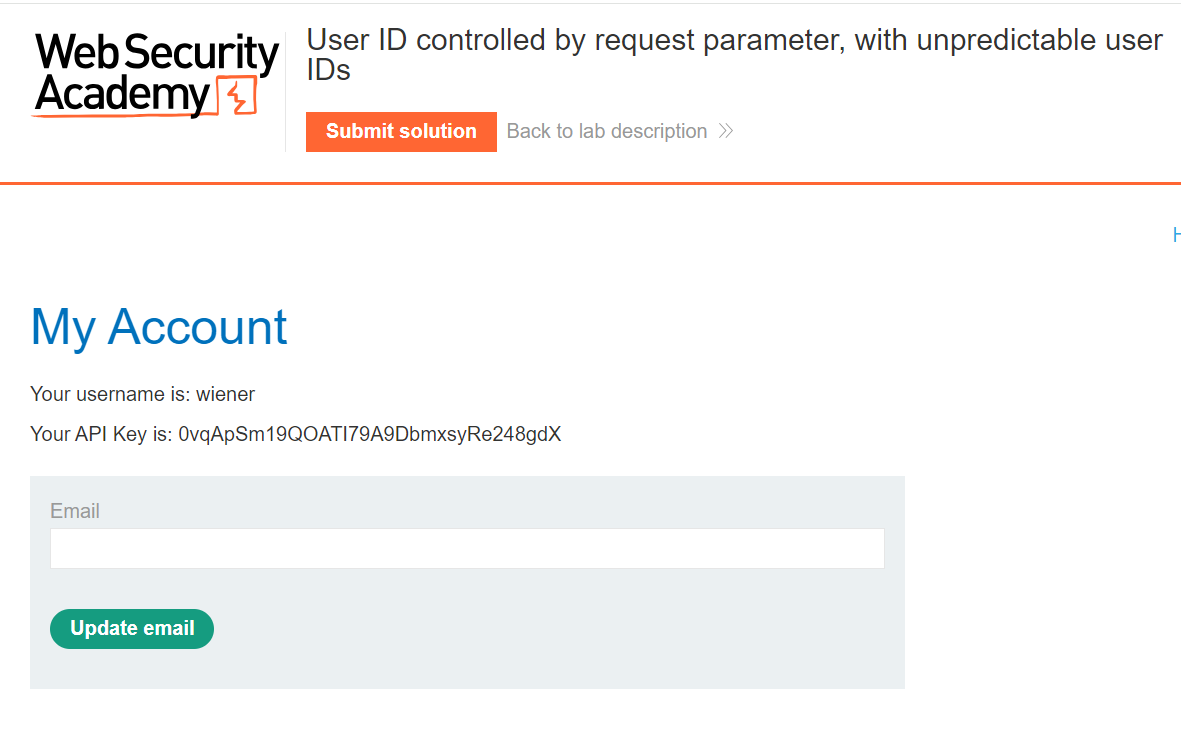
**Lab: User ID controlled by request parameter, with unpredictable user IDs**

Bài lab này sử dụng một tham số yêu cầu để xác định ID người dùng, nhưng các ID này không theo một mẫu dễ đoán. Tuy nhiên, ứng dụng không kiểm tra quyền truy cập một cách đúng đắn, cho phép kẻ tấn công thay đổi giá trị của tham số này để truy cập tài khoản của người dùng khác nếu họ có thể đoán được hoặc tìm ra ID người dùng tương ứng.

Mục tiêu của bài lab này là truy cập vào tài khoản của người dùng carlos bằng cách khai thác lỗ hổng trong cơ chế kiểm soát ID người dùng thông qua tham số yêu cầu với các ID người dùng không thể đoán trước. Để hoàn thành bài lab, bạn cần xác định ID người dùng của carlos và sử dụng nó để truy cập vào tài khoản của carlos.

Các bước thực hiện:

Đăng nhập bằng tài khoản wiener/peter

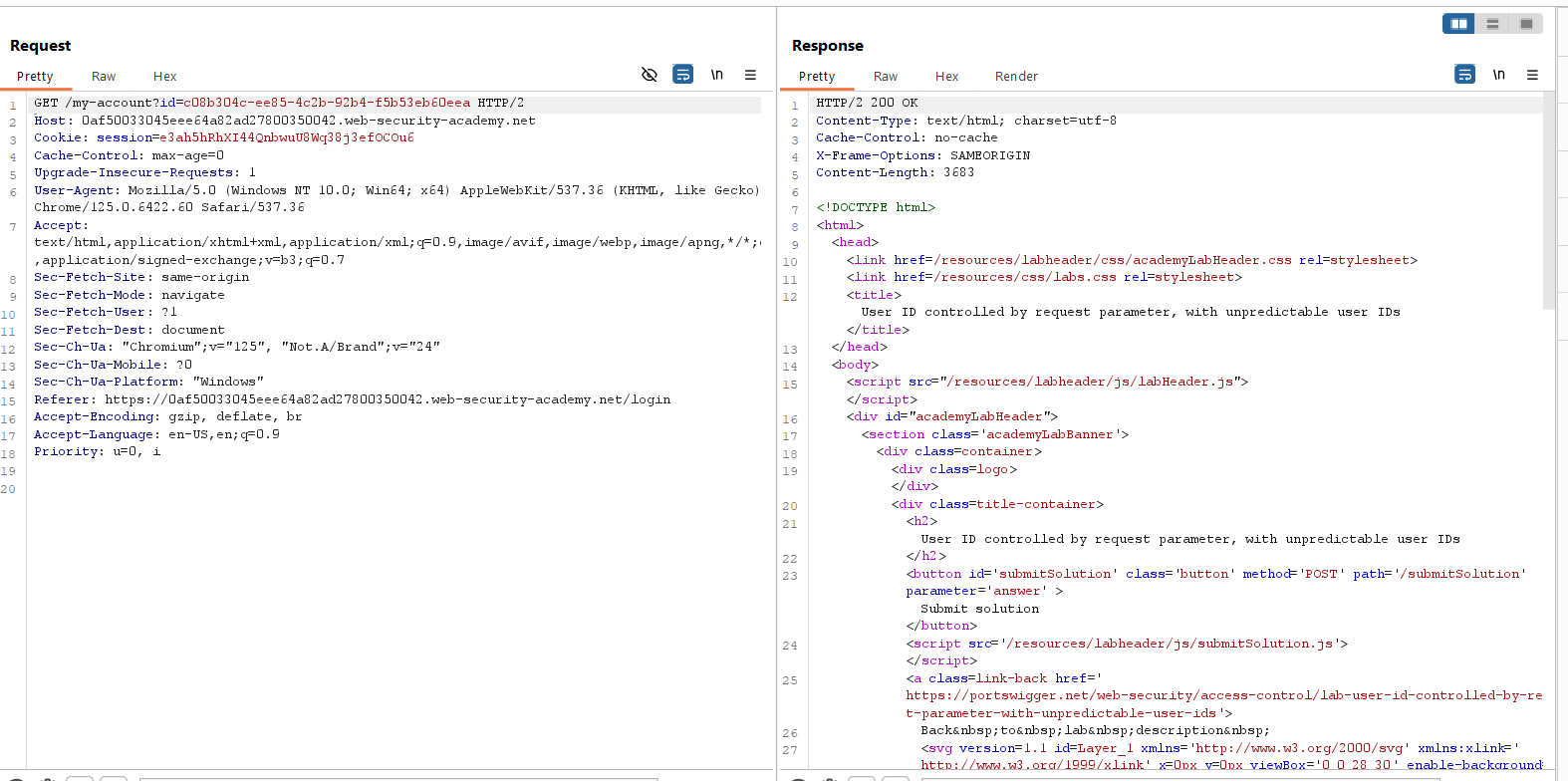


Hình 1. Đăng nhập thành công tài khoản wiener

Bắt request gửi sang Repeater



Hình 2. Request GET /myaccount?id=..

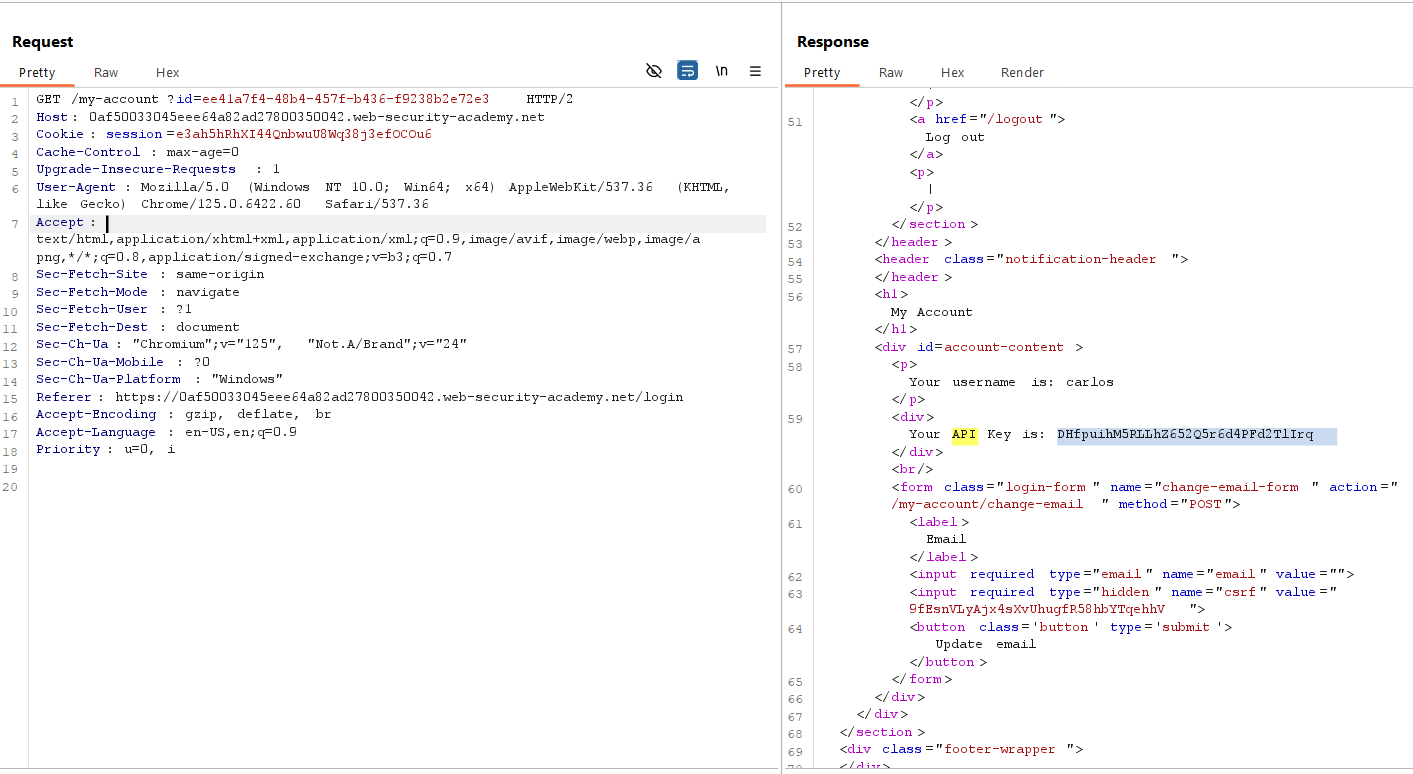


Hình 3. Gửi sang Reapeater để phân tích

Tìm kiếm blog carlos

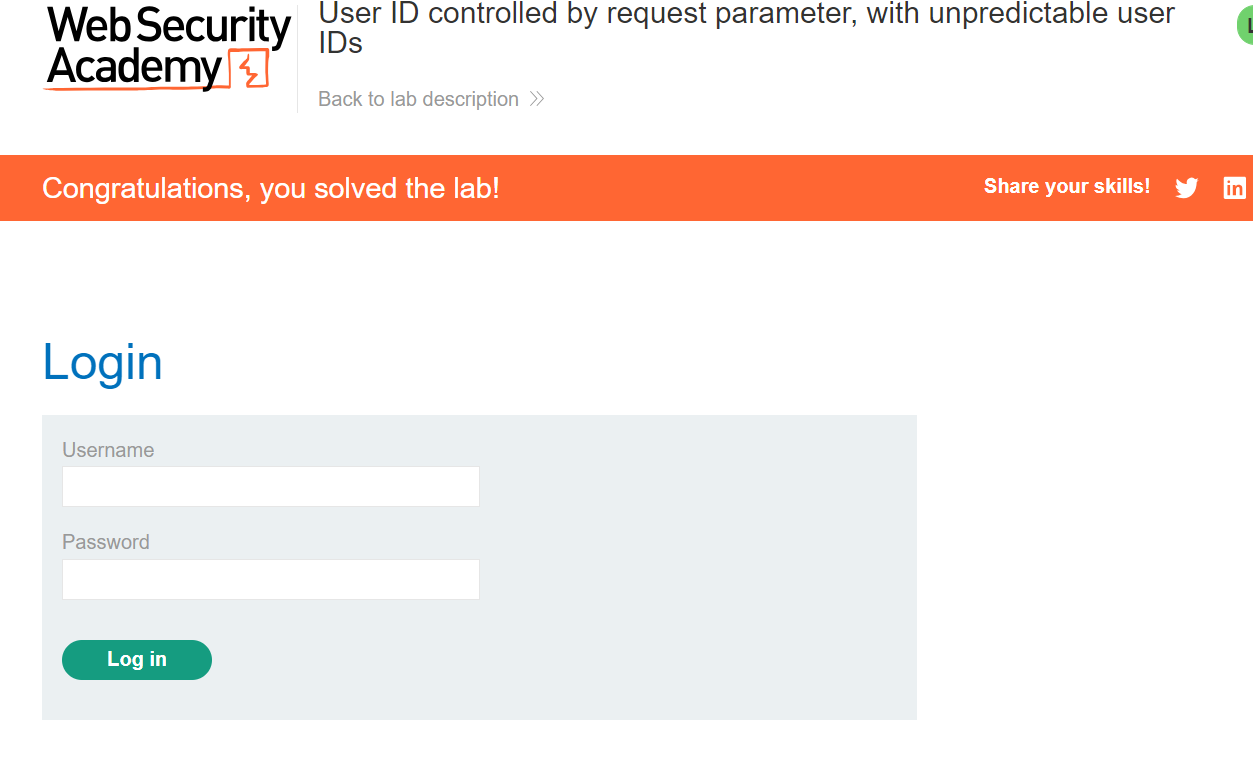
Hình 4. Blog của Carlos

Lấy được userid thông qua blog



Hình 5. Tìm được API của Carlos

Tìm được API của carlos và submit solution hoàn thành bài lab



Hình 6. Bài lab được hoàn thành