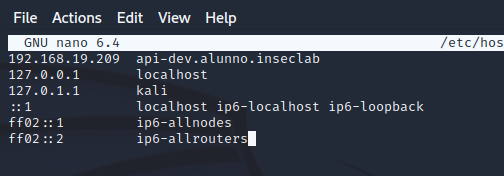
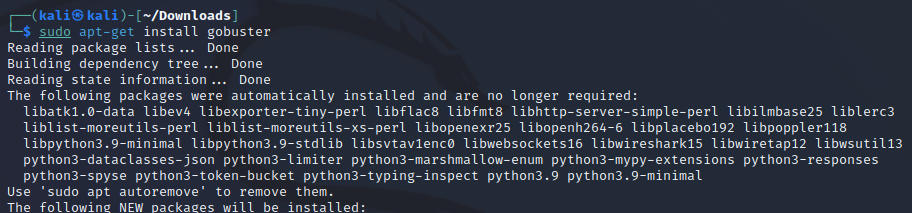
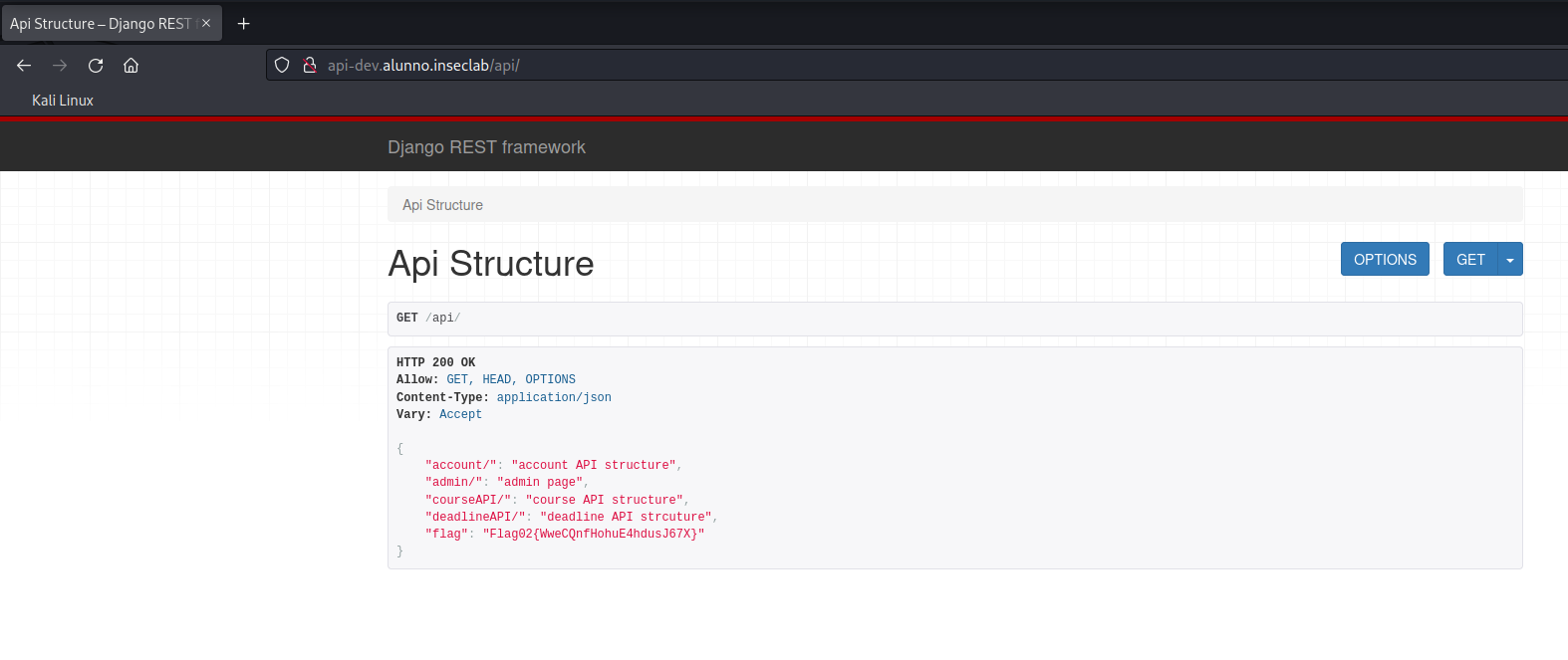
Câu 2:

- Vào sửa file etc/host => quét bằng gobuster => vào server tải trang



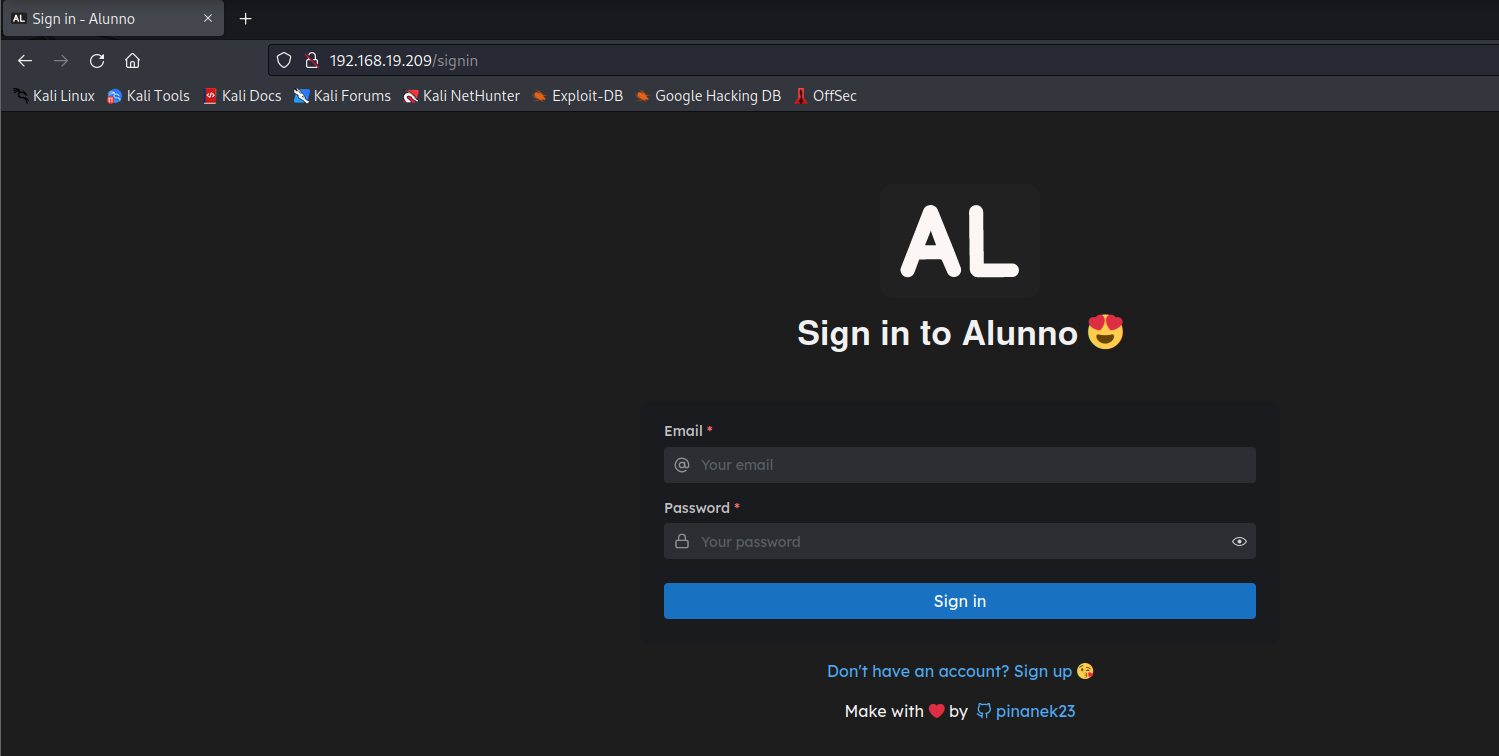


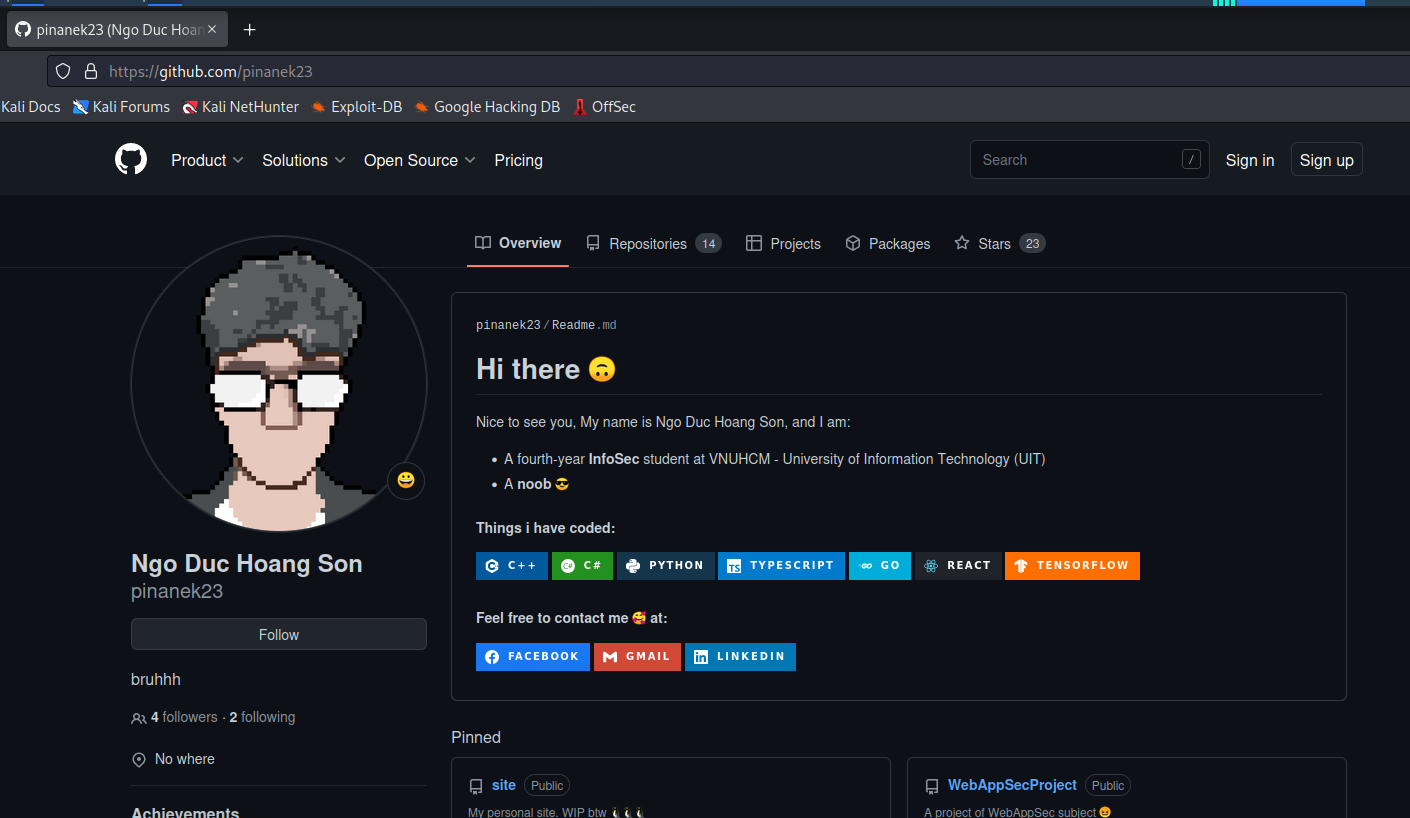


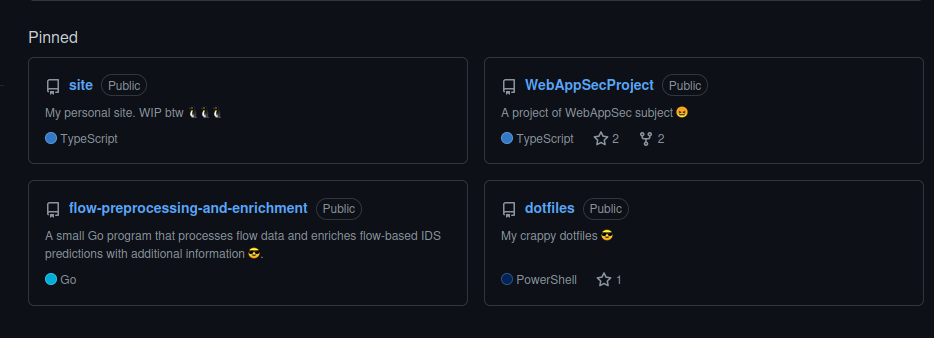


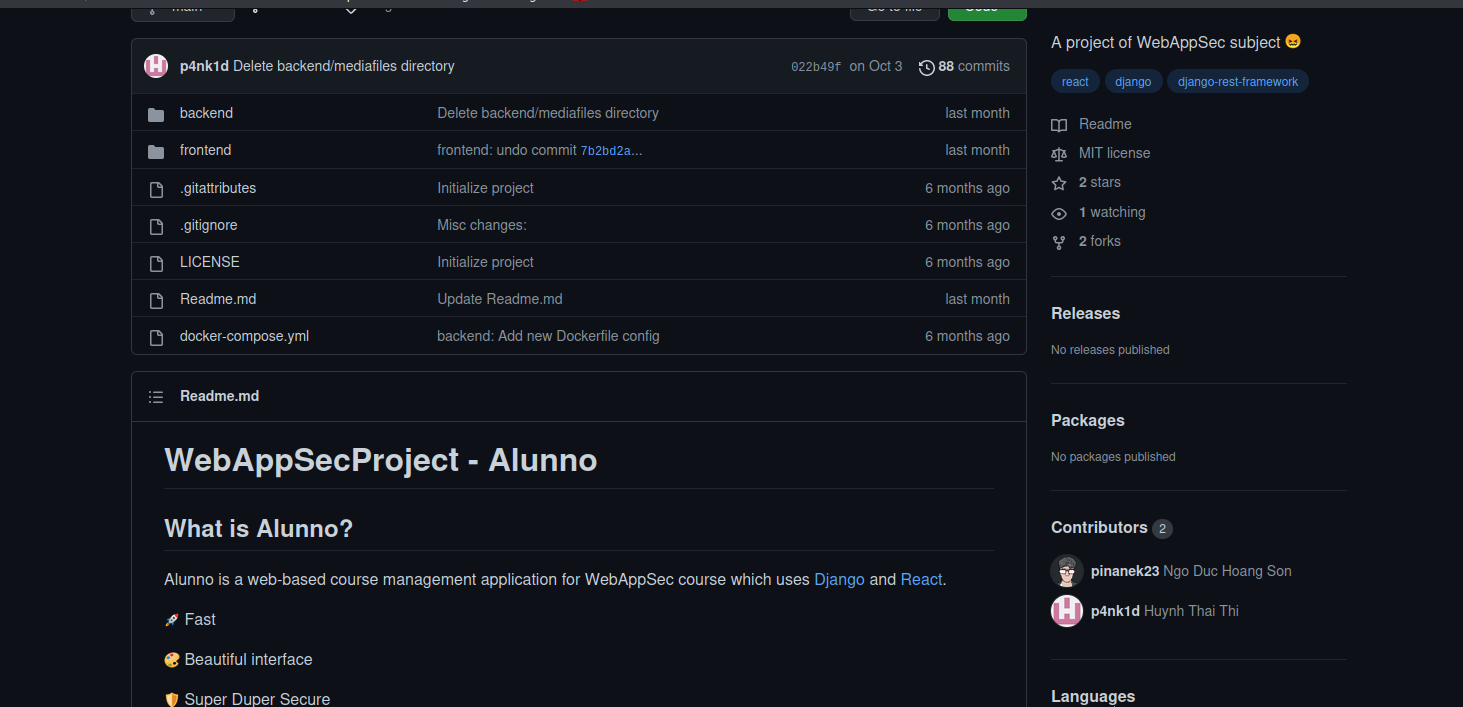
Câu 3:

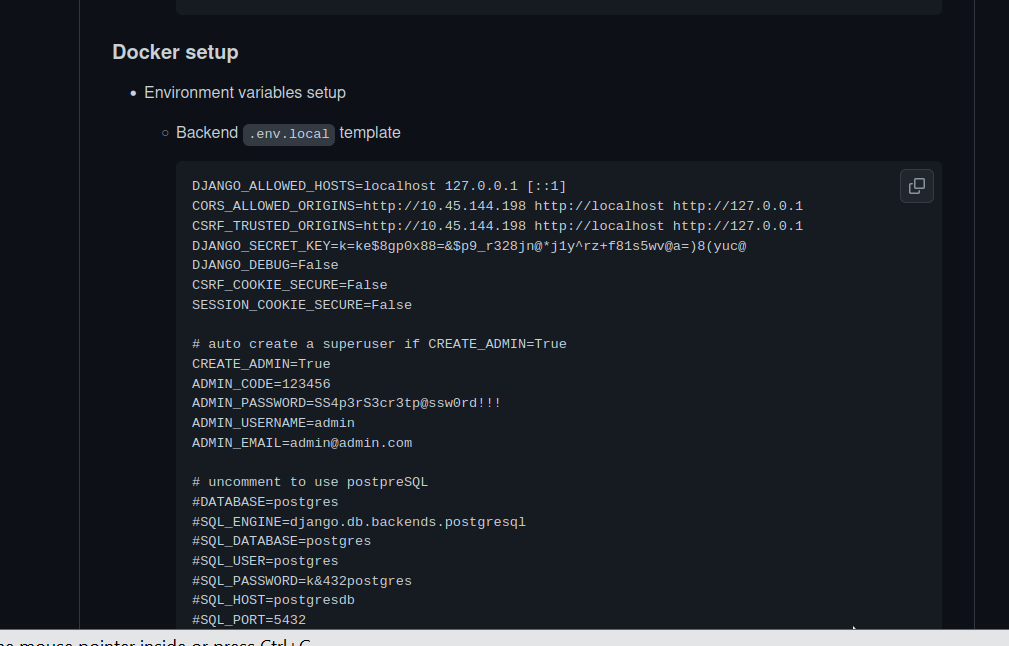
Signin vào server => lấy link guthub ở trang => vào rồi chọn webappsecprojec => lấy pass và email => sữa etc/hosts => quét bằng dirb tới link <http://alunno.inseclab/> => phát hiện được file admin => lấy đường link bỏ vào đăng nhập => nhập mail và pass vào được django => vào member lấy pass

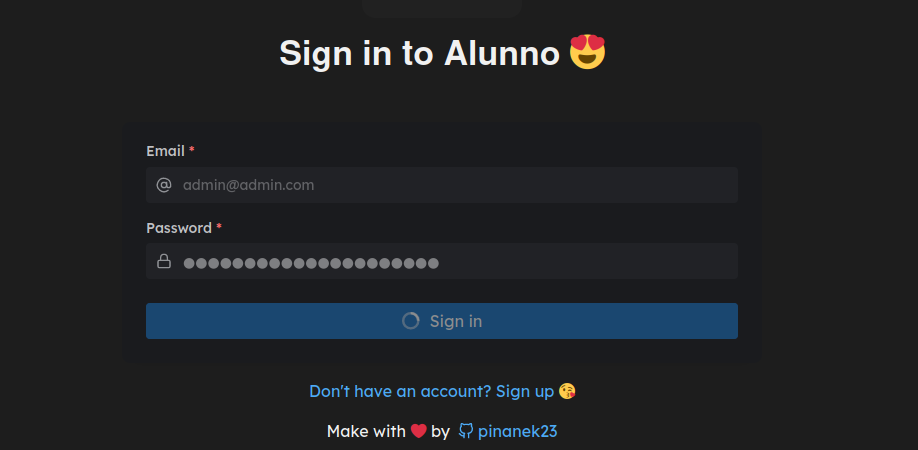


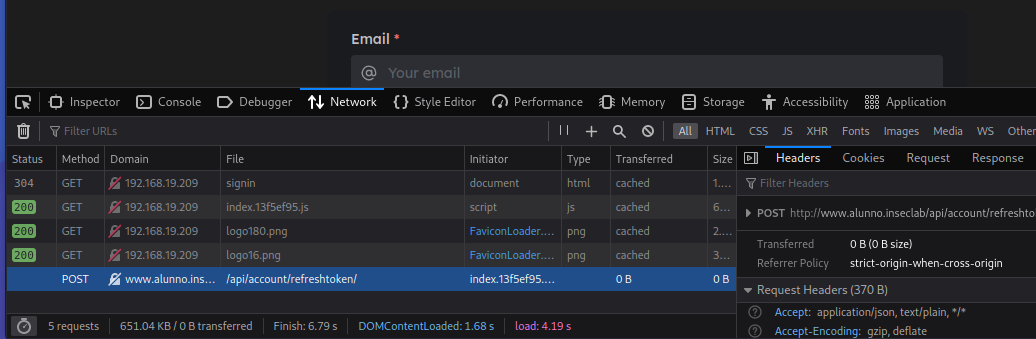


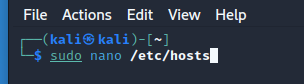


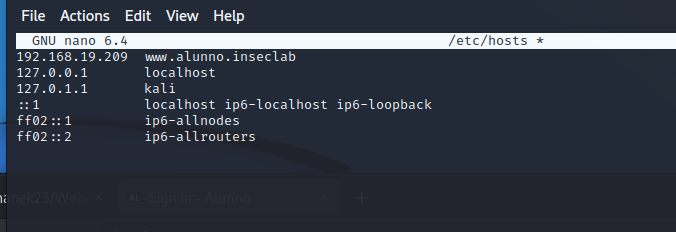


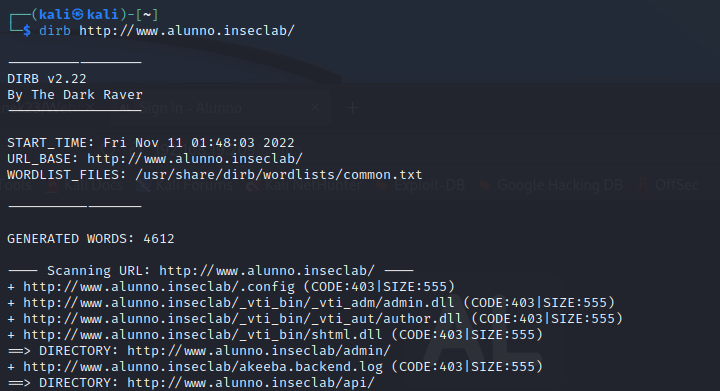


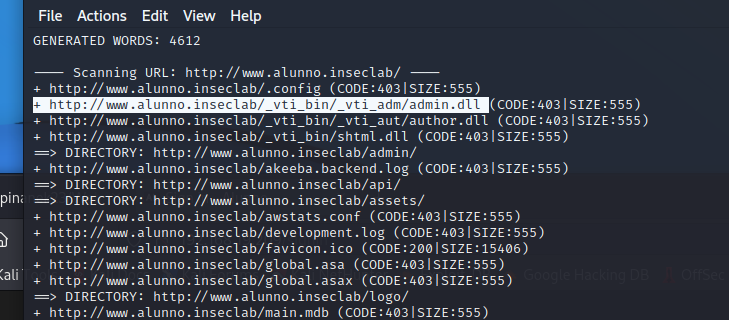


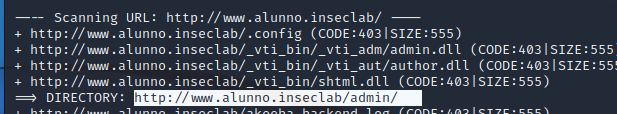


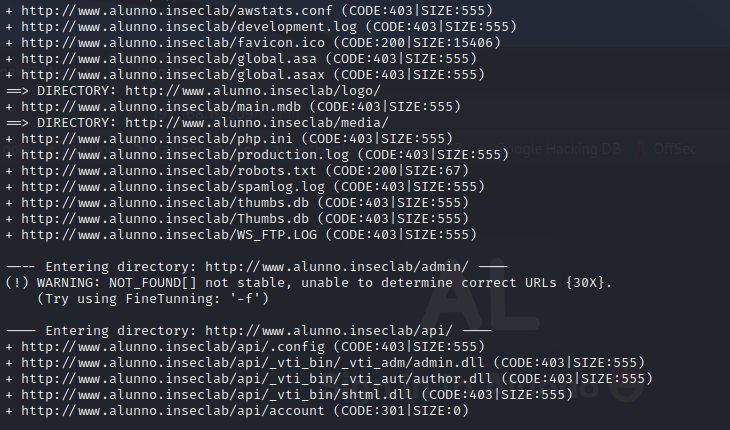


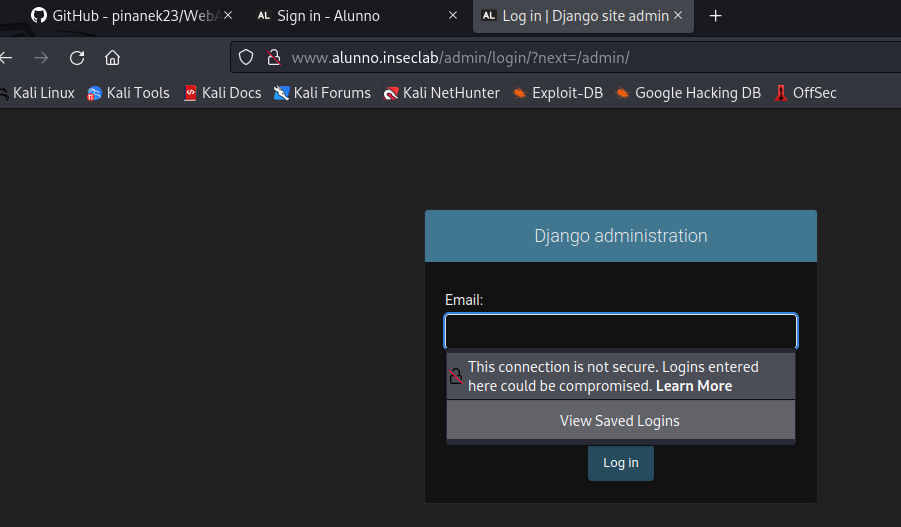


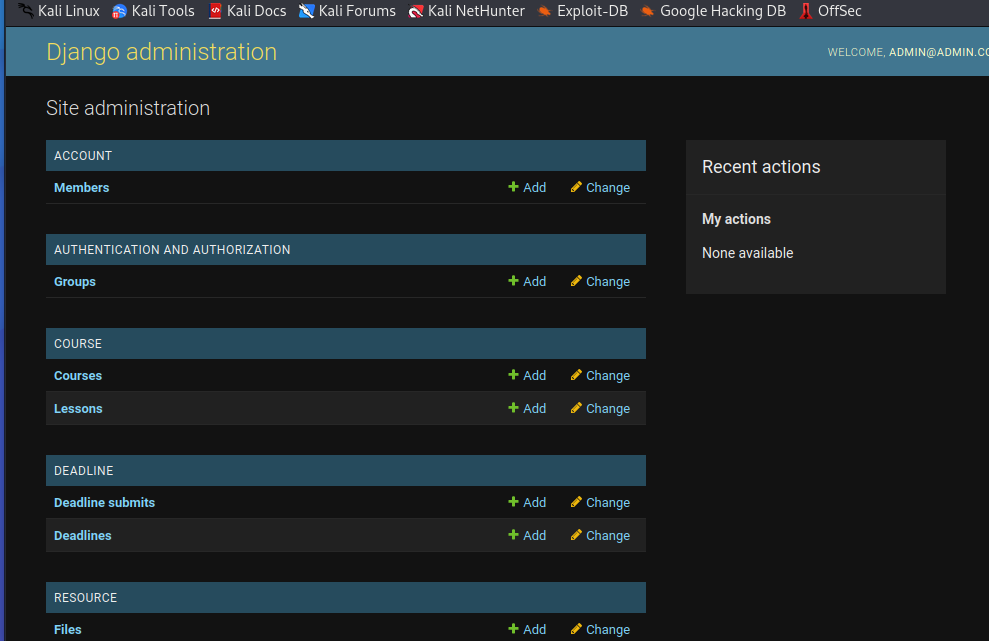




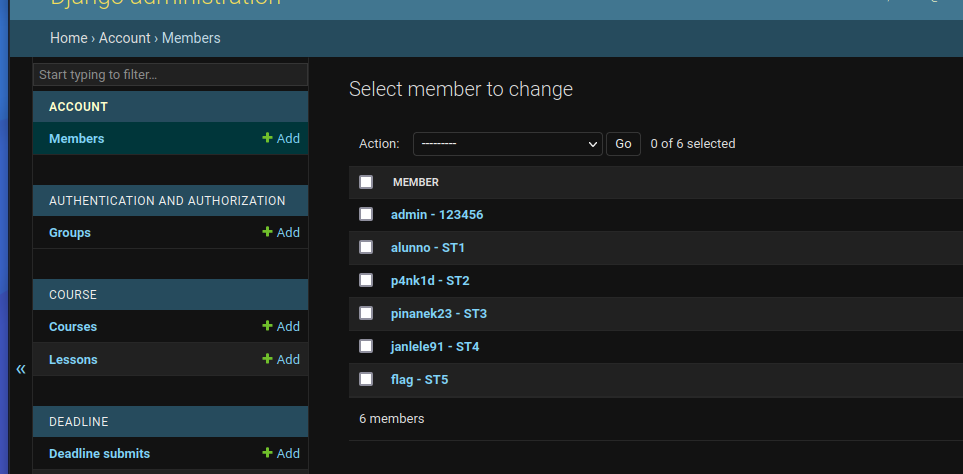


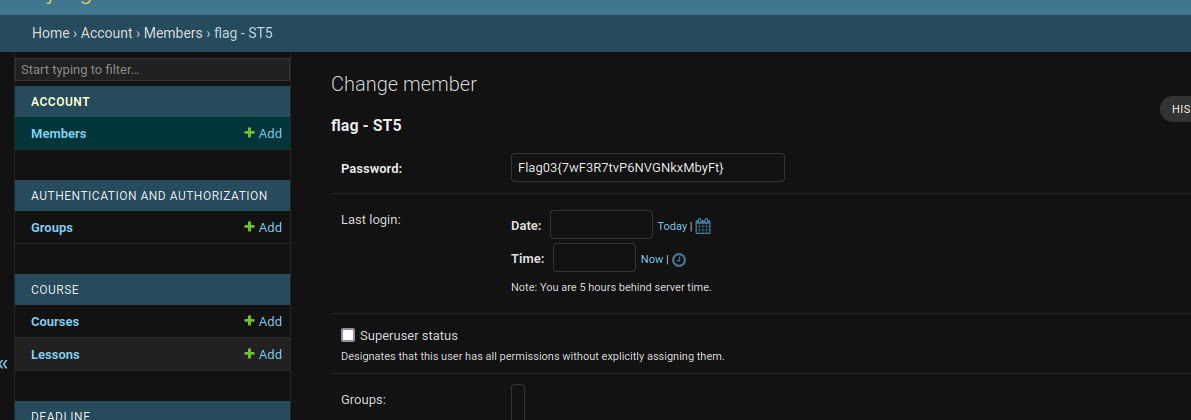




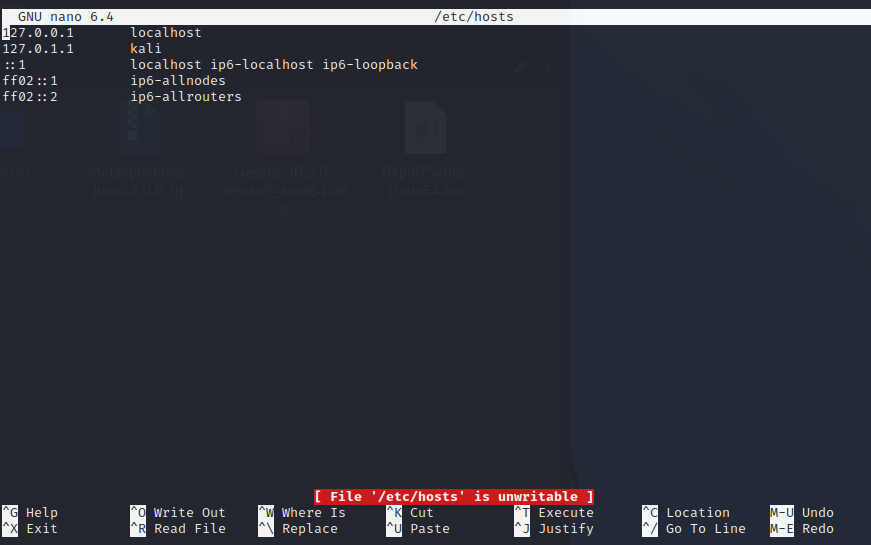


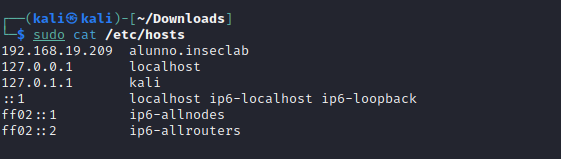
Pass với mk như bên github:





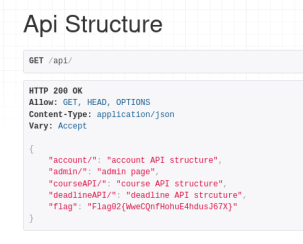
Flag03{7wF3R7tvP6NVGNkxMbyFt}





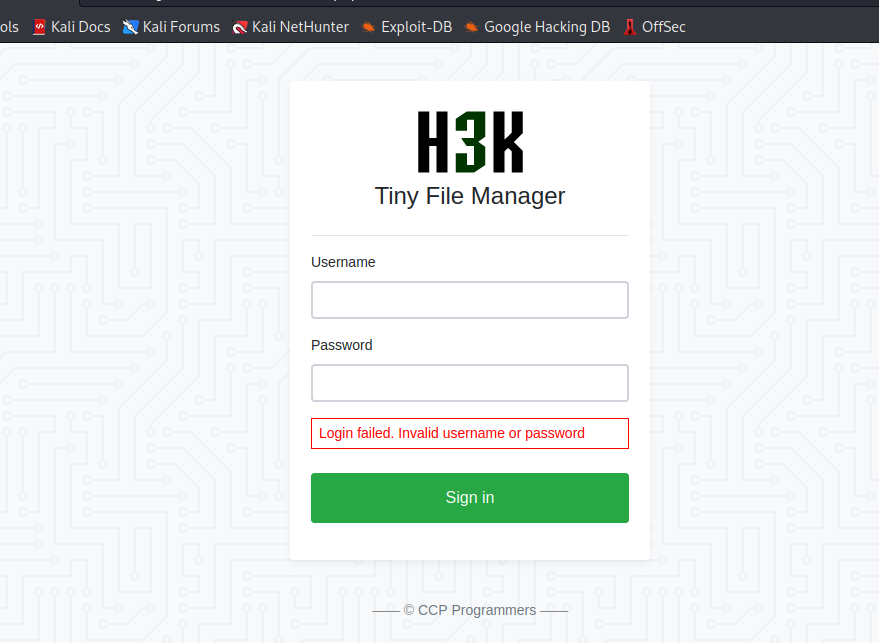
Câu 4:

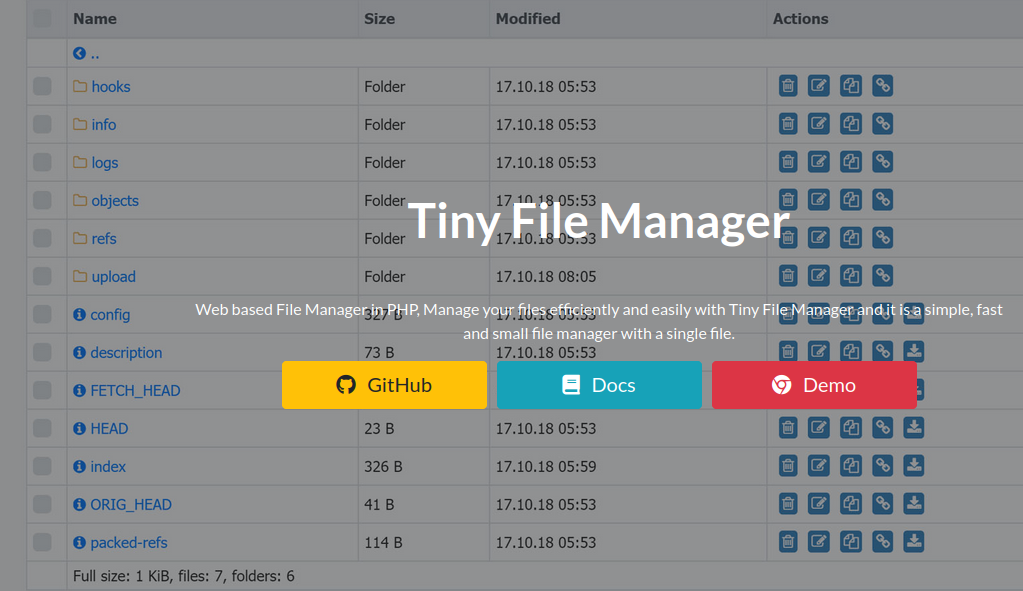
Dựa theo bài 2 => chỉnh lại etc/hosts => nhập lên lại server => lấy user và pass ở github bên trên => tìm trong file index lấy flag 4

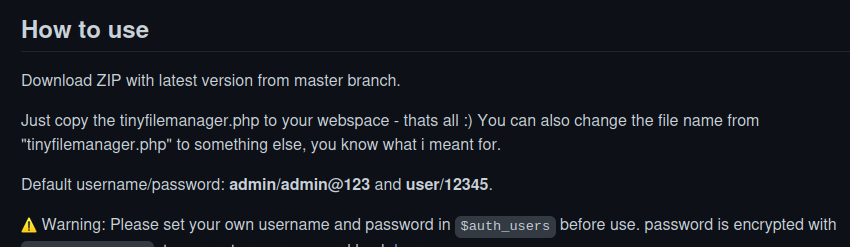


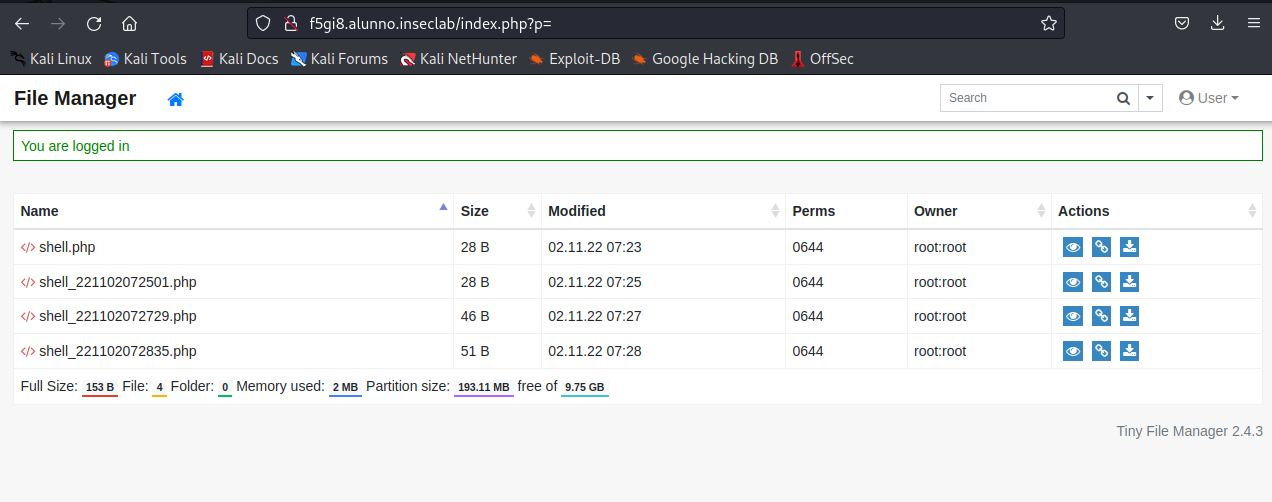
Text

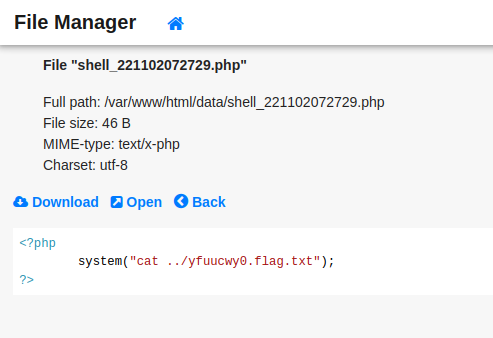
Description automatically generated

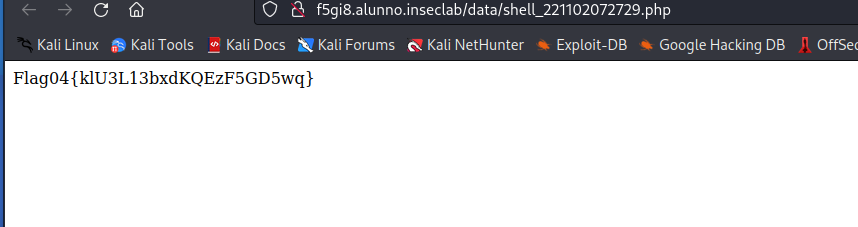












Câu 5+6:

Từ hint thầy với câu 4 => vào user f5gi8.alunno.inseclab => sau khi kiếm ra flag 4 thì sẽ kiếm các file php còn lại => nhận thấy có một file có chứa sshkey.private => lưu key về máy, chỉnh format, và connect ssh với key đó=> thấy được trong các thư mục /var/..., /usr/bin/... =>có chứa các file được tạo cùng ngày và chỉ có 2 file có thể dùng lệnh cat truy cập dc=>và đó là file chứa 2 flag

