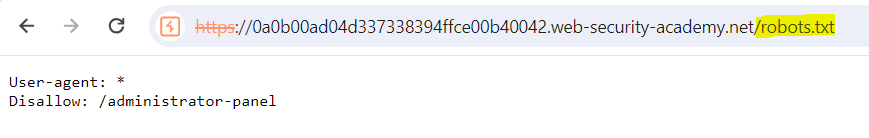
**Lab: User ID controlled by request parameter, with unpredictable user IDs**

Bài lab này có các chức năng quản trị không được bảo vệ đúng cách, cho phép kẻ tấn công có thể truy cập trực tiếp mà không cần xác thực hoặc kiểm tra quyền truy cập. Bằng cách truy cập vào các chức năng này, kẻ tấn công có thể thực hiện các hành động quản trị như xóa tài khoản người dùng.

Mục tiêu của bài lab này là khai thác lỗ hổng do thiếu cơ chế bảo vệ các chức năng quản trị để truy cập vào bảng điều khiển quản trị viên và xóa tài khoản của người dùng carlos. Để hoàn thành bài lab, bạn cần tìm và truy cập vào bảng điều khiển quản trị viên không được bảo vệ và sử dụng nó để xóa tài khoản của carlos.

Các bước thực hiện:

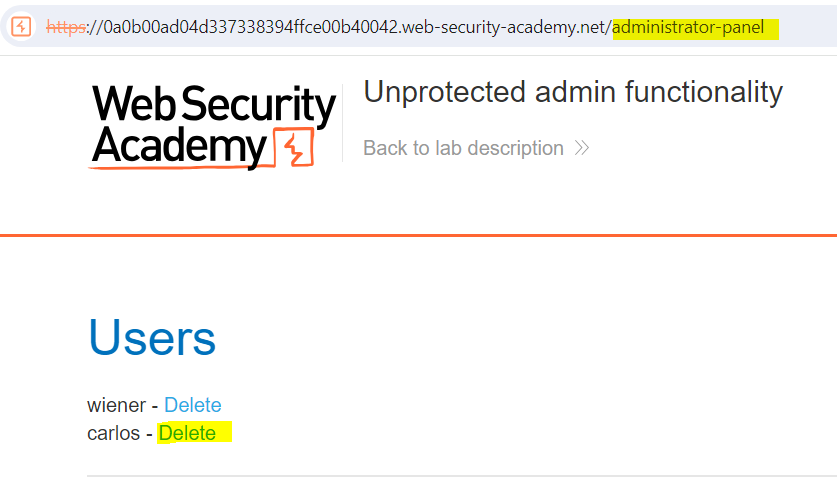
Xem “robots.txt” bằng cách thêm “/robots.txt” vào URL



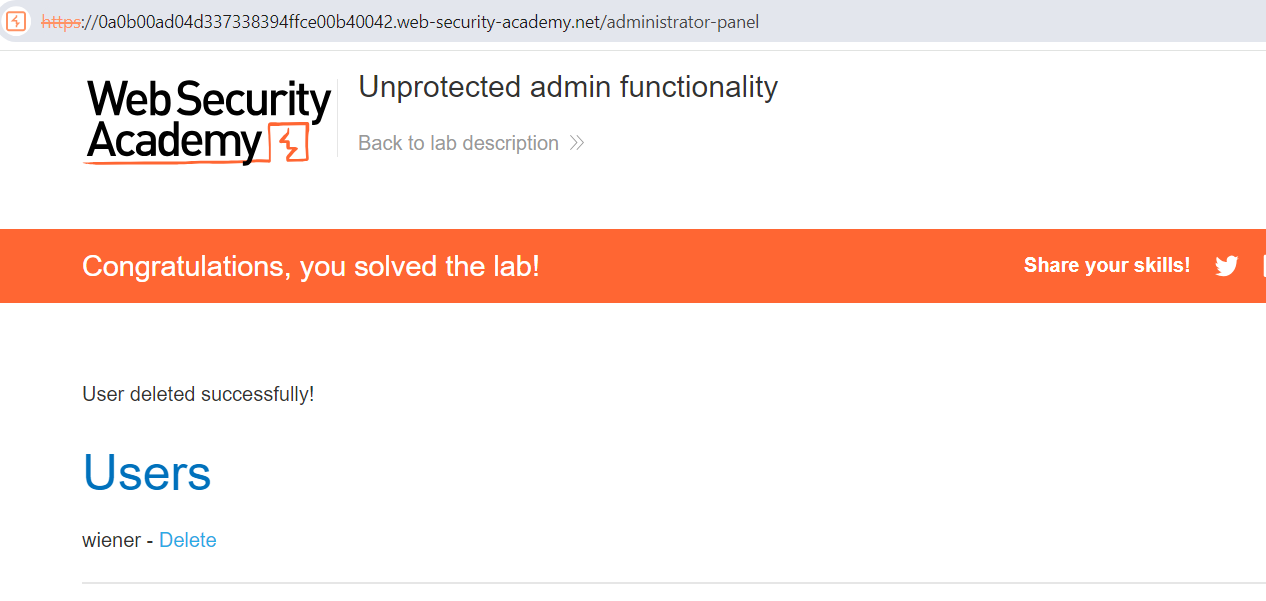
Hình 1. Đăng nhập thành công tài khoản wiener

“Disallow” tiết lộ đường dẫn đến bảng quản trị.

Truy cập vào bảng quản trị và thực hiện xoá carlos



Hình 2. Truy cập vào bảng quản trị



Hình 3. Bài lab được hoàn thành