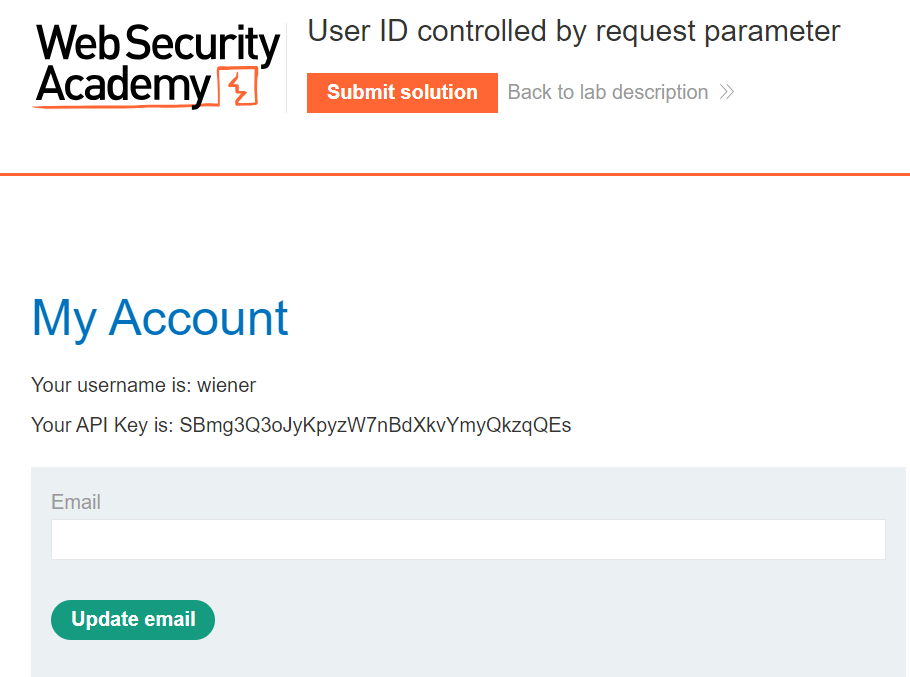
**Lab: User ID controlled by request parameter**

Bài lab này sử dụng một tham số yêu cầu để xác định ID người dùng. Tuy nhiên, nó 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.

Mục tiêu của bài lab này là truy cập tài khoản của người dùng carlos bằng cách khai thác lỗ hổng trong cơ chế kiểm soát ID người dùng.

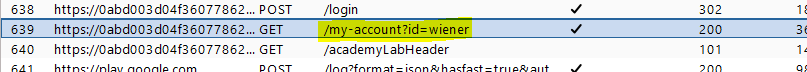
Các bước thực hiện:

Đăng nhập bằng tài khoản wiener/peter

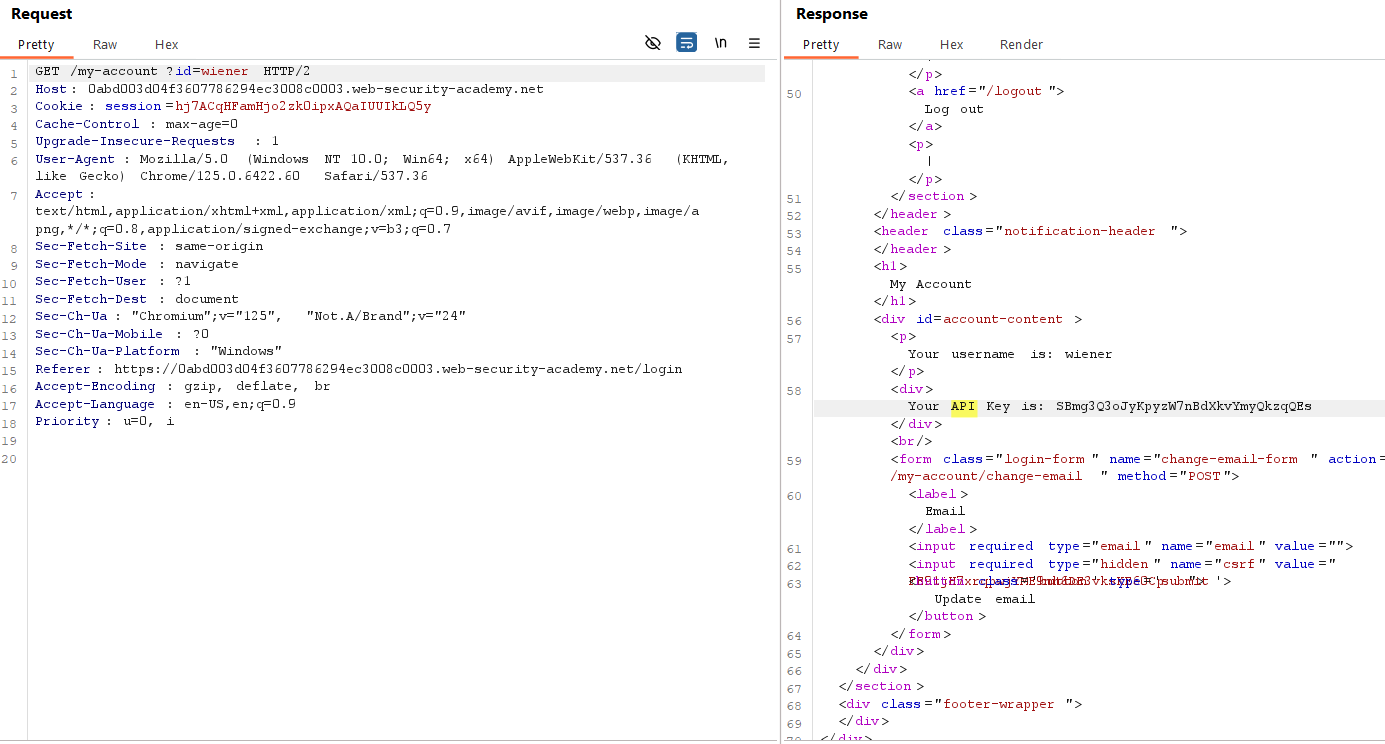


Hình 1. Đăng nhập thành công tài khoản wiener

Bắt request /myaccount?id=wiener gửi sang Repeater

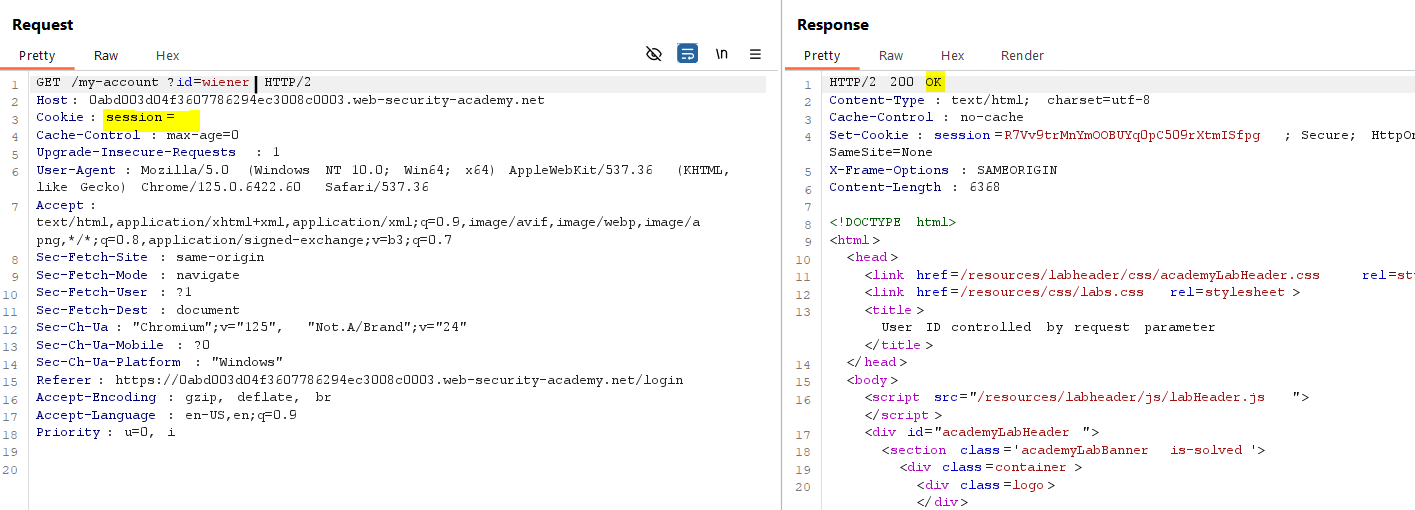


Hình 2. Request GET /myaccount?id=wiener



Hình 3. Gửi sang Reapeater để phân tích

Cookie không gán với người dùng có thể gây ra lỗ hổng leo thang đặc quyền



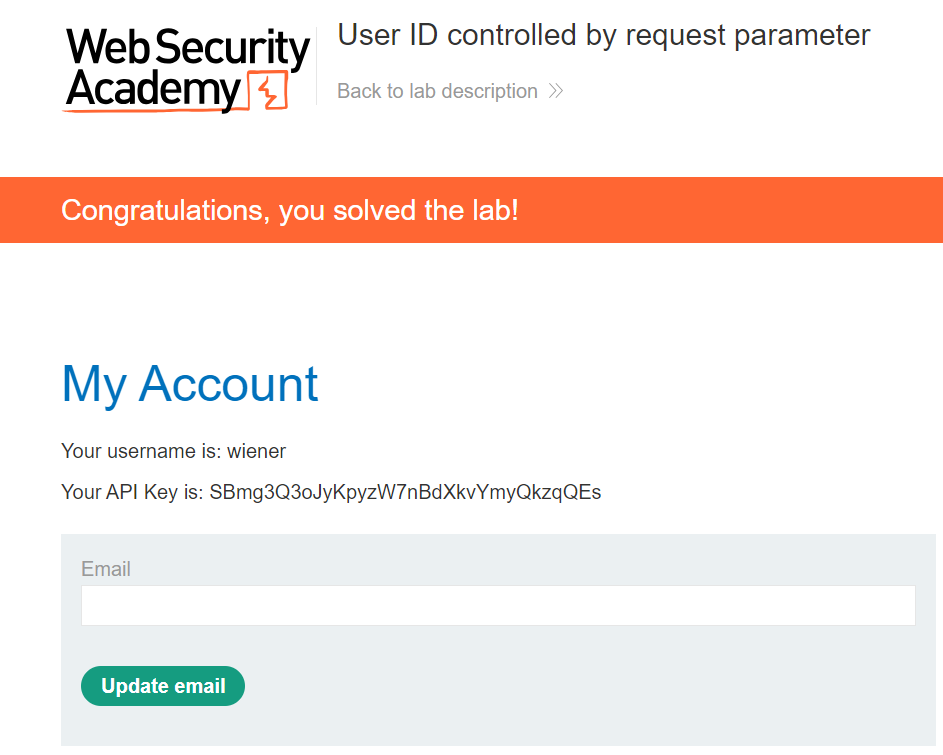
Hình 4. Xoá cookie nhưng vẫn nhận được mã 200

Sửa id = carlos và ấn “Send”. Kết quả ra được API của carlos



Hình 5. Tìm được API của carlos

Submit solution API vừa tìm được, bài lab được giải quyết



Hình 6. Bài lab được hoàn thánh