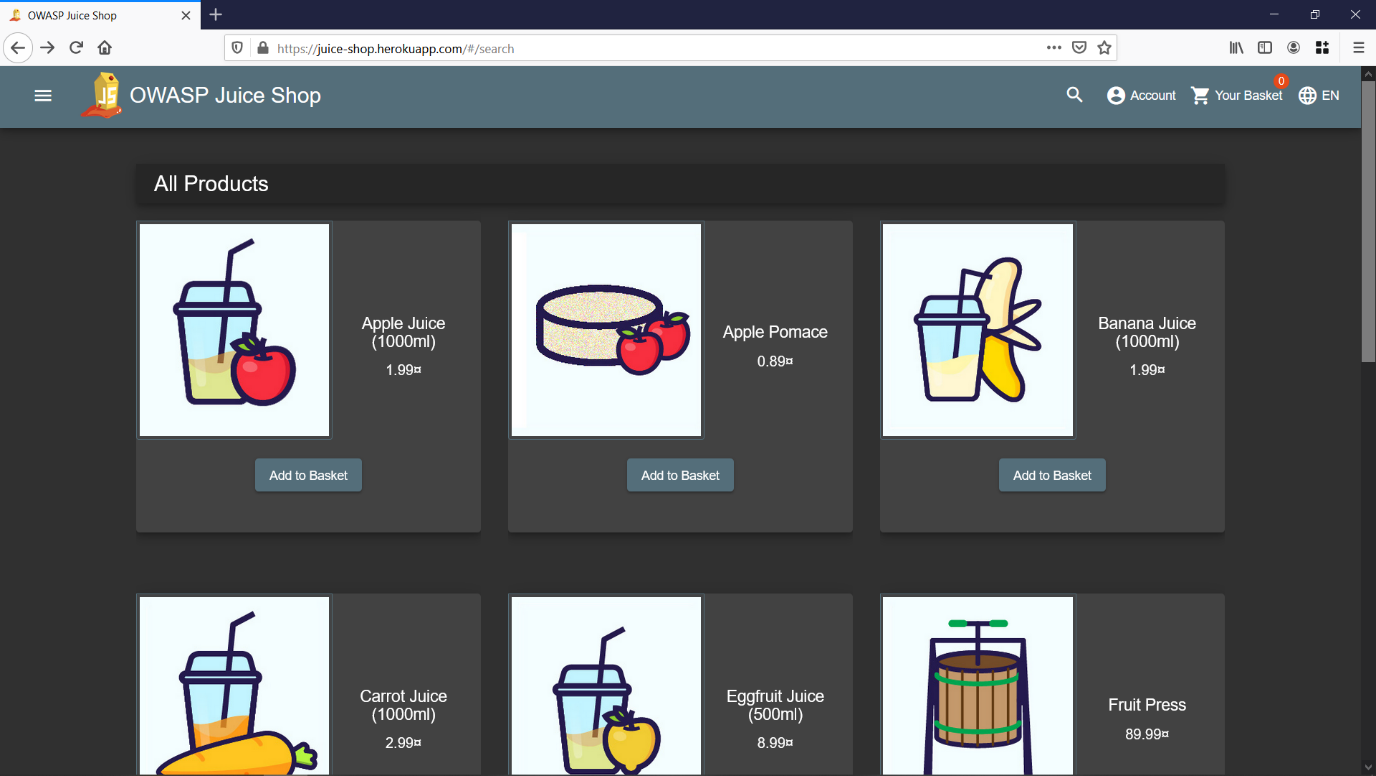
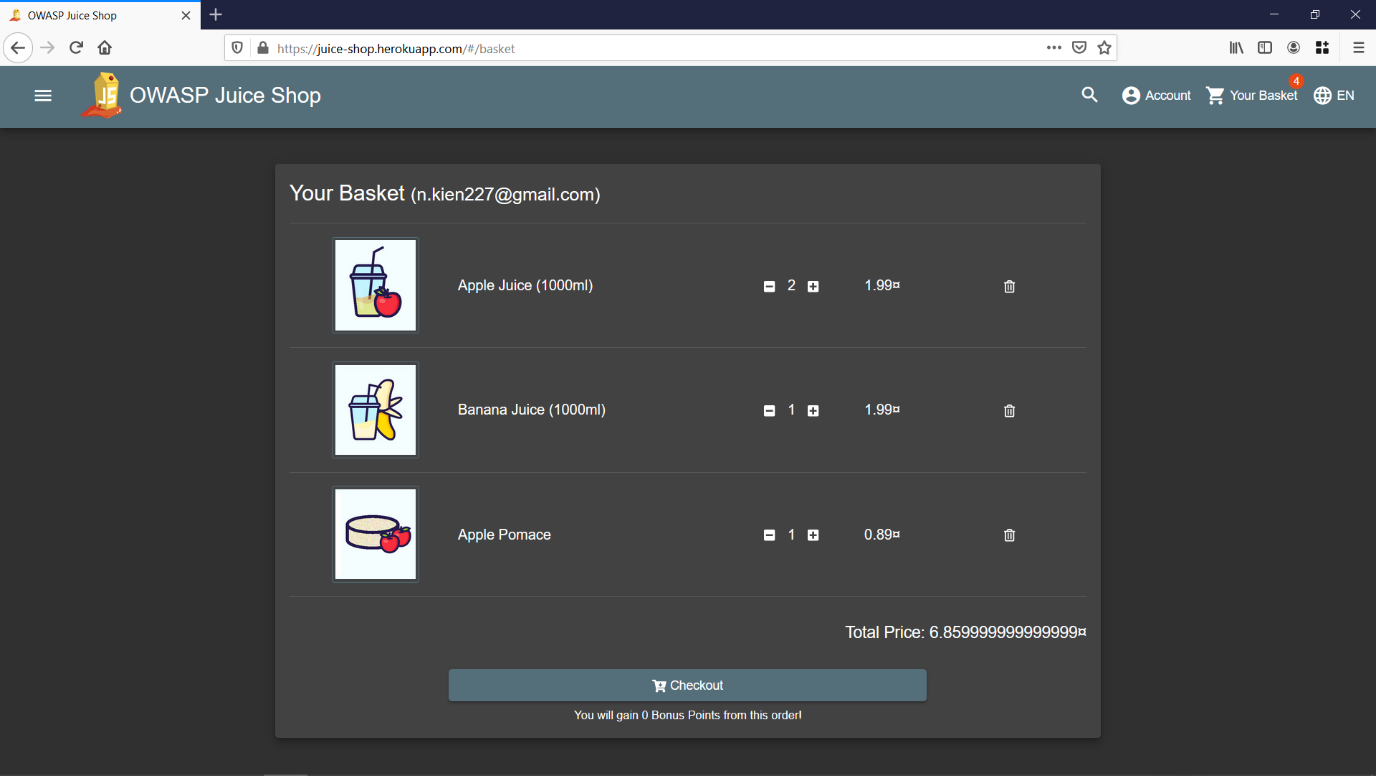
Using Burp to Test for Insecure Direct Object References

- Đầu tiên ta đăng kí một tài khoản trên web, giao diện của web như sau. 

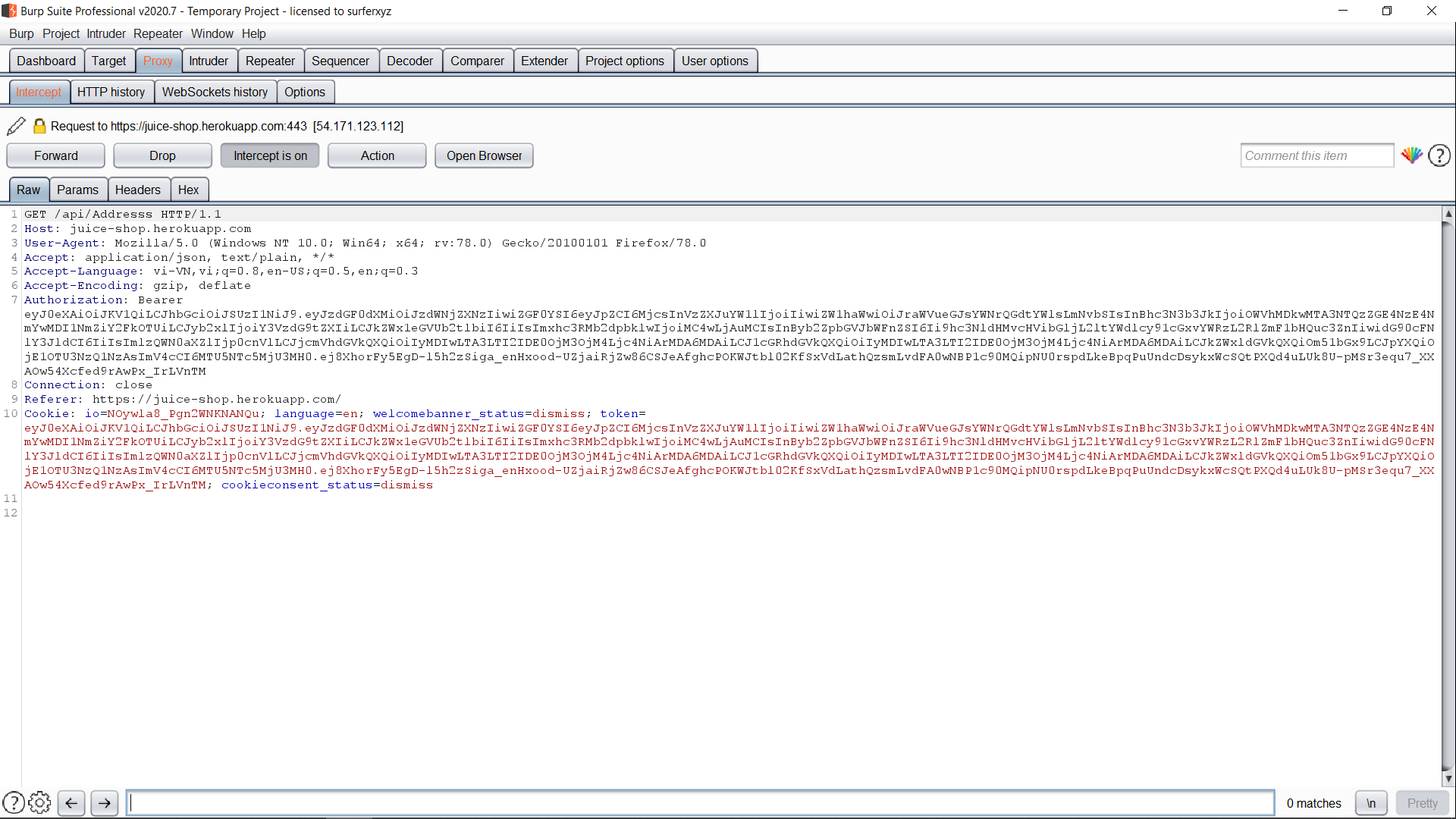
- Sau đó đăng kí và đăng nhập bằng tài khoản vừa tạo.

- Add các sản phẩm muốn mua vào “giỏ hàng” basket.

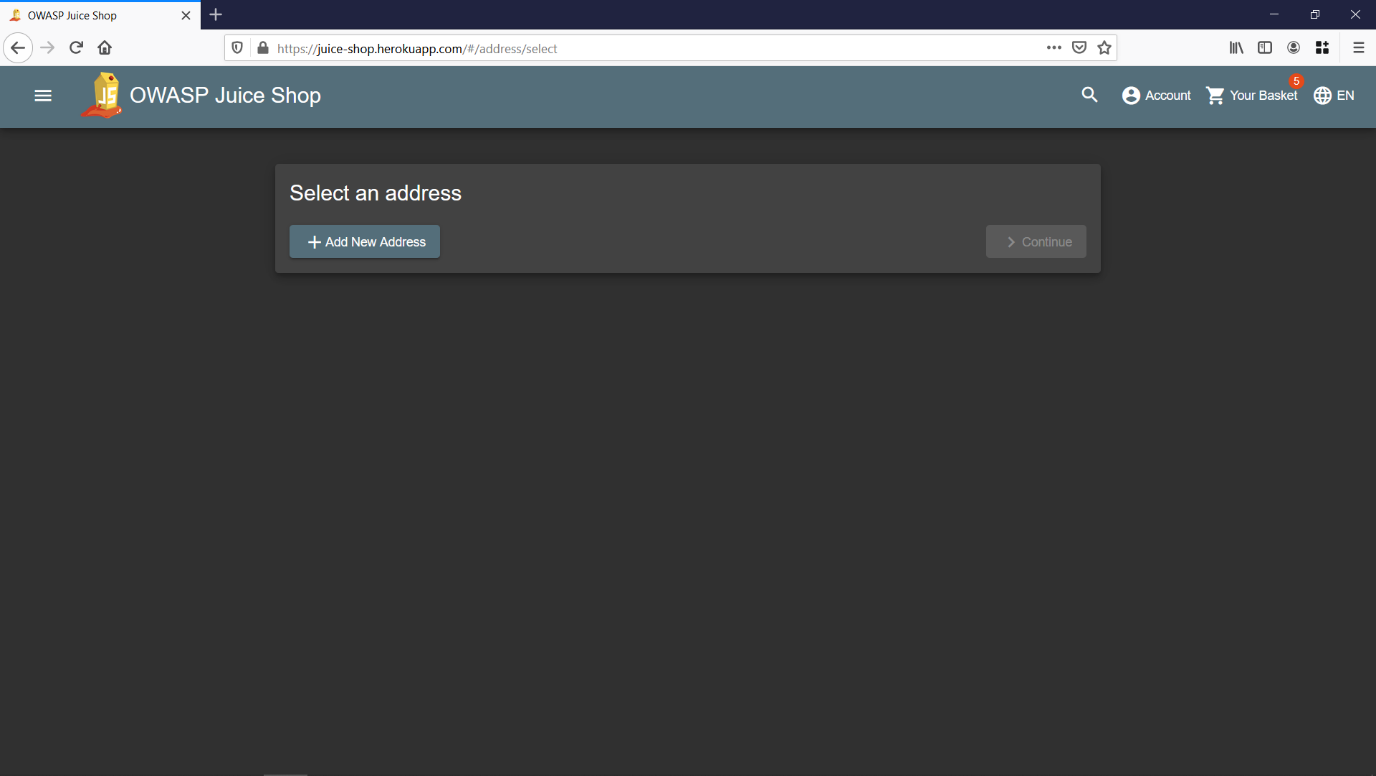
- Ta vào giỏ hàng để tiễn hành check out 

- Mở burp suite và bắt đầu test lỗi IDOR với intercept on tại tab Proxy.

- Bấm check out và bắt đầu theo dõi các lệnh được gửi đi.

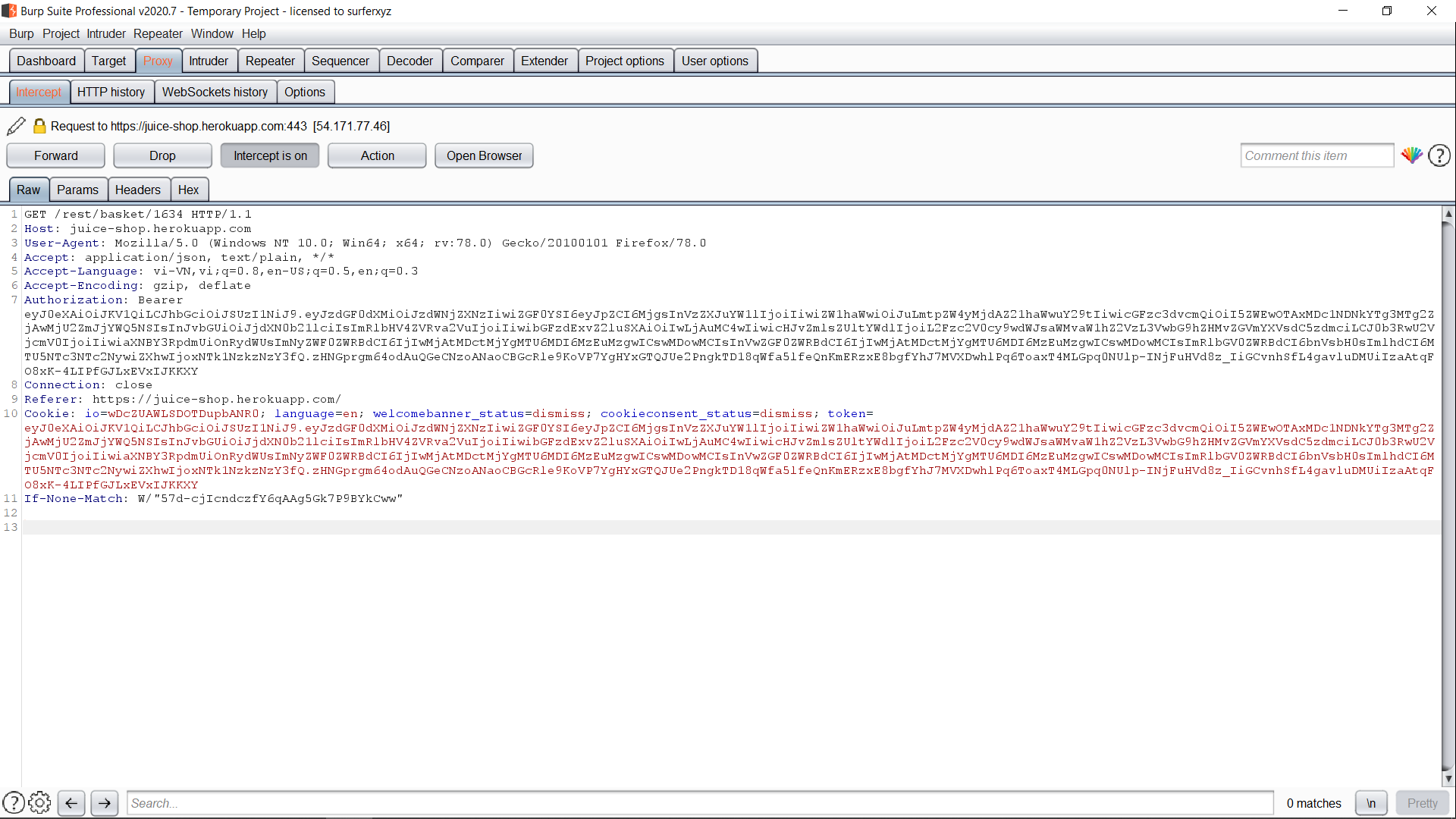


Tại website ta có giao diện



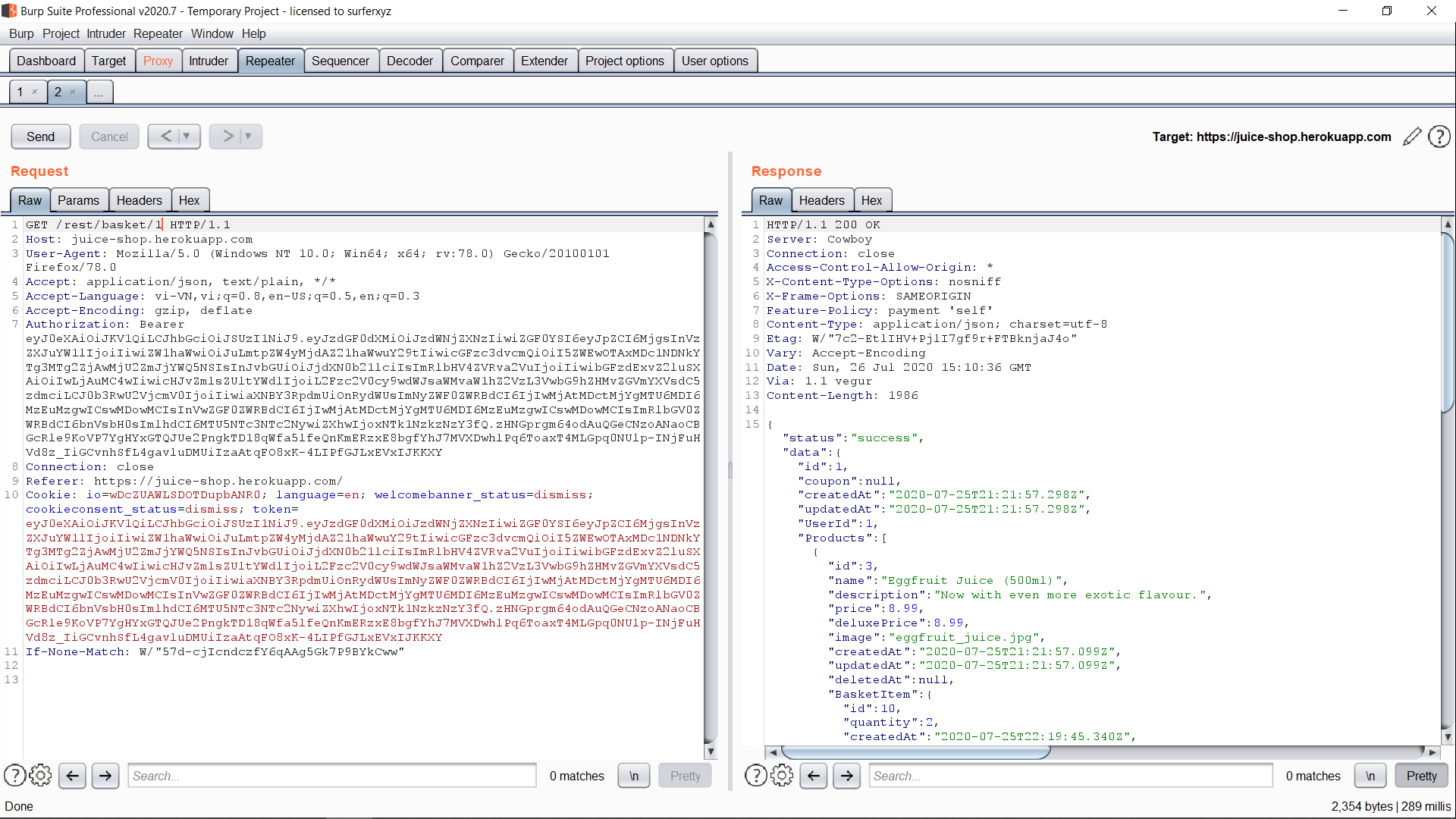
- Như đã thấy phần này ta cần provide address, tạm bỏ qua và chọn forward trong burpsuite.

- Dừng lại khi đã thấy mục tiêu (basket), goal của chúng ta ở đây sẽ là xem giỏ hàng của một người khác bằng lỗ hổng IDOR.



- Từ đây ta chọn send to repeater.

- Tại tab repeater ta sẽ thử thay đổi số liệu của basket cụ thể thành ../basket/1. Ta có kết quả tại phần response bên phải



- Dễ dàng nhận thấy các thông tin được trả về rất khác, điển hình như hóa đơn được tạo vào ngày 25-7, ta có Egg Juice, Green Smoothie, Juice Press và Juice Shop Adversary Trading Card thay vì các món hàng ta đã order, từ đây ta có thể quay lại website và access vào giỏ hàng của người kia và thay đổi thông tin giỏ hàng(thêm, bỏ các sản phẩm)

🡪 kết luận rằng website này có lỗ hổng IDOR.

1, IDOR là gì ?

- Về IDOR: là một dạng tấn công khi ta thay đổi các tham số đầu vào như userID, sessionID để đưa ta đến một giao diện với output khác (dữ liệu khác, của một người dùng khác), lỗ hổng này đã nằm trong danh sách top 10 OAWSP từ năm 2007 và sau 13 năm nó vẫn nằm trong top (giờ được gói trong lỗi Broken Access Control), lỗi này xảy ra khi lập trình viên hoặc người thiết kế web để lại một id quá dễ đoán và nhận ra (chưa được encrypt), khi đó tiềm ẩn nguy cơ lỗ hổng idor, hacker có thể truy vấn id và truy cập vào thông tin người dùng khác. Để khắc phục và tránh việc lỗ hổng này bị khai thác ta nên mã hóa, giấu đi các id dễ nhận thấy.

2, Nguyên nhân.

- Nguyên nhân là do các liên kết nhạy cảm của web, điển hình như tham số id dẫn đến user khác, các “giỏ hàng”, thông tin thanh toán không được bảo mật kĩ lưỡng.

3, Lỗ hổng trên có thể khai thác được để làm việc gì.

- Người tấn công có thể lợi dụng lỗ hổng này để thay đổi thông tin người dùng, thông tin thanh toán, hoặc khai thác sâu hơn để lấy thông tin quan trọng hơn.

4, Cách khắc phục.

- Các id, tham số của trình duyệt là phần nhạy cảm nhất để có thể bắt đầu khai thác lỗ hổng idor, để khắc phục ta cần generate các id khó đoán hơn thay vì “1, 2, hay tên người dùng”, hoặc giấu đi để các hành vi truy vấn thông tin qua tham số có thể phòng tránh được.