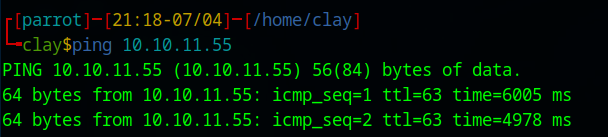
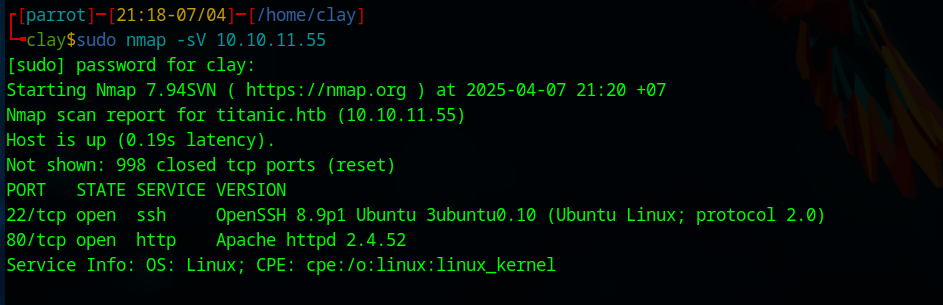
B1: Reconnaissance và scanning

Địa chỉ máy mục tiêu



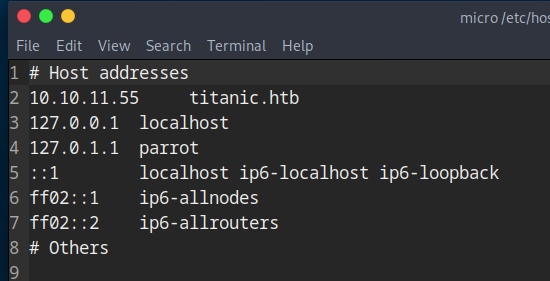
-Dùng nmap để scan các dịch vụ đang chạy



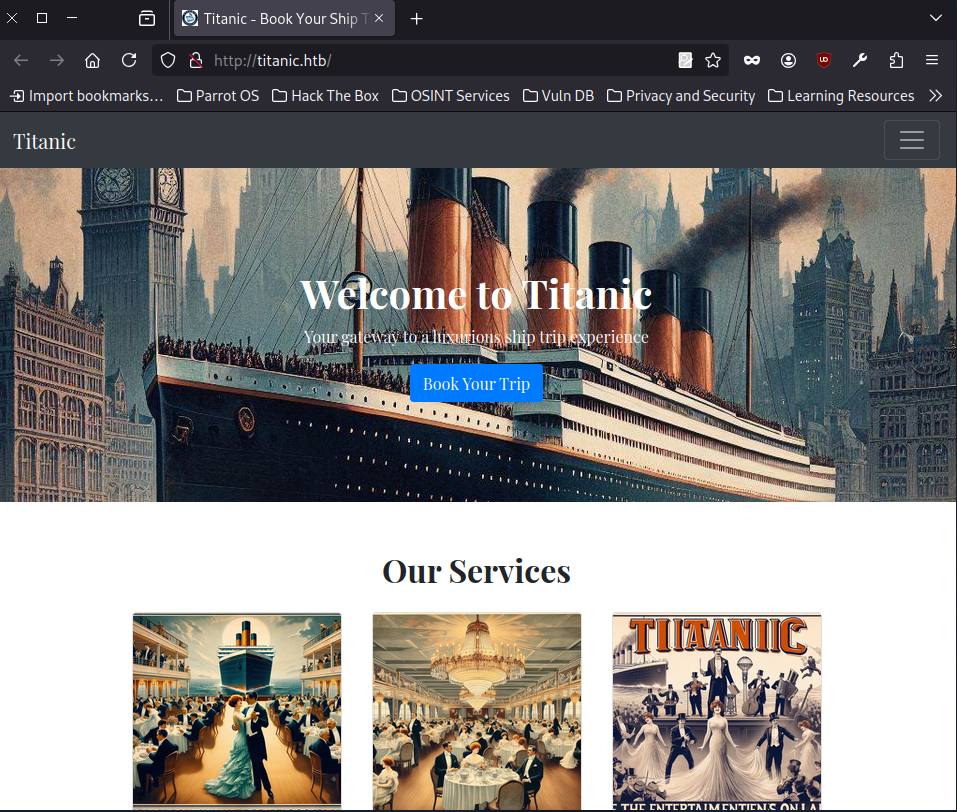
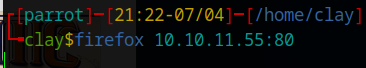
Ta thấy có 2 cổng 22 để ssh và cổng 80 web mở

B2: Enumaration và ganning access

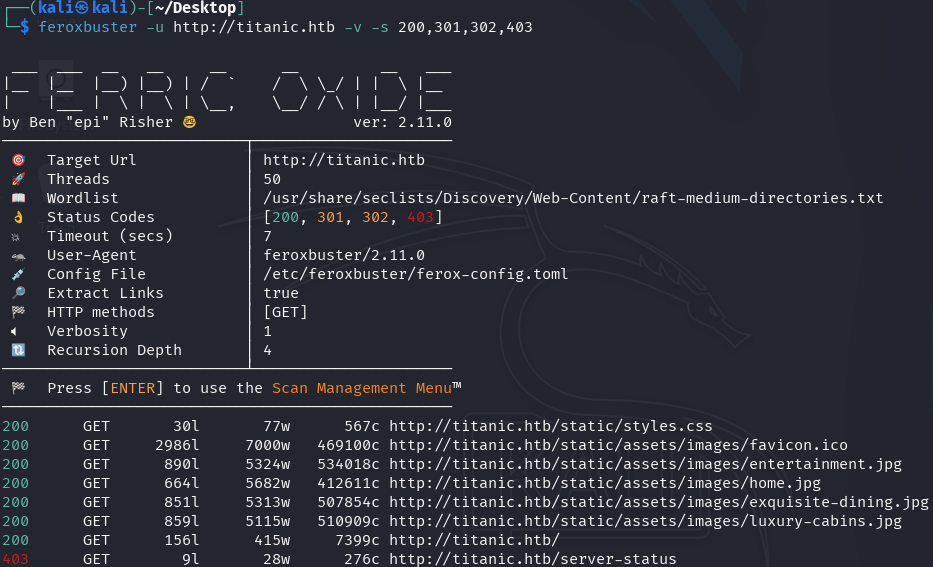
Ta thêm domain vào etc host



Ta truy cập web service của mục tiêu

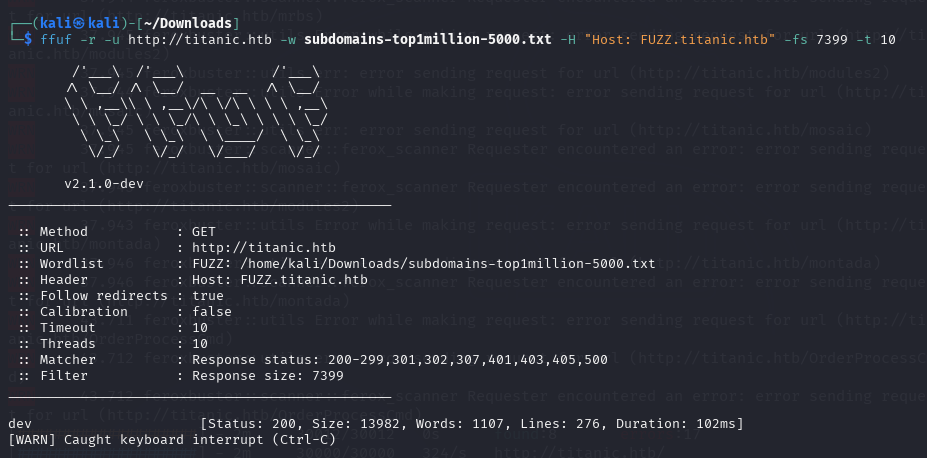


-Dùng feroxbuster để xem tất cả các đường dẫn của trang



Ko có gì đáng chú ý lắm

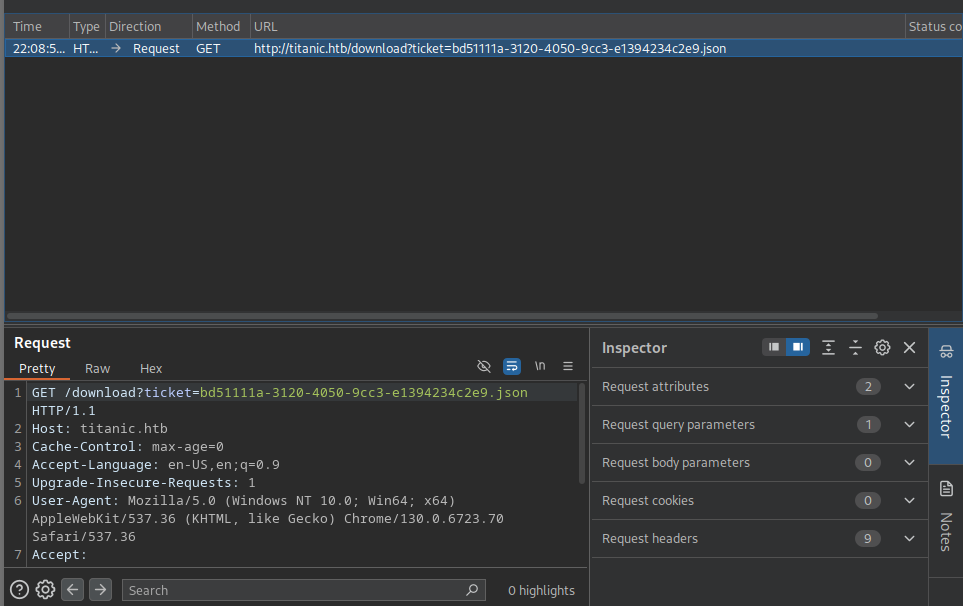
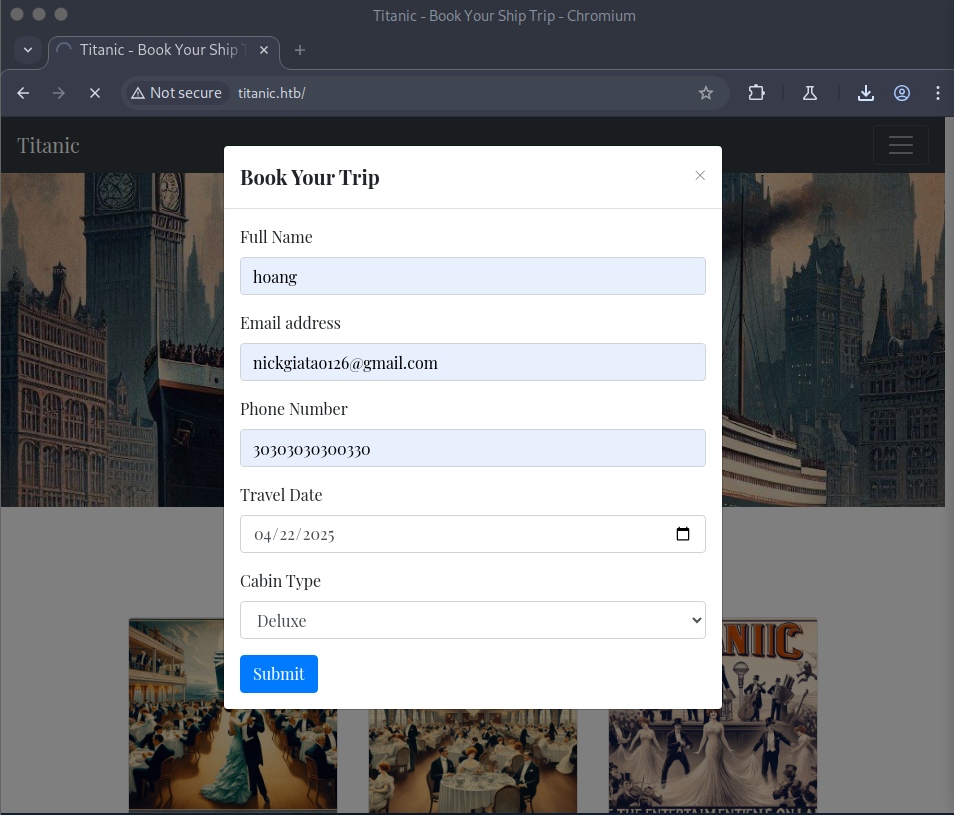
Sử dụng ffuf kiểm thử fuzzing để tìm các vhost



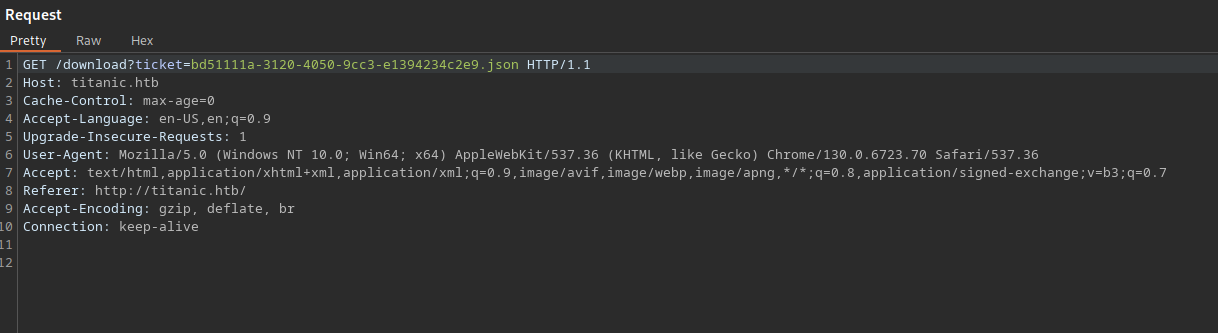
Ta tìm thấy 1 domain với tên dev.titanic.htb

Thêm vào etc/hosts

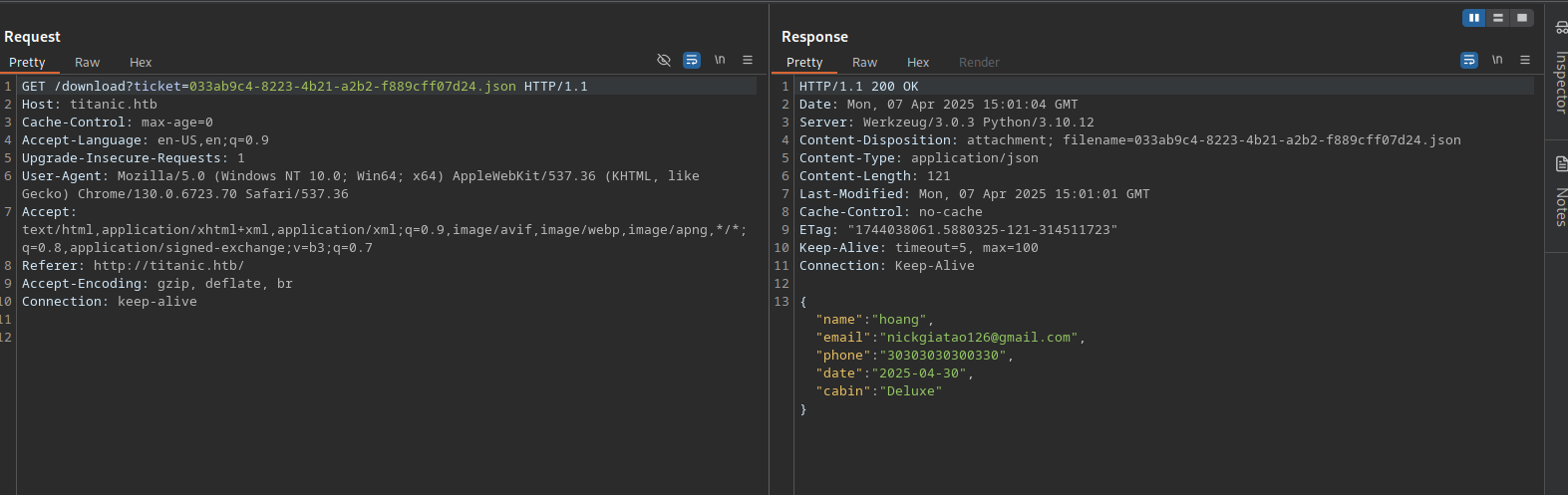
Ta thấy trên trang titanic có 1 lựa chọn book chỗ, ta dùng burp suite để chặn và xem xét gói tin



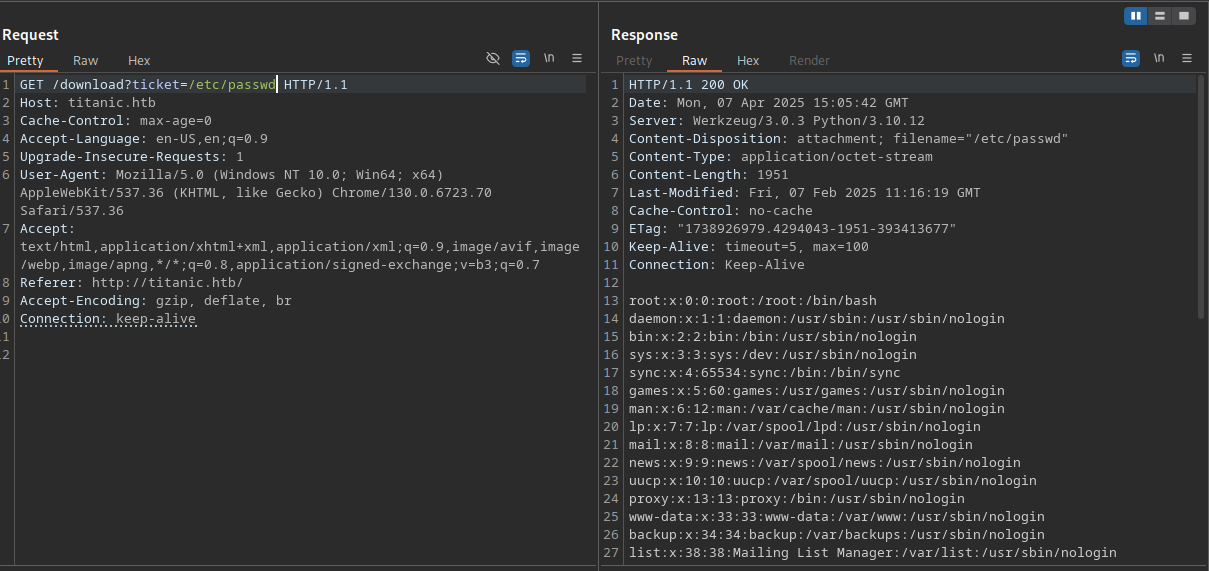
Ta thấy phương thức ở đây dùng là GET



Thông tin ở đây



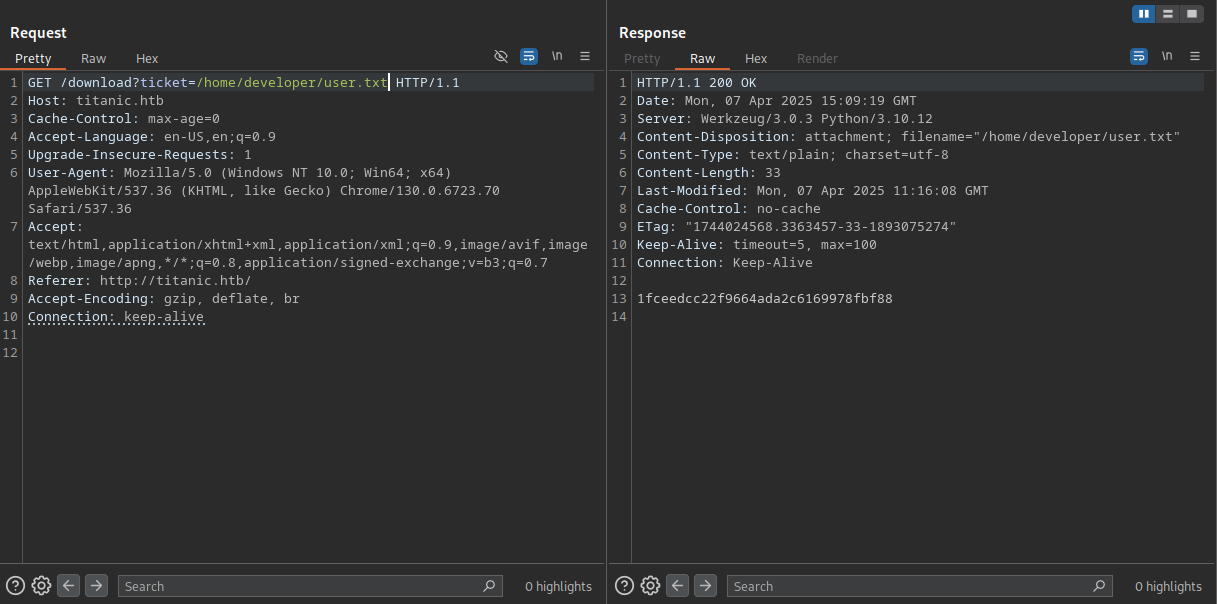
-> ta có thể nghĩ tới vc LFI



Ta sửa đổi gói tin và có thể lấy dc password của máy chủ



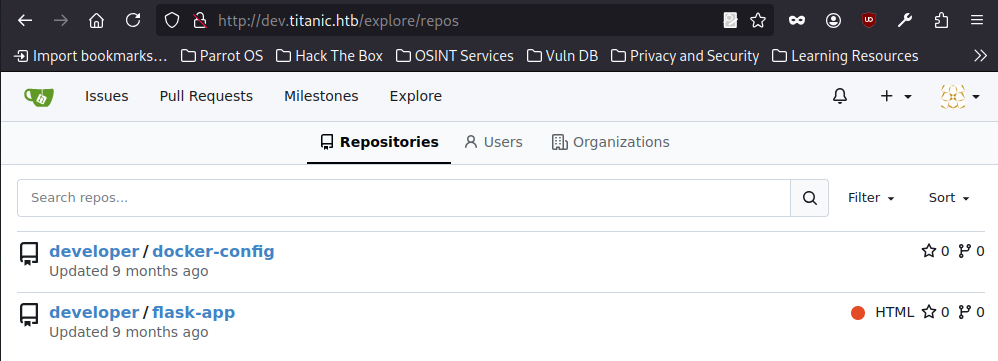
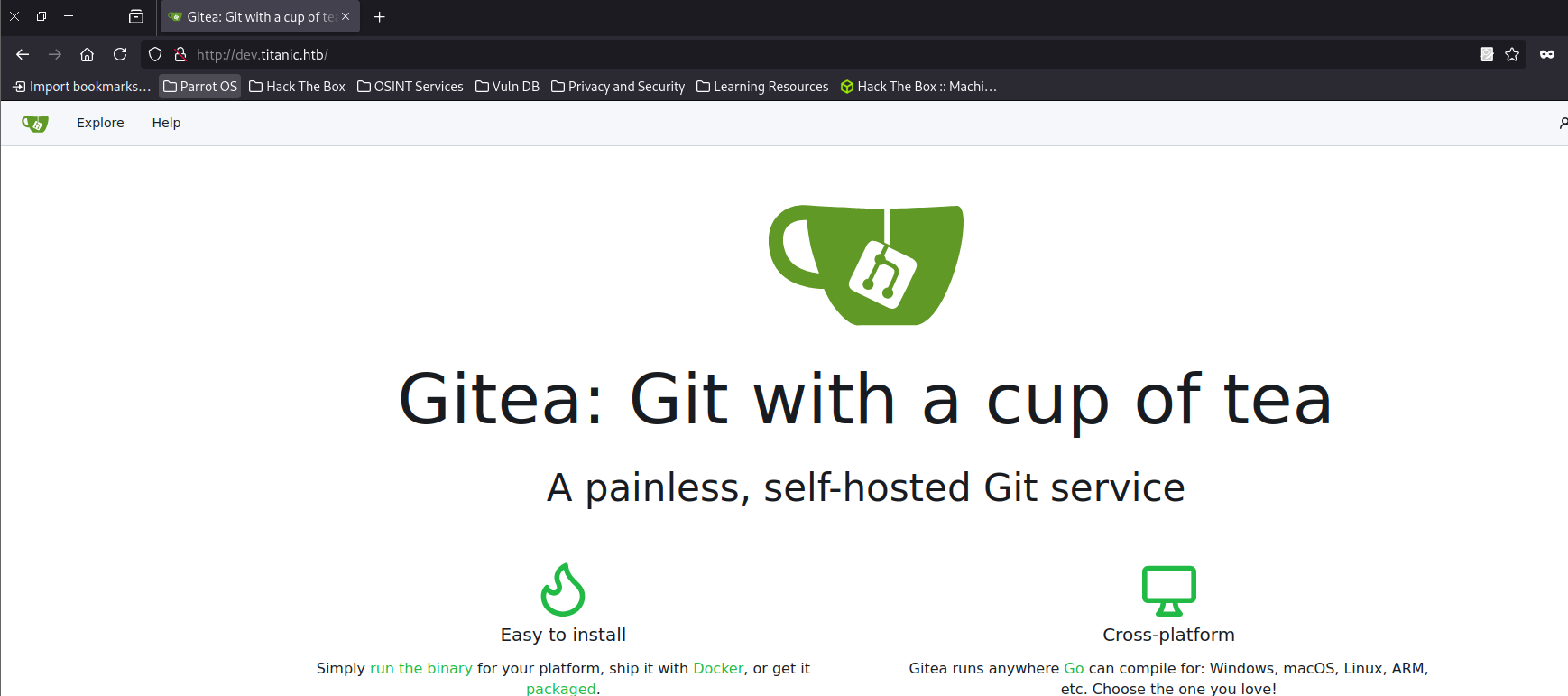
Ở đây có 1 user developer và đường dẫn file của tk, ta thử can thiệp tới



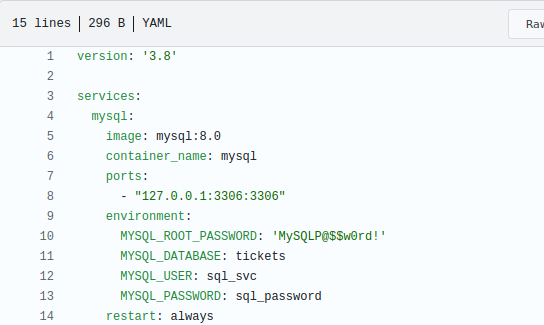
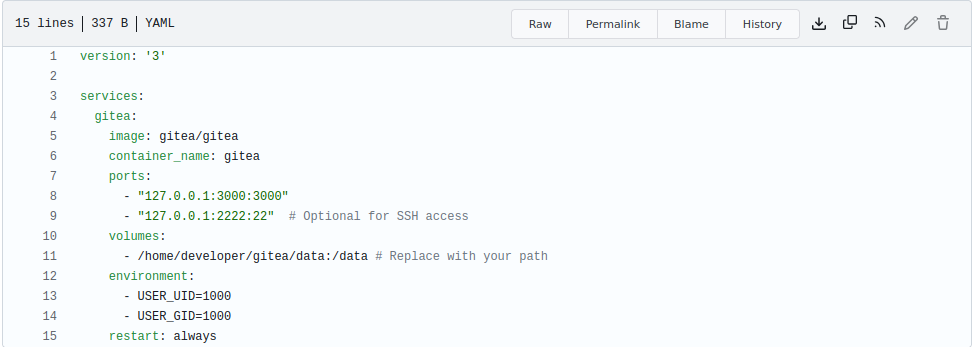
Truy cập vào và ta đã thấy dc flag đầu tiên

B3: Tìm root flag

Thử tìm kiếm trong domain dev.titanic.htb

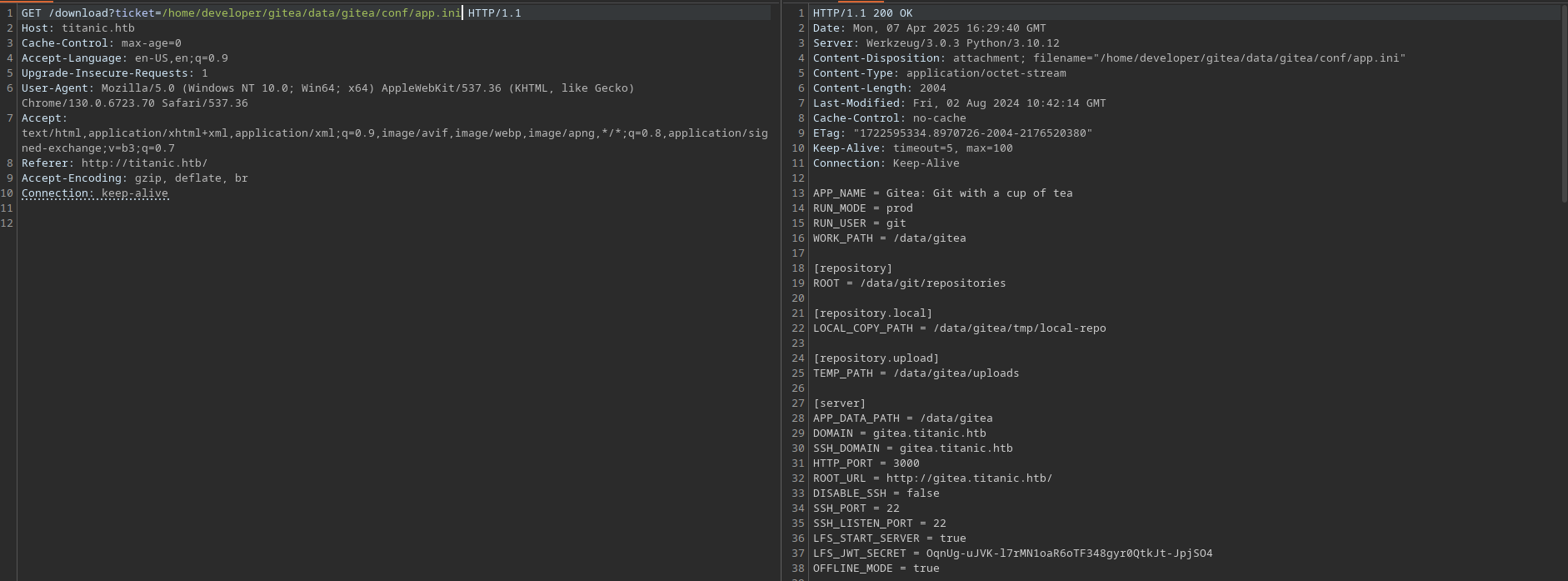


Trong đây có 2 repo

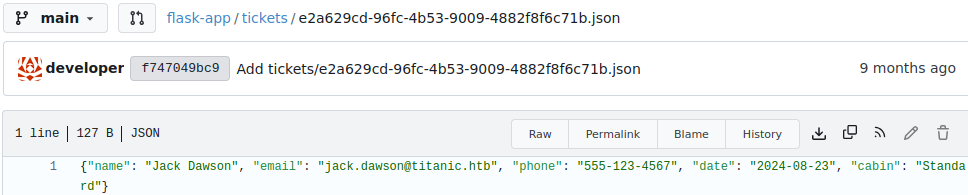
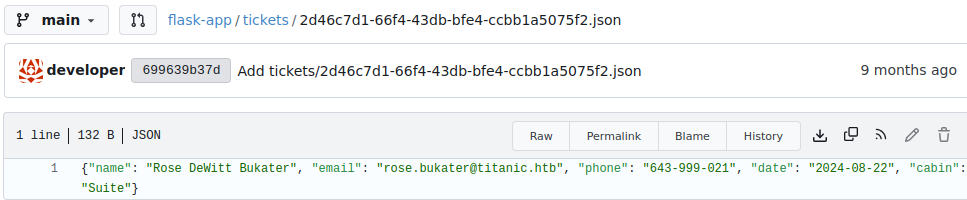


Kết hợp repo có thông tin volume và tra GG thì file config của gitea dc lưu tại app.ini

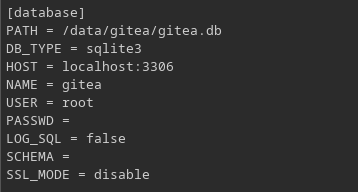
Tiếp tục dùng burp suit để đi đến file và xem cac thông tin



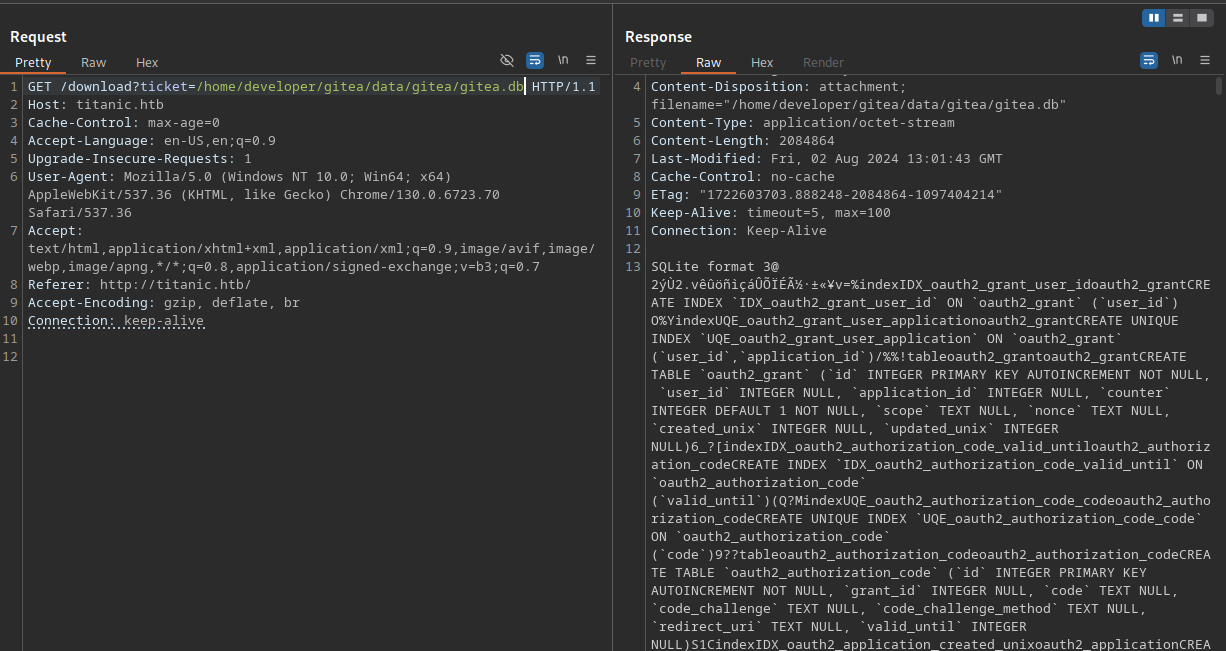
Xem repo của flask-app ta tìm dc 2 user nhg có lẽ k có tác dụng gì cả



Quay lại với thông tin file config lấy được ở trên

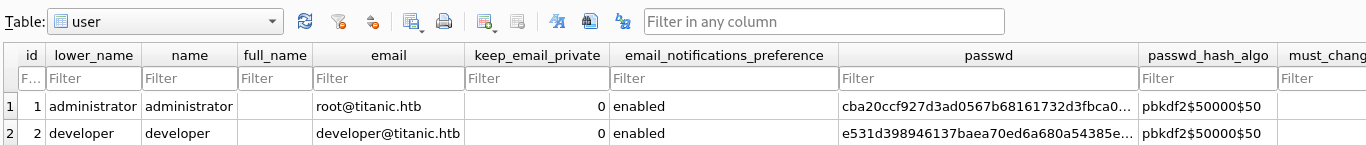
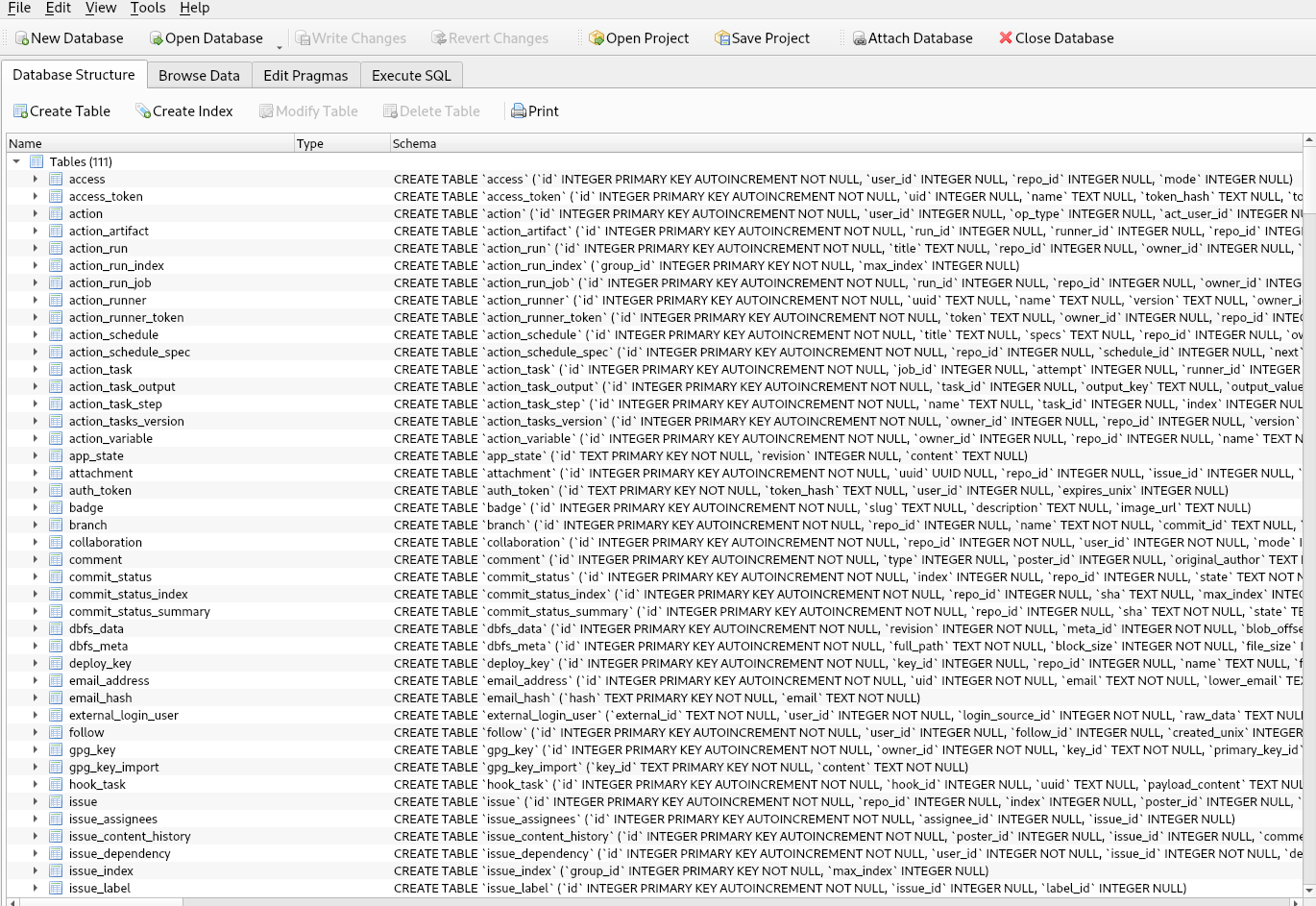


-> Có được đường dẫn của db



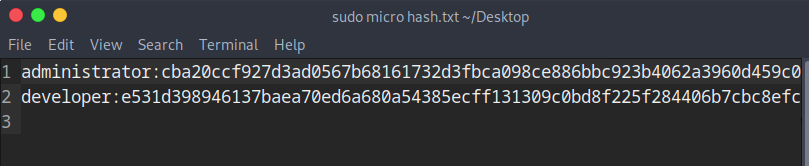
Quay lại với burp suite ta có nhập đường dẫn file db và phát hiện format SQLite.

Thực hiện mở với DB browser



Truy cập tới bảng của user ta có được hashs của mk của 2 tk admin và dev

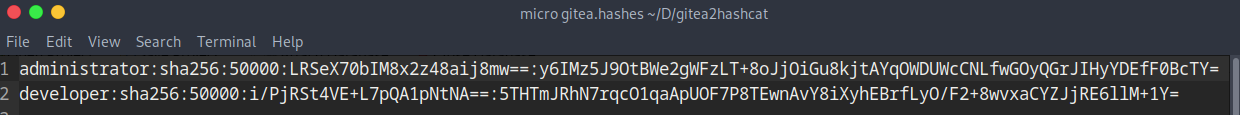
Ở đây có ghi phương thức hash luôn



Lưu lại thông tin hash

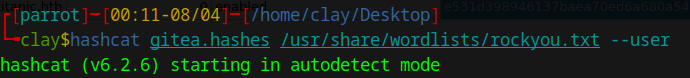
[F4dee3/gitea2hashcat: Script created in Bash to cracked the password of Gitea and export in Hashcat format.](https://github.com/F4dee3/gitea2hashcat)

Sử dụng tool này để giải mã hash

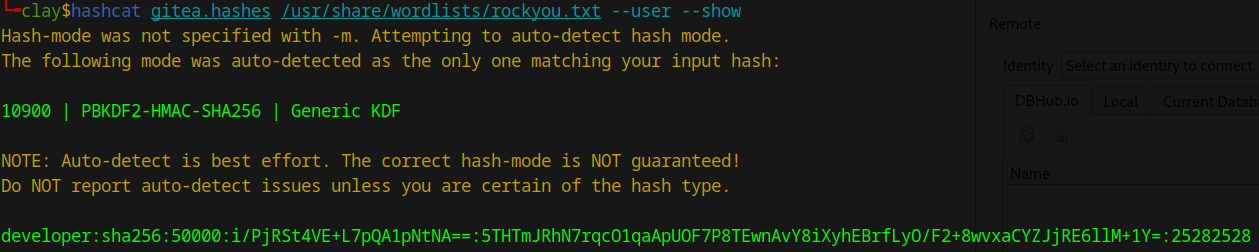


Ta có hash dạng chuẩn như sau và ta sẽ dùng hash cat để giải mã

Sử dụng hashcat



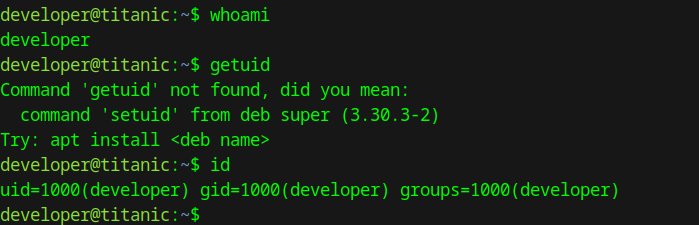
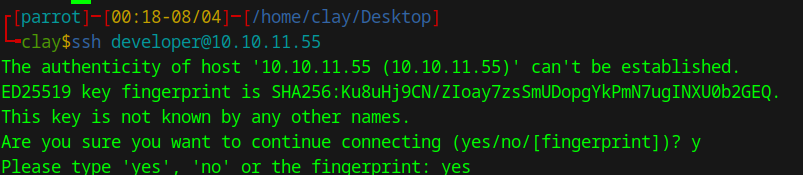
Ta giải mã thành công và chúng ta đã có dc mk



->passwd: 25282528

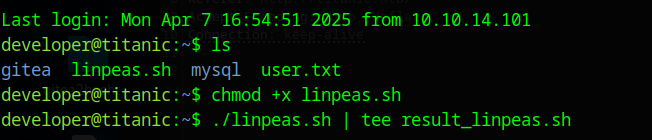
Ta SSH vào

xxxxxxxxxxxxx

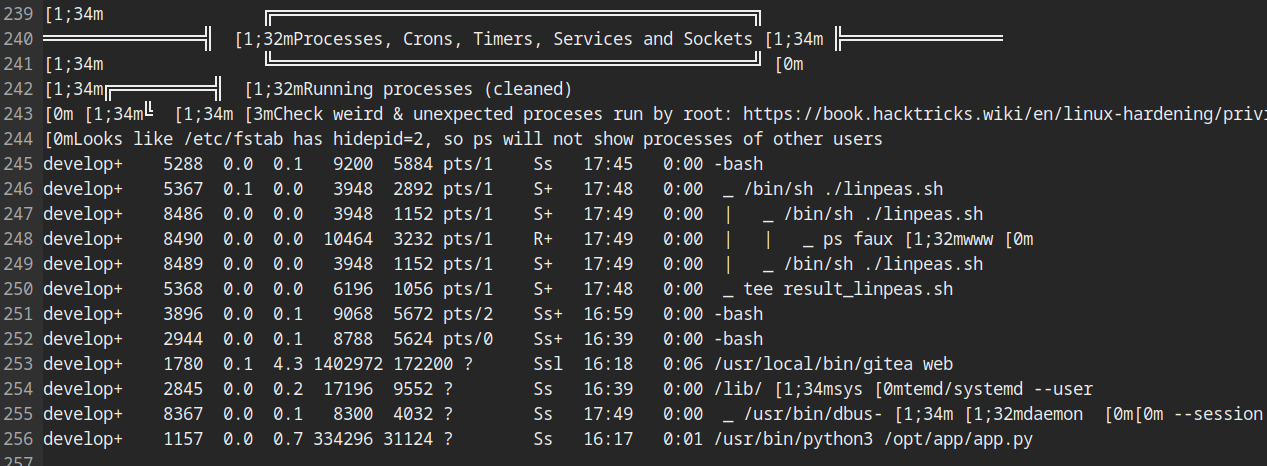
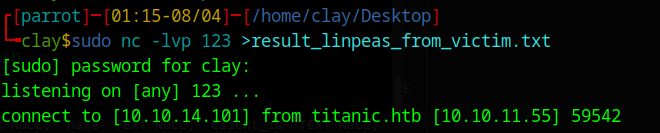


[PEASS-ng/linPEAS at master · peass-ng/PEASS-ng](https://github.com/peass-ng/PEASS-ng/tree/master/linPEAS)

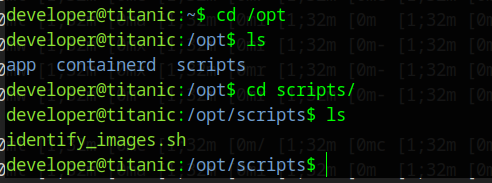
Ta sử dụng linPeas để quét các lỗ hổng leo thang đặc quyền trong máy nạn nhân



Dùng netcat để lấy file kq về ptich

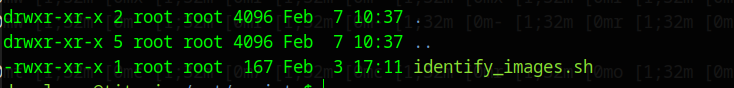


Ở dòng 256 cho thấy có 1 phần mềm python đang chạy và đường dẫn của nó

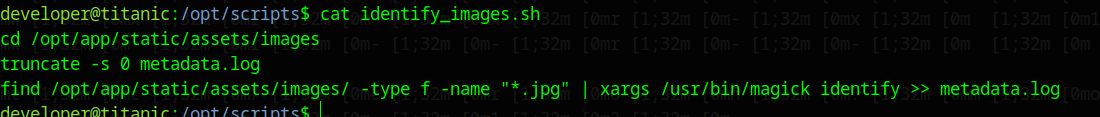


Ta truy cập vào thư mục trên và thấy có 1 file .sh

File thuộc quyền sở hữu của root

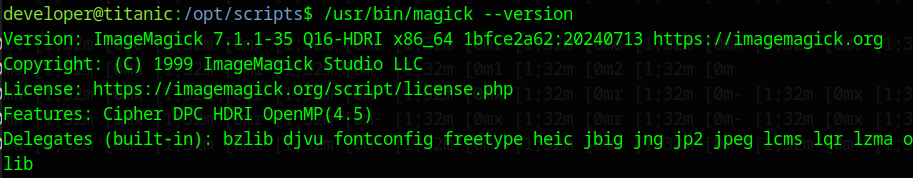


Nội dung như sau



-> cho thấy đang sử dụng tool ImageMagick

Ta sẽ kiểm tra và thử tận dụng ứng dụng này



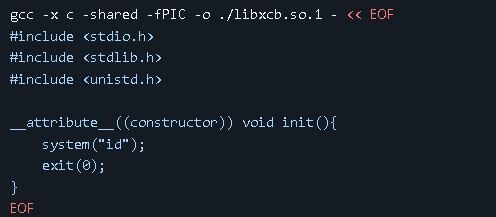
Đang chạy phiên bản 7.1

[NVD - CVE-2024-41817](https://nvd.nist.gov/vuln/detail/CVE-2024-41817)

Ta tìm dc 1 cve có thể exploit phần mềm này

[Arbitrary Code Execution in `AppImage` version `ImageMagick` · Advisory · ImageMagick/ImageMagick](https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-8rxc-922v-phg8)

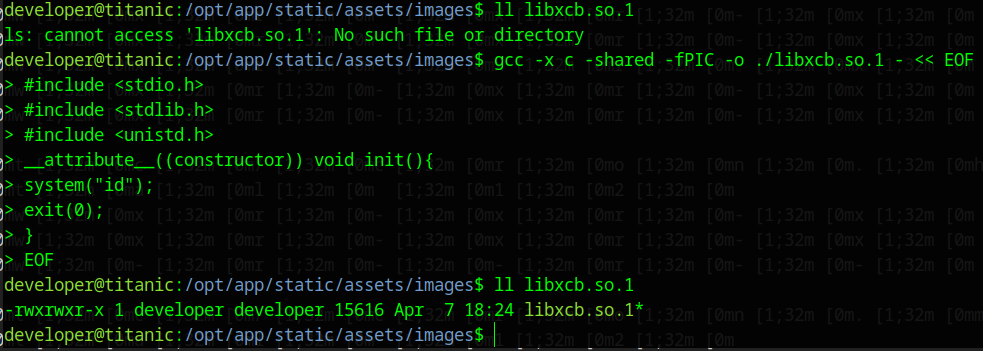
Ta tìm thấy 1 POC để khai thác



Ta thấy nếu tạo 1 shared libary vào thư mục hiện tại của hệ thống thì có thể thực thi câu lệnh mong muốn dc

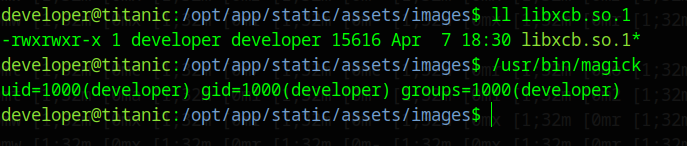
Với việc ở trong file bash identify\_image.sh có thông tin thư mục sẽ cd đến

-> ta thực hiện vào thư mục đó và tạo 1 shared library

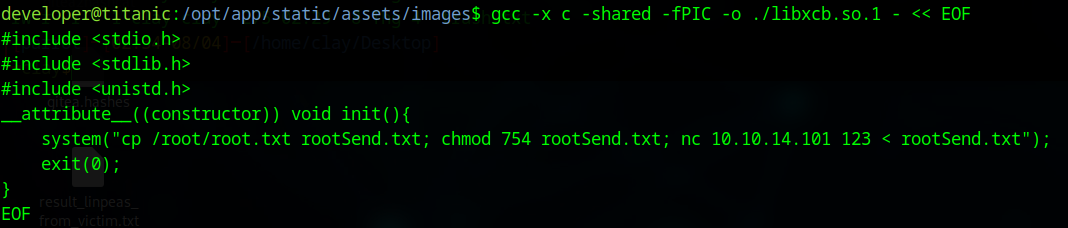


Ta thử xem có thực thi dc câu lệnh xem id k

Ta chạy tool magick thì thấy thực thi được câu lệnh xem id -> ta có thể thực thi câu lệnh tùy ý thông qua quyền root



Ta sẽ cp flag ở trong thư mục root ra và truyền qua netcat về máy tấn công



Ta cho chạy dòng lệnh cp file root và truyền qua net cat

Ta nhận được flag root

