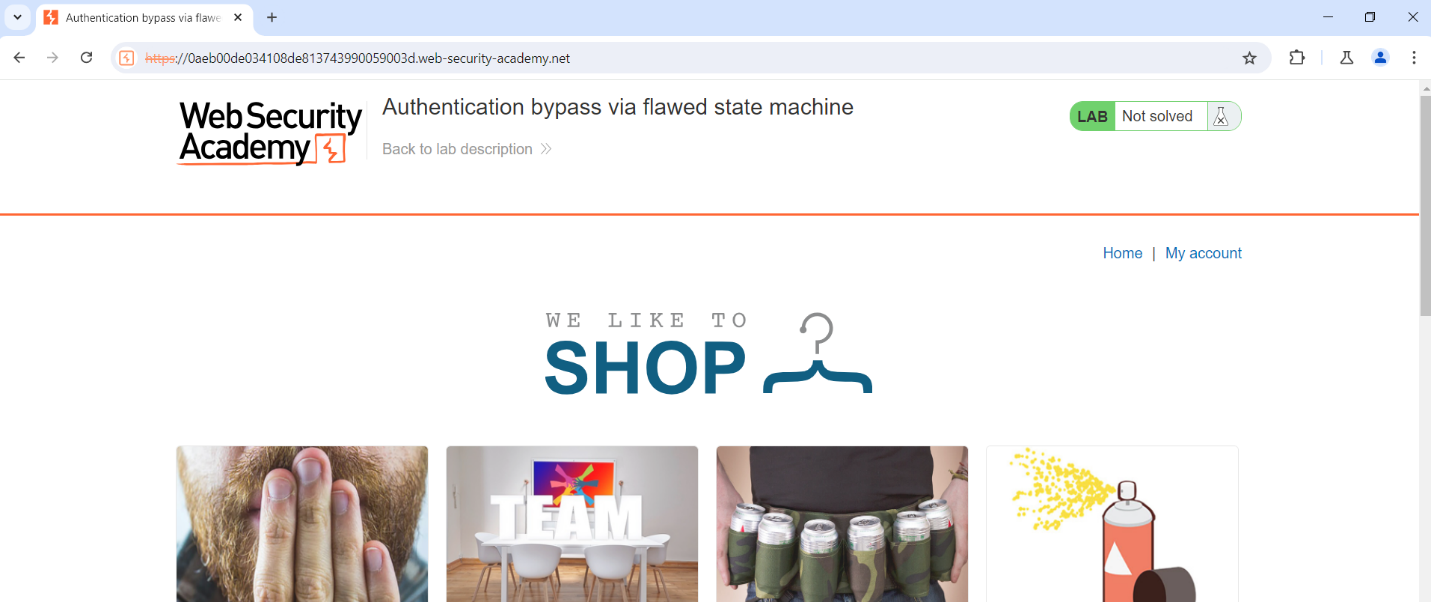
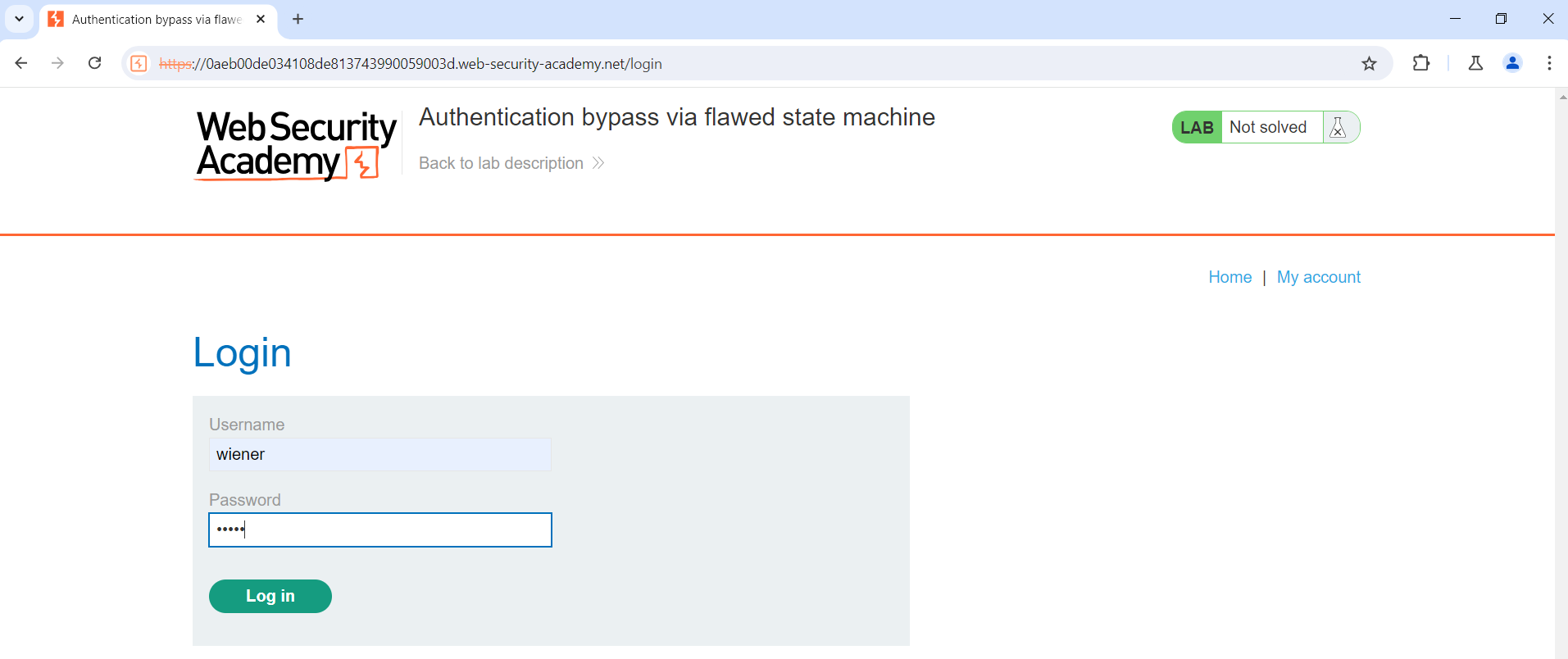


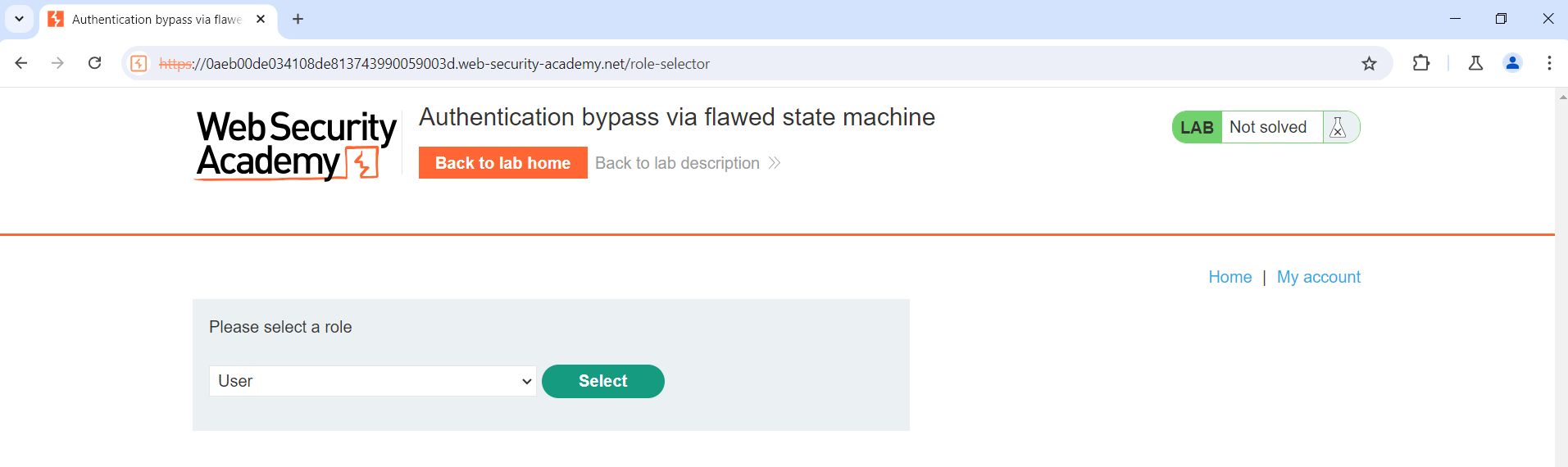
* Mục tiêu: Truy cập vào giao diện admin và xóa tài khoản carlos



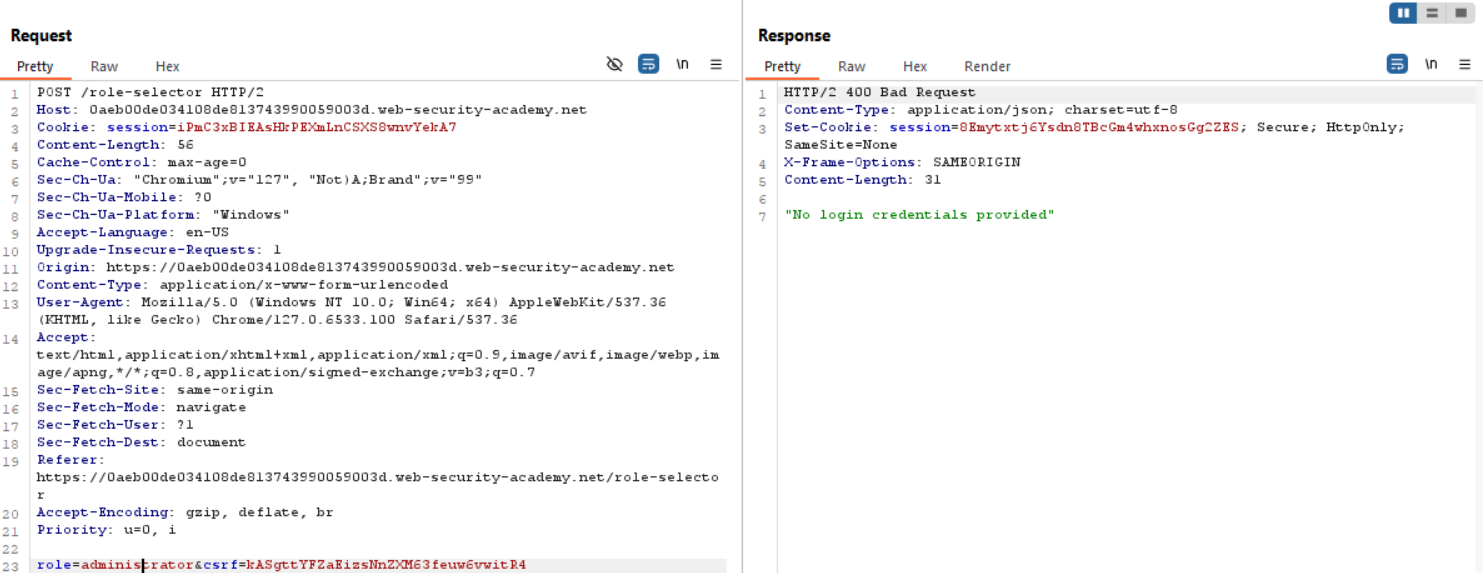
* Đăng nhập tài khoản người dùng



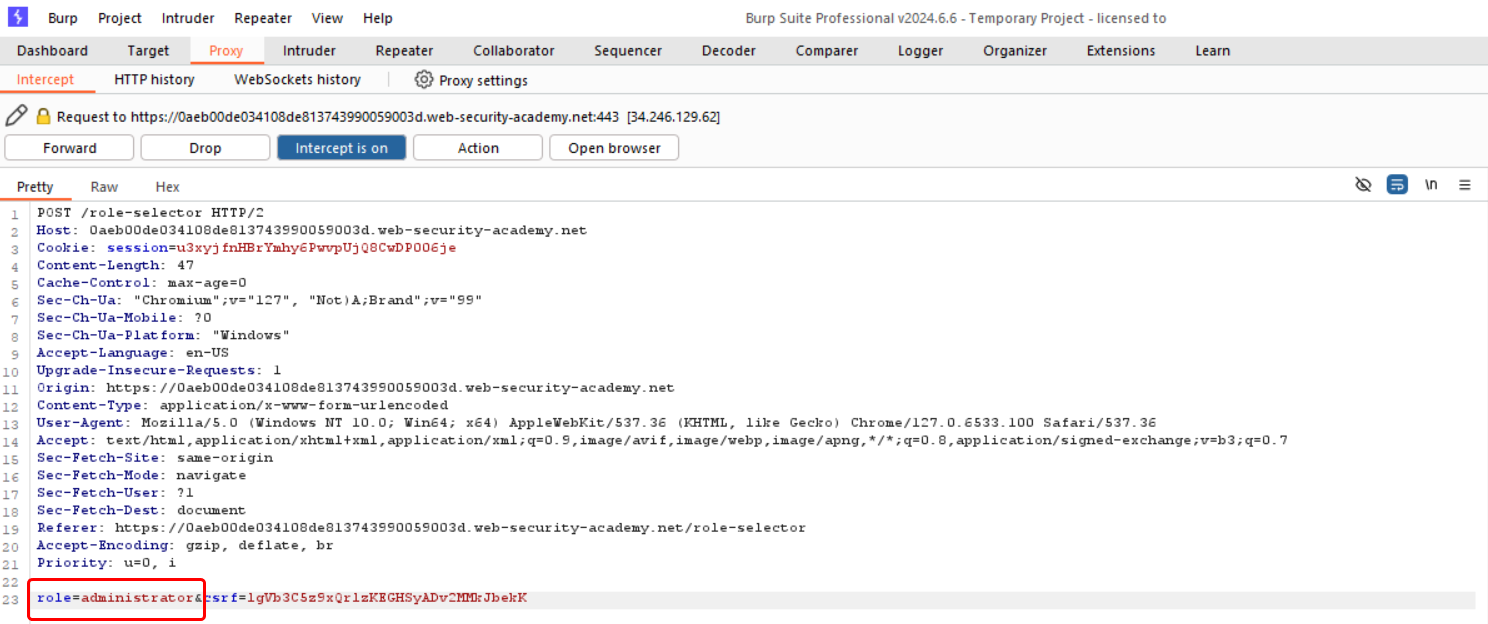
* Phát hiện có thêm chức năng chọn vai trò người dùng.



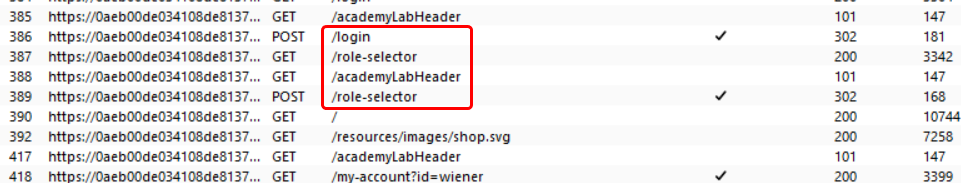
* Thử chuyển qua Repeater và sửa trường dữ liệu từ “user” sang “administrator”



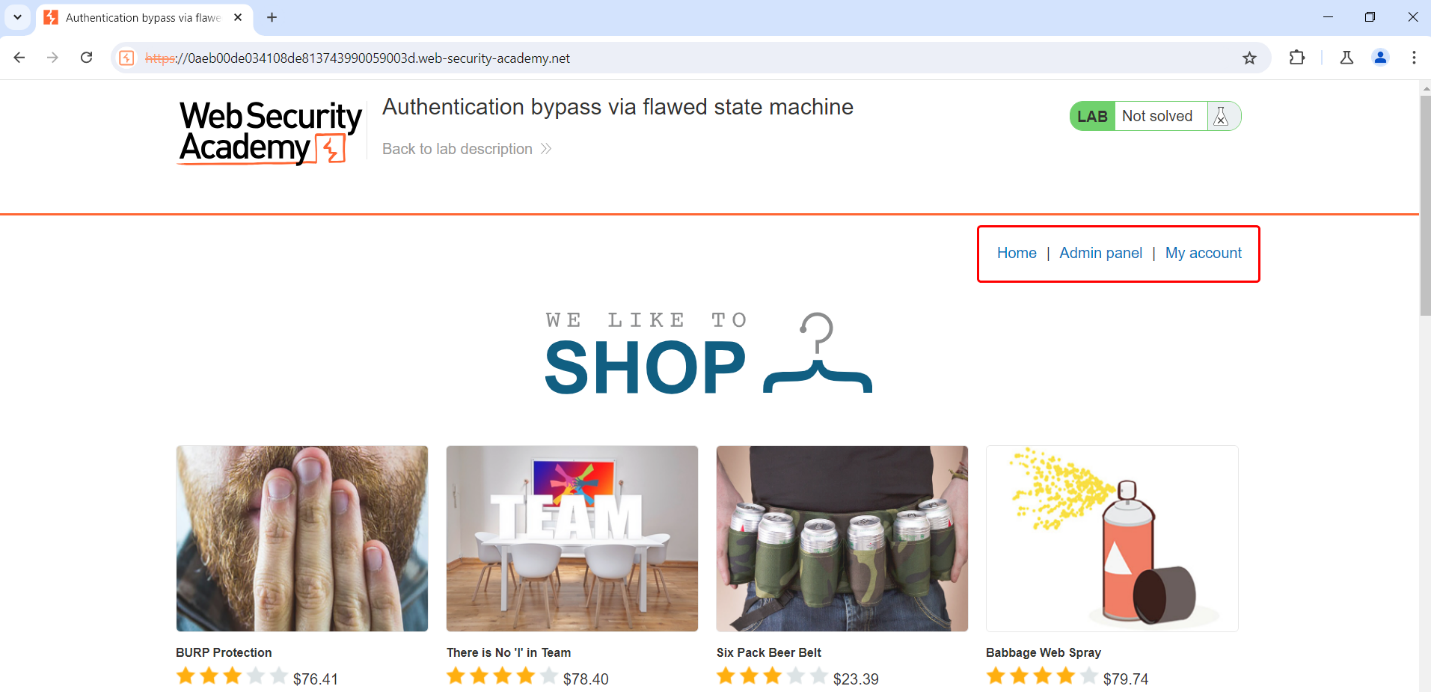
* Không được vì không phải phiên đăng nhập
* Ý tưởng: Ta sẽ đăng nhập lại và dùng Intercept để sửa trước khi gửi đi
* Không thực hiện được. Vẫn chỉ có vai trò là user



* Khi bắt Burpsuite, ta thấy rằng sau gói tin POST /login thì sẽ chuyển đến gói tin GET /role-selector.



* Ý tưởng: Ta sẽ dùng intercept để DROP gói tin GET /role-selector đi để không phải chọn vai trò nữa.



* Sau khi load lại trang thì đã xuất hiện “Admin panel”
* Xóa tài khoản carlos để hoàn thành lab

