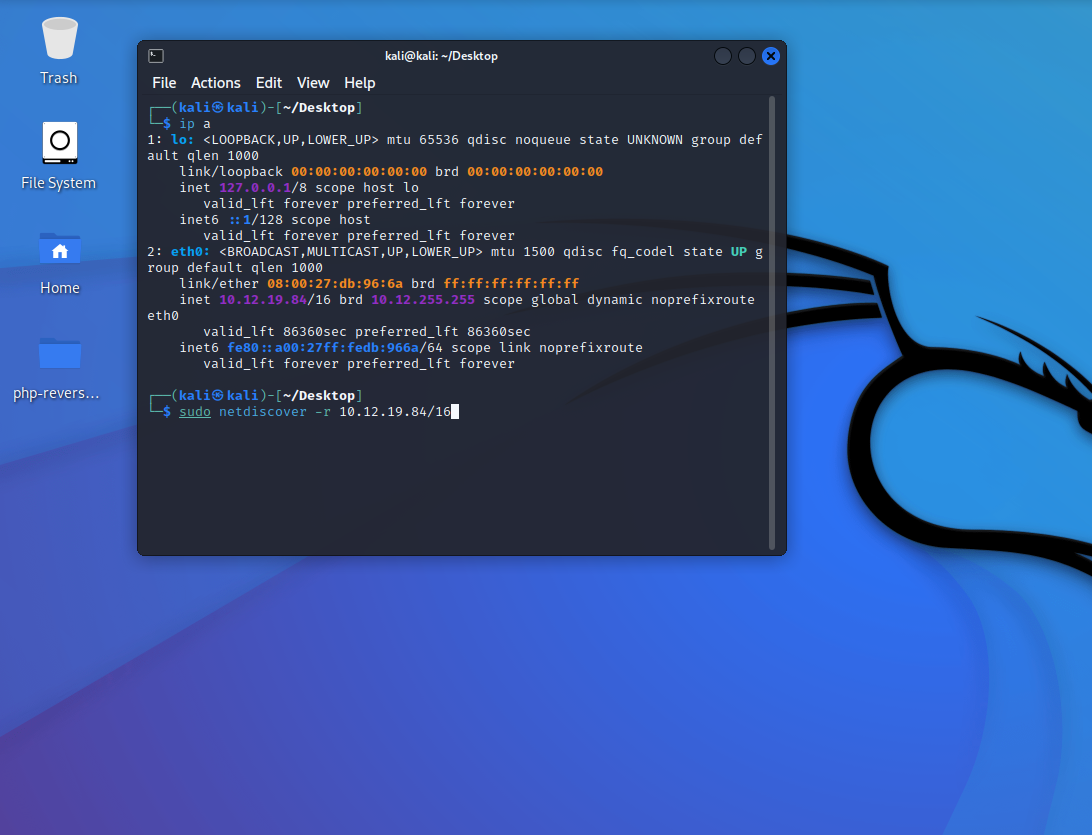
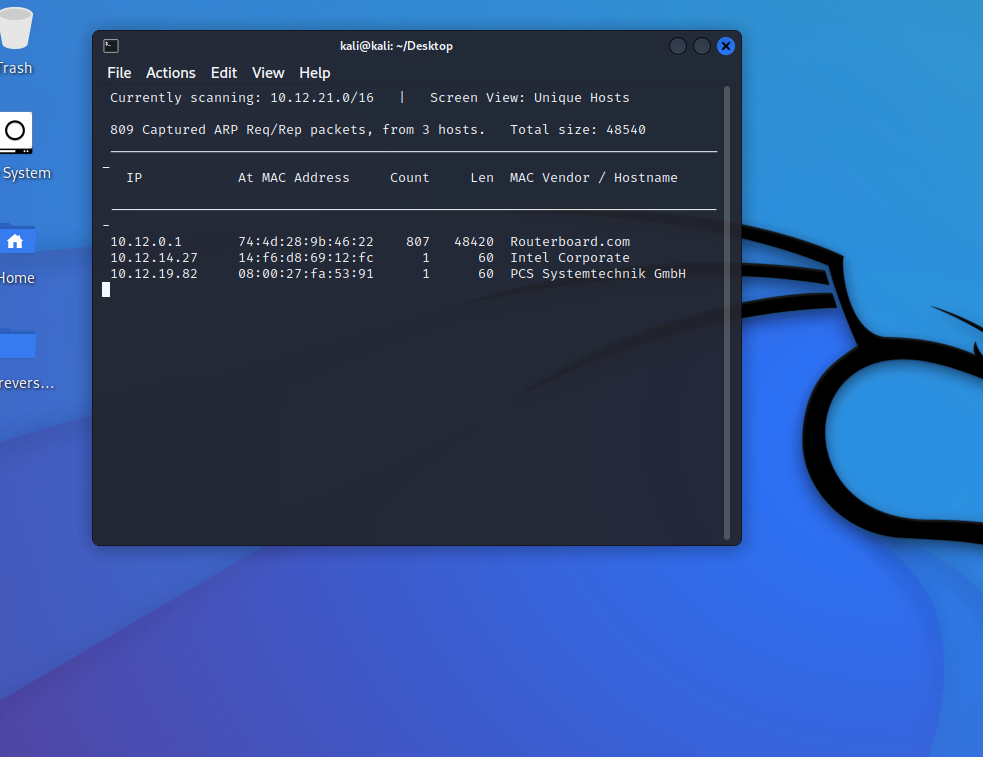
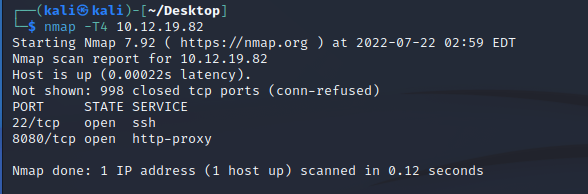
- Dùng netdiscover để dò ip của Mercury

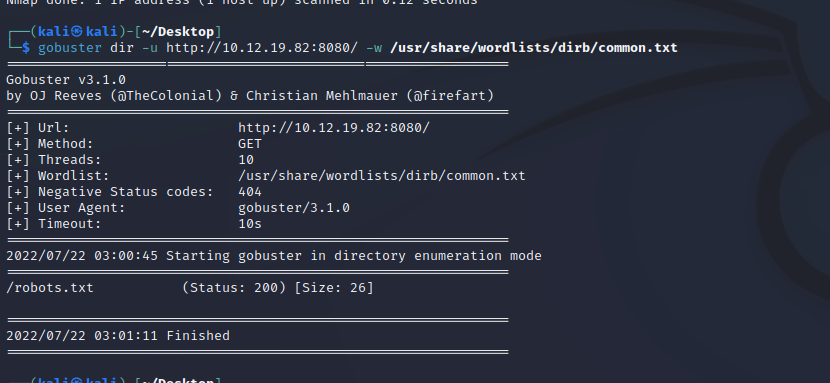




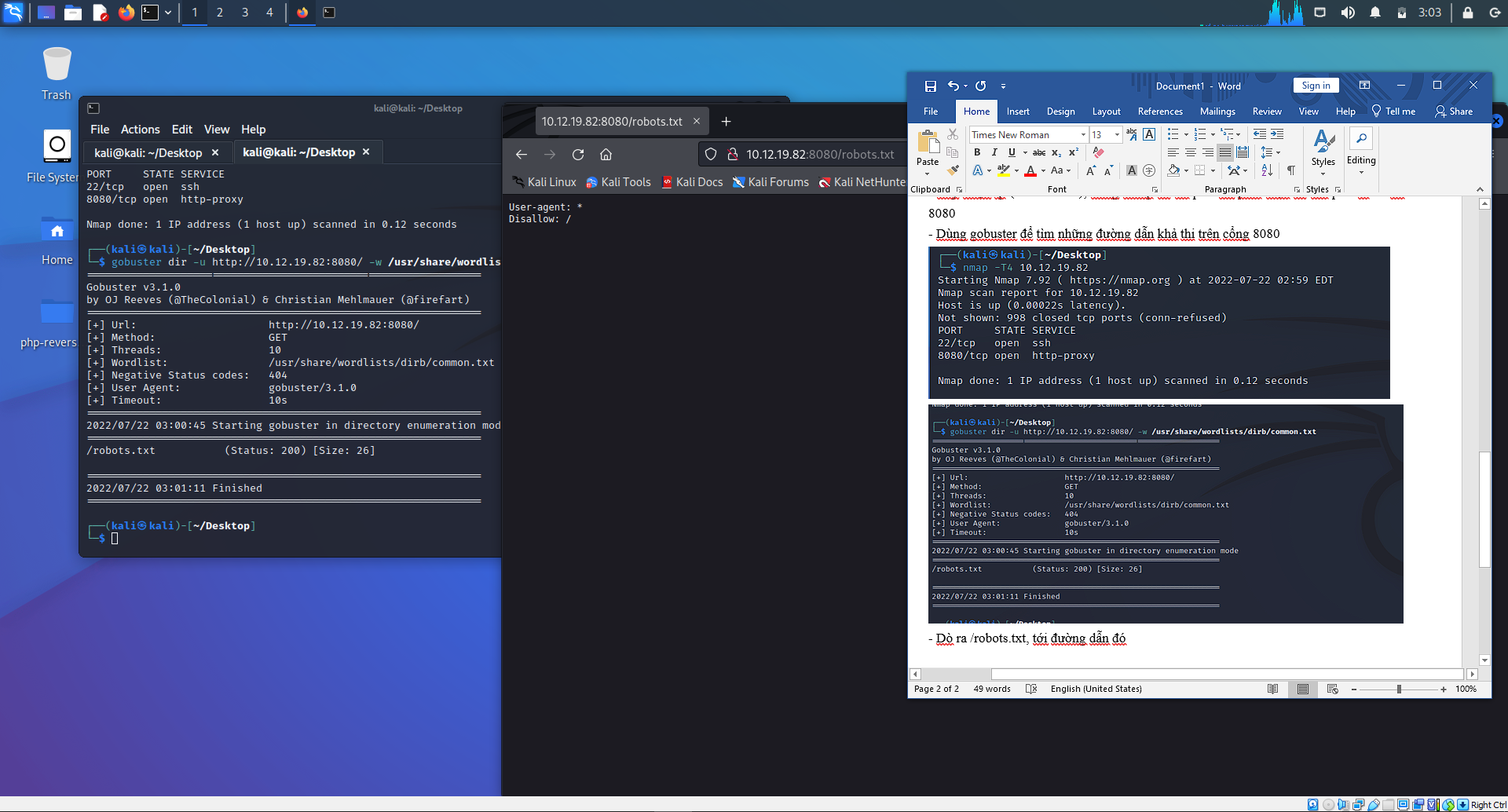
- Lấy được ip (10.12.19.82), dùng nmap để dò port thì phát hiện có hai port là 12 và 8080

- Dùng gobuster để tìm những đường dẫn khả thi trên cổng 8080

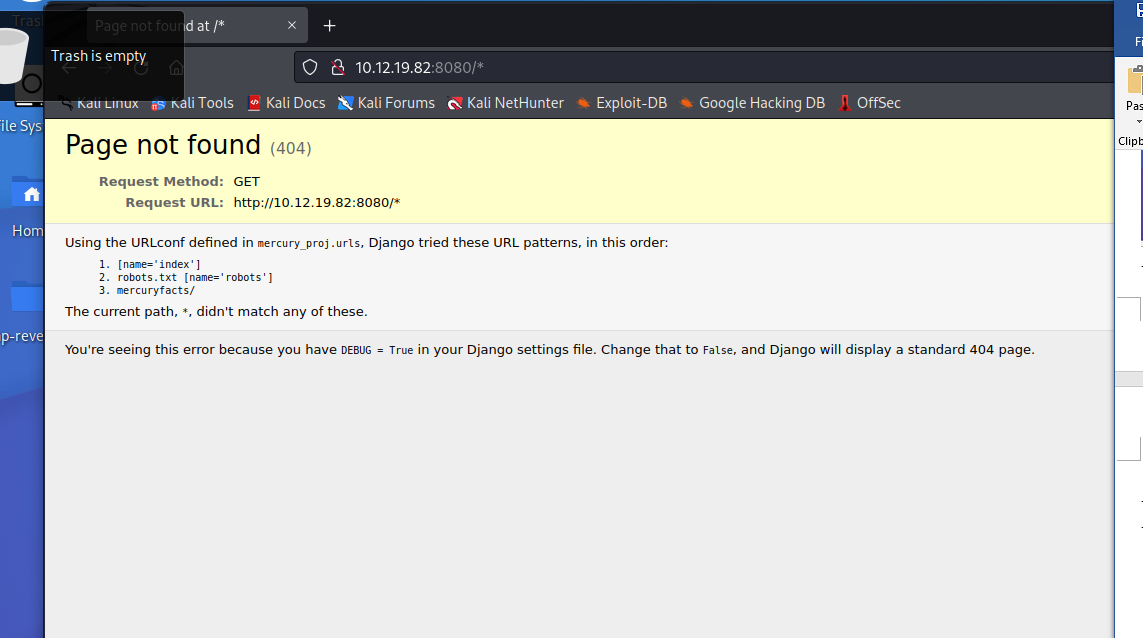




- Dò ra /robots.txt, tới đường dẫn đó

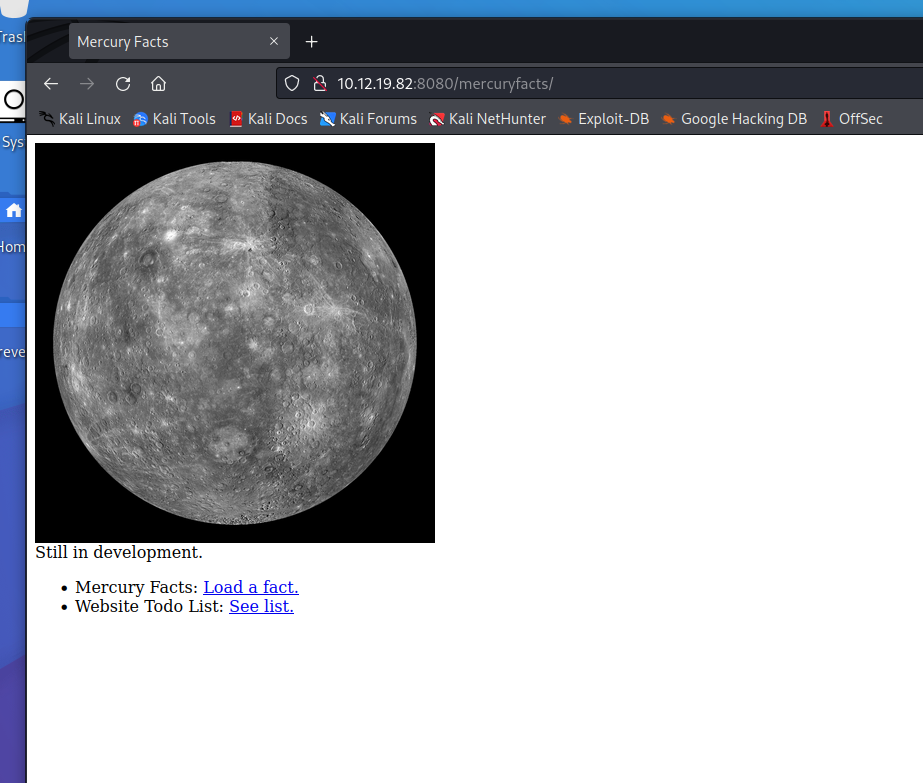


- Thấy có hint, ta thử tới /\*

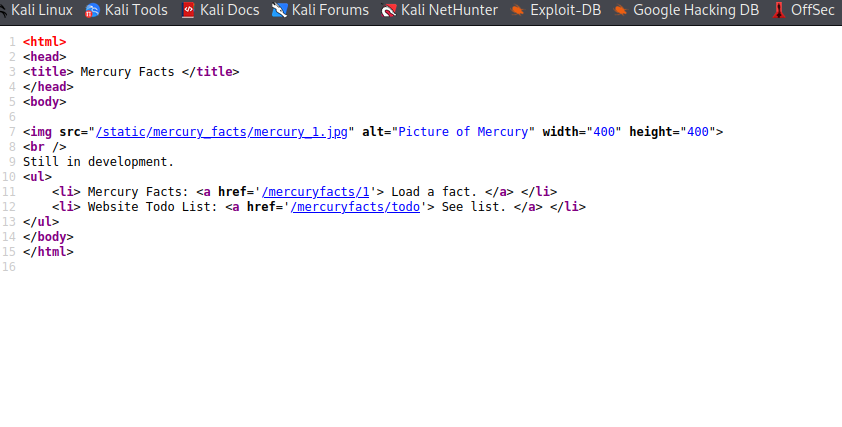


- Phát hiện thêm một đường dẫn /mercuryfacts

- Vào đường dẫn /mercuryfacts

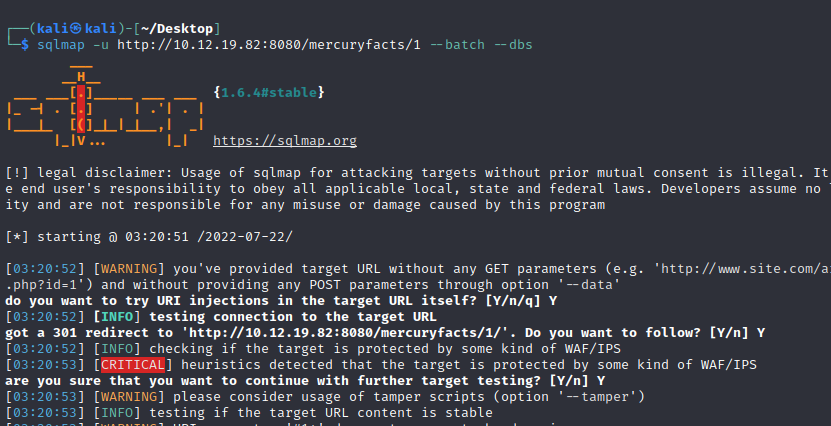


- View page source thì kiểm tra thấy có thêm đường dẫn /todo và /1

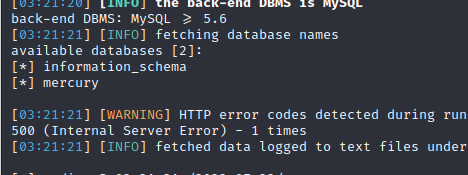


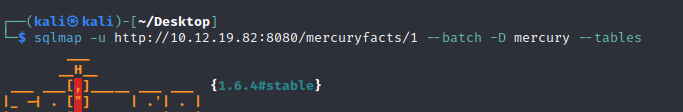
- Vào /mercuryfacts/1

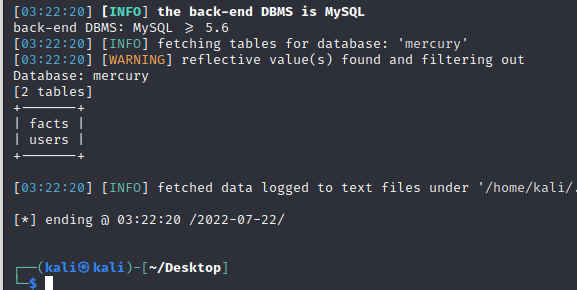
- Dùng sql injection để tìm ra những database đang có



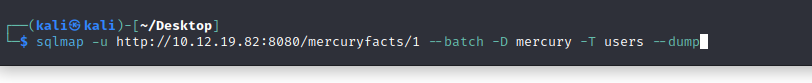
- Dò ra hai database



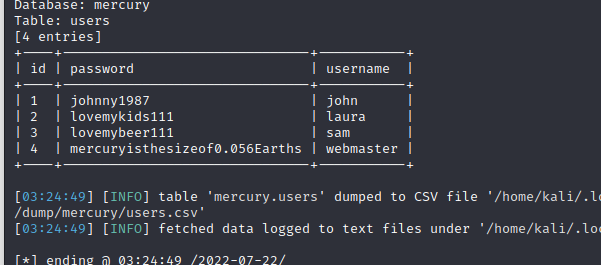
- Vào database mercury và xem table



- Có hai table là facts và users



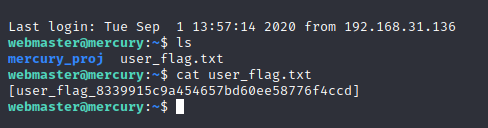
- Vào table users



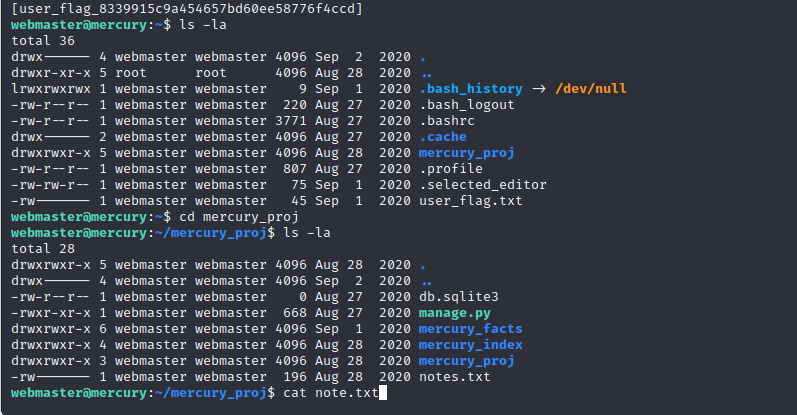
- Có cả username và password

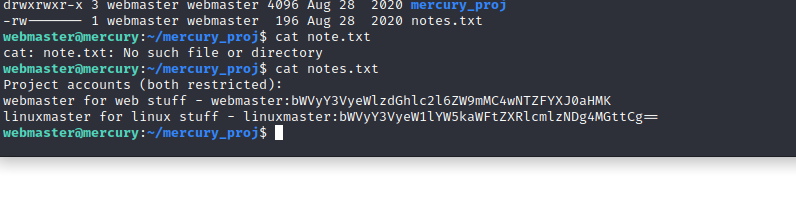
- Thử ssh vào username webmaster

- Tìm được flag đầu tiên

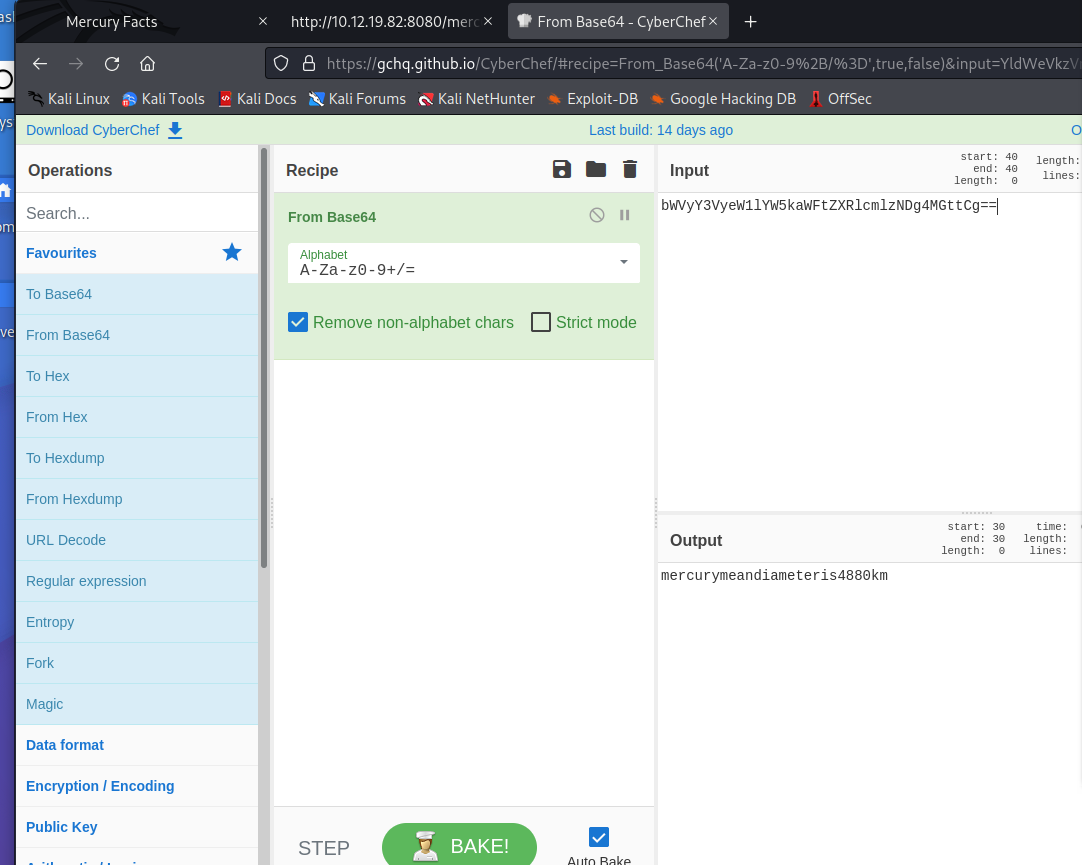


- Kiểm tra xung quanh xem có hint hay không

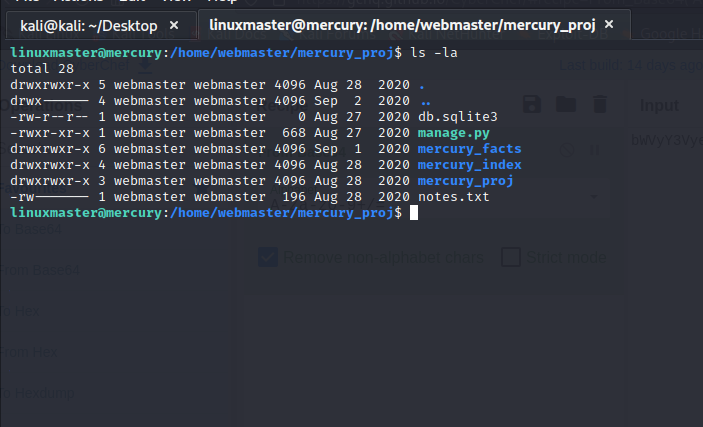




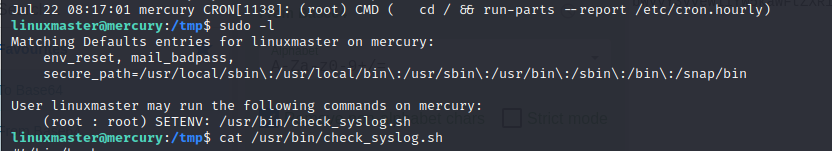
- Dùng cyberchef để crack mật khẩu của linuxmaster



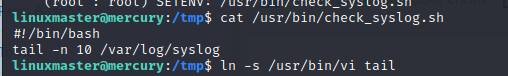
- Đăng nhập vào linuxmaster

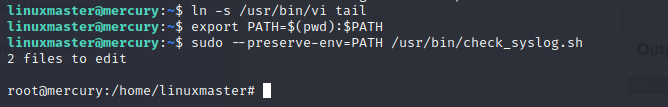


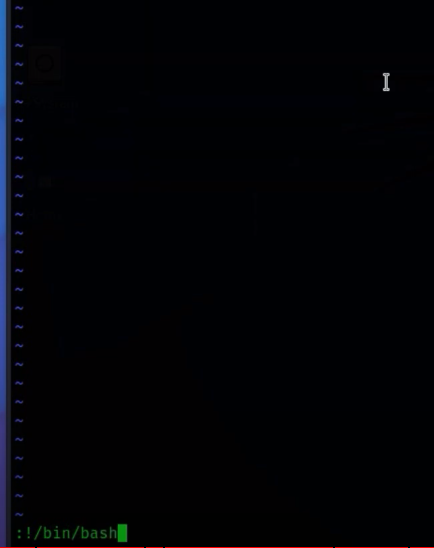
- Dùng sudo -l để kiểm tra các lệnh chạy được dưới quyền sudo



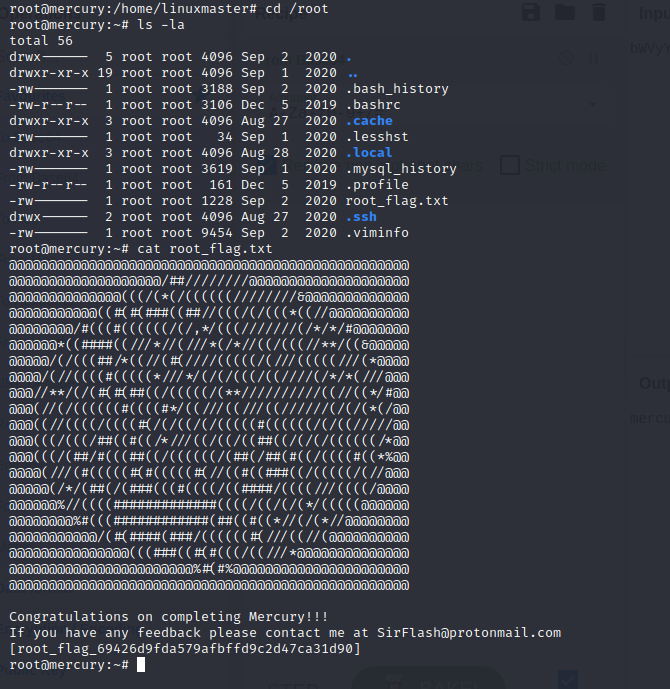
- Ta thử đọc file check\_syslog.sh xem có gì







- Một cách leo thang đặc quyền (Sửa đổi lại file check\_syslog.sh bằng vim)



- Vào thư mục root để lấy flag