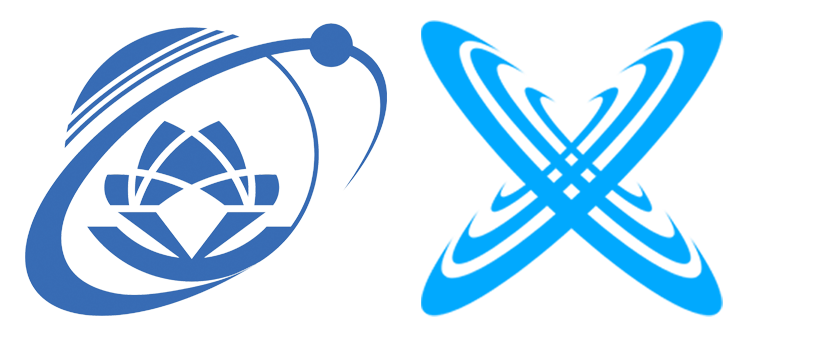
Báo cáo kết quả kiểm thử bảo mật hệ thống CNTT

Quamonthicoten

[20521649@gm.uit.edu.vn](mailto:[20521649@gm.uit.edu.vn) - Vương Đinh Thanh Ngân

[20521690@gm.uit.edu.vn](mailto:20521649@gm.uit.edi.vn) - Lê Minh Nhã



-- Lưu hành nội bộ --

Mục lục

[1.0 Tổng quan 3](#_Toc57241311)

[1.1 Khuyến nghị bảo mật 3](#_Toc57241312)

[2.0 Phương pháp kiểm thử 3](#_Toc57241313)

[2.1 Thu thập thông tin 3](#_Toc57241314)

[2.2 Kiểm thử xâm nhập 4](#_Toc57241315)

[2.2.1 Địa chỉ IP của máy tồn tại lỗ hổng:192.168.19.209 4](#_Toc57241316)

Alunno 1............................................................................................................................................5

Alunno 2............................................................................................................................................6

Alunno 3............................................................................................................................................8

Alunno 4..........................................................................................................................................15

Alunno user.....................................................................................................................................19

[2.3 Duy trì quyền truy cập](#_Toc57241320) 24

[2.4 Xóa dấu vết](#_Toc57241321) 24

# 1.0 Tổng quan

[N11.ATCL.2]-QUAMONTHICOTENđược giao nhiệm vụ thực hiện một bài kiểm tra xâm nhập nội bộ cho hệ thống CNTT đã được chuẩn bị sẵn. Mục tiêu của bài kiểm tra này là thực hiện các cuộc tấn công, tương tự như tấn công của tin tặc và cố gắng xâm nhập vào hệ thống CNTT của tổ chức.

Trong khi thực hiện kiểm tra xâm nhập, có một số lỗ hổng được xác định trên hệ thống CNTT của đơn vị. Khi thực hiện các cuộc tấn công, [N11.ATCL.2]-QUAMONTHICOTENcó thể truy cập vào nhiều máy, chủ yếu là do không cập nhật các bản vá lỗi và cấu hình bảo mật kém. Trong quá trình kiểm thử, [N11.ATCL.2]-QUAMONTHICOTENcó quyền truy cập cấp quản trị vào nhiều máy chủ trong hệ thống. Tất cả máy chủ đều được khai thác thành công và được cấp quyền truy cập. Các máy chủ mà [N11.ATCL.2]-QUAMONTHICOTENcó thể truy cập vào được liệt kê dưới đây

* [192.168.19.201 - 192.168.19.210]

## 1.1 Khuyến nghị bảo mật

[N11.ATCL.2]-QUAMONTHICOTEN khuyến nghị vá các lỗ hổng được xác định trong quá trình kiểm thử để đảm bảo rằng tin tặc không thể khai thác các máy chủ này trong tương lai. Cần lưu ý rằng các máy chủ này cần được vá thường xuyên và nên duy trì chính sách kiểm tra, vá lỗi định kỳ để phát hiện và ngăn chặn các lỗ hổng mới xuất hiện trong tương lai.

# 2.0 Phương pháp kiểm thử

[N11.ATCL.2]-QUAMONTHICOTEN đã sử dụng các phương pháp được áp dụng rộng rãi để quá trình kiểm tra thâm nhập đạt được tính hiệu quả trong việc kiểm tra mức độ an toàn của hệ thống CNTT của đơn vị. Dưới đây là sơ lược về cách [N11.ATCL.2]-QUAMONTHICOTEN có thể xác định và khai thác nhiều loại máy chủ và bao gồm tất cả các lỗ hổng riêng lẻ được tìm thấy..

## 2.1 Thu thập thông tin

Giai đoạn thu thập thông tin của quá trình kiểm thử xâm nhập tập trung vào việc xác định phạm vi kiểm thử. Trong đợt kiểm thử xâm nhập này, [N11.ATCL.2]-QUAMONTHICOTEN được giao nhiệm vụ khai thác vào các máy chủ với địa chỉ IP cụ thể là:

**Địa chỉ IP máy kẻ tấn công:**

* 192.168.238.129

**Địa chỉ IP của máy nạn nhân:**

* 192.168.19.201 - 192.168.19.210

## 2.2 Kiểm thử xâm nhập

Giai đoạn kiểm thử xâm nhập tập trung vào việc chiếm quyền kiểm soát vào nhiều loại máy chủ. Trong đợt kiểm thử xâm nhập này, [N11.ATCL.2]-QUAMONTHICOTEN đã có thể truy cập thành công vào 5 trong số 9 máy chủ.

### 2.2.1 Địa chỉ IP của máy tồn tại lỗ hổng: 192.168.19.201 - 192.168.19.210

#### *\*Các Flag Bonus vui lòng trình bày tích hợp trong phần khởi tại shell với quyền user người dùng và leo thang đặc quyền.*

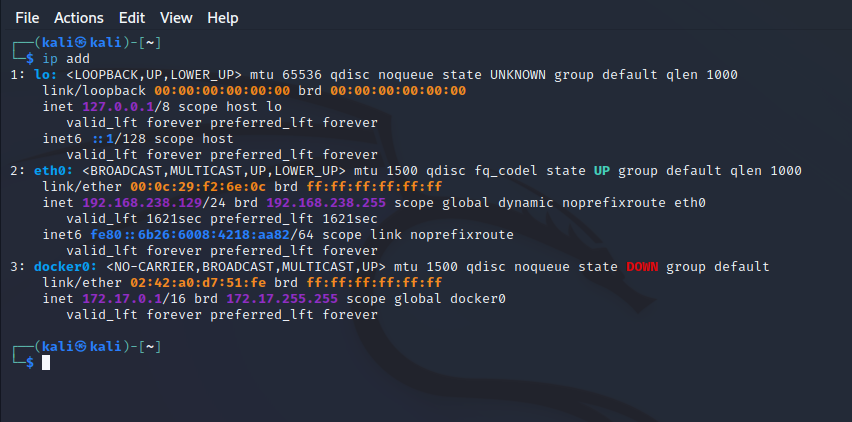
#### Khởi tạo shell với quyền user thường

**Giải thích lỗ hổng**: Quét thông tin

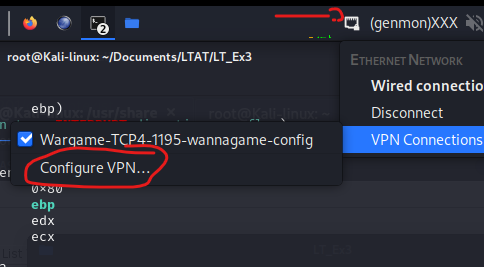
- Thực hiện khai thác lỗ hổng trên máy chạy kali linux

- Tải file đính kèm trên trang wanna CTF

- Cấu hình và bật kết nối onevpn để thực hiện



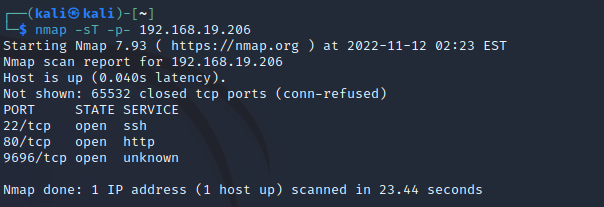
Hình 1: Ip máy kali sử dụng



Hình 2: Kết nối tới VPN

**Alunno 1:**

- Em thực hiện nmap để quét các port đang mở của máy nạn nhân với các option -sT và à option -p- để scan tất cả port ẩn của máy nạn nhân



- Sau đó em thực hiện nc tới máy nạn nhận với cổng vừa nhận được thì tìm ra flag

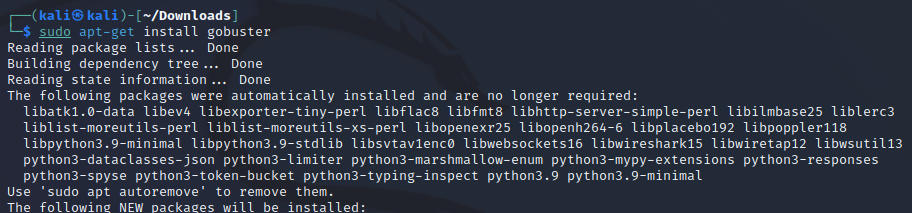


**Alunno 2:**

- Hint đã cho bao gồm gobuster, dns, vhost nên em thực hiện thử quét theo từng option dns và vhost tuy nhiên với vhost thì em quét sử dụng chung với wordlist:

<https://github.com/cujanovic/Virtual-host-wordlist/blob/master/virtual-host-wordlist.txt> .

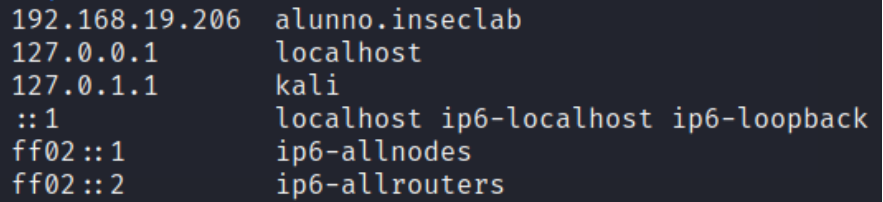
- Cài đặt gobuster



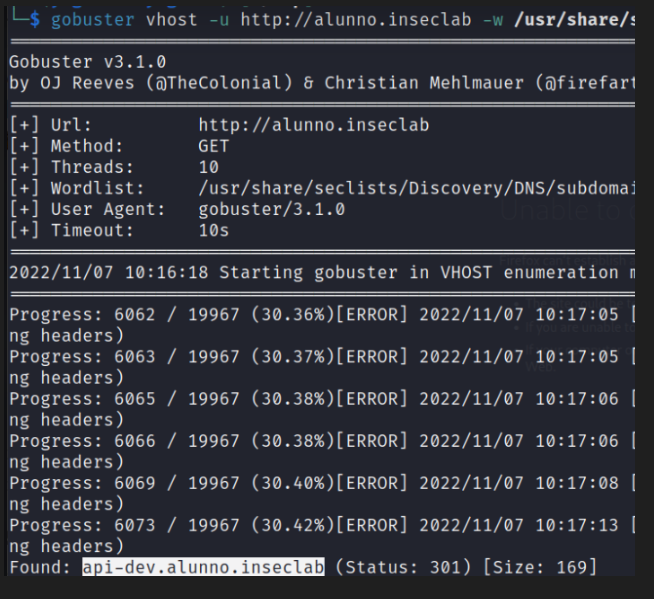
- Trước khi quét thì em sẽ vào etc/host để điều chỉnh thông tin



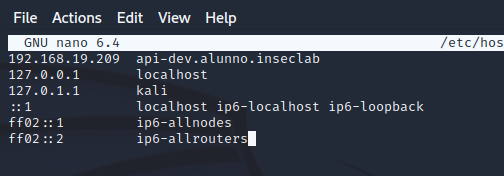
- Em đã điều chỉnh như sau:



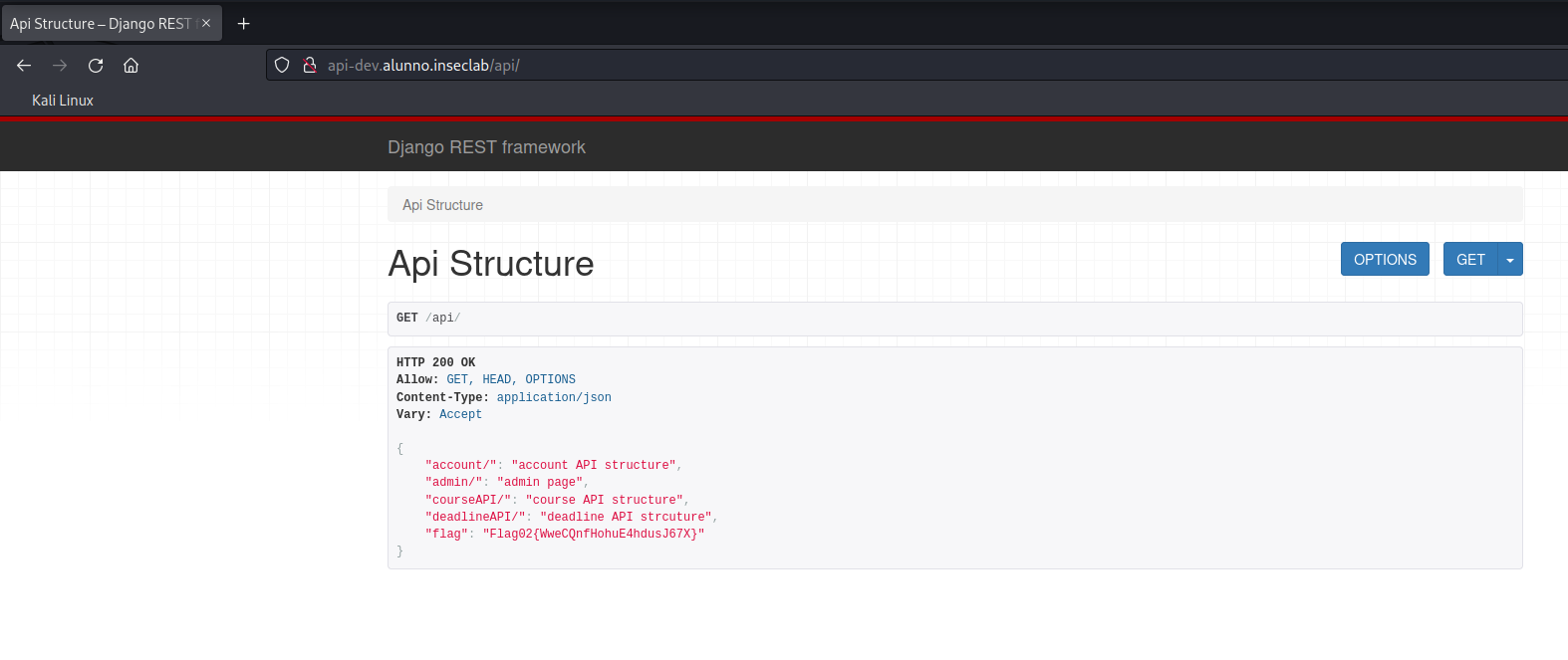
- Thực hiện quét



- Thực hiện quét sau khi điều chỉnh thì em phát hiện ra được thêm api-dev nên lại điều chỉnh etc/hosts thành:

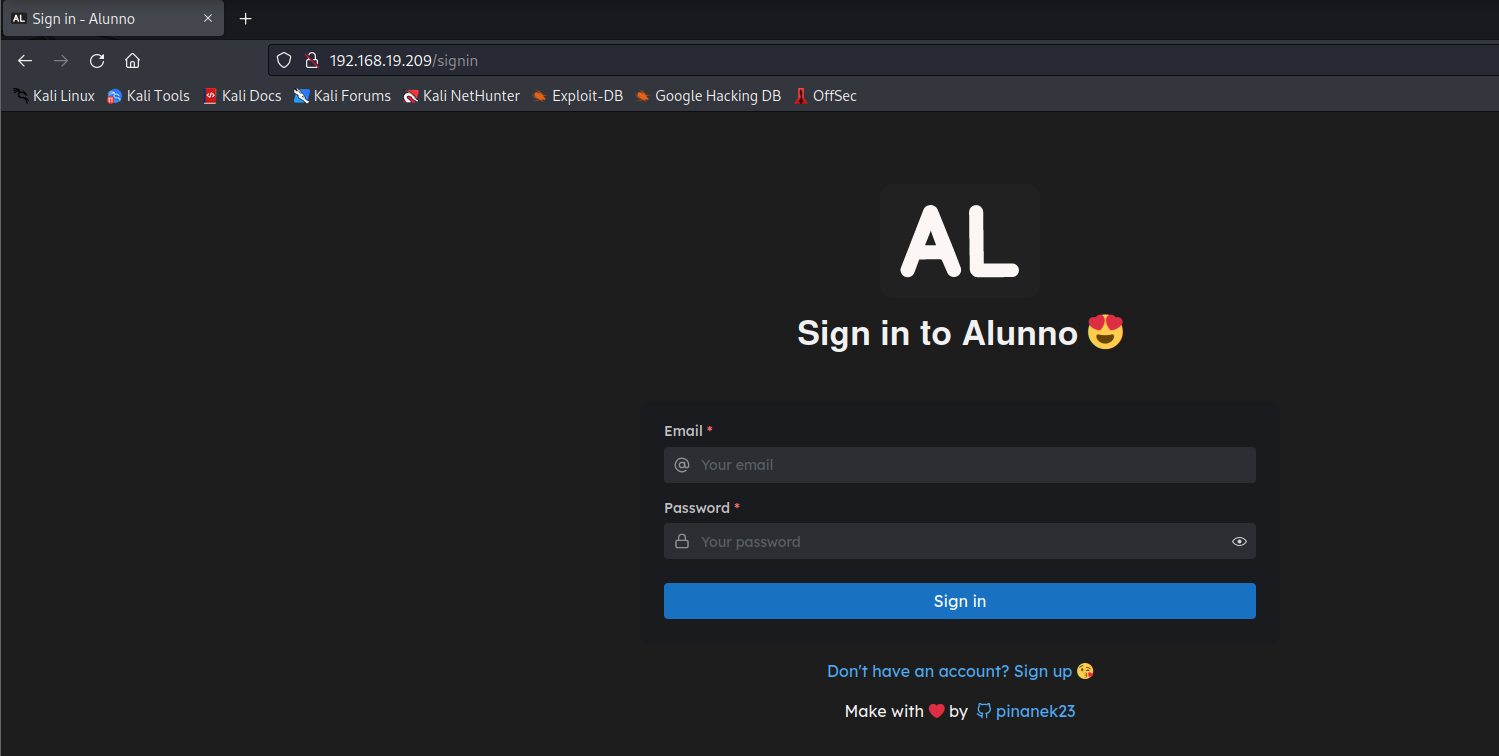


- Sau đó em sẽ nhập vhost cùng domain của trang web vào server và đã được redirect đến dir API thì tìm ra được flag2

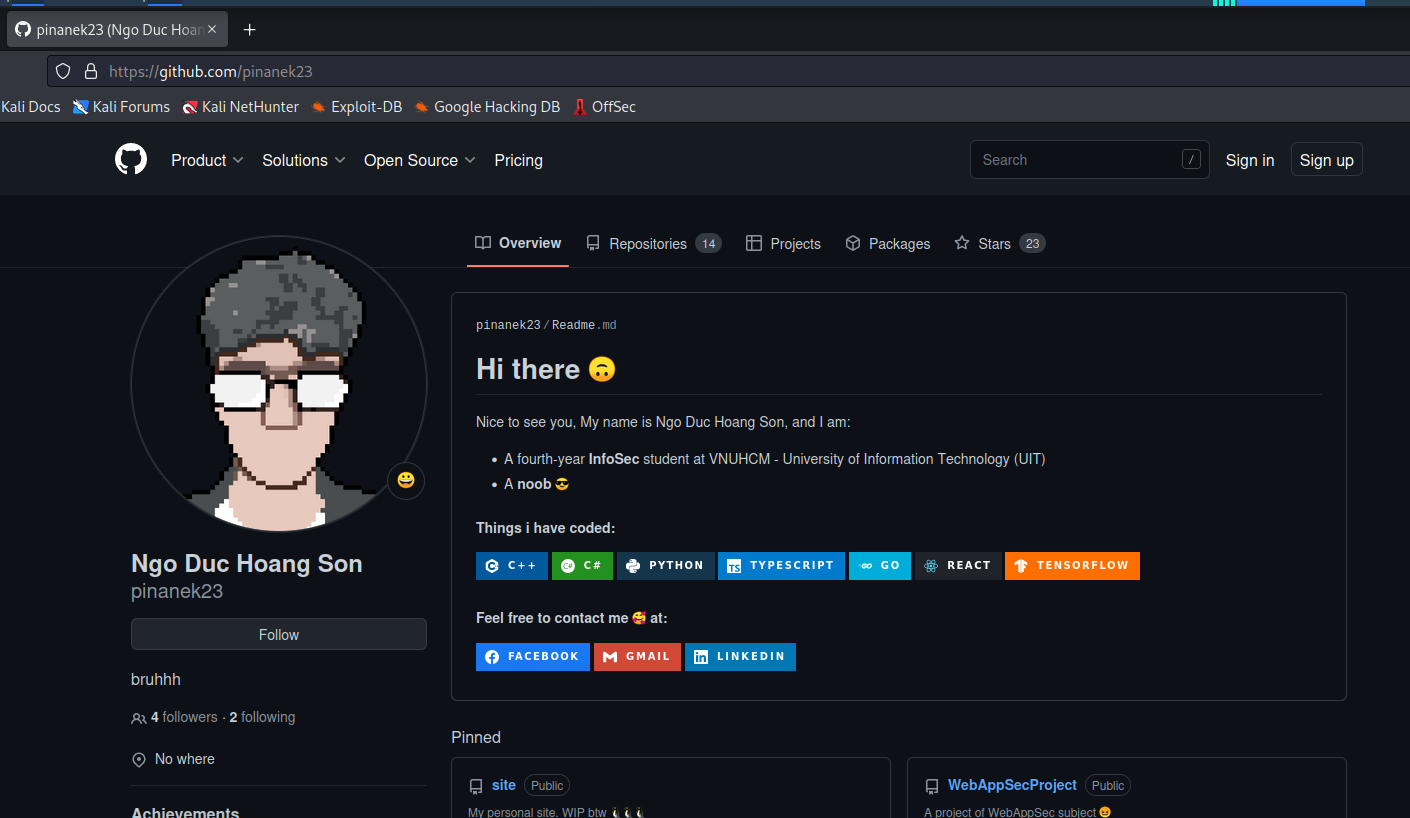


**Alunno 3:**

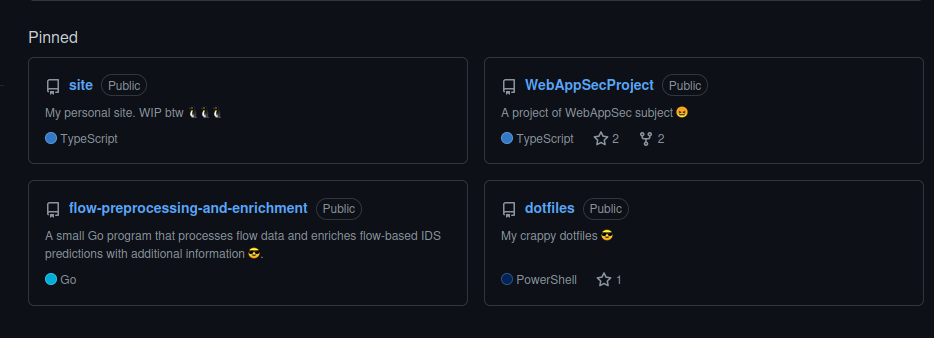
**-** Em thử signin theo máy của nạn nhân thì sẽ nhận được một giao diện đăng nhập như bên dưới, tuy nhiên em lại không có tài khoản và em phát hiện có một đường dẫn tới github hiện liên.



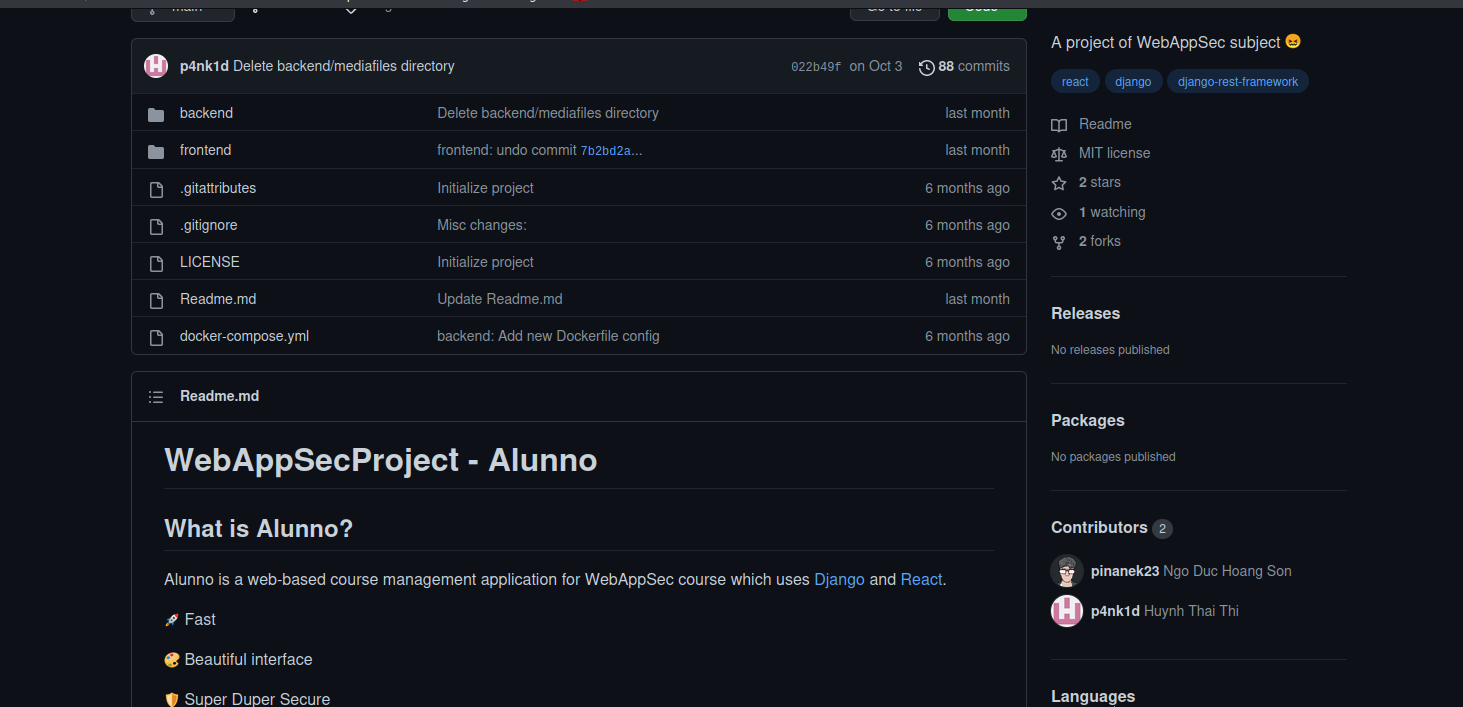
- Thực hiện nhấp vào đường dẫn sẽ hiện lên github có chưa nhiều thông tin



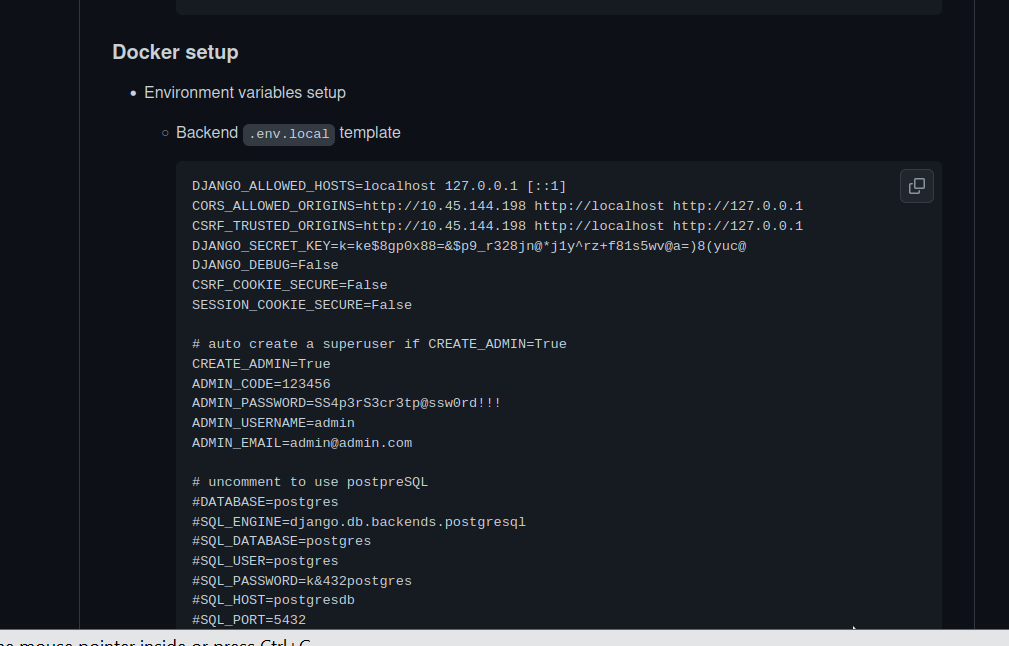
- Tại github này em đã mò tìm ở rất nhiều mục



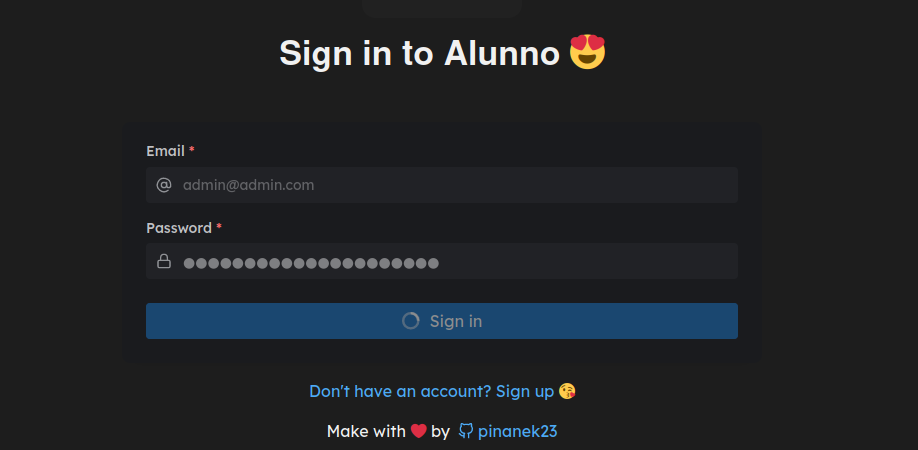
- Phát hiện ở mục WebAppSecProject có những dữ liệu liên quan tới Alunno nên em đã thực hiện tìm kiếm thông tin ở phần này.



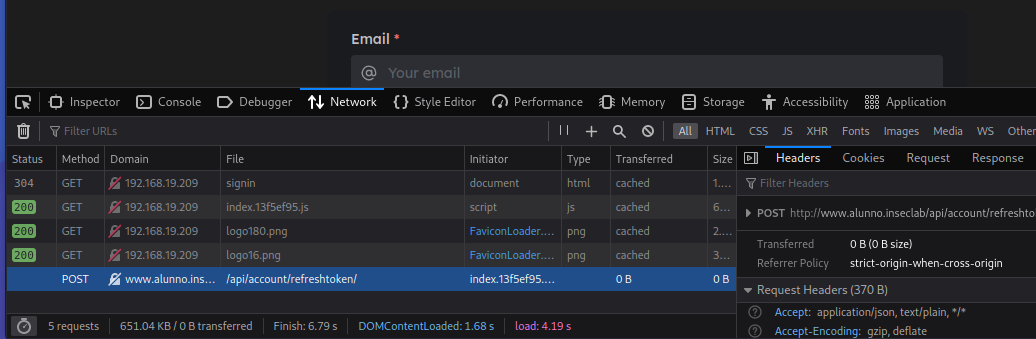
- Sau khi tìm kiếm em phát hiện ra phần phía dưới có chưa cả pass và email để em có thể đăng nhập



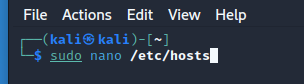
- Tuy nhiên em lại Không đăng nhập được



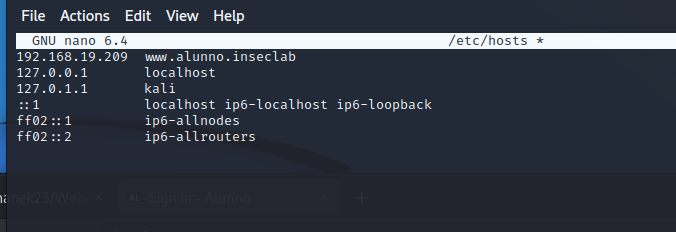
- Sau đó em phát hiện là do đã bị chặn



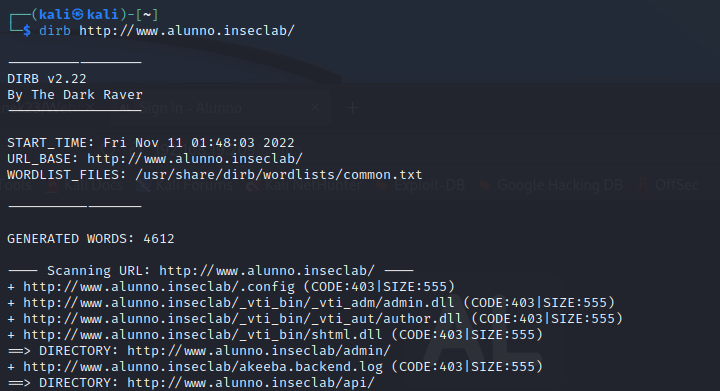
- Vì vậy em đã điều chỉnh etc/hosts



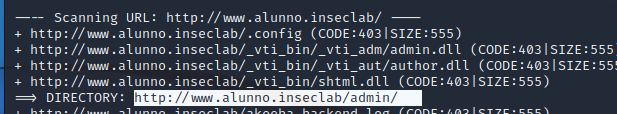
- Dựa theo tên web mà em đã thấy ở trên



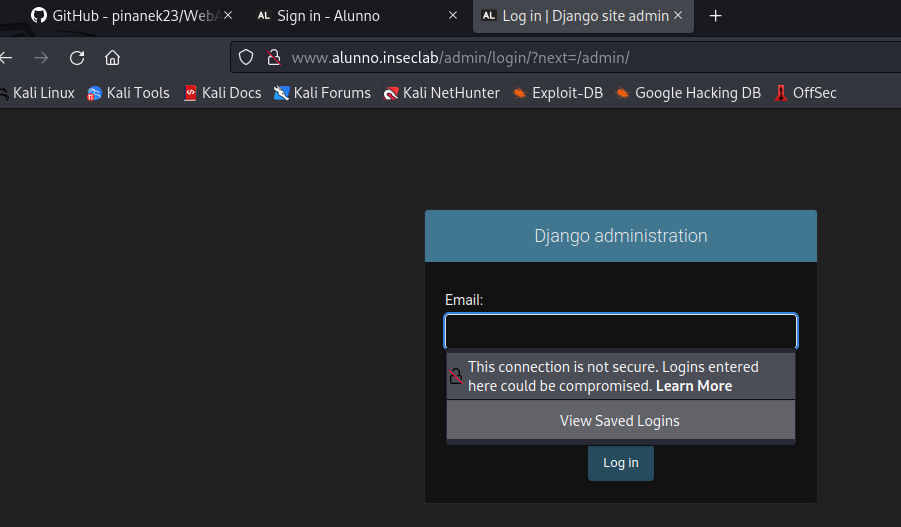
- Sau đó em đã thử quét với lệnh dirb tới [www.alunno.inseclab](http://www.alunno.íneclab) để tìm kiếm thêm thông tin



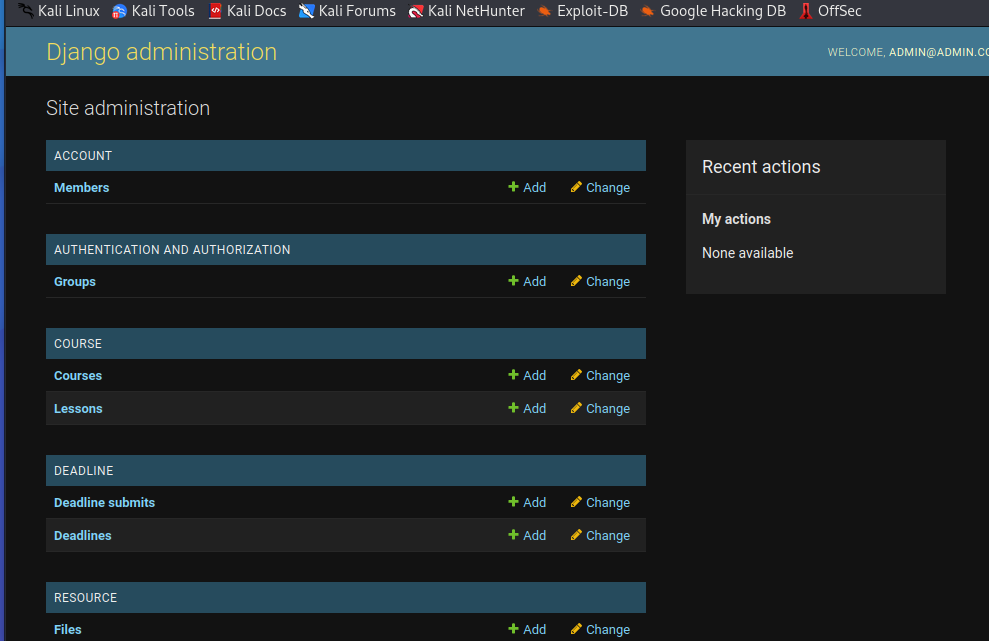
- Trong quá trình phân tích thông tin quét em tìm thấy được dòng dữ liệu admin



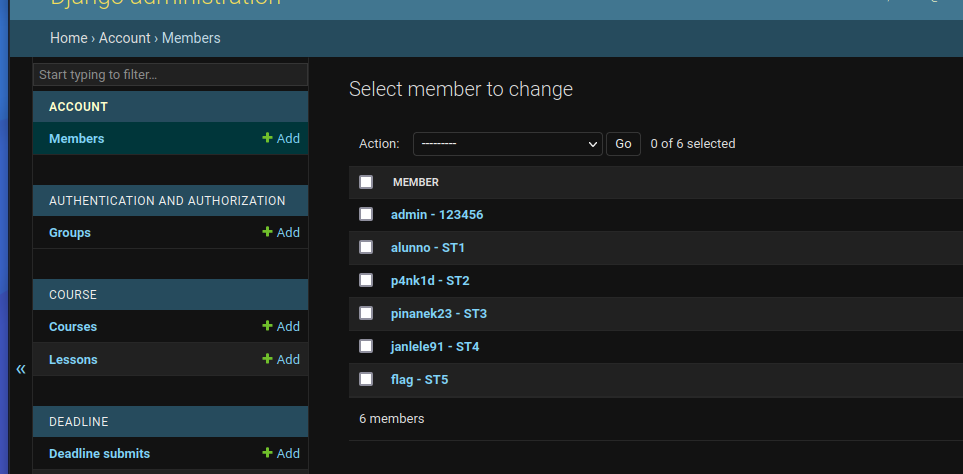
- Em đã quyết định nhập đường link này lên công cụ tìm kiếm và đã vào được một khùng đăng nhập



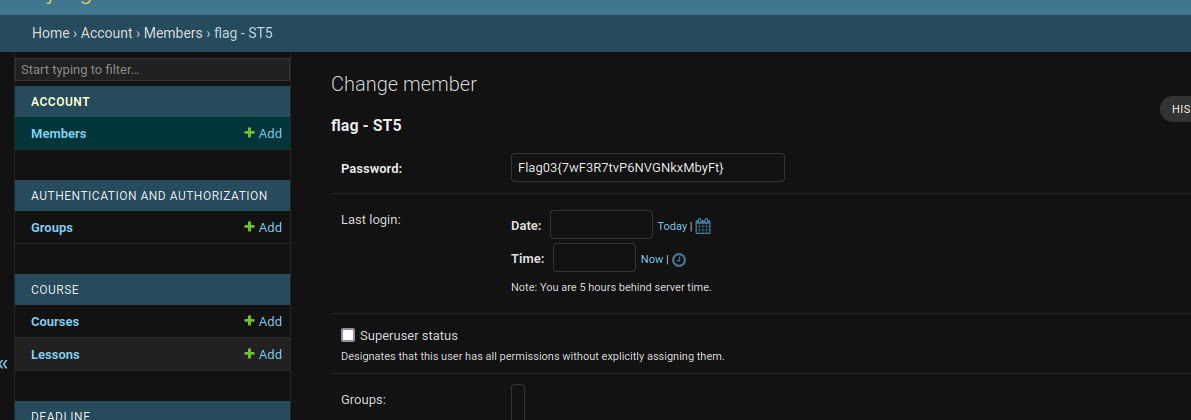
- Sau khi nhập pass và email như tìm ra ở trên thì em đã vào được Django Admin



- Em quyết định dò từng mục và trong đó có mục member xuất hiện dòng flag- ST5

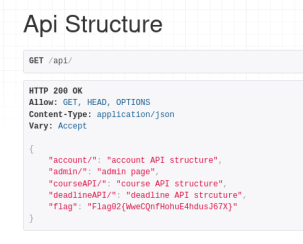


- Kết quả sau khi nhấp vào flag-ST5 thì em đã tìm ra được flag03

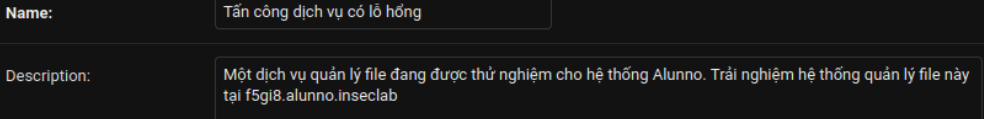


**Alunno 4:**

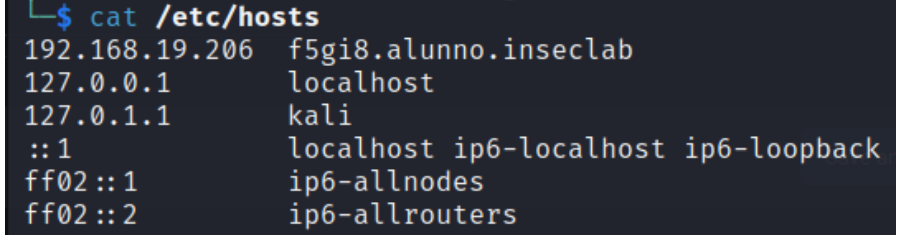
- Dựa theo những gì đã có ở các câu trước thì em đã vào dir admin thì được redirect vào Django Administrator



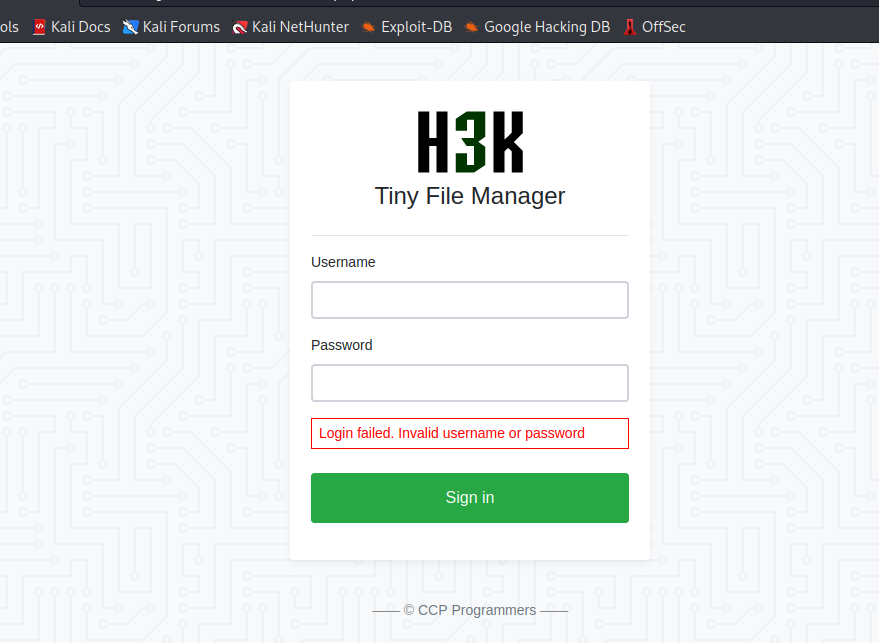
- Sau khi vào thì em có tìm thấy một dòng nằm trong mục Change Lesson như sau



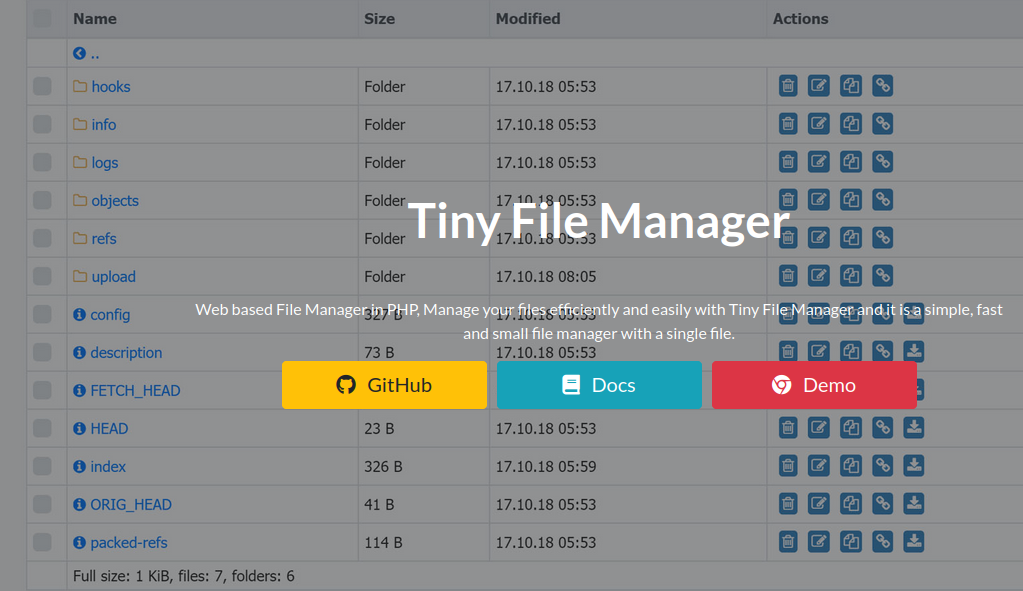
- Sau khi thấy vậy em đã vô etc/hosts chỉnh sửa lại như sau



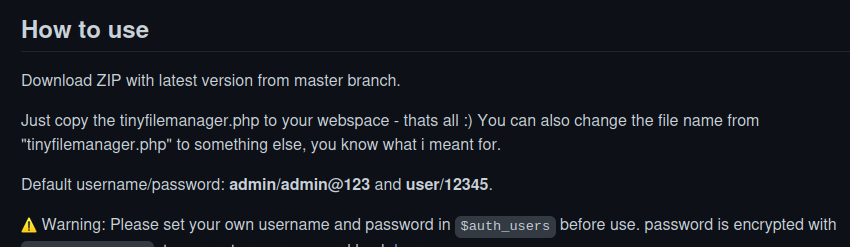
- Tiếp đến em đăng nhập vào /f5gi8.alunno.inseclab/ và hiện ra khung đăng nhập như dưới



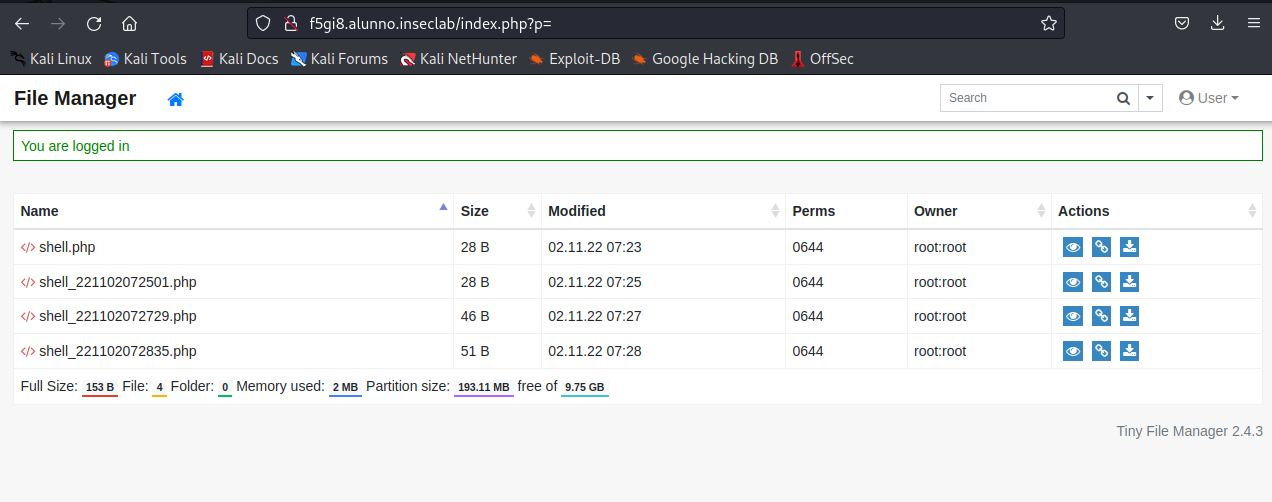
- Tương tự như bài trước, ở đây cũng không có mật khẩu và user nhưng có một đường link dẫn tại CCP Programmers.



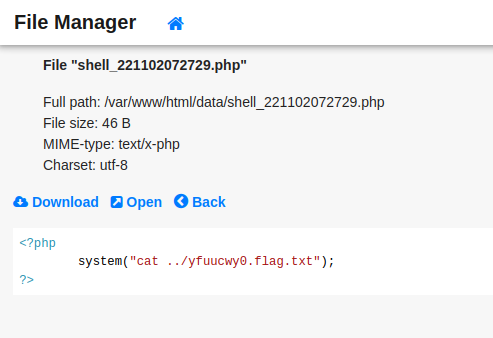
- Tại đây sẽ đưa đến link github và sau một thời gian tìm kiếm thì ngay phần how to use sẽ thấy được username và password, em nhập user/12345 vào phần đăng nhập



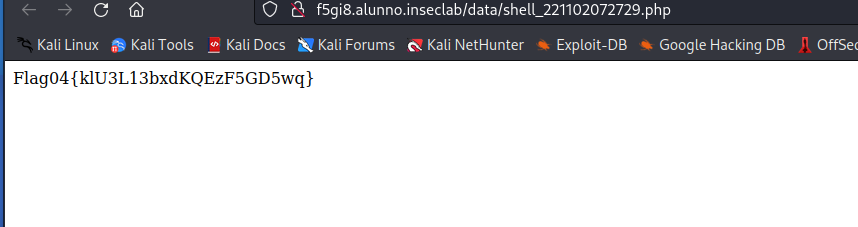
- Sau khi đăng nhập vào được thì ta sẽ thấy một loạt file php



- Thực hiện mở vào từng file php và chọn open thì ngay tại file Manager như hình dưới

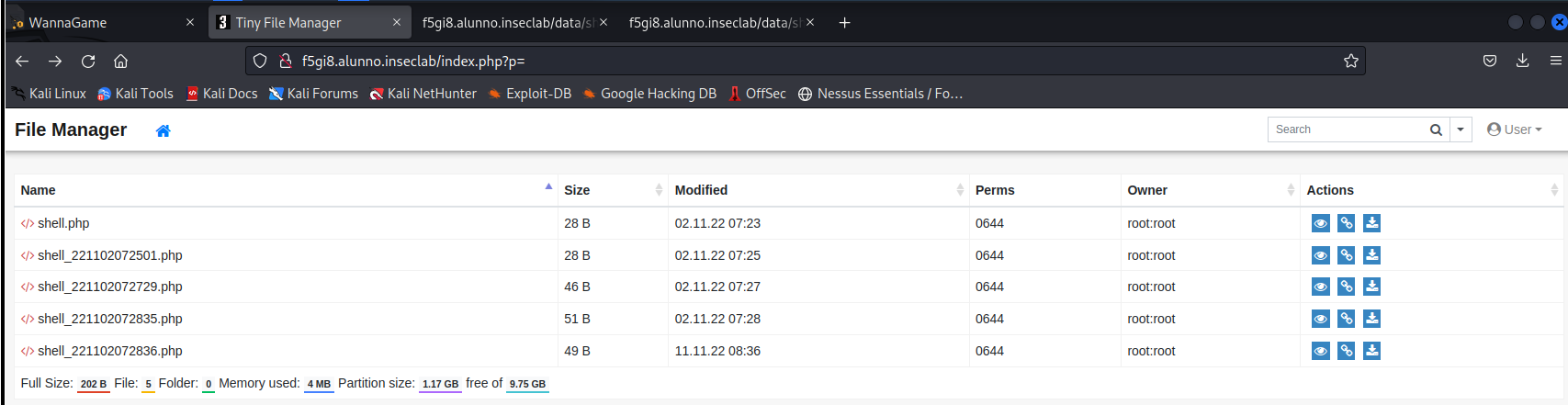


- Em đã kiếm được flag04

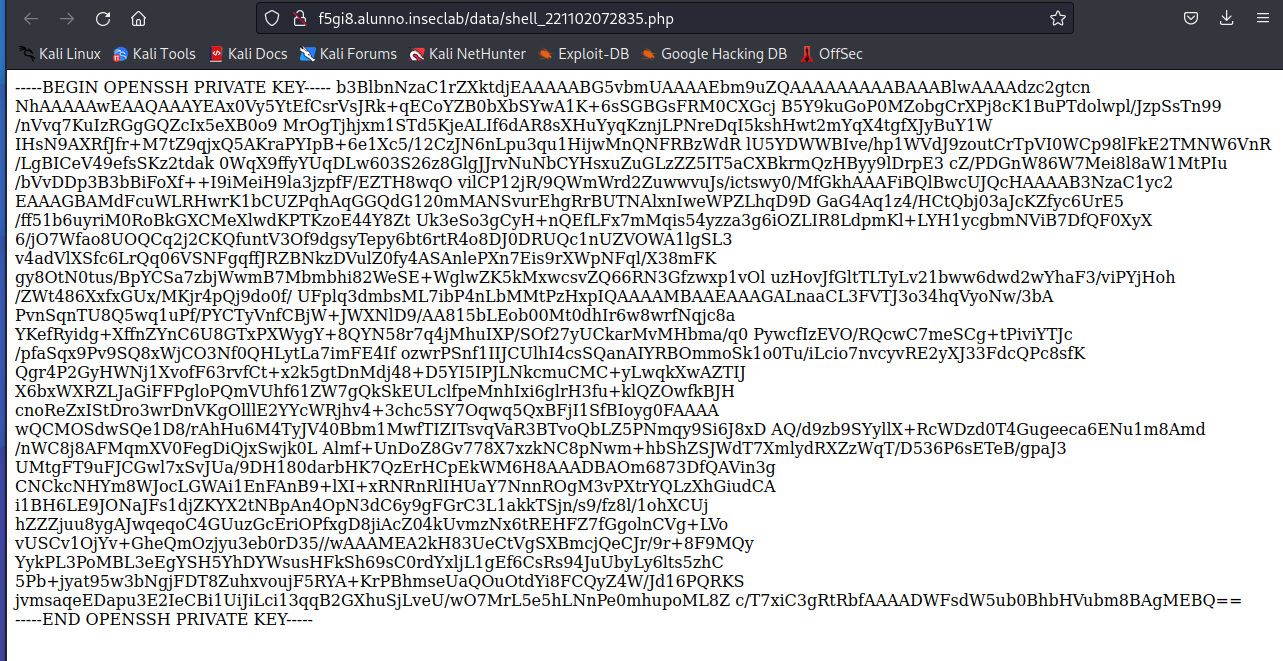


**Alunno user + flag 5 6:**

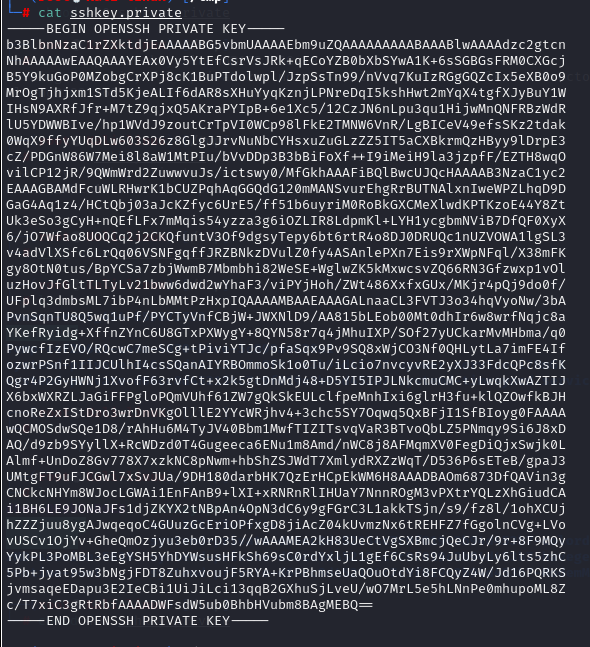
- Sau khi tìm được flag04 thì ta còn lại một vài file php



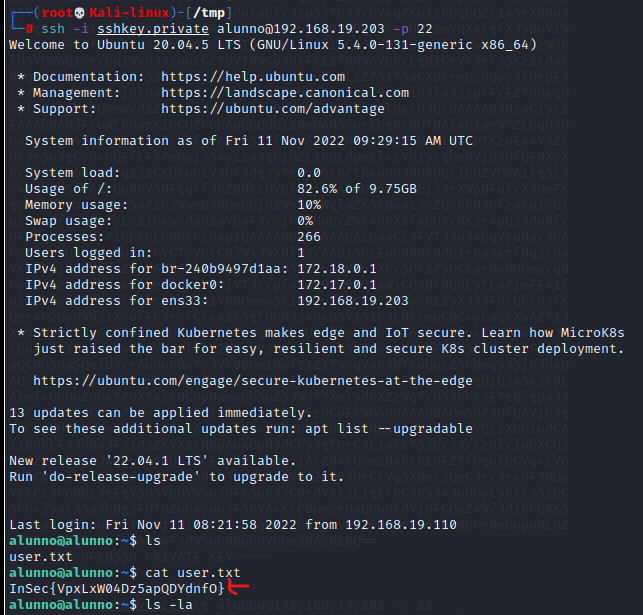
- Em thì mở vào và tìm kiếm trên file php cuối cùng thì thấy được một đoạn mã key rất dài



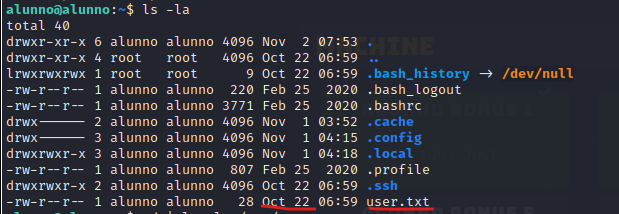
- Tại đây em đã quyết định lưu key về máy, chỉnh format, và connect ssh với key đó



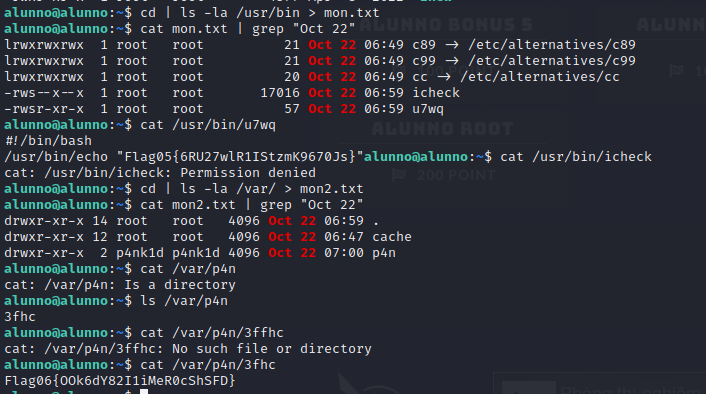
- Sau khi connect được vào user alunno thông qua port 22 và sshkey thì tìm được flag của alunno user tại file user.txt



- Sau đó em có thấy ngày tạo file user.txt là Otc 22 nên em đã tìm kiếm các file cũng ngày



- Trong đó em nhận ra 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 được nên em đã thử đọc hai file đó và đó là file chứa 2 flag05 và flag06



## 2.3 Duy trì quyền truy cập

Sau khi kiểm soát được các máy chủ, chúng tôi vẫn duy trì được phiên truy cập của mình, nhằm đảm bảo rằng chúng tôi vẫn có thể truy cập lại vào máy chủ bất kỳ lúc nào. Nhiều lỗ hổng chỉ có thể được khai thác một lần duy nhất, vì vậy việc duy trì phiên truy cập vào máy chủ là hết sức cần thiết. [N11.ATCL.2]-QUAMONTHICOTENđã thêm vào các tài khoản có quyền cao nhất (thuộc các group administrators hoặc sudo) trên các máy chủ mà chúng tôi đã kiểm soát. Ngoài quyền truy cập cao nhất, một shell Metasploit đã được cài đặt trên máy nhằm đảm bảo rằng các quyền truy cập bổ sung sẽ được thiết lập.

## 2.4 Xóa dấu vết

Giai đoạn xóa dấu vết nhằm đảm bảo rằng các dữ liệu/tài khoản được sinh ra trong quá trình kiểm thử xâm nhập được loại bỏ khỏi máy chủ. Thông thường, các phần nhỏ của công cụ hoặc tài khoản người dùng được để lại trên máy tính của tổ chức, điều này có thể gây ra các vấn đề về bảo mật. Chúng ta cần phải đảm bảo rằng không để sót lại bất kỳ dấu vết trong quá trình kiểm thử xâm nhập.

Sau khi có được các thông tin có giá trị trên máy chủ của đơn vị, [N11.ATCL.2]-QUAMONTHICOTEN đã xóa tất cả tài khoản và mật khẩu người dùng cũng như các dịch vụ được tạo ra bởi Metasploit.

**- HẾT-**