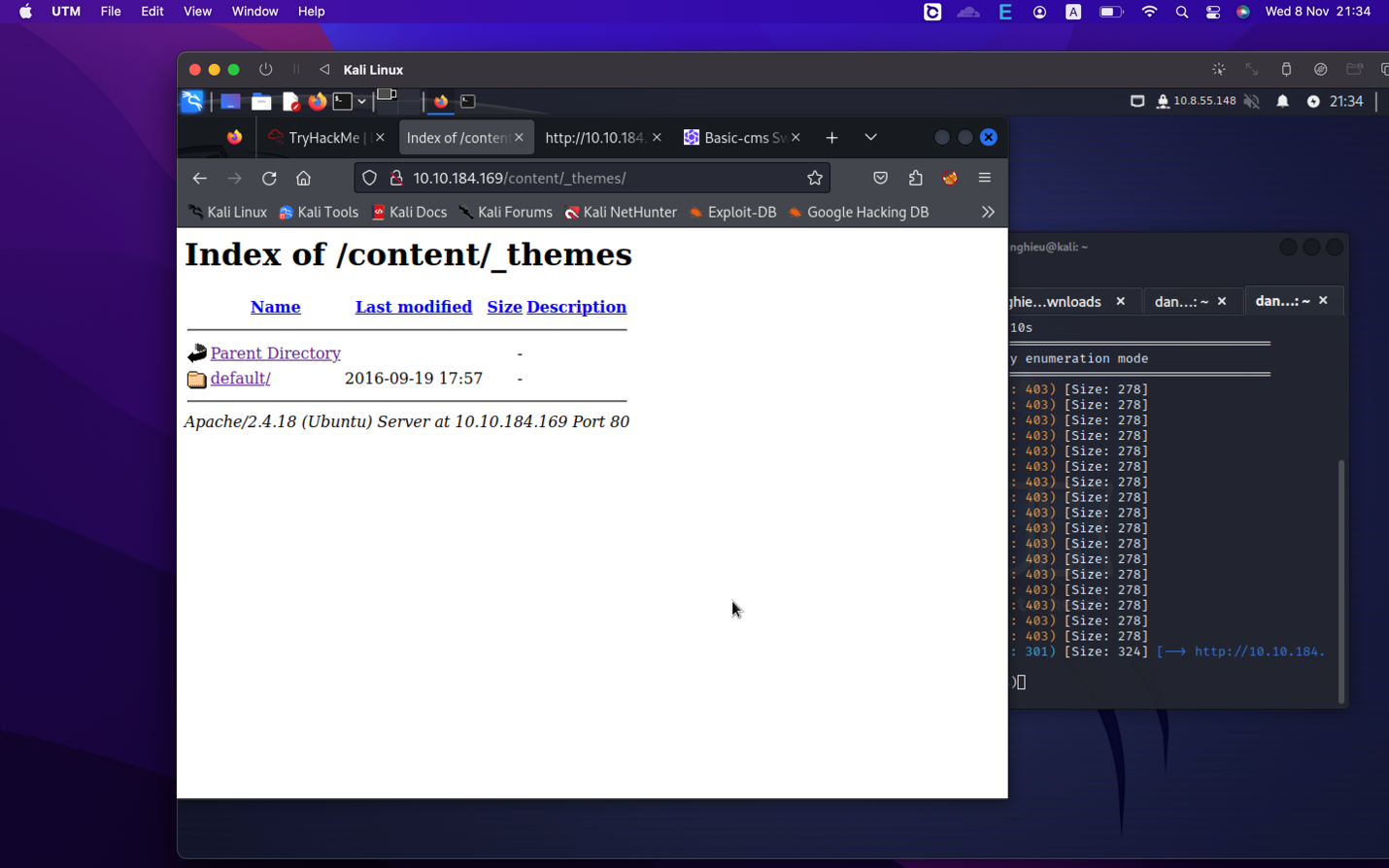
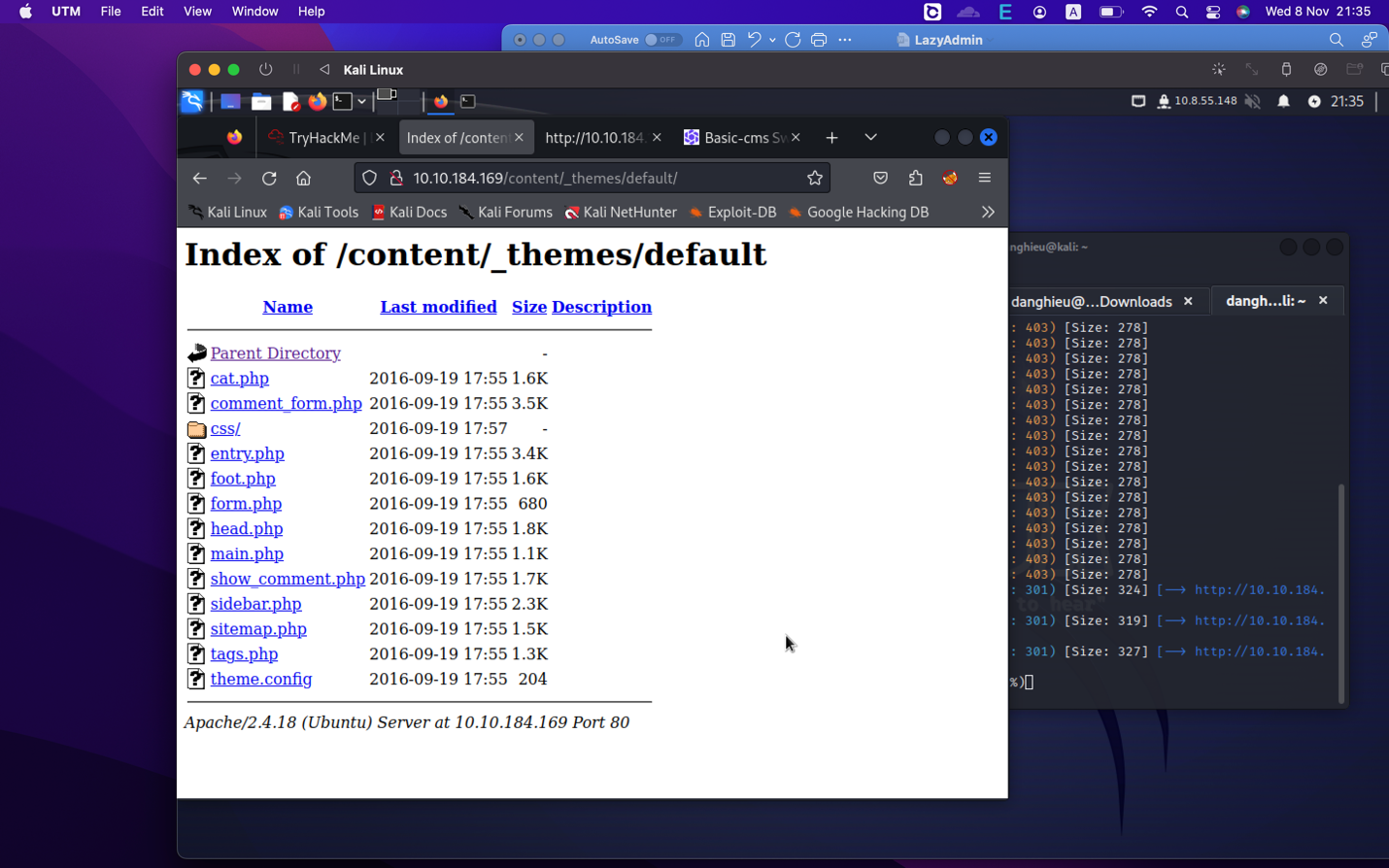
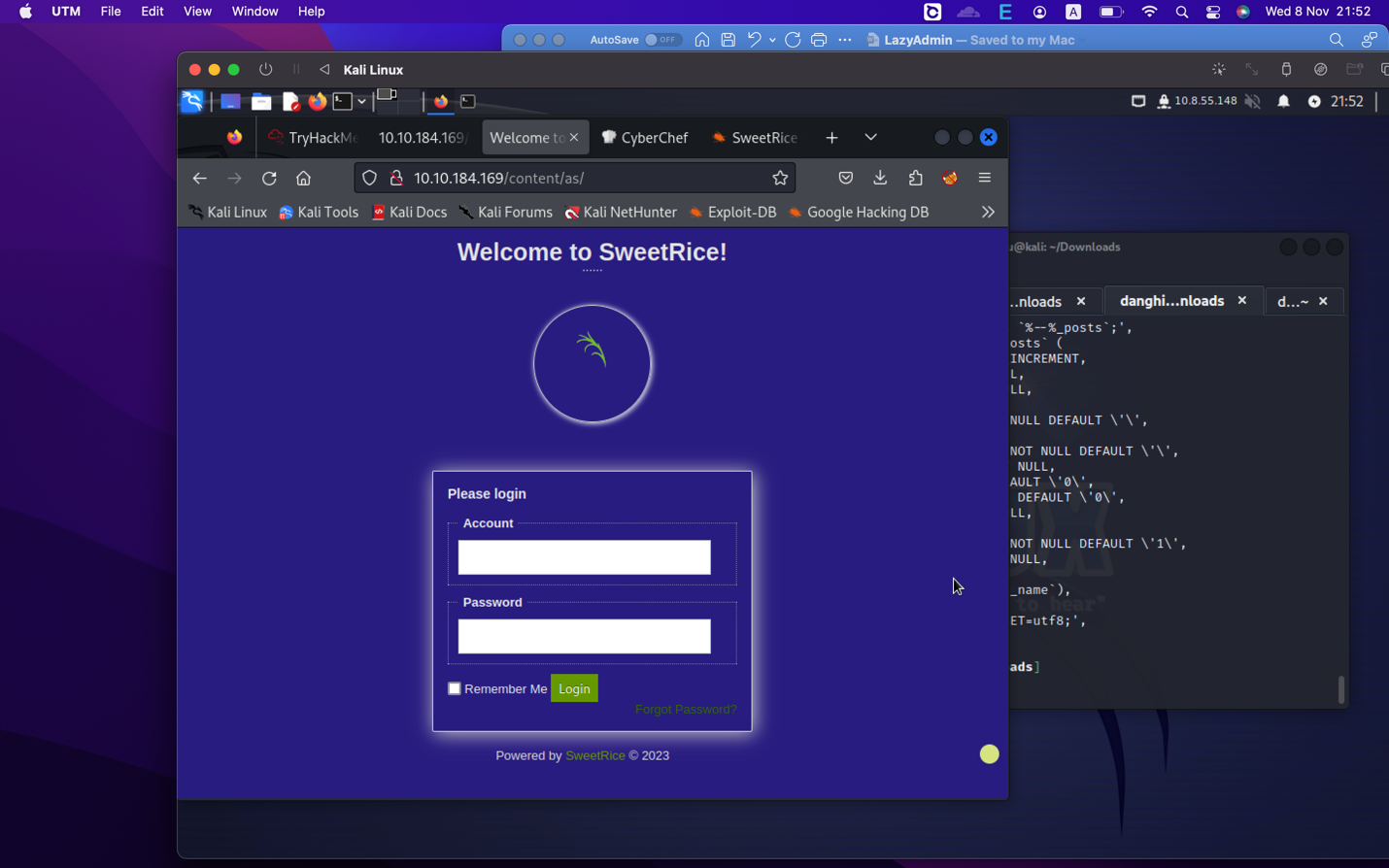
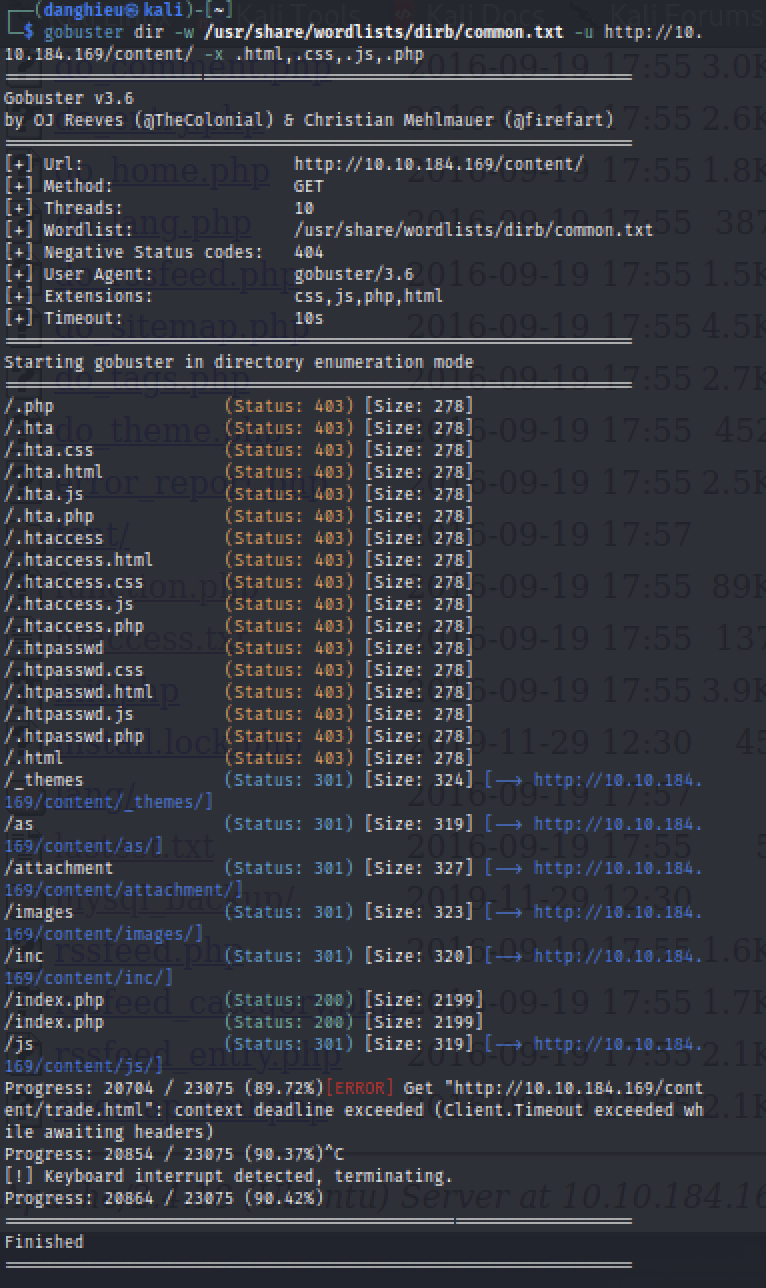


Một số cổng bị filter rồi.

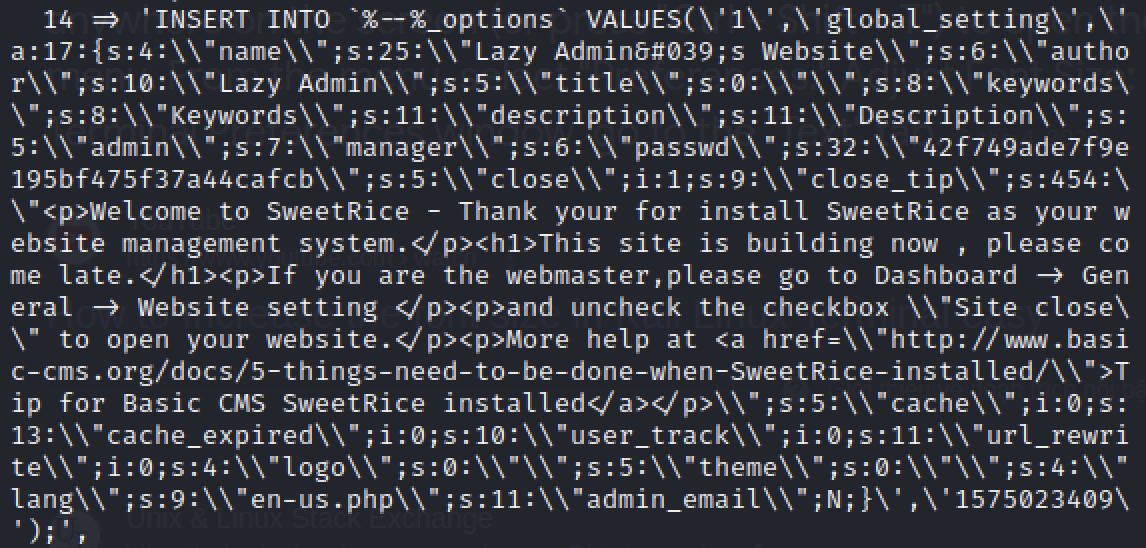






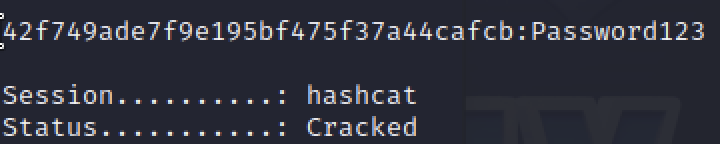


Mình có tìm được 1 file backup\_mysql:

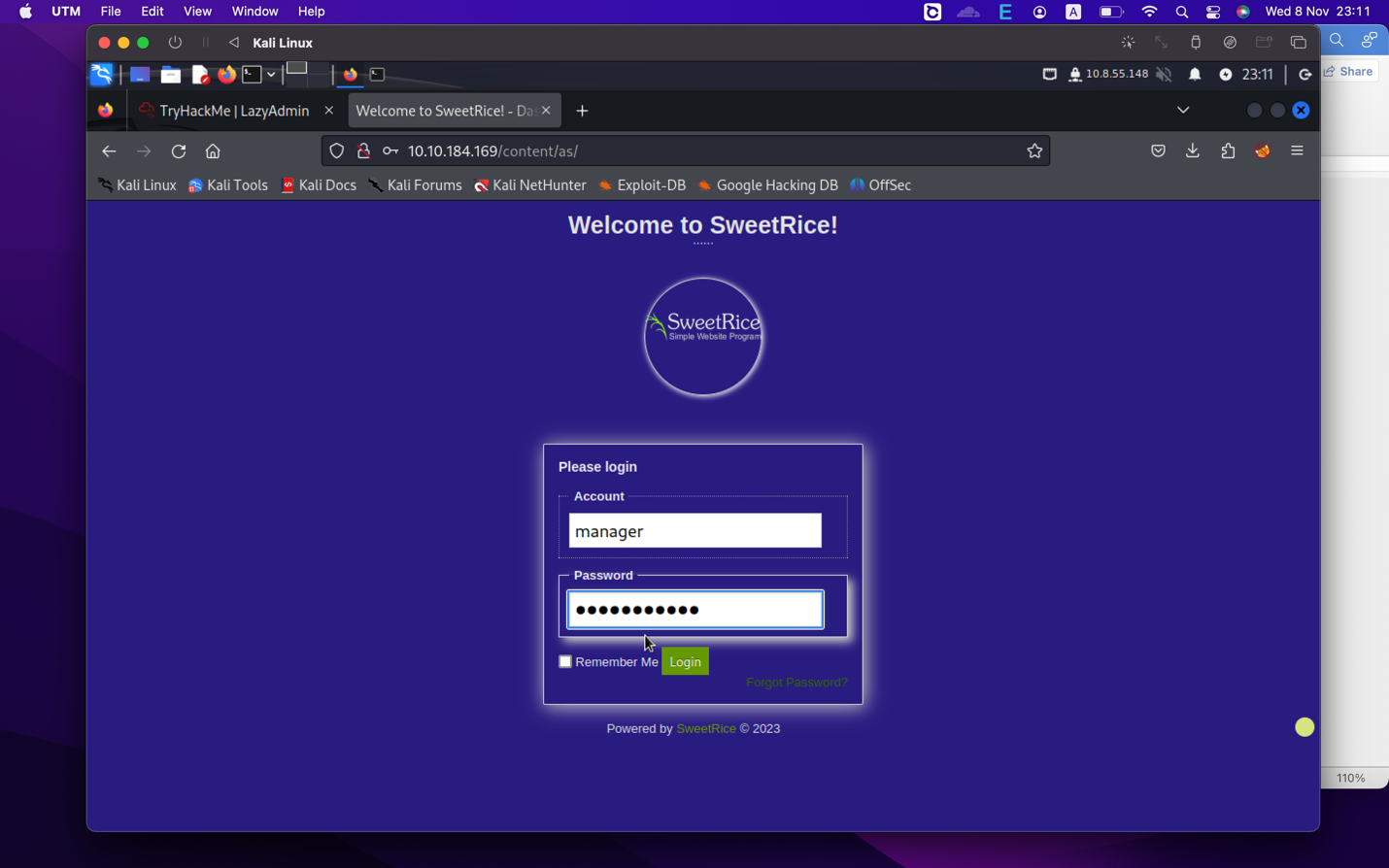


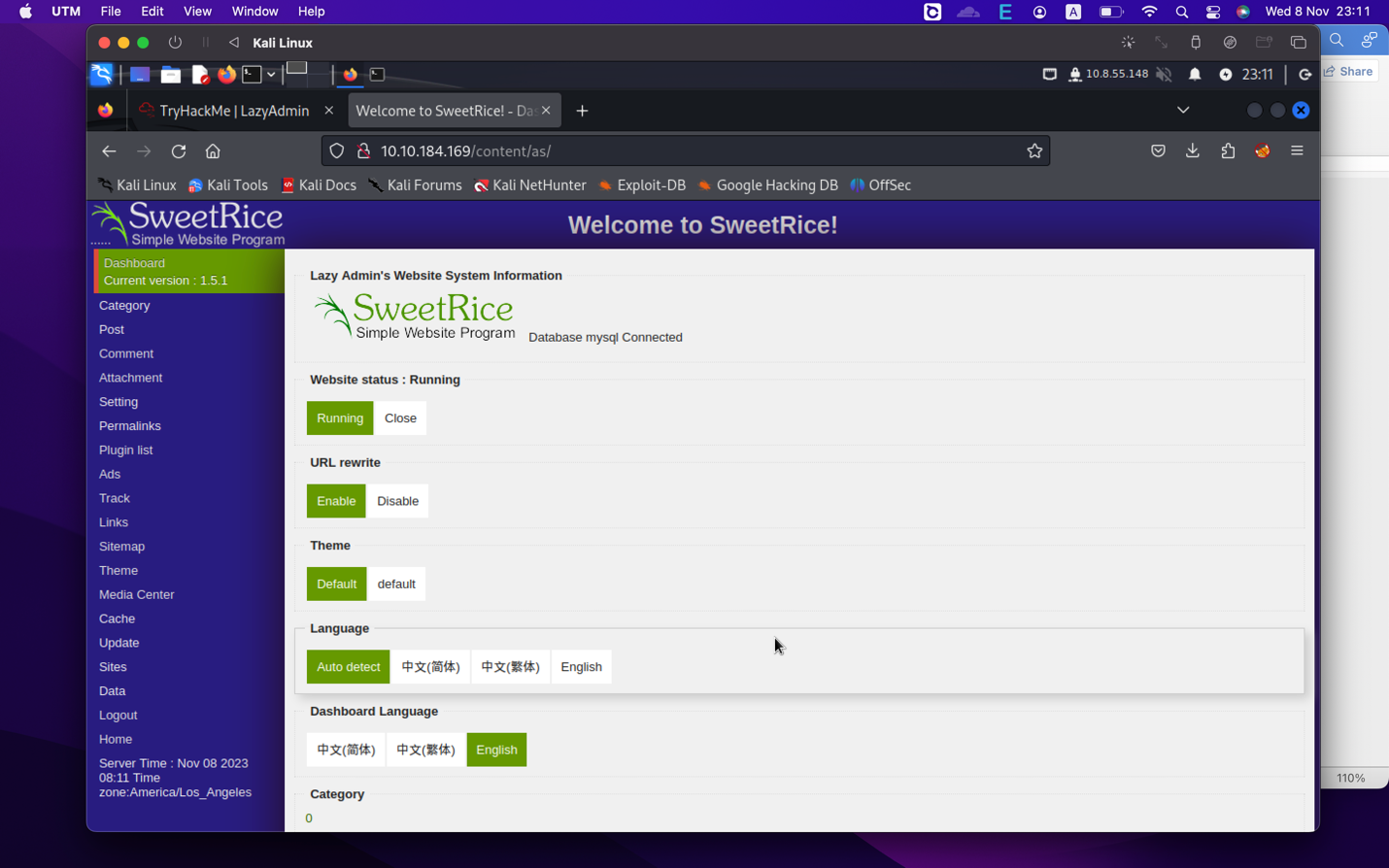
Crack mật khẩu:

hashcat -a 0 -m 0 42f749ade7f9e195bf475f37a44cafcb/usr/share/wordlists/rockyou.txt

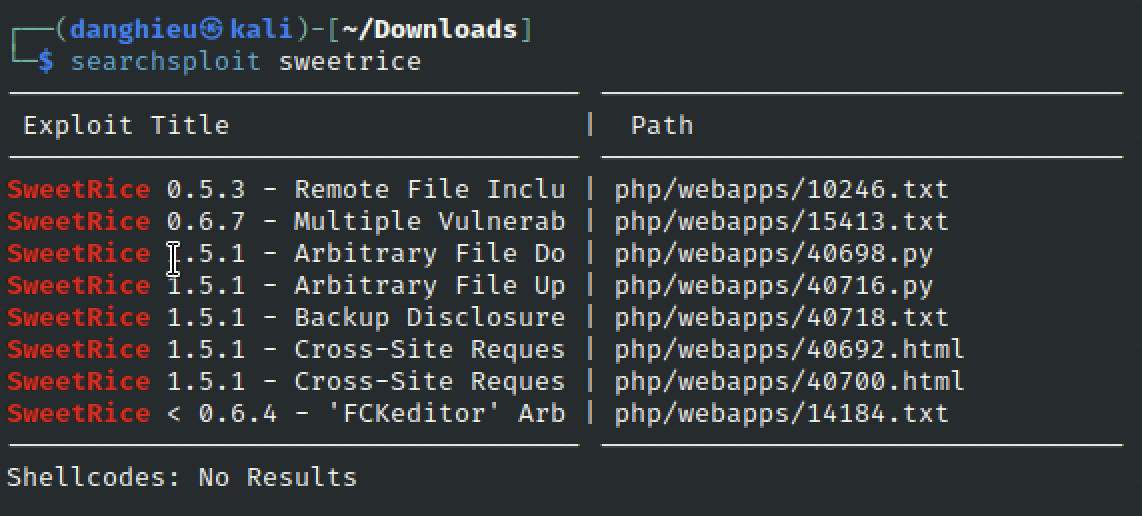


Đăng nhập thành công



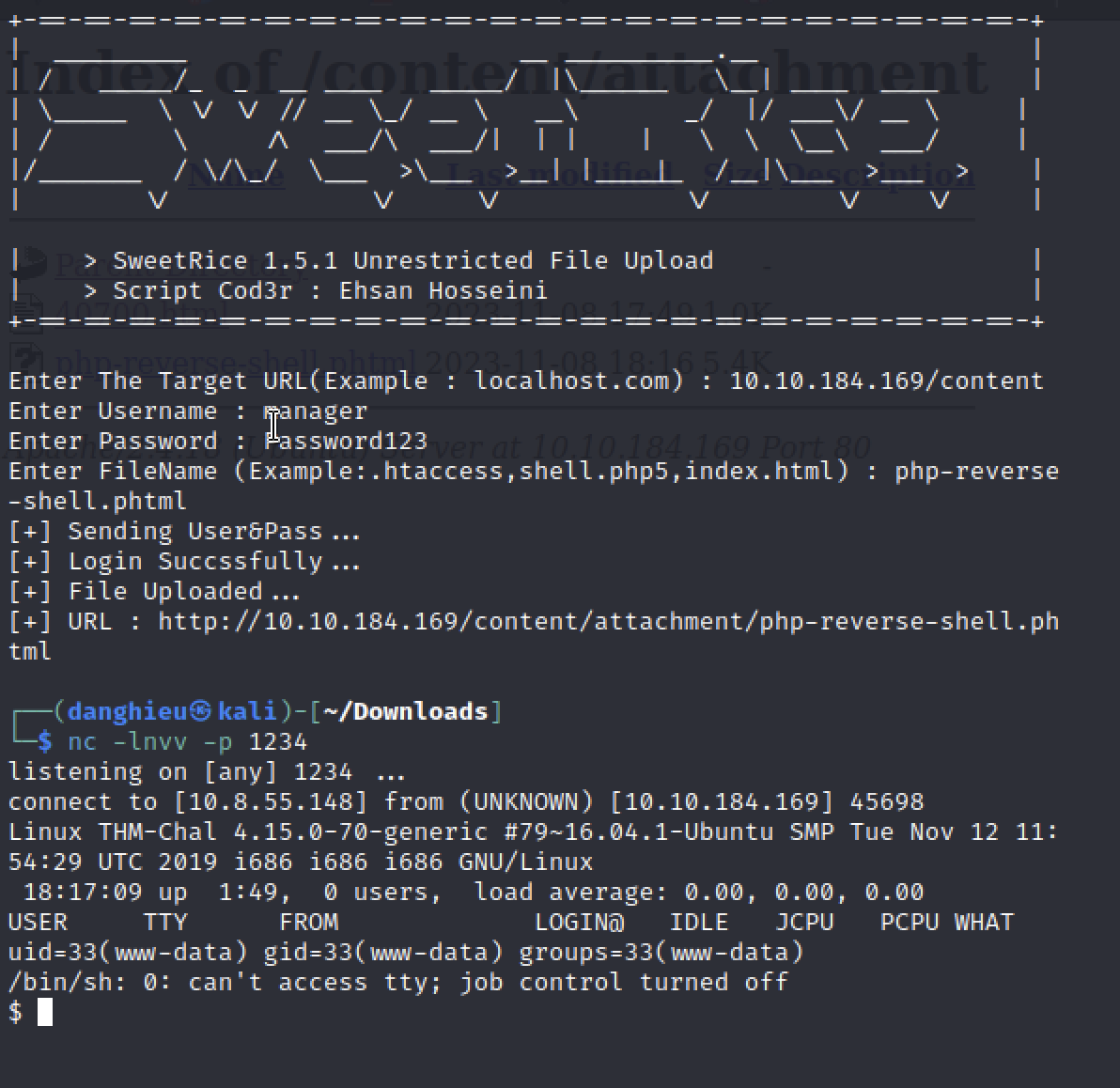


SweetRice current version: 1.5.1



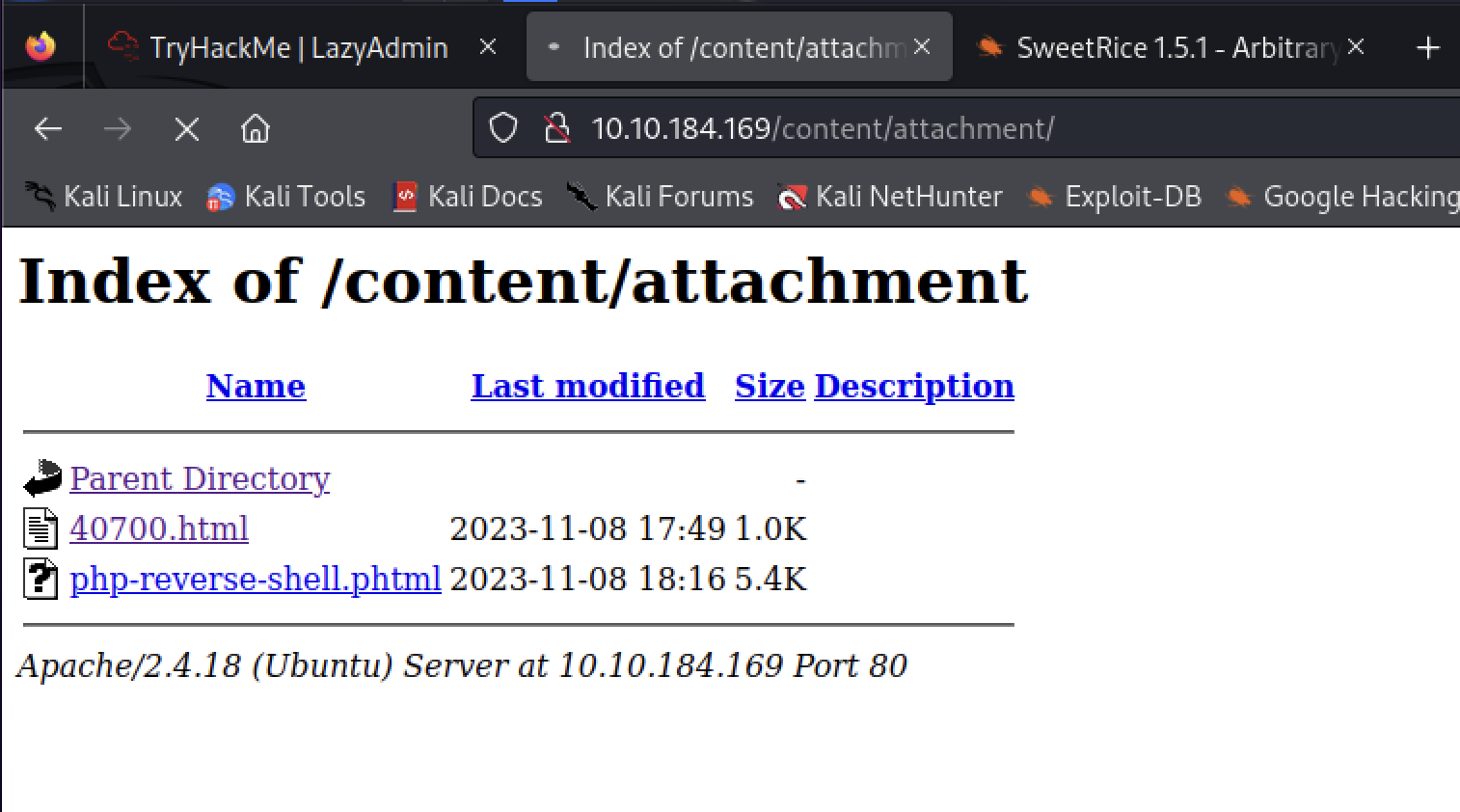
Mình sẽ chọn Arbitrary File Upload để exploit.

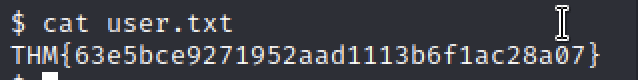


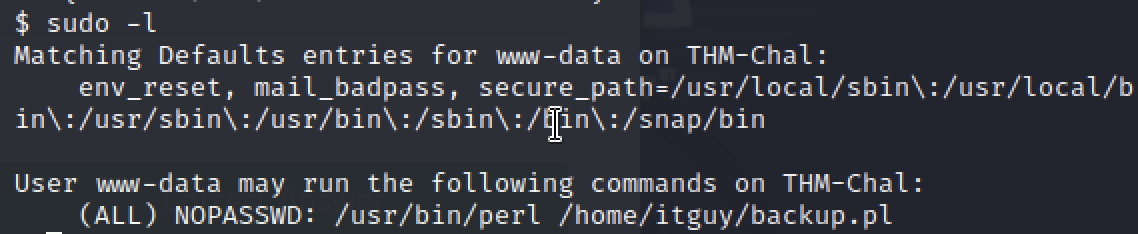


Bạn phải cấu hình đúng thì mới exploit được.

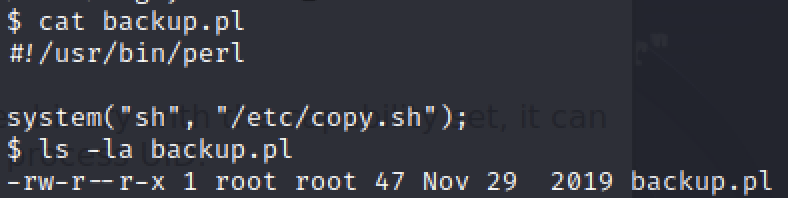
Thực thi reverse-shell ở url /content/attachment/php-reverse-shell.html







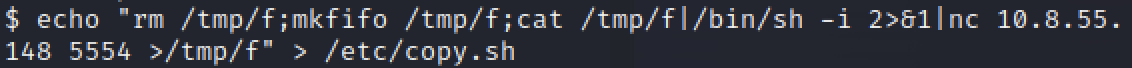
Ý nghĩa: hai file nhị phân nối nhau. Bạn được phép chạy perl backup.pl với quyền root mà không cần mật khẩu.

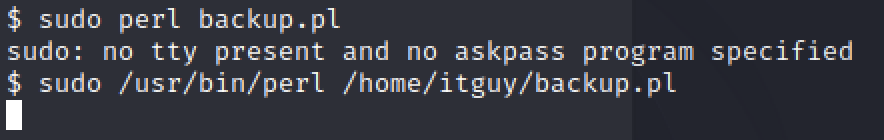


File backup.pl bạn không thể ghi đè nhưng nó lại thực thi tiếp /etc/copy.sh



Chúng ta đã có lệnh ghi, đã có quyền root. Tiếp theo là tiêm reverse-shell. (Đề đã gợi ý)





Không hiểu tại sao lệnh trên lại không được ☺

