

WRITE-UP Cyber Jawa 2022

Final

21 Desember 2022

anak kemaren sore
(*IPB University*)



» patsac «

» arai «

» jedi «

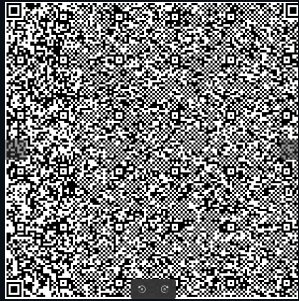
Daftar Isi

Daftar Isi	1
Forensic	2
Kui R Kode ? (300 pts)	2
Cryptography	4
Web	5
PWN	6
Reverse Engineering	7
madhag (300 pts)	7
Aplikasi Apa tuh ? (300 pts)	8

Forensic

Kui R Kode ? (300 pts)

Author: kang gorengan



Diberikan file gambar qr code dan soal ini Author nya kang gorengan berarti hanya soal peramai seperti kemarin :(. Tutorial solv nya seperti ini:

Pertama saya scan barcode nya, hasil nya berupa binary:

```
01000111 01100001 01110100 01101111 01110100 01101011
01100001 01100011 01100001 00100000 01100001 01110010
01100001 01100010 00100000 01101011 01100001 01101100
01101001 01100001 01101110 00100000 01100111 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
```

Copy

Saya decode:

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.

Lalu saya coba di stegsolve gambar nya kepotong ternyata:



Scan lagi hasilnya ini:

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 Saka Kresna. Sitisundari engkang dititipne teng istana Gatotkaca mireng nek Abimayu nikah maleh. Pak-lik Gatotkaca engkang namine Kalabendana, ngajak Abimayu wangsul. Hal niku damel Utari cemburu. Abimayu kepeksan matur nek mpun sesomah kecobo kalian utari. Mulai benjeng Arjuna badhe mati dikrukuk mungsuh. Banjur Kalabendana nemono Gatotkaca, CJ2022W0ng_j00wo_oJo_i14n9_J0w0_N3 ngaturake sikape Abima

Copy

Flag : CJ2022{W0ng_j00wo_oJo_i14n9_J0w0_N3}



jedi Today at 5:41 PM
!help



Quiz Bot **BOT** Today at 5:41 PM
Usage: To use quiz bot
!help : show help information
!question: give you a question
to answer just type the alphabet order: A



jedi Today at 5:41 PM
!question



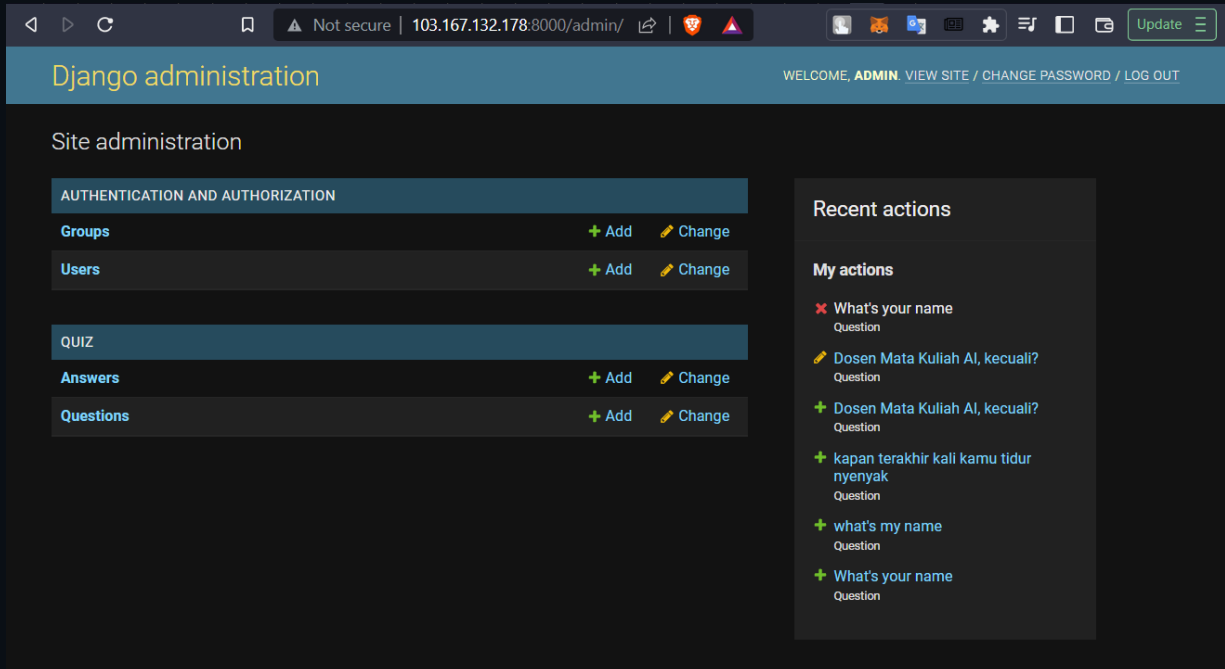
Quiz Bot **BOT** Today at 5:41 PM
Question:
Dosen Mata Kuliah AI, kecuali?
A. Bu Wulan
B. Bu Yeni
C. Bu Medria
D. Pak Auriza



jedi Today at 5:41 PM
D



Quiz Bot **BOT** Today at 5:41 PM
Correct!



Cryptography

Terlalu kerad bang 🤔

Web

Ngga solp bang :(

PWN

Ngga solp bang :(

Reverse Engineering

madhag (300 pts)

Description

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

Author : KangGorengan

[madhag](#)

Diberikan sebuah file binary. Ketika dicek, ternyata dia melakukan operasi xor antara sebuah string dengan 0x7f

```
break;
if ( v22 >= v32 )
    runtime_panicindex(v25 + 3);
if ( (v19 ^ 0x7F) == *(v31 + v22) )
{
    ++v22;
}
```

```
33 while ( &v26 <= *(__readfsqword(0xFFFFFFFF8) + 16) )
34     runtime_morestack_noctxt();
35 if ( &v15 == -83LL )
36     *(v25 + 3) = &v26;
37 v8 = &flag;
38 sub_455F84(v25 + 3, &flag);
39 v25[0] = *(&flag - 3);
```

String tersebut berada di dalam array flag

Cukup kita export isi array tersebut dan kita xor dengan 0x7f

Berikut solver yang dibuat

solver.cpp

```
#include<bits/stdc++.h>
using namespace std;

int main(){
    unsigned char kar[] =
    {
        60, 53, 77, 79, 77, 77, 4, 43, 75, 17,
        27, 10, 78, 77, 63, 17, 26, 32, 12, 42,
        18, 78, 19, 94, 13, 32, 47, 10, 79, 79,
```

```
79, 79, 51, 51, 51, 2, 117
};
int a;
for(int i=0; i<37; i++){
    cout << char(kar[i]^127);
}
}
```

```
/mnt/d/CTF/cyberjawara/rev 16:18:03
$ ./solver
CJ2022{T4ndu12@ne_sUm1l!r_Pu0000LLL}
```

Flag : CJ2022{T4ndu12@ne_sUm1l!r_Pu0000LLL}

Aplikasi Apa tuh ? (300 pts)

Description

Again not siti and slamet.
This Desktop Application Code Editor (Win7 & Win10)

Not Virus after scan VirusTotal

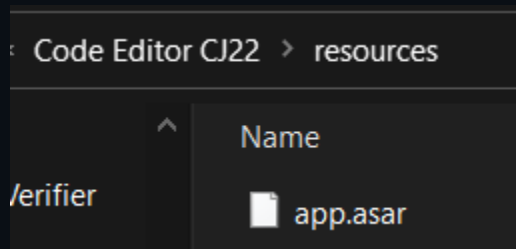
Code Editor [Download](#)

pisan2 boso inggris

Author : KangGorengan

Diberikan sebuah file windows installer. Setelah diinstall, dicoba untuk dibuka aplikasinya. Karena tidak ada apapun yang bisa dilakukan dan yang menarik, dicek ke dalam program files hasil menginstall aplikasinya

Terdapat folder yang menarik berupa "resources" yang memiliki file bertipe data .asar



Ketika dicari di google, terdapat cara untuk mengextract isi dari file app.asar tersebut. Kita install terlebih dahulu asar dengan npm, lalu extract isi dari app.asar. Ketika dibuka hasil extractnya, terdapat folder screenshot yang jika dibuka, kita bisa melihat gambar dengan flag yang kita cari

```
/mnt/d/CTF/cyberjawara/rev 17:24:29
$ asar extract app.asar aplikasi/

/mnt/d/CTF/cyberjawara/rev 17:24:51
$ cd aplikasi

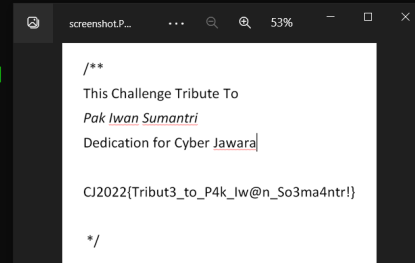
/mnt/d/CTF/cyberjawara/rev/aplikasi 17:25:00
$ ls
README.md  editor.js  index.html  main.js  package.json  screenshot

/mnt/d/CTF/cyberjawara/rev/aplikasi 17:25:01
$ cd screenshot

/mnt/d/CTF/cyberjawara/rev/aplikasi/screenshot 17:25:11
$ ls
screenshot.PNG

/mnt/d/CTF/cyberjawara/rev/aplikasi/screenshot 17:25:12
$ wslview screenshot.PNG

/mnt/d/CTF/cyberjawara/rev/aplikasi/screenshot 17:25:24
$ |
```



Flag : CJ2022{Tribut3_to_P4k_Iw@n_So3ma4ntr!}