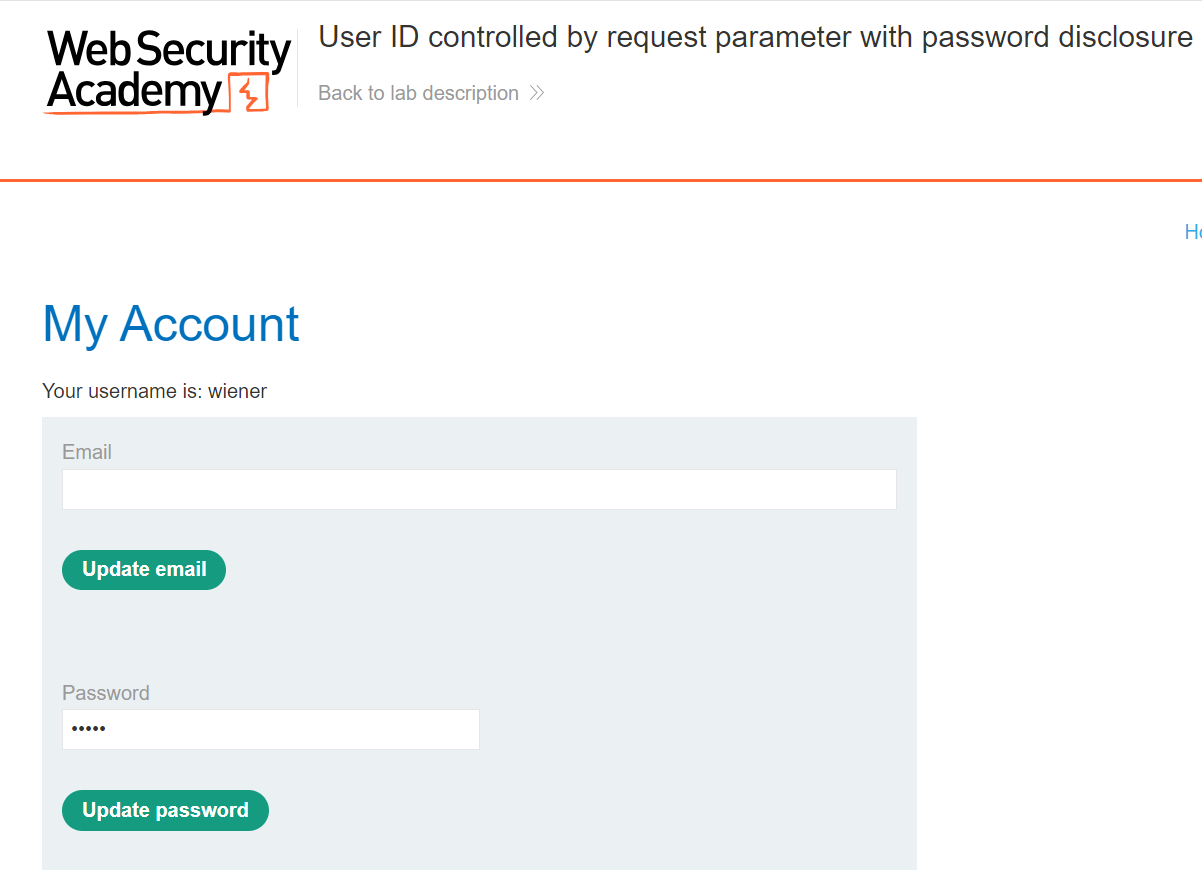
**Lab: User ID controlled by request parameter with password disclosure**

Bài lab này sử dụng một tham số yêu cầu để xác định ID người dùng, nhưng không kiểm tra quyền truy cập một cách đúng đắn. Hơn nữa, ứng dụng có thể tiết lộ mật khẩu của người dùng trong các phản hồi hoặc thông báo lỗi khi xử lý các yêu cầu..

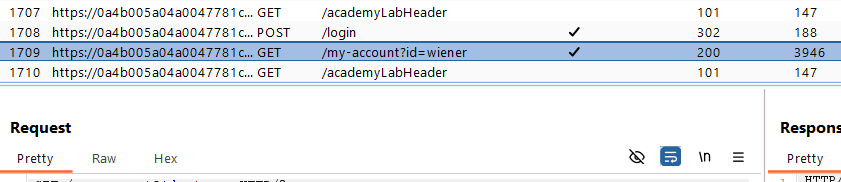
Mục tiêu của bài lab này là khai thác lỗ hổng trong việc kiểm soát ID người dùng thông qua tham số yêu cầu, dẫn đến việc rò rỉ mật khẩu của người dùng carlos. Để hoàn thành bài lab, bạn cần truy cập vào tài khoản của carlos và tìm thấy mật khẩu bị lộ.

Các bước thực hiện:

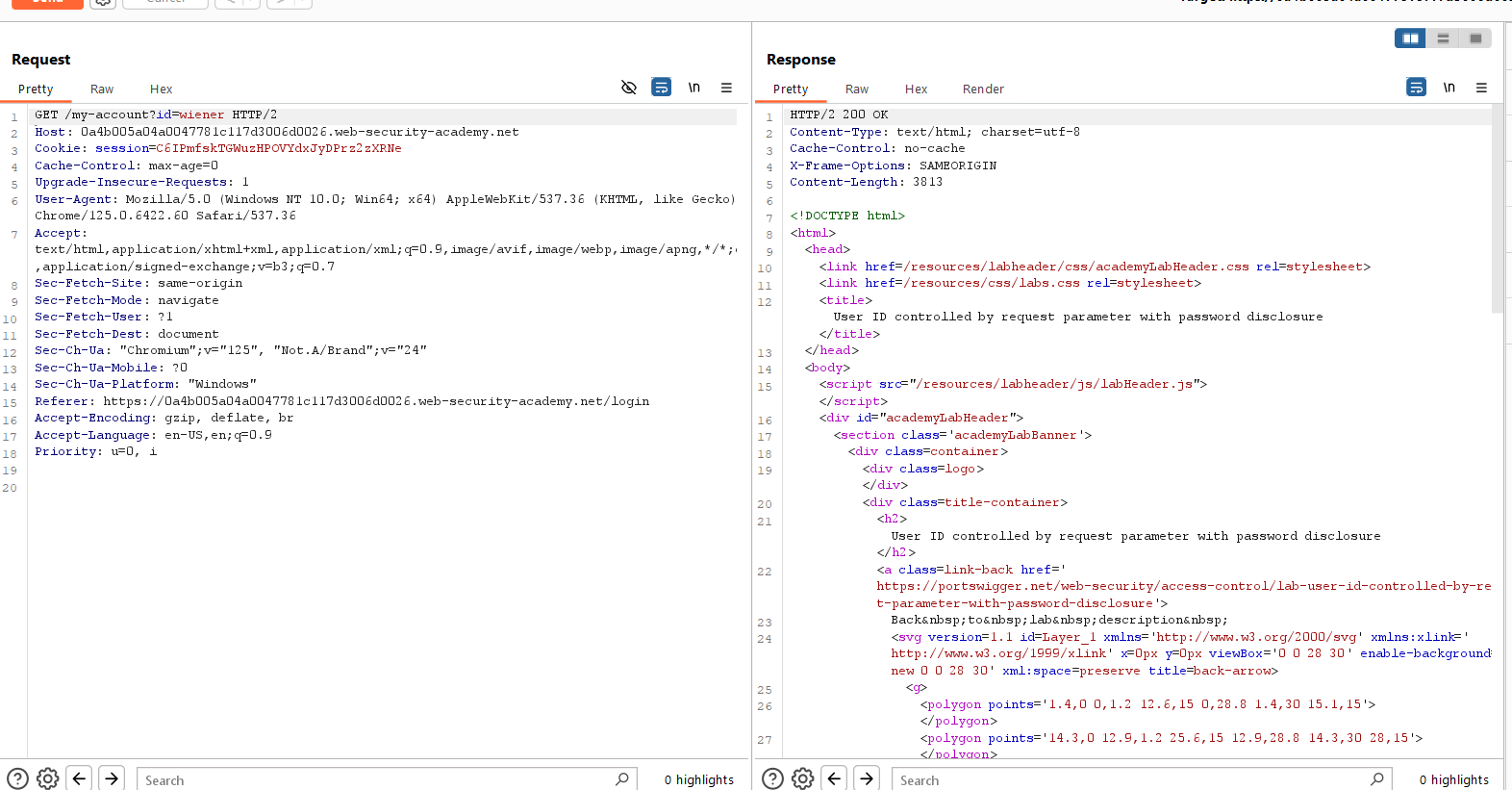
Đăng nhập bằng tài khoản wiener/peter



Hình 1. Đăng nhập thành công tài khoản wiener

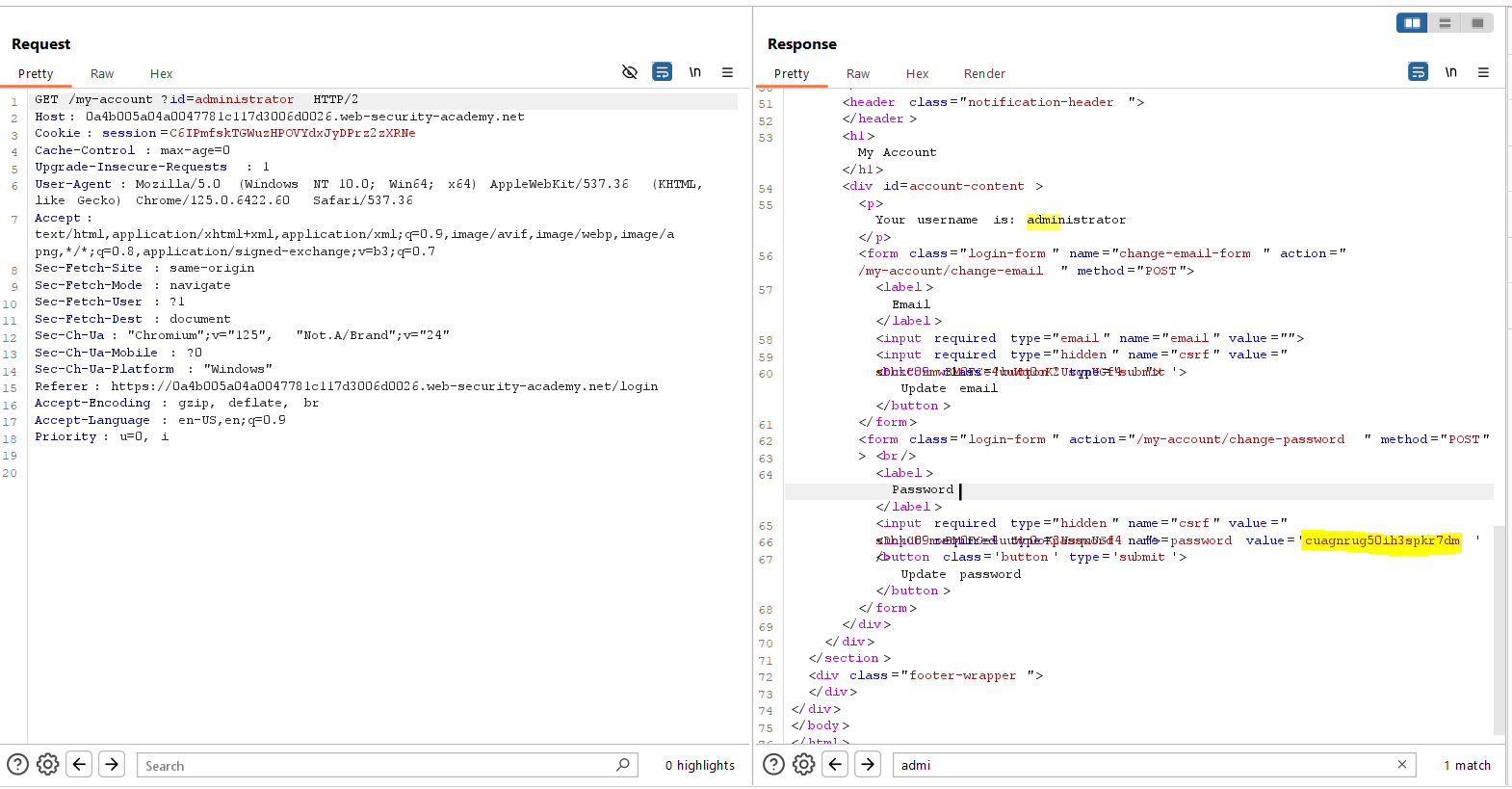


Hình 2. Request GET /myaccount?id=wiener



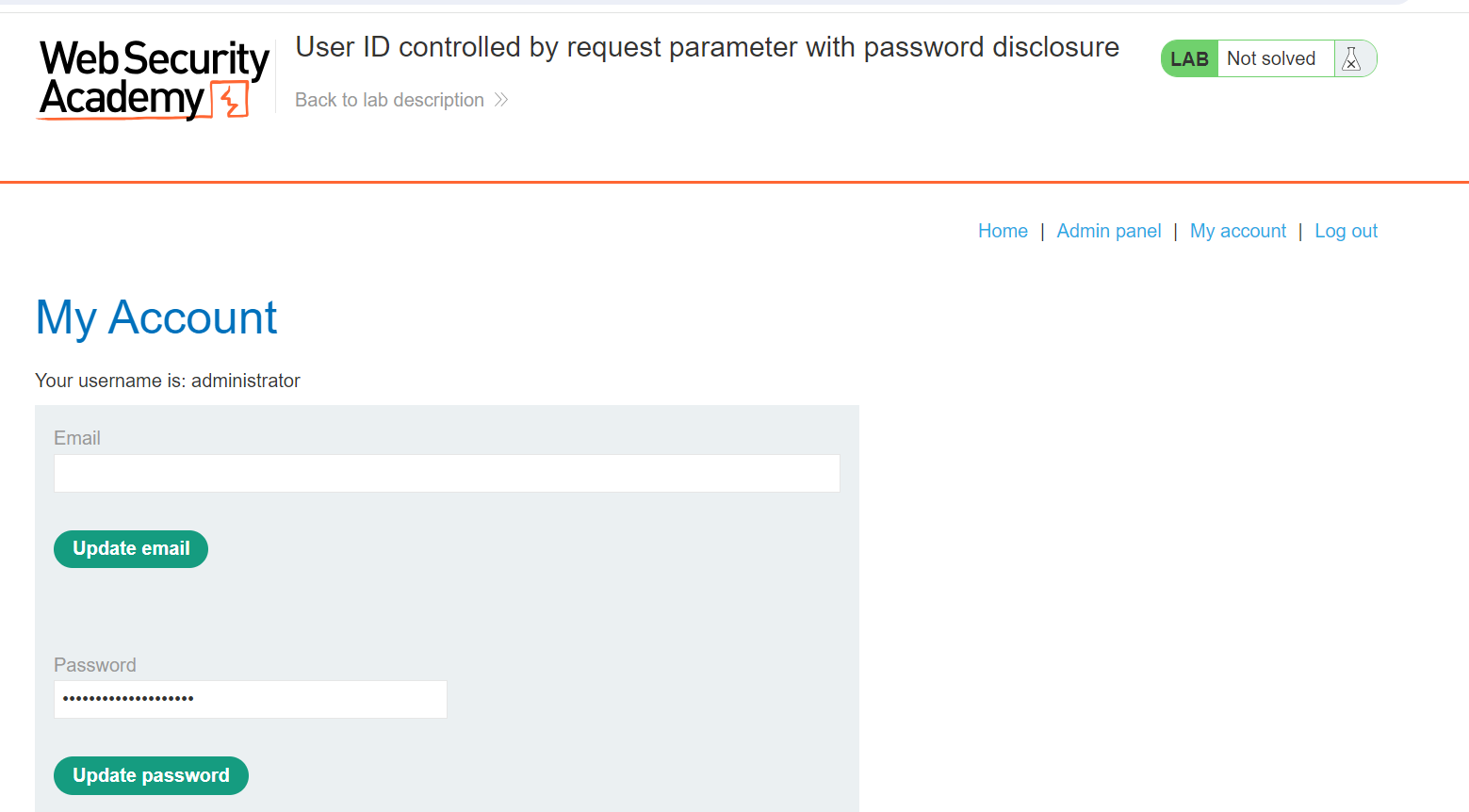
Hình 3. Gửi sang Reapeater để phân tích

Sửa id = administrator



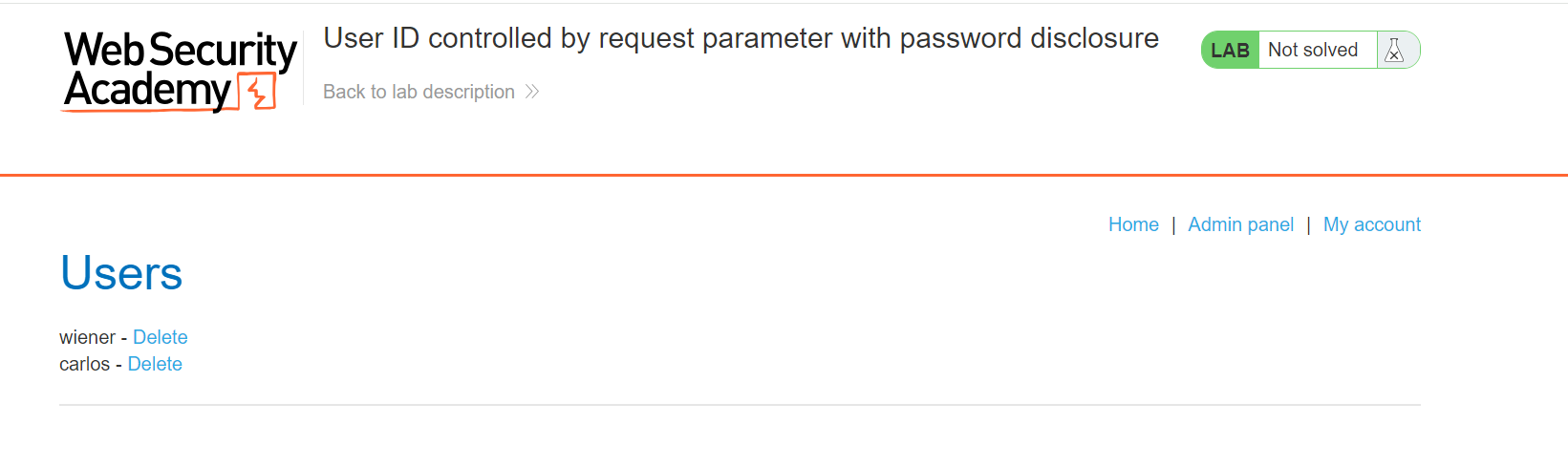
Hình 4. 1 respone 200 được trả về

Tìm ra được mật khẩu của admin



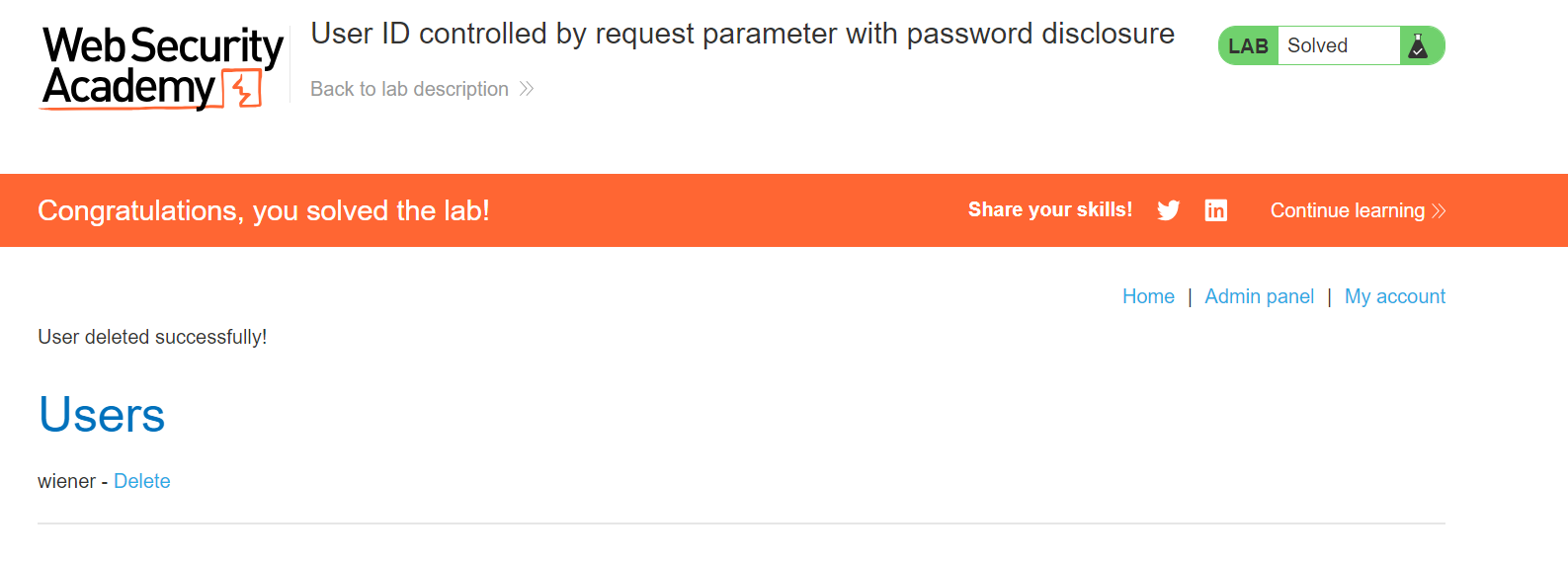
Hình 5. Login thành công admin

Truy cập vào admin panel



Hình 6. Trang admin panel

Delete tài khoản ‘carlos’



Hình 7. Xoá carlos và bài lab được hoàn thành