|  |  |
| --- | --- |
| **BÁO CÁO**  ***PENETRATION TESTING***  Website Lê Minh Quân  **http://172.16.31.214:8000/** |  |

**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 |
| **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)** |  |

1. **Danh sách lỗ hổng**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên Lỗi** | **Mô tả** | **Mức độ ảnh hưởng** |
| 1 | Lỗ hổng CSRF | Trong quá trình phân tích trang web, nhận thấy trang web có khả năng bị tấn công CSRF, giảm trải nghiệm người dùng | Cao |

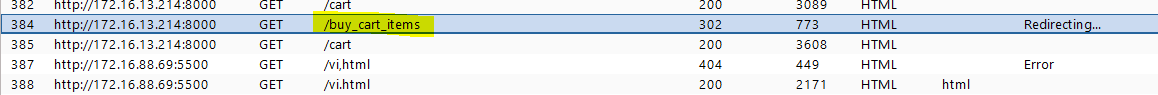
1. **Chi tiết lỗ hổng**
2. *Lỗ hổng CSRF*

* Mức độ: Cao
* Mô tả: Bắt request các nút như: “Add to Cart”, “Buy Now”, “SubmitFeedback”, thoả mãn 3 điều kiện xảy ra 1 cuộc tấn công CSRF

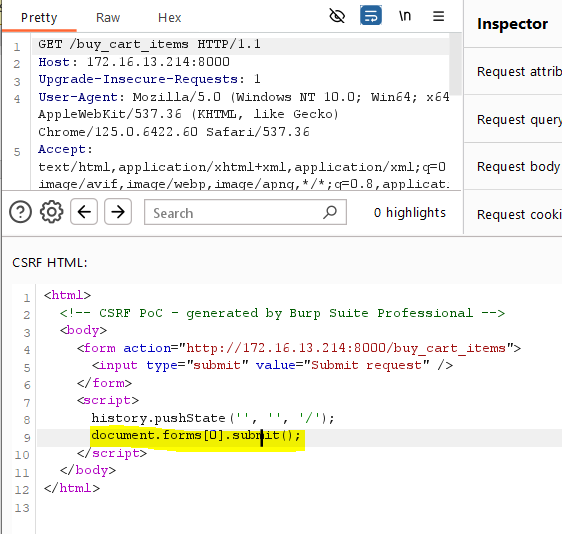
+ Điều kiện 1: Một hành động liên quan: Các nút thêm giỏ hàng, mua ngay, gửi feedback 🡪 Thoả mãn

+ Điều kiện 2: Xử lý phiên dựa trên cookie 🡪 Thoả mãn

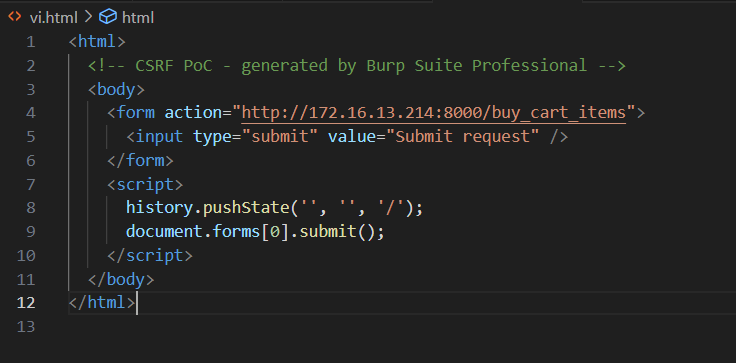
+ Điều kiện 3: Không có tham số yêu cầu không thể đoán trước 🡪 Thoả mãn



Hình 1. Bắt request hành động “Buy Now”



Hình 2. Tạo đoạn mã CSRF

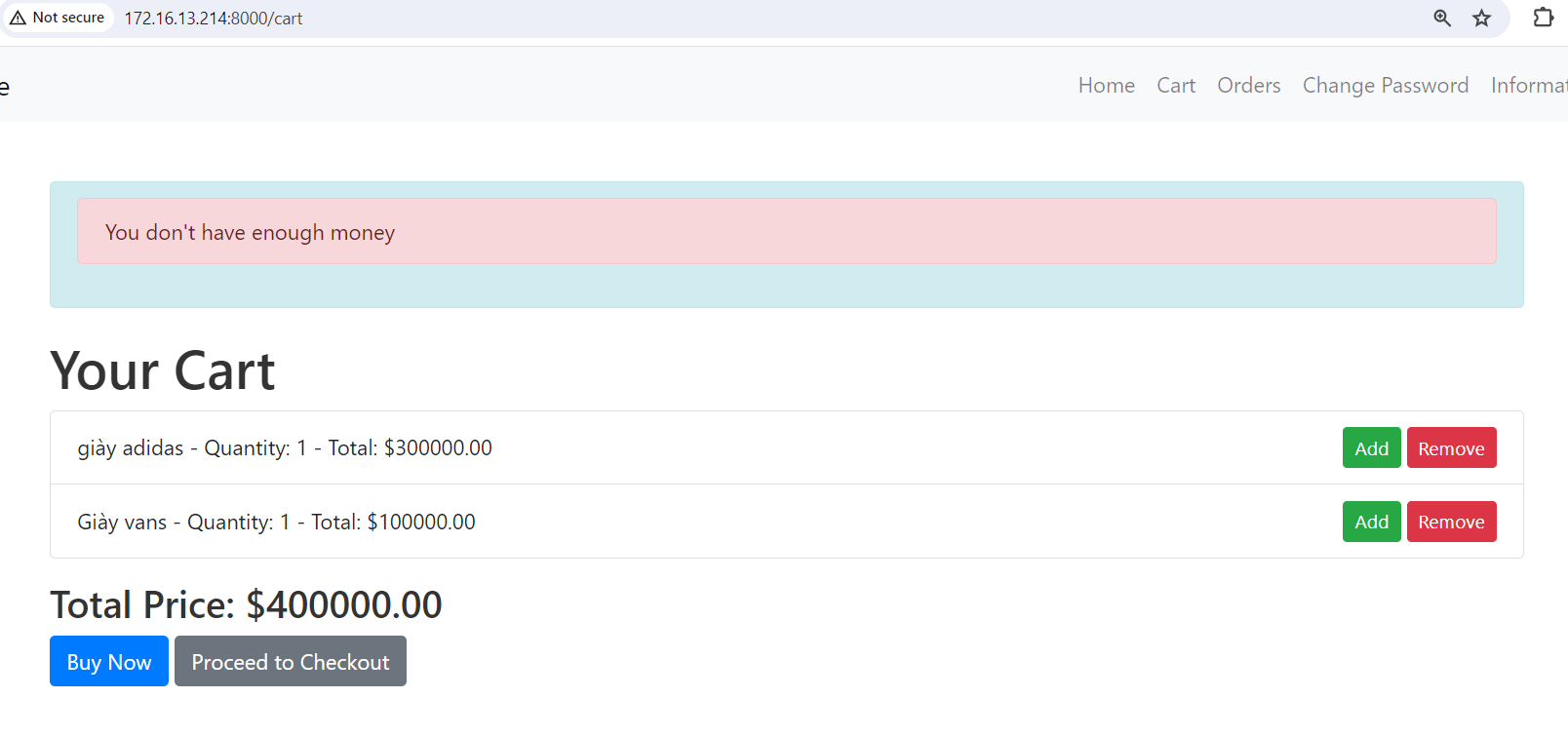


Hình 3. Chạy đoạn mã vừa tạo



Hình 4. IP của máy tính

Sau khi chạy code html, có thể gửi link: [**http://172.16.88.69:5500/vi.html**](http://172.16.88.69:5500/vi.html)cho nạn nhân, nạn nhân sau khi click link này sẽ tự động mua hàng ở giỏ hàng



Hình 5. Hoá đơn đã thay đổi