**Writeup LycoReco**

**Penyisihan CyberJawara 2022**



**Anggota tim:**

**Muhammad Garebaldhie Er Rahman**

**Frederik Imanuel Louis**

**Rachel Gabriela Chen**

# **Daftar Isi**

[**Daftar Isi**](#_jtobumv3ewy0) **2**

[**Rev**](#_qvpfgwk2a8qc) **3**

[**Madhang**](#_9i24r022rq0o) **3**

[Flag: CJ2022{T4ndu12@ne\_sUm1l!r\_Pu0000LLL}](#_fr2vz5x59zaf) 4

[Aplikasi Apa Tuh](#_xji6vf5ynask) 5

[Flag : CJ2022{Tribut3\_to\_P4k\_Iw@n\_So3ma4ntr!}](#_8fmwsd6rpirh) 5

[**Foren**](#_855p3vmv29gn) **6**

[Kiu R Code?](#_272aaiq5ksf1) 6

[Flag: CJ2022{WOng\_j00wo\_oJo\_il4n9\_J0wO\_N3}](#_z3b0o2nfvwca) 6

### 

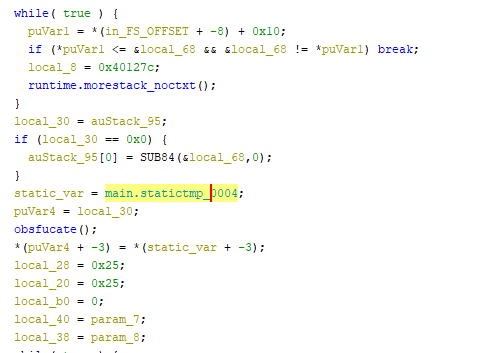
# 

# **Rev**

| Madhang **300**  Yuk bisa yuk XOR !!  Sat set lagi kaya penyisihan langsung submit Flag  Author: KangGorengan |
| --- |

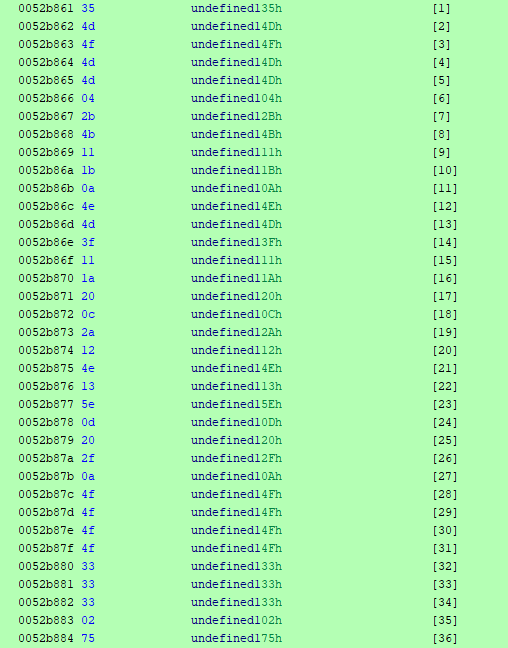
### 

Diberikan sebuah golang binary saya langsung melihat fungsi main.main namun nihil. Lalu saya melihat fungsi main.Madhang dan ternyata dia melakukuan banyak sekali operasi dengan suatu static var yaitu main.statictmp\_0004





Kami pun langsung melihat isi dari static tersebut dan terdapat suatu array yang berisi byte.



Setelah mendapatkan datanya pada bagian akhir kode terdapat operasi XOR dengan 0x7f



Tinggal dibuat scriptnya lalu didapat flag

*from* string *import* printable

*from* pwn *import* \*

arr = [

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,

]

text = b""

*for* j in range(len(arr)):

text += xor(arr[j], 0x7F)

*if* text.startswith(b"CJ"):

print(hex(0x7F), text)

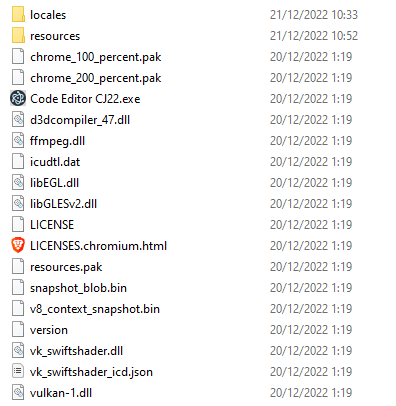


### Flag: CJ2022{T4ndu12@ne\_sUm1l!r\_Pu0000LLL}

| Aplikasi Apa Tuh **300**  Again not siti and slamet.  This Desktop Application Code Editor ( Win7 & Win10)  pisan2 boso inggris  Author : KangGorengan |
| --- |

### 

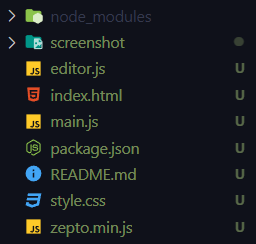
Diberikan sebuah installer windows file yang memilki ekstensi .msi, Setelah diinstall ternyata applikasi tersebut merupakan aplikasi code editor yang dibuat menggunakan electron



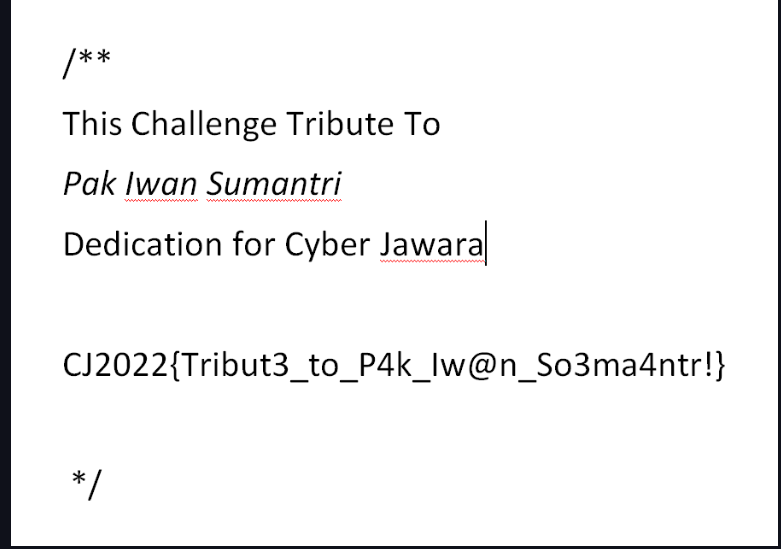
Kami pun membuka folder resource dan mendapat file dengan extensi .asar



Setelah melakukan research didapat bahwa .asar dapat di decompile dengan menggunakan package pada npm. Lalu didapat hasil sebagai berikut



Kami pun membuka screenshot dan terdapat screenshot yang berisi flag

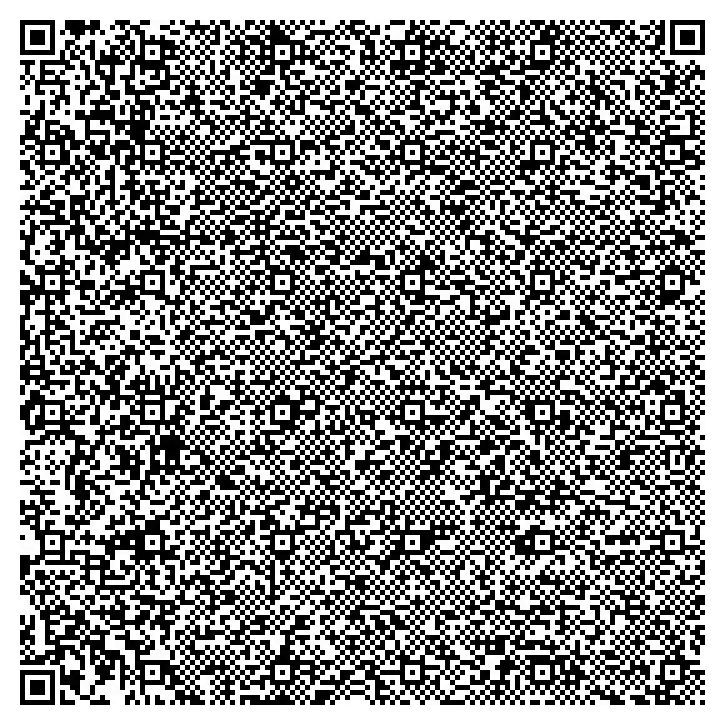


### Flag : CJ2022{Tribut3\_to\_P4k\_Iw@n\_So3ma4ntr!}

# Foren

| Kiu R Code? **300**  Ben Sat set tidak ada siti, slamet ataupun joko.  File langsung download  Author : KangGorengan |
| --- |

Diberikan sebuah image .png yang memuat sebuah QR code:



Setelah discan didapatkan:

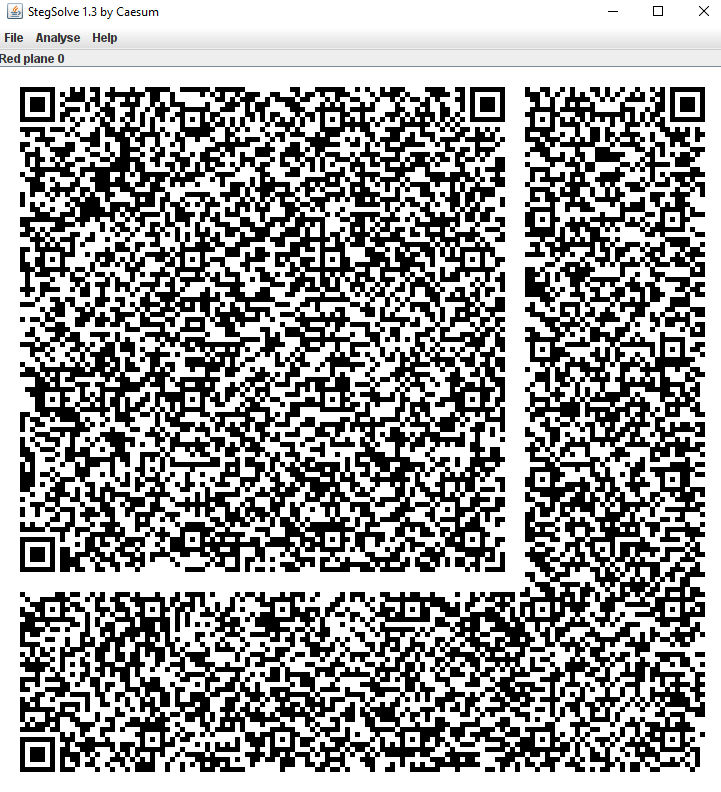
01000111 01100001 01110100 01101111 01110100 01101011 01100001 01100011 01100001 00100000 01100001 01110010 01100001 01100010 00100000 01101011 01100001 01101100 01101001 01100001 01101110 00100000 01110011 01100101 01110000 01110101 01110000 01110101 01101110 01100101 00100000 01100101 01101110 01100111 01101011 01100001 01101110 01100111 00100000 01100111 01100001 01100100 01100001 01101000 00100000 01110011 01100001 01101101 01100001 00100000 01000001 01100010 01101001 01101101 01100001 01111001 01110101 00100000 01110000 01110101 01110100 01110010 01100001 00100000 01000001 01110010 01101010 01110101 01101110 01100001 00101110 00100000 01010011 01100001 01110111 01101001 01101010 01101001 01101110 01101001 01101110 01100111 00100000 01100100 01101001 01101110 01110100 01100101 01101110 00100000 01000001 01100010 01101001 01101101 01100001 01111001 01110101 00100000 01101110 01101001 01101011 01100001 01101000 00100000 01101011 01100001 01101100 01101001 01101000 00100000 01010101 01110100 01100001 01110010 01101001 00100000 01110000 01110101 01110100 01110010 01100001 00100000 01110011 01100001 01101110 01100111 01101011 01101001 01101110 01100111 00100000 01101011 01100101 01110010 01100001 01101010 01100001 01100001 01101110 00100000 01010111 01101001 01110010 01100001 01110100 01100001 00101100 00100000 01110000 01100001 01110011 00100000 01101110 01101001 01101011 01110101 00100000 01000001 01100010 01101001 01101101 01100001 01111001 01110101 00100000 01101110 01100111 01100001 01101011 01110101 00100000 01110100 01100001 01110011 01100101 01101000 00100000 01110000 01100101 01110010 01101010 01100001 01101011 01100001 00101110 00100000 00001010 01010000 01100001 01100100 01100001 01101000 01100001 01101100 00100000 01000001 01100010 01101001 01101101 01100001 01111001 01110101 00100000 01110011 01100001 01101101 01110000 01110101 01101110 00100000 01101110 01101001 01101011 01100001 01101000 00100000 01101011 01100001 01101100 01101001 01100001 01101110 00100000 01010011 01101001 01110100 01101001 01110011 01110101 01101110 01100100 01100001 01110010 01101001 00100000 01110000 01110101 01110100 01110010 01101001 00100000 01000110 01101100 01100001 01100111 00100000 01000011 01001010 00100000 01101110 01111001 01100001 00100000 01110100 01101001 01100100 01100001 01101011 00100000 01100001 01100100 01100001 00100000 01100100 01101001 01110011 01101001 01101110 01101001 00100000 01101011 01100001 01110111 01100001 01101110 00101110.

Setelah didecode didapatkan:

“Gatotkaca arab kalian sepupune engkang gadah sama Abimayu putra Arjuna. Sawijining dinten Abimayu nikah kalih Utari putra sangking kerajaan Wirata, pas niku Abimayu ngaku taseh perjaka.

Padahal Abimayu sampun nikah kalian Sitisundari putri Flag CJ nya tidak ada disini kawan.”

Kami pun mencoba untuk melakukan ekstraksi menggunakan binwalk dan foremost namun tidak mendapat hasil. Lalu kami mencoba untuk membuka qr code tersebut dengan stegsolve lalu mulai memainkan plane nya. Pada red plane 0 ternyata terdapat qrcode baru yang melapisi qr code sebelumnya. Tinggal di scan lalu dapat flag



“GatotkacaarabkaliansepupuneengkanggadahsamaAbimayuputraArjuna.SawijiningdintenAbimayunikahkalihUtariputrasangkingkerajaanWirata,pasnikuAbimayungakutasehperjaka.PadahalAbimayusampunnikahkalianSitisundariputriSakaKresna.SitisundariengkangdititipnetengistanaGatotkacamirengnekAbimayunikahmaleh.Pak-likGatotkacaengkangnamineKalabendana,ngajakAbimayuwangsul.HalnikudamelUtaricemburu.Abimayukepeksanmaturnekmpunsesomahkecobokalianutari.MulaibenjengArjunabadhematidikrukukmungsuh.BanjurKalabendananemonoGatotkaca, **CJ2022WOng\_j00wo\_oJo\_il4n9\_J0wO\_N3** ngaturakesikapeAbimayu.Nangingmalahdiseneni,amergikewanennyampuriurusanesepupuneiku.Gatotkacaemosi,banjurgebugsiraheKalabendana.Senajankelakunnikuwaumbotensengaja,nangingdamelPaklikematisaknalika.”

### 

### Flag: CJ2022{WOng\_j00wo\_oJo\_il4n9\_J0wO\_N3}