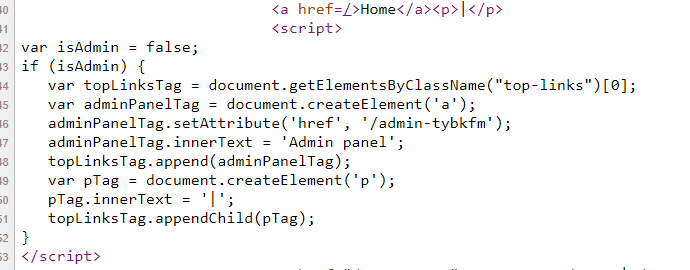
**Lab: Unprotected admin functionality with unpredictable URL**

Bài lab này có chức năng quản trị không được bảo vệ, nghĩa là không yêu cầu xác thực hoặc kiểm tra quyền truy cập. Tuy nhiên, URL của chức năng này là không thể đoán trước và phải được tìm ra thông qua tìm kiếm thông tin hoặc thử nghiệm.

Mục tiêu của bài lab này là tìm và truy cập URL không thể đoán trước của chức năng quản trị để xóa người dùng carlos.

Các bước thực hiện:

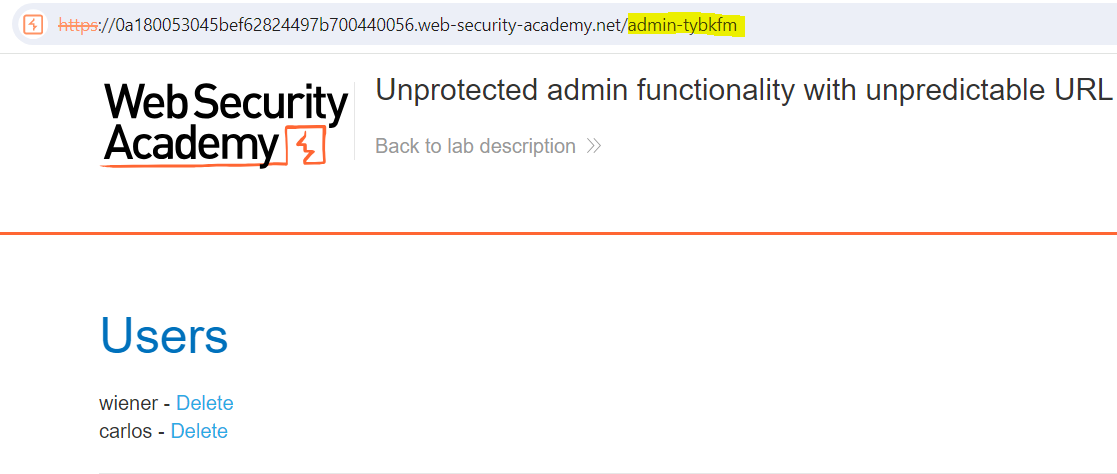
Xem mã nguồn để xem còn comment hay đoạn JS mà các dev để lại cho biết bảng quản trị ở đâu



Hình 1. Xem mã nguồn

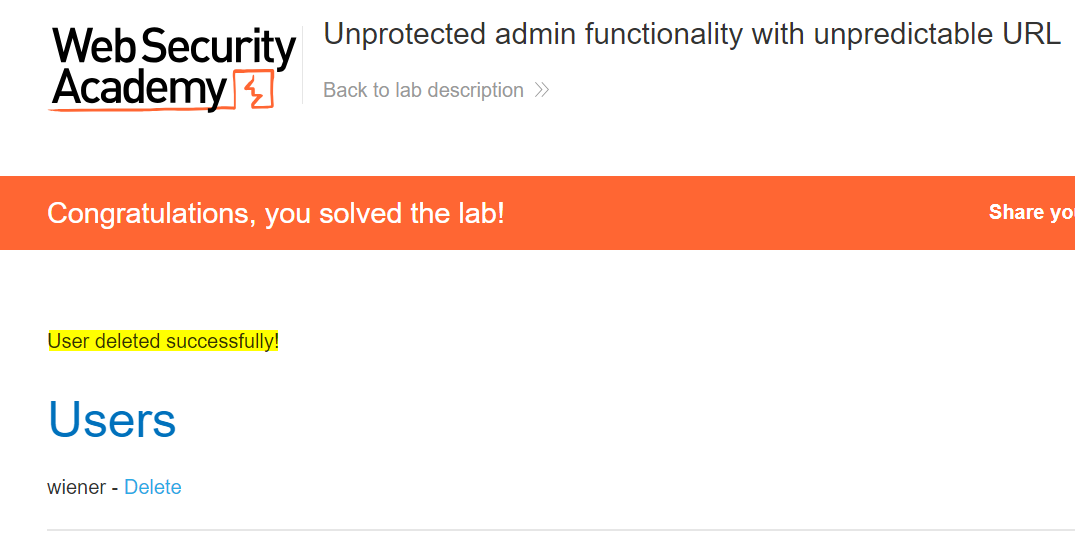
Nhận thấy đoạn mã JS có thư mục quản trị: /admin-tybkfm

Tìm kiếm thử thông qua URL



Hình 2. Truy cập được thư mục quản trị thông qua URL

Thực hiện xoá người dùng Carlos và bài lab được hoàn thành



Hình 3. Xoá ‘carlos’ thành công và hoàn thành bài lab