

ffuf -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.10.56/FUZZ/ -c

Tìm được điểm vào cgi-bin có trạng thái 403

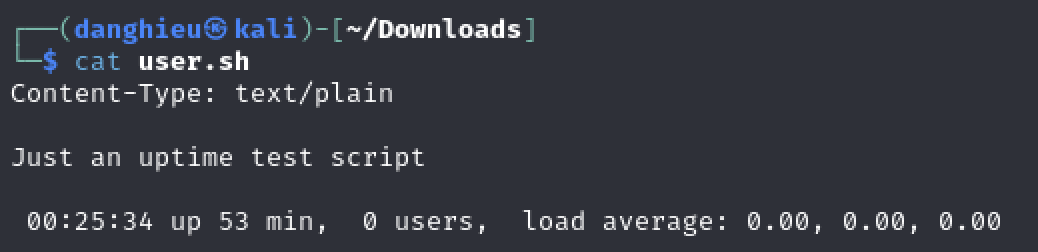
Common Gateway Interface (CGI) cung cấp phần mềm trung gian giữa máy chủ web với cơ sở dữ liệu và nguồn thông tin bên ngoài. Trong đó,

* Máy chủ đảm nhận quản lý các kết nối, việc thực hiện truyền dữ liệu đi và các vấn đề liên quan đến yêu cầu từ người dùng.
* CGI script chịu trách nhiệm xử lý các vấn đề của ứng dụng như truy cập vào dữ liệu và xử lý các tài liệu.

File Extension thường có trong thư mục cgi-bin là .cgi,.pl,.sh

ffuf -w /usr/share/wordlists/dirb/common.txt -u http://10.10.10.56/cgi-bin/FUZZ -c -e .cgi,.sh,.pl

Tìm được tập tin user.sh



Tên bài là shocker, có thư mục cgi-bin nên mình tìm thấy 1 cve tên Shellshocker mô tả lỗ hổng thực thi lệnh từ xa

