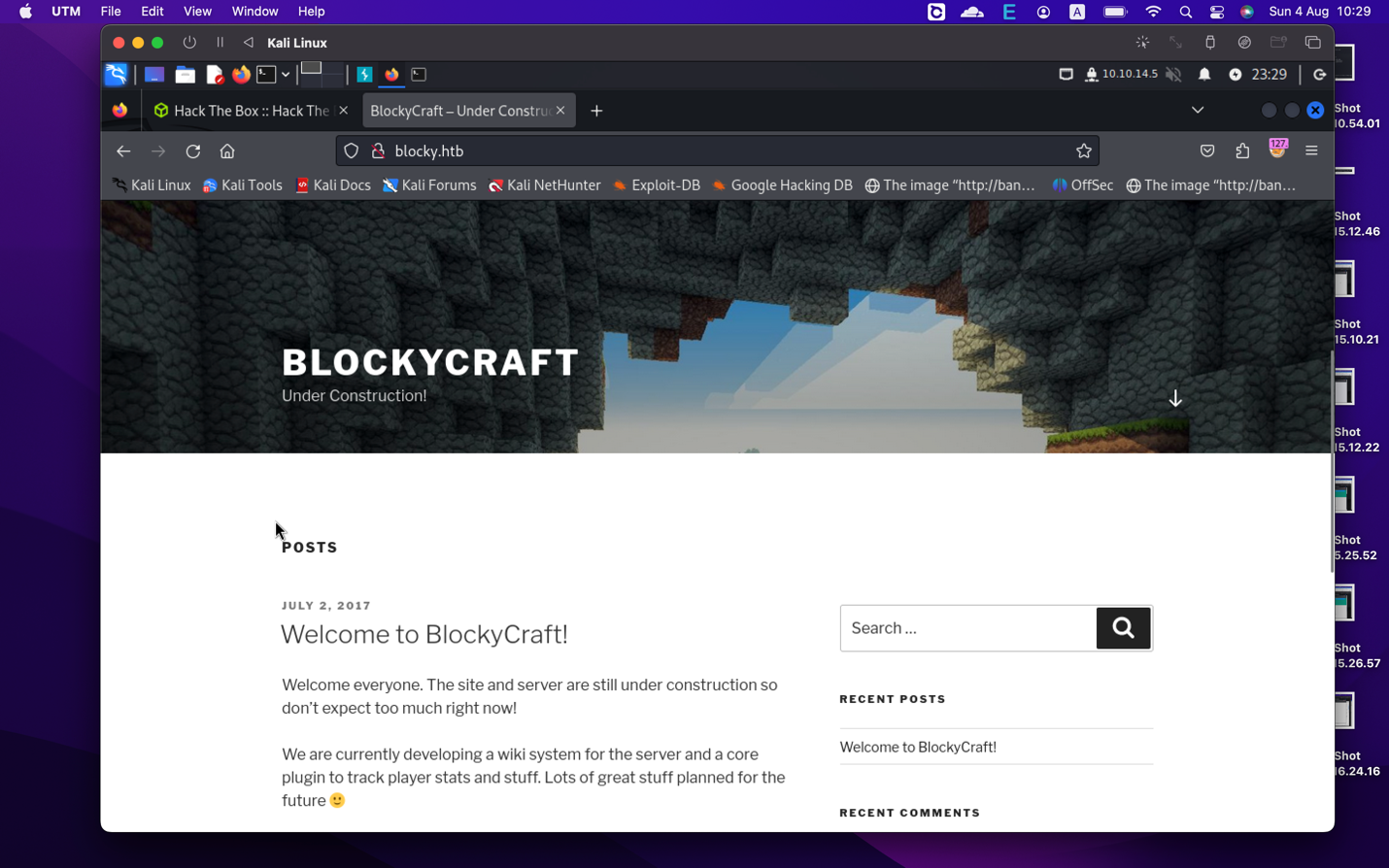


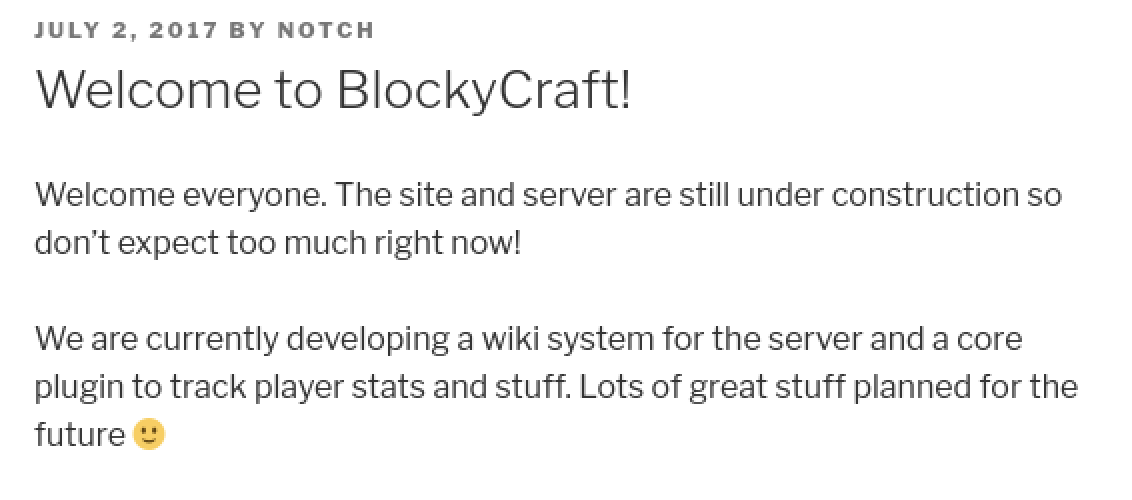
ProFTPD 1.3.5 nghe quen lắm, mình đã khai thác ở TryHackMe rồi



Giao diện trang web:



Có 1 bài viết của người dùng notch

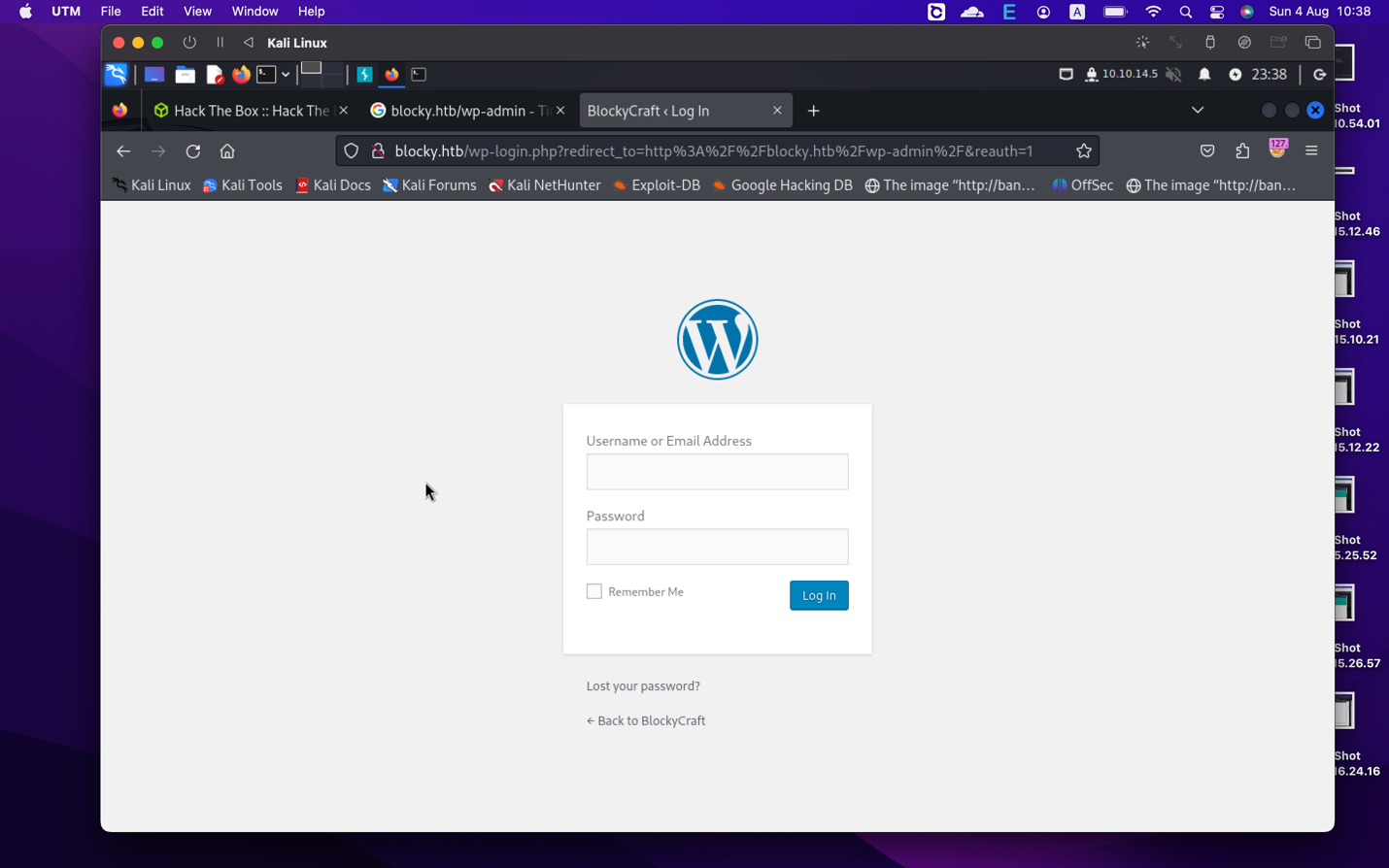


Tìm kiếm thư mục bị ẩn bằng ffuf:

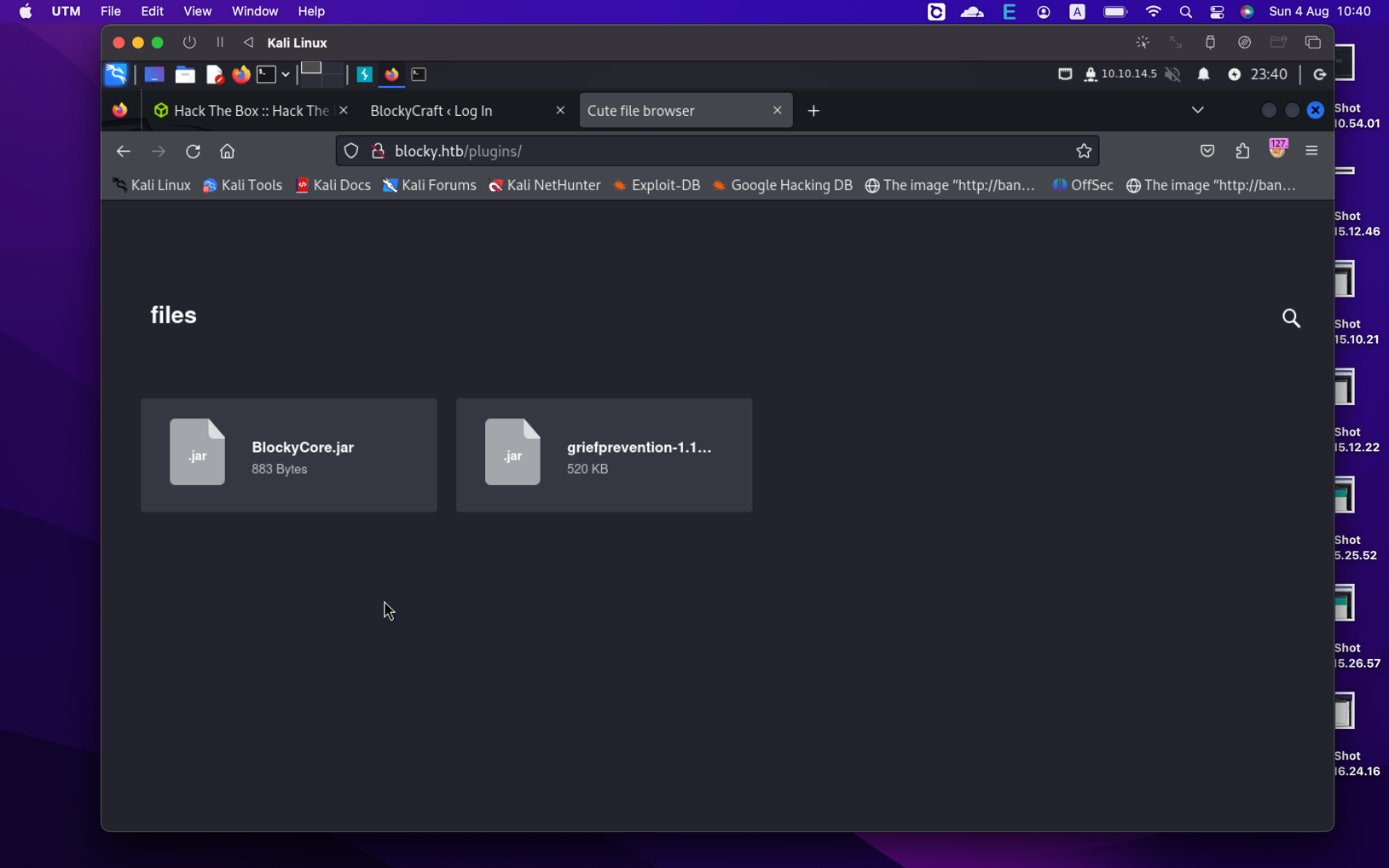
ffuf -w /usr/share/wordlists/dirbuster/directory-list-1.0.txt -u http://blocky.htb/FUZZ -c

Tìm được các điểm vào sau: wiki, plugins, wp-content, wp-admin

http://blocky.htb/wp-admin

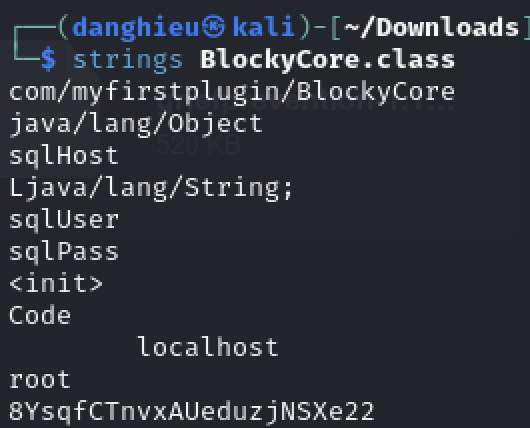


http://blocky.htb/plugins



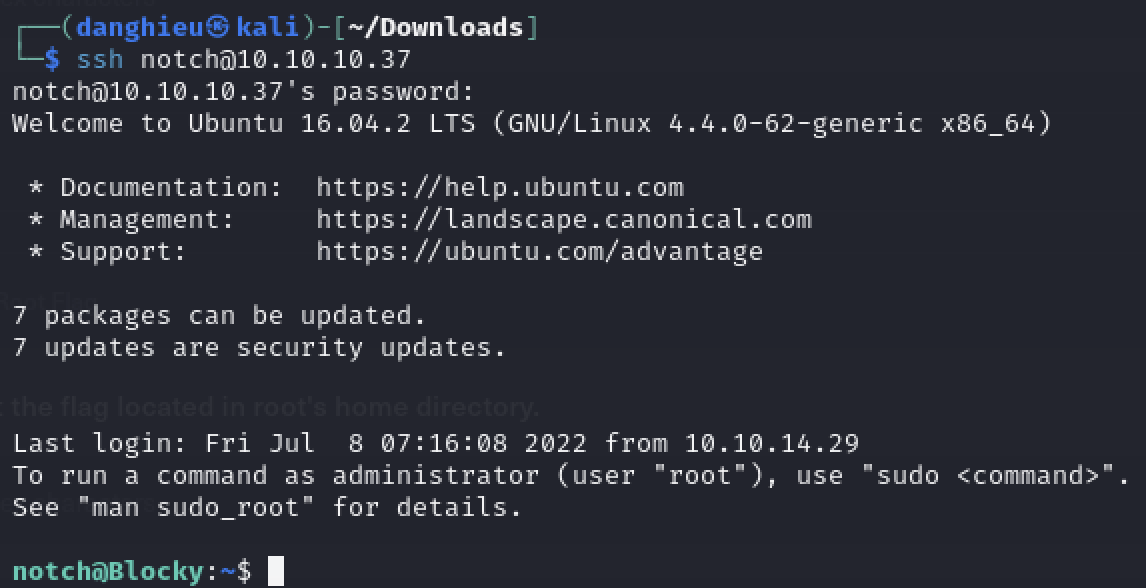
Trang plugins cho chúng ta 2 tệp .jar để tải về

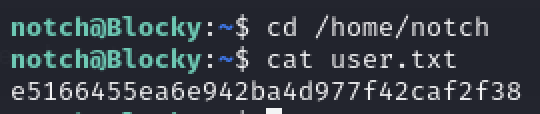
Giải nén Tập tin BlockyCore.jar để có BlockyCore.class



Không phải mật khẩu của root nha ☺

notch:8YsqfCTnvxAUeduzjNSXe22







Cú pháp: User <space> OnHost = (Runas-User:Group) <space> Commands

Ví dụ: root ALL = (ALL:ALL) ALL

Người dùng root có thể chạy bất cứ lệnh nào với đặc quyền của bất cứ người dùng nào thuộc bất kỳ nhóm nào

Trong trường hợp của chúng ta: người dùng notch có thể chạy bất cứ lệnh nào với đặc quyền của bất cứ người dùng nào thuộc bất kỳ nhóm nào

