

Jatim Cybersecurity Competition 2026

The writeups by Proxy Team SMAN 1 Mojokerto



Disusun oleh

1. Muhammad Ismail Yusuf
2. Alvino Clemence Nugroho

Daftar Isi

Daftar Isi	2
Ringkasan Hasil	1
crypto-101	3
Sanity Check	6
forensics-101	8
web-101	10
rev-101	13

Ringkasan Hasil :D

Challenge	Kategori	Poin	Solved by
crypto-101	Crypto	257	Suff
forensics-101	Forensics	260	himarichx
Sanity Check	Misc	250	Suff
web-101	Web	299	Suff
rev-101	Reverse	289	Suff

crypto-101

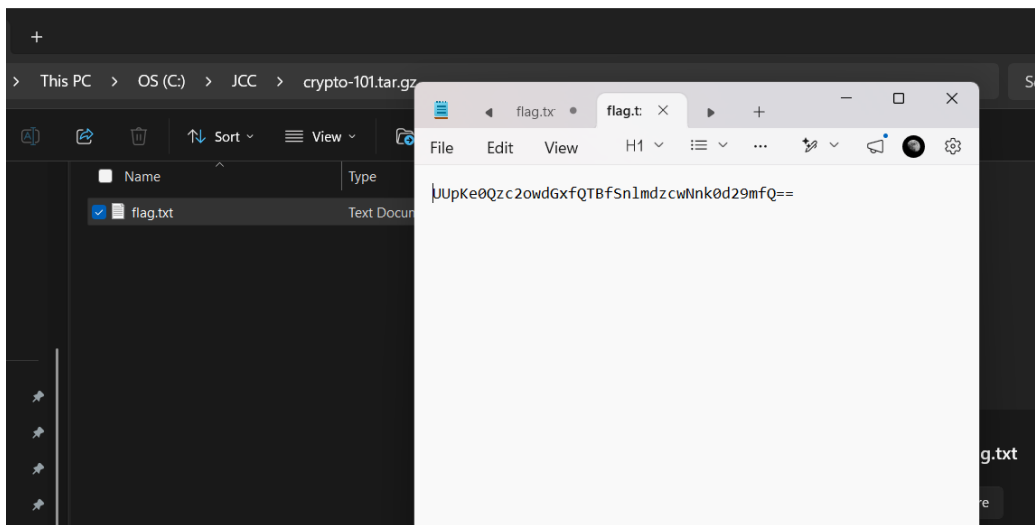
Kategori	Crypto
Poin	257
Solved by	Suff
Deskripsi Soal	Do you know what's the difference between encoding and encrypting? Why not try both? The key is missing, unfortunately.
File/Attachment	File .tar.gz — saat diekstrak berisi 1 file .txt

1. Initial Analysis

Setelah file .tar.gz diekstrak, ditemukan sebuah file .txt berisi string berikut:

UUpKe0Qzc2owdGxfQTBfSn1mdzcnNk0d29mfQ==

String tersebut diakhiri tanda '==', ciri khas encoding Base64 pada dugaan awal saya, karna sebelumnya mengerjakan warm up tanggal 8 sept 2026.



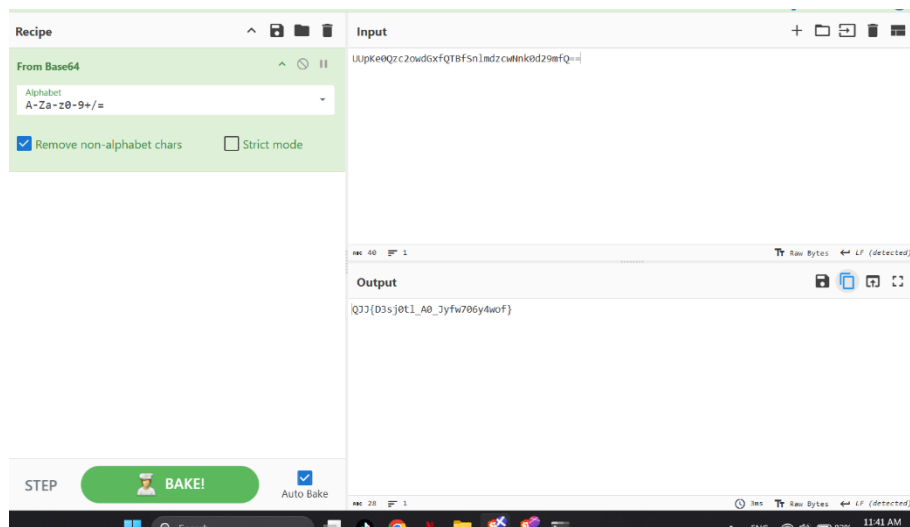
Screenshot — isi file .txt hasil ekstraksi tar.gz

2. Proses Investigasi

Langkah 1: dimasukkan ke CyberChef, operation "From Base64". Hasil:

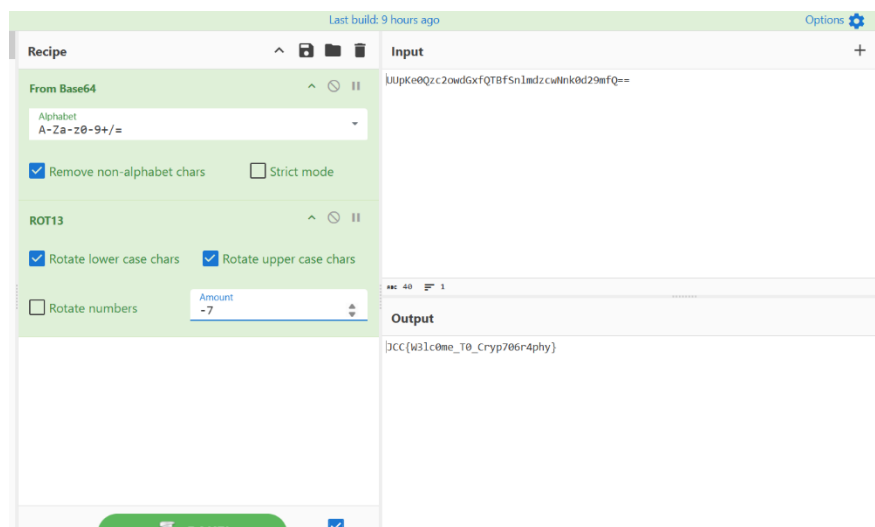
QJJ{D3sj0tl_A0_Jyfw706y4wof}

Sudah berpola flag (XXX{...}) tapi huruf tapi masih acak menurutku.



Screenshot 01 — "From Base64" di CyberChef

Langkah 2: ditambahkan "ROT13", amount dicoba-coba hingga muncul "JCC{". Amount tepat: -7.



Screenshot 02 — ROT13 amount -7 / flag final

3. Command / Script / Solver

Tidak ada script tambahan — murni recipe CyberChef:

Recipe:
 1. From Base64
 2. ROT13 (Amount: -7)

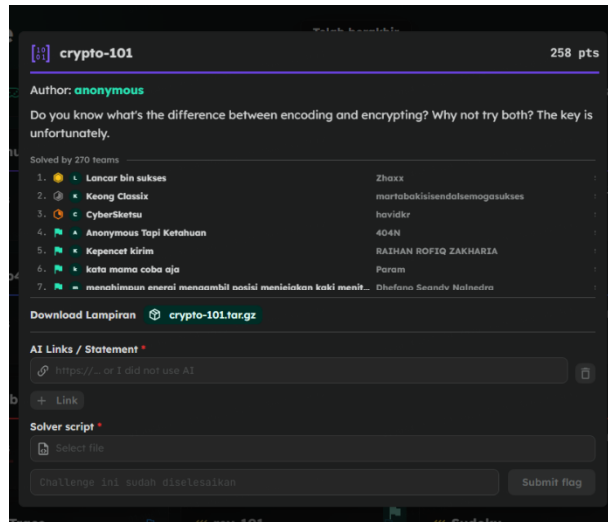
4. Breakthrough

Hasil "From Base64" sudah berbentuk pola flag meski acak — mengarahkan ke dugaan cipher rotasi huruf. Trial-and-error ROT13 menghasilkan awalan "JCC{".

5. Flag

JCC{W3lc0me_T0_Cryp706r4phy}

Disubmit dan dinyatakan benar (257 poin).



Screenshot 03 — bukti submit flag benar

6. AI Usage

Digunakan?	Tidak / I did not use AI
Provider	-
Free Tier?	-
Digunakan untuk	-
Link chat	-

Sanity Check

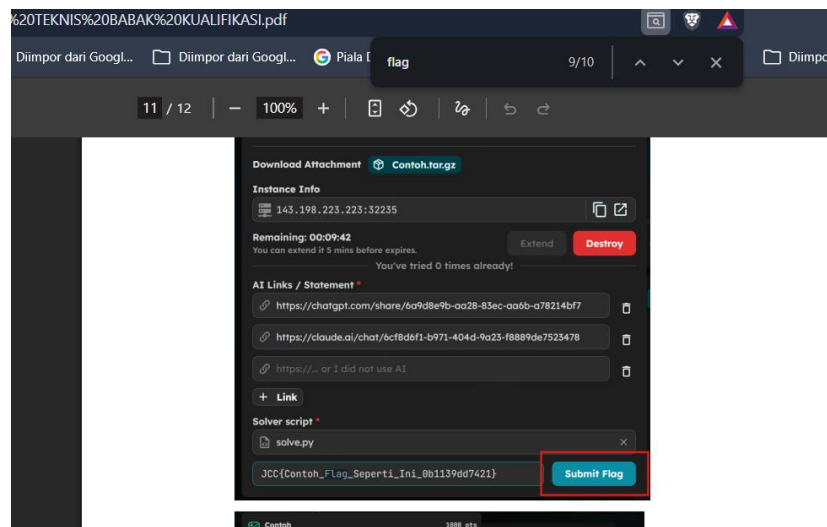
Kategori	Misc
Poin	250
Solved by	Suff
Deskripsi Soal	Author: N/A Selamat datang di Jatim Cybersecurity Competition 2026! Format flag untuk semua soal adalah JCC{.*}! Temukan flag untuk soal ini di dalam PDF Petunjuk Teknis.
File/Attachment	PDF Petunjuk Teknis (Juknis) JCC 2026

1. Initial Analysis

Memahami soal karna langsung to the point jirr , lalu membuka file PDF Petunjuk Teknis (Juknis) yang dibagikan panitia di dc.

2. Proses Investigasi

Menggunakan fitur pencarian (Ctrl+F) pada PDF dengan kata kunci "flag". Ditemukan bagian contoh tutorial pengerjaan yang menyertakan format flag secara langsung, aku iseng coba aja dan bener wowkww.



Screenshot — hasil pencarian 'flag' di PDF Juknis

3. Command / Script / Solver

Tidak ada — murni pencarian manual (Ctrl+F) di PDF viewer.

4. Breakthrough

Contoh tutorial di juknis ternyata langsung menyertakan flag sebagai ilustrasi format.

5. Flag

JCC{Contoh_Flag_Seperti_Ini_0b1139dd7421}

Langsung disubmit dan dinyatakan benar (250 poin).

6. AI Usage

Digunakan?	Tidak
Provider	-
Free Tier?	-
Digunakan untuk	-
Link chat	-

forensics-101

Kategori	Forensics
Poin	260
Solved by	himarichx
Deskripsi Soal	"Some login attempts looked unusual. Whether they were mistakes, guesses, or something else was unclear. The answer lies somewhere in the noise."
File/Attachment	[nama file tar.gz — perlu dikonfirmasi] berisi logs.jsonl

1. Initial Analysis

Challenge ini dikerjakan oleh himarichx (anggota tim). File log berformat JSON Lines (logs.jsonl) berisi banyak percobaan login (noise).

2. Proses Investigasi

Alih-alih menyaring baris satu per satu secara manual, dijalankan one-liner Python langsung di terminal/CMD untuk mencari pola flag dengan regex:

```
grep -oP 'JCC\[a-zA-Z0-9_\+\]' logs.jsonl | sort -u
```

Flag ditemukan utuh dalam satu baris log (bukan hasil gabungan potongan dari banyak baris).

```
result": "invalid_credentials"}', 'JCC{p4ck3t_c4pt7r3_m4st3ry__', "respo
lt": "invalid_credentials"}', 'JCC{w1nd0ws_3v3nt_l0gs-", "response": {"r
"invalid_credentials"}', 'JCC{_1nc1d3nt_r3sp0ns3", "response": {"result"
uf@ASUS:/mnt/c/JCC$ grep -oP 'JCC\[a-zA-Z0-9_\+\]' logs.jsonl | sort -u
CC{sp0t_0n_r3g3x}
uf@ASUS:/mnt/c/JCC$ |
```

Screenshot — output terminal Python one-liner

3. Command / Script / Solver

Bahasa: Python (one-liner, dijalankan langsung di terminal — tanpa file script terpisah).

```
python3 -c "import re; print(re.findall(r'JCC{.*?}', open('logs.jsonl').read()))"
```

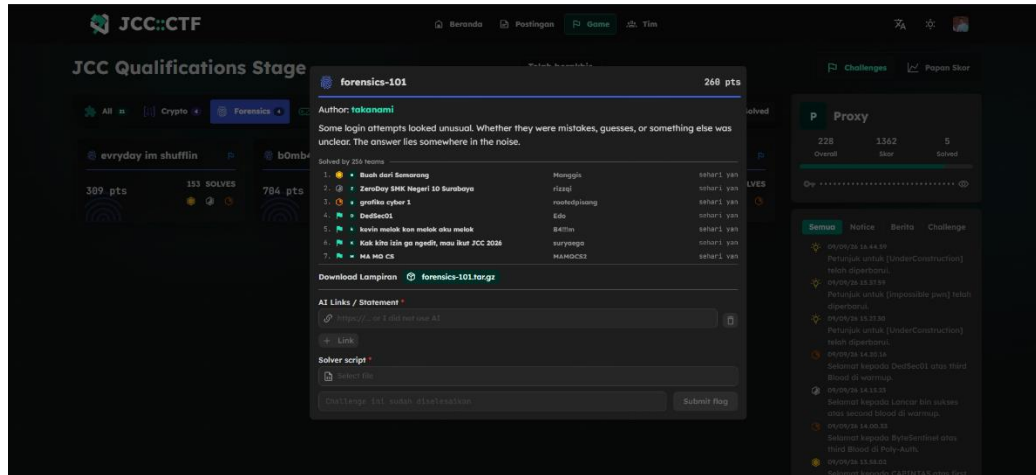
4. Breakthrough

Regex JCC{.*?} langsung menangkap pola flag dari keseluruhan isi file tanpa perlu menyaring baris gagal/sukses secara manual.

5. Flag

JCC{sp0t_0n_r3g3x}

Disubmit dan dinyatakan benar (260 poin).



Screenshot — bukti submit flag forensics-101 (sudah dikerjakan dan disubmit)

6. AI Usage

Digunakan?	Ya
Provider	Gemini
Free Tier?	Ya
Digunakan untuk	Diskusi pendekatan penyaringan log
Link chat	https://share.gemini.google/23zUN6sabOz8

web-101

Kategori	Web
Poin	299
Solved by	Suff
Deskripsi Soal	[salin deskripsi challenge di sini]
File/Attachment	Target web CTF (URL)

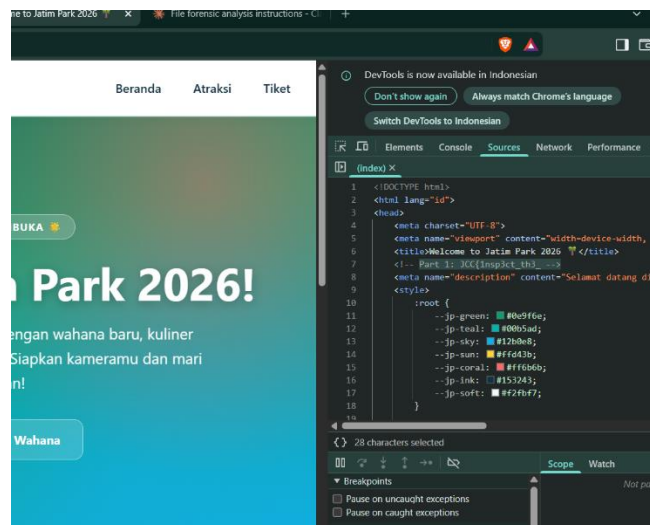
1. Initial Analysis

Memulai dengan Inspect Element pada halaman target untuk menelusuri source code, header, dan resource lain.

2. Proses Investigasi

Langkah 1: ditemukan komentar pada HTML yang berisi potongan flag pertama:

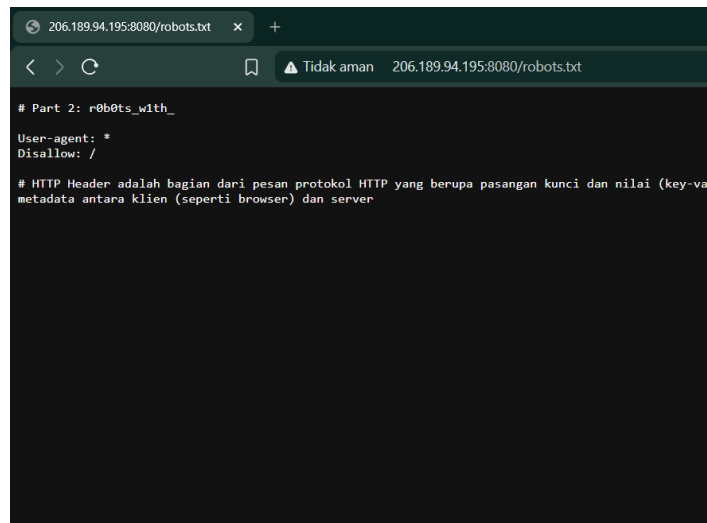
JCC{1nsp3ct_th3_



Screenshot 01 — komentar HTML

Langkah 2: petunjuk pada halaman mengarah ke robots.txt, memberi potongan:

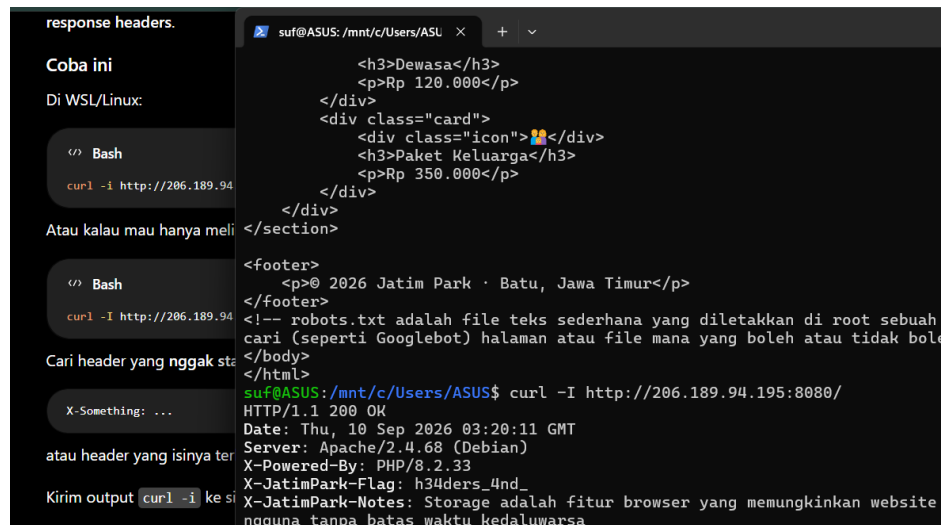
r0b0ts_w1th_



Screenshot 02 — isi robots.txt

Langkah 3: HTTP response header "X-JatimPark-Flag" memberi potongan:

h34ders_4nd_



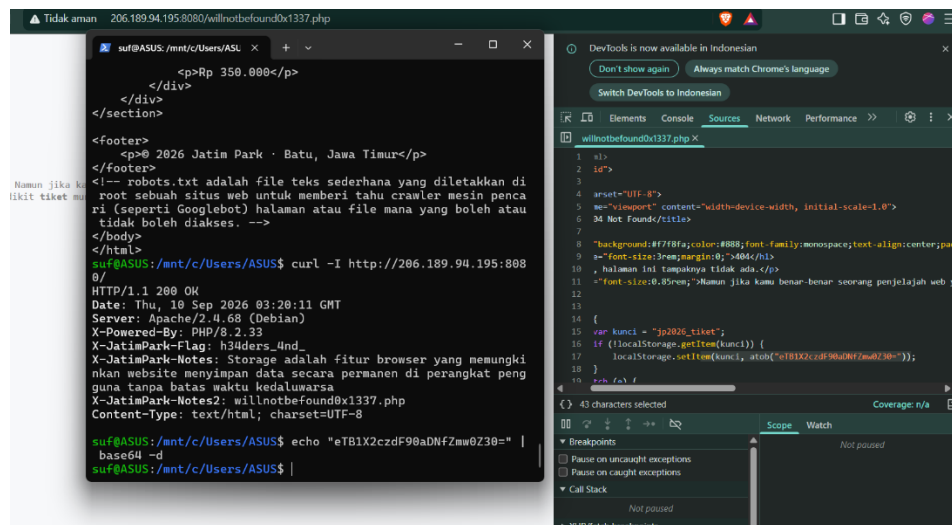
Screenshot 03 — HTTP response header X-JatimPark-Flag

Langkah 4: header juga mengarahkan ke file willnotbefound0x1337.php yang menghasilkan 404, namun JS pada halaman tersebut menyimpan value ke localStorage dengan key jp2026_tiket, berisi string Base64:

eTB1X2czdF90aDNfZmw0Z30=

Setelah di-decode Base64, menghasilkan potongan terakhir:

y0u_g3t_th3_fl4g}



Screenshot 04 — localStorage / halaman 404 JS

3. Command / Script / Solver

Decode Base64 (bisa lewat CyberChef atau terminal):

```
echo "eTB1X2czdF90aDNfZmw0Z30=" | base64 -d
```

4. Breakthrough

Menyadari bahwa kata "Storage" pada petunjuk header mengarah ke localStorage browser, dan value di dalamnya perlu di-decode dari Base64 (fungsi atob()) untuk mendapat potongan flag terakhir.

5. Flag

JCC{1nsp3ct_th3_r0b0ts_w1th_h34ders_4nd_y0u_g3t_th3_fl4g}

Seluruh potongan flag digabung sesuai urutan penemuan clue, lalu disubmit dan dinyatakan benar (299 poin).

6. AI Usage

Digunakan?	Ya
Provider	ChatGPT
Free Tier?	Ya
Digunakan untuk	Menghubungkan clue HTML/robots.txt/header/JS, dan mengidentifikasi perlu decode Base64 dari localStorage

Link chat: <https://chatgpt.com/share/6aa10c99-82d4-83ec-bfcb-79624ee6020b>

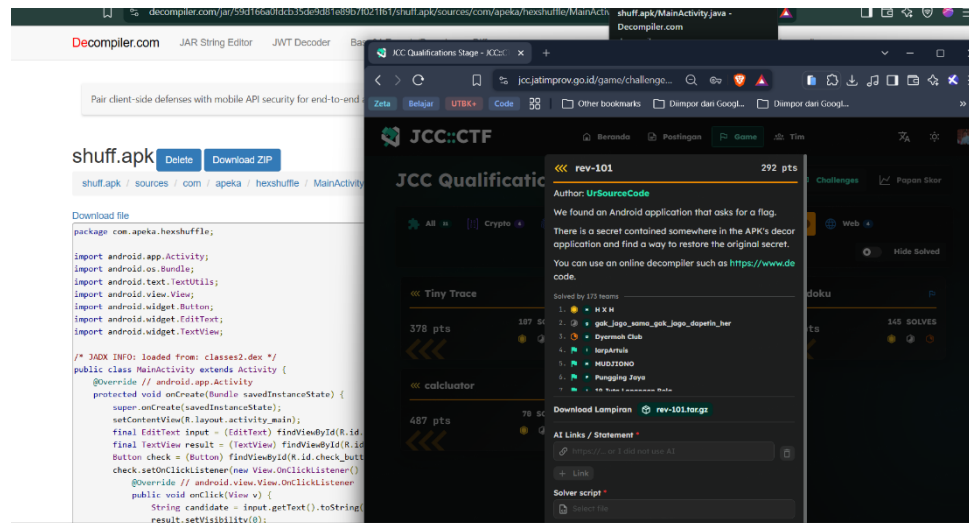
Kategori	Reverse
Poin	289
Solved by	Suff
Deskripsi Soal	[salin deskripsi challenge di sini]
File/Attachment	File APK

1. Initial Analysis

File APK di-decompile menggunakan JADX / decompiler.com untuk membaca source code Java hasil dekompilasi.

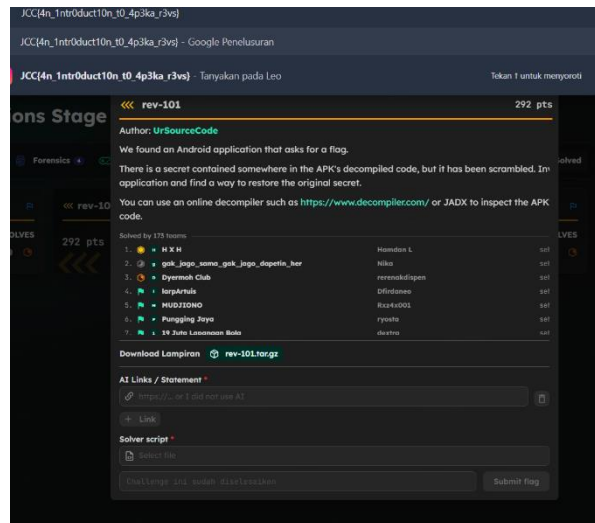
2. Proses Investigasi

Menelusuri class MainActivity, ditemukan pemanggilan fungsi SecretData.recover(). Diperiksa lebih lanjut array SecretData.ASCI dan IndexMap.ORDER.



Screenshot — kode SecretData & IndexMap di JADX

Setelah dipahami bahwa ORDER menentukan urutan indeks karakter yang harus diambil dari ASCII, karakter disusun secara manual satu per satu (bukan pakai script otomatis).



Screenshot — proses penyusunan flag manual, gaada ss asli bang ini juga udah complete

3. Command / Script / Solver

Tidak ada script otomatis — penyusunan flag dilakukan manual berdasarkan pembacaan array ASCII dan IndexMap.ORDER hasil decompile.

4. Breakthrough

Memahami bahwa IndexMap.ORDER adalah kunci urutan pengambilan karakter dari array ASCII — begitu pola ini disadari, flag bisa disusun manual.

5. Flag

JCC{4n_1ntr0duct10n_t0_4p3ka_r3vs}

Disubmit dan dinyatakan benar (289 poin).

6. AI Usage

Digunakan?	Ya
Provider	ChatGPT
Free Tier?	Ya
Digunakan untuk	Membantu menjelaskan/membaca kode hasil decompile dan mengarahkan analisis (decompile & penyusunan flag tetap dilakukan sendiri)

Link chat: <https://chatgpt.com/share/6aa219e6-0a38-83ec-a853-ac8984a0f95f>

PLEASE READ. :D !

Penyusunan WU ini dibantu dan digenerate CLAUDE AI Free Tier , lalu untuk penulisan , gambar dilakukan oleh SAYA SENDIRI, tapi untuk layout dibantu oleh claude. Agar rapi dan sesuai, apa yang kami kerjakan memang seperti ini tanpa diubah atau rekayasa. Kami hanya mencari pengalaman, AI yang dipakai juga telah ditanam instruksi yang memaksa mereka ikut ke aturan lomba JCC Yang telah disematkan di postingan web JCC maaf mungkin bila kami tak menyadari celah instruksi yang membuat AI dan saya melanggar ,
terimakasih panitia serta penyelenggara lomba.

-Tim Proxy SMAN 1 Mojokerto

Terima kasih.