**Multi-endpoint race conditions**

Để làm được thử thách này, phải mua thành công Lightweight L33t Leather Jacket.

Tài khoản wiener chỉ cho chúng ta 100$. Nhưng áo khoác da Lightweight L33t lên tới 1337$.

Dự đoán 1 xung đột có thể xảy ra

1. Đăng nhập và mua gift card để bạn có thể hiểu được luồng thanh toán của trang web
2. Từ lịch sử của proxy, xác định tất cả điểm cuối cho phép bạn tương tác với giỏ hàng. Ví dụ, yêu cầu POST /cart thêm sản phẩm vào giỏ hàng và yêu cầu POST /cart/checkout thanh toán đơn đặt hàng.
3. Thêm 1 gift card khác vào giỏ hàng, sau đó gửi yêu cầu GET /cart đến Burp Repeater
4. Trong Repeater, thử gửi yêu cầu GET /cart mà không có session cookie. Chúng ta thấy không có session cookie thì giỏ hàng sẽ trống rỗng. Từ đó, bạn có thể suy luận rằng:

* Trạng thái của giỏ hàng được lưu trong session cookie
* Bất cứ hoạt động nào trên giỏ hàng đều được ghi lại trên session ID hoặc user ID.

1. Để ý thấy xác nhận đơn đặt hàng và thanh toán đơn đặt hàng chỉ xảy ra với 1 yêu cầu/phản hồi
2. Có thể có 1 race window xảy ra khi đơn đặt hàng được xác nhận và đơn đặt hàng được thanh toán. Điều này cho phép bạn thêm nhiều sản phẩm vào đơn hàng sau khi máy chủ kiểm tra xem bạn có đủ tiền để thanh toán không.

Thăm dò manh mối

1. Gửi cả hai yêu cầu POST /cart và POST /cart/checkout đến Burp Repeater
2. Trong Repeater, thêm hai tabs vào 1 nhóm mới.
3. Gửi chuỗi yêu cầu qua 1 kết nối duy nhất một vài lần. Để ý thấy thời gian phản hồi của yêu cầu thứ nhất đều lâu hơn yêu cầu thứ hai.
4. Thêm yêu cầu GET / ở đầu nhóm
5. Gửi cả ba yêu cầu qua 1 kết nối duy nhất. Quan sát thấy yêu cầu đầu tiên vẫn mất nhiều thời gian, nhưng bằng cách làm nóng kết nối thì yêu cầu thứ hai và ba được hoàn tất trong 1 cửa sổ nhỏ hơn nhiều
6. Chúng ta suy luận sự trì hoãn này là do kiến trúc mạng phía back-end hơn là thời gian xử lí của từng điểm cuối. Do đó, nó không có khả năng can thiệp vào tấn công của bạn.
7. Xóa yêu cầu GET / khỏi nhóm
8. Đảm bảo bạn có 1 gift card trong giỏ hàng
9. Trong Repeater, điều chỉnh yêu cầu POST /cart trong nhóm để mà tham số productId đặt là 1, ID của Lightweight L33t Leather Jacket.
10. Gửi chuỗi yêu cầu 1 lần nữa
11. Quan sát thấy đơn đặt hàng đã bị từ chối vì không đủ tiền, đây là kết quả mà bạn mong đợi

Chứng minh ý tưởng

1. Xóa áo khoác khỏi giỏ hàng và thêm 1 gift card khác
2. Trong Repeater, thử gửi yêu cầu 1 lần nữa nhưng lần này ở chế độ parallel.
3. Quan sát phản hồi khi gửi yêu cầu POST /cart/checkout:
4. Nếu bạn nhận được phản hồi "insufficient funds", xóa áo khoác khỏi giỏ hàng và lặp lại tấn công.
5. Nếu bạn nhận được phản hồi thành công thì bạn đã mua thành công áo khoác.