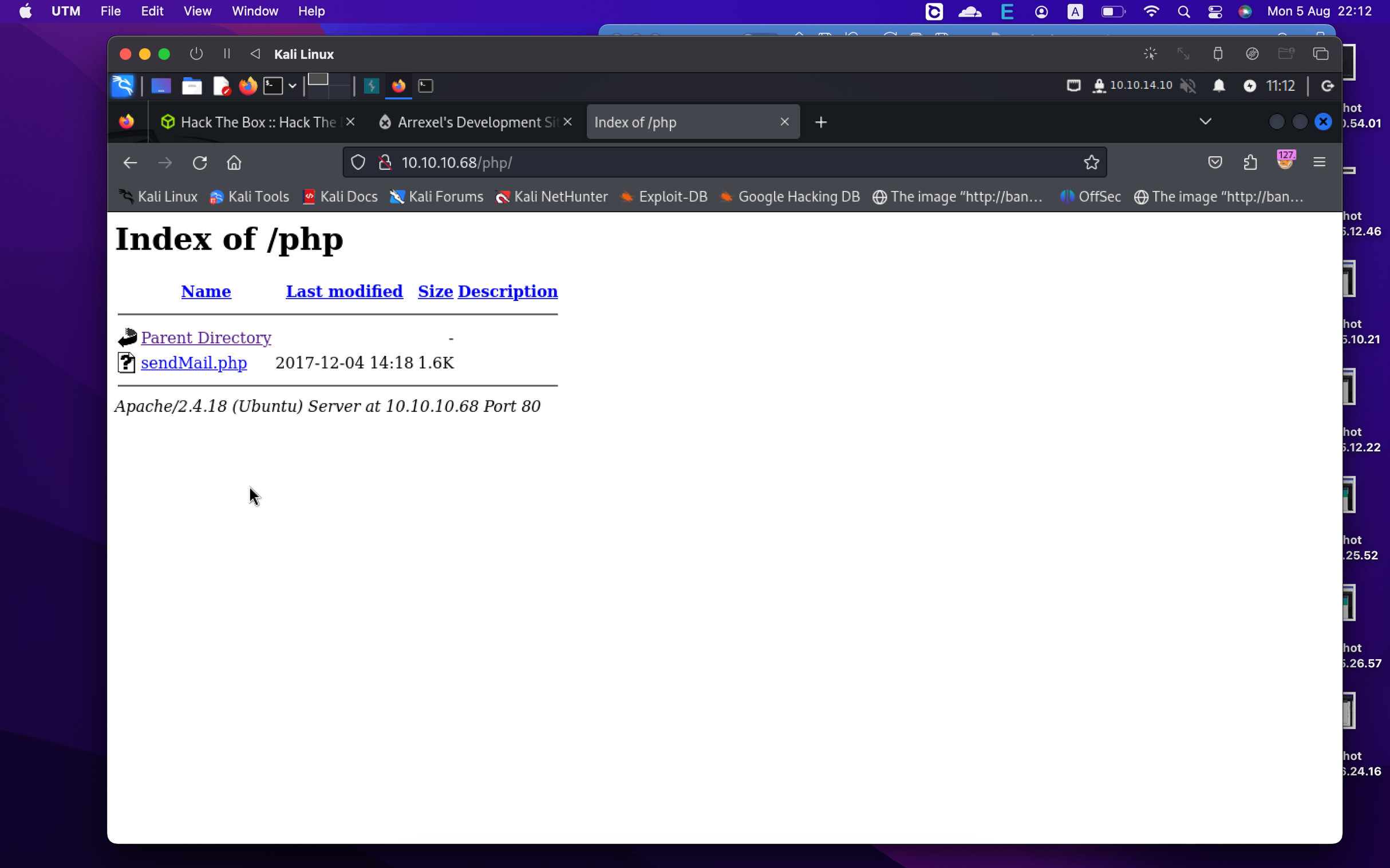


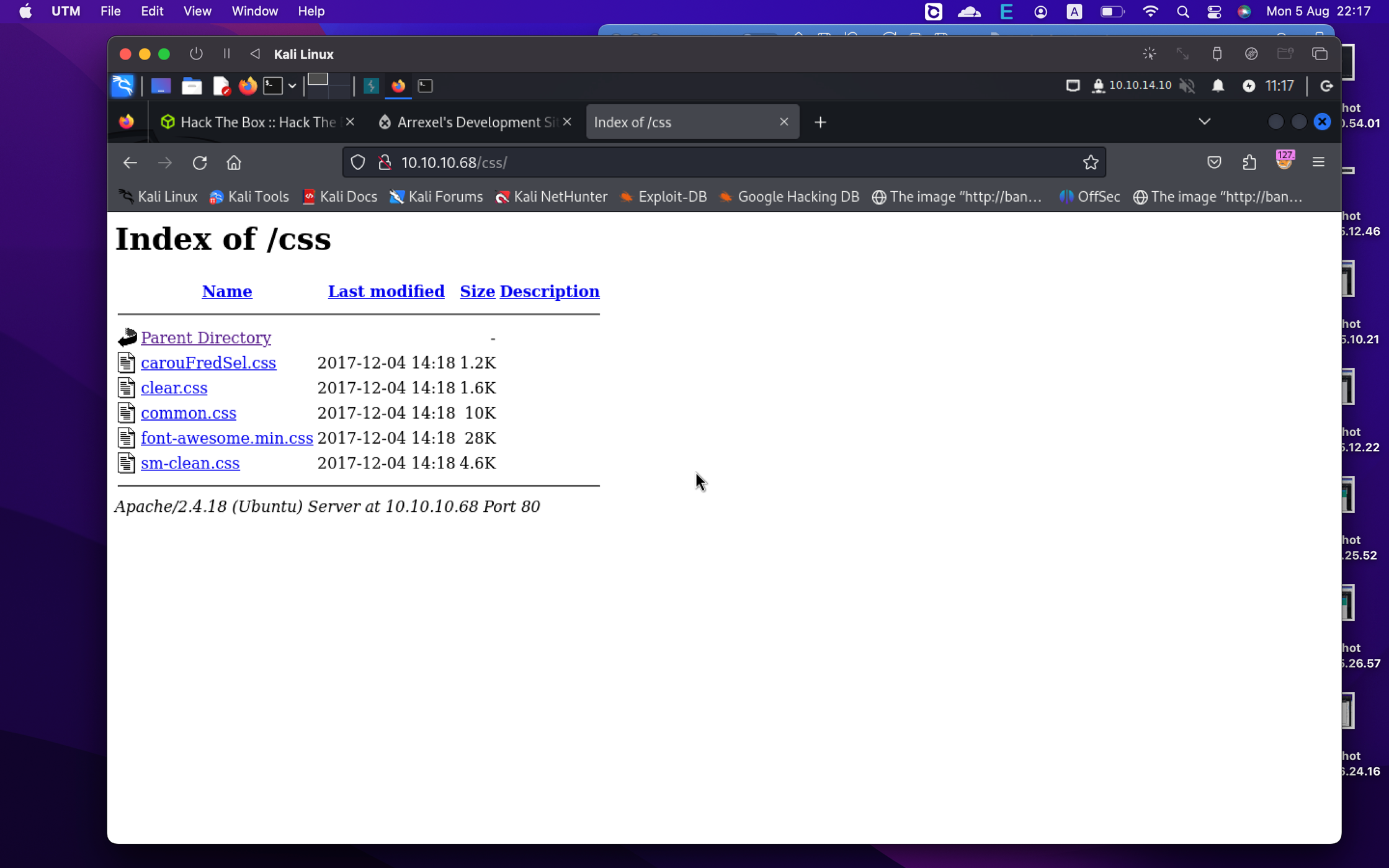
Tìm được tên người dùng arrexel

Tìm được điểm vào css,js,php,dev

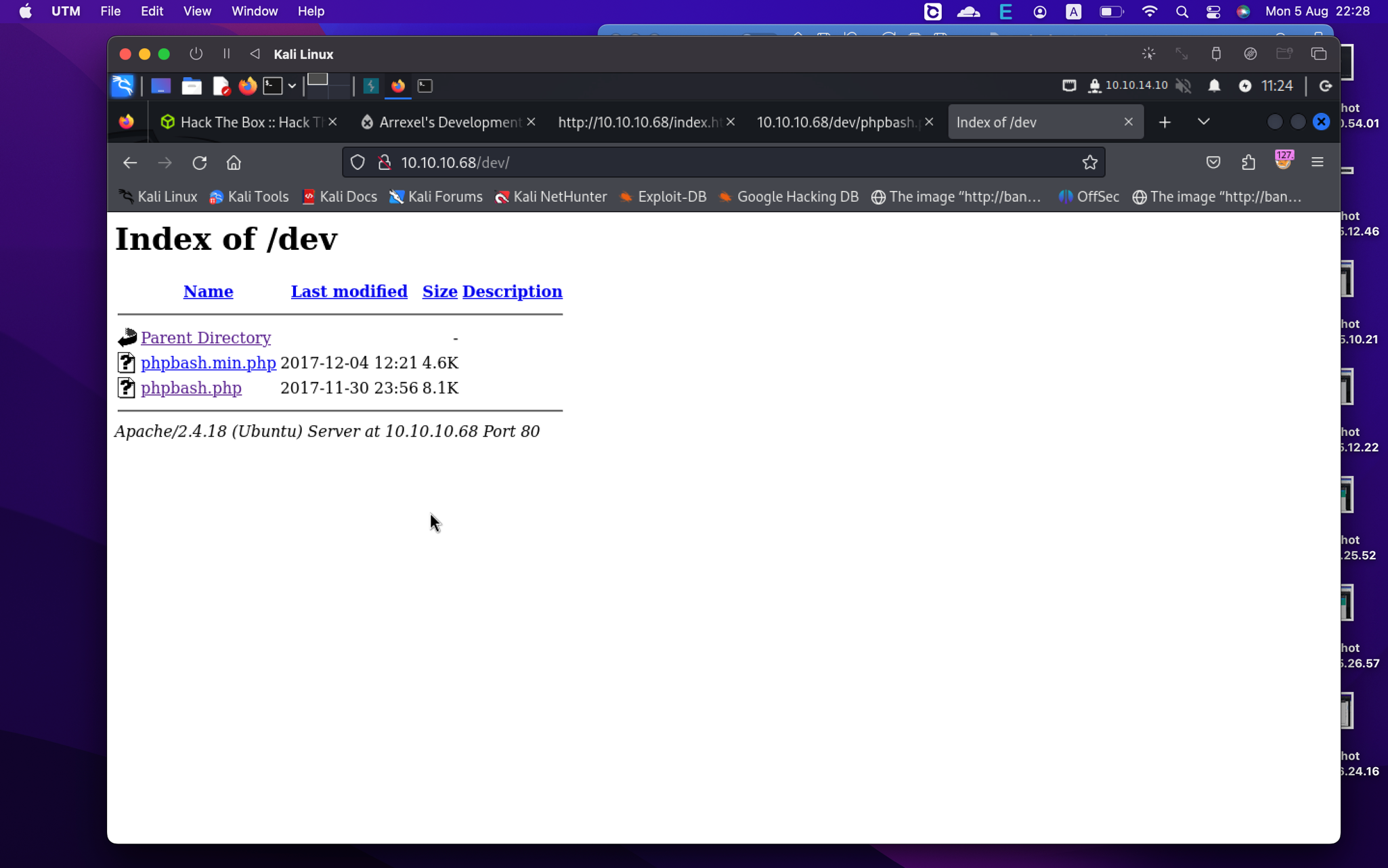
http://10.10.10.68/php



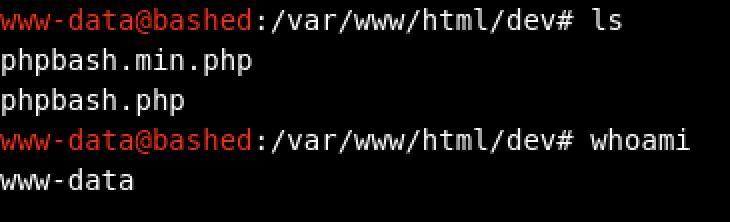
Trang web bị lỗi chỉ mục nên khi bạn vào thư mục nó hiện tất cả tập tin trong đó



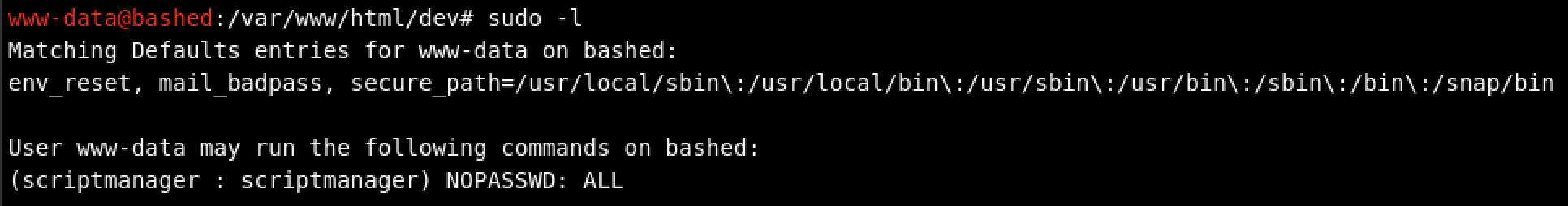
http://10.10.10.168/dev



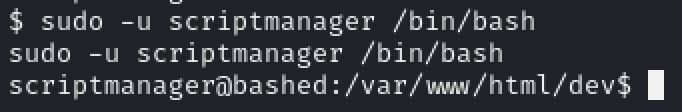
Bạn vào phpbash.php sẽ hiện ra web-based shell:





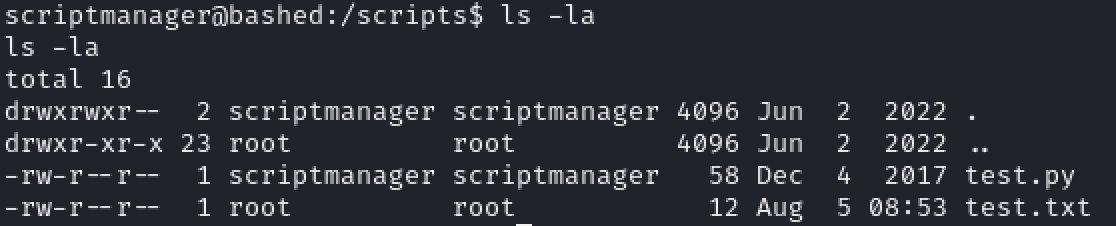


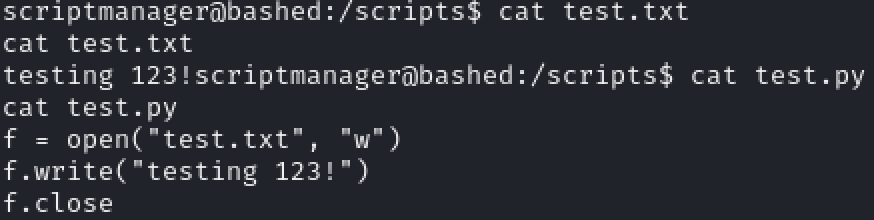
www-data có thể chạy bất cứ lệnh nào với đặc quyền của scriptmanager



Nếu bạn là scriptmanager, bạn có thể đọc thư mục /scripts

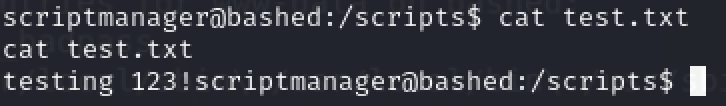






Tập lệnh test.py ghi “testing 123!” vào test.txt nhưng test.txt của root nên không ghi được

Nếu bạn kiểm tra test.txt sẽ thấy bất ngờ:



Nó vẫn ghi được, vậy rất có thể test.py đang chạy bởi root mỗi phút (giống như cronjob)

Mình chỉ cần sửa lại code test.py là có thể lấy shell của root dễ dàng: