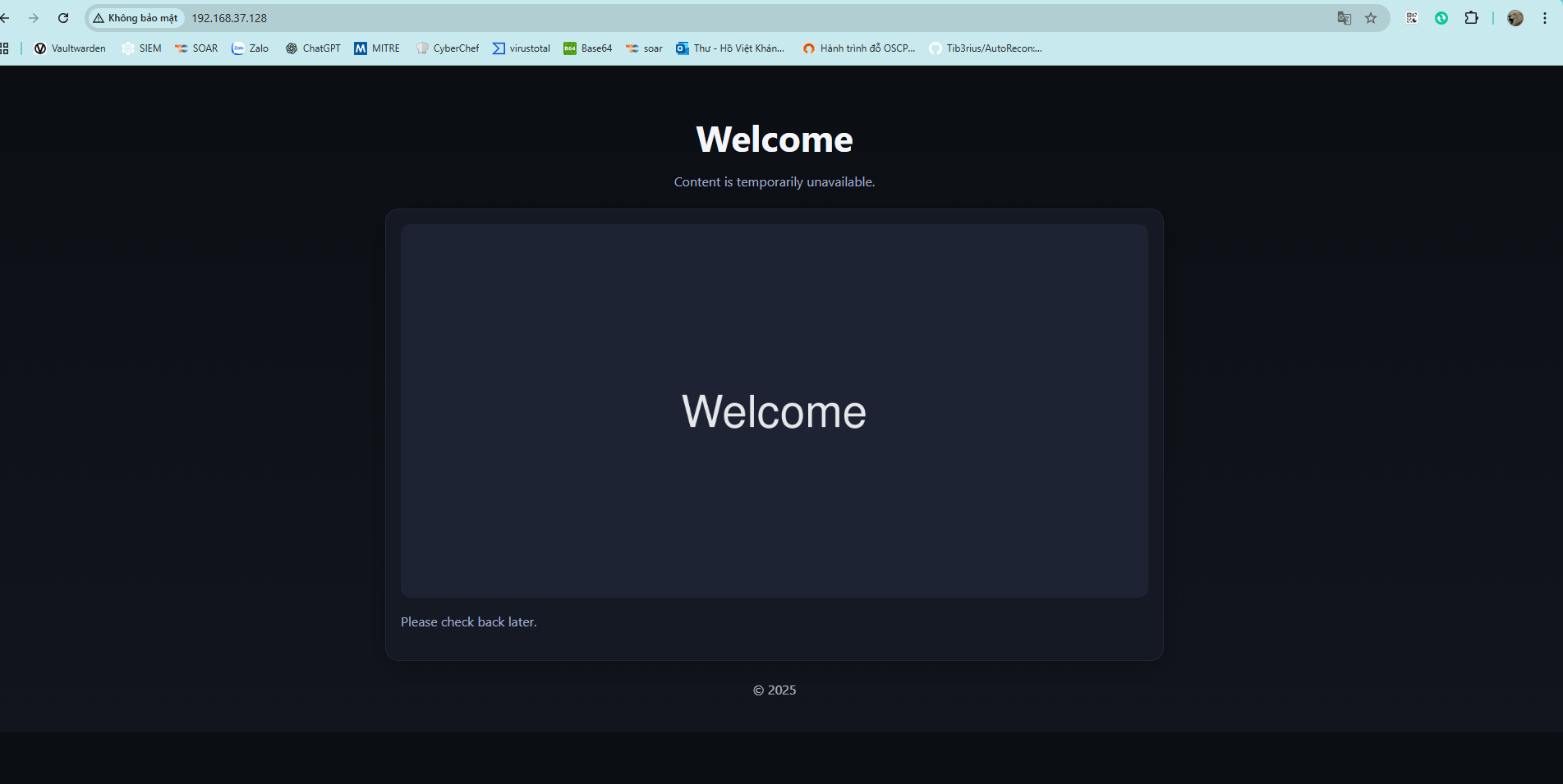
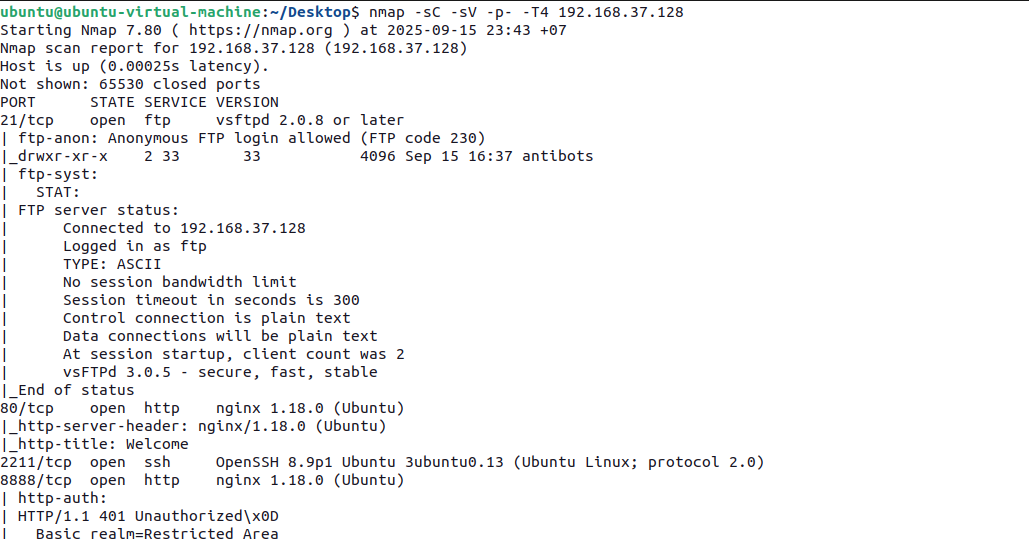
Đầu tiên mở trang web lên, chúng ta sẽ có giao diện như sau:

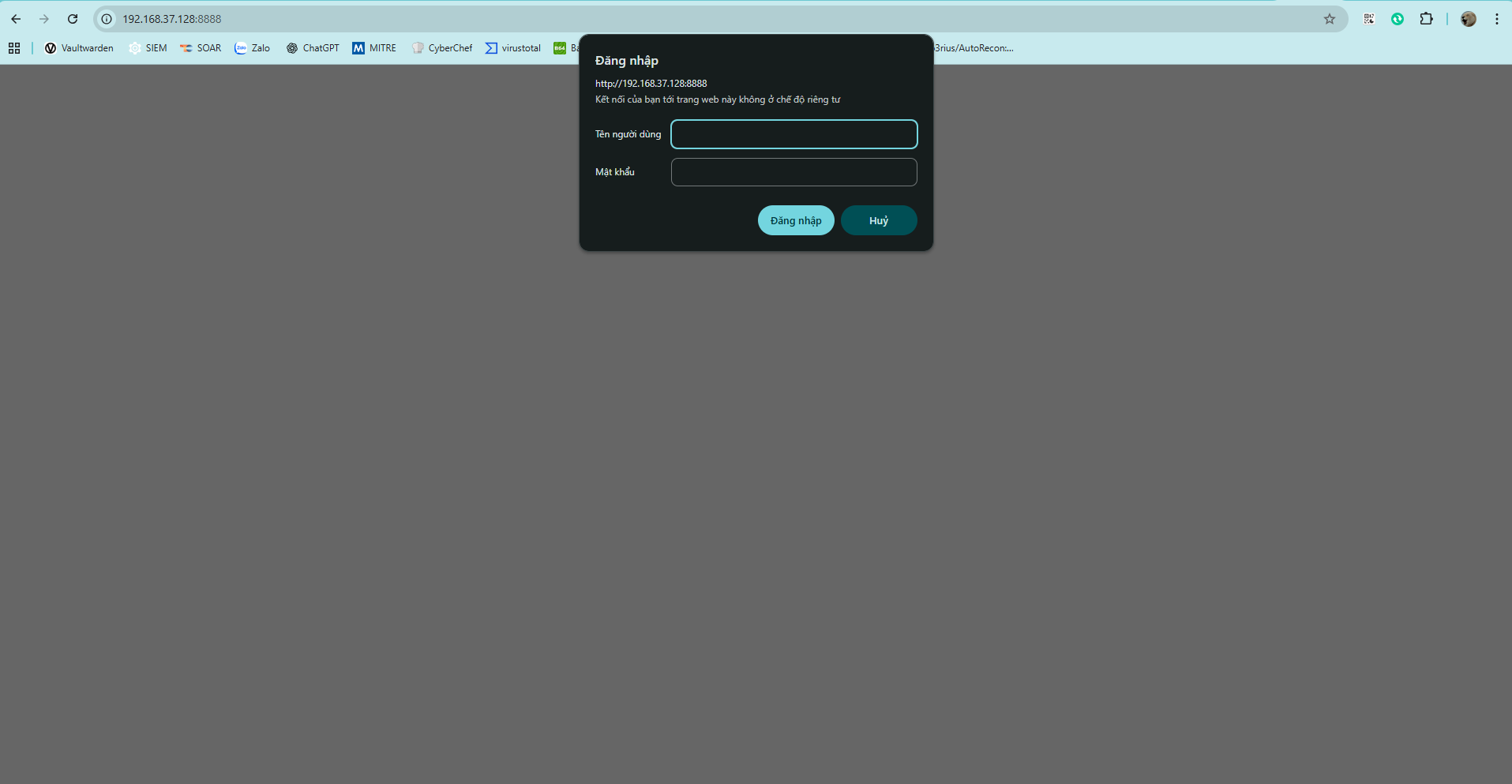


Để bắt đầu, chúng ta tiến hành recon xem thử bài lab sẽ cho chúng ta những gì

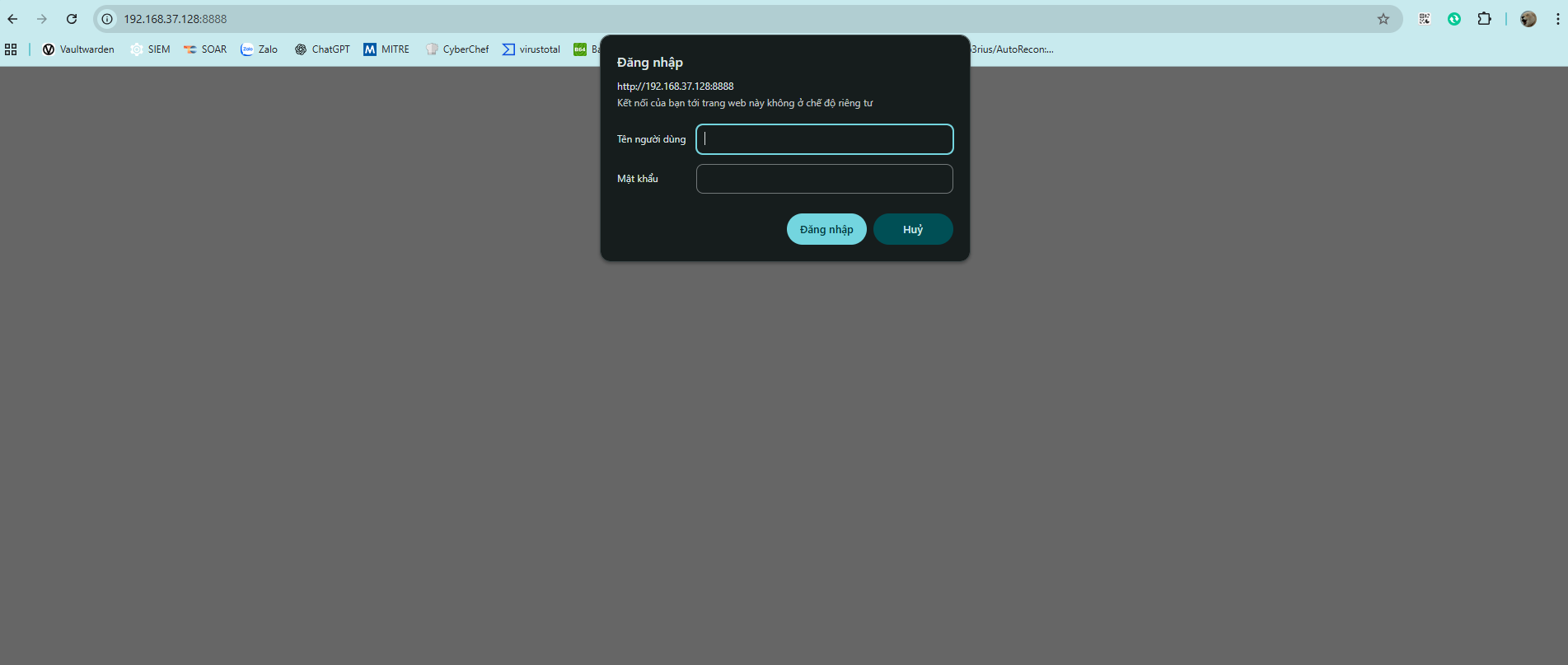
Đầu tiên hãy quét cổng bằng nmap



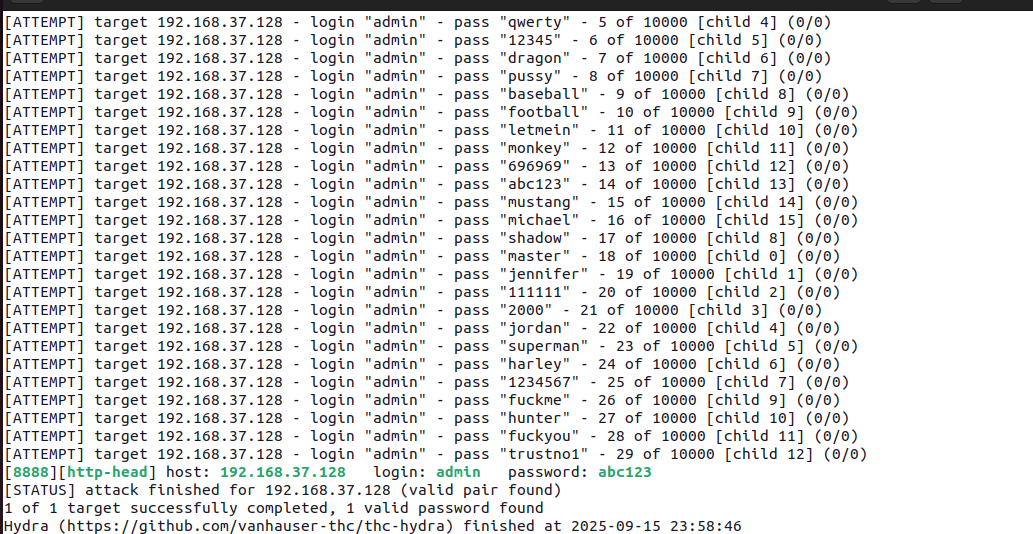
Ở đây, chúng ta có 1 số cổng đáng chú ý là 8888(http),21(ftp) và 2211(ssh), thử vào 8888



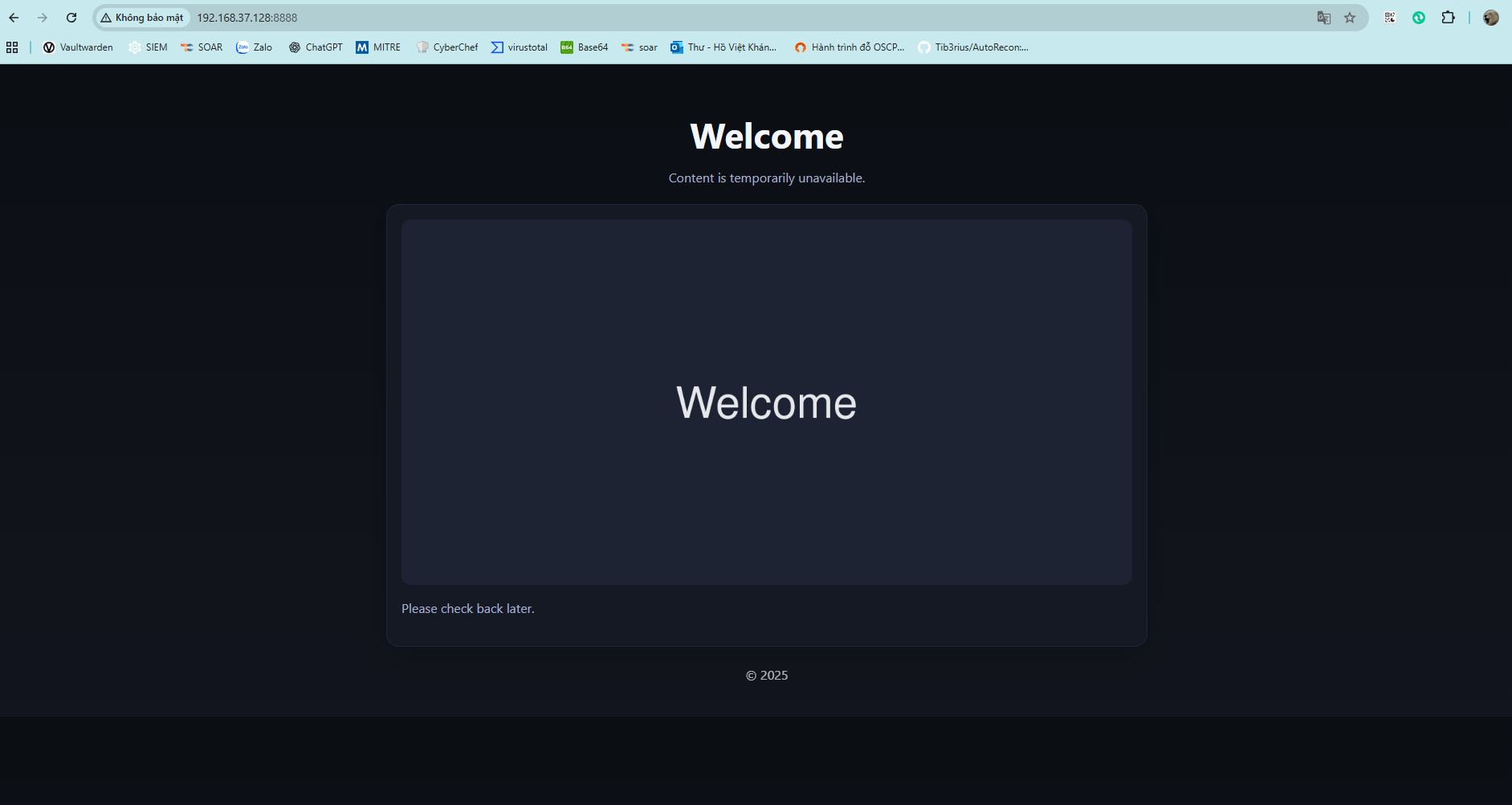
Ồ, ở đây có 1 mục đăng nhập, yêu cầu có user và passwd, thử nhập admin:admin xem sao



Sau 1 hồi thử các passwd đơn giản không được, ta sẽ chuyển sang thử brute-force vào bằng hydra.



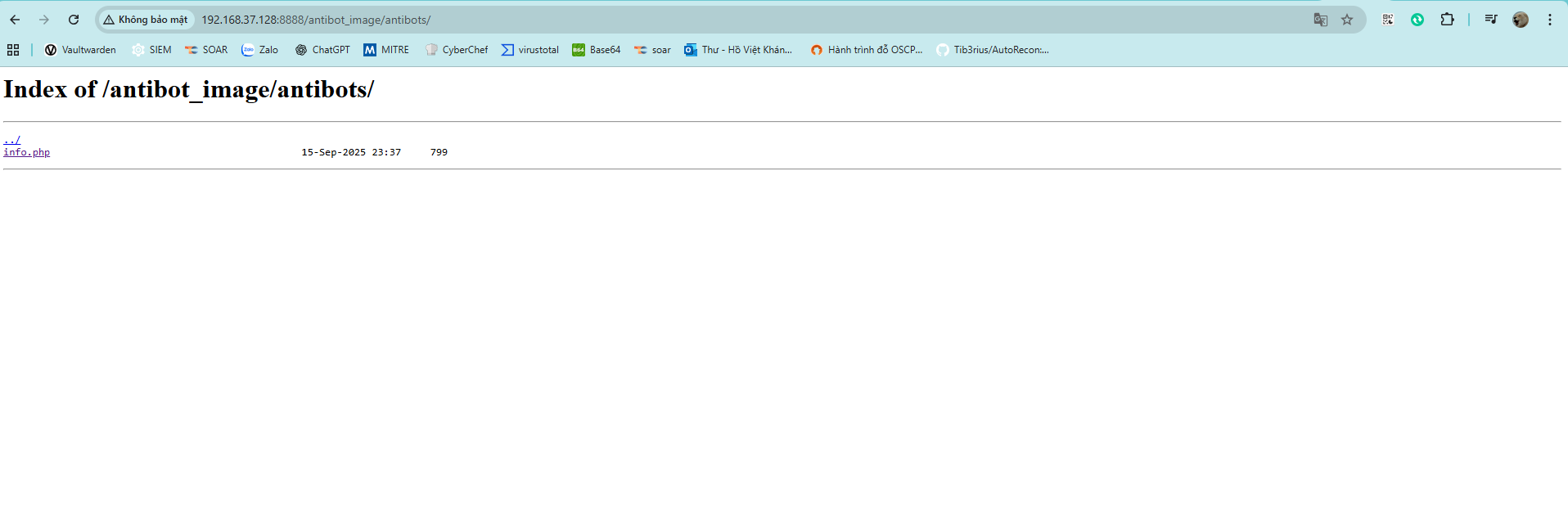
1 lúc sau khi brute-force với nhiều passwd khác nhau bằng hydra, có vẻ tác giả đã cho chúng ta 1 passwd dễ để có thể tiếp tục lab này



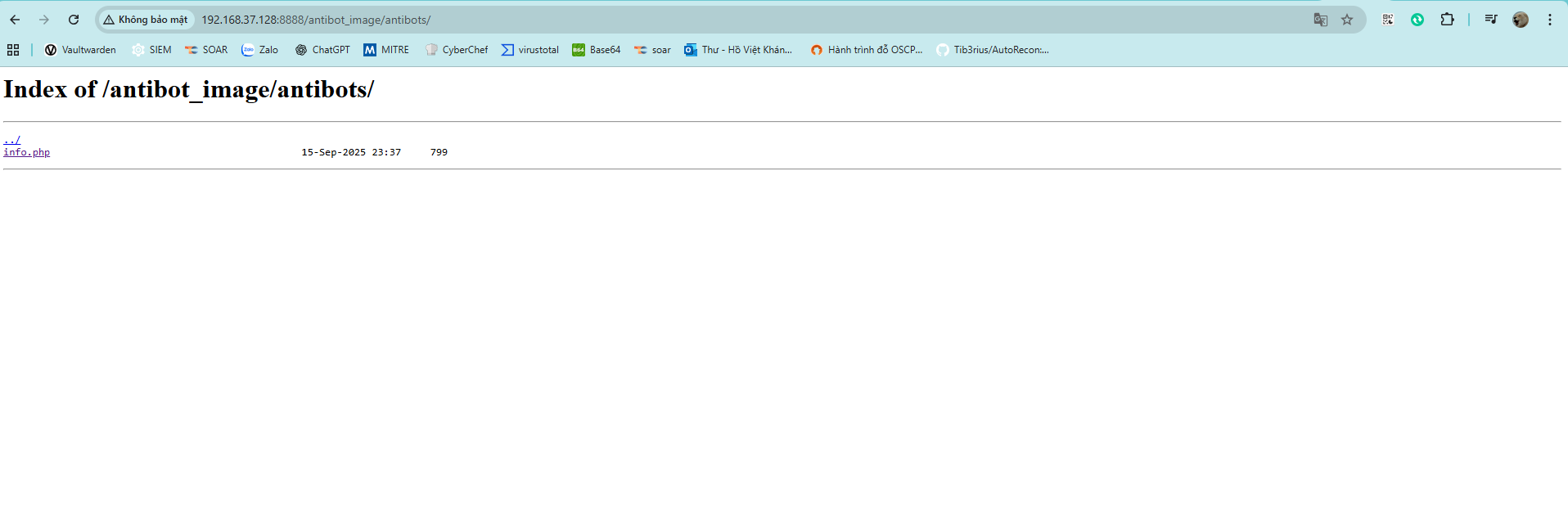
Khi vào thành công, chúng ta vẫn nhận được 1 trang giống y hệt ban nãy, hãy thử suy nghĩ nếu trang web này có những thu mục nào đó hay ho nên tác giả mới bắt xác thực khi vào nó thì sao, tiếp tục sử dụng dirb để liệt kê thư mục



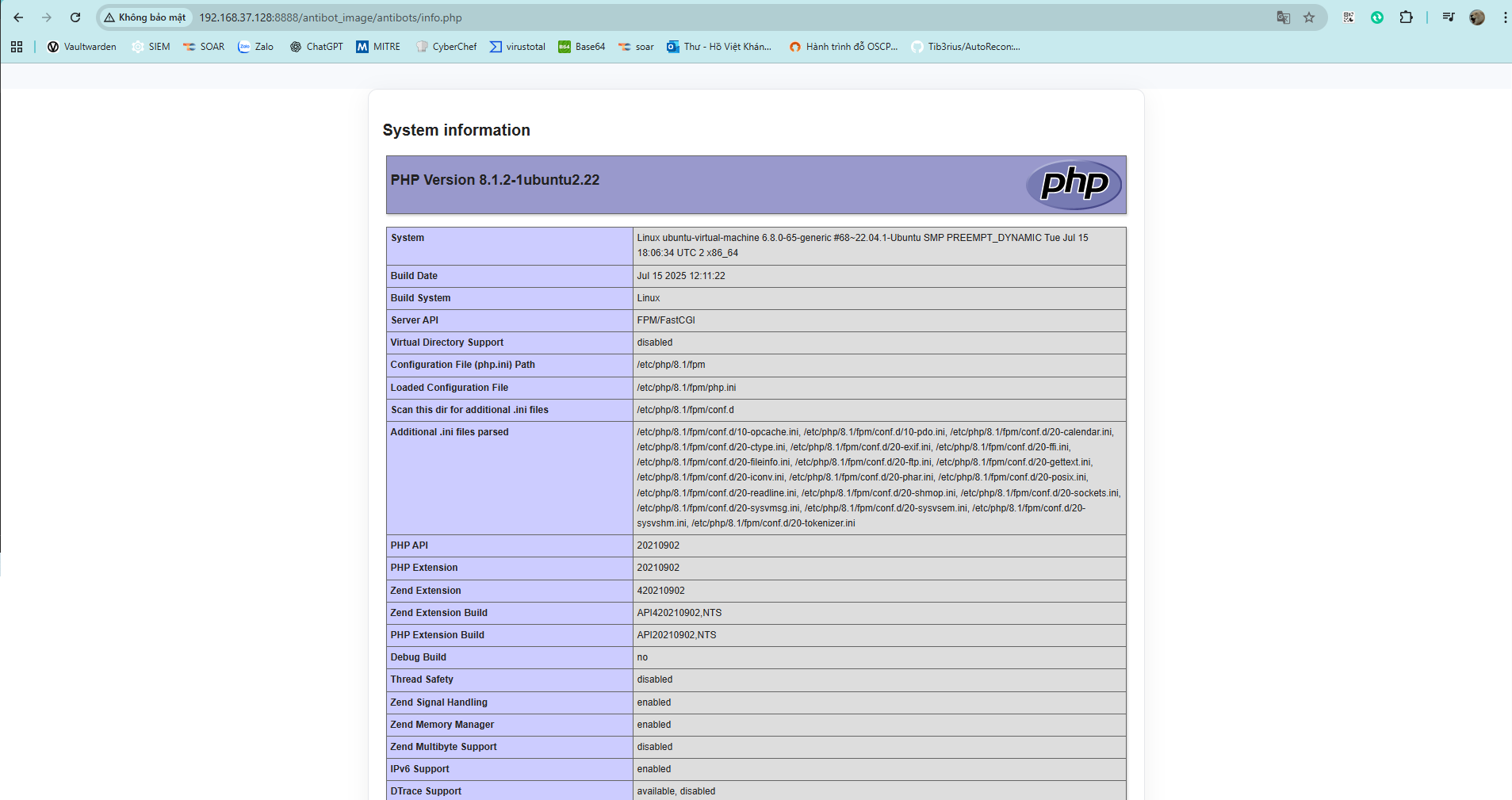
Ở đây, chúng ta tìm ra 2 thư mục là antibot\_image và assets. Hãy thử vào thư mục đầu tiên là antibot\_image



Ta nhìn thấy 1 file info.php ở đây(nếu muốn noise hơn có thể tạo nhiều folder và file để làm chậm quá trình tìm ra hướng đi)

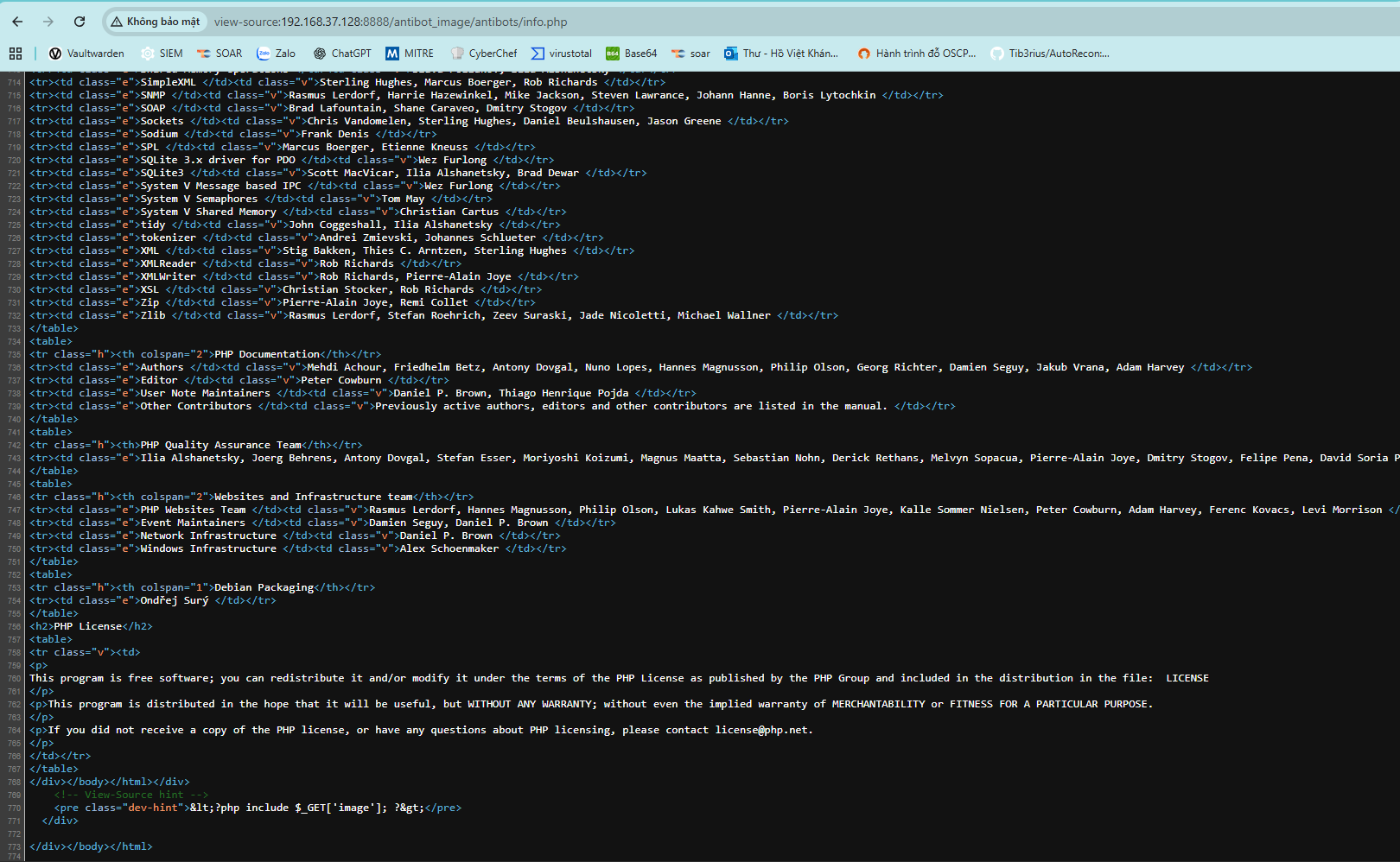


Truy cập theo đường dẫn dirb trả về:



Tiến hành view-source ta nhận được nội dung như sau:

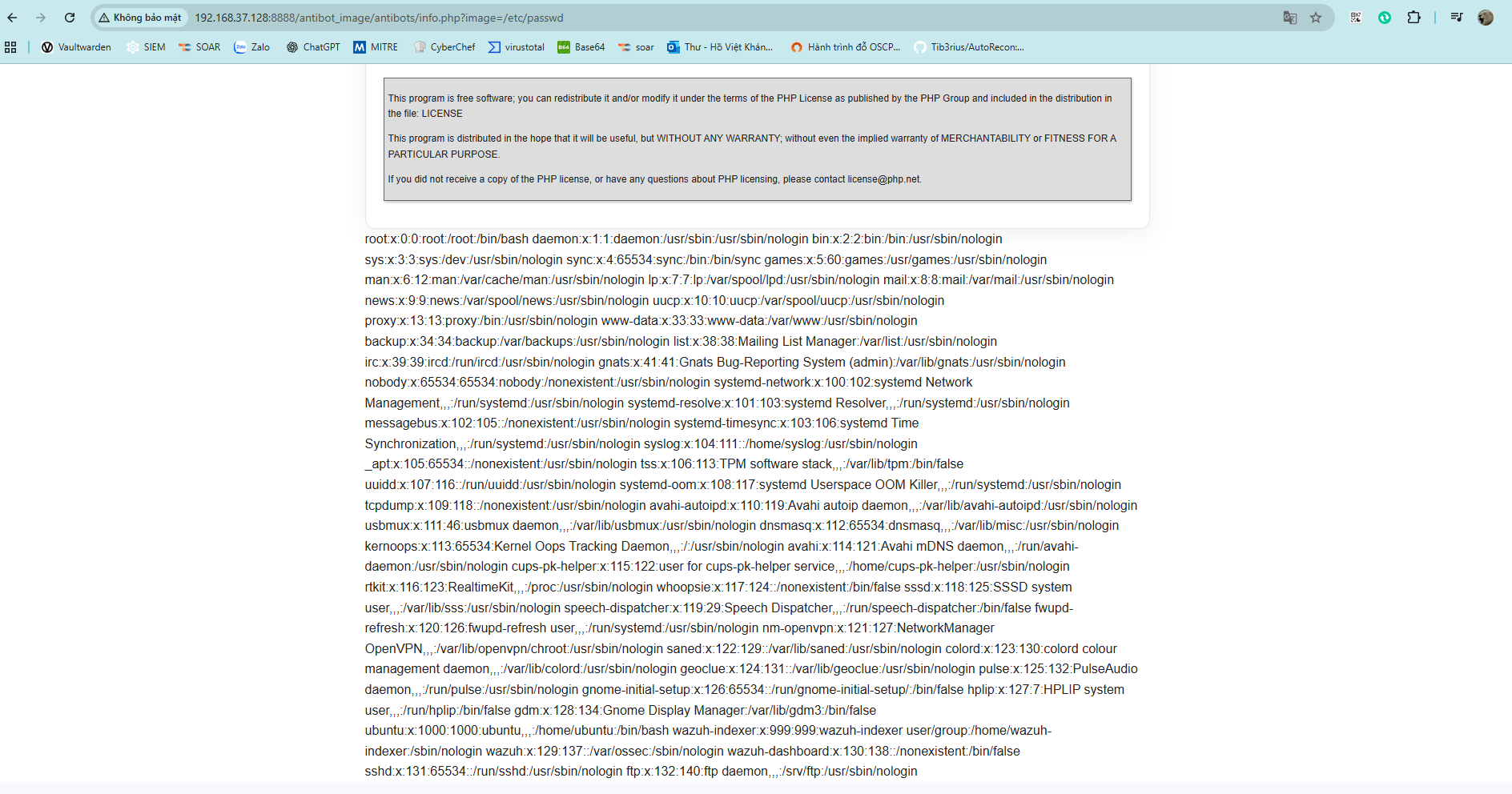
Nhấn CTR + U để xem src



Ta có thể nhìn thấy 1 dòng code ở đây cực kì nguy hiểm

</?php include $\_GET['image']; ?> gợi ý cho chúng ta về lỗ hổng Local File Inclusion (LFI)

Với gợi ý trên, ta sẽ thử ?image/etc/passwd và ta đã khai thác thành công



LFI to RCE

Cái lỗi gốc:

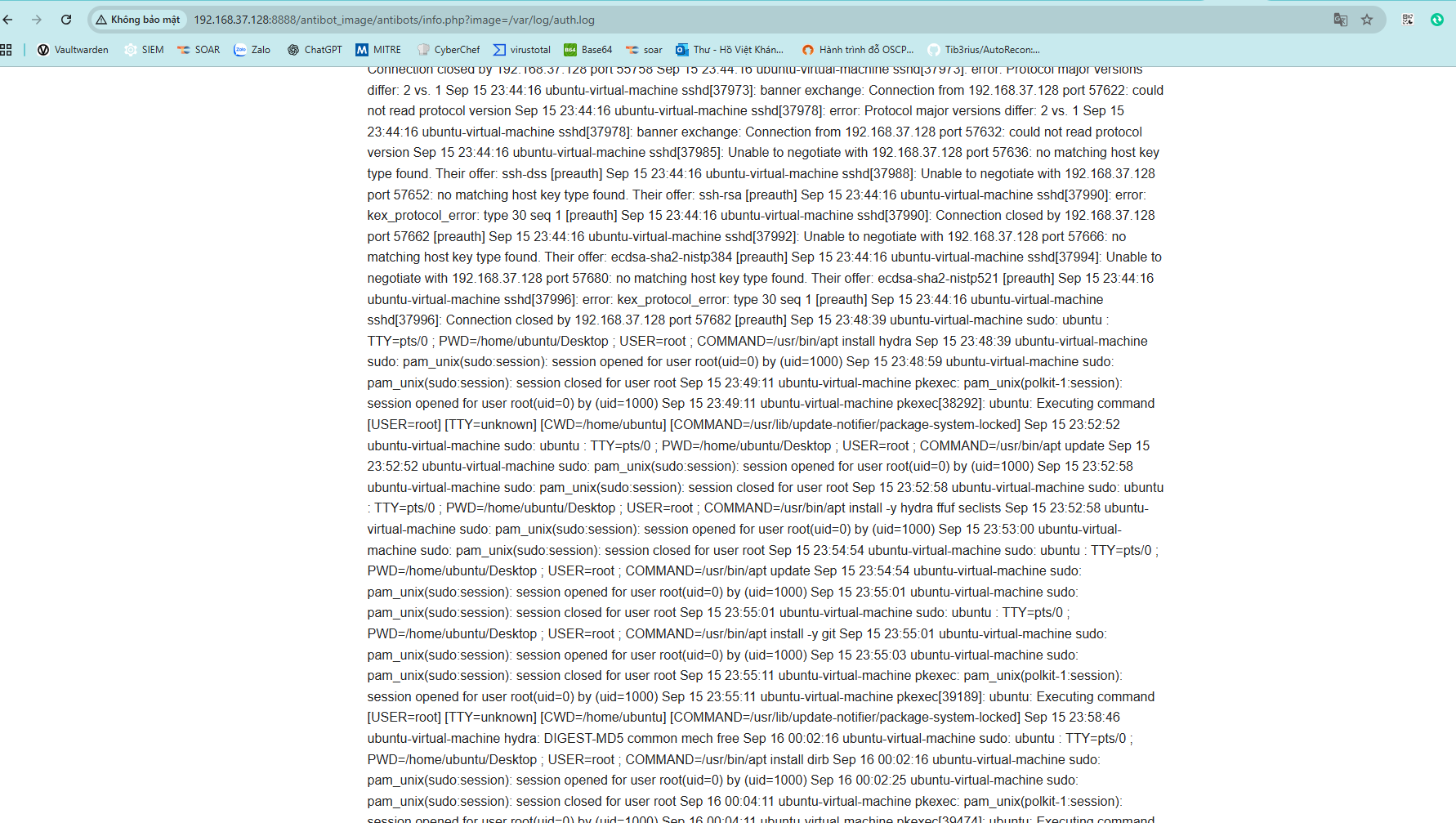
info.php có dòng (ẩn trong View-Source):

<?php include $\_GET['image']; ?>

include() đọc rồi thực thi nội dung file được chỉ ra.

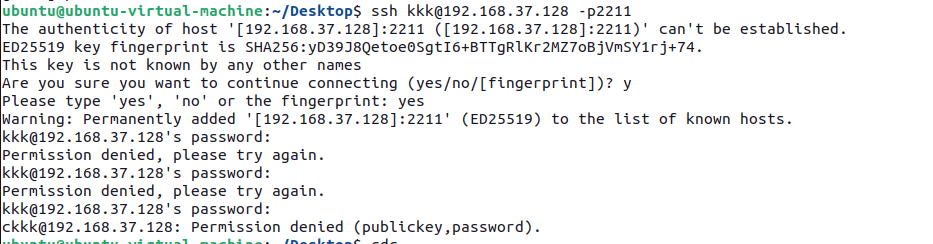
Vì không giới hạn (open\_basedir = no value trong phpinfo), bạn có thể đưa đường dẫn tuyệt đối như /etc/passwd, /var/log/auth.log, …

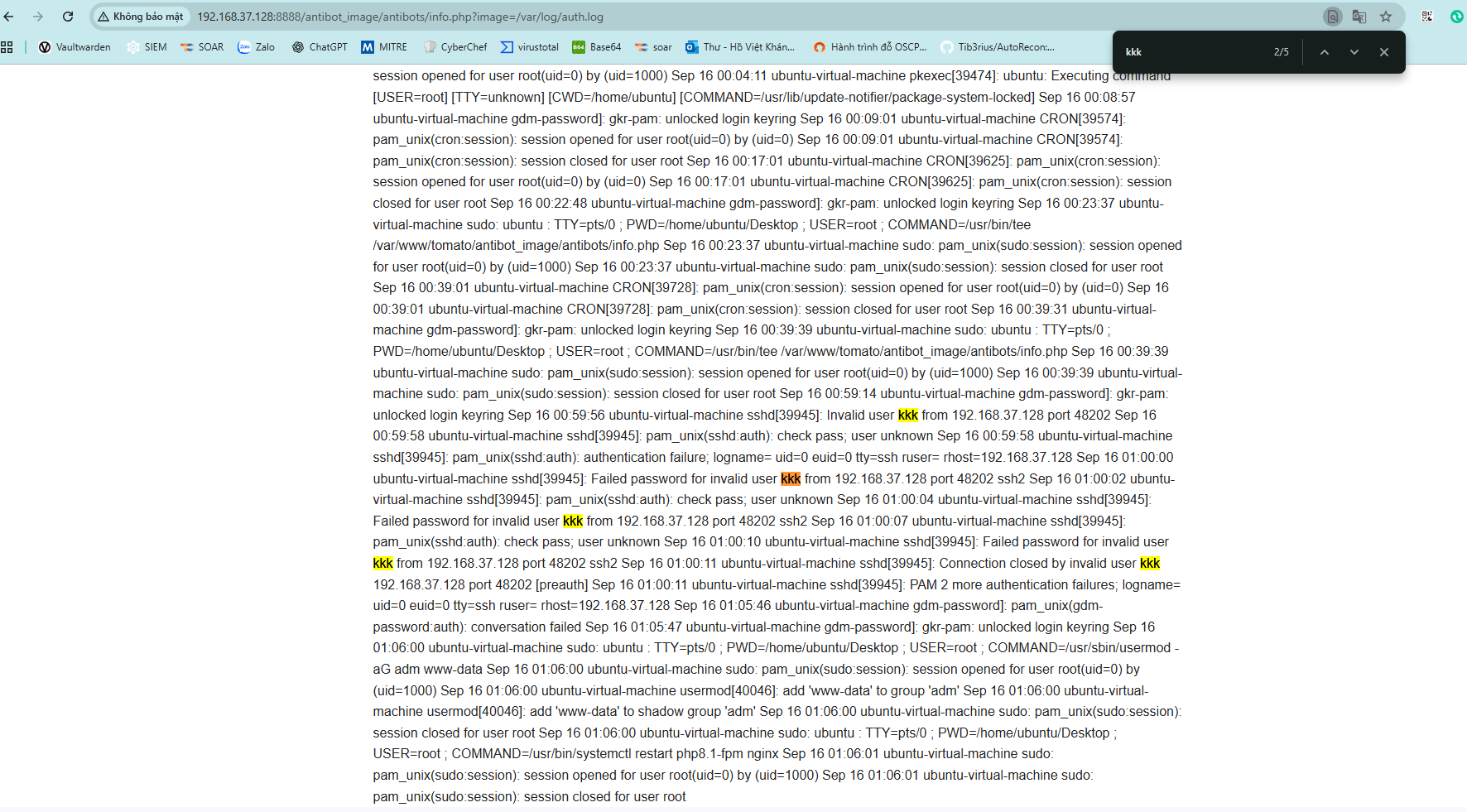
Với LFI, ta phát hiện auth.log có thể đọc được thông qua lỗ hổng này



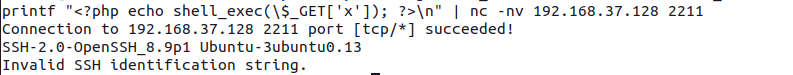
"auth.log" là file lưu trữ nhật ký truy cập hệ thống. Khi chúng ta đăng nhập thông qua giao diện chính hay qua SSH thì các thông tin đều được lưu trữ tại đây kể cả thành công hay thất bại.

Thử đăng nhập thất bại nhiều lần xem nó có lưu ra ngoài không

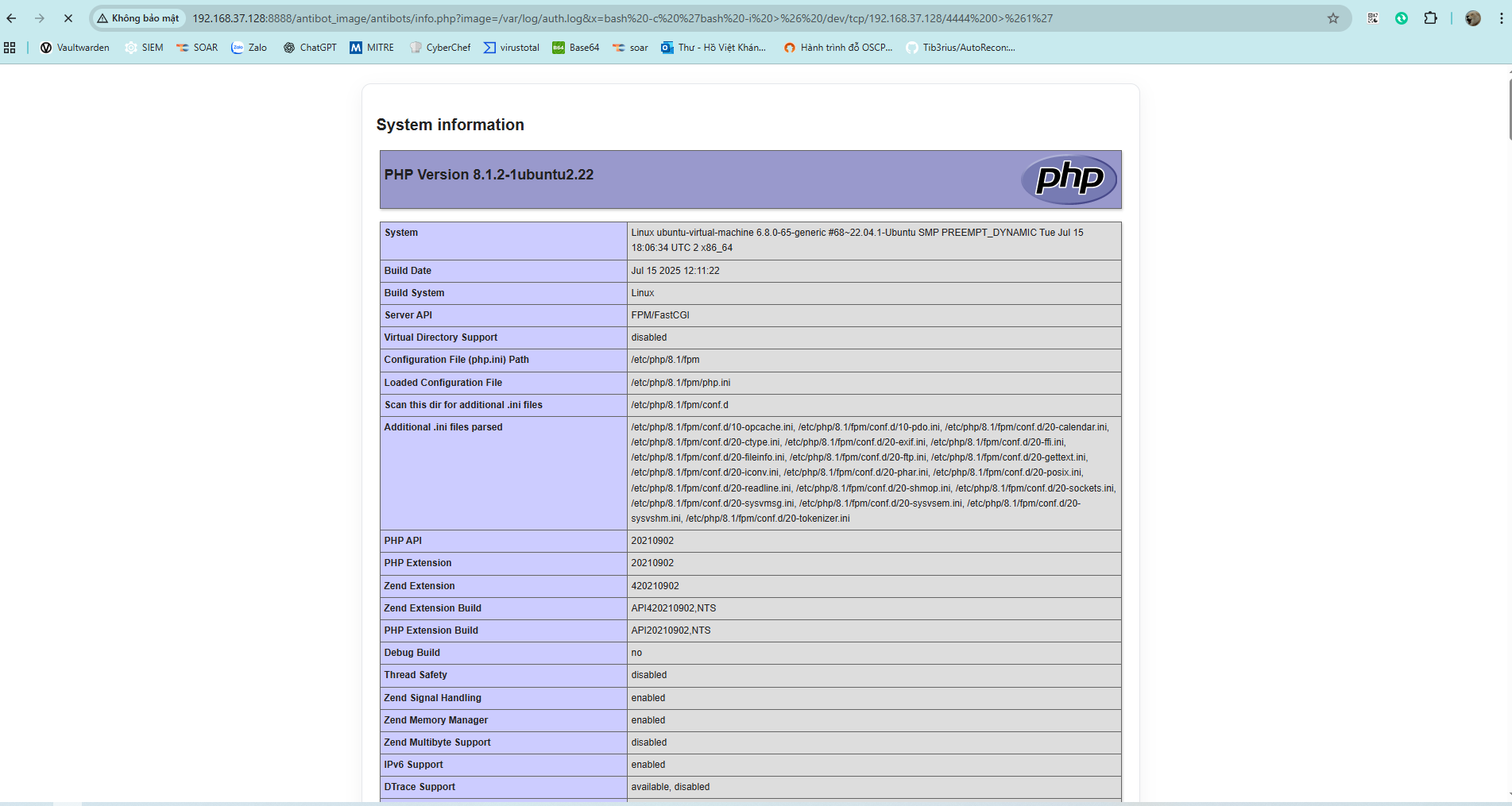


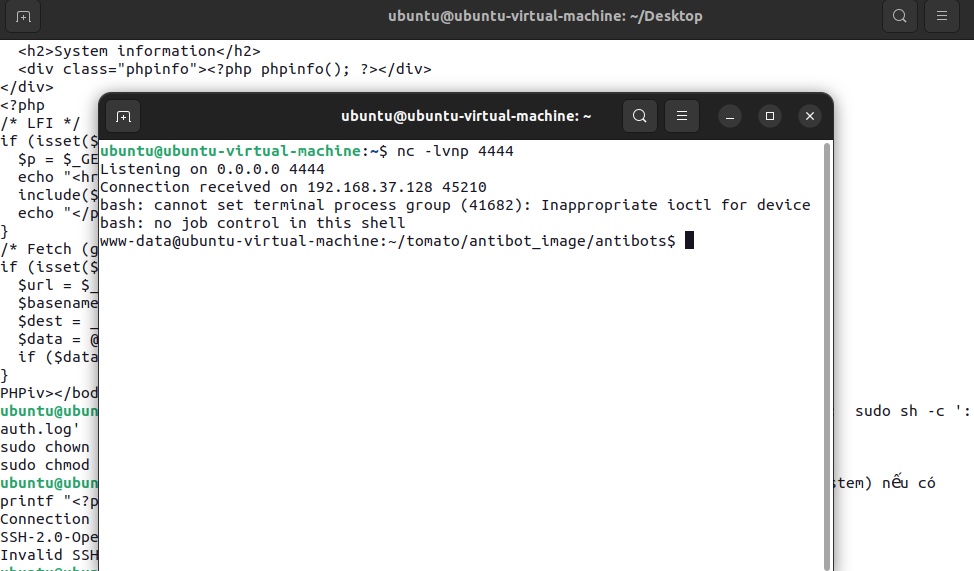


Nó có ghi lại, như vậy hãy thử bơm PHP vào log



Sau khi bơm xong, đưa reverse shell vào url và mở 1 cổng lắng nghe





Có 1 phiên shell, thành công



Ở đây có thể tiếp tục khai thác thêm bằng cách đưa thử thách lên root để cat flag để có thể hoàn thành