

Ancient Validator

Santarfhin

Reverse Engineering

Write-up Penyelesaian

1. Untuk Tools, saya menggunakan ghidra, import file seperti biasa dan lihat decompile MAIN. Ada loop

```
for (local_c = 0; local_c < local_14; local_c = local_c + 1) {  
    local_108[local_c] = local_98[local_c] ^ kunciXOR;  
}  
local_108[local_14] = 0;  
printf("Masukkan password: ");  
__isoc99_scanf(&DAT_00402018, local_78);
```

2. ambil kunci XOR (local_d) saya rename var nya biar enak dilihat.

```
local_98[0x16] = 0x26;  
local_98[0x17] = 0x22;  
kunciXOR = 0x5f;
```

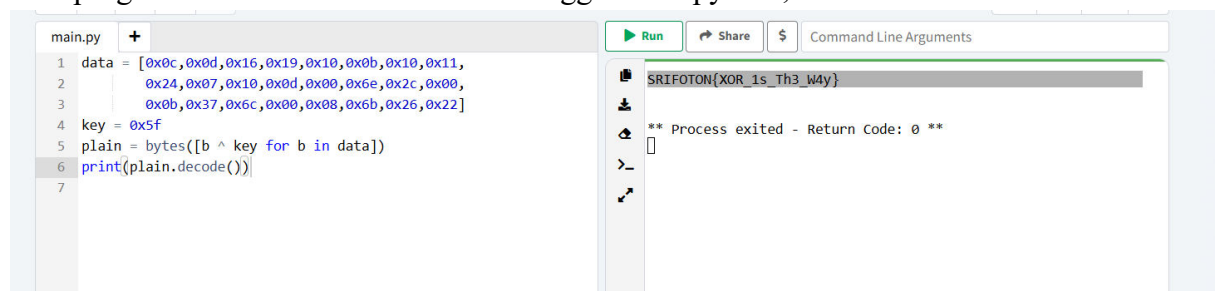
3. local_14 = 0x18(panjang = 24). Setelah di-XOR, dibuat string null-terminated dan dibandingkan dengan input via strcmp

4. solusi = restore local_108 dengan operasi XOR pada local_98 menggunakan kunci 0x5f untuk 24 byte

5. Ambil array local_98

```
0x0c,0x0d,0x16,0x19,0x10,0x0b,0x10,0x11,  
0x24,0x07,0x10,0x0d,0x00,0x0e,0x2c,0x00,  
0x0b,0x37,0x6c,0x00,0x08,0x6b,0x26,0x22
```

6. buat program sederhana untuk decode menggunakan python, melalui kunci xor tersebut



```
main.py +  
1 data = [0x0c,0x0d,0x16,0x19,0x10,0x0b,0x10,0x11,  
2         0x24,0x07,0x10,0x0d,0x00,0x0e,0x2c,0x00,  
3         0x0b,0x37,0x6c,0x00,0x08,0x6b,0x26,0x22]  
4 key = 0x5f  
5 plain = bytes([b ^ key for b in data])  
6 print(plain.decode())  
7
```

Run Share Command Line Arguments

SRIFOTON{XOR_1s_Th3_W4y}

** Process exited - Return Code: 0 **

SRIFOTON{XOR_1s_Th3_W4y}

Friend Project

Santarfhin

Cryptography

Write-up Penyelesaian

1. Diberikan sebuah attachment File GOT_CHA.rar dan friend_project.html
2. Setelah dilakukan Analisa terhadap file friend_project.html, ditemukan komen yang sus:

```
<!doctype html>
<html lang="id">
  <head>
    <meta charset="utf-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1" />
    <title>why number -3</title>

    <script src="https://cdn.tailwindcss.com"></script>
  </head>
  <body class="min-h-screen bg-gray-700 shadow-md rounded-lg p-6 text-center flex items-center justify-center leading-normal tracking-normal"> <!--mxvwjrwwkhsdvv-->
    <!-- not here -->
    <span class="font-bold leading-normal text-black tracking-tight">
      caesar might be proud
    </span>
    <!-- i think u got the pass -->
  </body>
</html>
```

“mxvwjrwwkhsdvv”

3. Decrypt menggunakan Caesar cipher melalui website <https://www.dcode.fr/caesar-cipher>

↕	↕
➔3 (↵23)	justgotthepass
➔9 (↵17)	domnainnbyjumm
➔18 (↵8)	ufderzeespaldd
➔4 (↵22)	itrsfnssgdozrr
➔21 (↵5)	rcabowbbpmxiaa
➔17 (↵9)	vnefsafftqhmea

CAESAR SHIFTED CIPHERTEXT

mxvwjrwwkhsdvv

Test all possible shifts (26-letter alphabet A-Z)

▶ DECRYPT (BRUTEFORCE)

Maka didapatkan passwordnya “justgotthepass”

4. Buka GOT_CHA.rar dengan password yang diberikan, maka akan didapatkan flagnya yaitu : SRIFOTON{1_kN0w_U_c4N}

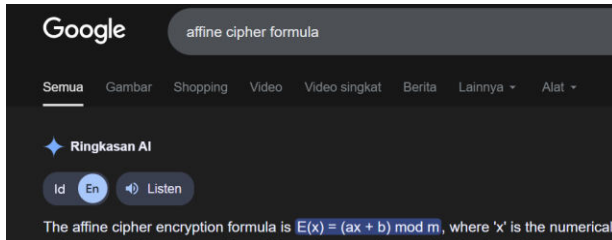
Gaming Friend

Santarfhin

Cryptography

Write-up Penyelesaian

1. plain = DIAMOND cipher= KNDFBQK
2. cek apakah ini affine cipher, cek juga formula affine



3. $D = 3$ $K = 10$ $I = 8$ $N = 13$
4. $(a*3 + b) \equiv 10 \pmod{26}$ $(a*8 + b) \equiv 13 \pmod{26}$
5. kurangi diatas menjadi, $a*5 \equiv 3 \pmod{26}$
6. modular inverse 5 mod 26 adlh 21
7. jadi $a \equiv 21*3 \equiv 63 \equiv 11 \pmod{26}$
8. $11*3 + b \equiv 10 \rightarrow 33 + b \equiv 10 \rightarrow b \equiv -23 \equiv 3$
a=11, b=3.
9. saya cek perkata ternyata benar, ini affine cipher
10. hint dari soal (affinity) 'affine cipher'
11. MPGMMSKFNJDHMSPFBIIDTHFRI adalah hasilnya, ini ternyata alternating-Caesar. shift nya 12,5. jadi per huruf shiftnya berubah ubah. contoh M shift -12, P -5, dan seterusnya. saya langsung membuat tools sederhana untuk menyelesaikan chall ini. (12, 5) diambil dari soal level 5 affinity, dan 12 noon
12. Cipher : MPGMMSKFNJDHMSPFBIIDTHFRI
Shifts : 12, 5
Plain : AKUHANYABERCANDAPDROVAFD

```
const ALPHABET = "ABCDEFGHIJKLMNOPQRSTUVWXYZ";
function isLetter(ch) {
  return ch >= "A" && ch <= "Z";
}
function shiftChar(ch, shift) {
  const pos = ALPHABET.indexOf(ch);
  const newPos = (pos + shift) % 26;
  const result = ALPHABET[newPos];
  return result;
}
function decryptAlternatingCaesar(ciphertext, shifts, startShiftPos = true) {
  const result = [];
  for (let i = 0; i < ciphertext.length; i++) {
    const ch = ciphertext[i];
    if (!isLetter(ch)) {
      result.push(ch);
      continue;
    }
    const offset = (i % 2 === 0) ? shifts[0] : shifts[1];
    const shifted = shiftChar(ch, offset);
    result.push(shifted);
  }
  return result.join("");
}
const CIPHERTEXT = "MPGMMSKFNJDHMSPFBIIDTHFRI";
const SHIFTS = [12, 5];
const PLAINTEXT = decryptAlternatingCaesar(CIPHERTEXT, SHIFTS, true);
console.log("Cipher:", CIPHERTEXT);
console.log("Shifts:", SHIFTS);
console.log("Plain:", PLAINTEXT);
```

FLAG : SRIFOTON{AKUHANYABERCANDAPDROVAFD}

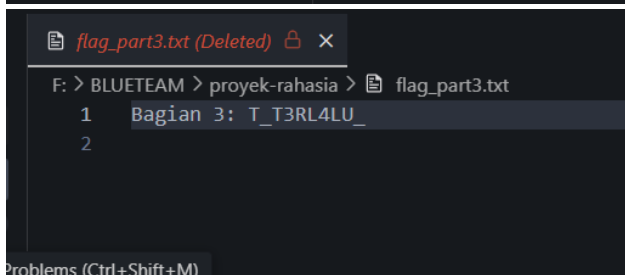
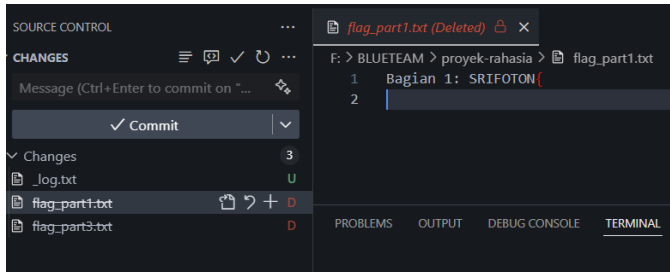
Git Timeline

Santarfhin

Forensic

Write-up Penyelesaian

1. ini adalah chall, mengumpulkan flag yang terpecah, untuk part 1, mudah saja cukup lihat pada deleted di source control, begitupun flag part 3



2. untuk flag part 2, saya craft one liner command, untuk mencari konten yang berisi 'Bagian 2' dan blob OID nya

```
Pongo@dhafin5858 MINGW64 /f/BLUETEAM/proyek-rahasia (main)
$ for oid in $(git rev-list --objects --all | awk '{print $1}'); do
  if [ "$(git cat-file -t "$oid")" = blob ] && git cat-file -p "$oid" | grep -q "Bagian 2"; then
    echo "$oid"
    git cat-file -p "$oid"
  fi
done
8717d5900240d4f5ab674822cba00e6596b138d8
Bagian 2: JEJAK_D1G174L
```

3. untuk flag part 4, menggunakan perintah git fsck --lost-found --full, untuk melihat dangling commits. dan selanjutnya tinggal menjalankan perintah cat, lalu flag bagian 4 akan ter-reveal

```
Pongo@dhafin5858 MINGW64 /f/BLUETEAM/proyek-rahasia (main)
$ git fsck --lost-found --full
Checking object directories: 100% (256/256), done.
dangling commit c62dfa866b41c152efa360deb1b43a53881ef262
dangling blob 24211b34b97efffcbbbea292988ef0edb713cc0e

Pongo@dhafin5858 MINGW64 /f/BLUETEAM/proyek-rahasia (main)
$ git cat-file -p 24211b34b97efffcbbbea292988ef0edb713cc0e
Bagian 4: SUL1T_D1H4PUS}
```

```
Pongo@dhafin5858 MINGW64 /f/BLUETEAM/proyek-rahasia (main)
$ git cat-file -p 24211b34b97efffcbbbea292988ef0edb713cc0e
Bagian 4: SUL1T_D1H4PUS}
```

SRIFOTON{JEJAK_D1G174L_T_T3RL4LU_SUL1T_D1H4PUS}

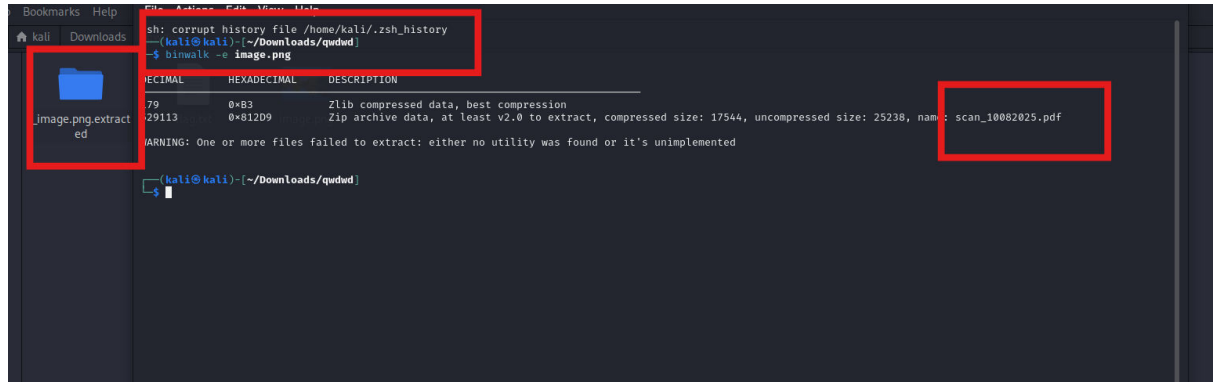
Landscape

Santarfhin

Forensic

Write-up Penyelesaian

1. diberikan sebuah file, bernama img.png. untuk identifikasi awal, saya menggunakan tools binwalk



2. terdapat informasi bahwa file mengandung informasi tersembunyi, di dalam folder tersebut, ada sebuah pdf, yang bisa kita lihat.

3. jika kita drag ke kanan, maka informasi rahasia akan muncul (flag)

SRIFOTON{EvacuateTheIslandNow}

Matrix Protocol

Santarfhin

Cryptography

Write-up Penyelesaian

1. Diberikan sebuah attachment file kode assembly, setelah dianalisa kita dapat mendapatkan flag dengan cara decrypt data dari build_list :

[20,14,7,7,5,24,16,4,60,41,125,28,41,120,51,26,24,58,127,197,
21,123,13,23,118,58,17,20,121,21,51,13,51,109,30,28,46,120,60,123]

2. Kemudian kita perlu mengambil cipher_key, yang berisi "G`PCLL_J"

```
84 LOAD_CONST          40 ('G')
86 STORE_NAME          1 (cipher_key)

88 LOAD_CONST          41 ('')
90 LOAD_NAME           1 (cipher_key)
92 BINARY_ADD
94 STORE_NAME          1 (cipher_key)

96 LOAD_NAME           1 (cipher_key)
98 LOAD_CONST          42 ('P')
100 BINARY_ADD
102 STORE_NAME          1 (cipher_key)

104 LOAD_NAME           1 (cipher_key)
106 LOAD_CONST          43 ('C')
108 BINARY_ADD
110 STORE_NAME          1 (cipher_key)

112 LOAD_NAME           1 (cipher_key)
114 LOAD_CONST          44 ('L')
116 BINARY_ADD
118 STORE_NAME          1 (cipher_key)

120 LOAD_NAME           1 (cipher_key)
122 LOAD_CONST          45 ('L')
124 BINARY_ADD
126 STORE_NAME          1 (cipher_key)

128 LOAD_NAME           1 (cipher_key)
130 LOAD_CONST          46 ('_')
132 BINARY_ADD
134 STORE_NAME          1 (cipher_key)

136 LOAD_NAME           1 (cipher_key)
138 LOAD_CONST          47 ('J')
```

3. Kemudian saya menemukan kode ini

```

Disassembly of <code object <listcomp> at 0x7f704e8a4d40, file "secret.py", line 11>:
11      0 BUILD_LIST          0
      2 LOAD_FAST              0 (.0)
    >>  4 FOR_ITER              16 (to 22)
      6 STORE_FAST            1 (char)
      8 LOAD_GLOBAL           0 (ord)
     10 LOAD_FAST              1 (char)
     12 LOAD_CONST             0 (1)
     14 BINARY_SUBTRACT
     16 LOAD_CONST             1 (7)
     18 BINARY_XOR
     20 CALL_FUNCTION          1
     22 LIST_APPEND            2
     24 JUMP_ABSOLUTE          4
    >> 26 RETURN_VALUE

```

Dia akan melakukan pengurangan 1 dan XOR dengan 7, setelah dimasukkan ke dalam ord(). Key_bytes akan diulang sampai dia sama panjang dengan encrypted_data

4. Kemudian lakukan XOR

```

17    >> 194 LOAD_CONST          54 (<code object <listcomp> at 0x7f704e8a4df0, file "secret.py", line 17>)
      196 LOAD_CONST          55 ('<listcomp>')
      198 MAKE_FUNCTION        0
      200 LOAD_NAME            5 (zip)
      202 LOAD_NAME            0 (encrypted_data)
      204 LOAD_NAME            2 (key_bytes)
      206 CALL_FUNCTION        2
      208 GET_ITER
      210 CALL_FUNCTION        1
      212 STORE_NAME          6 (xor_result)

```

5. Kemudian buat kembali string dan lakukan kembali pengurangan 1 dan XOR dengan 7, setelah dimasukkan ke dalam ord(). Untuk mendapatkan final_flag
6. Maka flagnya akan muncul, FLAG :
SRIFOTON{w3_c4nT_f1x_1T_1f_W3_nEv3R_f4c3_iT}

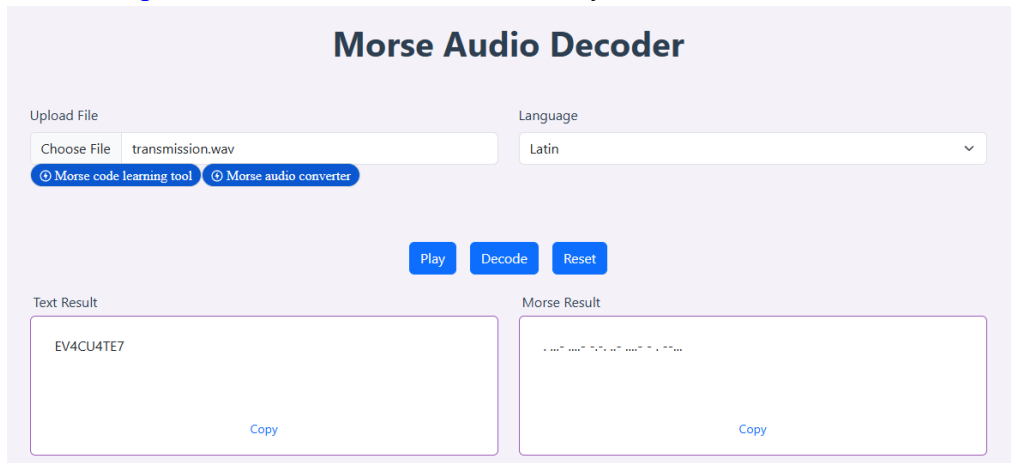
Mysterious Sound

Santarfhin

Forensics

Write-up Penyelesaian

1. Diberikan sebuah file Bernama transmission.wav, setelah didengarkan dapat diamsukan itu merupakan morse code.
2. Buka web <https://morsefm.com/> Masukkan filenya, kemudian klik decode



Maka akan muncul hasilnya “EV4CU4TE7”

3. Setelah saya buka filenya menggunakan notepad, sepertinya terdapat sesuatu disana, saya coba mengekstraknya menggunakan steghide

```
(base) └─(archet@LAPTOP-5D1DTDBP)─[~/CTF/srifoton]
└─$ steghide extract -sf transmission.wav
Enter passphrase:
wrote extracted data to "final_arsip.zip".
```

4. Isi dari final_arsip.zip ini Adalah arsip_rahasia.zip dan arsip_rahasia2.zip
Kemudian Ketika arsip pertama ingin dibuka, makai ia akan meminta password, kita masukkan teks yang kita dapat sebelumnya sebagai password “EV4CU4TE7”.
Maka kita akan mendapatkan flag pertama : SRIFOTON{13_N0v3mb3r_
Selain itu ada juga file PW2.png
5. Kita coba buka PW2.png menggunakan notepad :



Maka didapatkan password untuk arsip kedua yaitu : GARUDAANGKASA

- Buka arsip kedua dengan memasukkan password “GARUDAANGKASA”, maka kita akan mendapatkan part kedua flagnya : 2026_K14m4t_H04x}
Satukan kedua flag tersebut : SRIFOTON{13_N0v3mb3r_2026_K14m4t_H04x}

New Password

Santarfhin

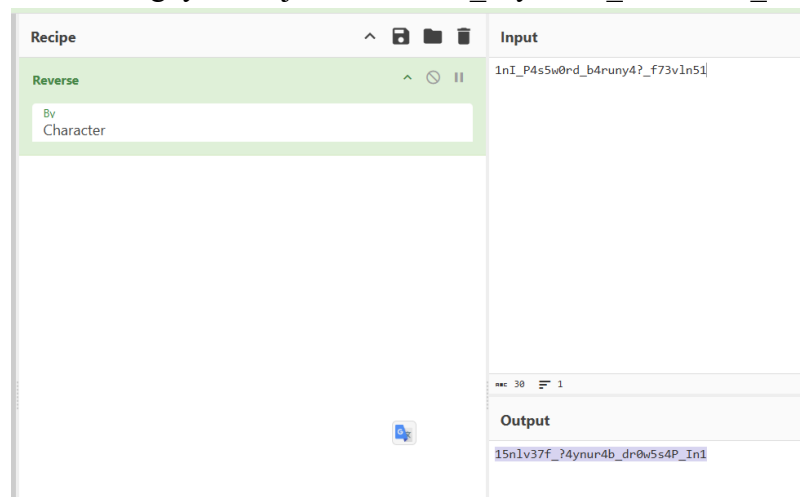
Reverse Engineering

Write-up Penyelesaian

1. Diberikan sebuah attachment python, yang Ketika dijalankan akan meminta kita untuk memasukkan sebuah password.
2. Karena di hintnya terdapat kata kalimat “You need to look at things from the other side” saya coba masukkan password “NOTOFIRS”, yang merupakan kebalikan dari “SRIFOTON”

```
what's the password? NOTOFIRS
SRIFOTON{1nI_P4s5w0rd_b4runy4?_f73v1n51}
```

3. Kemudian saya muter-muter disini cukup lama, dan akhirnya mencoba untuk membalikkan isi dari flagnya, menjadi “15nlv37f_?4ynur4b_dr0w5s4P_In1”



4. Sehingga didapatkan flagnya : SRIFOTON{15nlv37f_?4ynur4b_dr0w5s4P_In1}

Old Portal

Santarfhin

Web Exploitation

Write-up Penyelesaian

1. Diberikan sebuah attachment file Bernama “Portal.zip”, didalamnya terdapat index.html dan script.js.
2. Pada index.html kita diminta untuk memasukkan kode akses

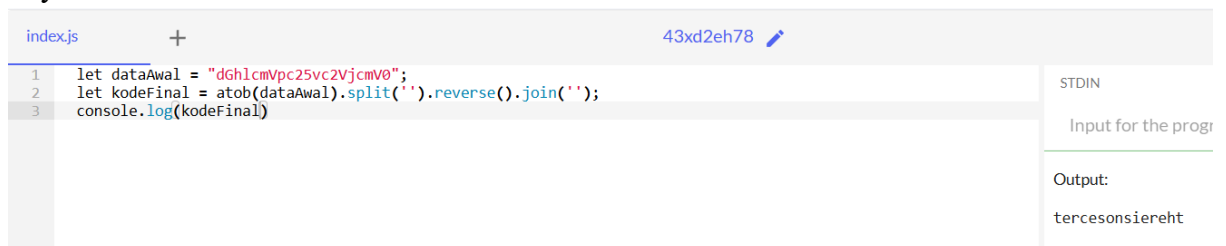
Portal

Masukkan kode akses yang benar untuk membuka kunci.

3. Dengan begitu kita coba lakukan Analisa pada script.js Terdapat fungsi untuk membuat kode rahasia

```
function buatKodeRahasia() {  
  let dataAwal = "dGhlcmVpc25vc2VjcmV0";  
  let kodeFinal = atob(dataAwal).split('').reverse().join('');  
  return kodeFinal;  
}
```

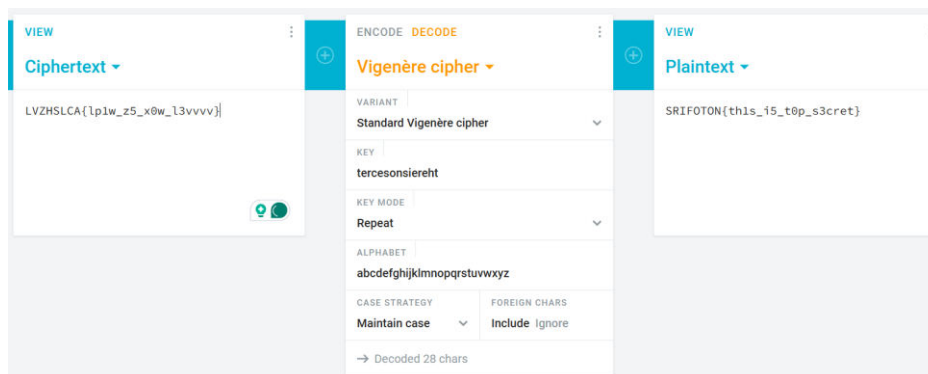
4. Saya coba untuk melihat isi dari kodeFinal



```
index.js  +  43xd2eh78  ✎  
1 let dataAwal = "dGhlcmVpc25vc2VjcmV0";  
2 let kodeFinal = atob(dataAwal).split('').reverse().join('');  
3 console.log(kodeFinal)  
STDIN  
Input for the progr  
Output:  
tercesonsiereht
```

Hasilnya adalah “tercesonsiereht”

5. Kemudian dari hint pada script.js “Seorang diplomat Prancis dari abad ke-16 meninggalkan metode ini. Gunakan kunci yang telah kau dapatkan”, saya coba menggunakan vignere cipher untuk flag LVZHSICA{lp1w_z5_x0w_l3vvvv} dengan key “tercesonsiereht”



Maka didapatkan flagnya adalah SRIFOTON{th1s_i5_t0p_s3cret}

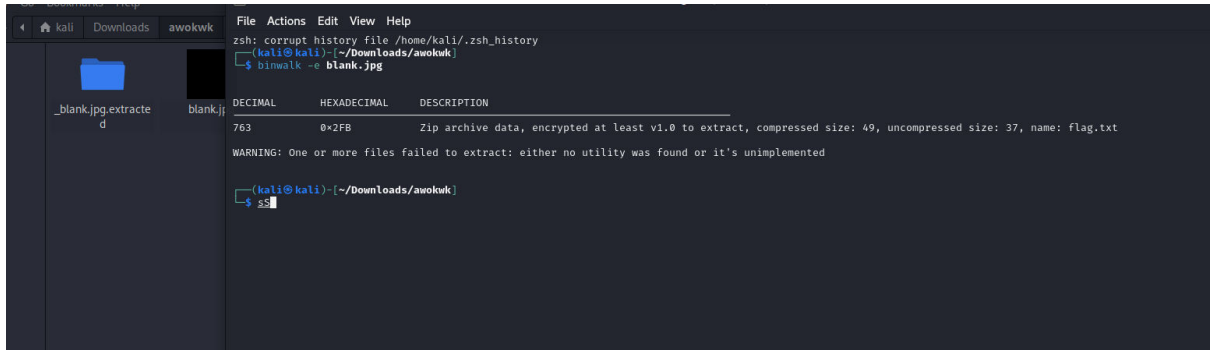
Picture Puzzle

Santarfhin

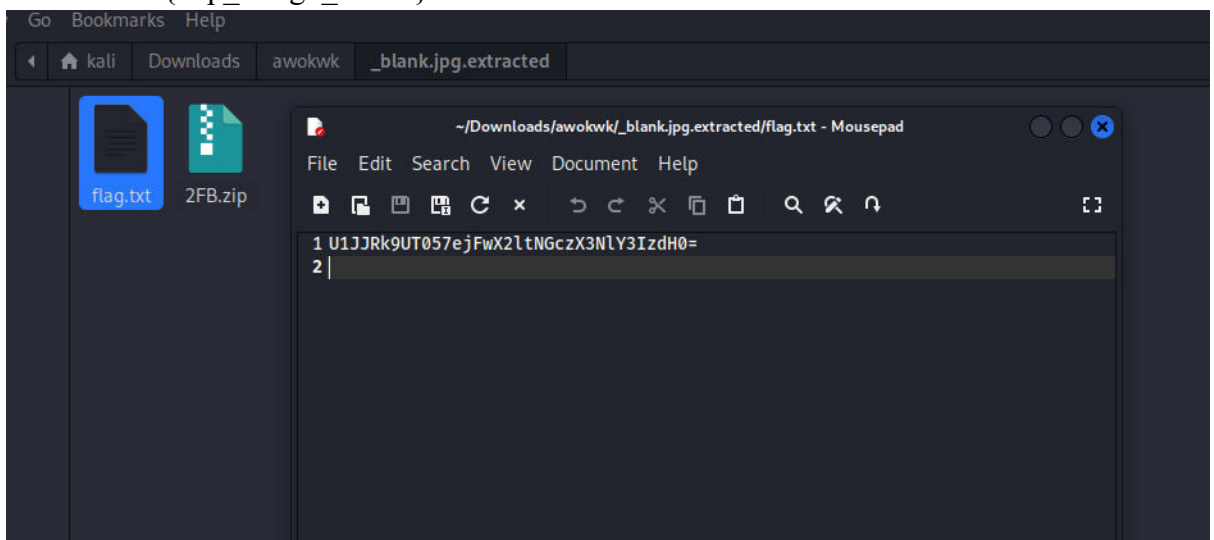
Forensic

Write-up Penyelesaian

1. diberikan sebuah file blank.jpg, seperti biasa saya mencari informasi terlebih dahulu menggunakan tools binwalk, binwalk -e (extract) blank.jpg



2. terdapat dua info disini, yang pertama ada flag.txt, saya mengubah nama blank.jpg jadi nama flag.txt, dan ada HEX yang jika di konversikan menjadi **forgottenclock**, itu adalah password untuk zip yang tersembunyi, masukan password zip tersebut, dan buka flag.txt
3. terdapat base64, yang jika kita konversikan akan menghasilkan SRIFOTON{z1p_im4g3_secr3t}



Quantum Belt
Santarfhin
Reverse Engineering

Write-up Penyelesaian

1. Diikan sebuah attachment code.py dan flag.txt. Dari hasil Analisa code.py, dia melakukan scramble terhadap flag.
2. Fungsi get_flag() membuat setiap karakter flag menjadi sebuah objek dictionary

```
def get_flag():  
    flag = open('flag.txt', 'r').read()  
    flag = flag.strip()  
  
    hex_flag = []  
    for i, c in enumerate(flag):  
        char_data = {  
            'hex': str(hex(ord(c))),  
            'pos': i,  
            'char': c  
        }  
        hex_flag.append([char_data])  
  
    return hex_flag
```

3. Fungsi advance_scramble() melakukan pop kemudian menempelkan data lain ke dalam dictionary.
4. Kita hanya perlu melakukan decode, dengan membalikkan kode yang telah diberikan, maka akan didapatkan flagnya : SRIFOTON{I0nlYtHr3wTh15p4rTyFOrY0u}

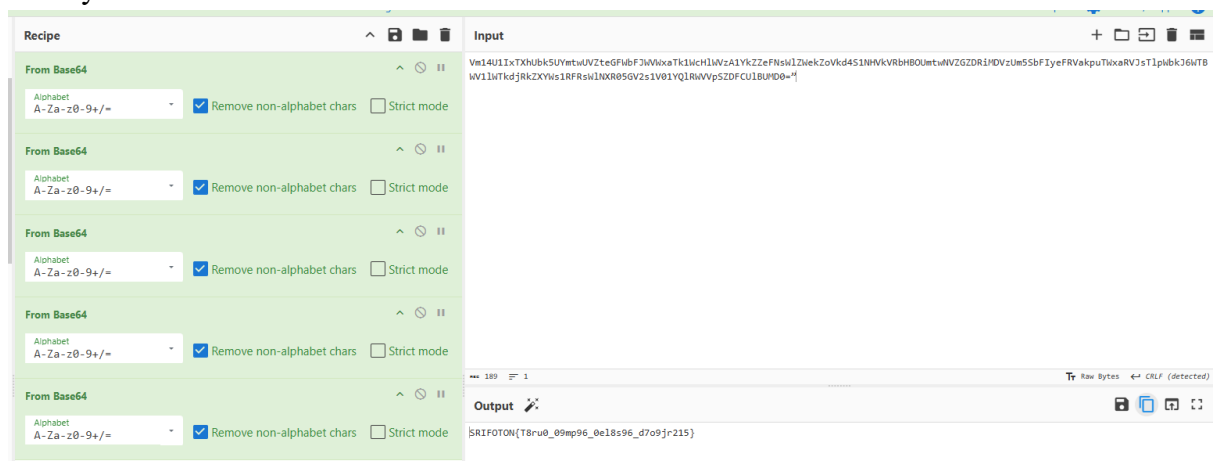
Ruins Inscription

Santarfhin

Cryptography

Write-up Penyelesaian

1. Diberikan sebuah file berisi tulisan kuno:
“Vm14U1IxTXhUbk5UYmtwUVZteGFWbFJWVWxaTk1WcHIWVzA1YkZZeFNsWlZWekZoVkd4S1NHVkvRbHBOUmtwNVZGZDRiMDVzUm5SbFIyeFRVakpuTWxaRVJsTlpWbkJ6WTBWV1lWtkdjRkZXYWslRFRsWINXR05GV2s1V01YQIRWVpSZDFCUIBUMD0=”
2. Karena diakhirnya terdapat “=” saya coba decode menggunakan base64, ketika dilakukan sekali, sepertinya kita masih dapat mendecodenya, saya lakukan decode ini sebanyak 5 kali



Saya kira ini sudah selesai karena telah membentuk format flag SRIFOTON{}, namun ternyata kita perlu menggeser “angka” 5 langkah ke depan.

3. Geser angka menjadi 5 angka setelahnya, akhirnya flagnya menjadi SRIFOTON{T3ru5_54mp41_5el3s41_d2o4jr760}

Secret Message Simulation

Santarfhin

Cryptography

Write-up Penyelesaian

1. awalnya ini adalah ROT13, saya coba decode

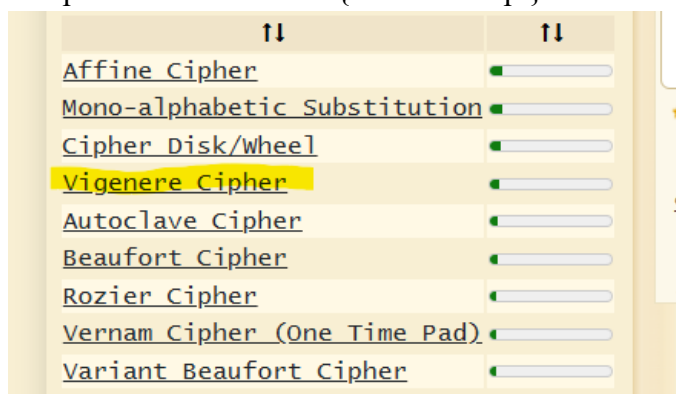
```
Enfun: Ucyxbj, lbh'er va?
Appbvc: V nã va, cëbtäbvf?
Enfun: V inã gë uvqr fbär zffntc
Appbvc: Ru, jung xvag?
Enfun: N pvcure, bs pbhefc
Appbvc: Xnl, fcvg va bbg
Enfun: KRAMOLOF{hwwakfknlpt}
Appbvc: Uru, nabgure pvcure va cyngc?
Enfun: Jryv, V thcfff va jvvy fgyxy or rnfj
Appbvc: Vagrrc
Enfun: Xnl, frr lbh
Appbvc: Frr lbh
```

↓

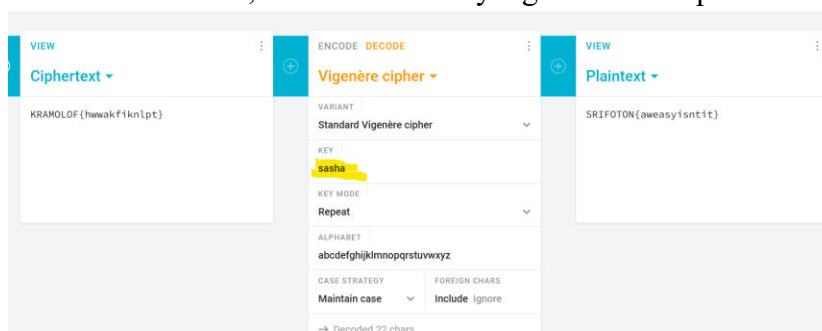
ROT13 ↓

Sasha: Hello, you're in?
Nicole: I am in, prognosis?
Sasha: I want to hide some message
Nicole: Eh, what kind?
Sasha: A cipher, of course
Nicole: Kay, spit it out
Sasha: KRAMOLOF{hwwakfknlpt}
Nicole: Heh, another cipher in place?
Sasha: Well, I guess it will still be easy
Nicole: Indeed
Sasha: Kay, see you
Nicole: See you

2. didapatkan KRAMOLOF{hwwakfknlpt}



3. saya langsung mencoba vigenere cipher, dengan kunci sasha, saya memiliki asumsi sasha adalah kunci, karena tentu dia yang membuat cipher tersebut

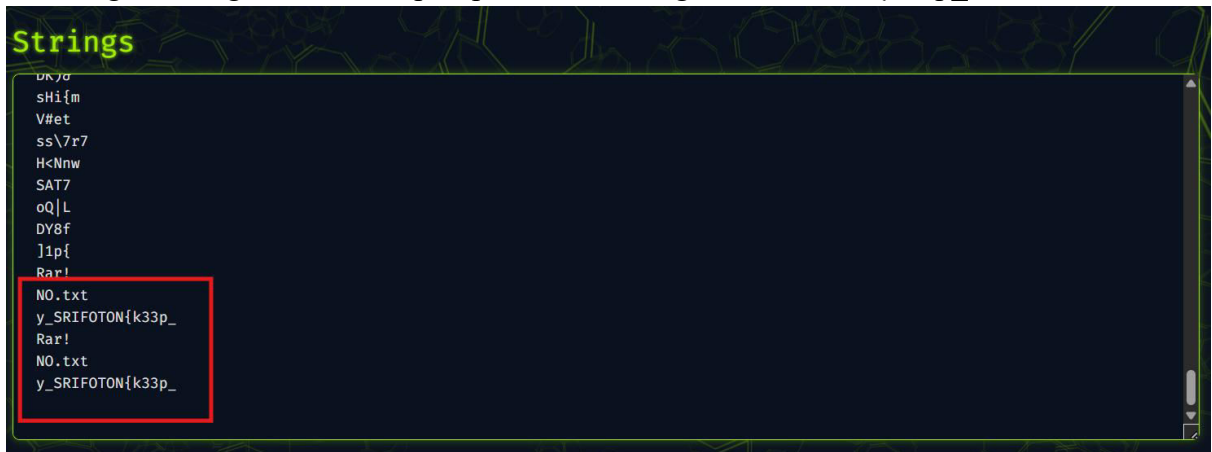


SRIFOTON{awesomeisntit}

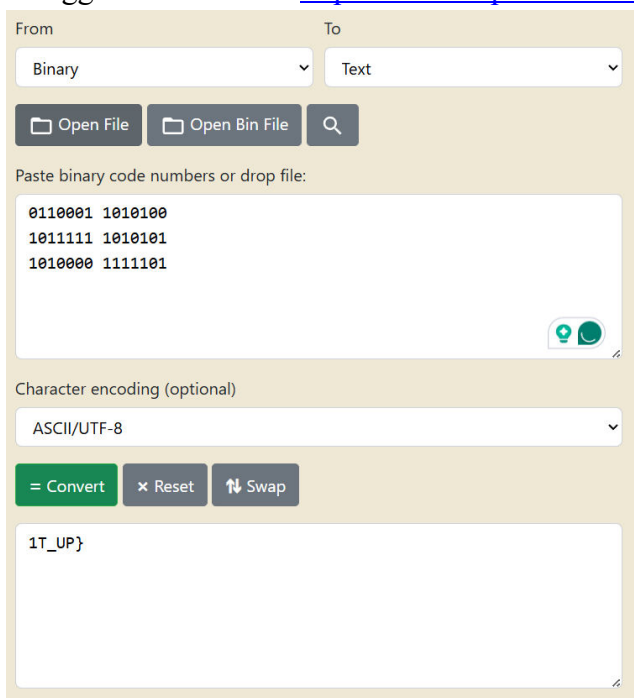
Sus Stranger
Santarfhin
Cryptography

Write-up Penyelesaian

1. Diberikan sebuah attachment Bernama Aneh.jpg
2. Kita coba lakukan Analisa dengan menggunakan website <https://www.aperisolve.com/>
3. Pada bagian strings, ditemukan part pertama dari flag : SRIFOTON{k33p_



4. Kemudian pada visual Aneh.jpg terdapat biner, yang kemudian saya ubah ke teks menggunakan website <https://www.rapidtables.com/convert/number/binary-to-ascii.html>

A screenshot of a web application for converting binary to text. It has two dropdown menus: "From" set to "Binary" and "To" set to "Text". Below these are buttons for "Open File", "Open Bin File", and a search icon. A text area labeled "Paste binary code numbers or drop file:" contains the following binary code:
0110001 1010100
1011111 1010101
1010000 1111101
Below the text area is a "Character encoding (optional)" dropdown set to "ASCII/UTF-8". At the bottom are buttons for "Convert", "Reset", and "Swap". The "Convert" button is highlighted in green. Below the buttons is a text area showing the result of the conversion: "1T_UP}".

Maka didapatkan part ke-2nya yaitu : 1T_UP}

5. Satukan flagnya menjadi SRIFOTON{k33p_1T_UP}

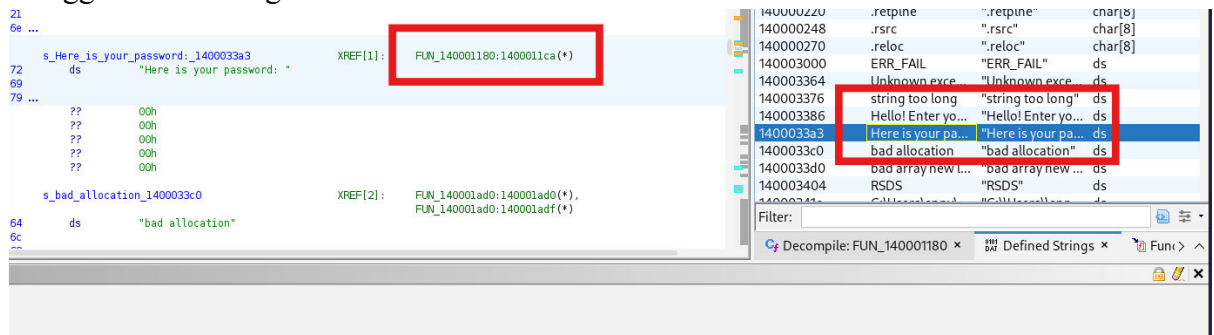
The Bos's Password

Santarfhin

Reverse Engineering

Write-up Penyelesaian

1. di beri file windows exe, diminta memberikan 6 digit pin, seperti biasa saya menggunakan tools ghidra



2. di sini ada sebuah fungsi yang menarik, saya double click strings, dan menuju FUN_140001180

```
pcVar1 = cout_exref;
local_24[1] = -2;
local_24[2] = -1;
FUN_1400012e0((basic_ostream< *)cout_exref,"Hello! Enter your PIN h
std::basic_istream<::operator>>((basic_istream< *)cin_exref,local_
FUN_140001000(local_48,local_24[0]);
pbVar3 = FUN_1400012e0((basic_ostream< *)pcVar1,"Here is your passw
pppuVar4 = local_48;
if (0xf < local_30) {
    pppuVar4 = (undefined8 ***)local_48[0];
}
pbVar3 = FUN_140001740(pbVar3,pppuVar4,local_38);
cVar2 = std::basic_ios<::widen((basic_ios< *)pbVar3 + *(int *)('
std::basic_ostream<::put(pbVar3,cVar2);
std::basic_ostream<::flush(pbVar3);
_File = (FILE *)__acrt_iob_func(0);
fflush(_File);
std::basic_istream<::ignore((basic_istream< *)cin_exref,0x7fffffff
if (0xf < local_30) {
    pppuVar4 = (undefined8 ***)local_48[0];
}
```

3. ada sebuah function menarik lagi yaitu FUN_140001000 karena dia menyimpan pin yang kita butuhkan

```
builtin_strncpy(local_30,"ERR_FAIL",9);
local_30[9] = '\0';
if (param_2 == 0x1d8a6) {
    builtin_strncpy(local_30,"HeLLoboS",8);
}
param_1[2] = 0;
param_1[3] = 0;
```

4. di dalamnya terdapat literal flag 'HeLLoboS' dan sebuah 0x1D8A6 = 120998 (pin yang dibutuhkan si bos)
Flagnya : SRIFOTON{HeLLoboS}