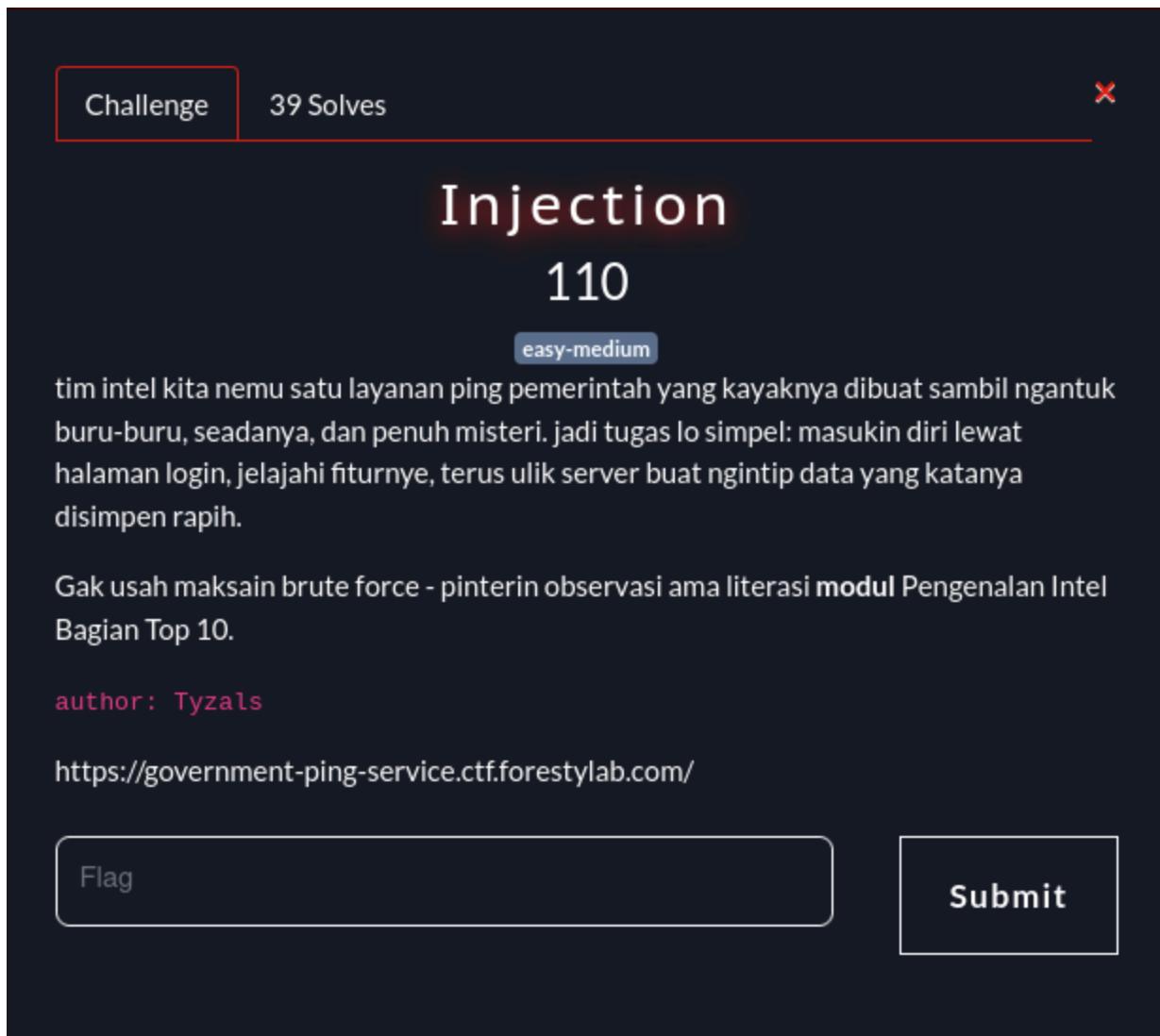


# Injection

Player: Constantine

Category: Web Exploitation



A challenge card for the 'Injection' challenge. At the top left is a button labeled 'Challenge'. To its right is the text '39 Solves'. In the top right corner is a red 'X' icon. Below these, the challenge title 'Injection' is displayed in large white letters, followed by its value '110'. Underneath the value is a blue rectangular button labeled 'easy-medium'. The challenge description is written in Indonesian: 'tim intel kita nemu satu layanan ping pemerintah yang kayaknya dibuat sambil ngantuk buru-buru, seadanya, dan penuh misteri. jadi tugas lo simpel: masukin diri lewat halaman login, jelajahi fiturnya, terus ulik server buat ngintip data yang katanya disimpan rapih.' Below the description, there is a note: 'Gak usah maksain brute force - pinterin observasi ama literasi modul Pengenalan Intel Bagian Top 10.' At the bottom left is a button labeled 'Flag', and at the bottom right is a button labeled 'Submit'.

## Konteks Dikit

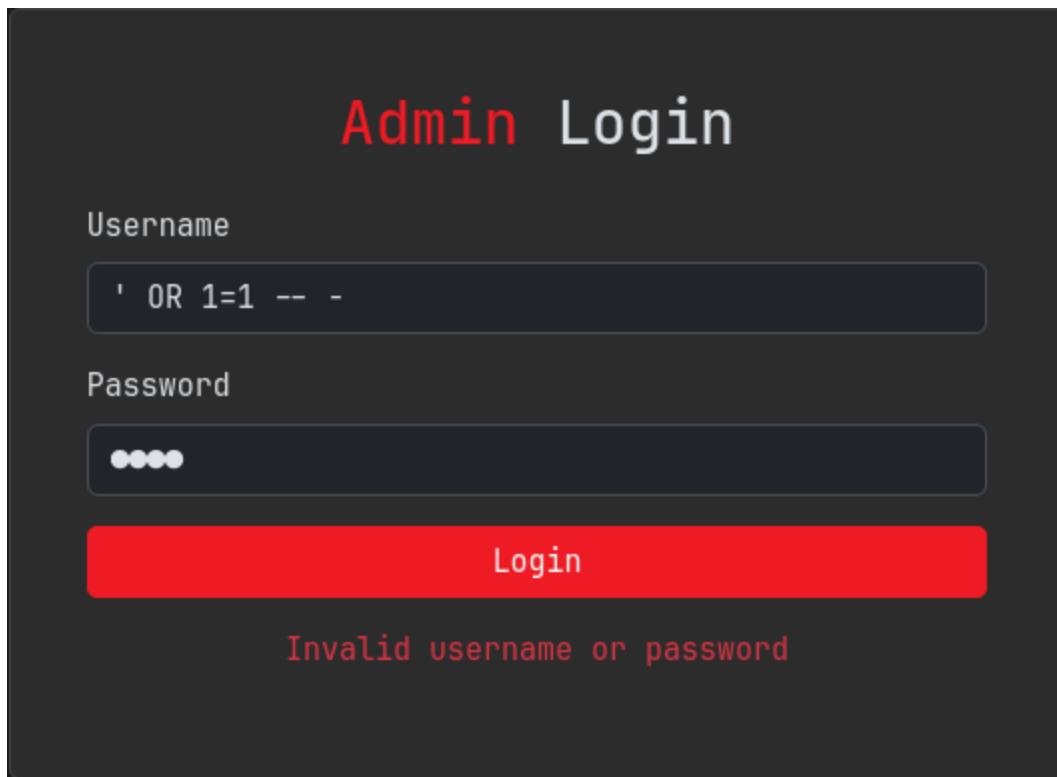
Sebuah layanan ping pemerintah, kita disuguhinya halaman login admin standar. Tugas kita masuk, cari celah, dapatin flag aja.

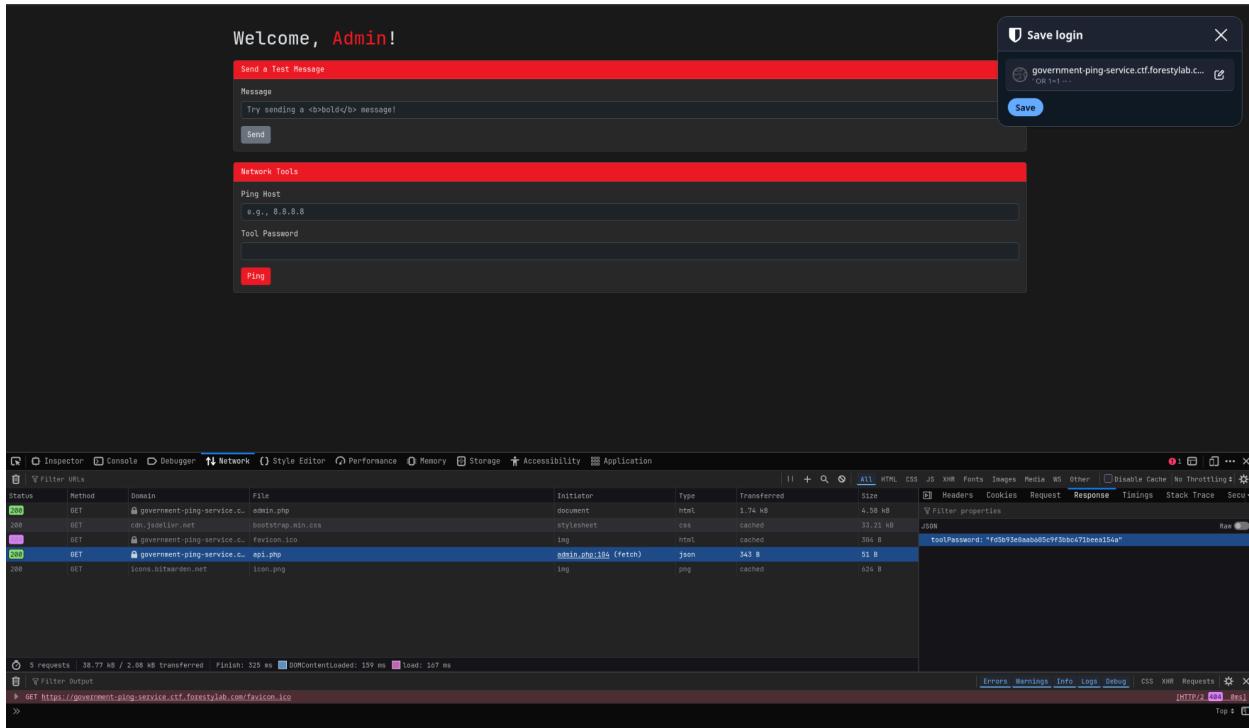
## Phase 1: Initial Access (SQL Injection)

Saat pertama kali buka challenge, kita langsung dihadang halaman login. Coba kredensial default admin:admin gabisa. Teringat obrolan sama si Amor beberapa minggu lalu soal cara bypass autentikasi tanpa harus bruteforce yang makan waktu, aku langsung coba SQL Injection.

**Payload:**

```
' OR 1=1 -- -
```

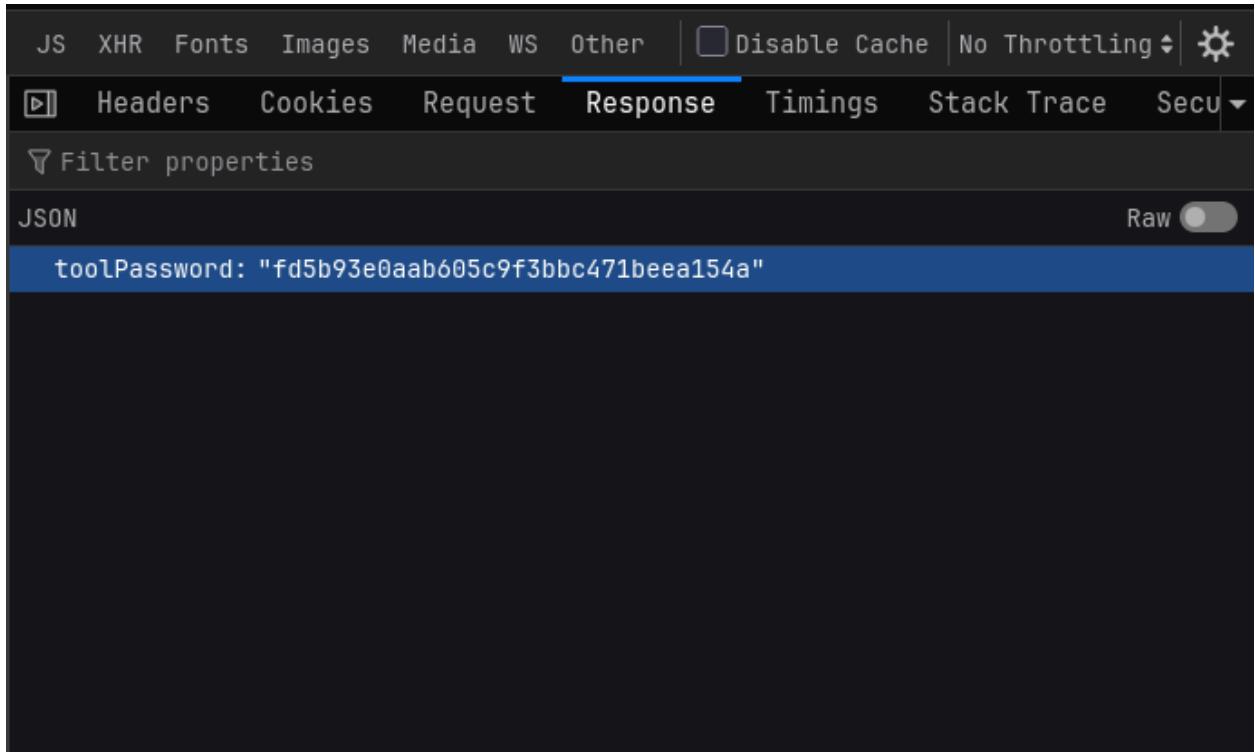




Boom. Masuk. Kita sekarang berada di dashboard Admin.

## Phase 2: Recon & Information Disclosure

Di dalam dashboard, ada fitur Network Tools untuk melakukan Ping. Masalahnya, fitur ini dikunci dengan "Tool Password". Daripada nebak-nebak, langsung aja pakai DevTool dan pindah ke tab Network. Refresh aja halaman untuk melihat bagaimana traffic bekerja. Ternyata, ada request menarik ke endpoint api.php.



Di bagian Response, server mengirimkan password dalam format JSON text:

```
toolPassword: "fd5b93e0aab605c9f3bbc471beea154a"
```

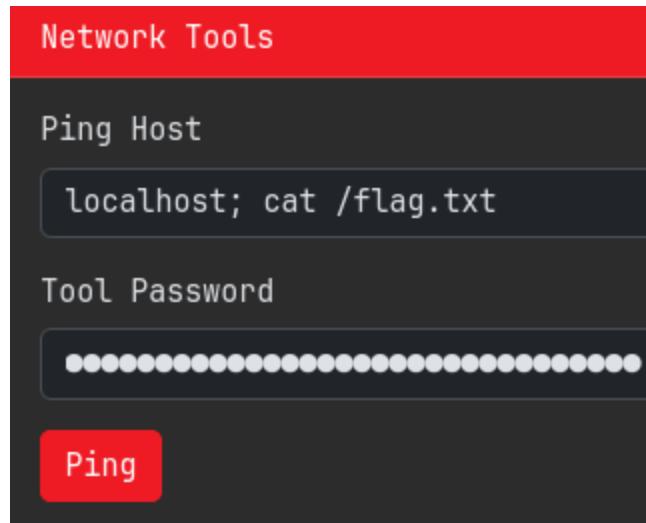
---

### Phase 3: Execution (OS Command Injection)

Sekarang kita punya akses ke fitur Ping. Kita bisa coba menyuntikkan perintah OS lain menggunakan separator seperti ;, |, atau &&. Aku coba payload untuk memverifikasi RCE sekaligus membaca file flag.

**Payload:**

```
localhost; cat /flag.txt
```



Server menjalankan ping localhost, lalu lanjut menjalankan cat /flag.txt. Output langsung muncul di layar.

---

#### Phase 4: Flag



Flag:

**FORESTY{sqlิ\_xss(just\_see\_net-traffic&localStorage)\_command\_injection\_is\_EASY}**