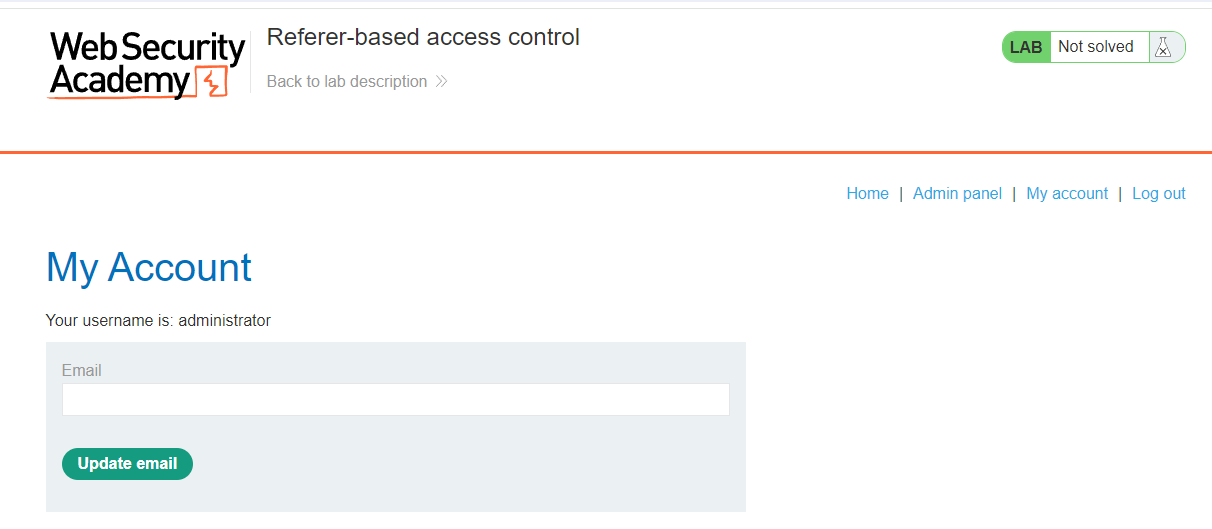
**Lab: Referer-based access control**

Bài lab này sử dụng tiêu đề HTTP Referer để kiểm soát quyền truy cập vào các chức năng cụ thể. Tuy nhiên, vì tiêu đề Referer có thể bị giả mạo hoặc thay đổi dễ dàng, cơ chế kiểm soát này không đủ an toàn. Kẻ tấn công có thể khai thác lỗ hổng này để thực hiện các hành động không được phép.

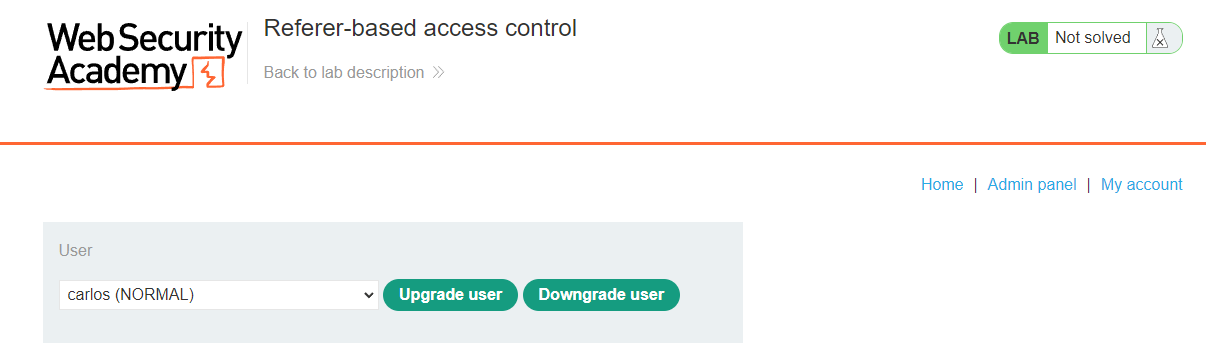
Mục tiêu của bài lab này là khai thác lỗ hổng trong kiểm soát truy cập dựa trên tiêu đề Referer để truy cập vào các chức năng không được phép. Để hoàn thành bài lab, bạn cần truy cập vào chức năng xóa người dùng, vốn bị bảo vệ bởi cơ chế kiểm soát truy cập dựa trên Referer.

Các bước thực hiện:

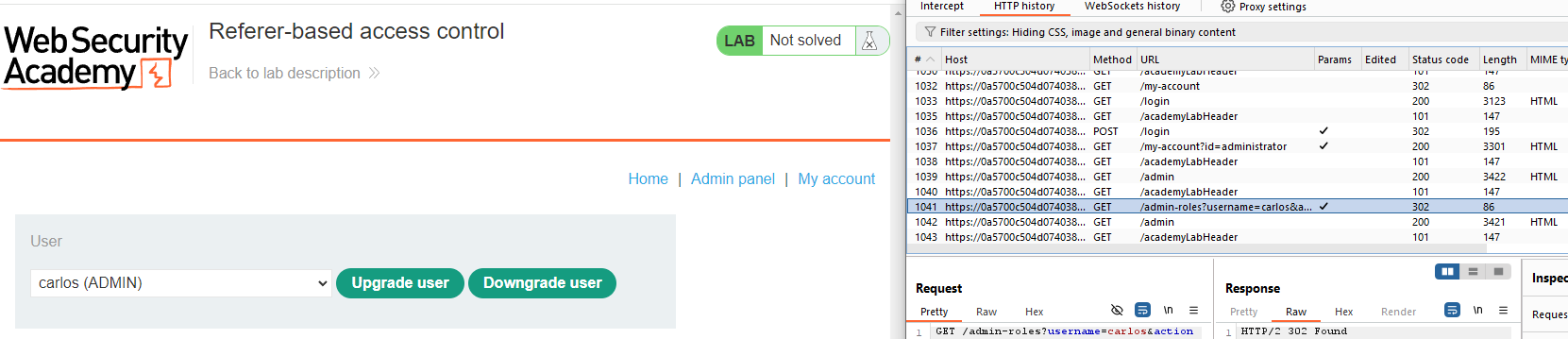
Đăng nhập adminstrator/admin để tìm hiểu chức năng hoạt động



Hình 1. Đăng nhập thành công admin

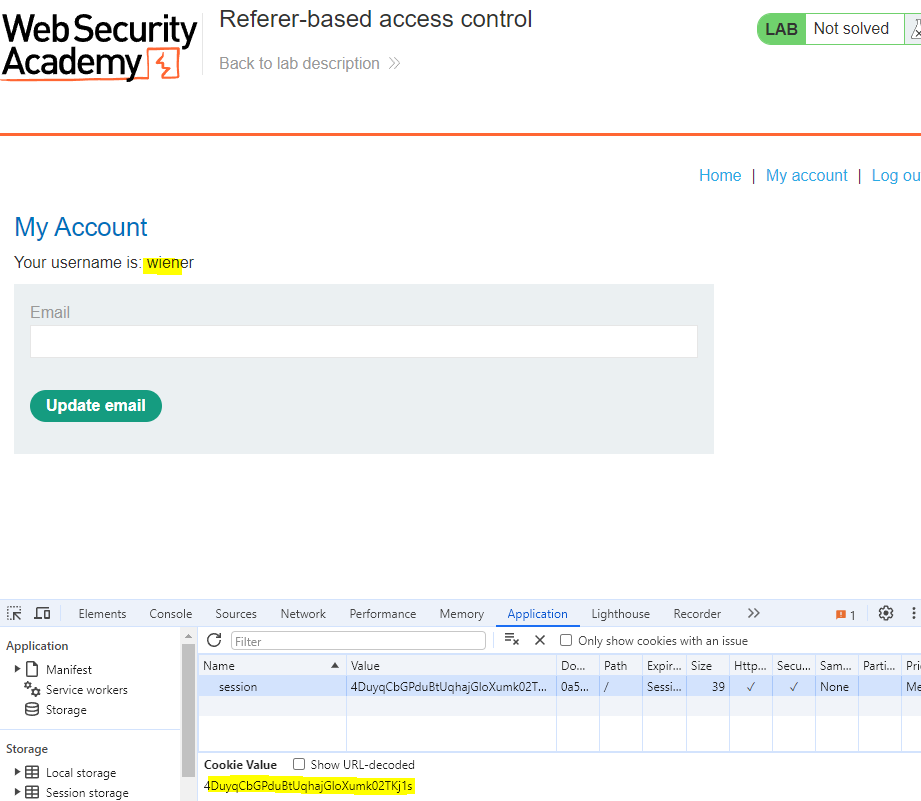


*Hình 2.* Truy cập mục admin panel



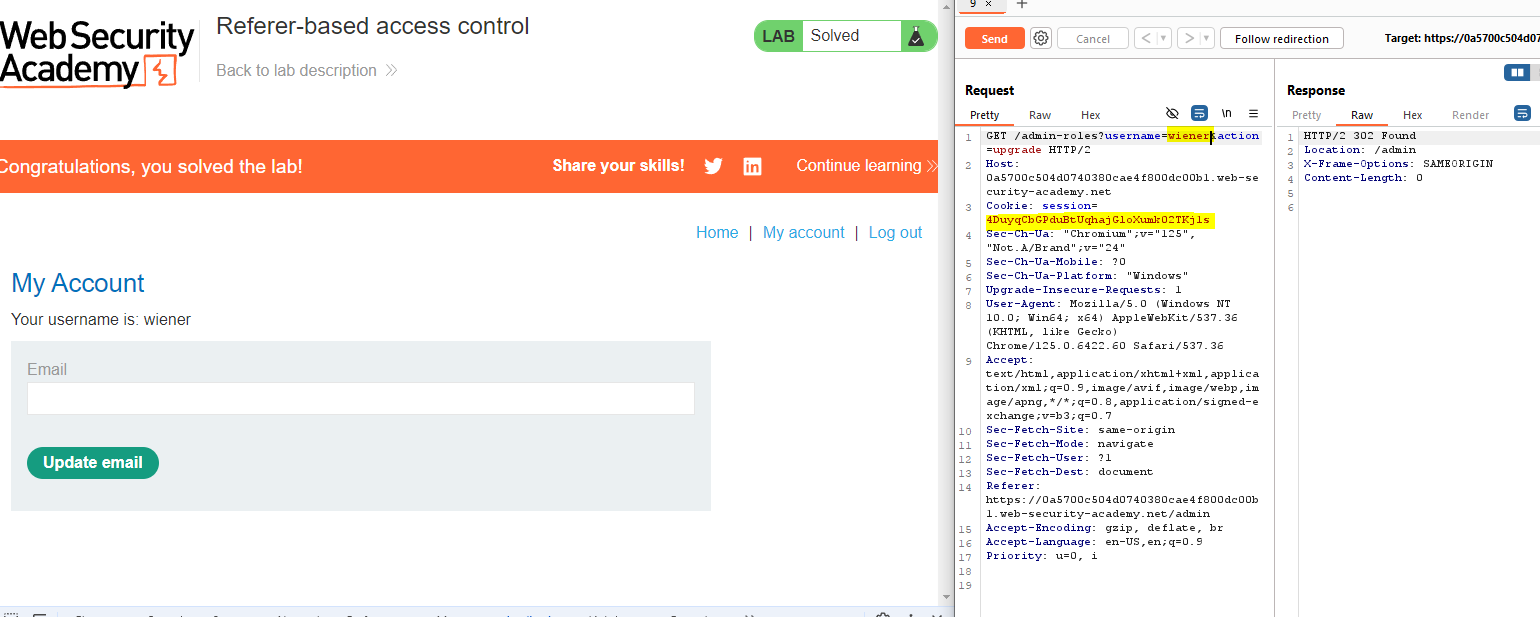
Hình 3. Nâng carlos lên admin

Đăng xuất admin, đăng nhập wiener/peter và lấy được cookie của wiener



Hình 4. Cookie của wiener

Sửa phiên và username, sau đó Send request, bài lab được hoàn thành



Hình 5. Bài lab được hoàn thành