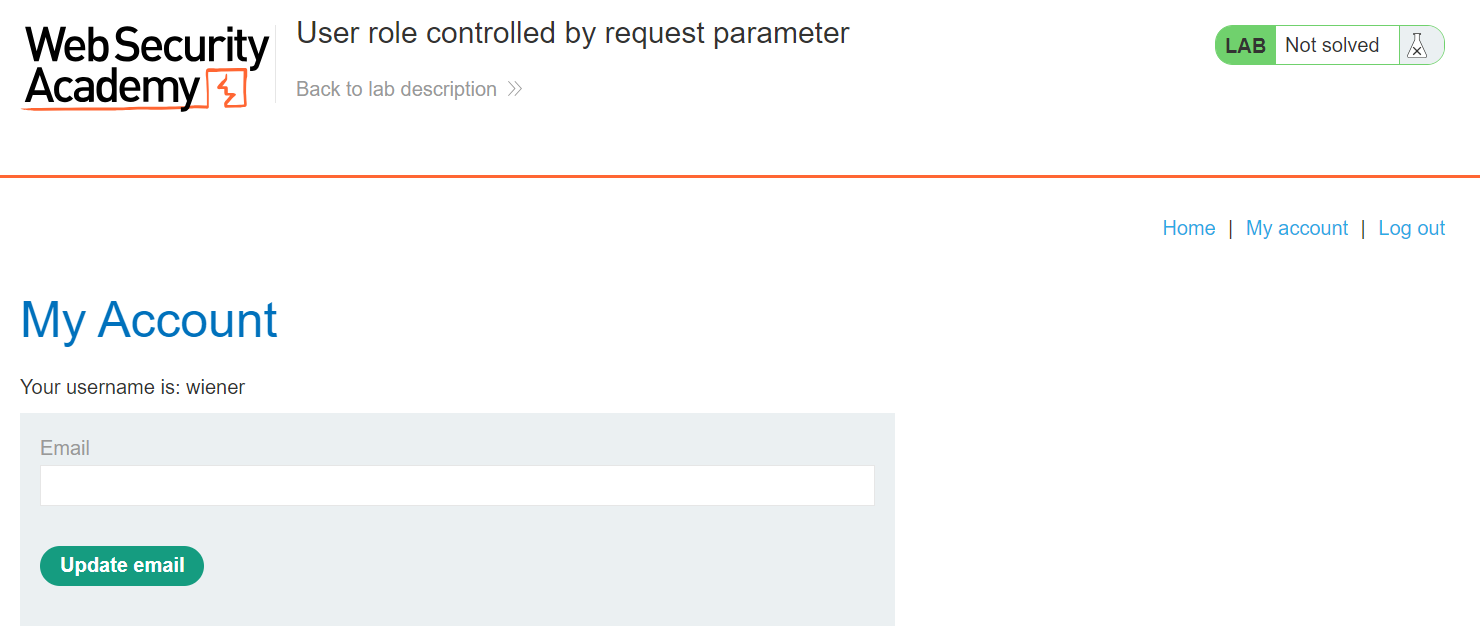
**Lab: User role controlled by request parameter**

Bài lab này kiểm soát quyền truy cập dựa trên vai trò của người dùng, và vai trò này được truyền qua một tham số trong yêu cầu HTTP. Nếu tham số này không được bảo vệ đúng cách, kẻ tấn công có thể thay đổi giá trị của tham số để giả mạo quyền hạn quản trị viên và truy cập vào các chức năng quản trị.

Mục tiêu của bài lab này là khai thác lỗ hổng kiểm soát quyền truy cập dựa trên tham số yêu cầu để nâng cấp quyền hạn của người dùng lên quyền quản trị viên. Để hoàn thành bài lab, bạn cần sửa đổi tham số yêu cầu để truy cập vào bảng điều khiển quản trị viên và xóa tài khoản của người dùng carlos.

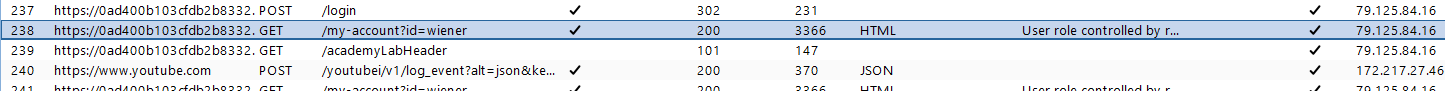
Các bước thực hiện:

Đăng nhập bằng tài khoản wiener/peter

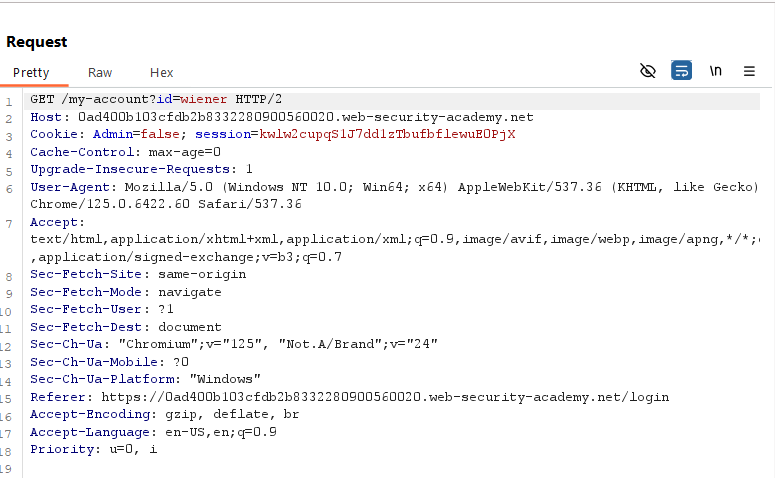


Hình 1. Đăng nhập thành công tài khoản wiener

Bắt request gửi sang Repeater

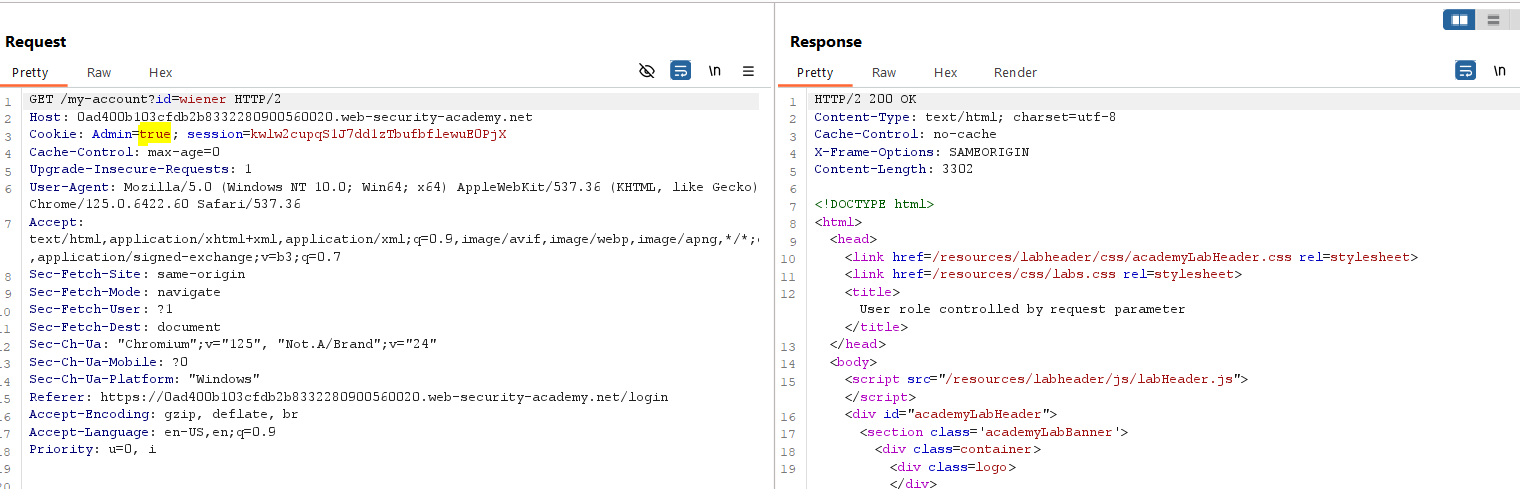


Hình 2. Request GET /myaccount?id=wiener



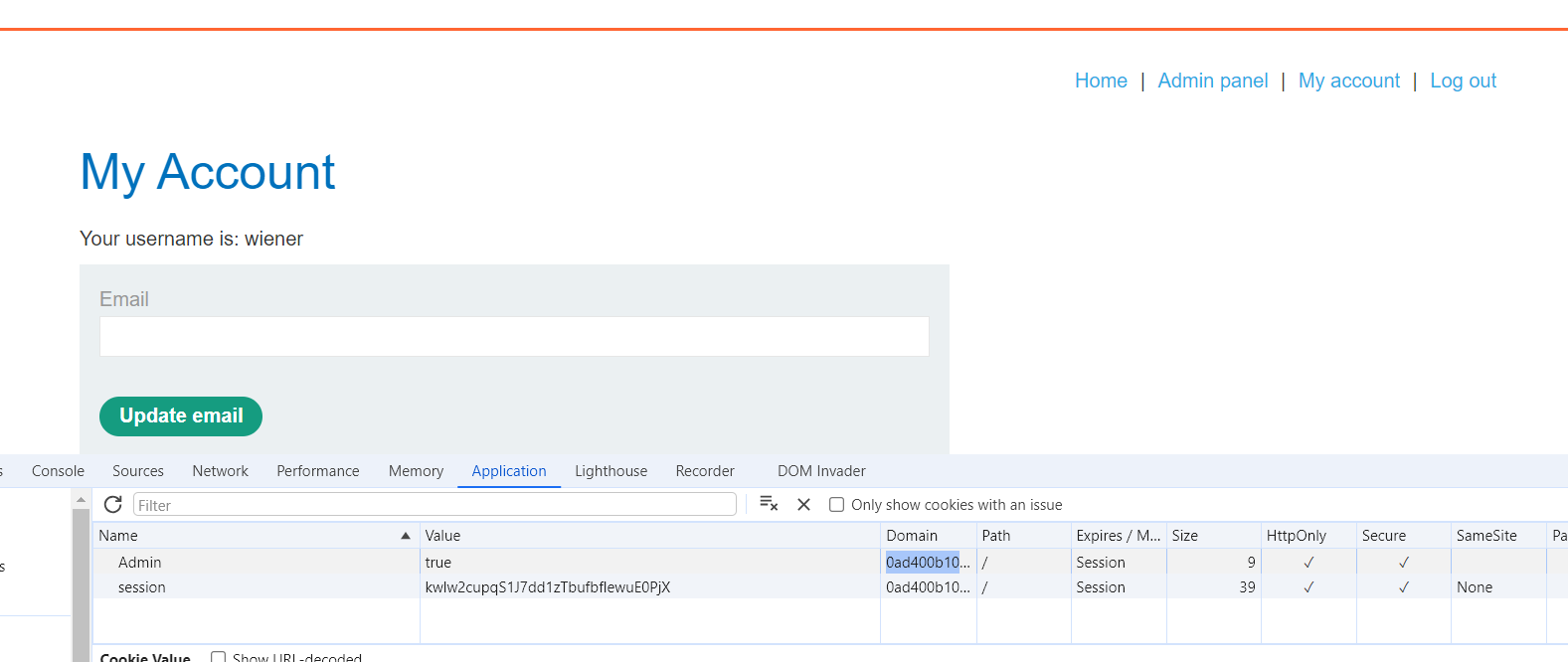
Hình 3. Gửi sang Reapeater để phân tích

Sửa admin = true



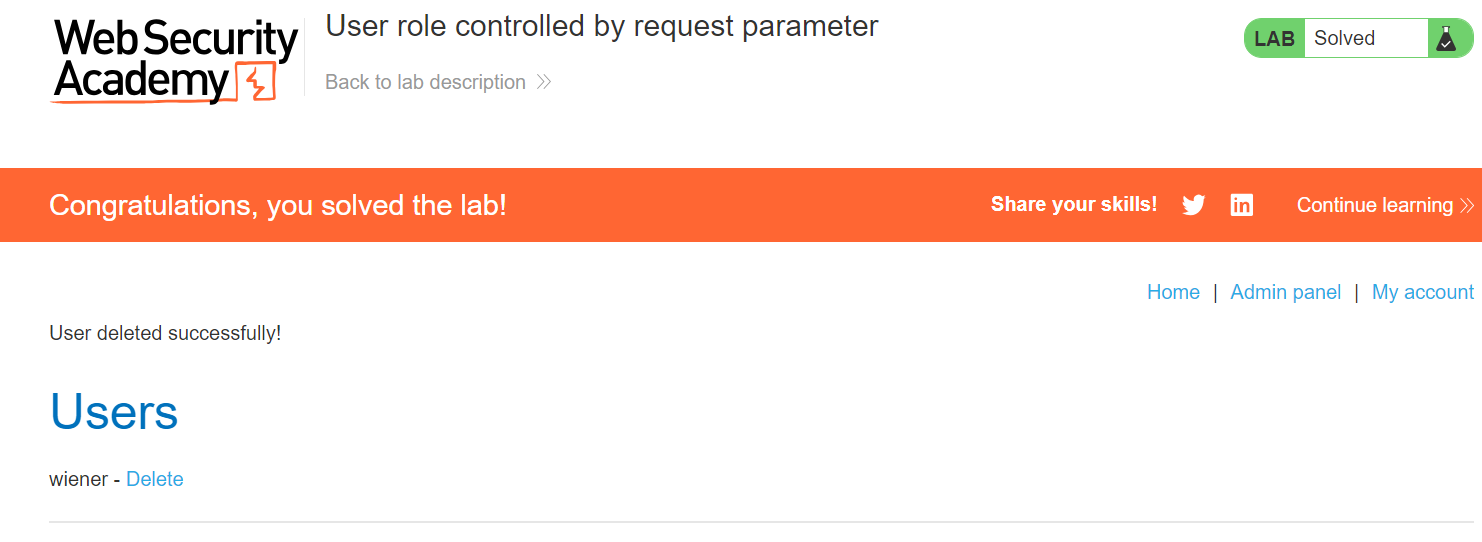
Hình 4. Sửa request

Follow redirection -> Copy -> Dán vào trình duyệt, Inspect sửa value, wiener đã lên quyền quản trị



Hình 5. Wiener lên quyền admin

Xoá tài khoản carlos, bài lab được hoàn thành



Hình 6. Bài lab được hoàn thành