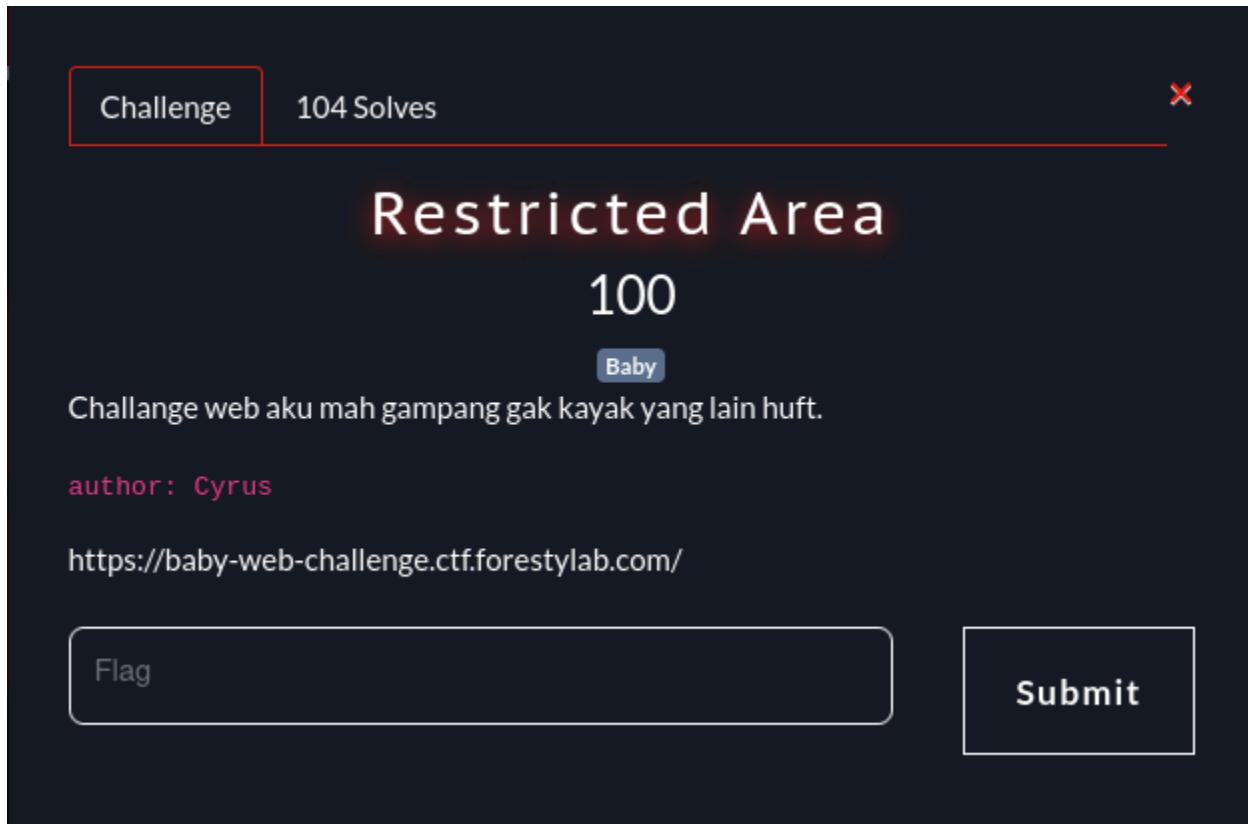


Write-up: Restricted Area

Player: Constantine

Kategori: Web Exploit

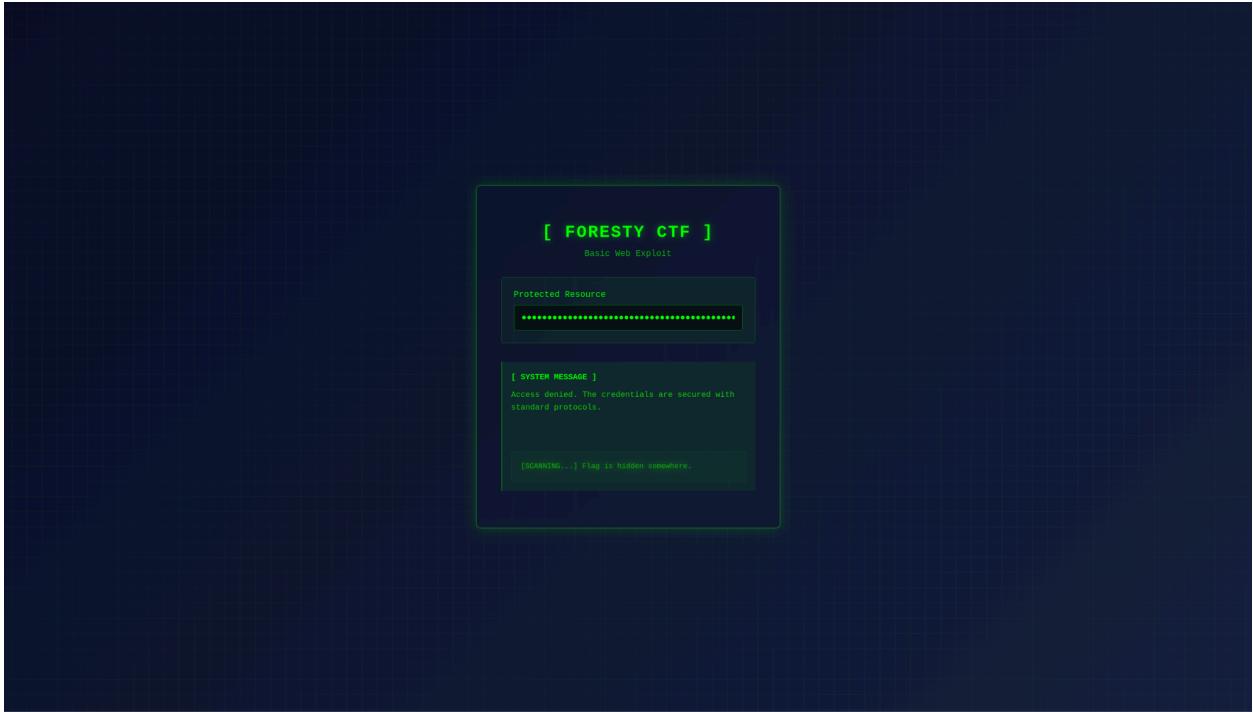


Konteks Dikit

Challenge ini nggak pakai exploit atau payload. Lihat source pagennya aja. Tugas kita cuma nemuin di mana flag tersebut disembunyikan.

Phase 1: Recon

Begitu halaman dibuka, tampilannya keliatan kaya gini:



Keliatan kayak bakal butuh brute-force atau bypass auth, tapi sebenarnya cukup CTRL+U aja

Phase 2: Source Code Analysis

Di dalam source, keliatan ada sebuah input field:

```
<input type="password"  
value="FORESTY{easy_web_exploit_lmao_next_challenge_please_cyrus}" placeholder="Enter  
credentials...">>
```

```
<div class="challenge-box">  
    <Label class="Label">Protected Resource</Label>  
    <input type="password"  
value="FORESTY{easy_web_exploit_lmao_next_challenge_please_cyrus}"  
placeholder="Enter credentials...>  
    </div>
```

Phase 3: Eksekusi

Nggak perlu submit form, nggak perlu bypass apa pun.
Flagnya sudah ada di depan mata.

Flag

FORESTY{easy_web_exploit_lmao_next_challenge_please_cyrus}