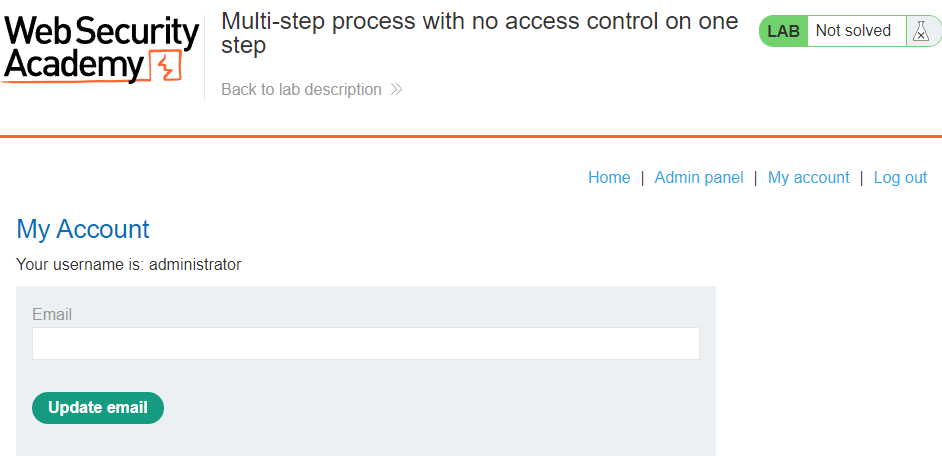
**Lab: Multi-step process with no access control on one step**

Bài lab này sử dụng một quy trình đa bước để thực hiện các hành động quan trọng, chẳng hạn như xóa tài khoản người dùng. Quy trình này có thể bao gồm nhiều bước, mỗi bước yêu cầu quyền truy cập cụ thể. Tuy nhiên, có thể có một bước trong quy trình không được bảo vệ đúng cách, cho phép kẻ tấn công bỏ qua các bước trước đó để thực hiện hành động trái phép.

Mục tiêu của bài lab này là khai thác lỗ hổng trong quy trình đa bước mà không có kiểm soát truy cập ở một bước nào đó để thực hiện hành động trái phép. Để hoàn thành bài lab, bạn cần tìm và lợi dụng bước trong quy trình mà không có kiểm soát truy cập, nhằm thực hiện hành động trái phép như xóa tài khoản của người dùng.

Các bước thực hiện:

Đăng nhập với administrator/admin



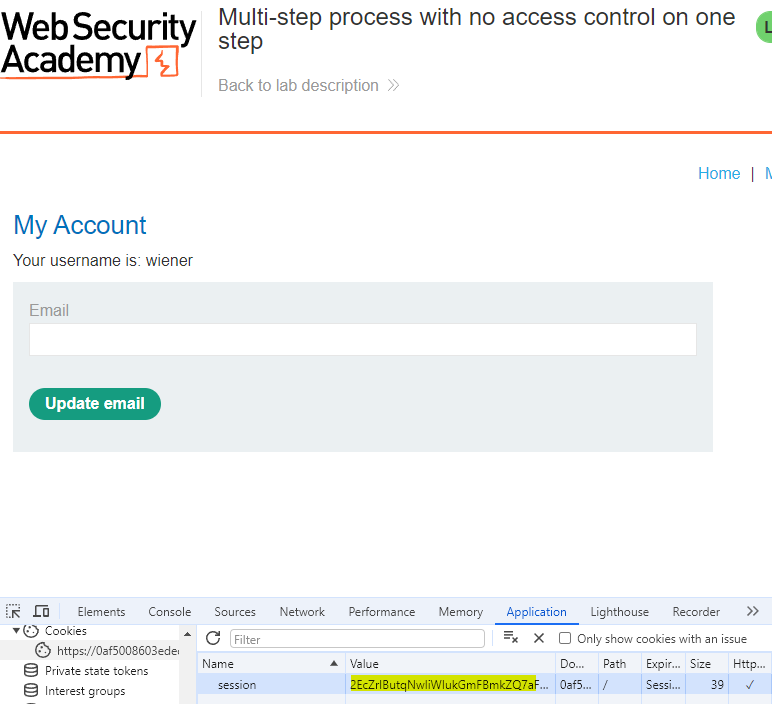
Hình 1. Đăng nhập thành công tài khoản admin

Test thử chức năng nâng quyền người dùng và bắt 2 request gửi sang Repeater để phân tích



*Hình 2. Hai request để nâng quyền người dùng*

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



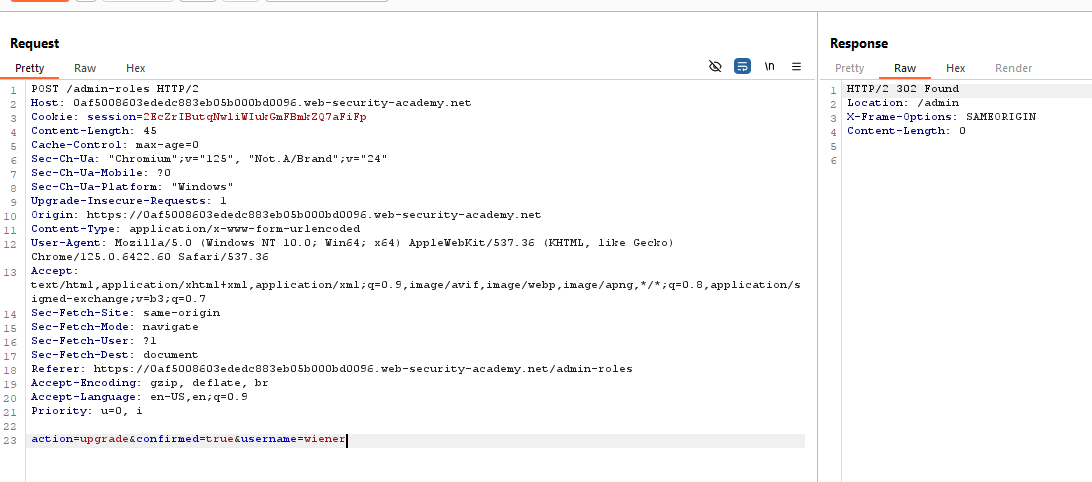
Hình 3. Cookie của wiener

Sửa request đầu tiên



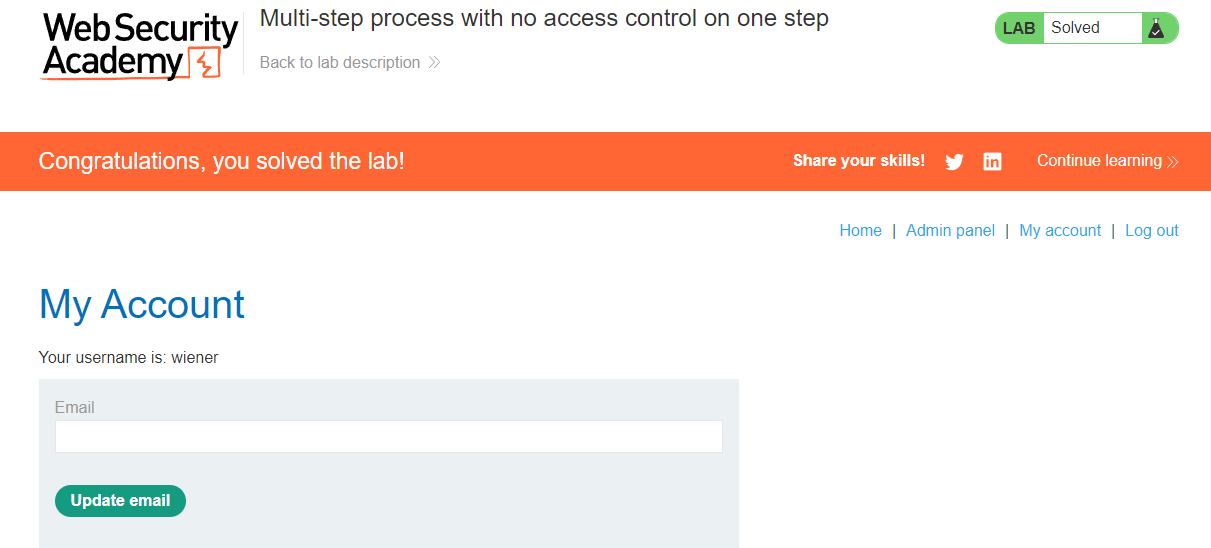
Hình 4. Sửa request thứ nhất

Sửa request thứ hai



Hình 5. Sửa request thứ hai, nhận respone 302

Load lại trang, tài khoản wiener đã được nâng thành quyền admin



Hình 6. Wiener đã lên quyền admin, bài lab được hoàn thành