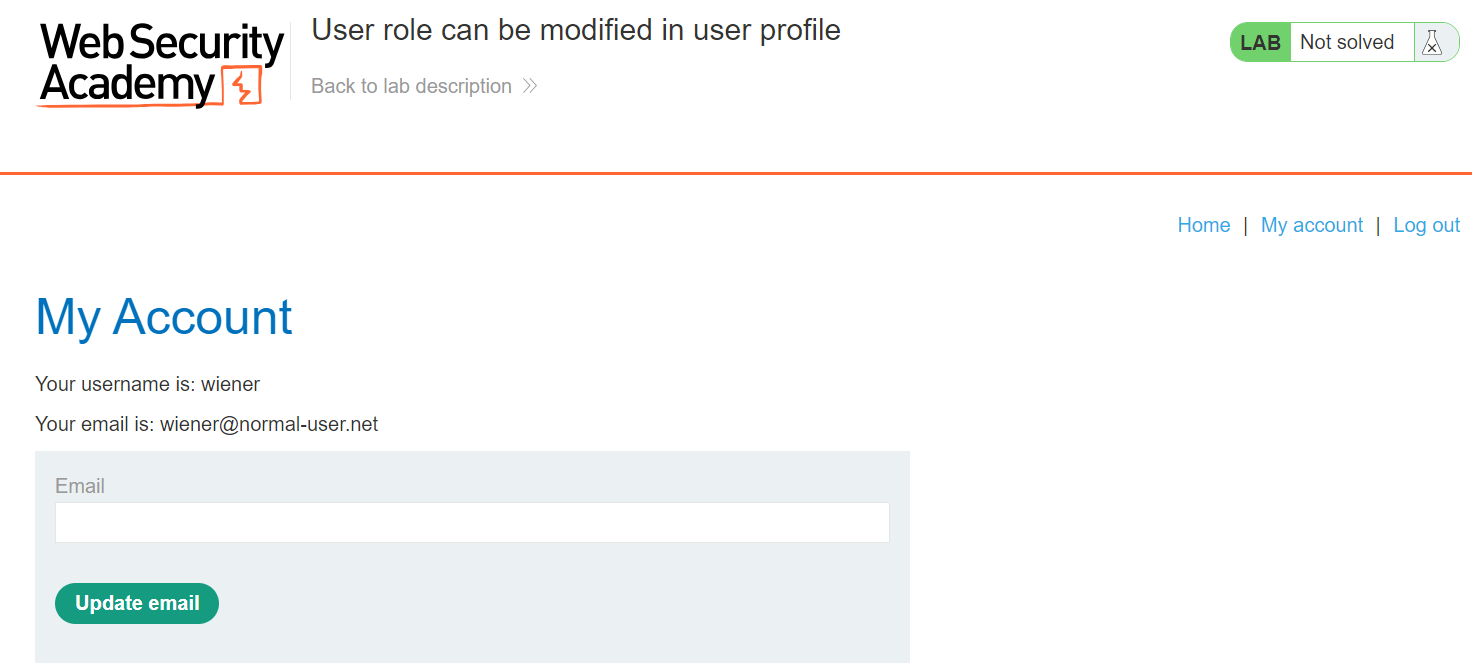
**Lab: User ID controlled by request parameter, with unpredictable user IDs**

Bài lab này cho phép người dùng chỉnh sửa hồ sơ cá nhân của họ. Tuy nhiên, có một lỗ hổng trong quá trình này cho phép người dùng thay đổi vai trò của mình thành quản trị viên bằng cách sửa đổi yêu cầu HTTP khi gửi thông tin hồ sơ cá nhân. Bằng cách khai thác lỗ hổng này, kẻ tấn công có thể nâng cấp quyền hạn của mình và truy cập vào các chức năng quản trị.

Mục tiêu của bài lab này là khai thác lỗ hổng trong việc chỉnh sửa quyền hạn người dùng thông qua hồ sơ cá nhân. Để hoàn thành bài lab, bạn cần thay đổi vai trò của mình thành quản trị viên bằng cách sửa đổi yêu cầu HTTP khi chỉnh sửa hồ sơ cá nhân, sau đó truy cập vào bảng điều khiển quản trị viên và xóa tài khoản của người dùng carlos.

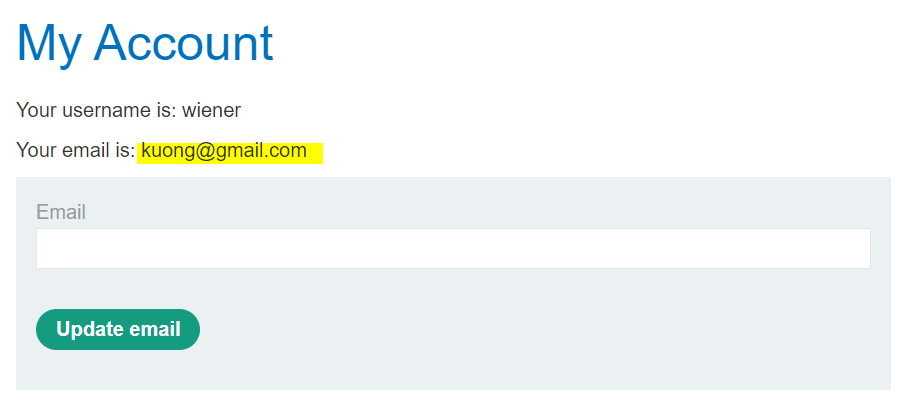
Các bước thực hiện:

Đăng nhập bằng tài khoản wiener/peter



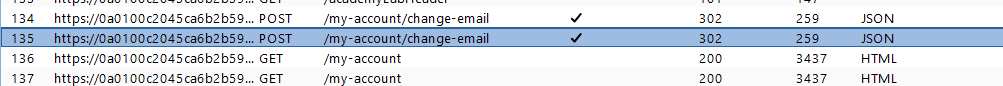
Hình 1. Đăng nhập thành công tài khoản wiener

Test chức năng thay đổi email



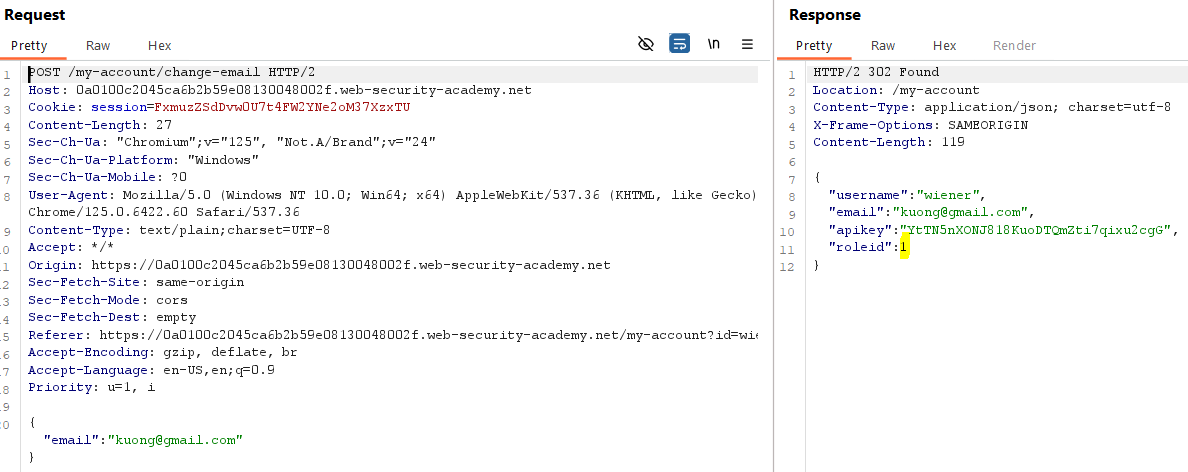
Hình 2. Email đã thay đổi thành kuong@gmail.com

Bắt request gửi sang Repeater để phân tích



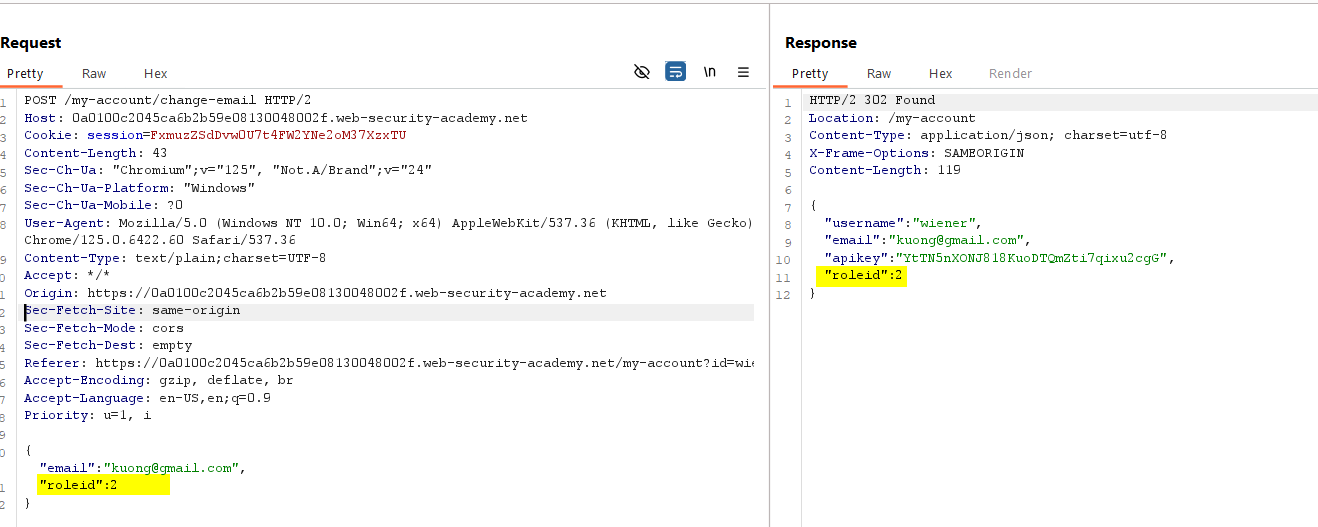
Hình 3. Request thay đổi email

Thoạt nhìn nhận thấy không có khả năng xảy ra lỗ hổng, nhưng nhìn sang Respone thì thấy roleid:1 -> nghi ngờ.



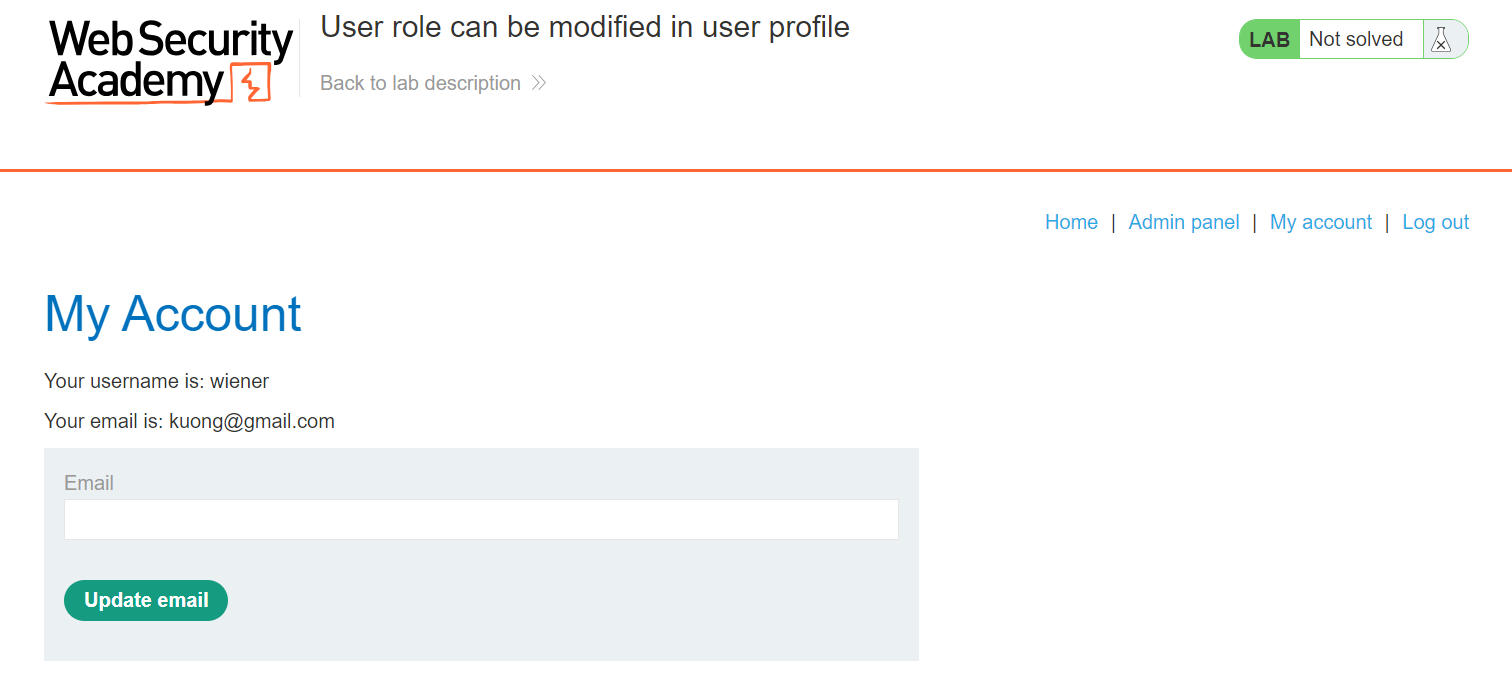
Hình 4. Phân tích request thay đổi email

Thay đổi roleid, thử = 2, và sau đó ấn Send, Respone đã chuyển roleid=2



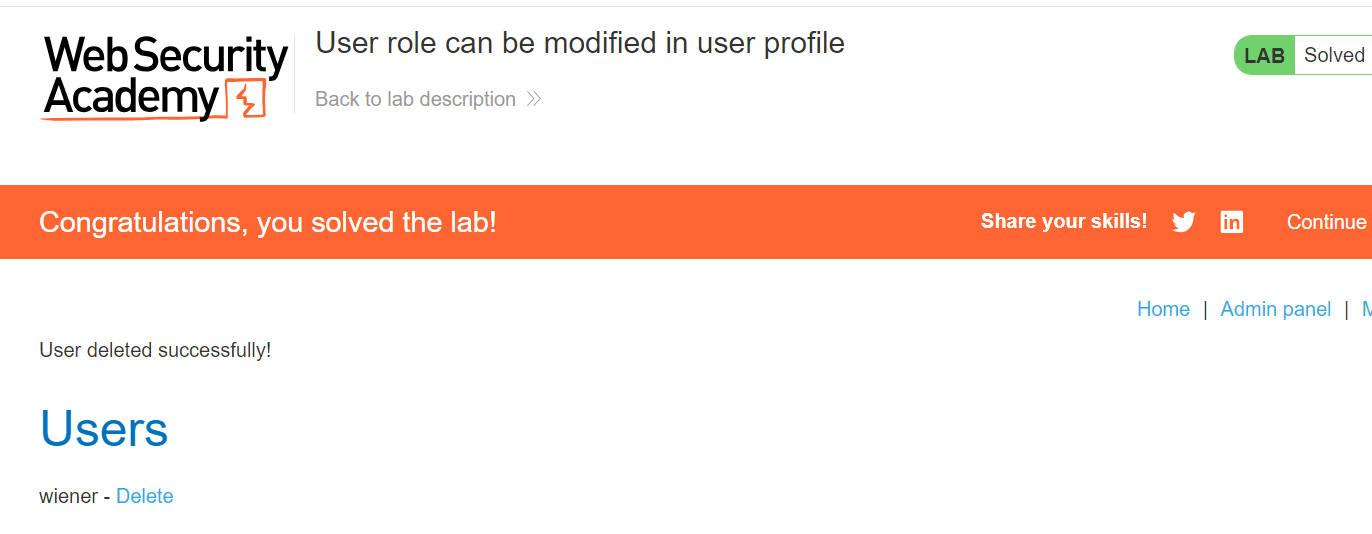
Hình 5. RoleID của wiener đã được thay đổi

Load lại trang web, tài khoản wiener đã lên quyền quản trị



Hình 6. Tài khoản wiener có quyền quản trị

Truy cập Admin panel và xoá người dùng carlos, bài lab được hoàn thành



Hình 7. Bài lab được hoàn thành