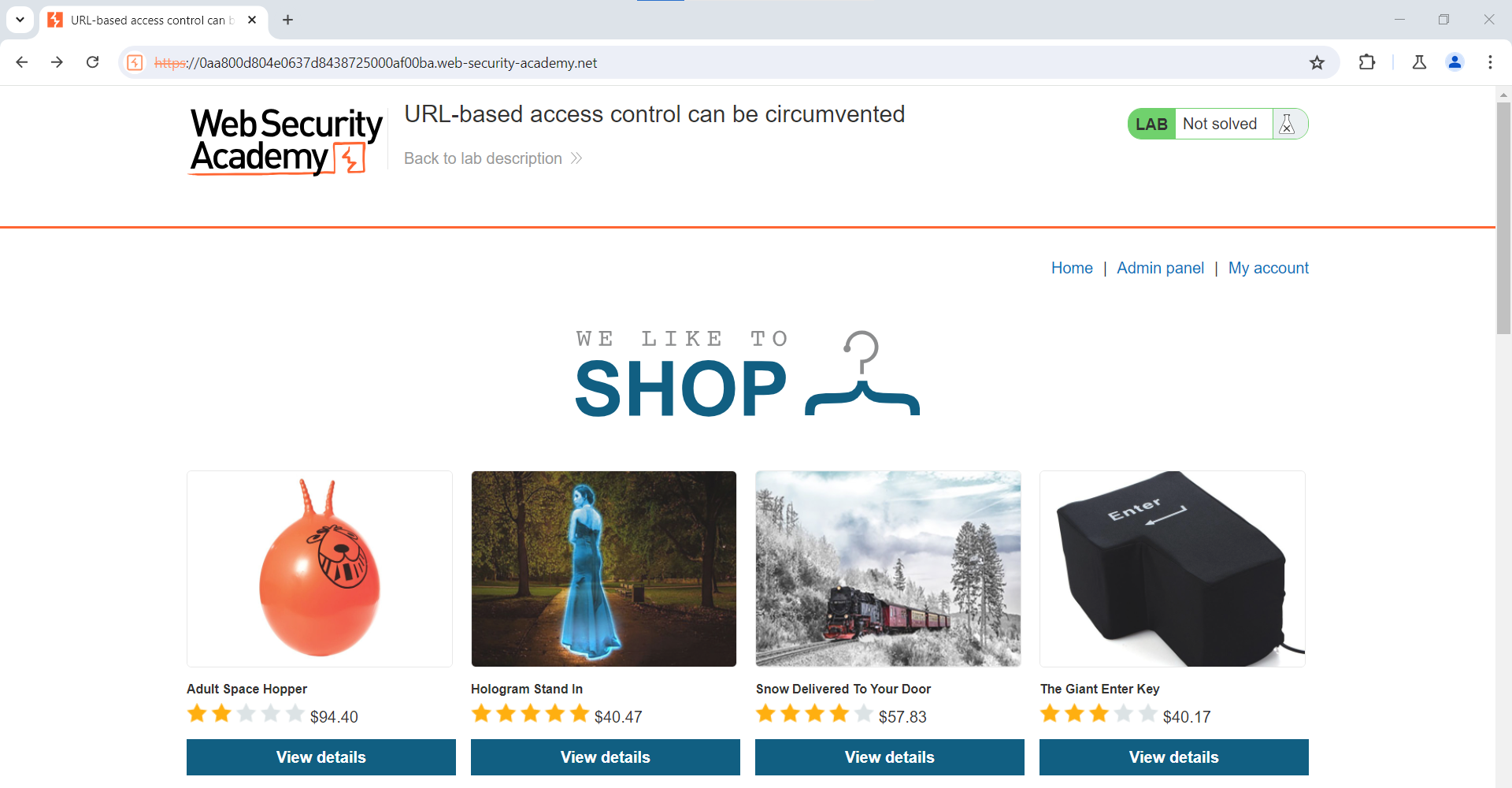
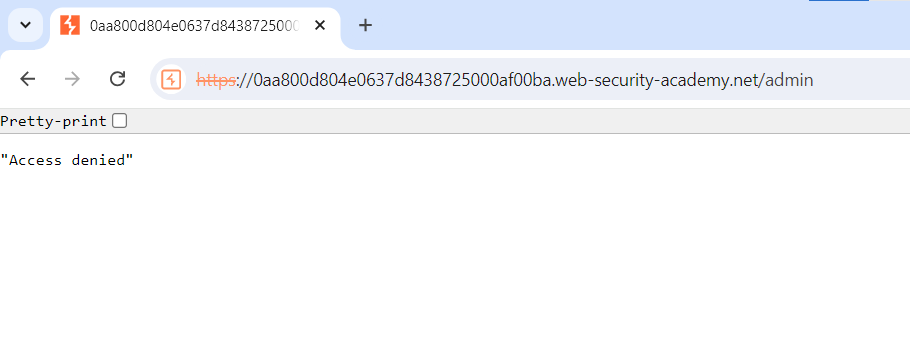


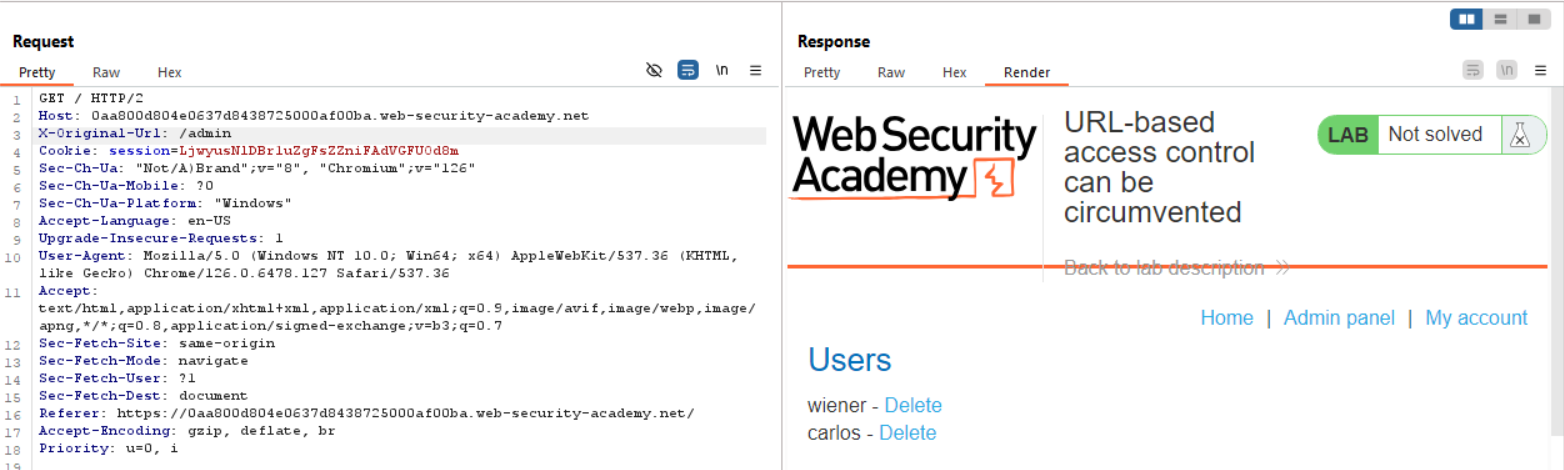
* Mục tiêu: Leo thang đặc quyền lên admin để xóa tài khoản “carlos”



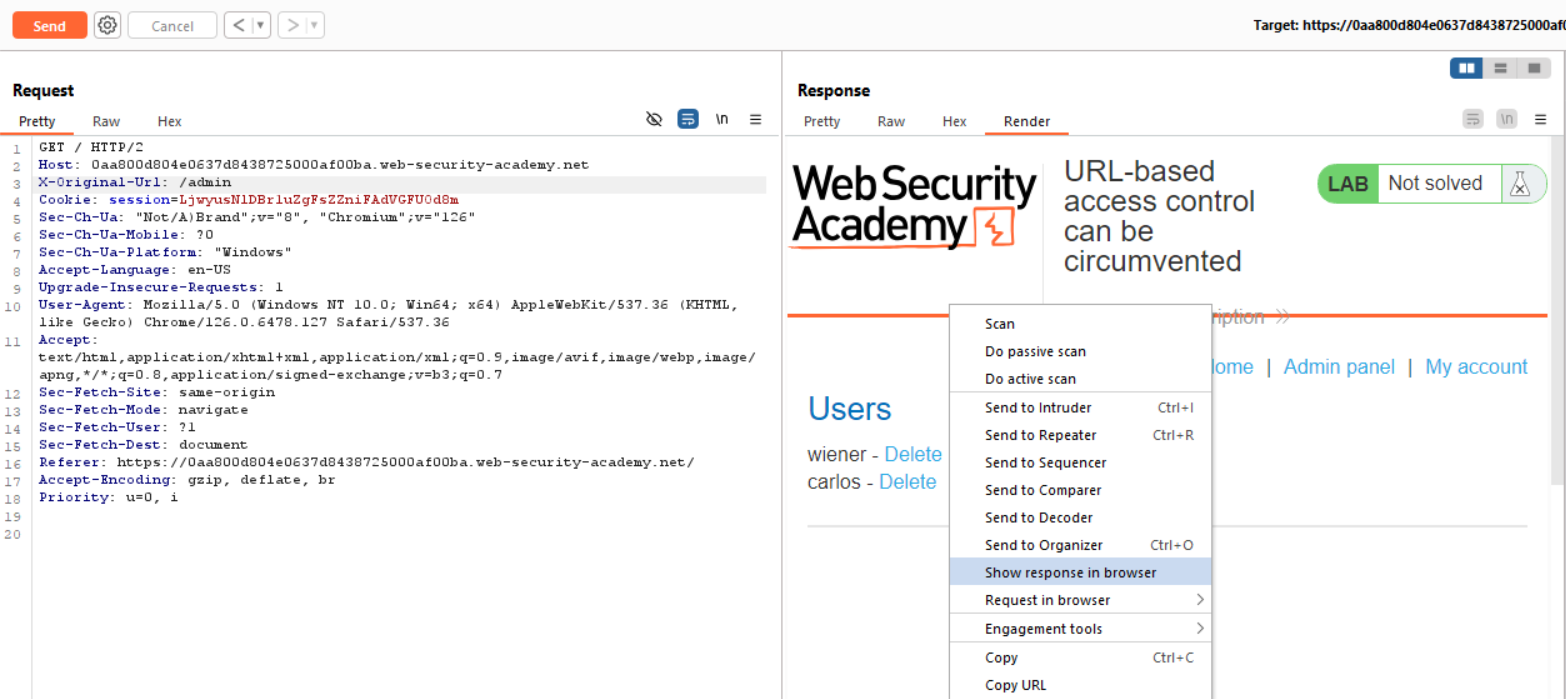
* Thử truy cập vào Admin Panel



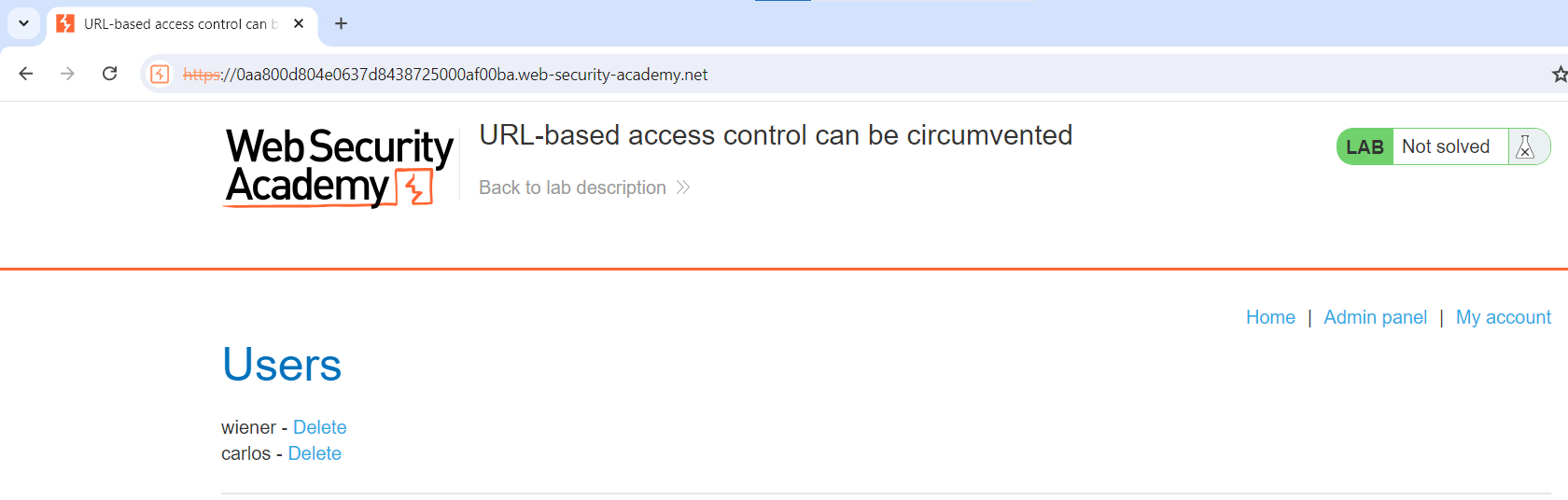
* Đã bị chặn do không có quyền truy cập.
* Theo như đề bài gợi ý thì hệ thống front-end đã được cấu hình để chặn truy cập bên ngoài vào đường dẫn đó
* Tuy nhiên, hệ thống back-end được xây dựng trên một khuôn hỗ trợ header X-Original-URL.
* Bắt gói tin truy cập vào trang admin và thêm header X-Original-URL.



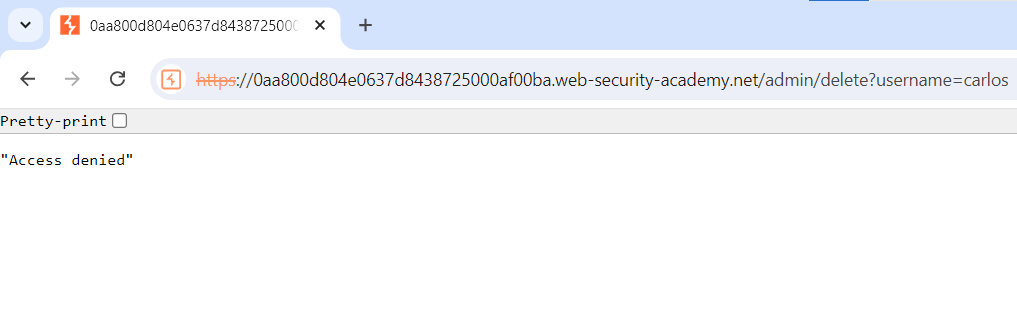
* Đã vào được trang Admin Panel
* Chuột phải và chọn “Show response in browser” để có thể truy cập trực tiếp



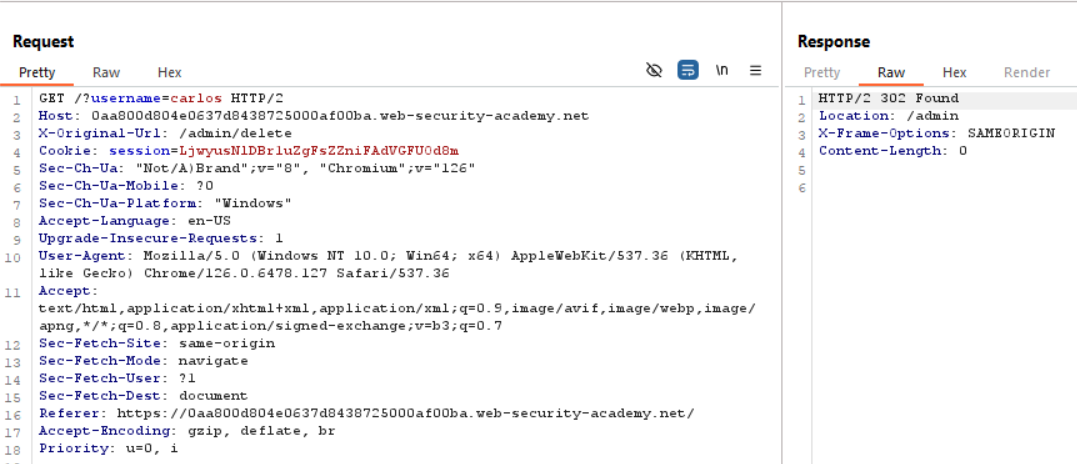
* Đã vào được trang web



* Thử xóa tài khoản carlos



* Lại bị chặn do không có quyền
* Ta lại thực hiện thủ thuật như trên
* Bắt gói tin và chuyển sang Repeater để thêm trường X-Original-URL



* Respone trả về thông báo thành công.
* Đã hoàn thành bài lab.

