|  |  |
| --- | --- |
| **BÁO CÁO**  ***PENETRATION TESTING***  Website Mai Anh Quân  **http://172.16.88.108:9999/ShoeStore** |  |

**Phần 1: Kết quả đánh giá**

|  |  |
| --- | --- |
| **Thời gian đánh giá** | Tháng 07/2024 |
| **Kết quả chung** | Website đang có lỗ hổng liên quan tới business logic, cho phép người dùng bỏ qua các bước xác thực quan trọng. |
| **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** | 1 |
| **Số lượng lỗi cao** | 1 |
| **Số lượng lỗi trung bình** | 0 |
| **Số lượng lỗi thấp** | 0 |
| **Ghi chú (nếu có)** |  |

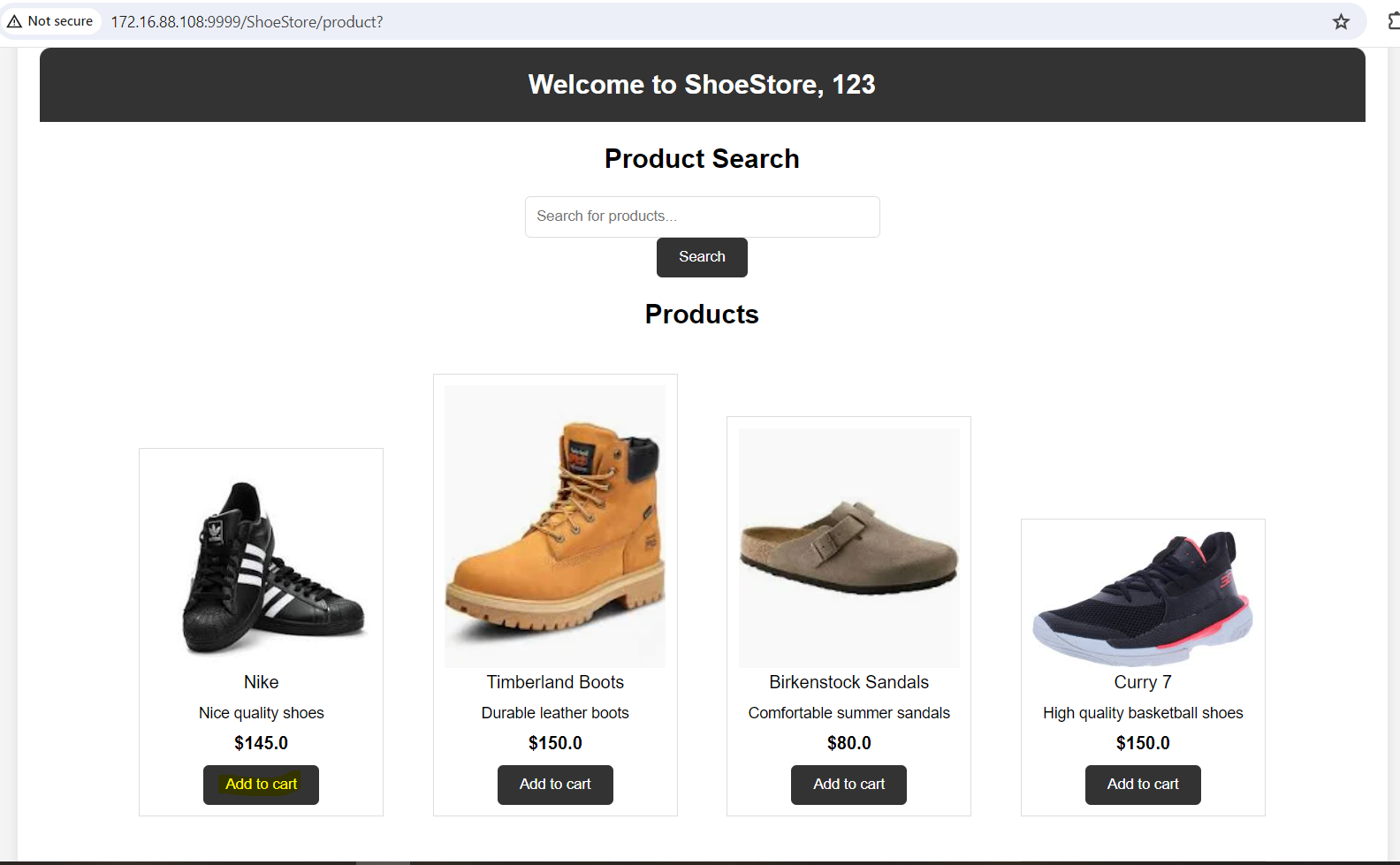
**Phần 2: Thông tin về các lỗ hổng**

1. **Danh sách lỗ hổng**

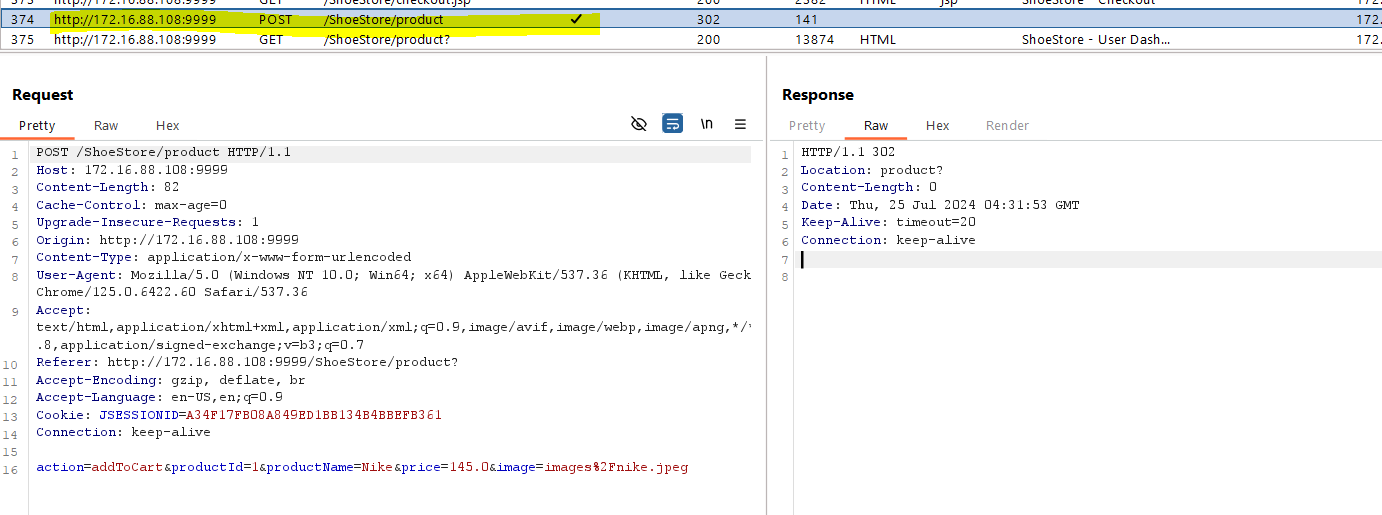
|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên Lỗi** | **Mô tả** | **Mức độ ảnh hưởng** |
| 1 | Lỗ hổng business logic chỉnh giá tiền trong giỏ hàng | Trong quá trình phân tích của trang web, request thêm vào giỏ hàng, các thuộc tính của đơn hàng hiện dưới dạng bản rõ, như id, tên, giá,…Điều này dẫn đến nguy cơ cao kẻ tấn công có thể sửa các thông tin đơn hàng, và mua với giá 0đ, làm ảnh hưởng tới việc kinh doanh của cửa hàng | Nghiêm trọng |
| 2 | Lỗ hổng chèn bất kỳ vào thuộc tính của đơn hàng | Kẻ tấn công cũng có thể chèn bất kỳ vào thuộc tính của đơn hàng, khi người dùng ấn vào có thể bị đánh cắp cookie,… chiếm quyền vào tài khoản | Cao |

1. **Chi tiết lỗ hổng**
2. *Lỗ hổng business logic có thể chỉnh giá tiền trong giỏ hàng*

* Mức độ: Nghiêm trọng
* Mô tả: Bắt request nút “Add to cart” các thuộc tính đơn hàng hiện bản rõ, kẻ tấn công có thể chỉnh sửa để mua hàng mà không cần tiền.

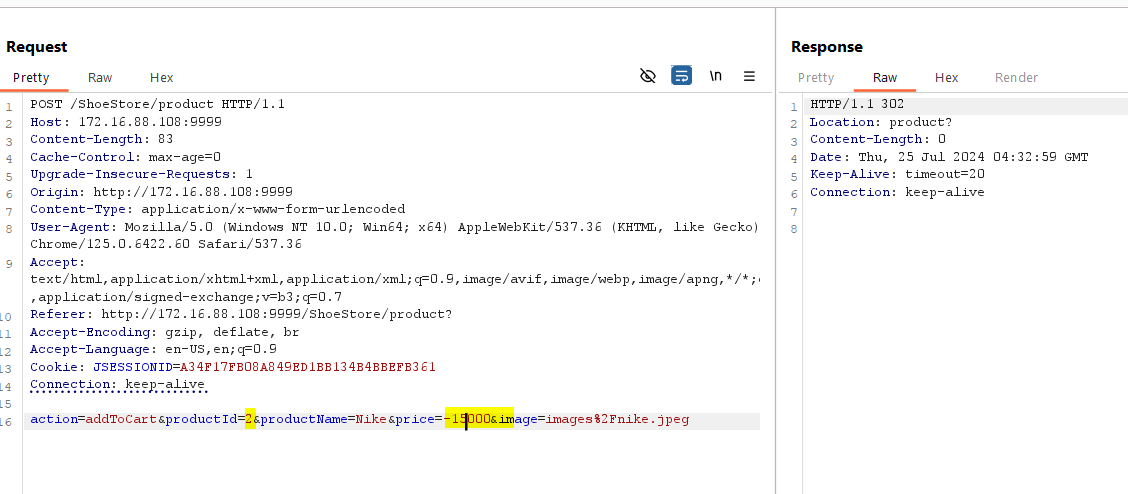


Hình 1. Bắt request hành động “Add to cart”



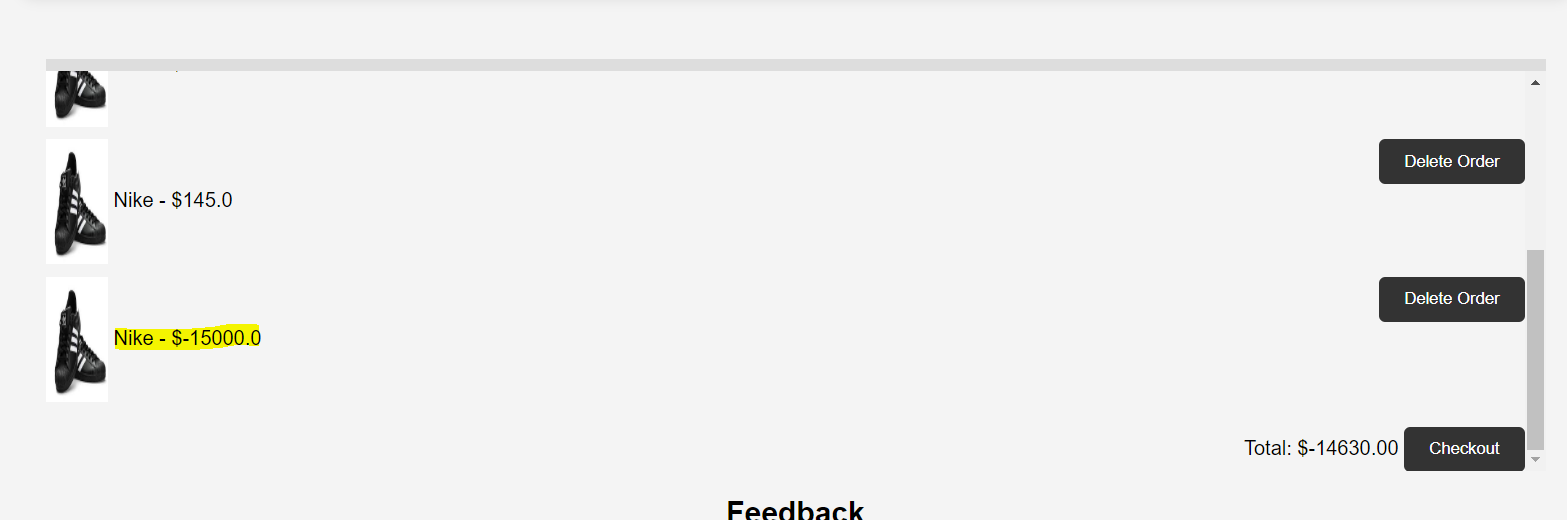
Hình 2. Gửi sang Repeater

Sửa “productId = 2” và “price=-15000” và “Send”



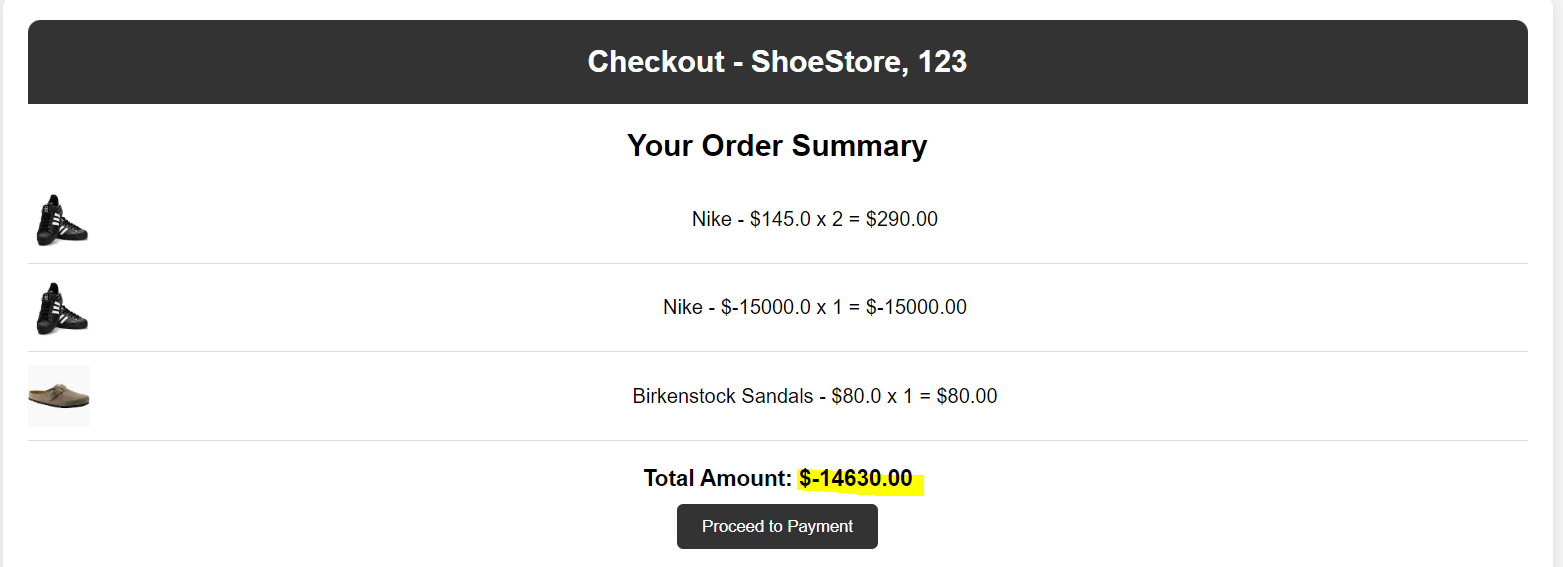
Hình 3. Sửa mã sản phảm và giá tiền

Trong giỏ hàng, số tiền đã bị thay đổi.



Hình 4. Giỏ hàng được thay đổi

Sau khi thay đổi giá tiền, có thể mua hàng

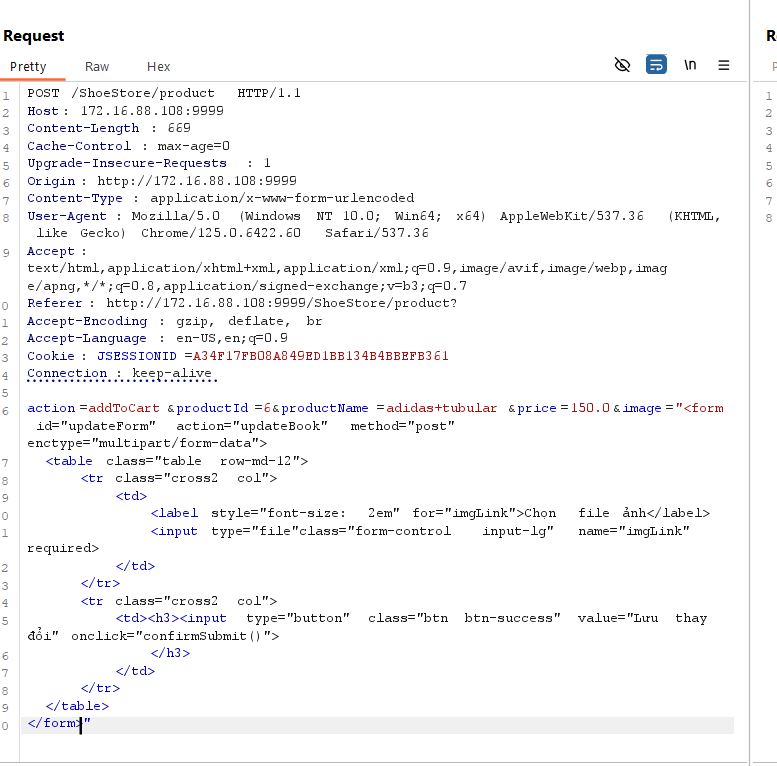


Hình 5. Hoá đơn đã thay đổi

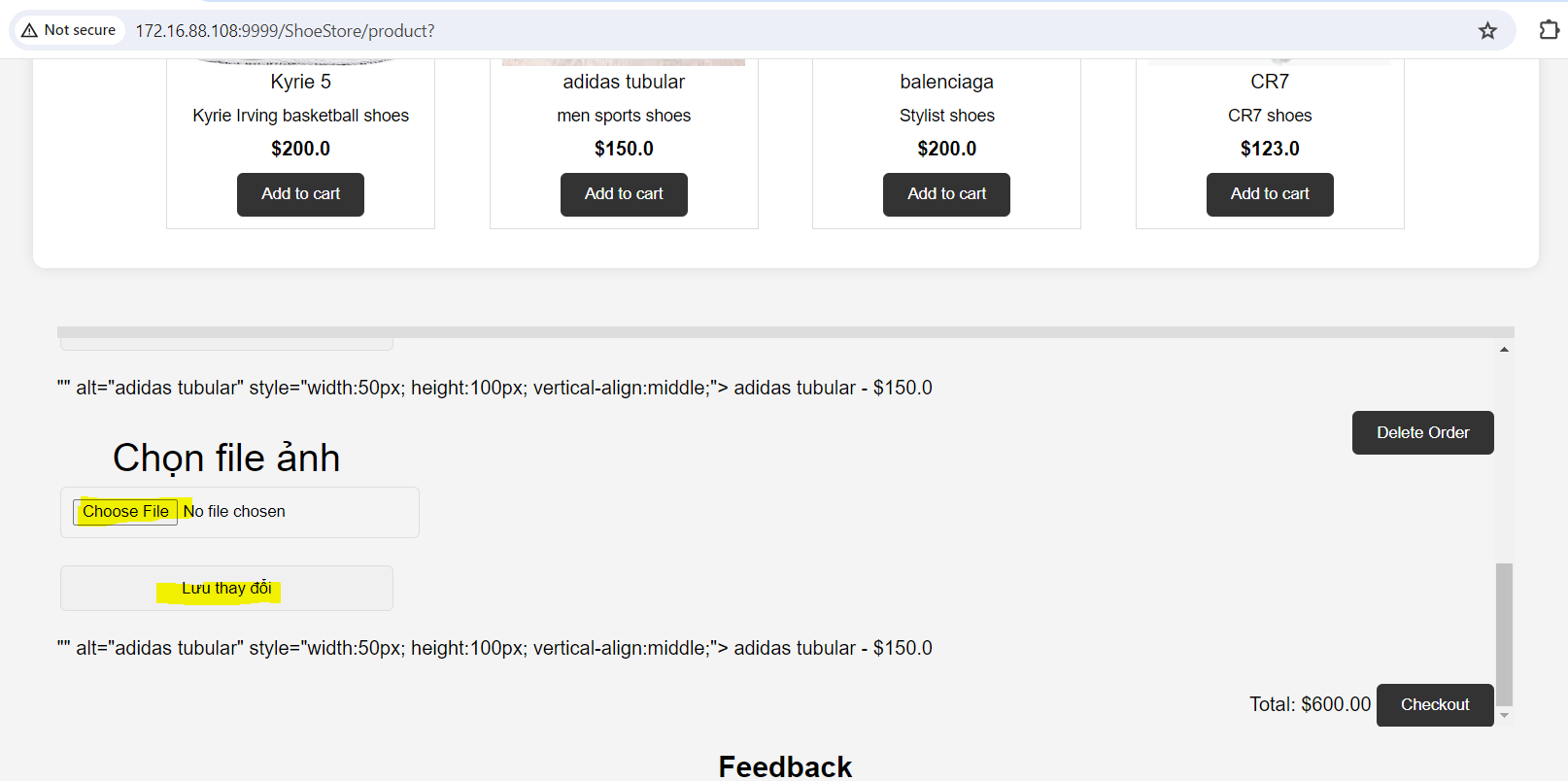
* Khuyến nghị:
  + Mã hóa các thuộc tính quan trọng của đơn hàng như id, tên, giá, v.v.
  + Xác thực thông tin đơn hàng trên server trước khi xử lý thanh toán.
  + Không lưu trữ hoặc truyền các giá trị nhạy cảm dưới dạng bản rõ trong request.
  + Sử dụng các token hoặc mã bảo mật để xác thực tính hợp lệ của các thuộc tính đơn hàng.

1. *Lỗ hổng chèn bất kỳ vào thuộc tính của đơn hàng*

* Mức độ: Cao
* Mô tả: Chèn 1 form bất kỳ vào thuộc tính images, giao diện trang web bị thay đổi



Hình 6. Sửa request “addToCart”



Hình 7.Giao diện trang web bị thay đổi

* Khuyến nghị:
  + Kiểm tra kỹ tất cả đầu vào từ người dùng để ngăn chặn việc chèn mã độc.
  + Sử dụng các header bảo mật như Content Security Policy (CSP) để hạn chế mã độc chạy trên trang.
  + Đảm bảo cookie được lưu trữ an toàn bằng cách sử dụng thuộc tính HttpOnly và Secure.