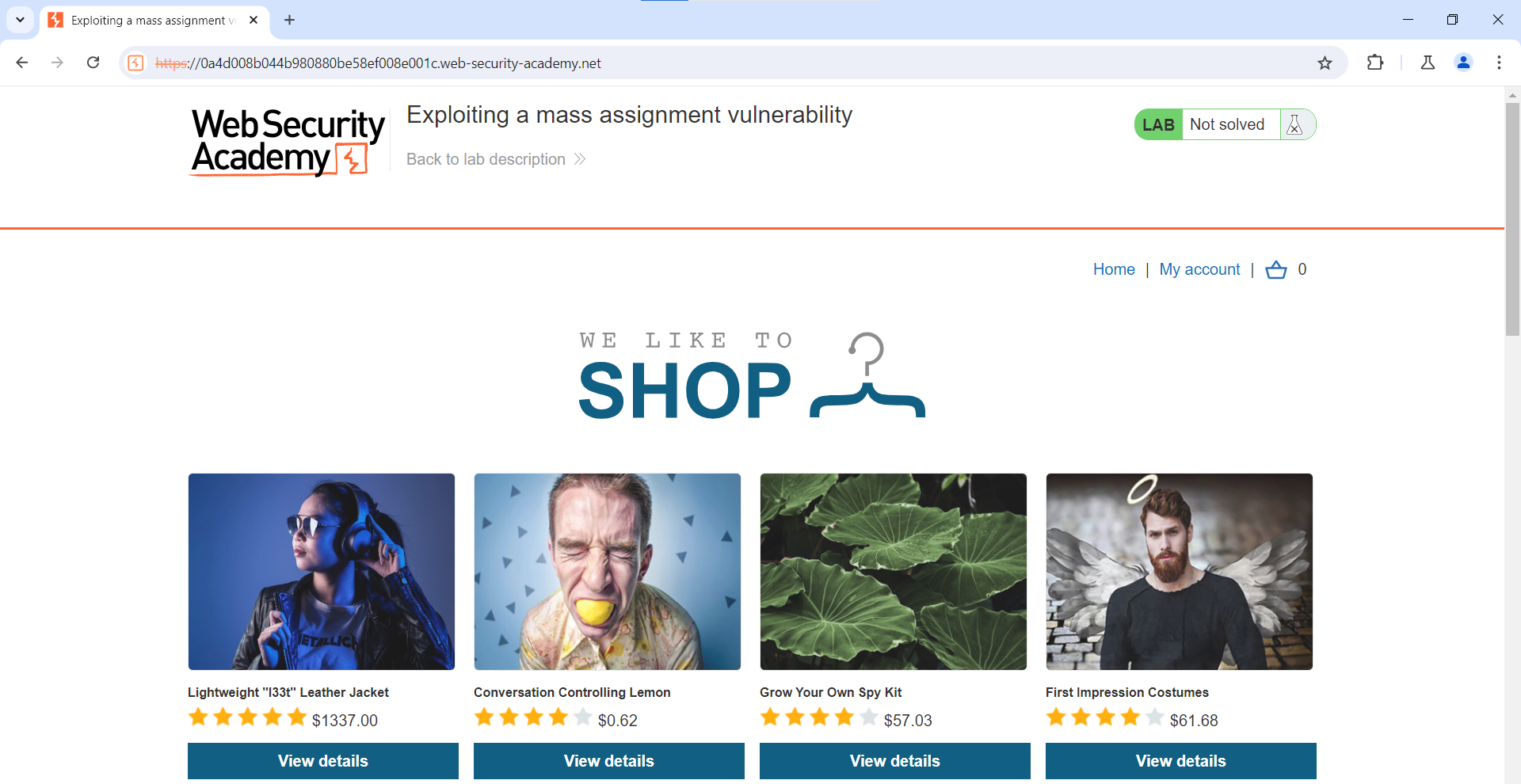
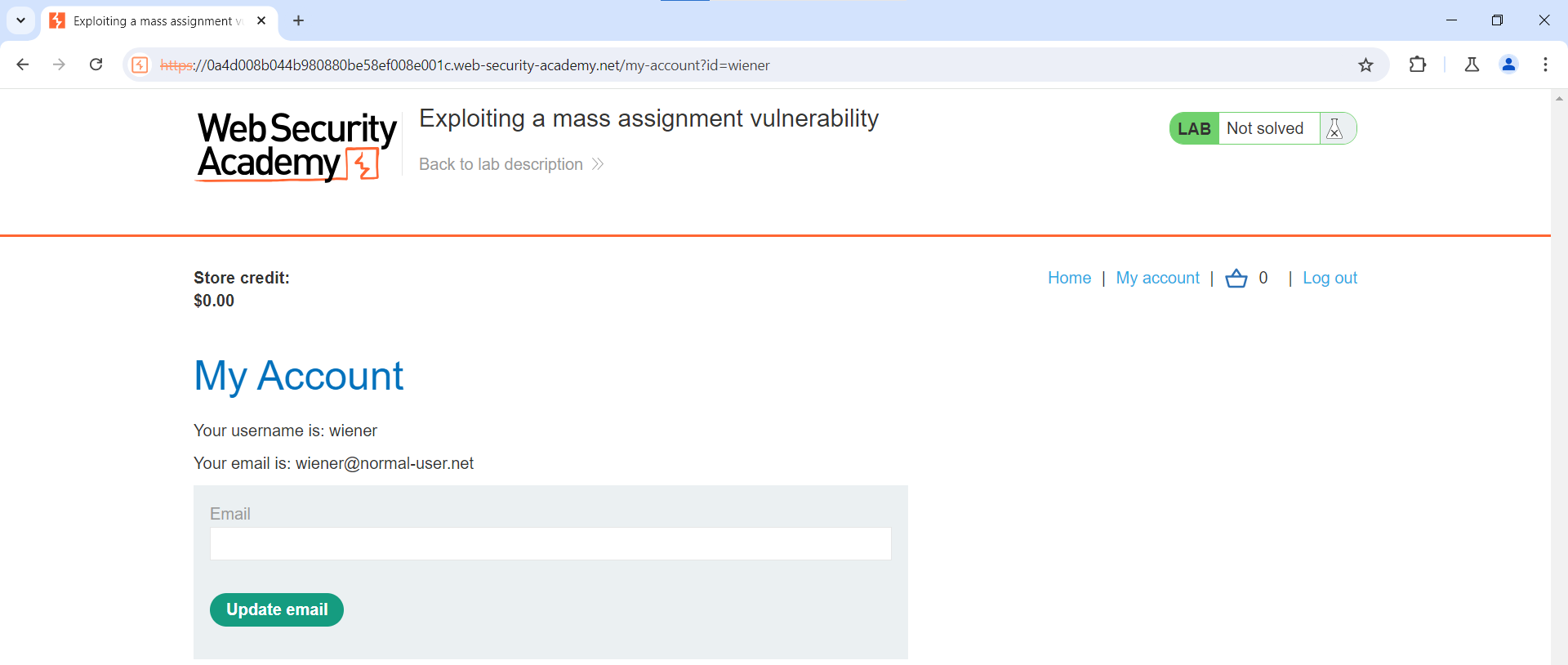


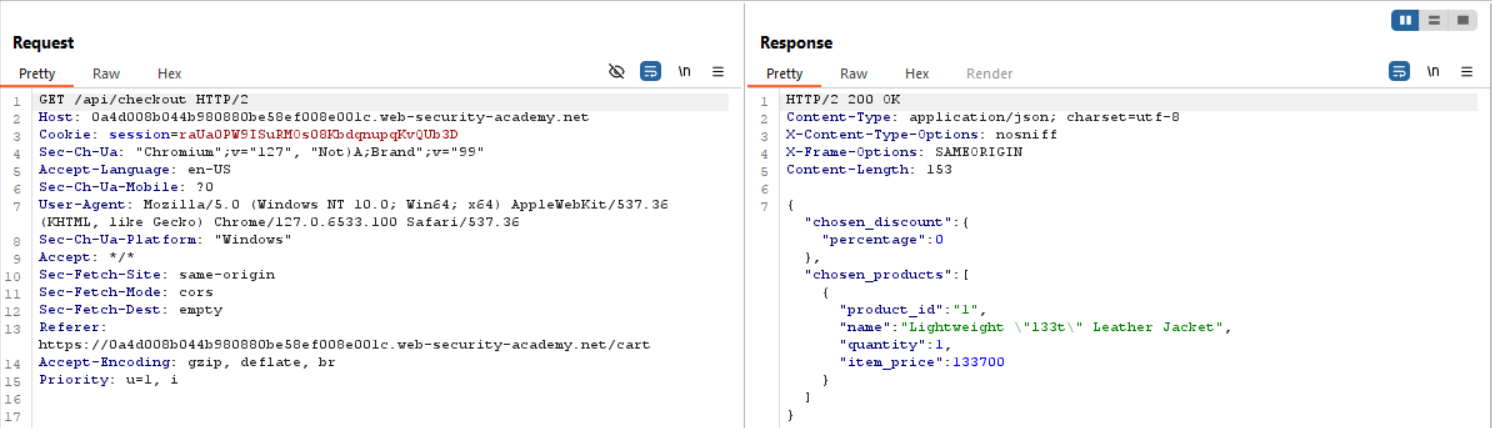
* Mục đích: Mua sản phẩm “Lightweight l33t Leather Jacket”

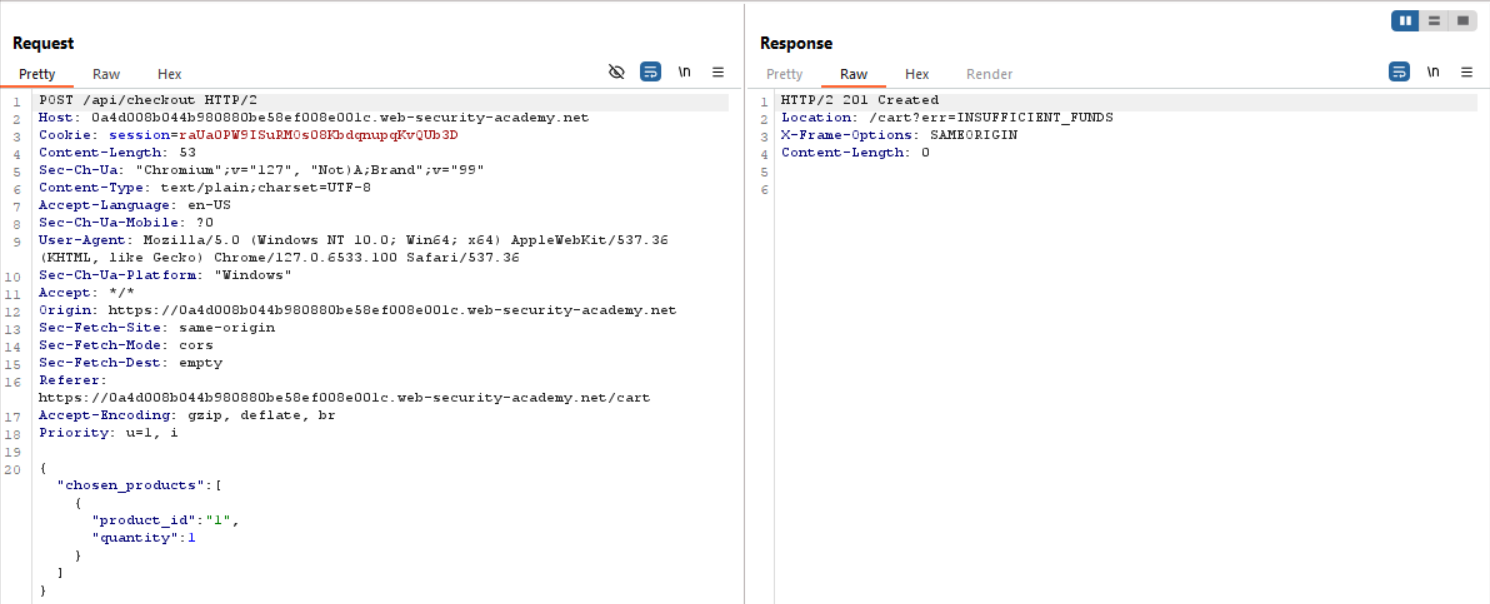


* Đăng nhập tài khoản người dùng wiener

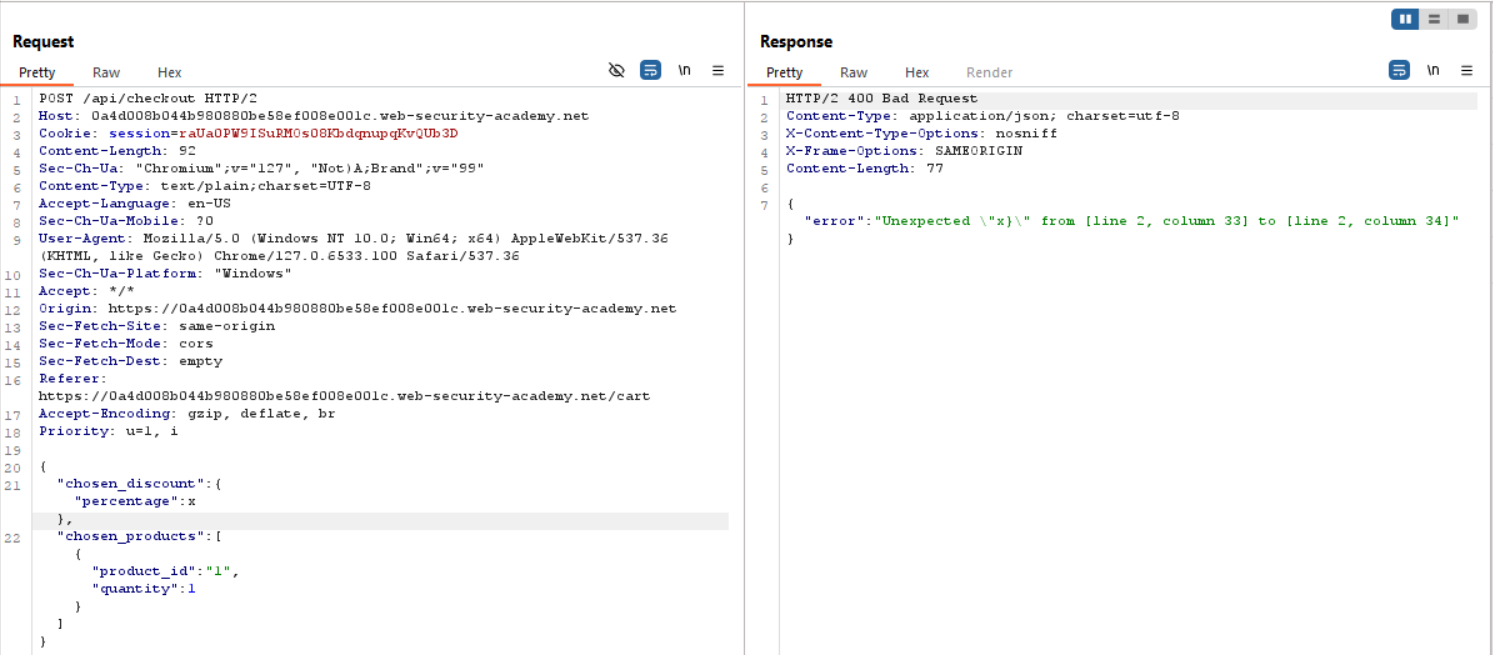


* Thử đọc các gói tin bắt bằng BurpSuite nhưng không có thông tin gì đặc biệt
* Khi thử mua sản phẩm nhưng không đủ tiền, tuy nhiên ta lại bắt được một gói tin có chứa API

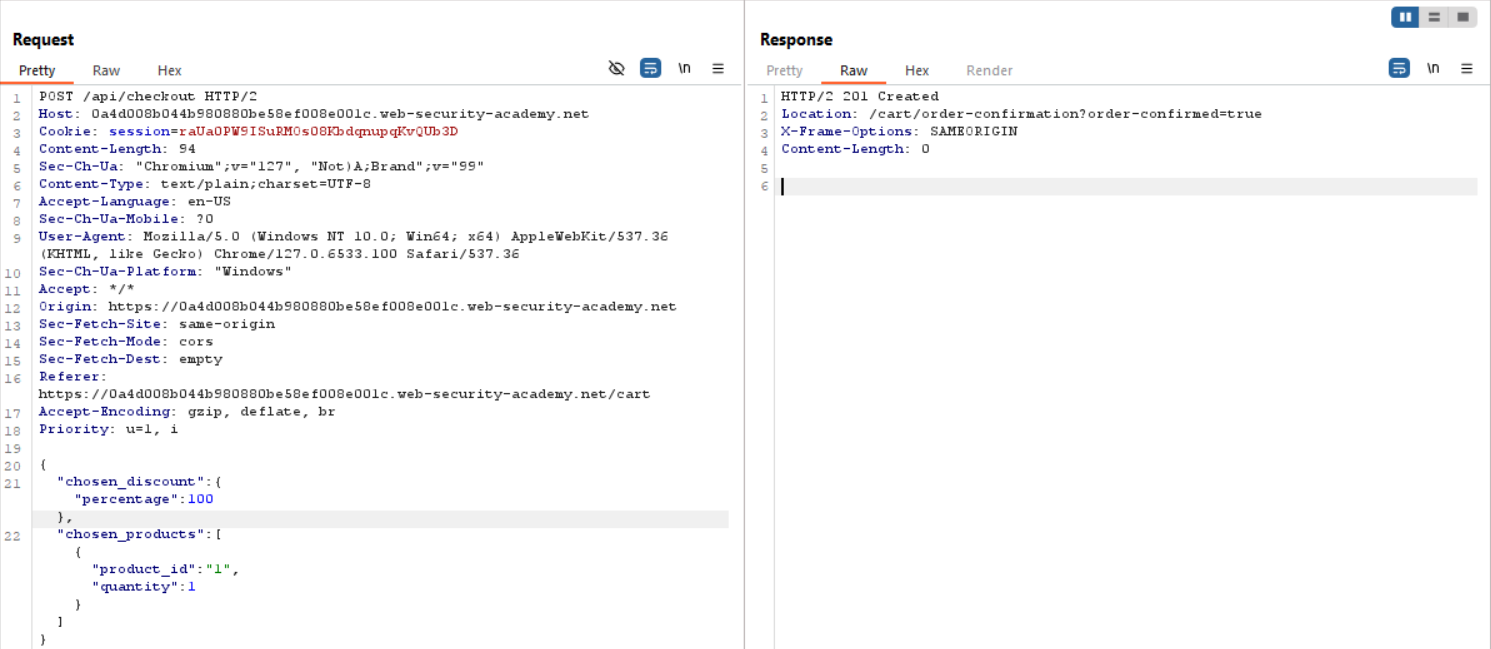




* Nhận thấy rằng gói tin GET có respone chứa trường “chosen\_discount” mà ở gói tin POST không có
* Ta sẽ thử thêm trường này vào gói POST và test thử



* Có vẻ như trường “chosen\_discount” hoàn toàn được server chấp nhận làm đầu vào và xử lý
* Ta sẽ đổi lên 100 để giảm giá xuống còn 0



* Tại đây, phản hồi sẽ chuyển qua trang mua sản phẩm thành công

