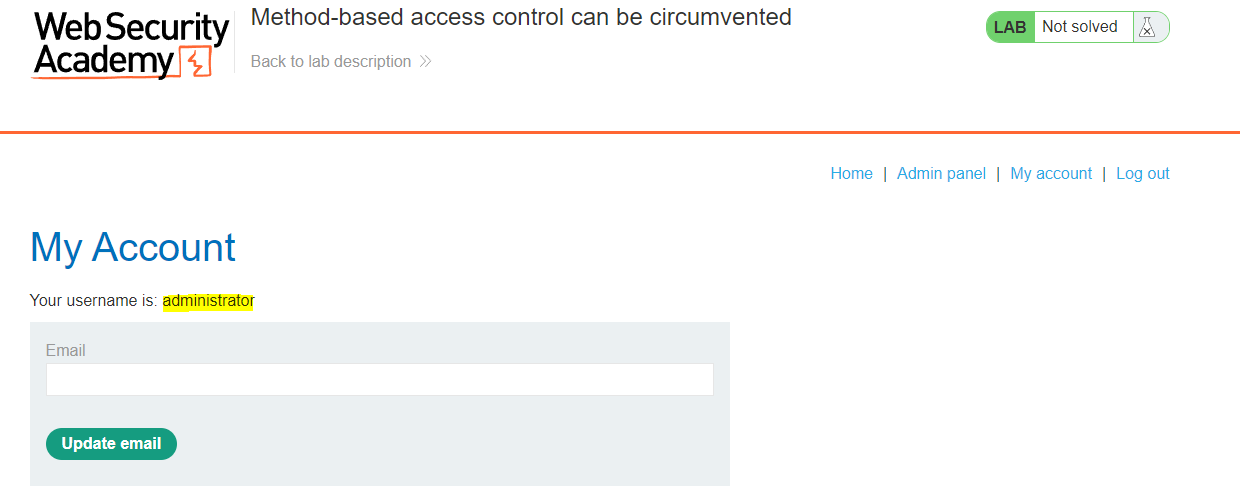
**Lab: Method-based access control can be circumvented**

Bài lab này sử dụng các phương thức HTTP (GET, POST, PUT, DELETE, v.v.) để kiểm soát quyền truy cập vào các chức năng và dữ liệu. Tuy nhiên, ứng dụng có thể không kiểm tra quyền truy cập một cách đúng đắn dựa trên phương thức HTTP, dẫn đến việc kẻ tấn công có thể thay đổi phương thức HTTP để truy cập vào các chức năng quản trị viên hoặc dữ liệu nhạy cảm.

Mục tiêu của bài lab này là khai thác lỗ hổng trong việc kiểm soát truy cập dựa trên phương thức HTTP để truy cập vào các chức năng không được phép. Để hoàn thành bài lab, bạn cần truy cập vào các chức năng quản trị viên hoặc các dữ liệu nhạy cảm mà bạn không được phép truy cập bằng cách thay đổi phương thức HTTP của yêu cầu.

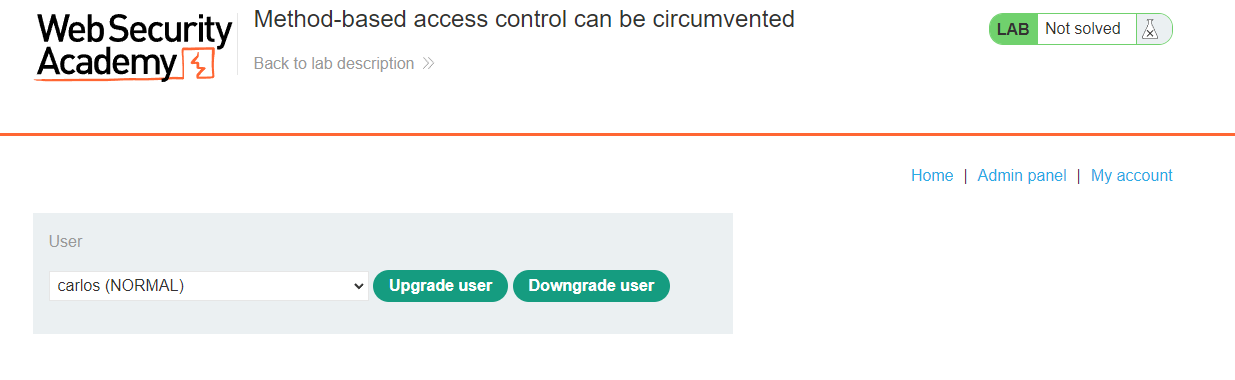
Các bước thực hiện:

Đăng nhập với administrator/admin để test chức năng



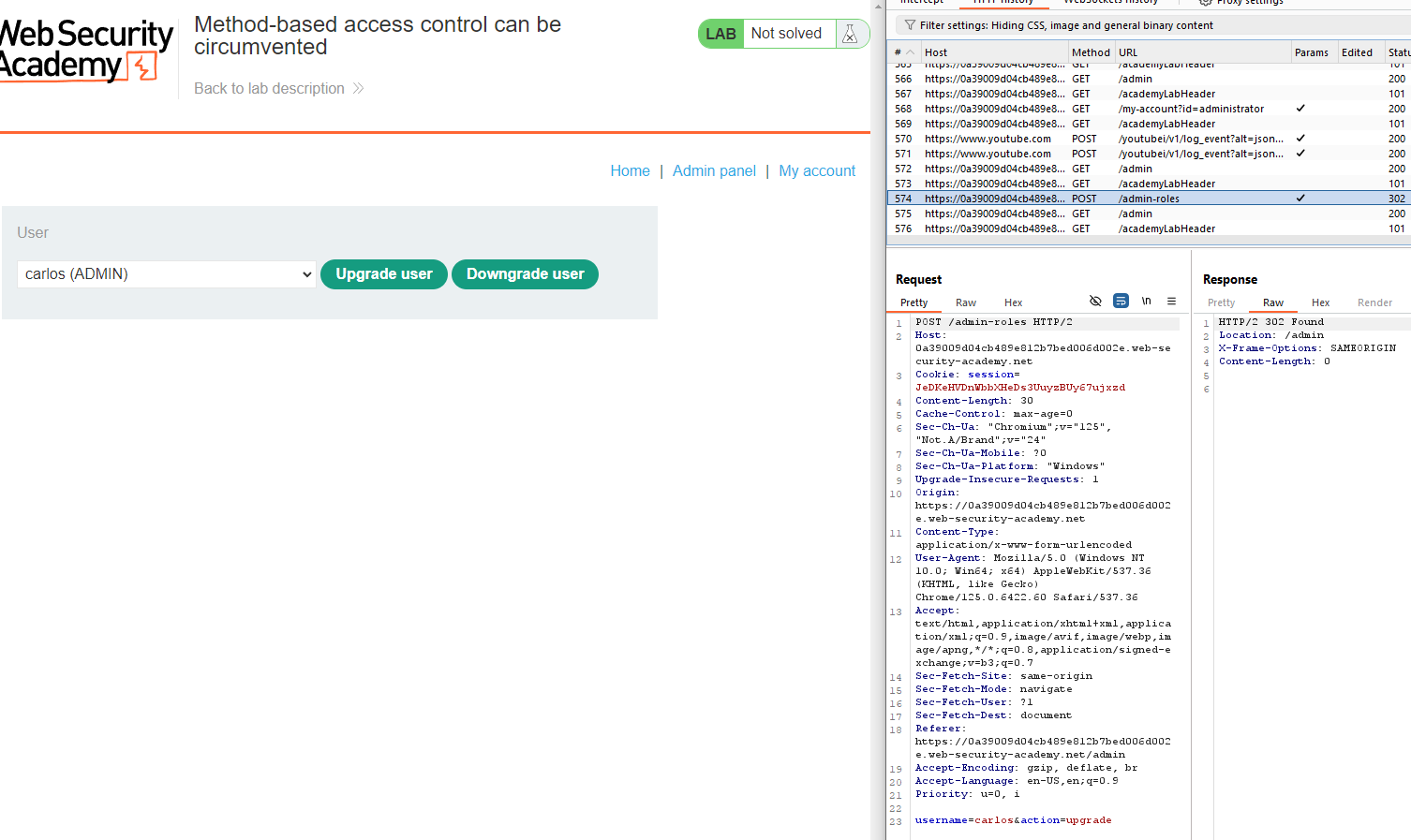
Hình 1. Đăng nhập thành công admin

Chức nâng nâng/ hạ quyền người dùng



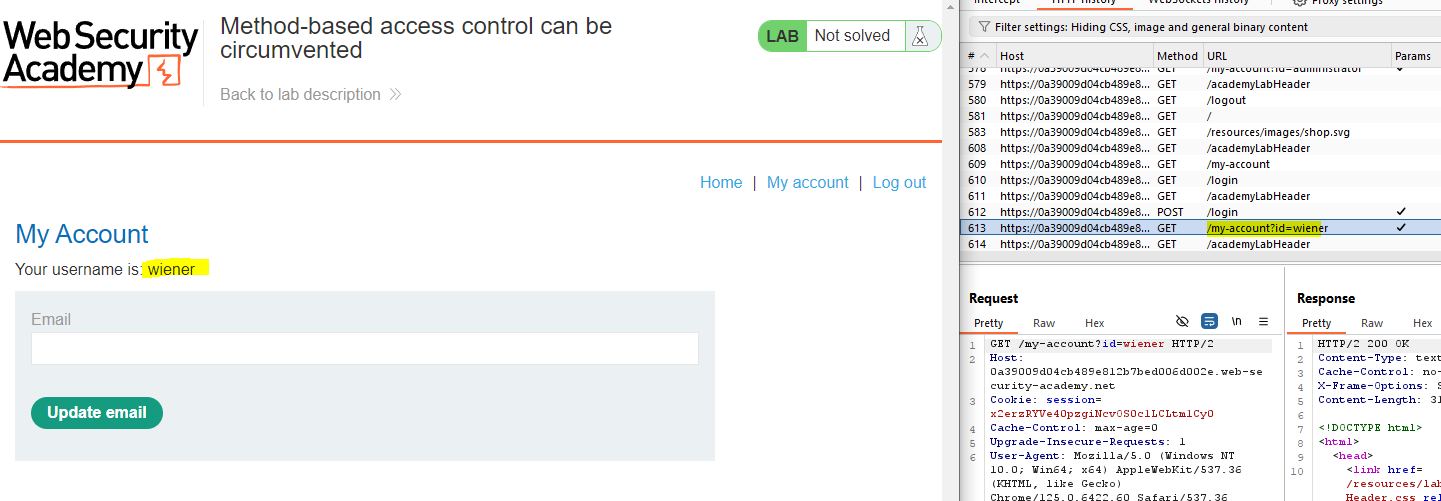
*Hình 2.* Truy cập mục admin panel

Thử nâng quyền carlos để xem cách hoạt động



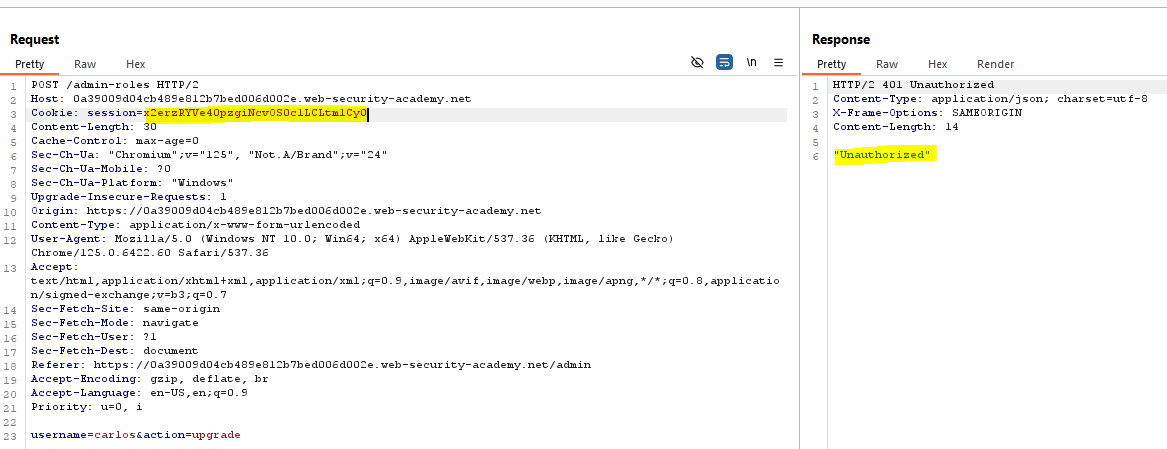
Hình 3. Nâng carlos lên admin

Đăng xuất admin và đăng nhập với wiener/peter



Hình 4. Đăng nhập thành công tài khoản wiener

Thử copy phiên của wiener gắn vào request admin-roles vừa bắt được



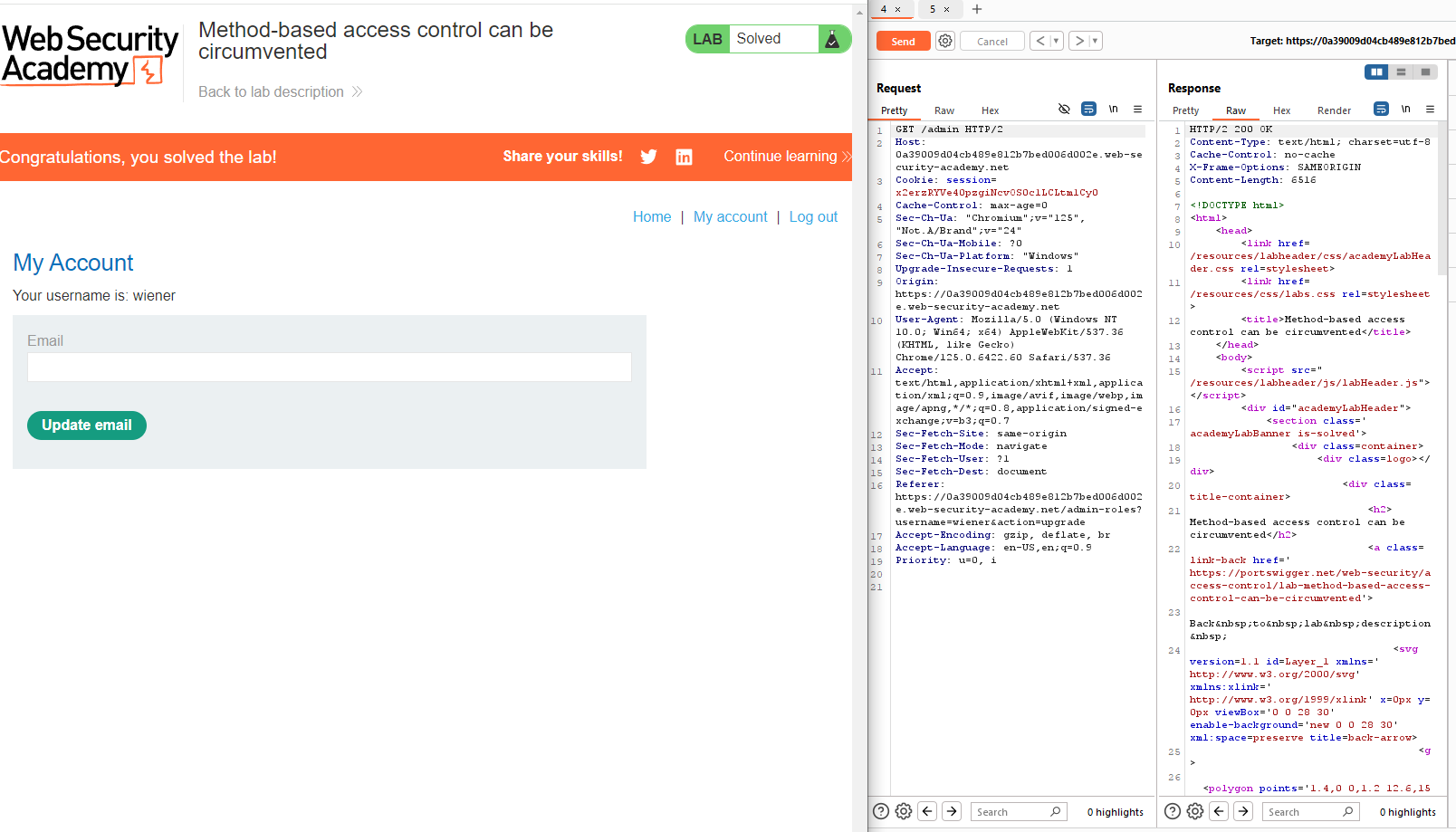
Hình 5. Người dùng thông thường không có khả năng nâng quyền người dùng

Chuyển thành phương thức GET, 1 mã 302 trả về



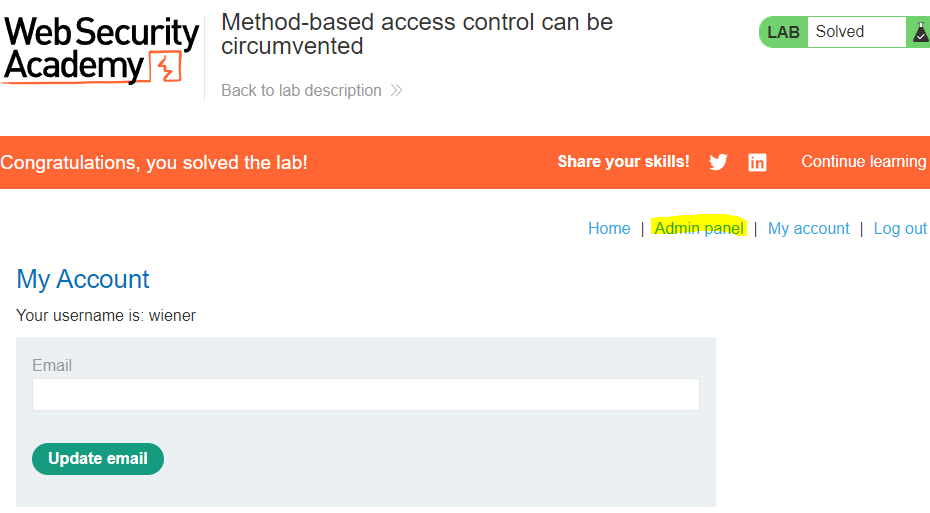
Hình 6. Respone 302 được trả về

Follow redirection -> hoàn thành bài lab



Hình 7. Bài lab được hoàn thành

Load lại trang web tài khoản wiener đã được nâng quyền



Hình 8. Tài khoản wiener đã leo lên quyền admin