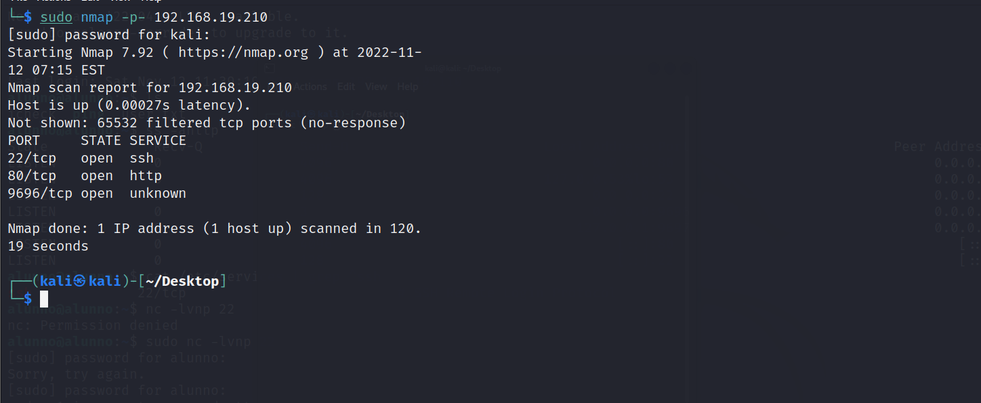
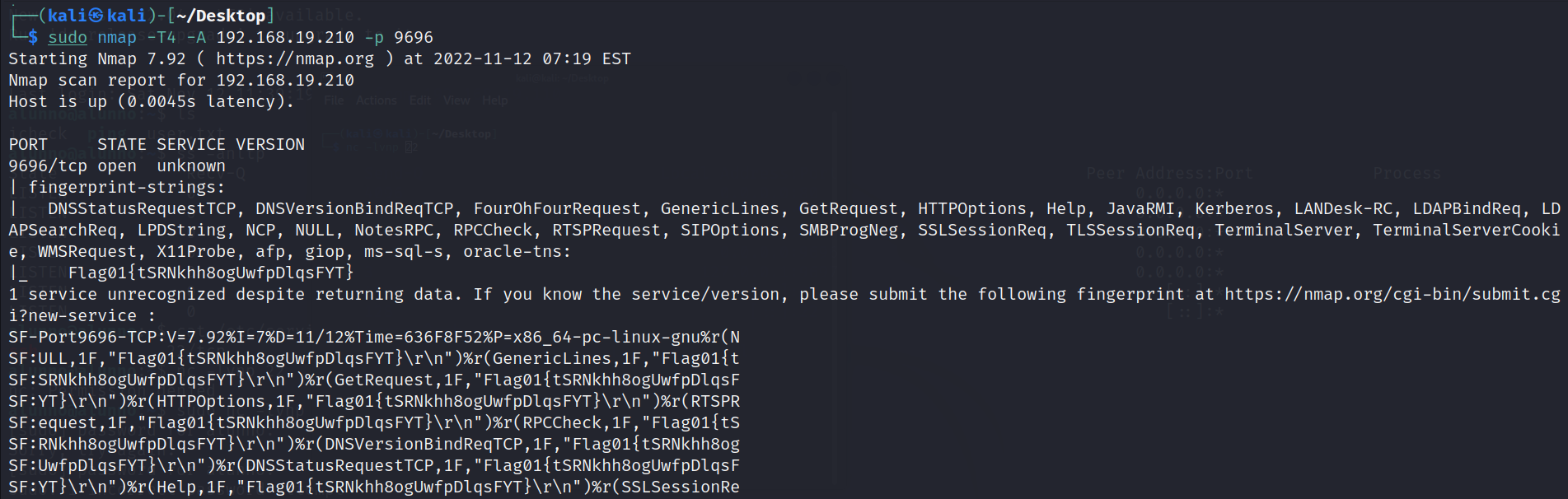
Alunno 1:

Thử quét bằng nmap thử xem có lỗ hổng hay port nào đang mở hay không



Kết quả là tìm thấy 3 port với port 9696 là một ẩn số, thử quét kỹ hơn port này xem sao

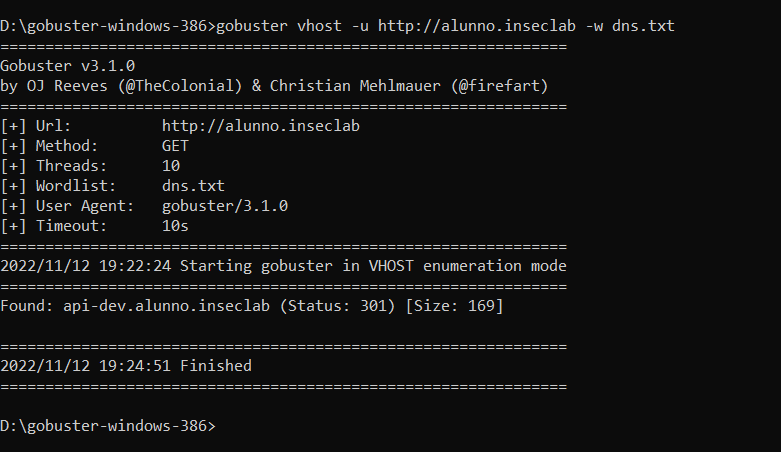


Kết quả là tìm được flag1 trong kết quả trả về

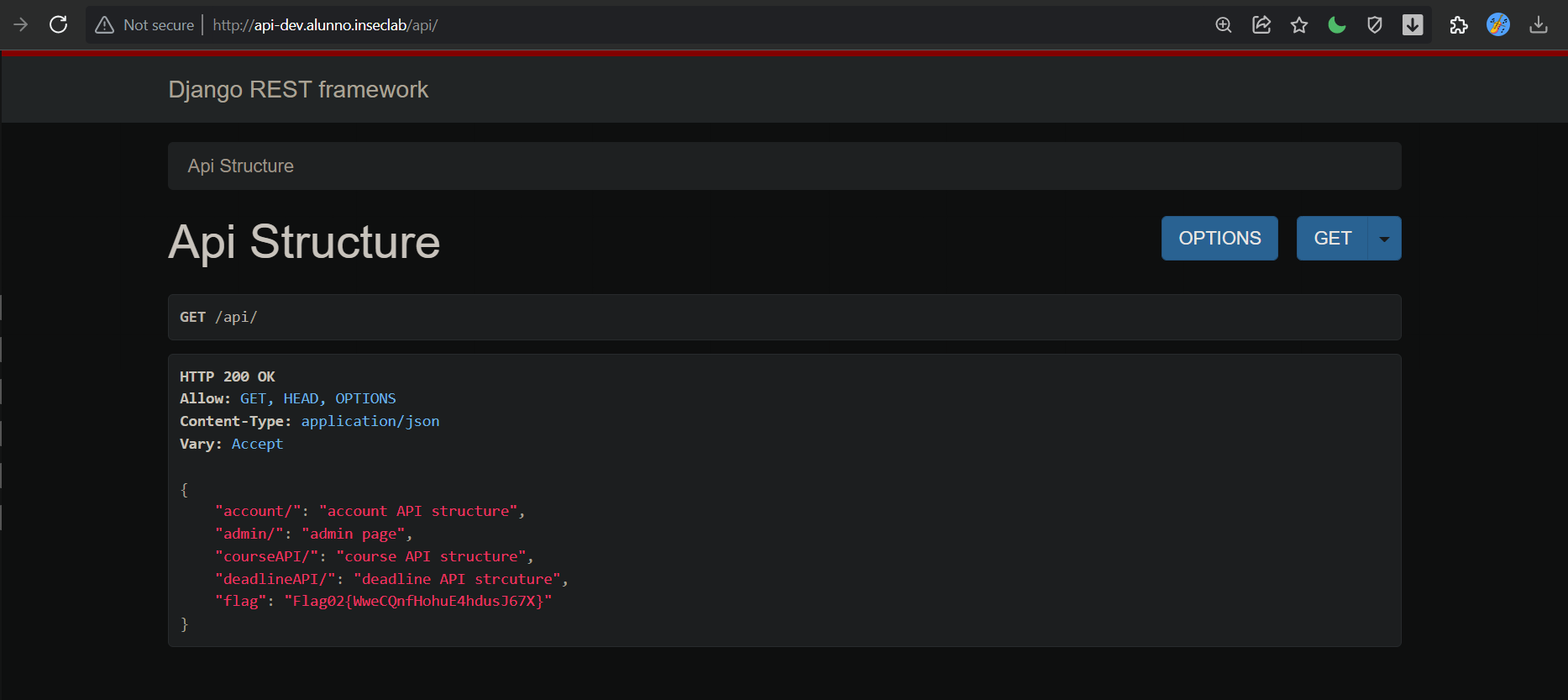
Flag01{tSRNkhh8ogUwfpDlqsFYT}

Alunno 2:

Theo hint và sau khi tìm hiểu thì ta sẽ dùng gobuster với mode vhost để bruteforce tìm ra một domain để truy cập



Sau khi quét thì ta thấy được một domain mới được tìm ra thử truy cập vào domain này. Lưu ý phải chỉnh sửa file hosts thì mới truy cập vào được.



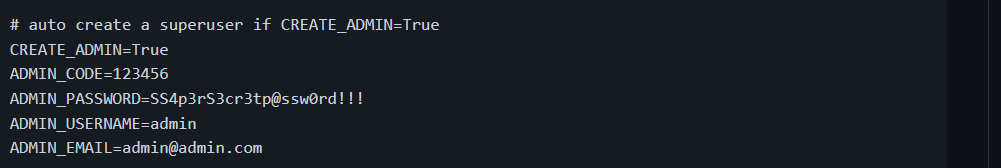
Sau khi truy cập thì ta có ngay flag2

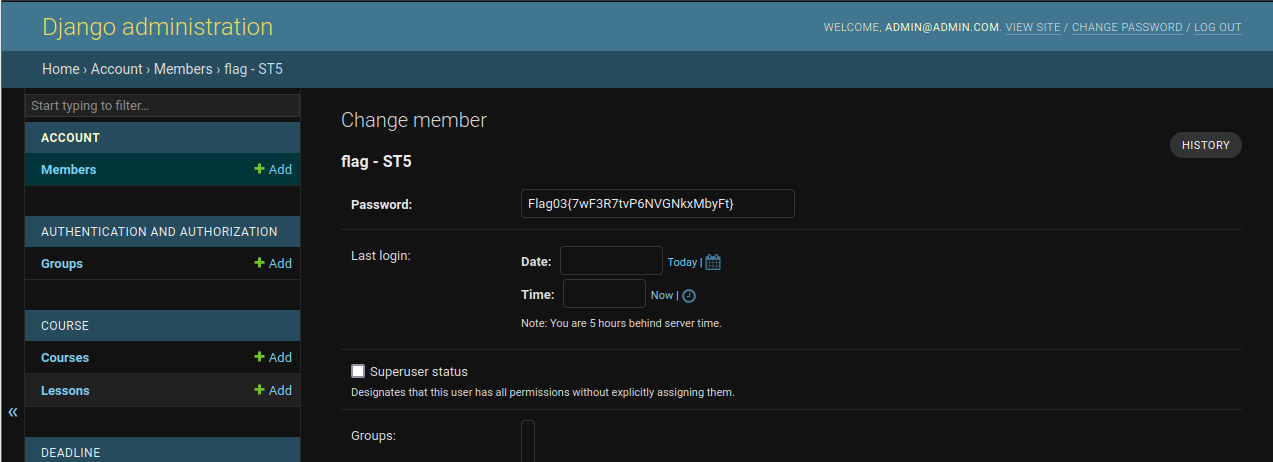
Flag02{WweCQnfHohuE4hdusJ67X}

Alunno 3:

Sau khi tìm hiểu qua trang github của tác giả thì biết được rằng web này được viết bằng django. Tìm hiểu một tí trên mạng thì biết là django có phần là admin site. Thay đổi url thành [www.alunno.inseclab](http://www.alunno.inseclab)/admin để có thể truy cập.

Email và password tác giả cũng đã để ở github luôn rồi nên chỉ cần đăng nhập vào thoi

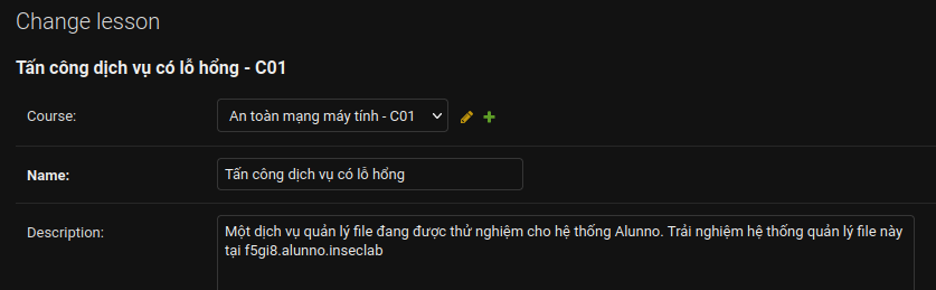


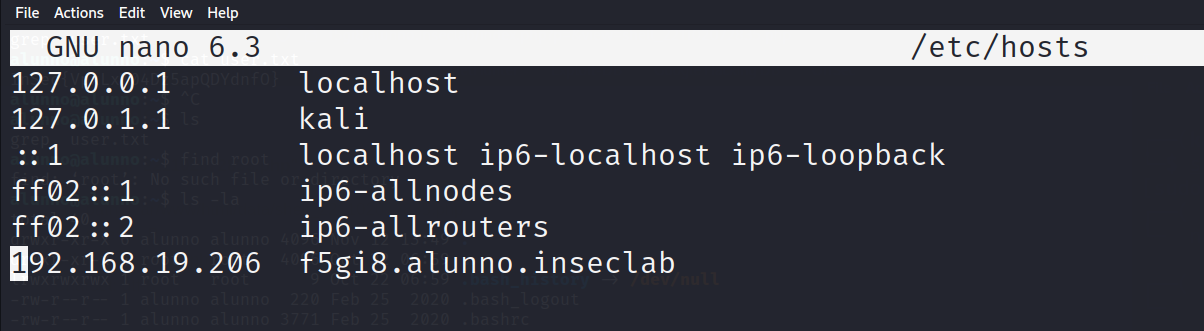


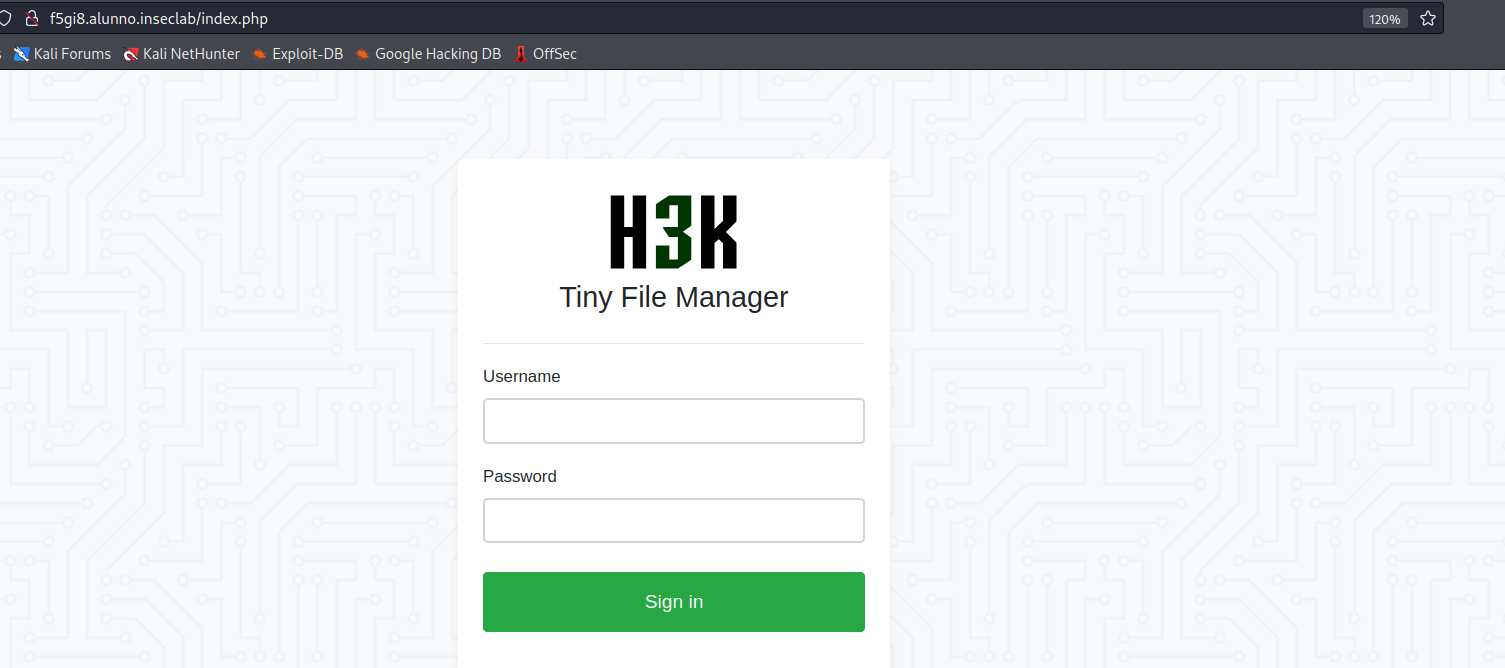
Sau khi truy cập vào được admin site thì tìm xem flag nằm ở đâu.

Alunno 4:

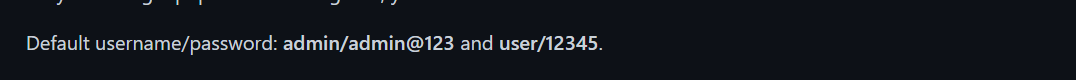
Theo một chỉ dẫn trong admin site ta sửa url thành f5gi8.alunno.inseclab trong file hosts rồi truy cập vào

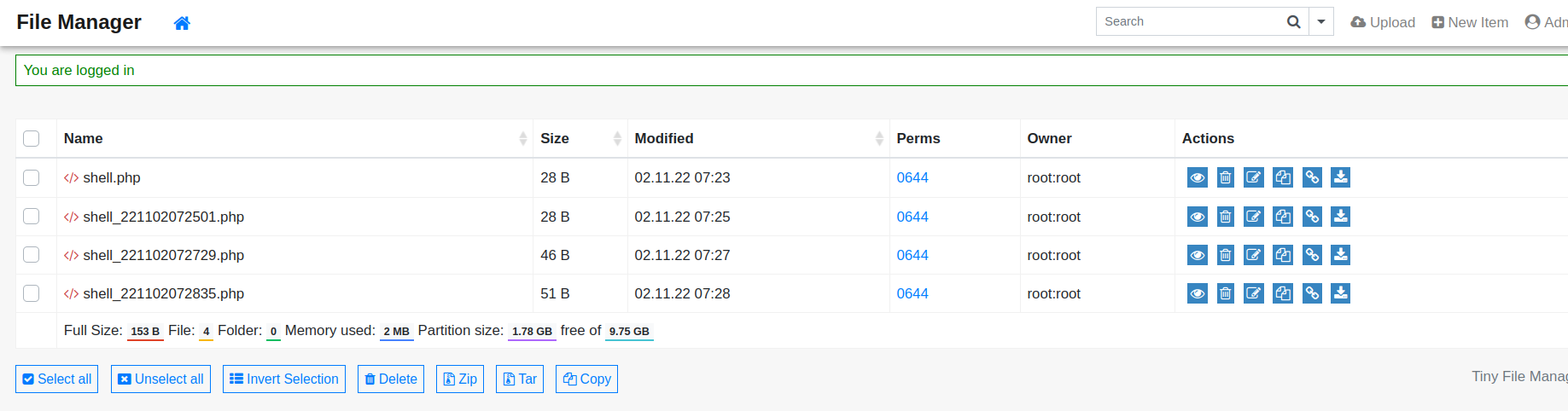




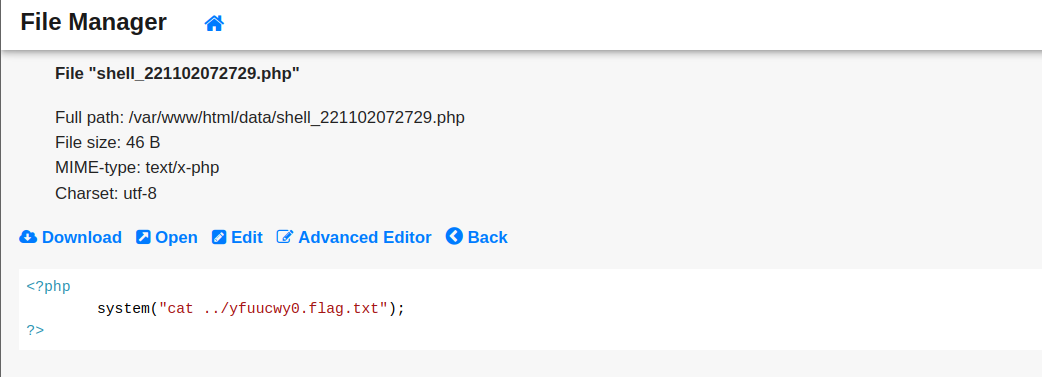


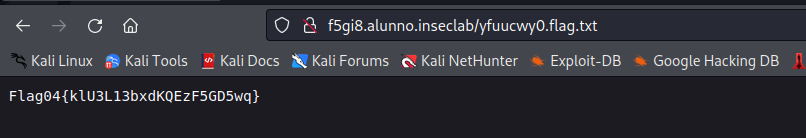
Tìm kiếm về Tiny File Manager trên github thì tìm thấy được username và password thử đăng nhập vào xem.





Vào được giao diện thì ta tìm thấy một lệnh thư một có tên là …flag.txt thử truy cập tới đó xem thì ta thu được flag

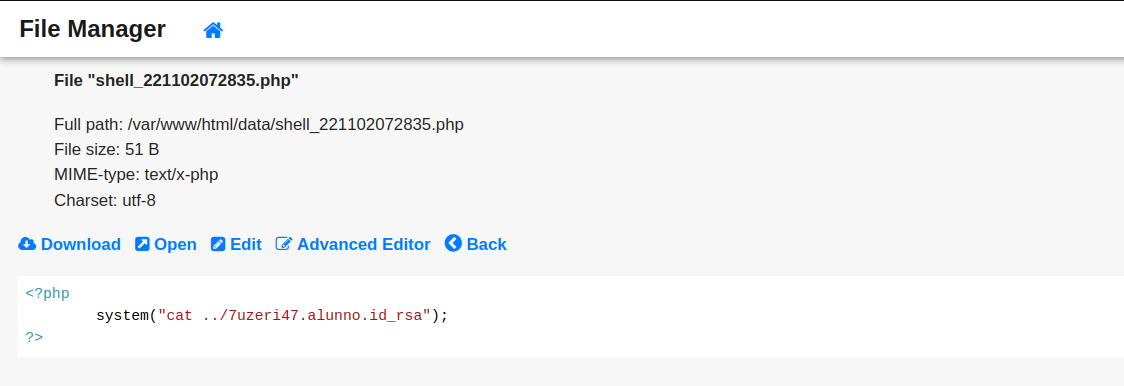




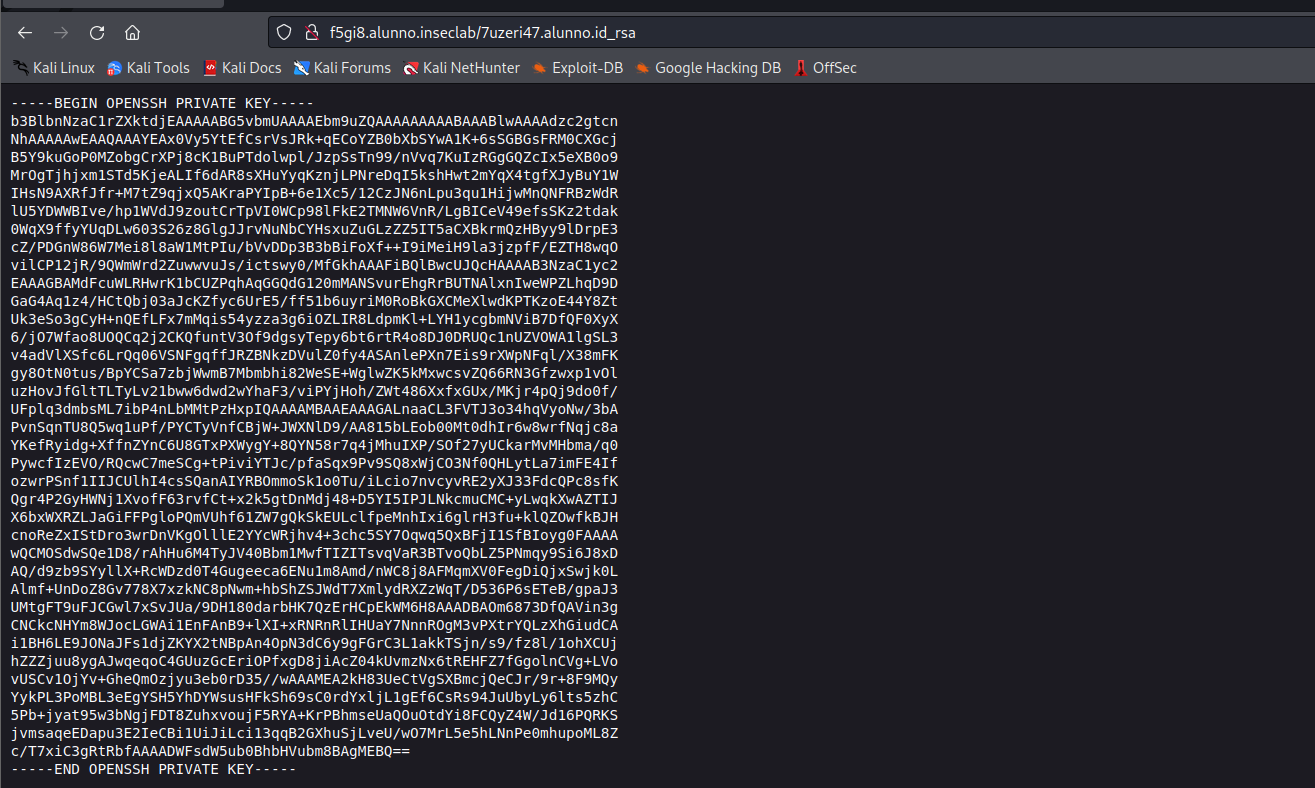
Flag04{klU3L13bxdKQEzF5GD5wq}

Alunno User

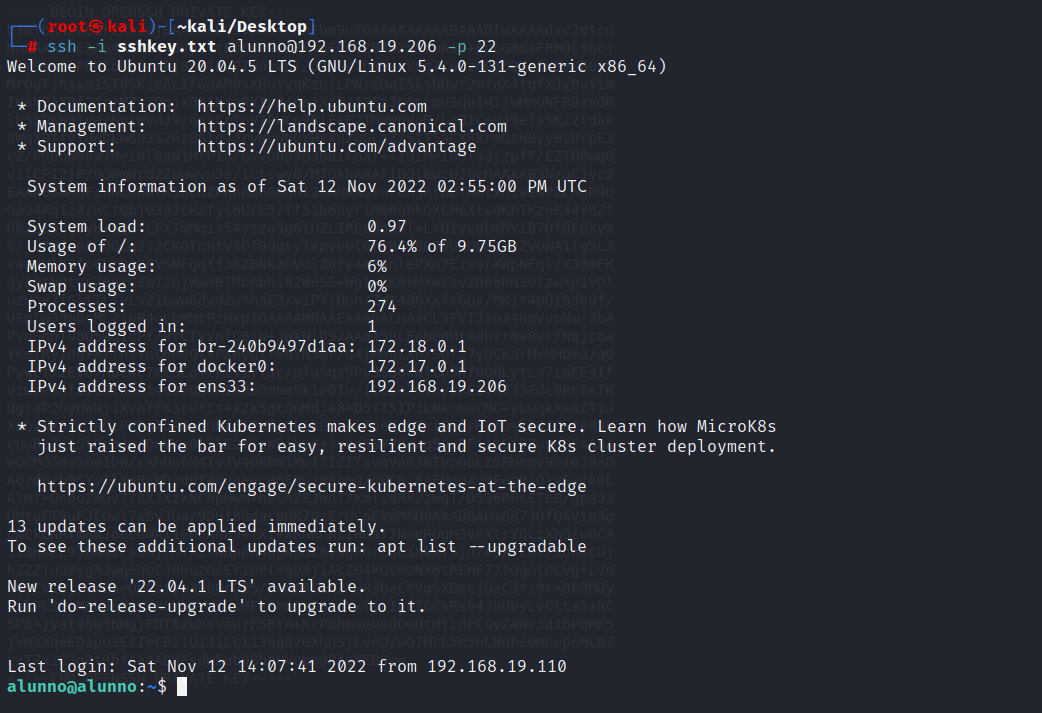
**Trong challenge alunno 4 ta tìm được một đường dẫn khác là ../7uzeri47.alunno.id\_rsa**



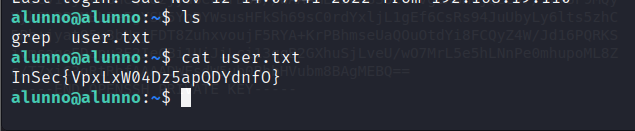
Thử truy cập vào đường dẫn này thì ta nhận được đoạn mã RSA như sau.



Có thể đây là private key để xác thực đăng nhập với máy chủ qua kết nối ssh. Thử truy cập vào máy chủ



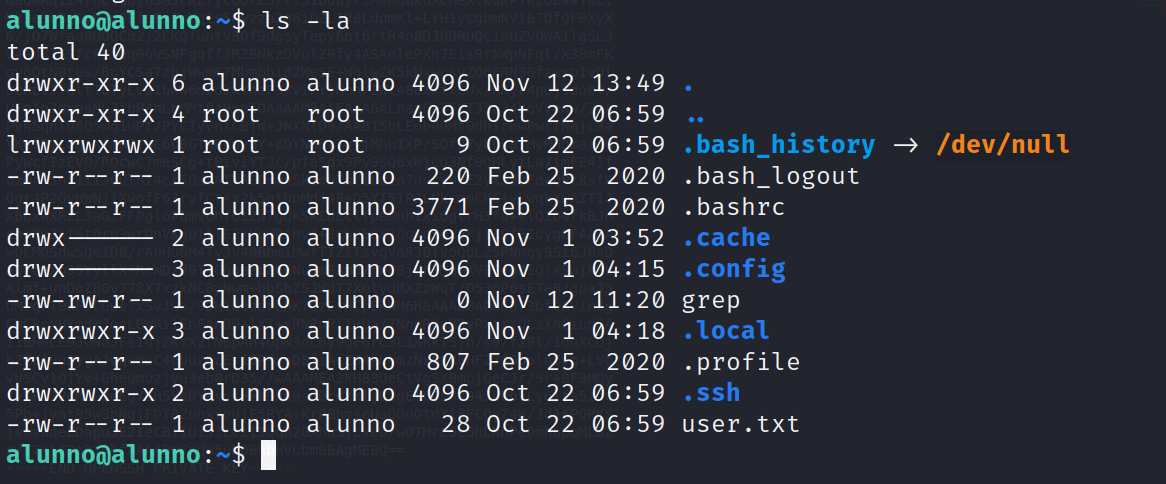
Đã thành công truy cập máy chủ giờ thì chỉ cần xem trong đây có gì. Kết quả là phát hiện 1 file user.txt thử xem file này và ta tìm được flag của challenge alunno user



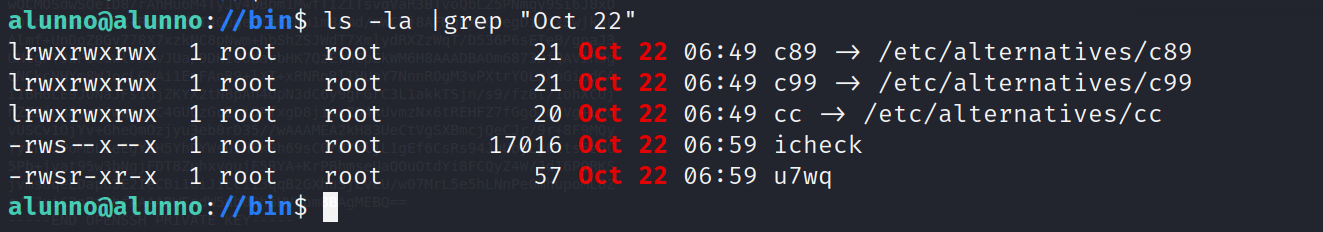
InSec{VpxLxW04Dz5apQDYdnfO}.

Alunno 5

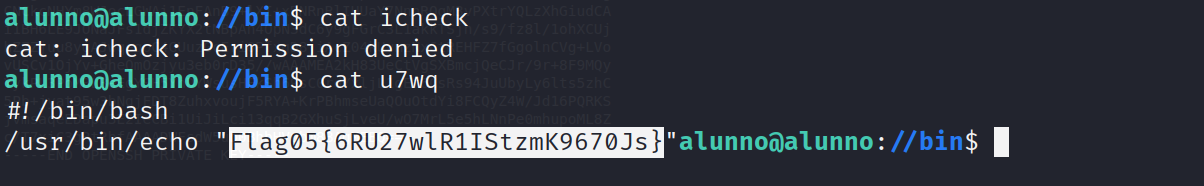
Sau khi có được flag của alunno user thì ta thử liệt kê các file ẩn khác



Ta thấy có 3 file khác được tạo cùng ngày cùng giờ với user.txt nên có thể những file này chứa flag. Ta thử tìm ngoài root các file có ngày tạo là Oct 22.



Trong bin có 2 file thử cat xem

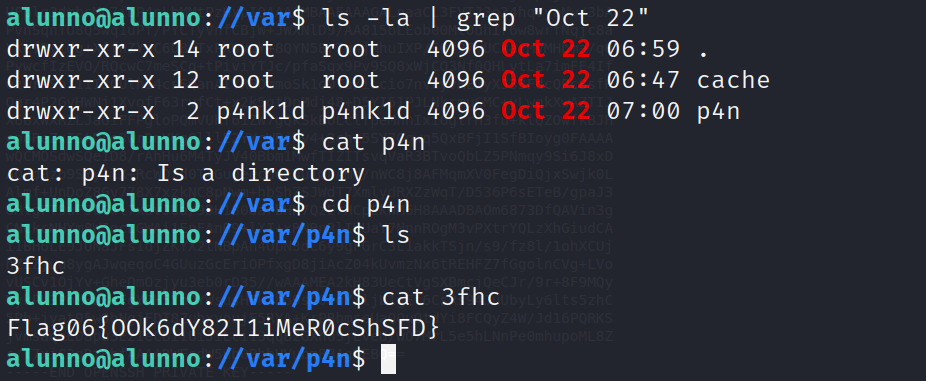


Ta tìm được flag5

Flag05{6RU27wlR1IStzmK9670Js}

Alunno 6:

Thử tìm kiếm ở nơi khác thì phát hiện trong var cũng có chứa thư mục tạo vào Oct 22 nên thủ coi trong đây có gì

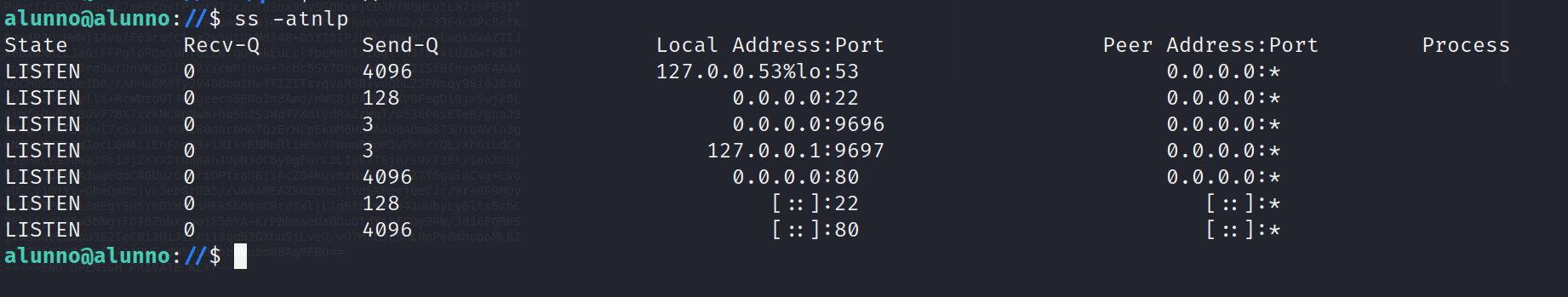


Qua các bước đơn giản thì cũng tìm ra được flag6

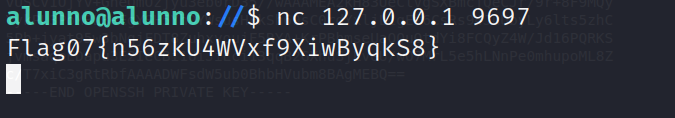
Flag06{OOk6dY82I1iMeR0cShSFD}

Alunno 7

Tìm kiếm các file khác thì chả thấy flag7 đâu nên có thể nó nằm ở một nơi nào khác trên máy chủ. Thử kiểm tra có các dịch vụ nào đang được mở trên máy chủ



Phát hiện một kết nối lạ với port 9697 thử nc tới đây xem có gì không

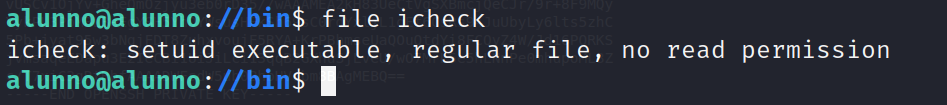


Tìm ra được flag7 rồi hehe

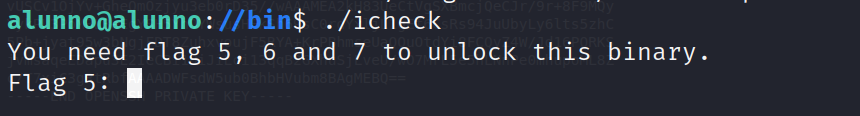
Flag07{n56zkU4WVxf9XiwByqkS8}

Alunno root:

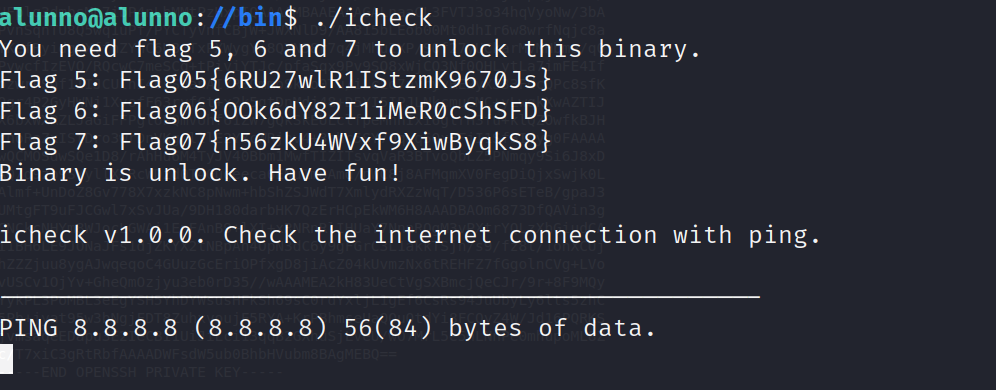
Lúc tìm flag5 thì file icheck đã permission denied nên thử xem nó là file gì.



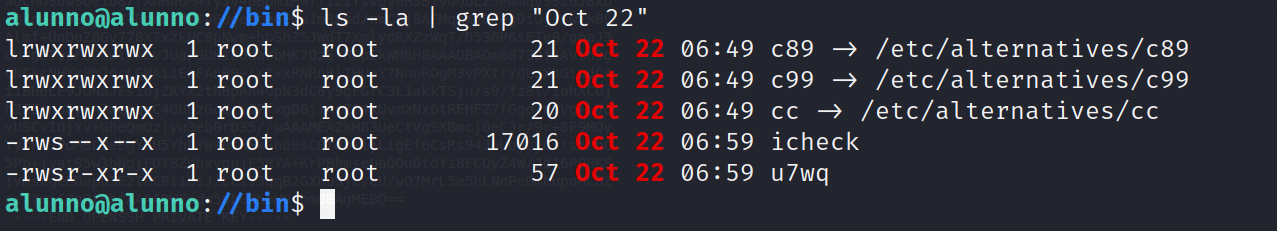
Thì ra là một file thực thi, thực thi nó luôn xem sao.



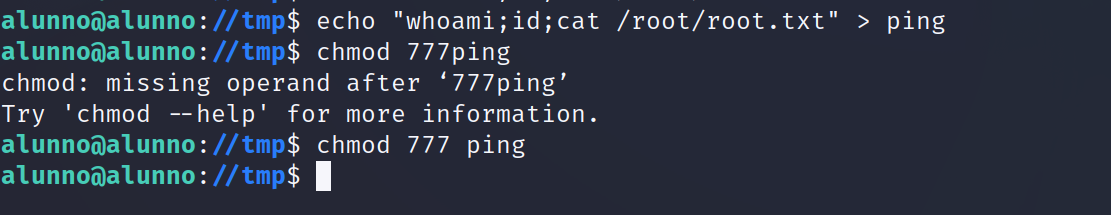
Yêu cầu nhập vào flag 5 6 7 để mở khóa binary gì đấy



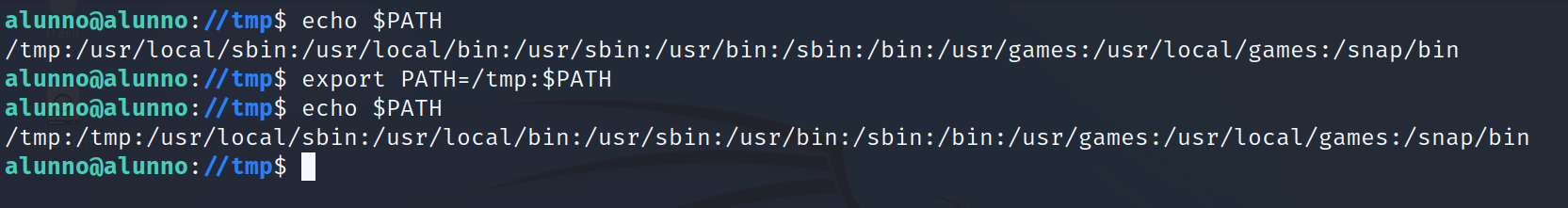
Kết quả là nó thực hiện lệnh ping tới 8.8.8.8



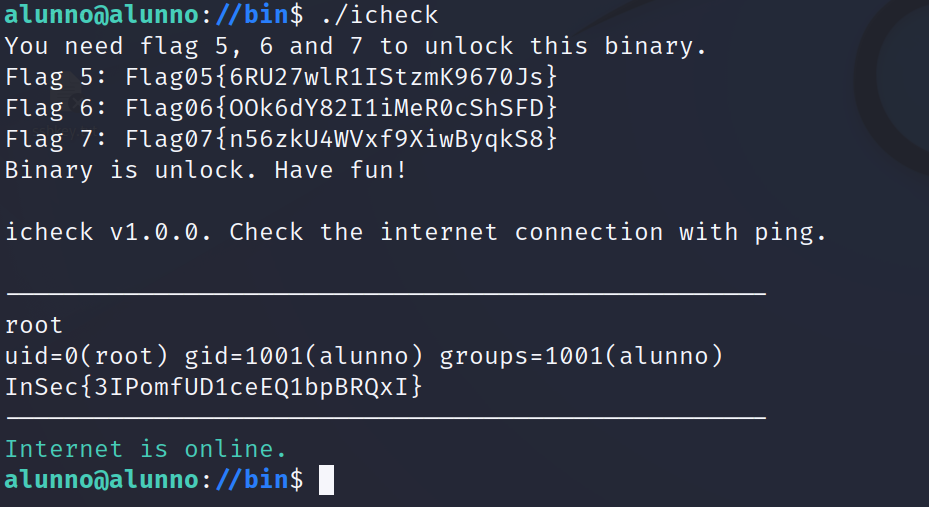
File thực thi này được tạo và thực thi dưới quyền root. Để khai thác thì chúng ta tạo 1 file với nội dung whoami; id; cat root/root.txt và cấp quyền thực thi cho nó (lưu file trong /tmp).



Tiếp theo ta sẽ trỏ PATH đến tmp để khi thực thi lệnh ping sẽ thực thi file ping trong tmp với các lệnh đã ghi



Quay lại thực thi file icheck thì ta có được flag của alunno root



InSec{3IPomfUD1ceEQ1bpBRQxI}