

Injection

Player: constantine

Kategori: Web Exploitation

Challenge 39 Solves X

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 fiturnya, terus ulik server buat ngintip data yang katanya disimpan rapih.

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

author: Tyzals

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

Flag Submit

Phase 1: Initial Access (SQL Injection)

Kita langsung bertemu halaman login.

Admin Login

Username

Password

Login

Login `admin:admin` tidak berhasil. Daripada menebak password, kita coba pendekatan *authentication bypass* dengan SQL Injection pada field username.

Payload yang kita gunakan:

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

Welcome, Admin!

Logout

Send a Test Message

Message

Try sending a **bold** message!

Send

Network Tools

Ping Host

e.g., 8.8.8.8

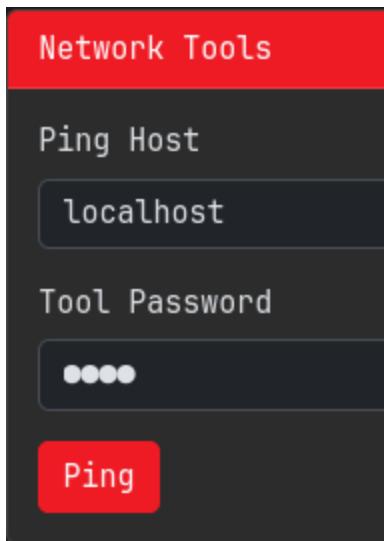
Tool Password

Ping

Server tidak melakukan sanitasi input. Payload tersebut membuat query SQL selalu bernilai true → kita masuk sebagai admin.

Phase 2: Recon & Information Disclosure

Setelah berhasil masuk, dashboard menampilkan menu *Network Tools*, tetapi fitur ini terkunci oleh sebuah **Tool Password**.



Password tidak diberikan di UI, jadi kita membuka *Developer Tools* → *Network* untuk melihat request internal.

Saat merefresh halaman, kita menemukan request menuju:



Status	Method	Domain	File
200	GET	government-ping-service.c...	admin.php
200	GET	cdn.jsdelivr.net	bootstrap.min.css
200	GET	government-ping-service.c...	favicon.ico
200	GET	government-ping-service.c...	api.php

Ketika kita buka Responsenya, server mengirimkan password secara terang-terangan dalam JSON.

Begini responsenya:

```
toolPassword: "fd5b93e0aab605c9f3bbc471beea154a"
```

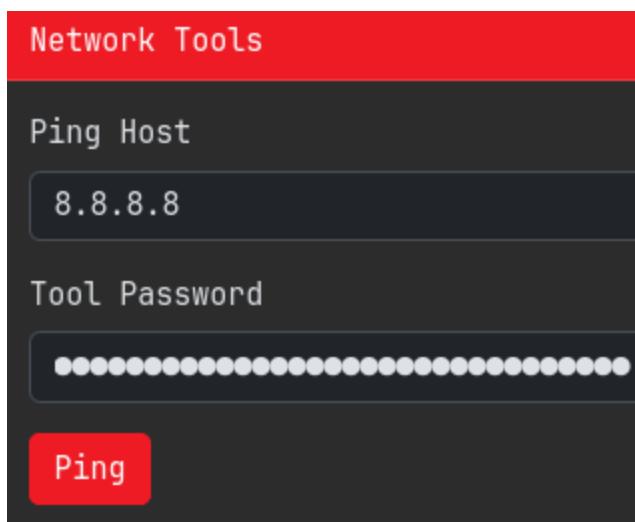


The screenshot shows the Network tab of a browser's developer tools. The Response section displays a JSON object with a single key-value pair: `toolPassword: "fd5b93e0aab605c9f3bbc471beea154a"`.

Ini murni *Information Disclosure*. Password sudah diberikan langsung oleh server.

Phase 3: Execution (OS Command Injection)

Setelah memasukkan password, fitur Ping dapat digunakan.



Kita uji dengan command injection sederhana menggunakan:

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

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}
```

ping localhost dieksekusi lebih dulu, lalu server mengeksekusi cat /flag.txt.

File flag muncul langsung di output menandakan RCE (*Remote Command Execution*) sepenuhnya bekerja.

Final Flag

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