|  |  |
| --- | --- |
| **BÁO CÁO**  ***PENETRATION TESTING***  Website Đào Hoàng Anh  **http://172.16.88.156:1234/index** |  |

**Phần 1: Kết quả đánh giá**

|  |  |
| --- | --- |
| **Thời gian đánh giá** | Tháng 07/2024 |
| **Kết quả chung** | Website đang có lỗ hổng liên quan tới CSRF, kẻ tấn công thực hiện các hành động không mong muốn thay mặt người dùng hợp lệ. Điều này làm giảm trải nghiệm người dùng |
| **Đề xuất** | Khắc phục các lỗi được đưa ra trong báo cáo. Về dài hạn, cần triển khai đồng bộ các giải pháp ATTT nhằm phát hiện, cảnh báo các hành vi bất thường khi truy cập vào hệ thống, đồng thời triển khai việc theo dõi các lỗ hổng, nguy cơ mới để từ đó có phương án nâng cấp, giảm thiểu các rủi ro này. |
| **Số lượng lỗi nghiêm trọng** | 0 |
| **Số lượng lỗi cao** | 1 |
| **Số lượng lỗi trung bình** | 0 |
| **Số lượng lỗi thấp** | 0 |
| **Ghi chú (nếu có)** |  |

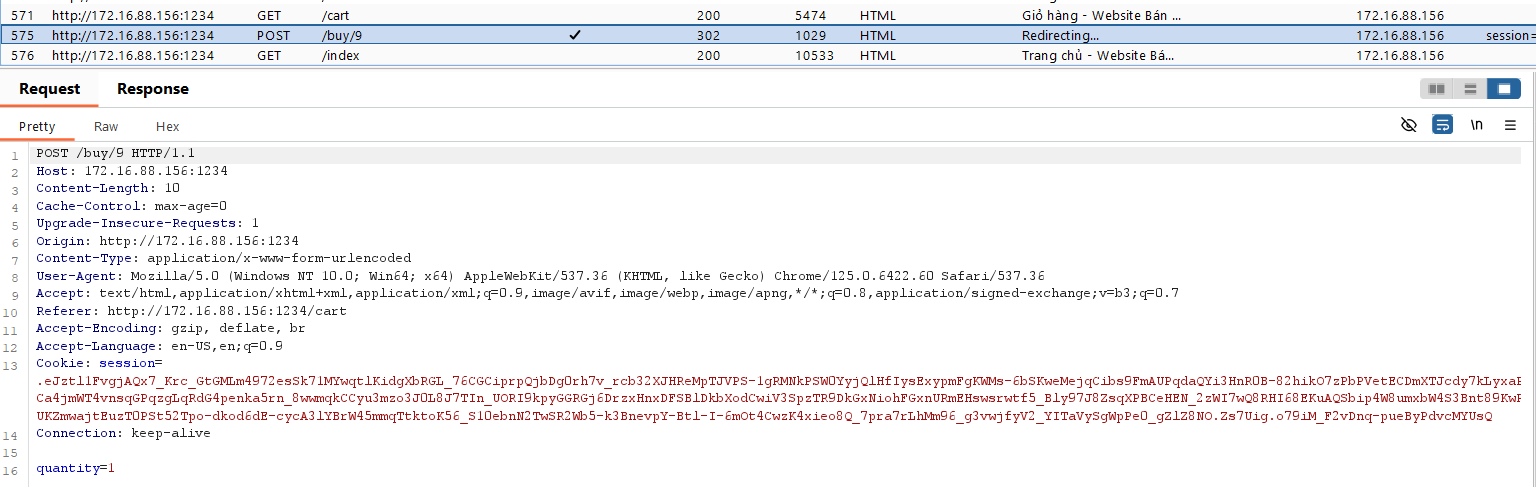
**Phần 2: Thông tin về các lỗ hổng**

1. **Danh sách lỗ hổng**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên Lỗi** | **Mô tả** | **Mức độ ảnh hưởng** |
| 1 | Lỗ hổng CSRF thêm vào giỏ hàng và mua hàng | Trong quá trình phân tích trang web, các request thêm vào giỏ hàng, mua hàng thoả mãn điều kiện một cuộc tấn công CSRF, người dùng hợp lệ không may truy cập vào link của kẻ tấn công sẽ tự động mua hàng, giảm trải nghiệm người dùng | Cao |
|  | **SSTI** |  |  |

1. **Chi tiết lỗ hổng**
2. **Lỗ hổng CSRF thêm giỏ hàng và mua hàng**

* **Mức độ: Cao**
* **Mô tả:** Test chức năng mua hàng, nhận thấy request mua hàng thoả mãn 3 điều kiện của 1 cuộc tấn công CSRF

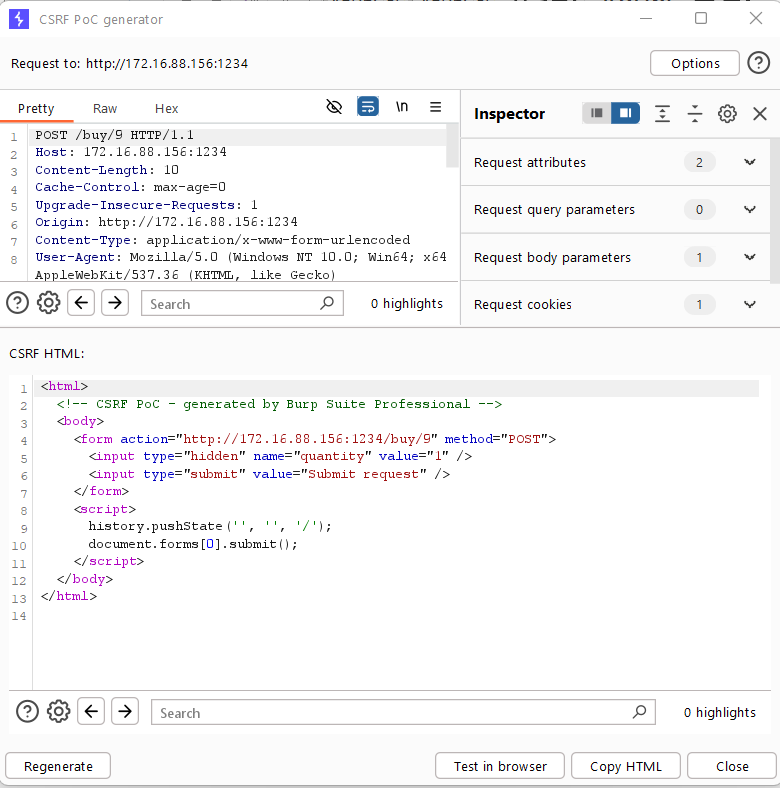


Hình 1: Request /buy/9 – mua hàng có id = 9

Thoả mãn 3 điều kiện của 1 cuộc tấn công CSRF:

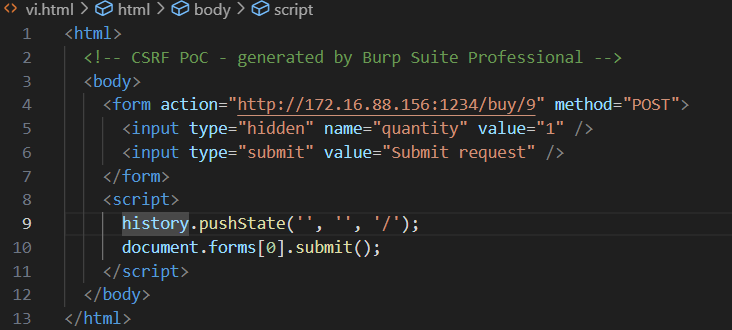
* Một hành động liên quan: Hành động mua hàng
* Xử lý phiên làm việc dựa trên cookie: cookie session = .eJzt….
* Không có tham số yêu cầu không thể đoán trước: Thoả mãn vì các tham số đều biết trước

Thực hiện tạo yêu cầu độc hại



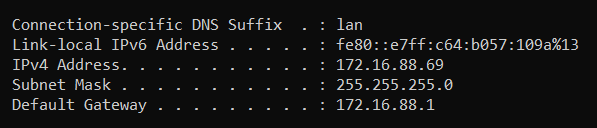
Hình 2: Yêu cầu độc hại

Chạy code vừa được sinh ra



Hình 3: Run code

IP của máy tính:



Hình 4: IP của máy tính là 172.16.88.69

Gửi đường dẫn: 172.16.88.69:5500/vi.html cho nạn nhân

Khi nạn nhân truy cập đường dẫn trên sẽ tự động mua hàng



Hình 5: Người dùng đã thực hiện hành động mua hàng không mong muốn

* **Khuyến nghị:**
  + Áp dụng token CSRF ngẫu nhiên và duy nhất cho mỗi phiên làm việc.
  + Xác thực nguồn gốc yêu cầu bằng cách kiểm tra các header Origin hoặc Referer.
  + Cấu hình cookie phiên làm việc với thuộc tính SameSite.
  + Yêu cầu người dùng xác nhận lại các hành động nhạy cảm.