FINAL

NAMA TIM : [Pengen Solved Soal PWN]

Rabu, 21 Desember 2022

MEMBER	
1	Muh Fani Akbar
2	Muhammad Ichwan
3	Paska Parahita

Daftar Isi

Reverse Engineering

Madhang

Soal:

Yuk bisa yuk XOR !! Sat set lagi kaya penyisihan langsung submit Flag Author : KangGorengan

Solving Scenario:

Diberikan sebuah file ELF-64 dengan nama madhang. Kami melakukan decompile file tersebut menggunakan ida. Pada fungsi main, terdapat beberapa kondisi apabila argumen tidak terpenuhi, apabila argumen tersebut terpenuhi maka kondisi akan menjalankan fungsi runtime_text. Berikut hasil decompile fungsi main:

```
67    fmt_Println(v2);
68    v12 = -1LL;
69    os_Exit();
70  }
71  if ( (unsigned __int64)qword_5855A8 <= 1 )
72    runtime_panicindex(v2, os_Args, v1, v6, v4, v5);
73  runtime_text(
74    v2,
75    os_Args + 16,
76    v1,
77    *(_QWORD *)(os_Args + 24),
78    v4,
79    v5,
80    *(_QWORD *)(os_Args + 16),
81    *(_QWORD *)(os_Args + 24));
82}
```

Kami melakukan pengecekan fungsi runtime_text tersebut. Untuk mendapatkan flag adalah dengan cara reverse kondisi yang melakukan XOR, dapat dilihat pada bagian yang diparser warna kuning gambar dibawah. Diketahui bahwa variable v13 berisikan hex dari .rodata main_statictmp_0004, dimana setiap hex data tersebut akan dikurang 3. Kemudian variabel v35[0] berisikan v13. Pada variabel v41 berisikan variabel v35 + 3. Dari variabel v41 tersebut dapat kita ketahui bahwa data hex nya akan kembali ke nilai semula sehingga tidak ada perubahan pada .rodata main_statictmp_0004. Jadi, untuk mendapatkan flagnya yaitu nilai hex dari main_statictmp_0004 ^ 0x7F, dimana output setiap hasil XOR tersebut adalah flag.

```
v13 = *(_QWORD *)((char *)&main_statictmp_0004 - 3);
v35[0] = v13;
v42 = 37LL;
v43 = 37LL;
v41 = (__int64)v35 + 3;
v32 = 0LL;
v39 = a7;
v40 = a8;
result = 0LL;
while ( 1 )
{
  v34 = result;
  runtime_stringiter2((__int64)v35 + 3, (__int64)v9, v10, v13, v11, v12, v39, v40, result);
  v9 = (void *)v42;
  v10 = v32;
  result = v28;
  v13 = (unsigned int)v29;
  v33 = v28;
  if ( !v28 )
    break;
  if ( v32 >= v42 )
    runtime_panicindex((int)v35 + 3, v42, v32, (unsigned int)v29, v11, v12);
  if ( ((unsigned __int8)v29 ^ 0x7F) == *(_BYTE *)(v41 + v32) )
  {
    ++v32;
  }
```

Berikut hasil decompile untuk melihat data hex dari main_statictmp_0004:

```
.rodata:000000000052B860 main_statictmp_0004 db  3Ch ; <
.rodata:000000000052B861                     db  35h ; 5
.rodata:000000000052B862                     db  4Dh ; M
.rodata:000000000052B863                     db  4Fh ; O
.rodata:000000000052B864                     db  4Dh ; M
.rodata:000000000052B865                     db  4Dh ; M
.rodata:000000000052B866                     db    4
.rodata:000000000052B867                     db  2Bh ; +
.rodata:000000000052B868                     db  4Bh ; K
.rodata:000000000052B869                     db  11h
.rodata:000000000052B86A                     db  1Bh
.rodata:000000000052B86B                     db  0Ah
.rodata:000000000052B86C                     db  4Eh ; N
.rodata:000000000052B86D                     db  4Dh ; M
.rodata:000000000052B86E                     db  3Fh ; ?
.rodata:000000000052B86F                     db  11h
.rodata:000000000052B870                     db  1Ah
.rodata:000000000052B871                     db  20h
.rodata:000000000052B872                     db  0Ch
.rodata:000000000052B873                     db  2Ah ; *
.rodata:000000000052B874                     db  12h
.rodata:000000000052B875                     db  4Eh ; N
.rodata:000000000052B876                     db  13h
.rodata:000000000052B877                     db  5Eh ; ^
.rodata:000000000052B878                     db  0Dh
.rodata:000000000052B879                     db  20h
.rodata:000000000052B87A                     db  2Fh ; /
```

Untuk solvernya:

solver-madhang.py

```python
XOR = [0x3C,0x35,0x4D,0x4F,0x4D,0x4D,0x04,0x2B,0x4B,0x11,0x1B,0x0A,
    0x4E,0x4D,0x3F,0x11,0x1A,0x20,0x0C,0x2A,0x12,0x4E,0x13,0x5E,0x0D,
    0x20,0x2F,0x0A,0x4F,0x4F,0x4F,0x4F,0x33,0x33,0x33,0x02,0x75,0x00]

flag = ""
for i in range(len(XOR)):
    flag += chr(XOR[i] ^ 0x7F)

print(flag)
```

```
[10:02:12]-banua@banua:~/Desktop/FINAL-CJ2022/Rev
Shell-$ python3 solver-madhang.py
CJ2022{T4ndu12@ne_sUm1l!r_Pu0000LLL}
```

FLAG : CJ2022{T4ndu12@ne_sUm1l!r_Pu0000LLL}

Aplikasi Apa Tuh?

Soal:

Again not siti and slamet.

This Desktop Application Code Editor (Win7 & Win10)

Not Virus after scan VirusTotal

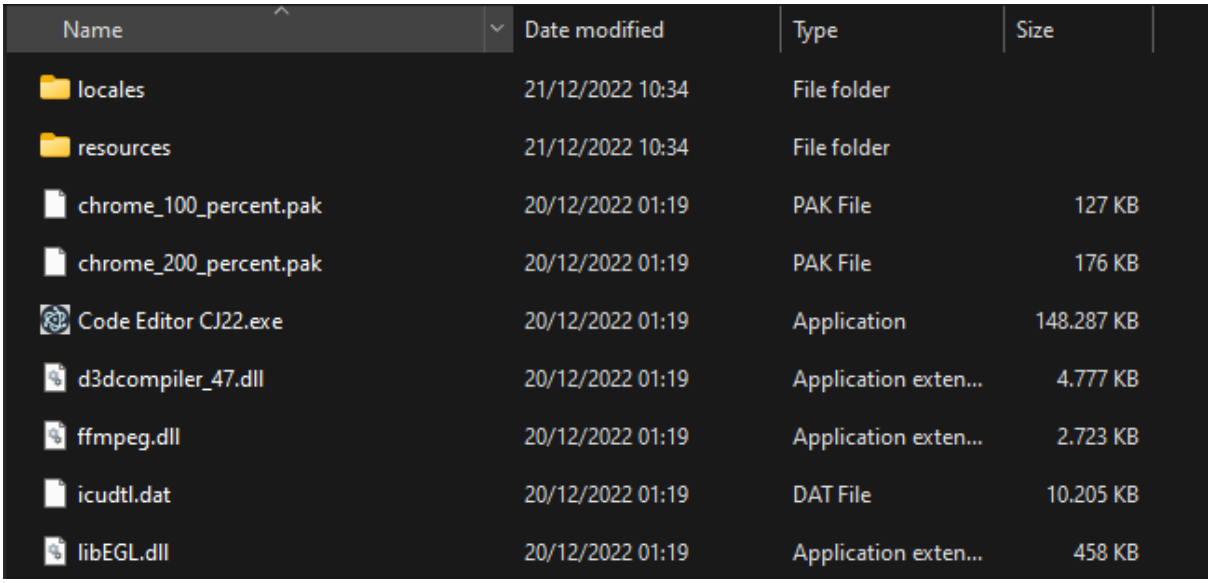
Code Editor Download

pisan2 boso inggris

Author : KangGorengan

Solving Scenario:

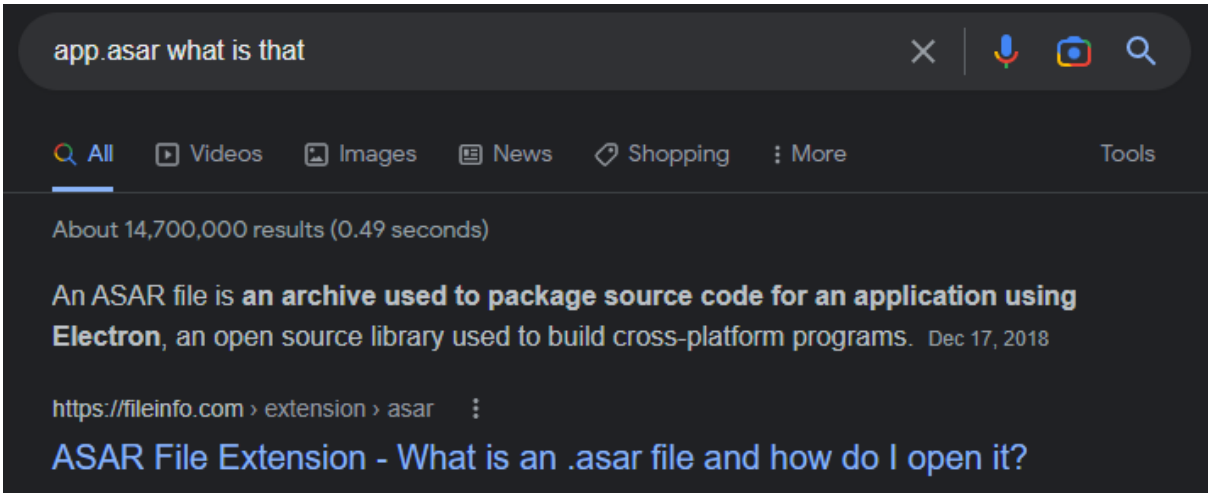
Diberikan sebuah file dengan ekstensi .msi. Disini kami melakukan browsing tentang reversing .msi. Diketahui bahwa perlu dilakukan extract terlebih dahulu. Untuk ekstrak kami mengikuti referensi ini dibanding menggunakan 7z. Berikut referensinya (http://devonenote.com/2010/03/uncompress-msi-file/)



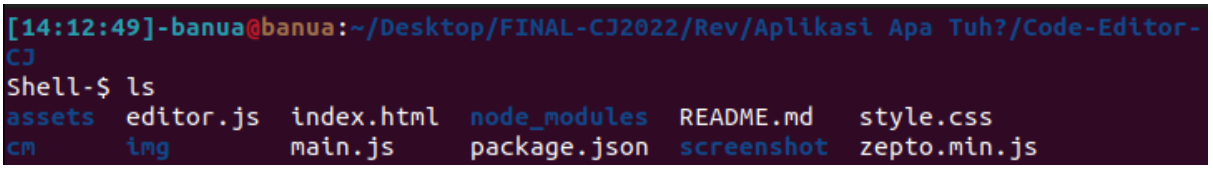
Name	Date modified	Type	Size
locales	21/12/2022 10:34	File folder	
resources	21/12/2022 10:34	File folder	
chrome_100_percent.pak	20/12/2022 01:19	PAK File	127 KB
chrome_200_percent.pak	20/12/2022 01:19	PAK File	176 KB
Code Editor CJ22.exe	20/12/2022 01:19	Application	148.287 KB
d3dcompiler_47.dll	20/12/2022 01:19	Application exten...	4.777 KB
ffmpeg.dll	20/12/2022 01:19	Application exten...	2.723 KB
icudtl.dat	20/12/2022 01:19	DAT File	10.205 KB
libEGL.dll	20/12/2022 01:19	Application exten...	458 KB

Setelah dilakukan ekstract, didapatkan banyak file binary didalam foldernya. Kami coba cek satu persatu. Pada folder resources, terdapat sebuah file bernama “app.asar”. Diketahui

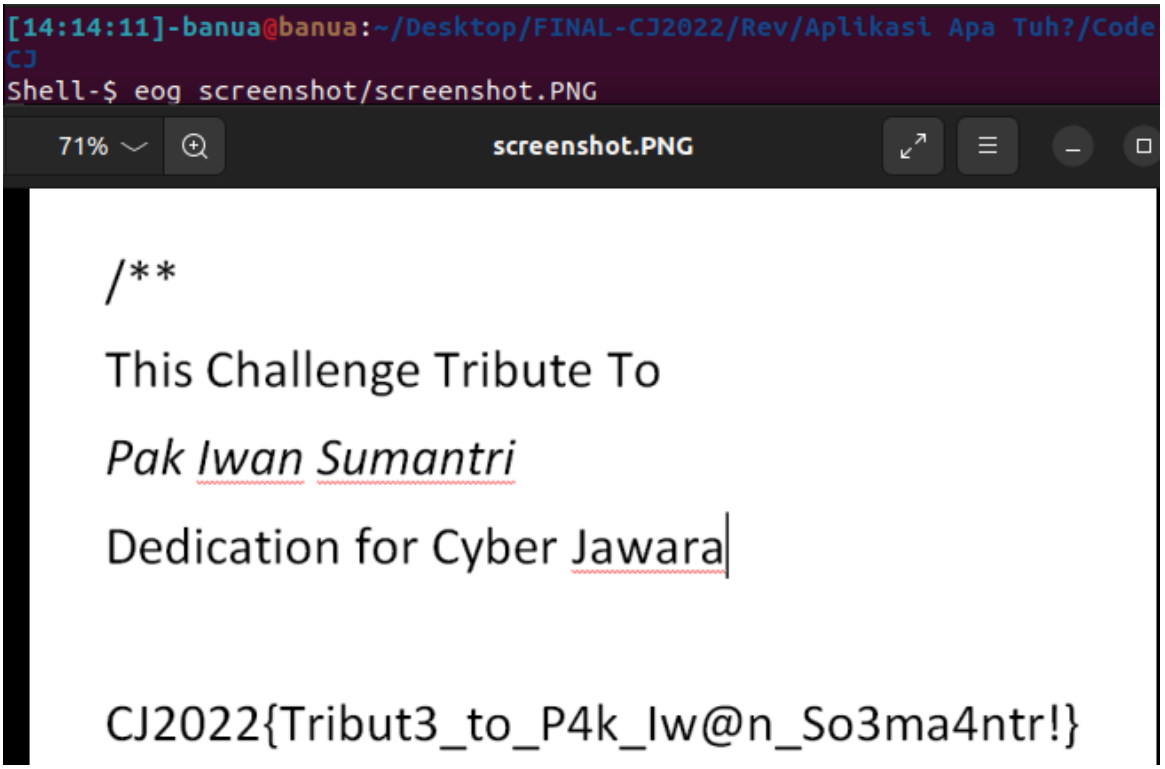
bahwa file tersebut berekstensi .asar. Kami coba cek di google ekstensi apa itu, didapatkan bahwa file .asar adalah sebuah archive source code aplikasi yang dibuild dengan Electron.



Berdasarkan artikel (https://r0075h3ll.github.io/Hacking-Electron-Applications-101/) kita bisa melakukan extract terhadap file app.asar tersebut untuk mendapatkan source code aplikasinya menggunakan npm asar. Setelah di ekstrak didapatkan source code nya.



Kami melakukan pengecekan file yang mengandung flag dengan melakukan grep namun tidak ada apa-apa. Karena terdapat folder screenshot, yang mana biasanya file image berada dalam folder img, kami mencurigai nya, coba buka file image screenshot.PNG didalam folder screenshot tersebut dan didapatkan flagnya.



FLAG : CJ2022{Tribut3_to_P4k_Iw@n_So3ma4ntr!}

Forensic

Kui R Kode ?

Soal:

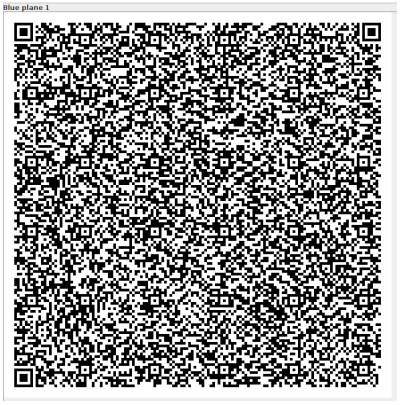
Ben Sat set tidak ada siti, slamet ataupun joko.

File langsung download

Author : KangGorengan

Solving Scenario:

Diberikan file png, ketika di scan qr codenya dengan tool online tidak ditemukan flag. Kemudian buka dengan stegsolve lalu pada blue pane 1 terlihat qr code yang berbeda dengan sebelumnya, coba save lalu scan dengan zbarimg didapat flagnya.




```
exzettabyte@ExpectoPatronum:/media/sf_pinguin/fincj$ zbarimg -q qr.png|grep CJ2022
QR-Code:Gatotkaca arab kalian sepupune engkang gadah sama Abimayu putra Arjuna. Sawij
ining dinten Abimayu nikah kalih Utari putra sangking kerajaan Wirata, pas niku Abima
yu ngaku taseh perjaka. Padahal Abimayu sampun nikah kalian Sitisundari putri Saka Kr
esna.Sitisundari engkang dititipne teng istana Gatotkaca mireng nek Abimayu nikah mal
eh. Pak-lik Gatotkaca engkang namine Kalabendana, ngajak Abimayu wangsul. Hal niku da
mel Utari cemburu. Abimayu kepeksan matur nek mpun sesomah kecobo kalian utari. Mulai
 benjeng Arjuna badhe mati dikrukuk mungsuh.Banjur Kalabendana nemono Gatotkaca, CJ20
22WOng_j00wo_oJo_il4n9_J0wO_N3 ngaturake sikape Abimayu. Nanging malah diseneni, amer
```

FLAG : CJ2022{WOng_j00wo_oJo_il4n9_J0wO_N3}