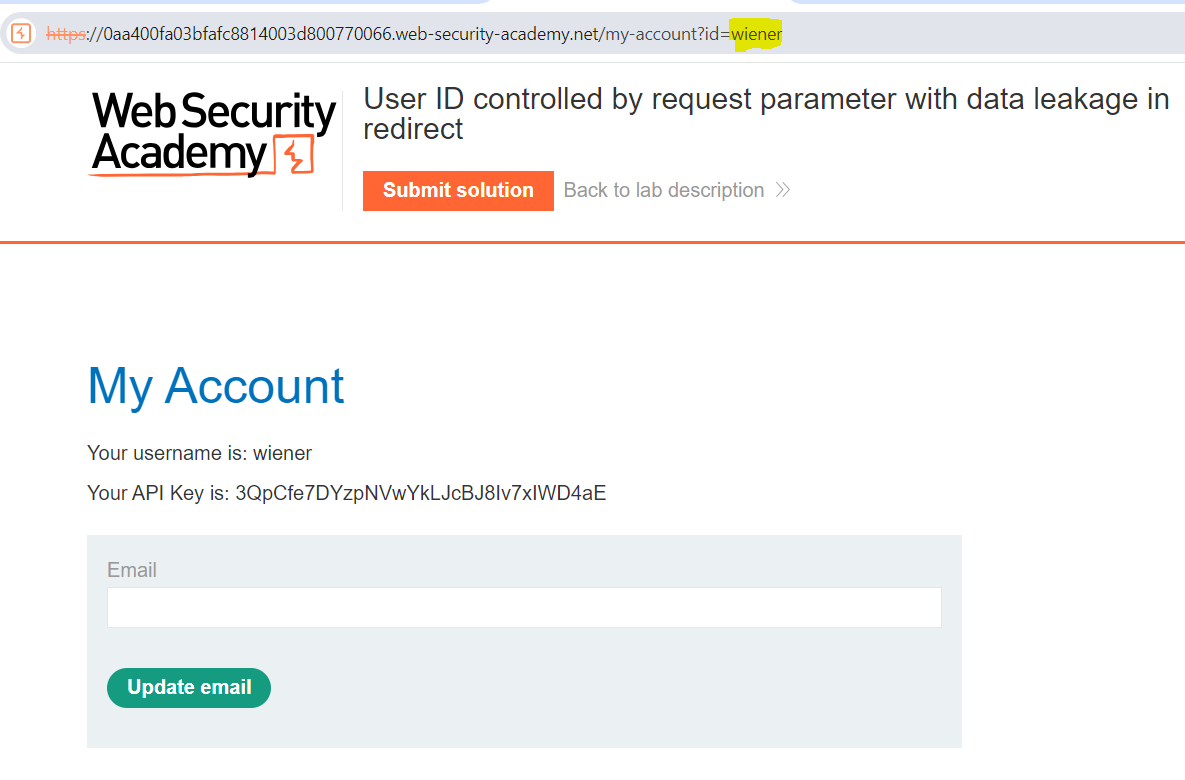
**Lab: User ID controlled by request parameter with data leakage in redirect**

Bài lab này sử dụng một tham số yêu cầu để xác định ID người dùng, nhưng các ID này không được kiểm tra và bảo vệ đúng cách. Ngoài ra, có một lỗ hổng rò rỉ dữ liệu khi ứng dụng thực hiện chuyển hướng, cho phép kẻ tấn công truy xuất ID người dùng từ các phản hồi chuyển hướng.

Mục tiêu của bài lab này là khai thác lỗ hổng trong việc kiểm soát ID người dùng thông qua tham số yêu cầu và rò rỉ dữ liệu trong quá trình chuyển hướng để truy cập vào tài khoản của người dùng carlos.

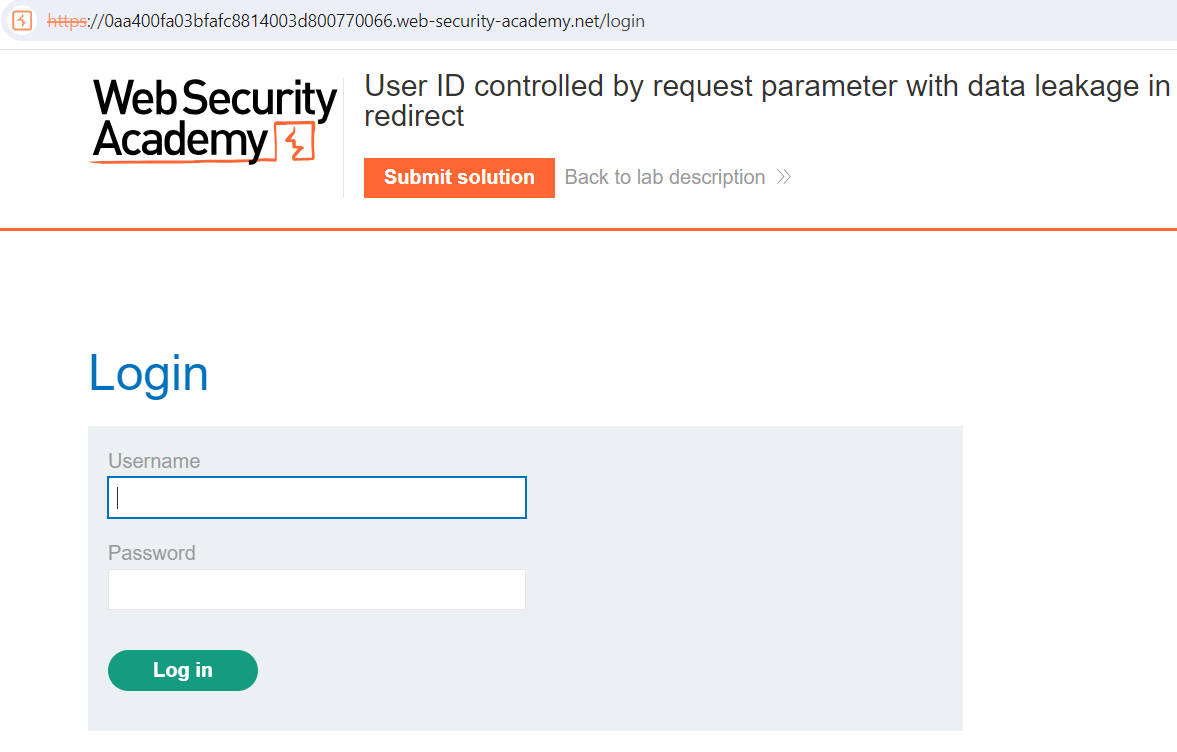
Các bước thực hiện:

Đăng nhập bằng tài khoản wiener/peter



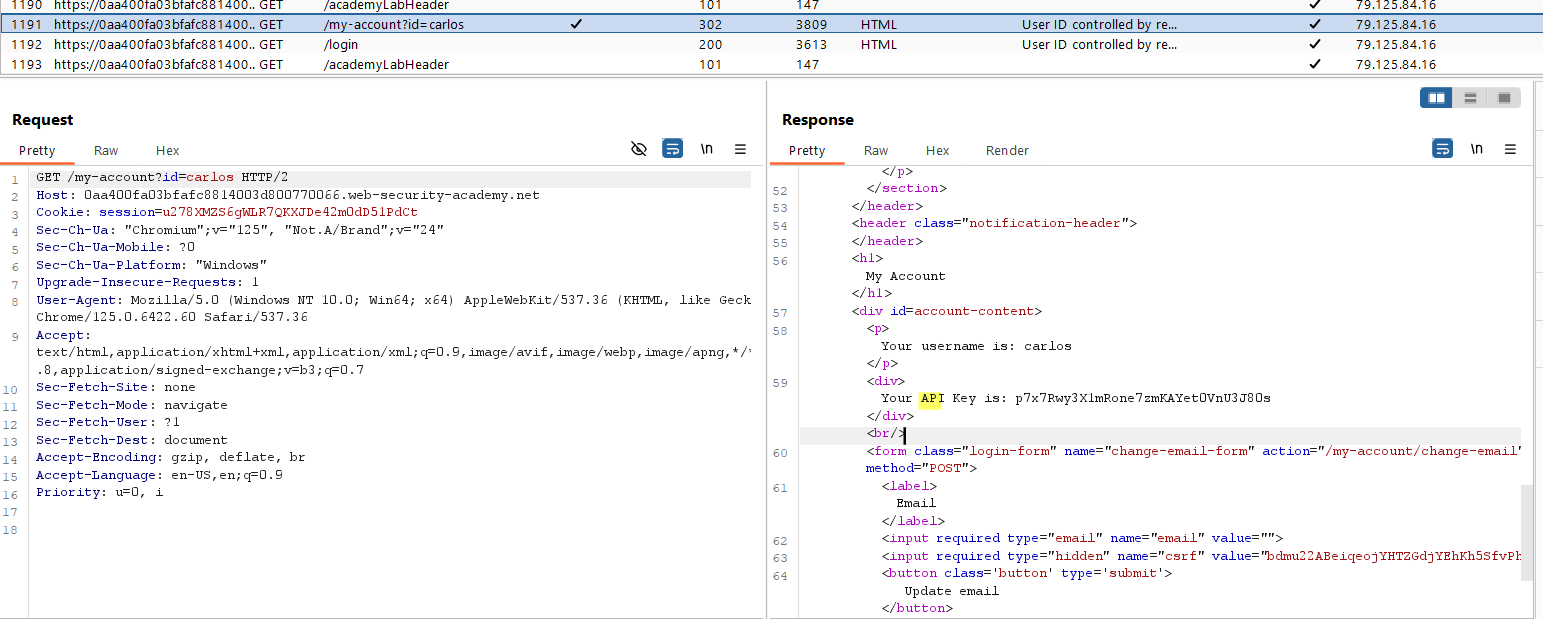
Hình 1. Đăng nhập thành công tài khoản wiener

Sửa “id=carlos”



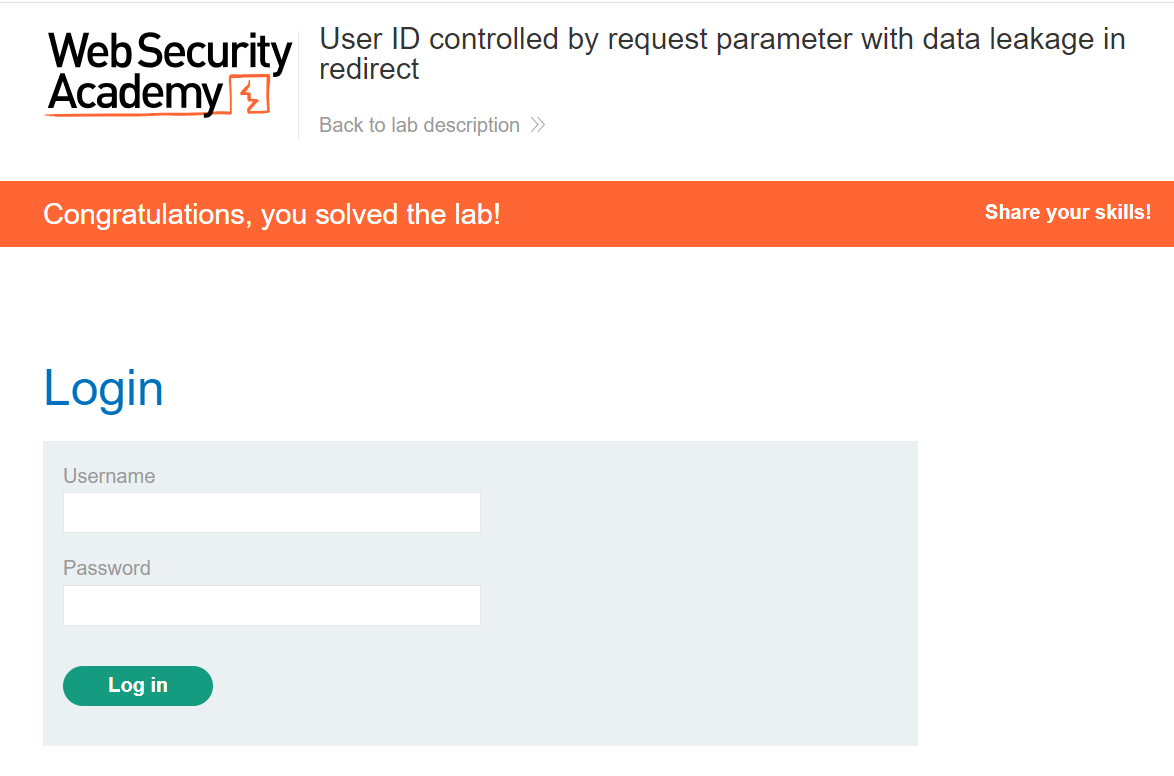
Hình 2. Trang web chuyển hướng tới trang login

Phân tích request cho thấy chuyển hướng 302 và chuyển tới trang login, tuy nhiên nó thực sự xuất ra trang trong chuyển hướng 302



Hình 3. Gửi sang Reapeater để phân tích

Bài lab được hoàn thành



Hình 4. Hoàn thành bài lab