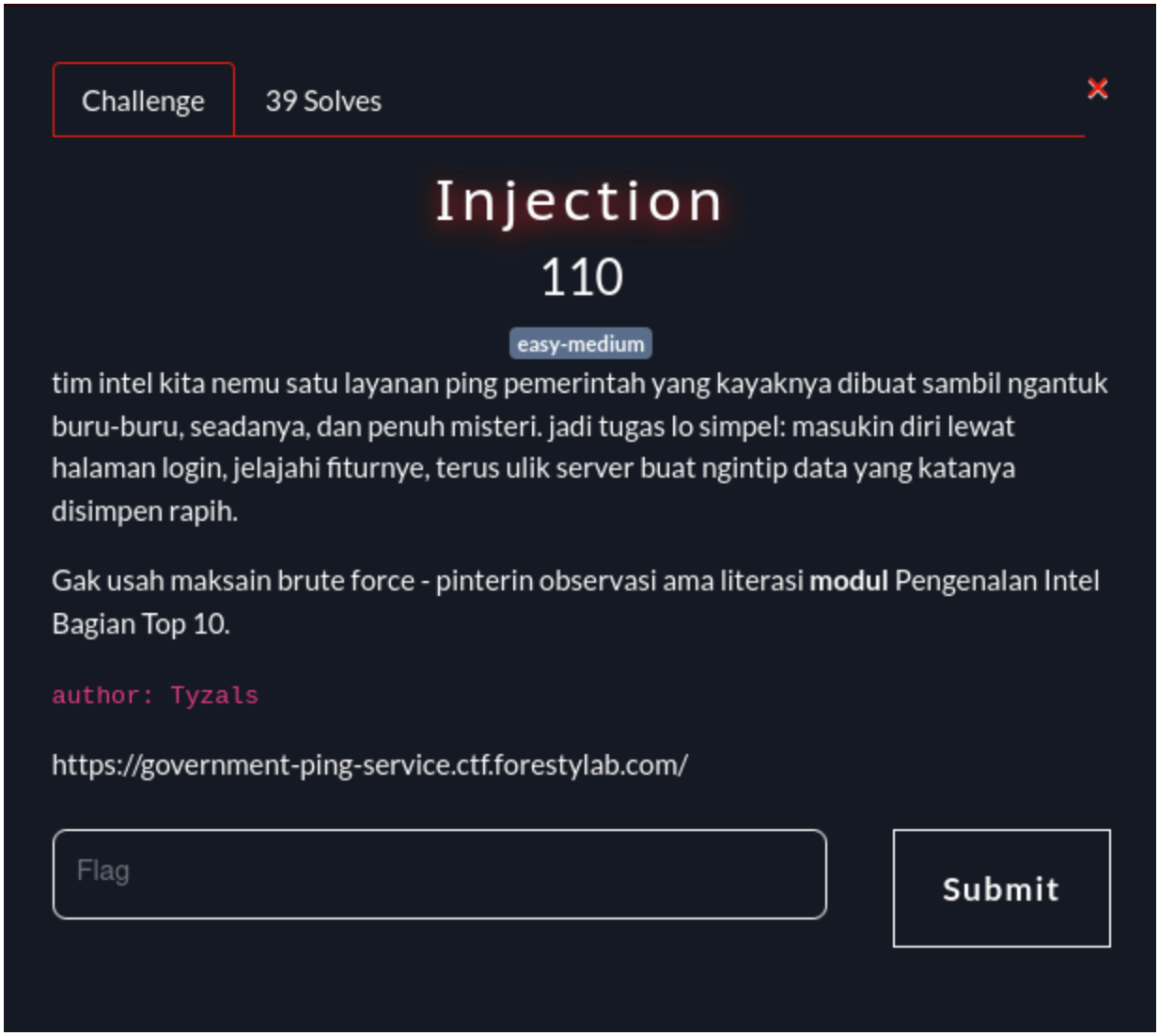
Injection

Player: Constantine
Category: Web Exploitation



Konteks Dikit

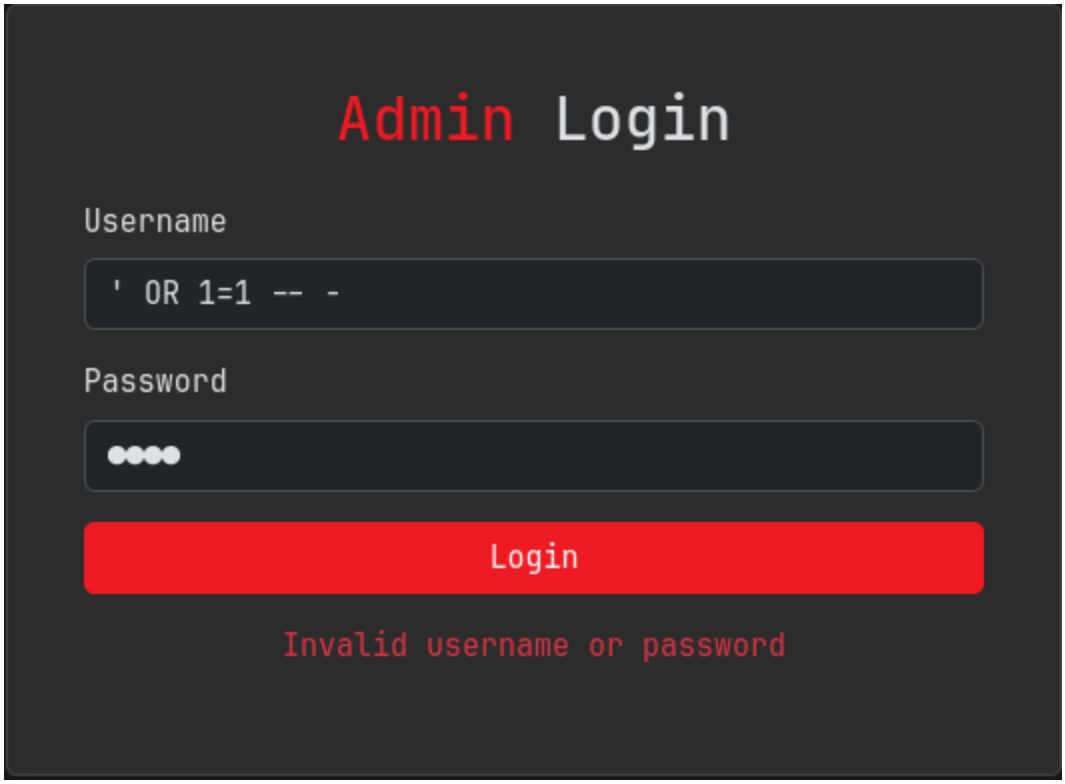
Sebuah layanan ping pemerintah, kita disuguhi halaman login admin standar. Tugas kita masuk, cari celah, dapatin flag aja.

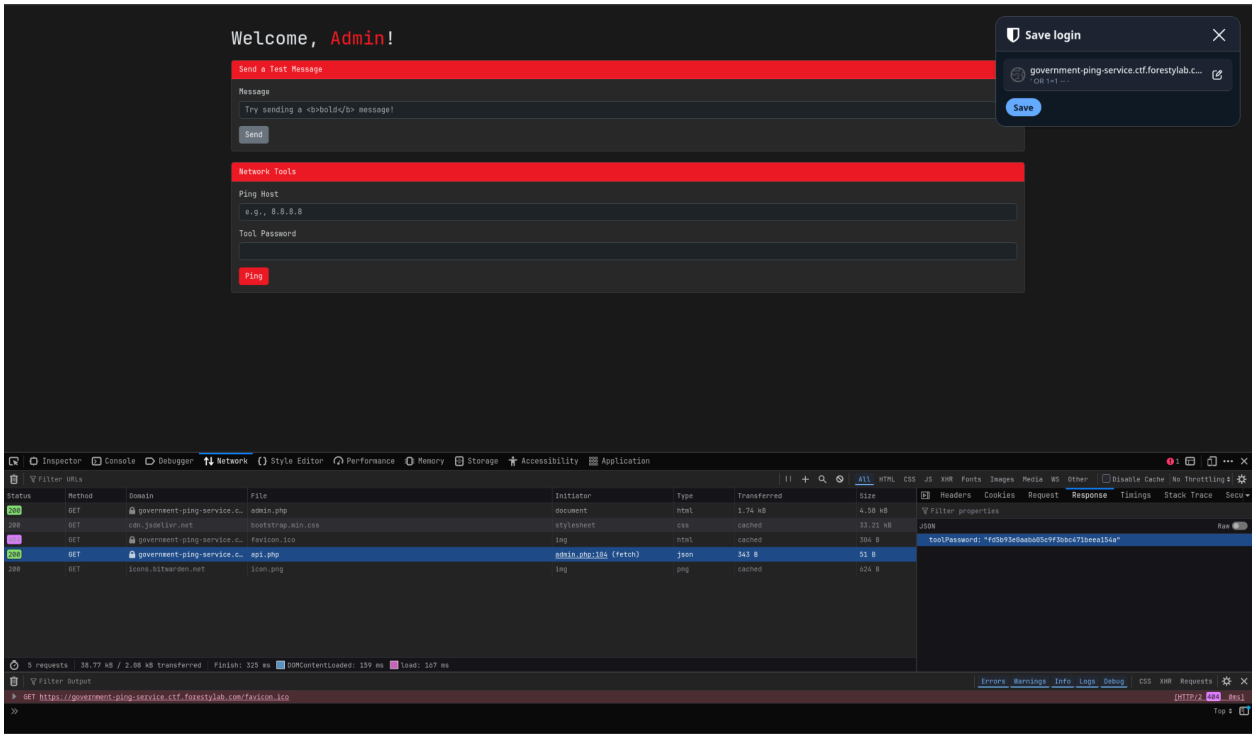
Phase 1: Initial Access (SQL Injection)

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 -- -
```

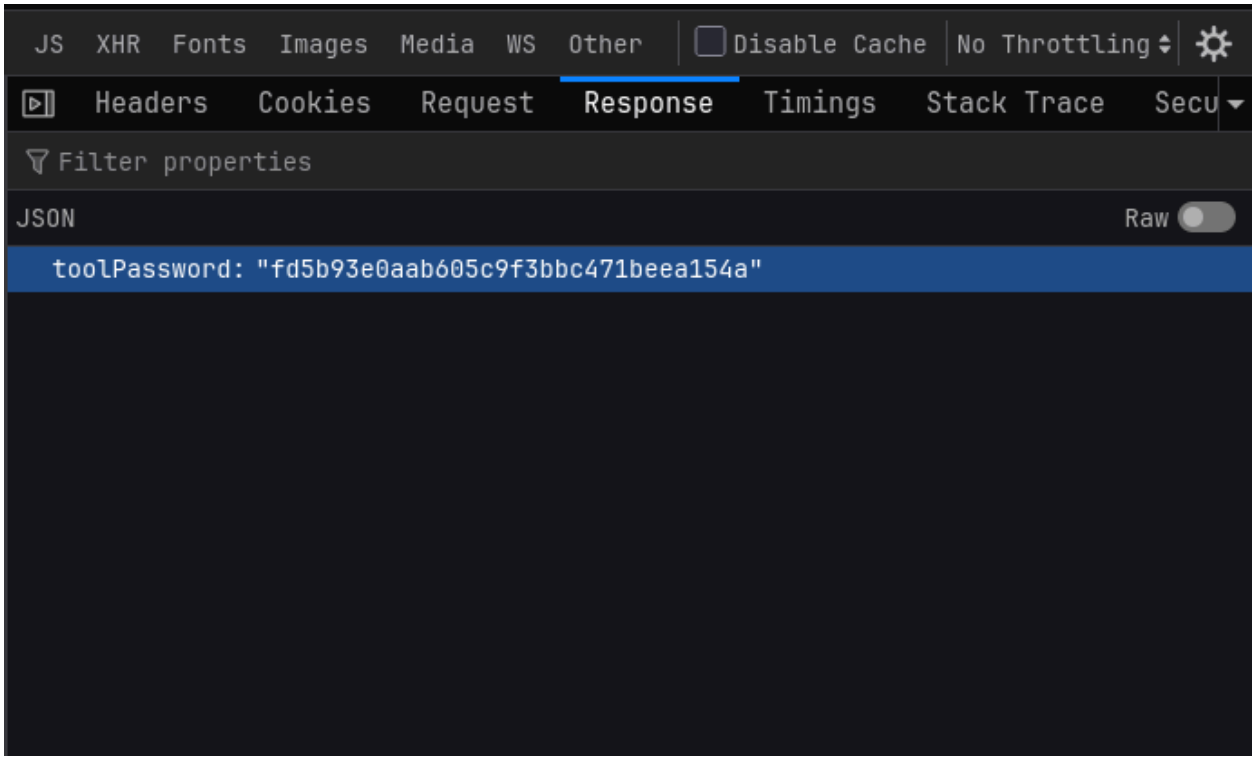




Boom. Masuk. Kita sekarang berada di dashboard Admin.

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:

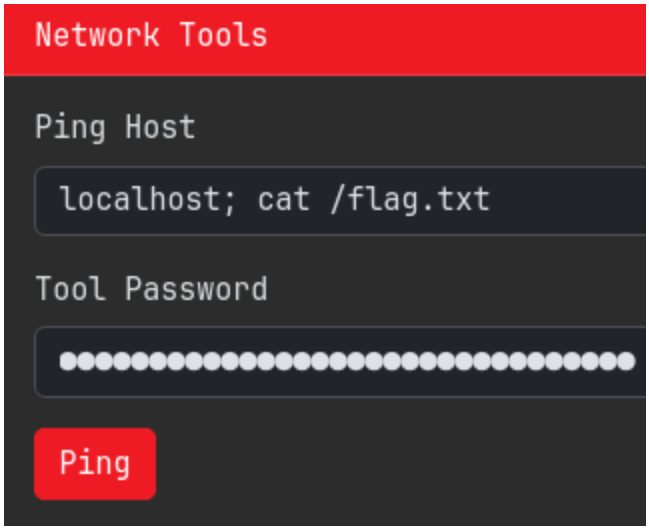
```
toolPassword: "fd5b93e0aab605c9f3bbc471beea154a"
```

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{sqli_xss(just_see_net-traffic&localstorage)_command_injection_is_EASY}