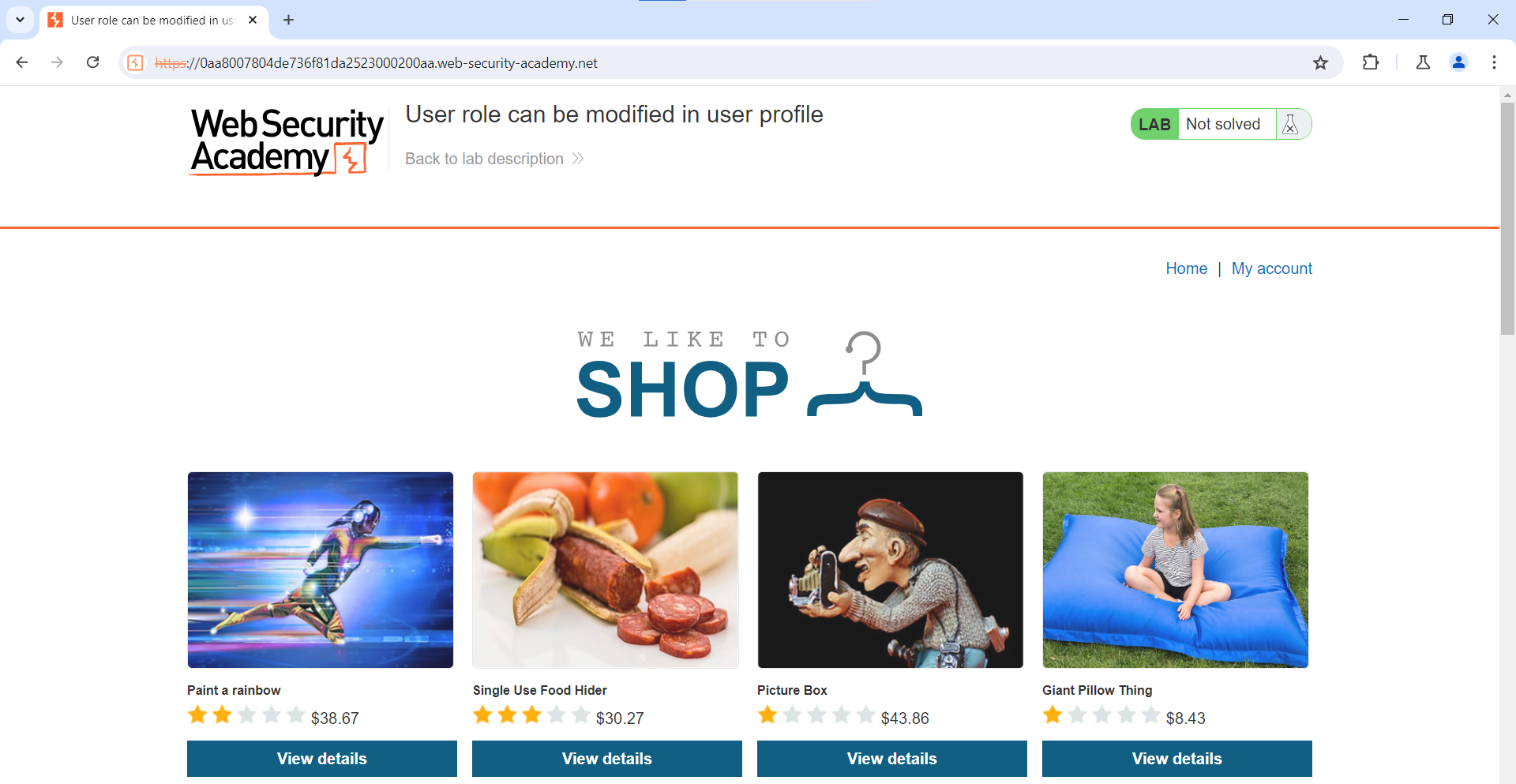
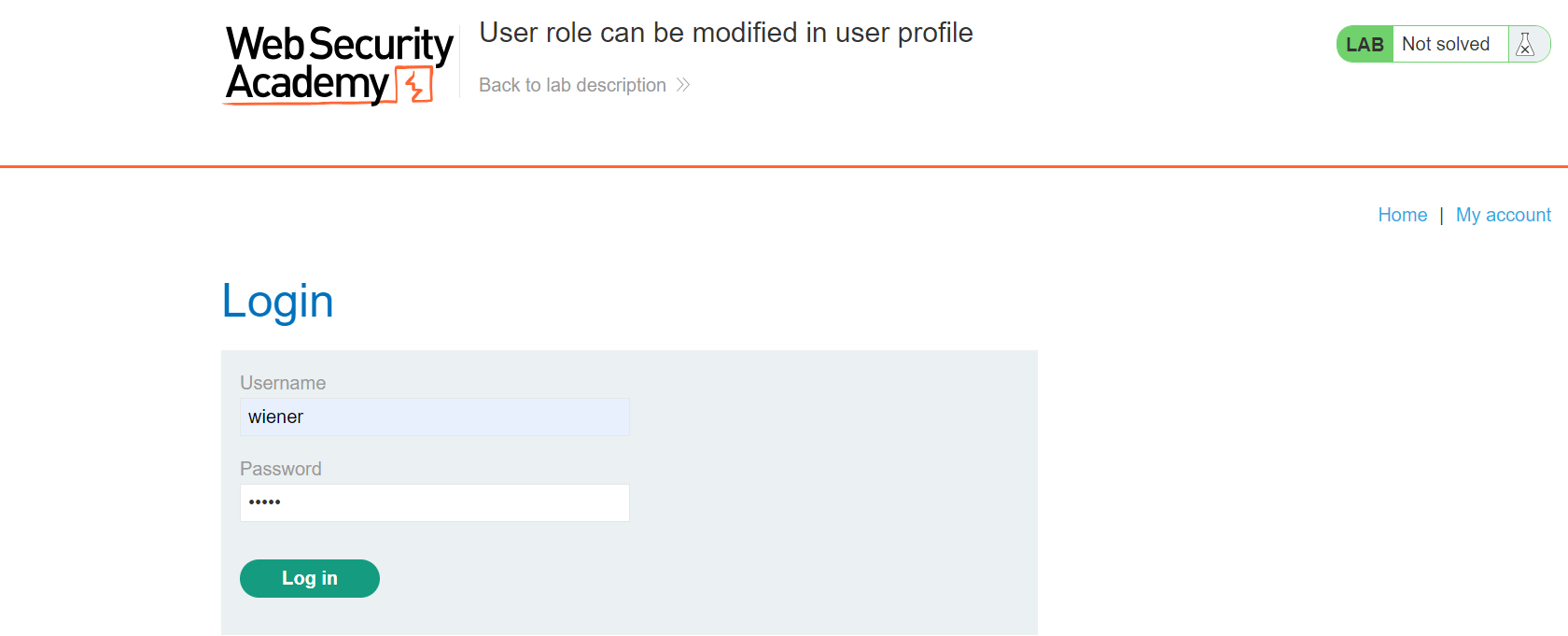


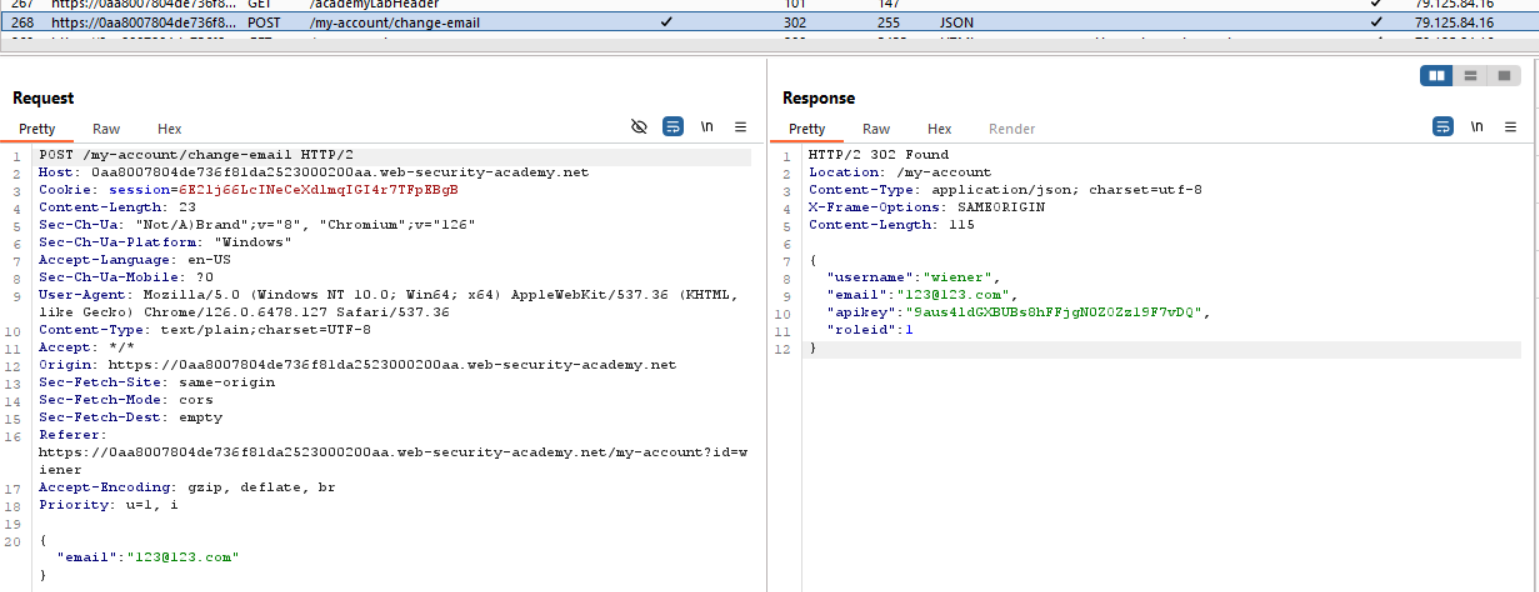
* Mục tiêu: Leo thang đặc quyền lên admin với roleid=2 để xóa tài khoản “carlos”



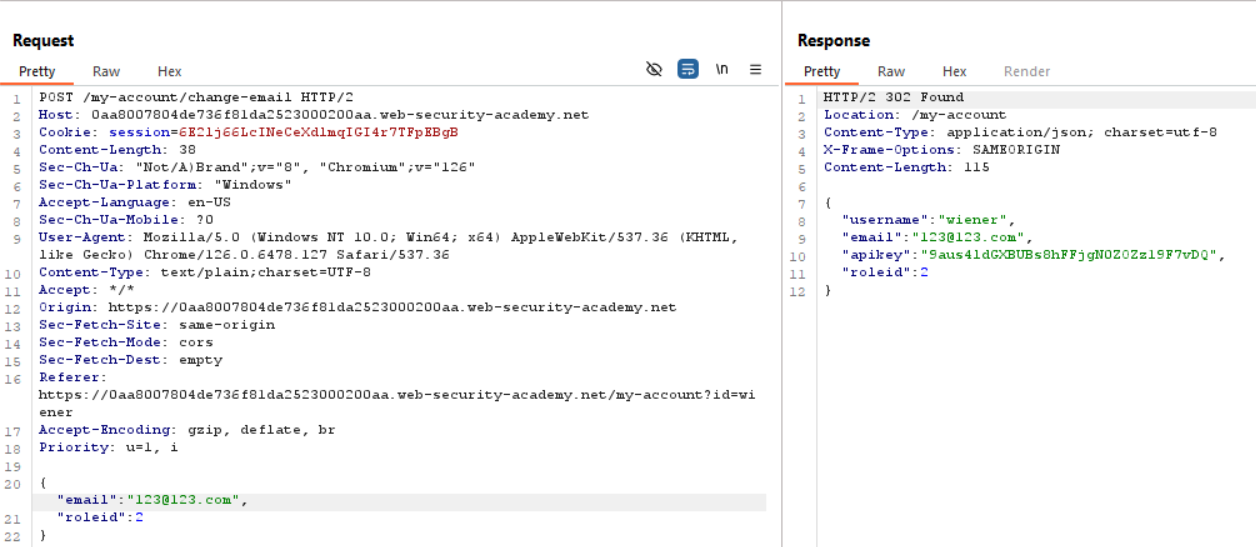
* Đăng nhập tài khoản người dùng bình thường



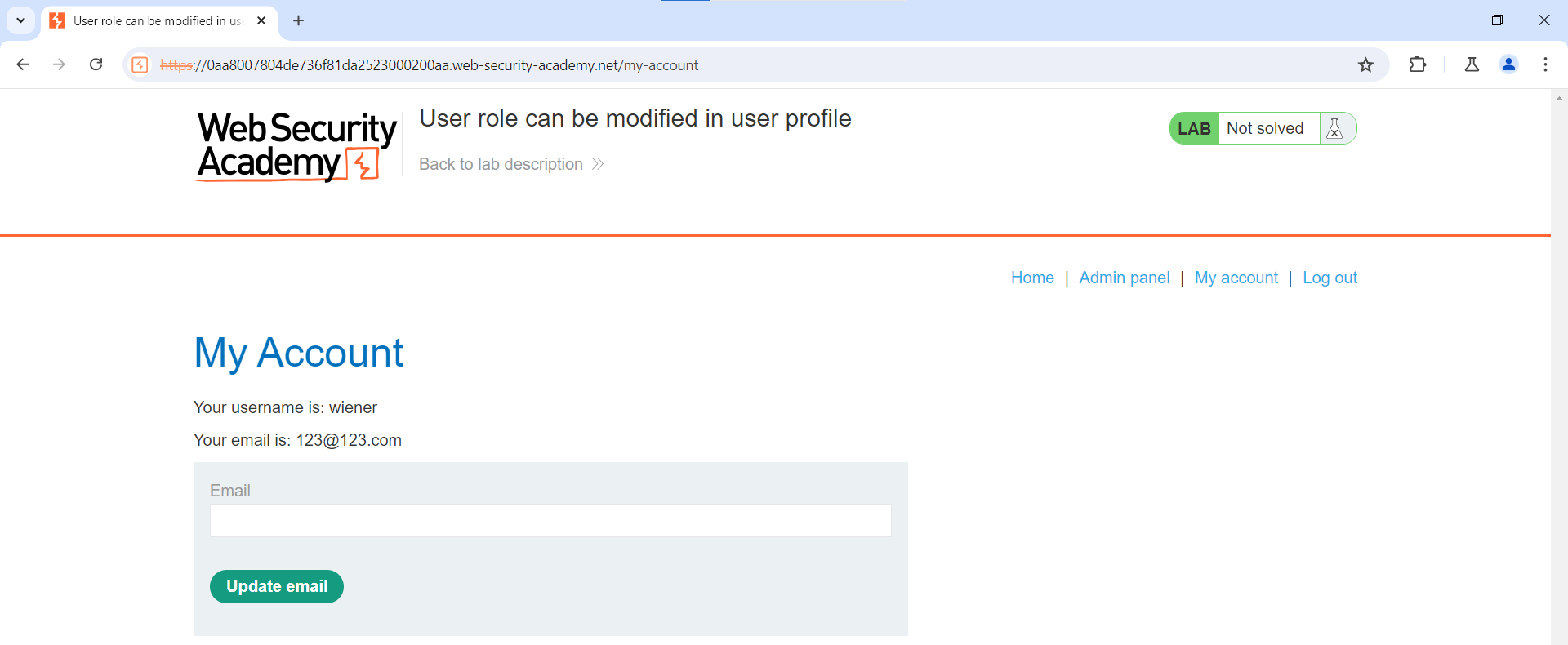
* Bắt các gói tin đăng nhập bằng BurpSuite nhưng vẫn chưa xuất hiện trường roleid như đề bài gợi ý.
* Thử đổi email và bắt bằng BurpSuite



* Phản hồi trả về file JSON với thông tin của người dùng sau khi thay đổi
* Đã xuất hiện trường roleid:1
* Cần phải sửa thành 2 để lên quyền của admin
* Chuyển gói tin POST sang bên repeater và thêm trường roleid ngay sau email để thử xem có nâng được quyền lên admin không



* Phản hồi trả về thông báo đổi thành công với trường roleid = 2
* Đã lên được quyền admin
* Load lại trang web



* Đã xuất hiện thêm “Admin panel” trên menu
* Truy cập trang quản trị và xóa tài khoản carlos

