

Injection

Player: Constantine

Category: Web Exploitation

Challenge

39 Solves

✕

Injection

110

easy-medium

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 fitur nye, terus ulik server buat ngintip data yang katanya disimpen rapih.

Gak usah maksain brute force - pinterin observasi ama literasi **modul** Pengenalan Intel Bagian Top 10.

author: Tyzals

<https://government-ping-service.ctf.forestylab.com/>

Flag

Submit

Konteks Dikit

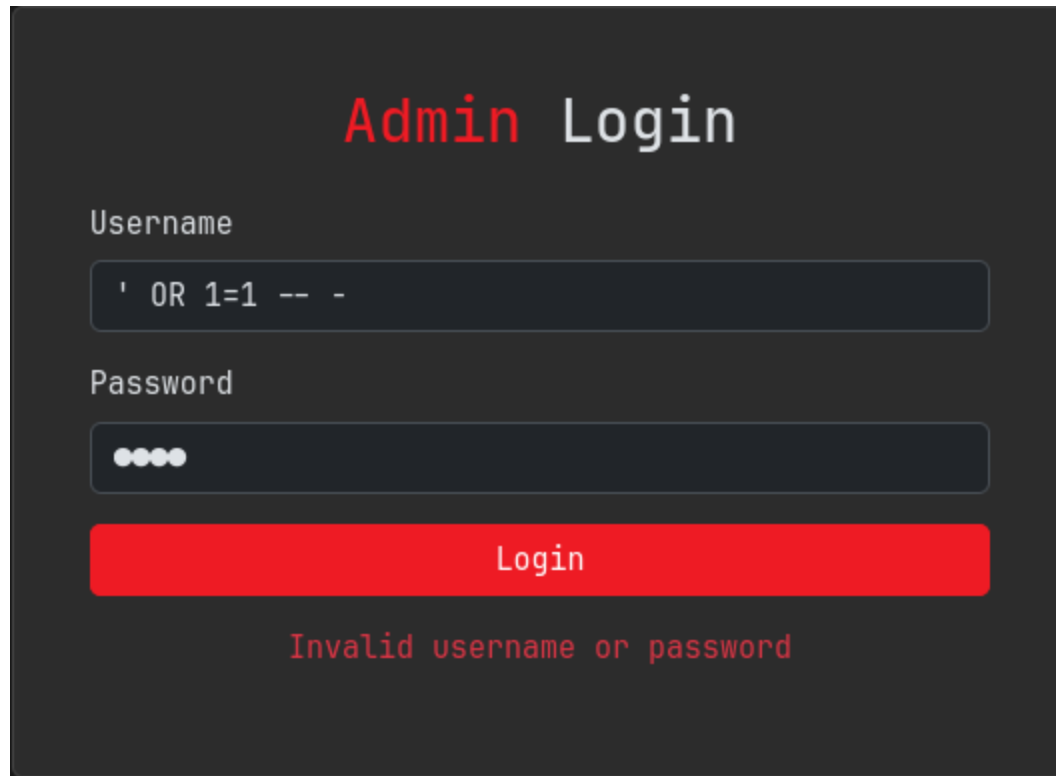
Sebuah layanan ping pemerintah, kita disuguhi halaman login admin standar. Tugas kita masuk, cari celah, dapatin flag aja.

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 -- -
```



The image shows a dark-themed login interface titled "Admin Login" in red and white text. It features two input fields: "Username" and "Password". The "Username" field contains the payload `' OR 1=1 -- -`. The "Password" field is masked with four white dots. Below the fields is a red "Login" button. At the bottom, a red error message reads "Invalid username or password".

Admin Login

Username

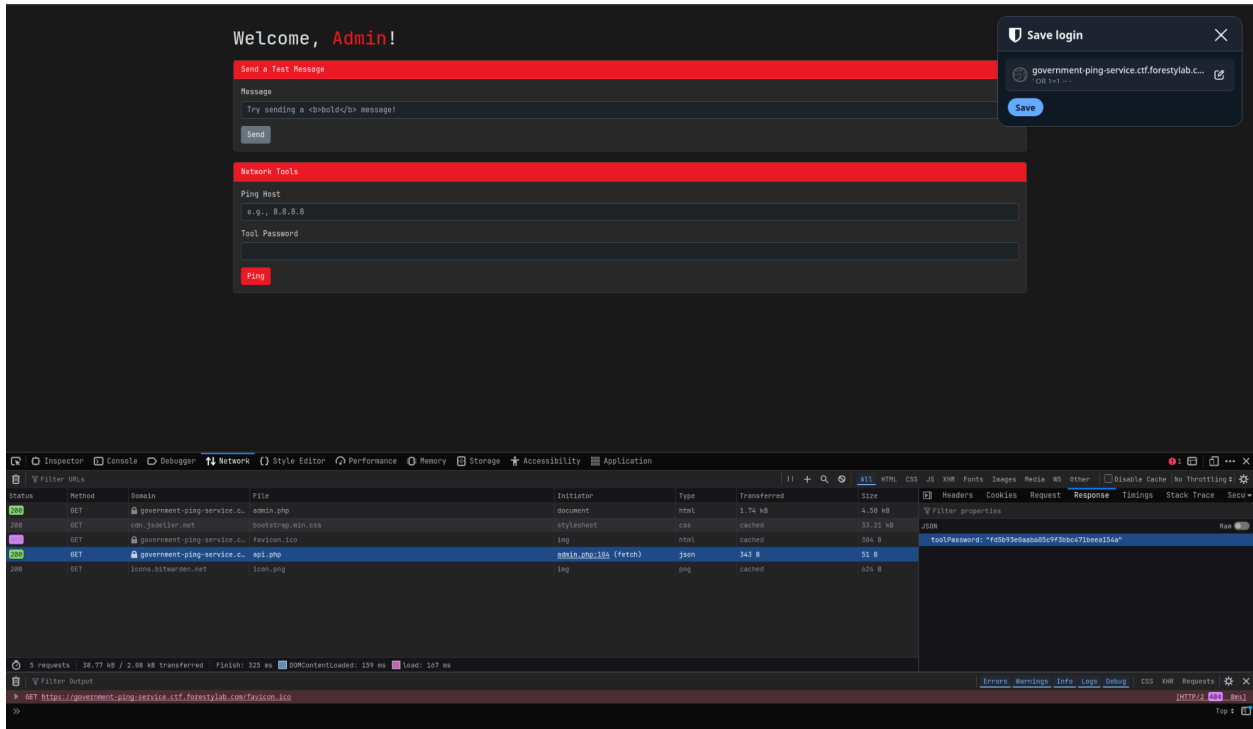
`' OR 1=1 -- -`

Password

••••

Login

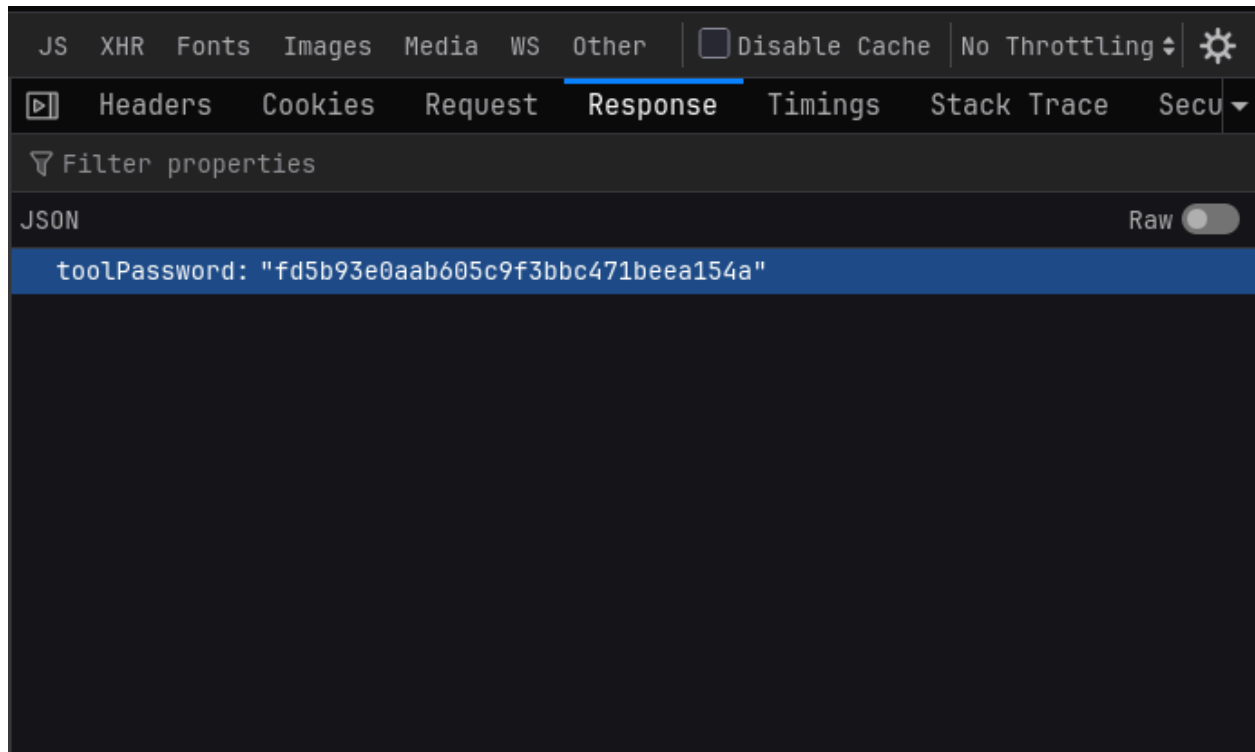
Invalid username or password



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
```

Network Tools

Ping Host

localhost; cat /flag.txt

Tool Password

Ping

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

Phase 4: Flag

Network Tools

Ping Host

e.g., 8.8.8.8

Tool Password

Ping

Output:

FORESTY{sql_i_xss(just_see_net-traffic&localstorage)_command_injection_is_EASY}

Flag:

FORESTY{sql_i_xss(just_see_net-traffic&localstorage)_command_injection_is_EASY}