

Injection

Player: constantine

Kategori: 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 fiturnya, 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

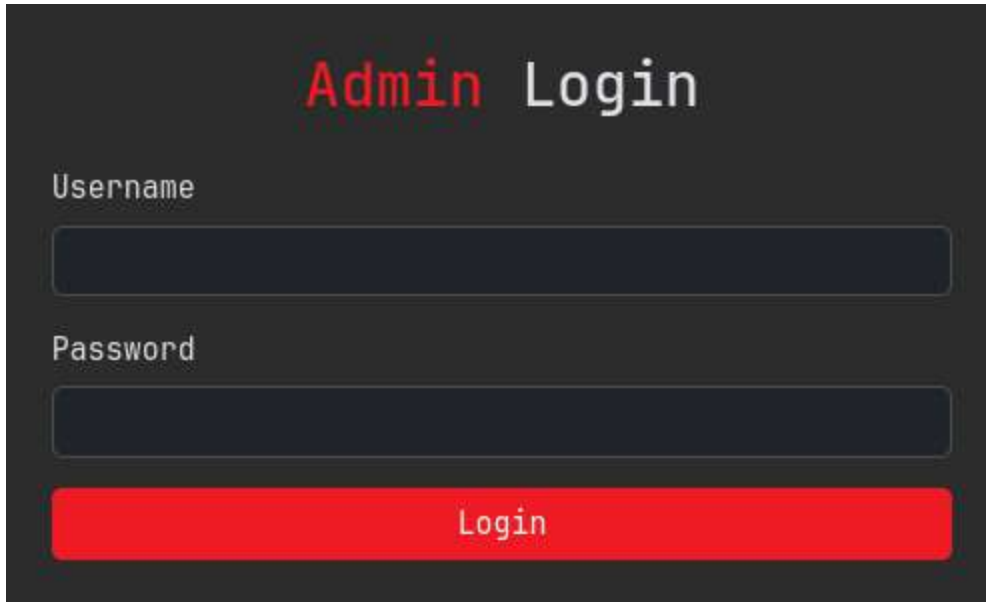
<https://government-ping-service.ctf.forestylab.com/>

Flag

Submit

Phase 1: Initial Access (SQL Injection)

Kita langsung bertemu halaman login.

A screenshot of a web application's login page. The title "Admin Login" is displayed in red and white text at the top. Below the title, there are two input fields: "Username" and "Password". The "Username" field is empty. The "Password" field is also empty. At the bottom of the form, there is a red button labeled "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 -- -
```

A screenshot of the admin dashboard after a successful login. The title "Welcome, Admin!" is displayed in red and white text at the top. In the top right corner, there is a "Logout" link. The dashboard is divided into two main sections: "Send a Test Message" and "Network Tools". The "Send a Test Message" section has a "Message" input field with the text "Try sending a bold message!" and a "Send" button. The "Network Tools" section has a "Ping Host" input field with the text "e.g., 8.8.8.8" and a "Tool Password" input field. At the bottom of the "Network Tools" section, there is a red button labeled "Ping".

Welcome, Admin! Logout

Send a Test Message

Message

Try sending a bold message!

Send

Network Tools

Ping Host

e.g., 8.8.8.8

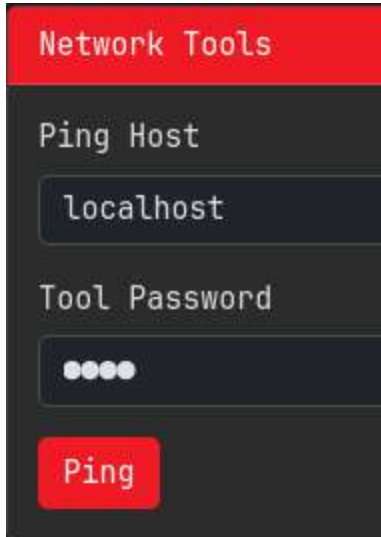
Tool Password

Ping

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

Phase 2: Recon & Information Disclosure

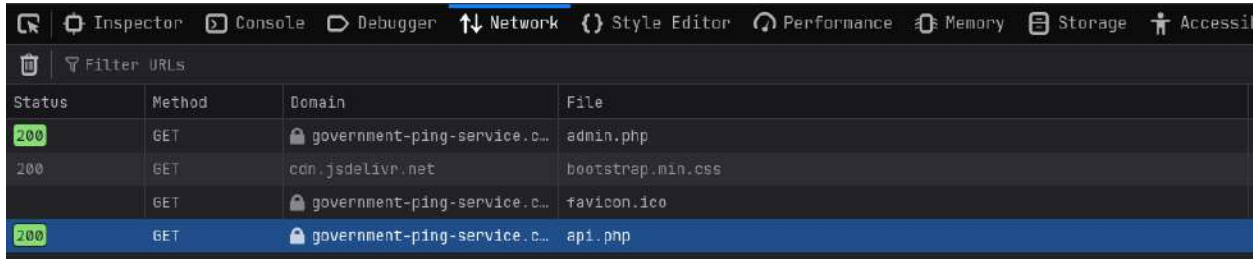
Setelah berhasil masuk, dashboard menampilkan menu *Network Tools*, tetapi fitur ini terkunci oleh sebuah **Tool Password**.



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

Saat merefresh halaman, kita menemukan request menuju:

```
api.php
```

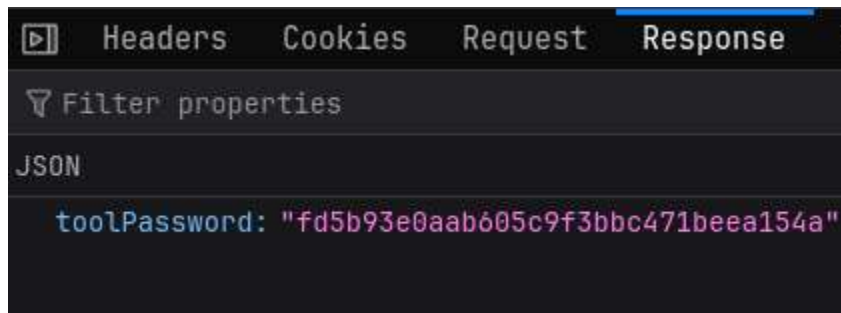


Status	Method	Domain	File
200	GET	government-ping-service.c...	admin.php
200	GET	cdn.jsdelivr.net	bootstrap.min.css
	GET	government-ping-service.c...	favicon.ico
200	GET	government-ping-service.c...	api.php

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

Begini responsenya:

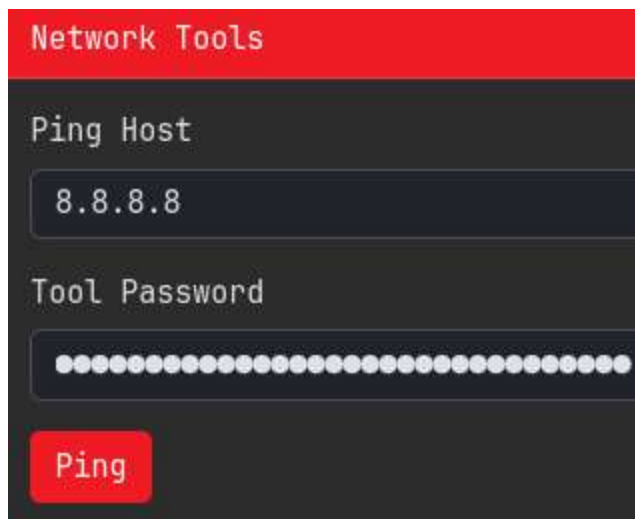
```
toolPassword: "fd5b93e0aab605c9f3bbc471beea154a"
```



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{sqli_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{sqli_xss(just_see_net-traffic&localstorage)_command_injection_is_EASY}