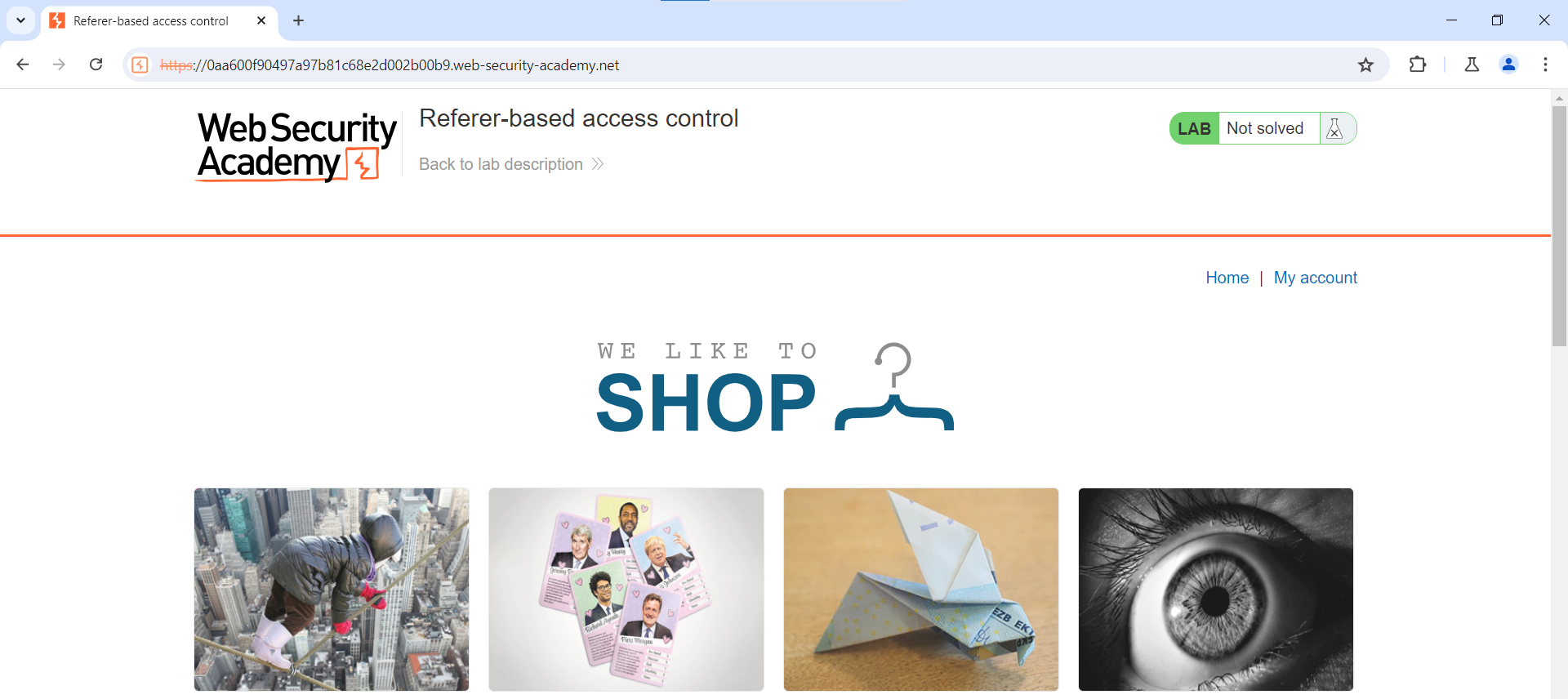
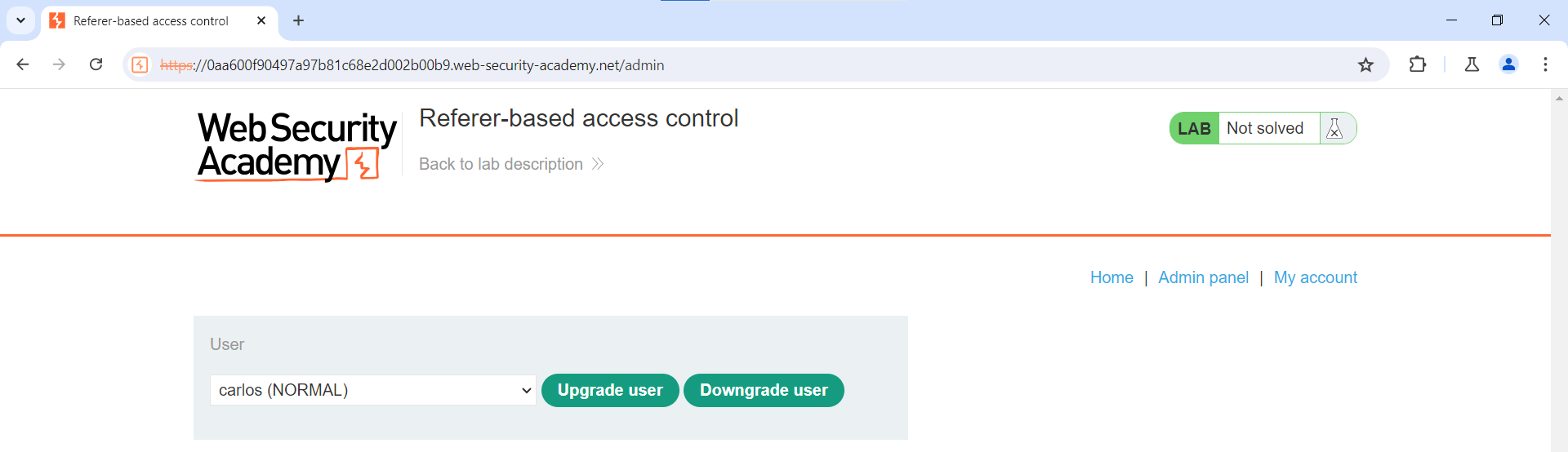


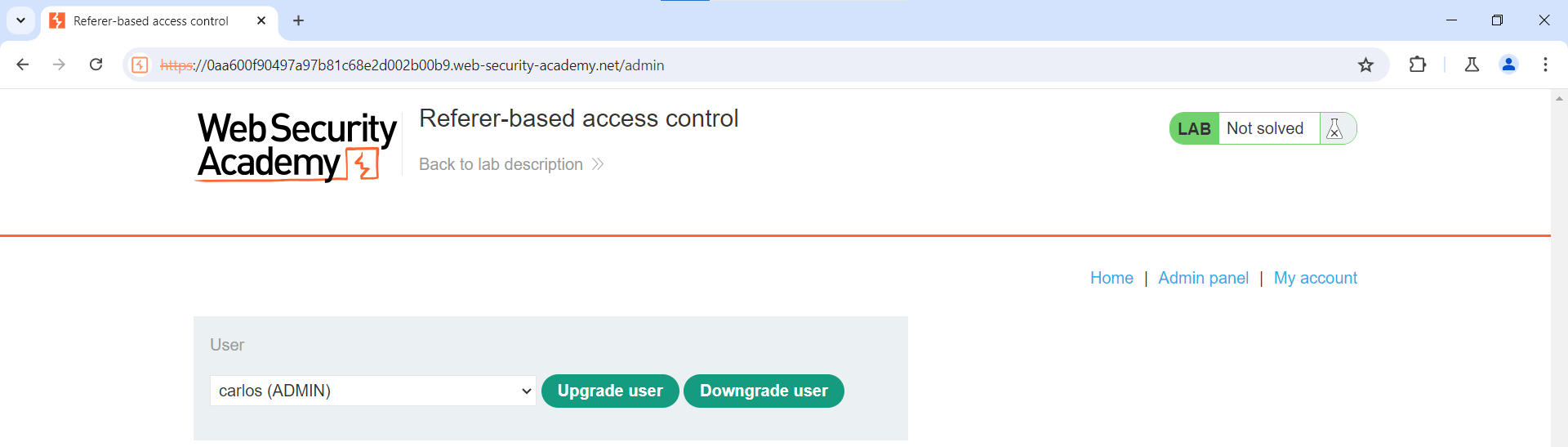
* Mục tiêu: Sử dụng tài khoản của wiener để nâng quyền bản thân lên admin



* Đăng nhập tài khoản admin và kiểm tra các chức năng admin



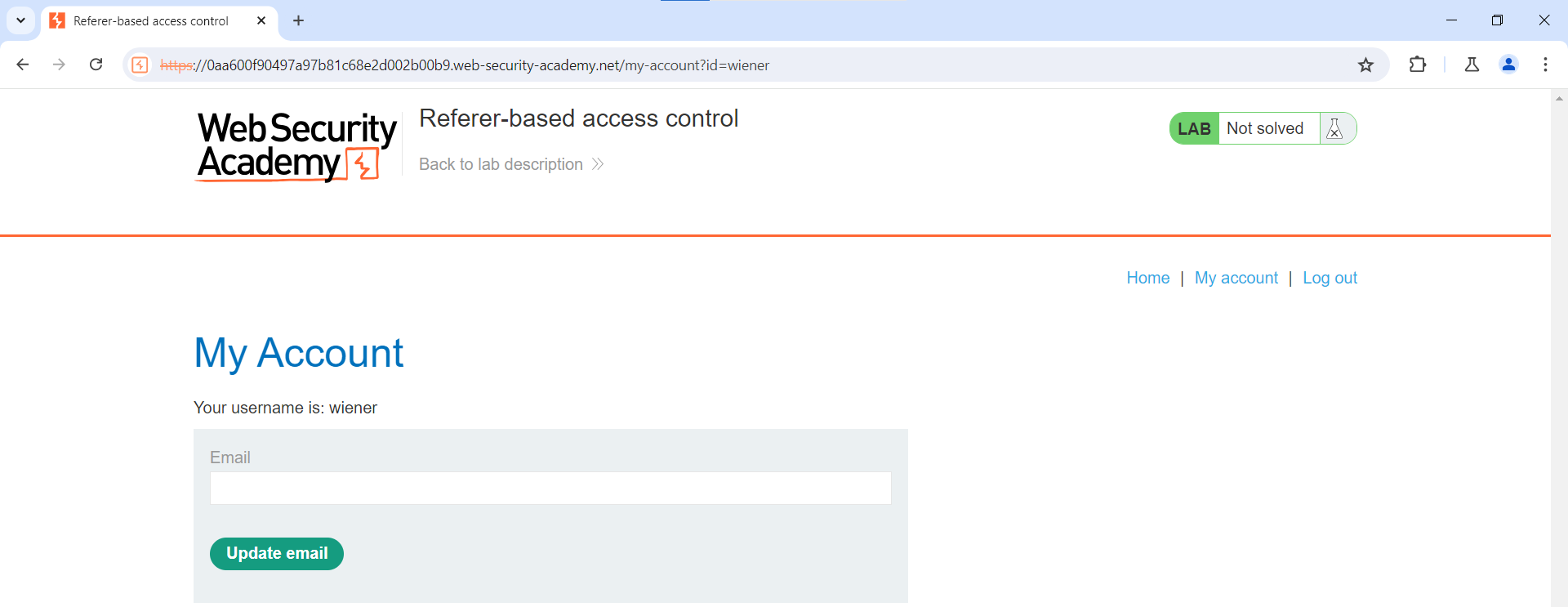
* Ta sẽ thử nâng quyền tài khoản carlos



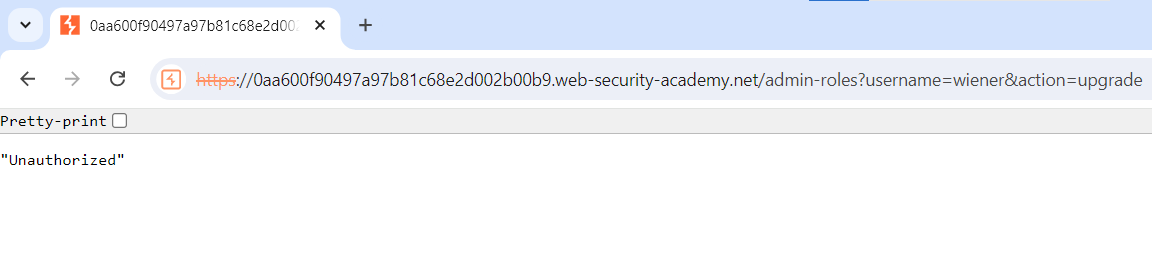
* Bắt gói tin bằng Burpsuite



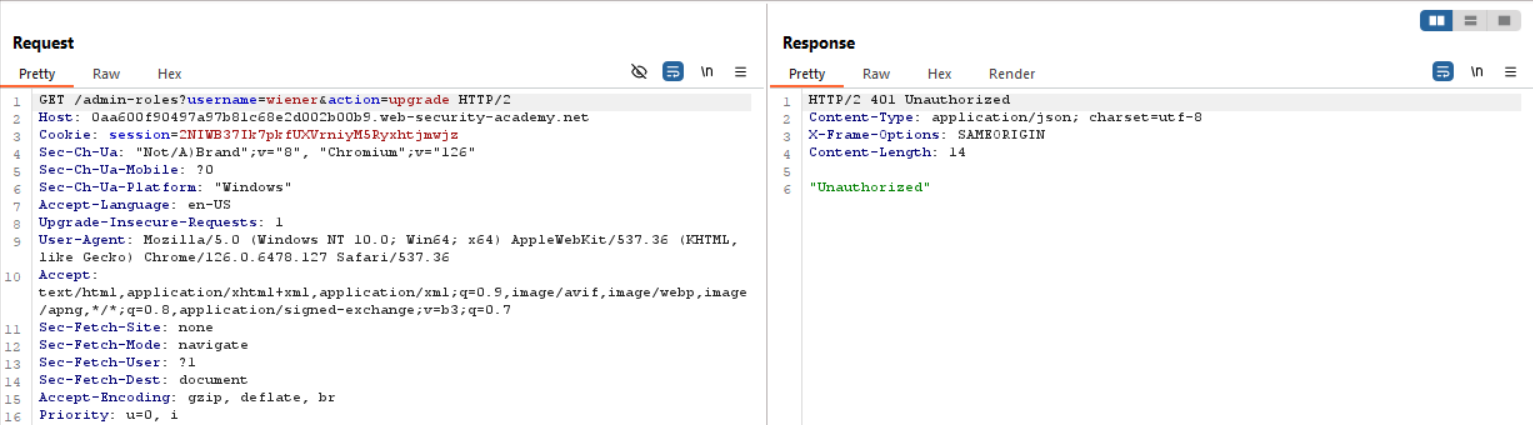
* Yêu cầu nâng quyền được thực hiện bằng GET
* Ta có thể sử dụng đường dẫn URL để nâng quyền thử
* Đăng xuất và đăng nhập tài khoản wiener



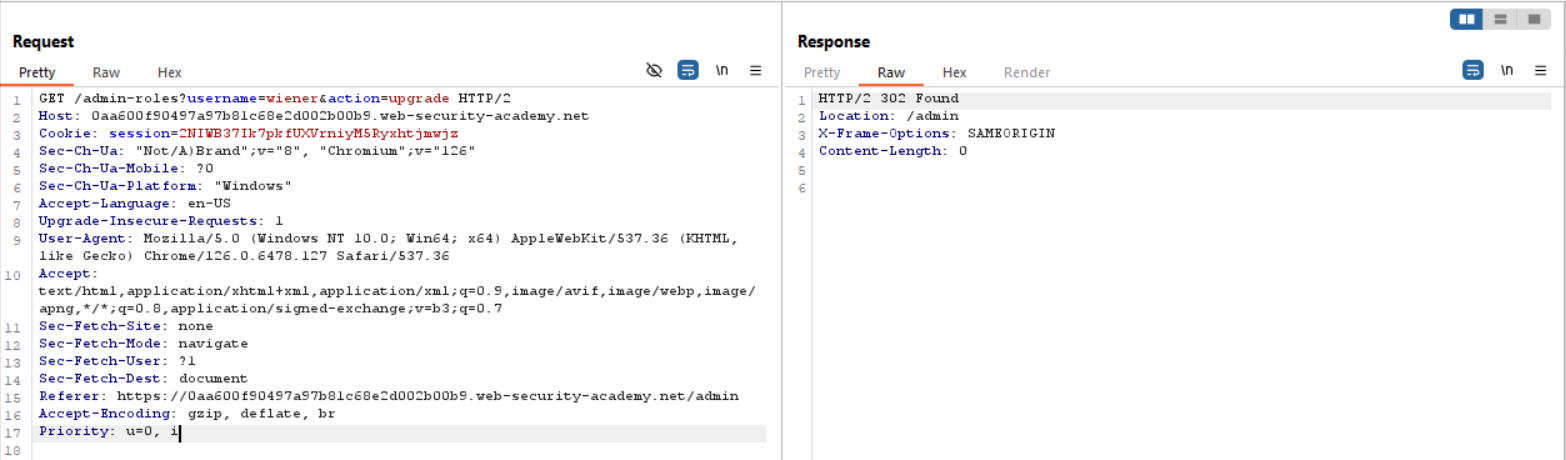
* Truy cập đường dẫn /admin-roles?username=wiener&action=upgrade để nâng quyền bản thân.



* Phản hồi trả về không thành công vì không có quyền
* Bắt thử gói tin và phân tích



* Sau khi so sánh với gói tin ở bước trước, ta phát hiện rằng gói tin này thiếu một trường header là Referer: <https://0aa600f90497a97b81c68e2d002b00b9.web-security-academy.net/admin>
* Thêm trường dữ liệu mới và gửi đi bằng repeater



* Phản hồi trả về thành công
* Load lại trang web và wiener đã nâng quyền lên admin thành công

