**Lab: URL-based access control can be circumvented**

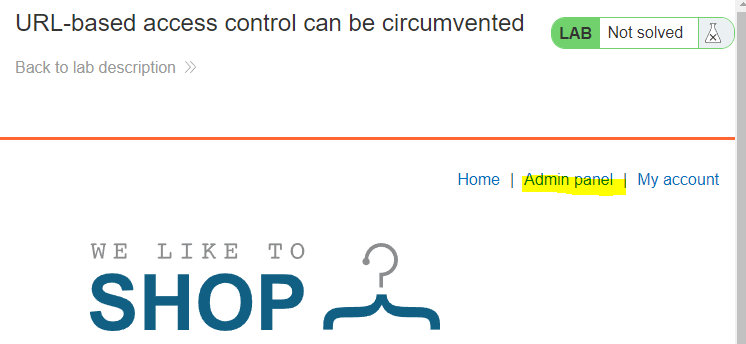
Bài lab này sử dụng các URL cụ thể để kiểm soát quyền truy cập vào các chức năng quan trọng. Tuy nhiên, cơ chế kiểm soát truy cập chỉ dựa trên URL và không có kiểm tra bổ sung nào, dẫn đến việc kẻ tấn công có thể đoán và truy cập vào các URL này để thực hiện các hành động trái phép.

Mục tiêu của bài lab này là khai thác lỗ hổng kiểm soát truy cập dựa trên URL để truy cập vào tài khoản quản trị viên và xóa một người dùng khác. Để hoàn thành bài lab, bạn cần xác định URL quản trị viên và sử dụng nó để xóa tài khoản của người dùng carlos.

X-Original-URL là một phần thông tin trong một yêu cầu web. Nó lưu trữ đường dẫn gốc mà người dùng yêu cầu trước khi yêu cầu đó được thay đổi hoặc chuyển hướng bởi các hệ thống trung gian như proxy hoặc gateway. Điều này giúp hệ thống biết được đường dẫn ban đầu mà người dùng đã nhập vào.

Các bước thực hiện:

Truy cập vào “Admin panel”

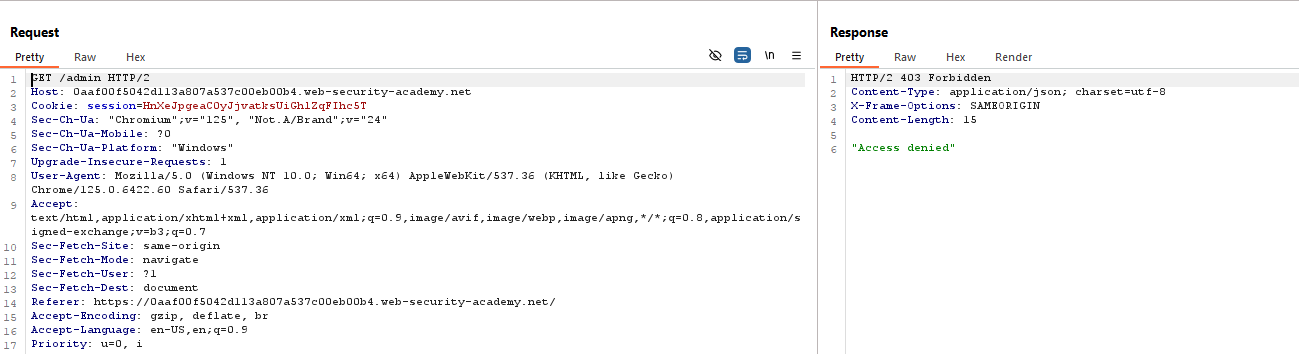


Hình 1. Truy cập vào Admin Panel

Bắt request gửi sang Reapeater

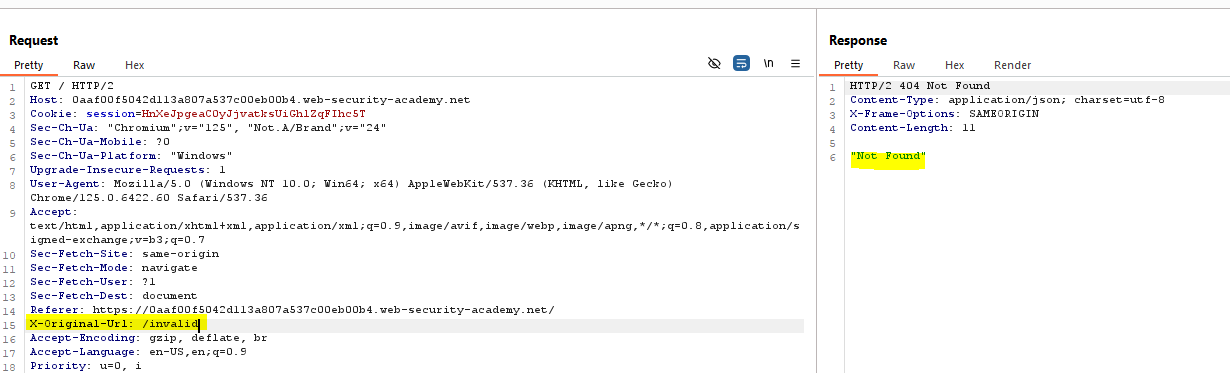


*Hình 2.* Request GET /admin



Hình 3. Gửi sang Reapeater để phân tích

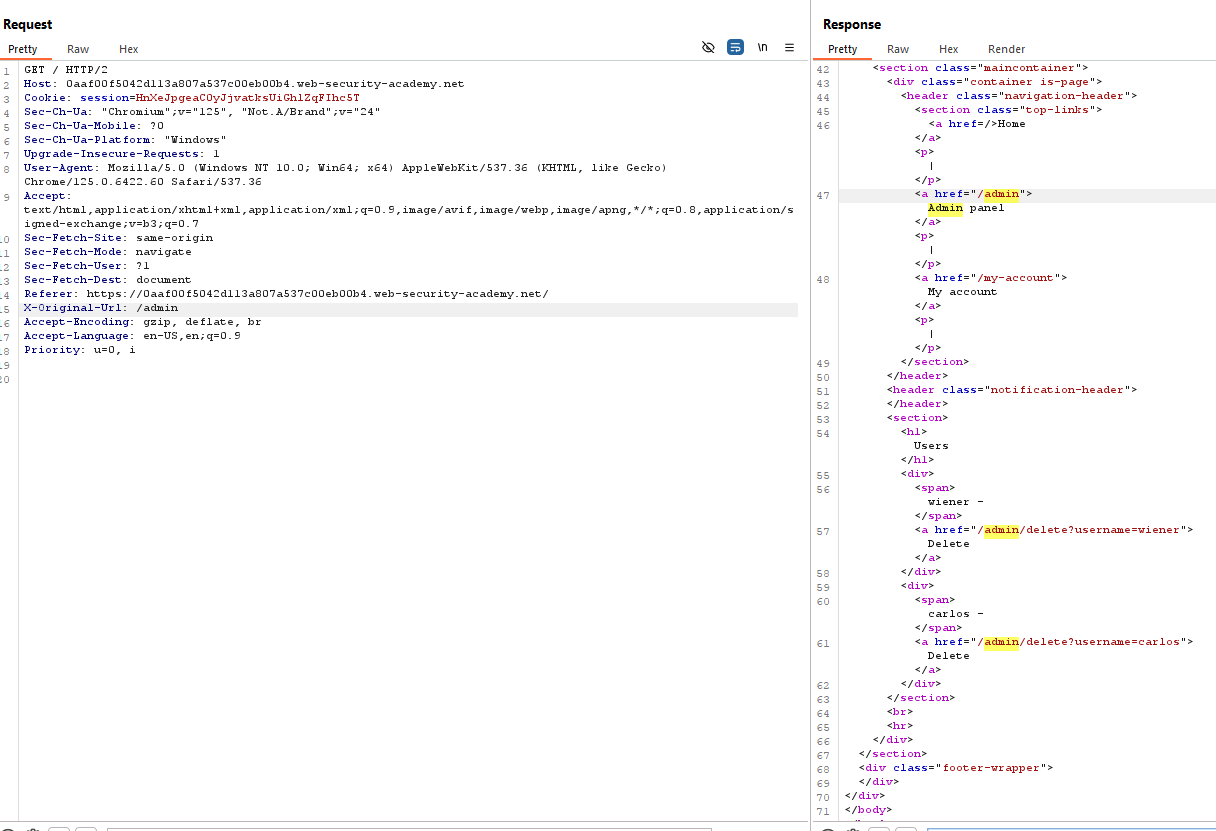
Thử thêm trường X-Original-URL xem web có hỗ trợ header này không



Hình 4. 1 response 404 được trả về

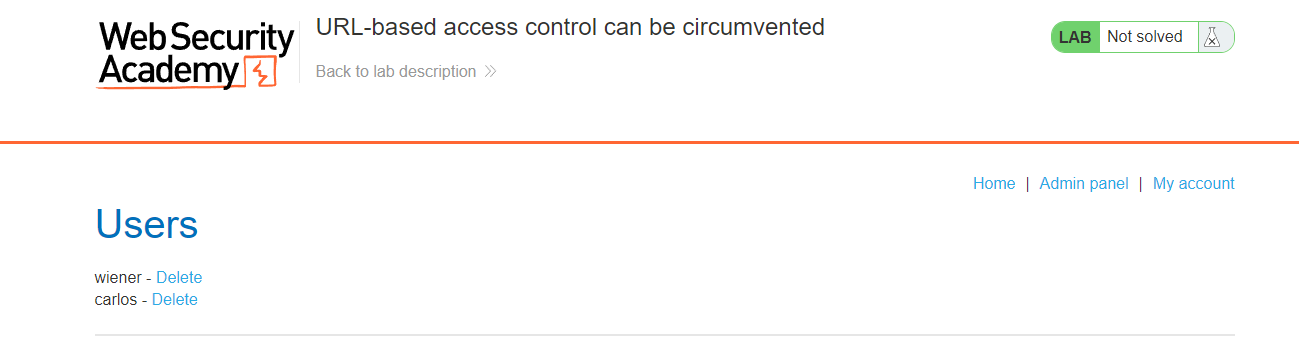
* Web hỗ trợ header X-Original-URL.

Sửa X-Origin-URL: /admin



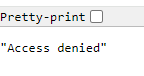
Hình 5. 1 mã 200 được trả về

Show respone in browser -> Copy -> Dán vào trình duyệt



Hình 6. Truy cập được vào admin panel

Thử delete “Carlos”

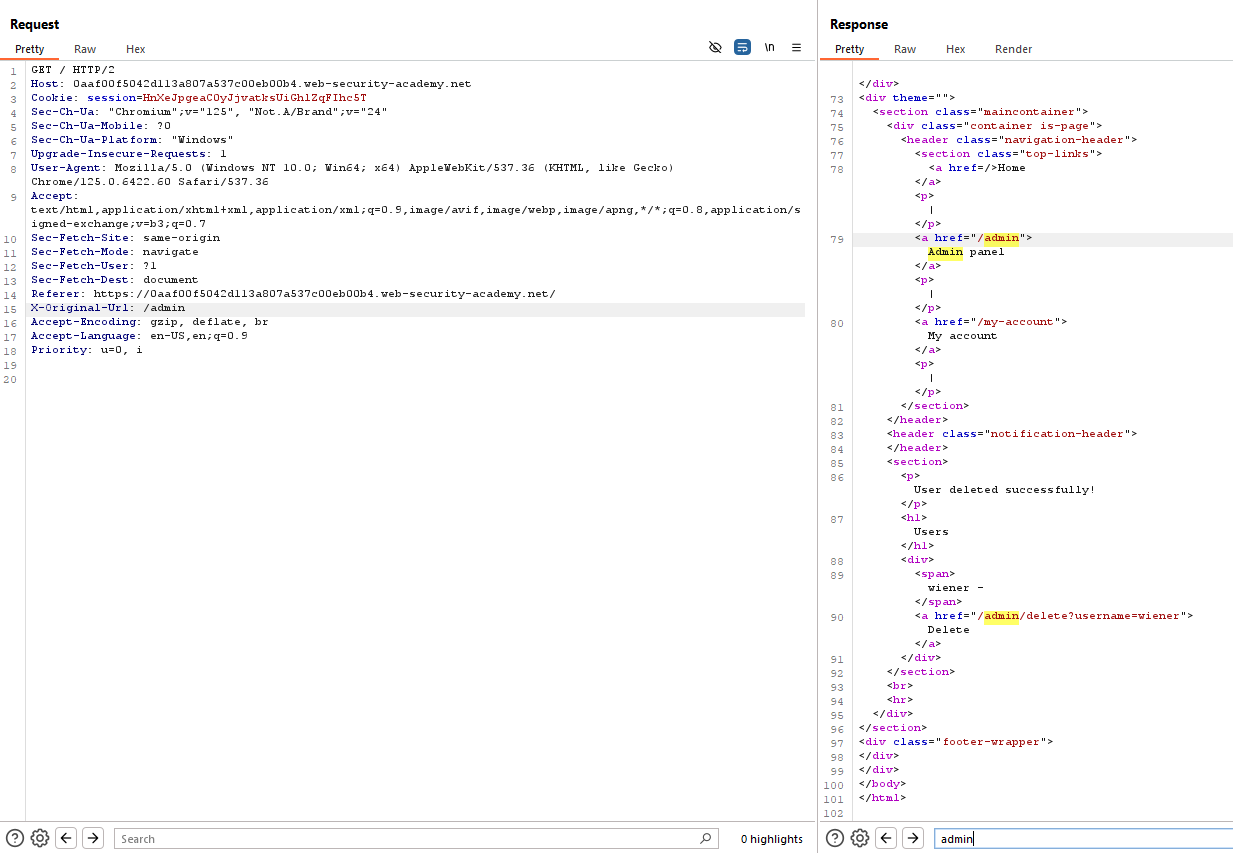


Hình 7. Không cho phép delete “Carlos”

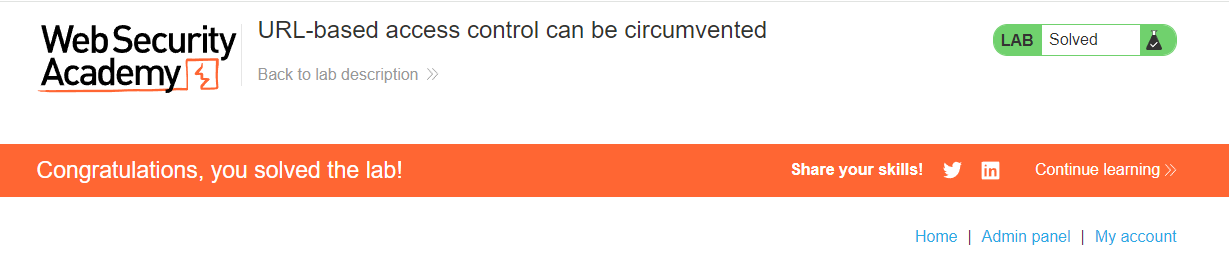
Sửa request và Send lại



Hình 8. Yêu cầu lấy dữ liệu từ máy chủ với tham số username=carlos, và liên quan đến việc thử truy cập vào một đường dẫn quản trị (/admin/delete) được lưu trữ trong X-Original-Url.



Hình 9. Tài khoản carlos đã không còn ở admin panel



Hình 10. Bài lab được hoàn thành