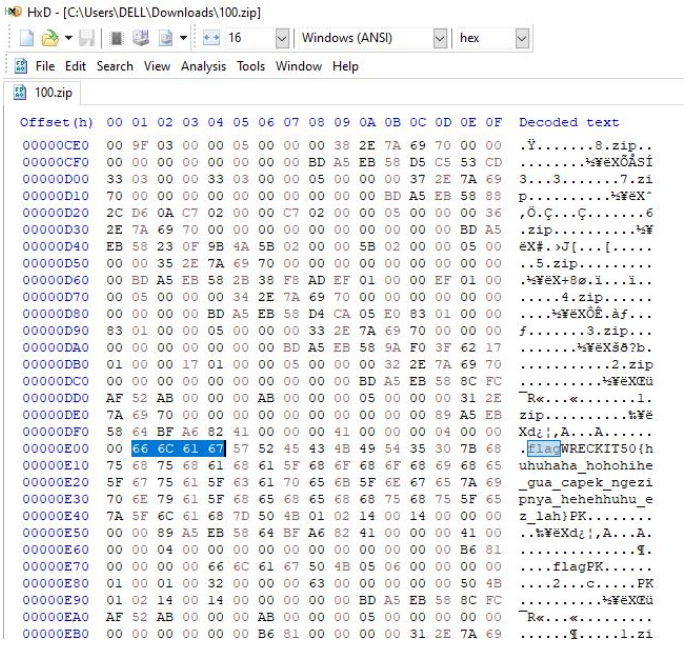


Oh noo, the file is broken`~`

Kalau gitu coba kita liat file nya pake HxD



Voila ternyata ketahuan Cuma pake HxD



Flag:WRECKIT50{huhuhaha_hohohihe_gua_capek_ngezipnya_hehehhuhu_ez_lah}