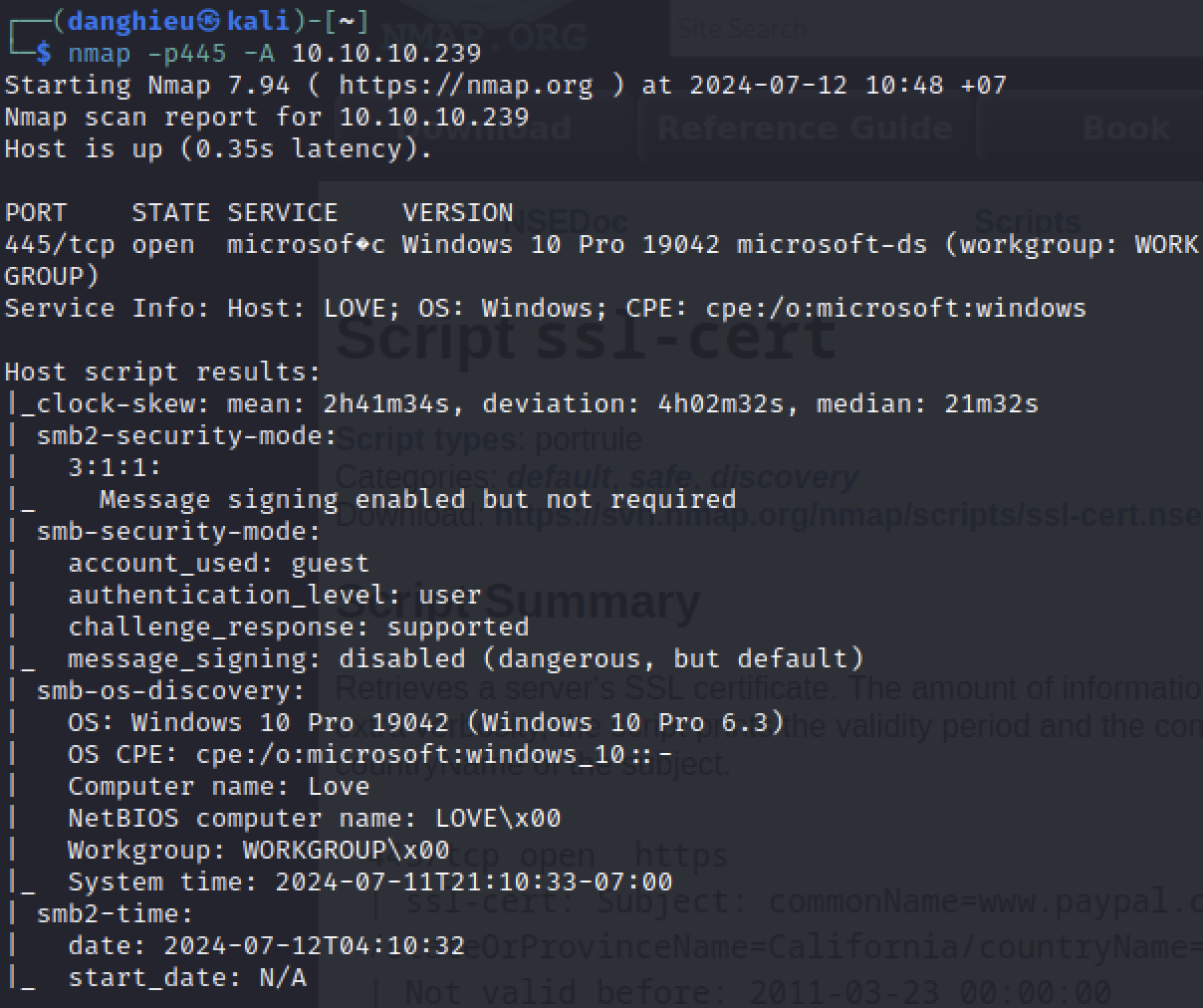


Có một dịch vụ chúng ta không nhận ra đang chạy trên cổng 5000.





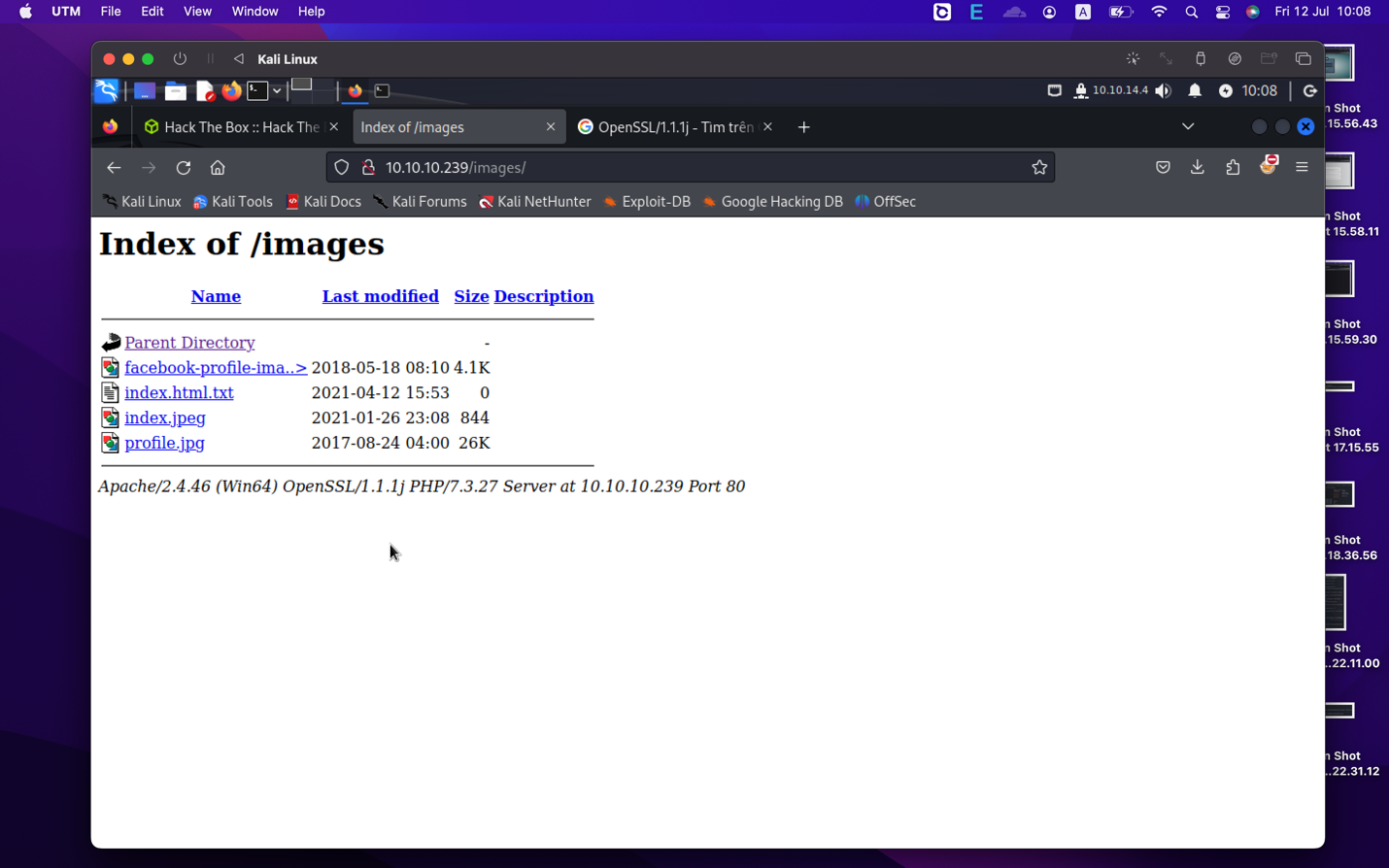
Hostname Love bị rò rỉ qua smb và chúng ta cũng tìm được staging.love.htb qua chứng chỉ SSL trên cổng 443.

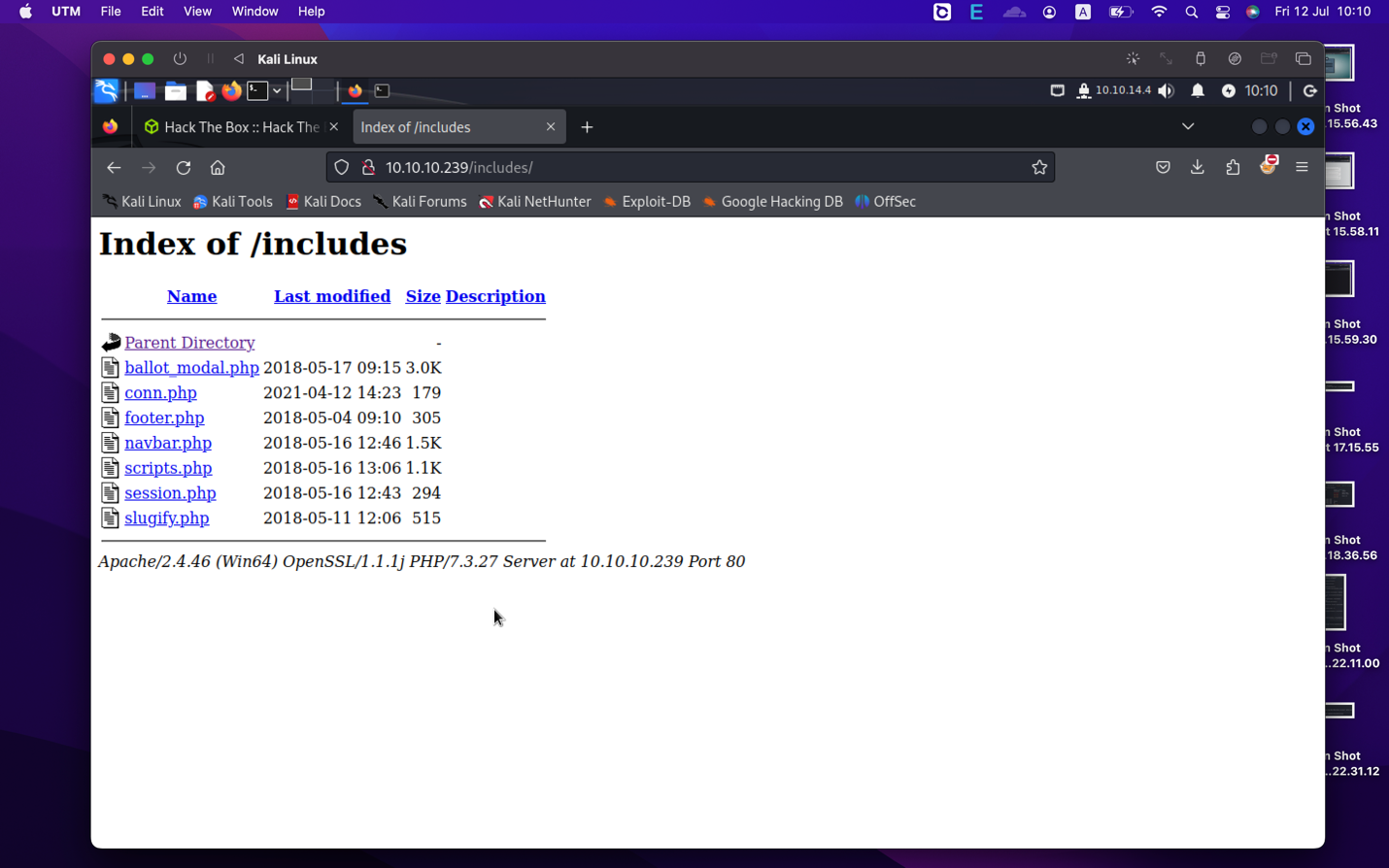
Thêm staging.love.htb vào /etc/hosts.

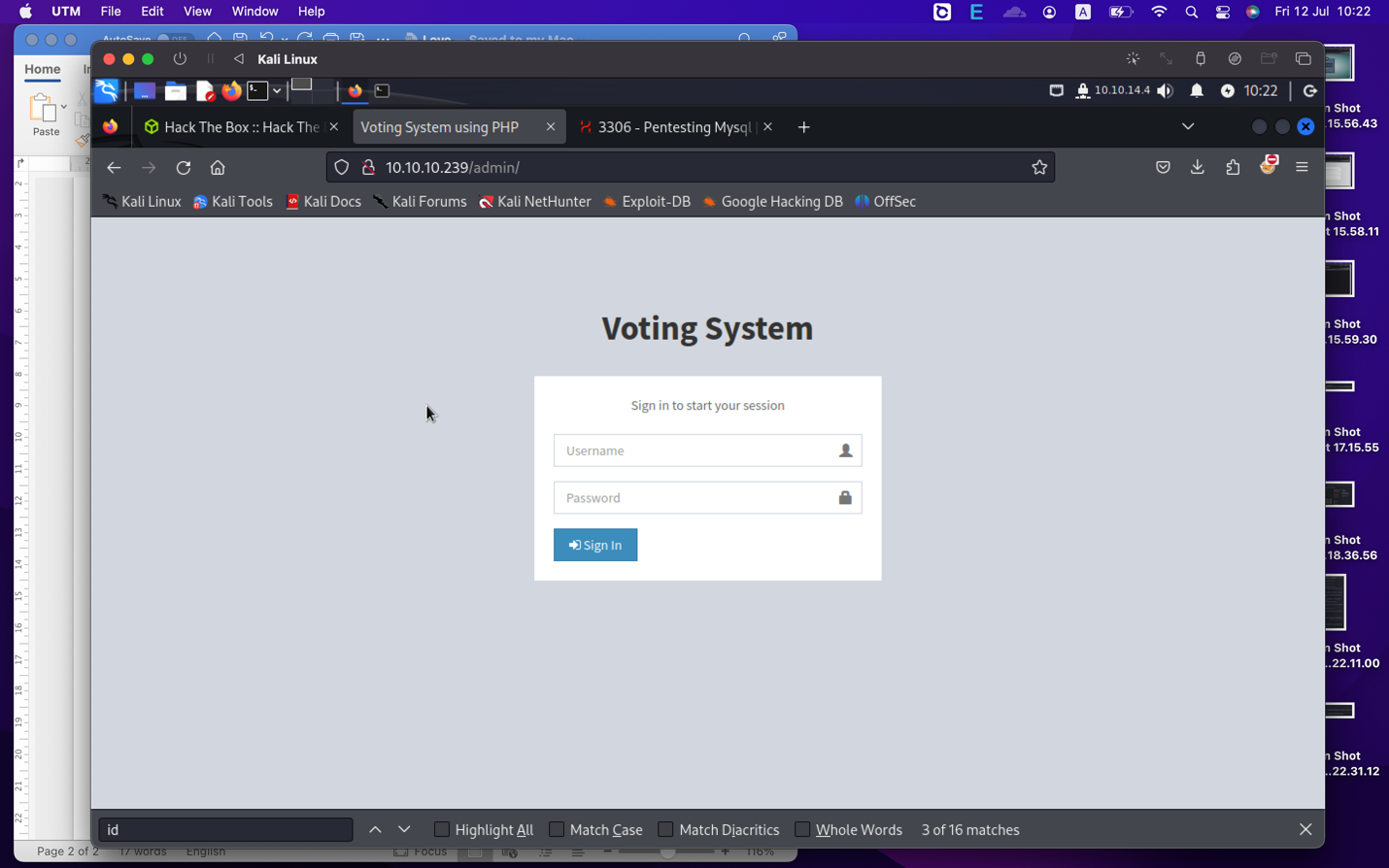
**Web Enumeration**

gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-1.0.txt -u http://10.10.10.239

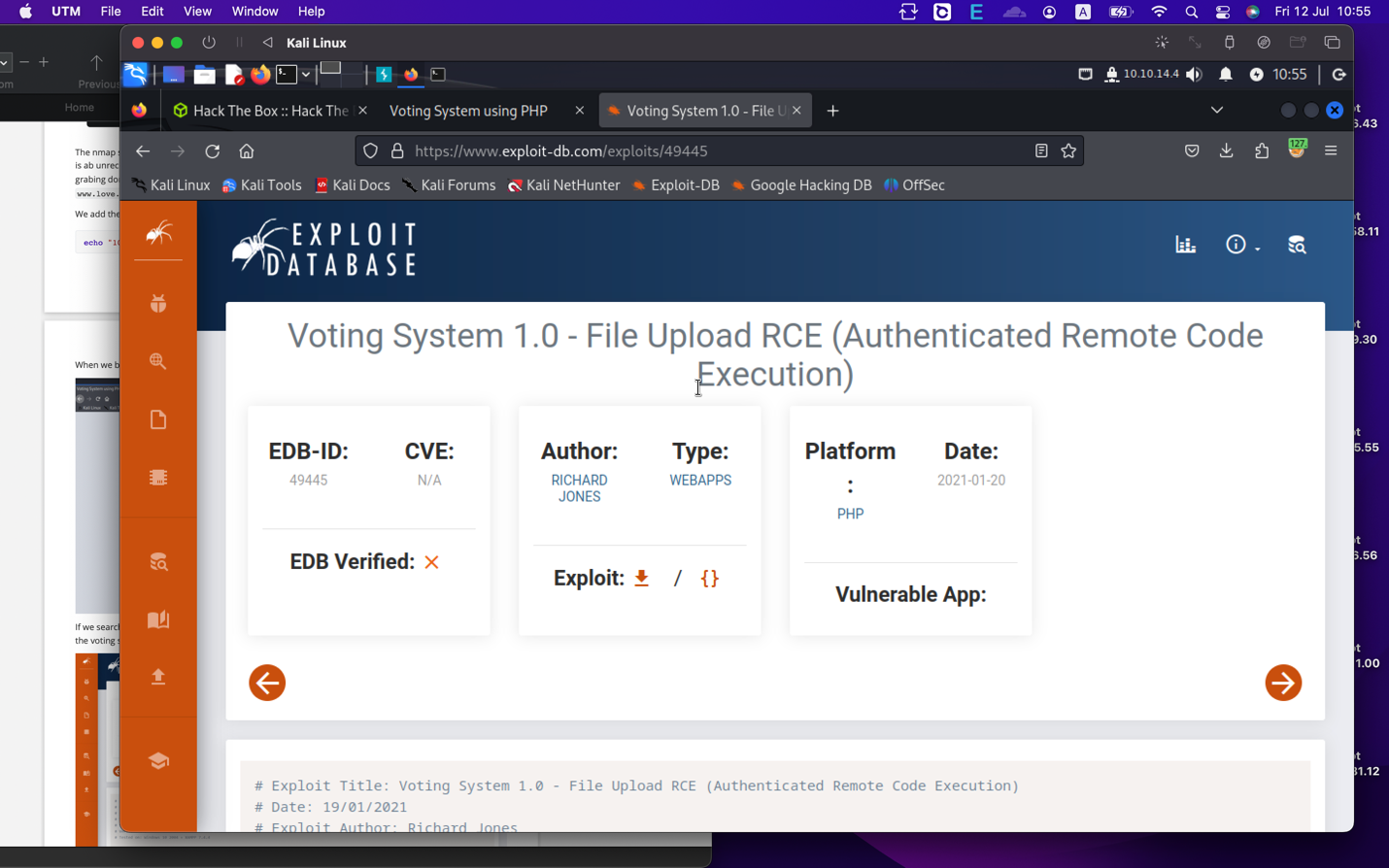
🡪Tìm được thư mục: images, includes, plugins, dist, admin





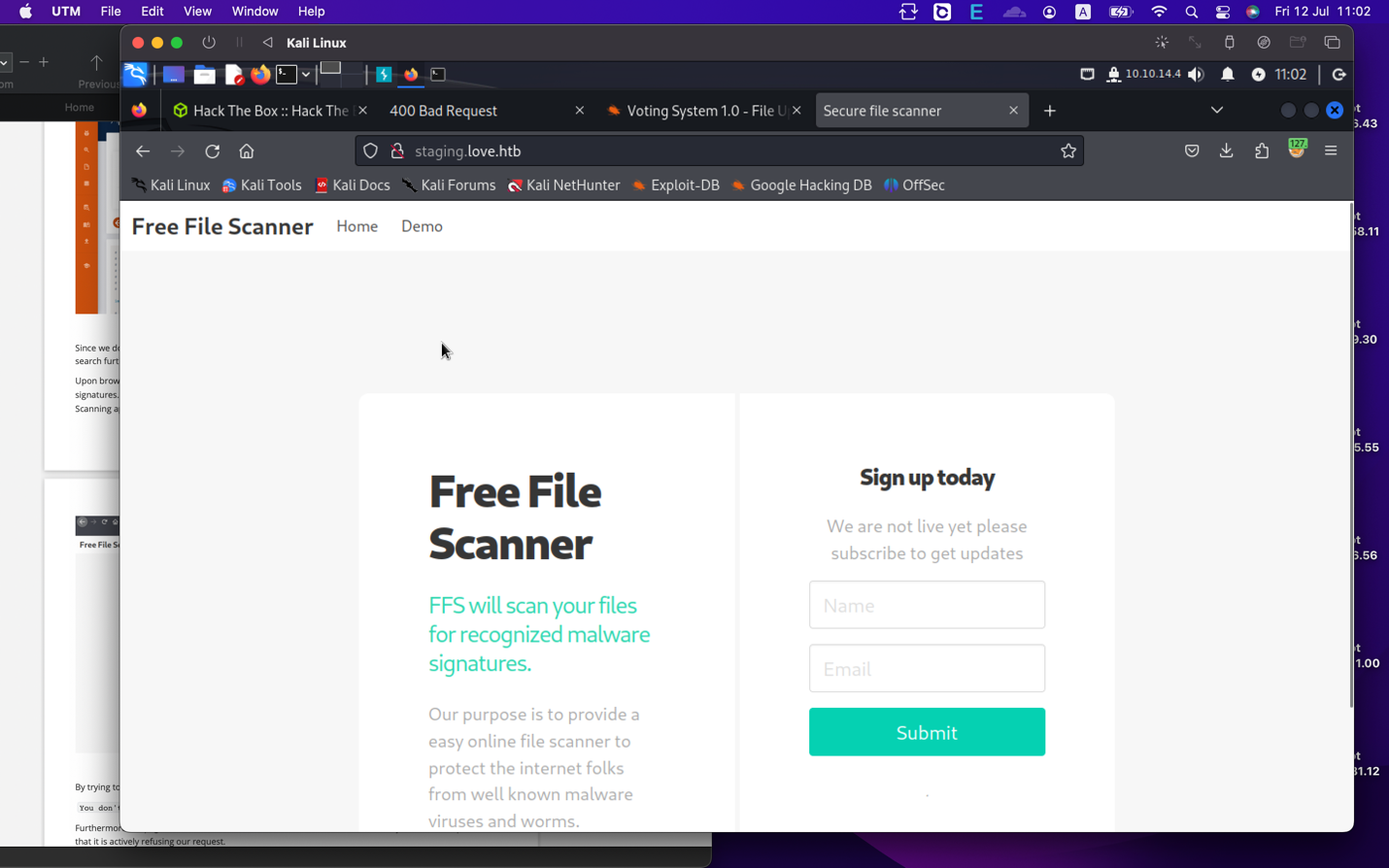


Có 1 cve thực thi mã từ xa trên voting system.



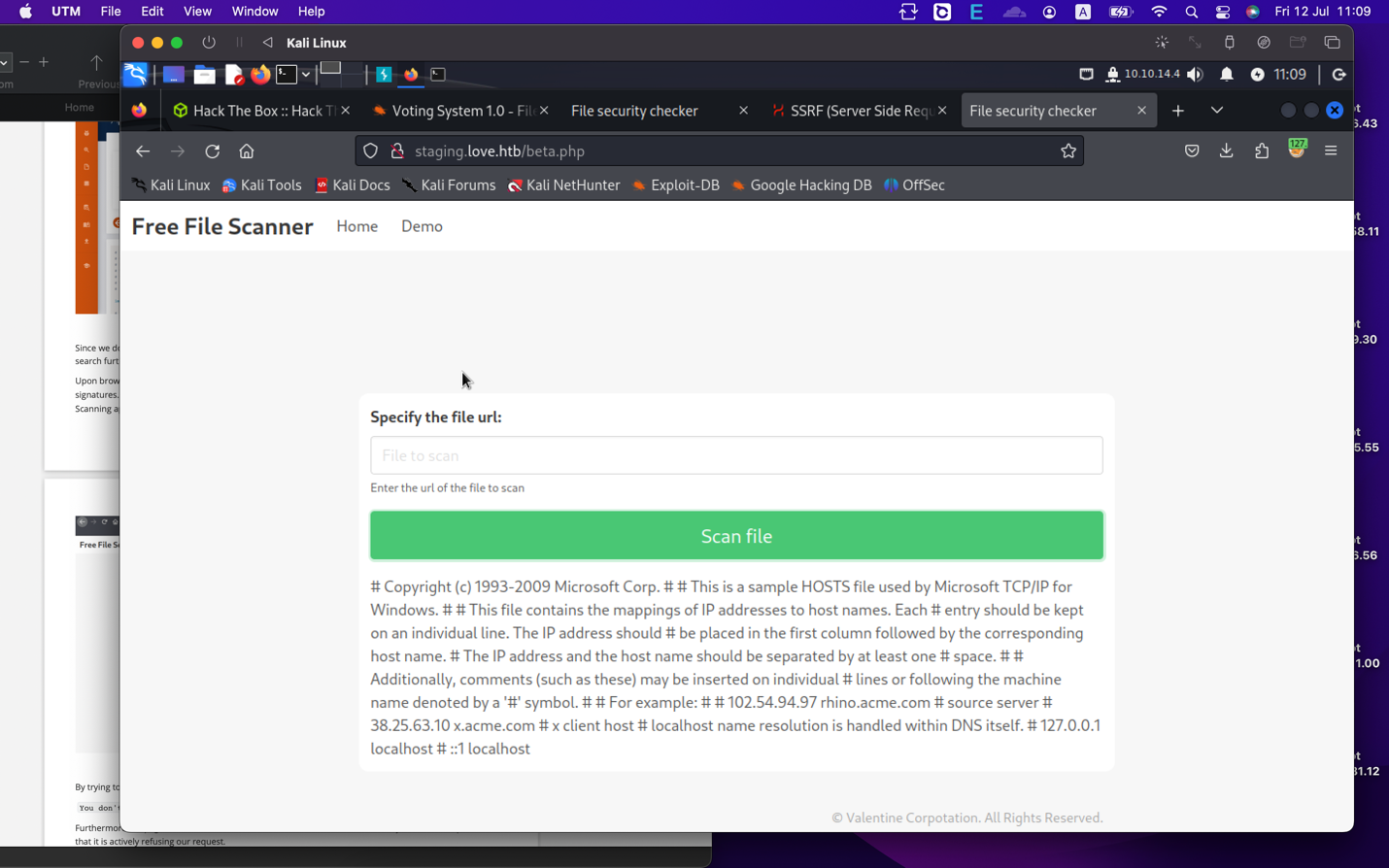
Bạn phải tìm được thông tin đăng nhập mới làm tiếp được.

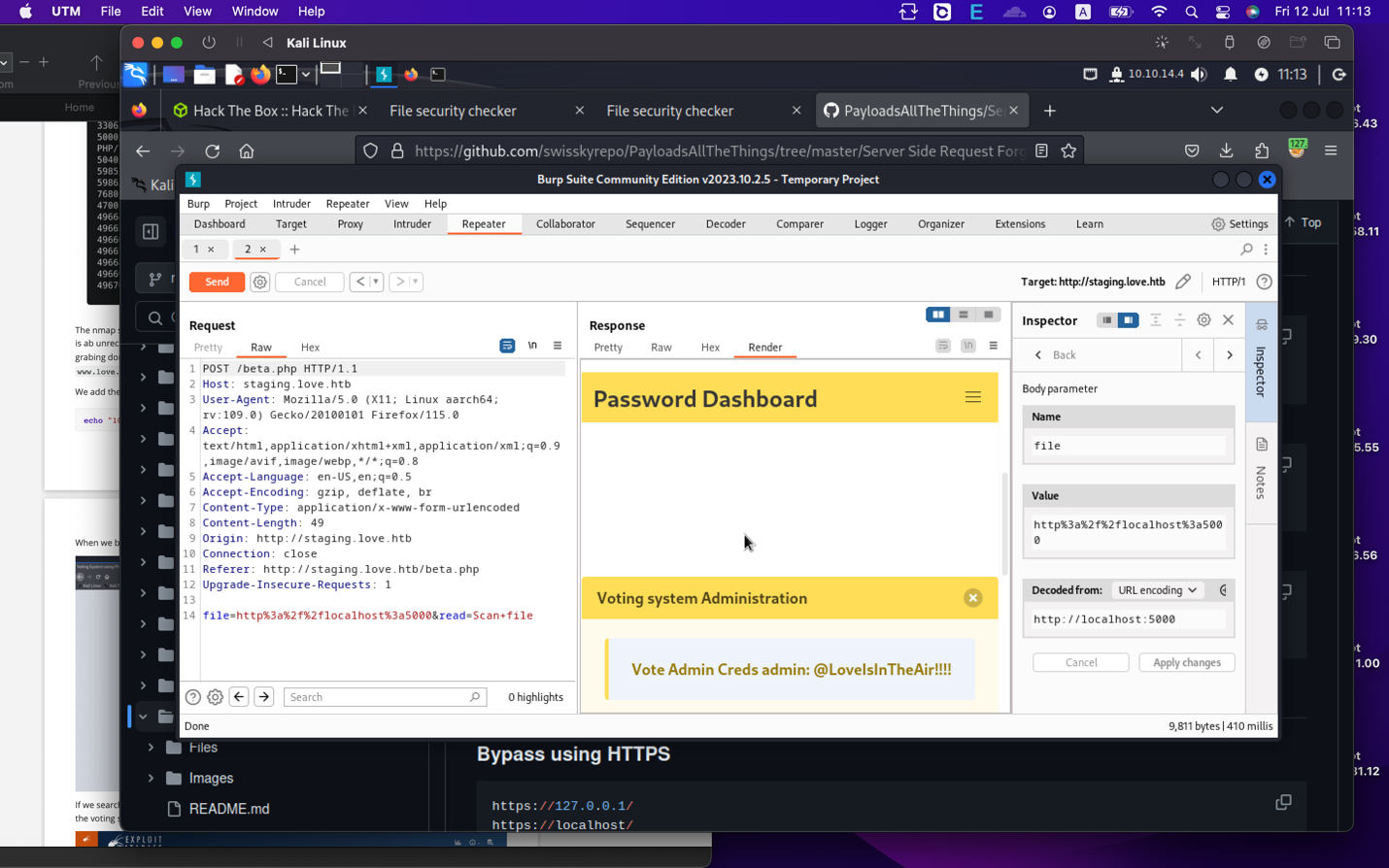
Trong khi đó ở một tên miền khác:



Trang web bị dính lỗ hổng SSRF:

file:///C:\Windows\System32\drivers\etc\hosts





admin: @LoveIsInTheAir!!!!

