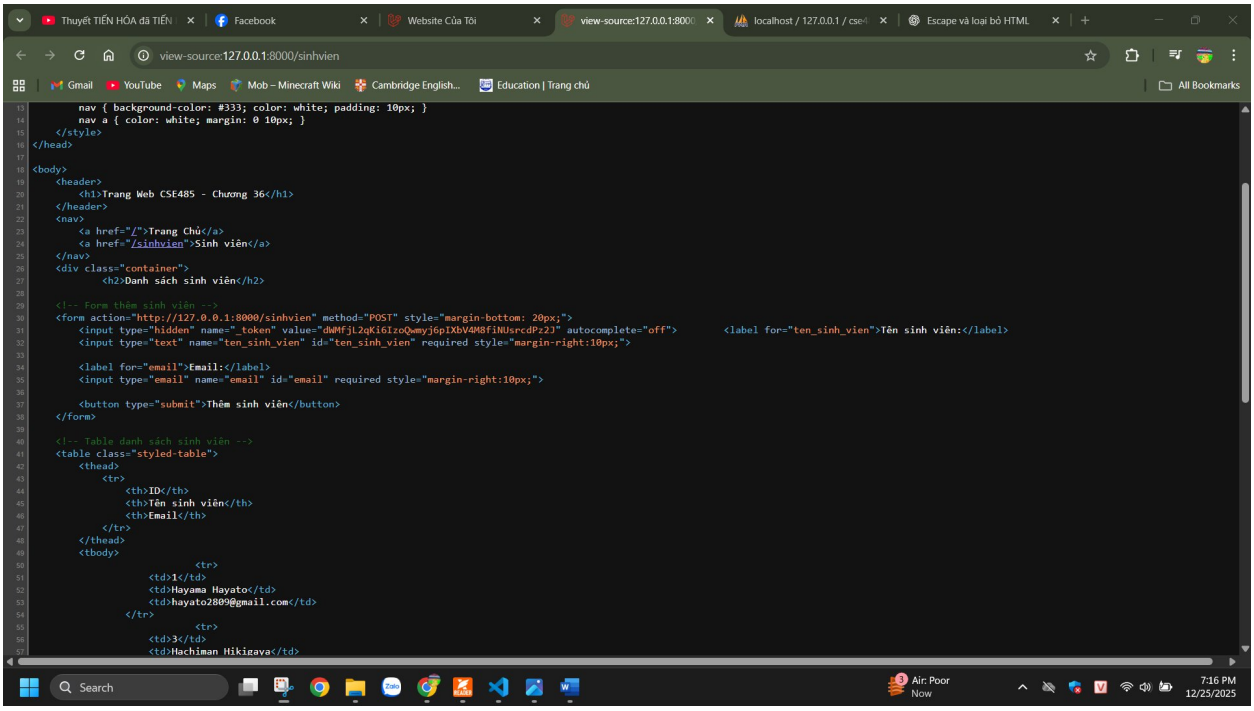
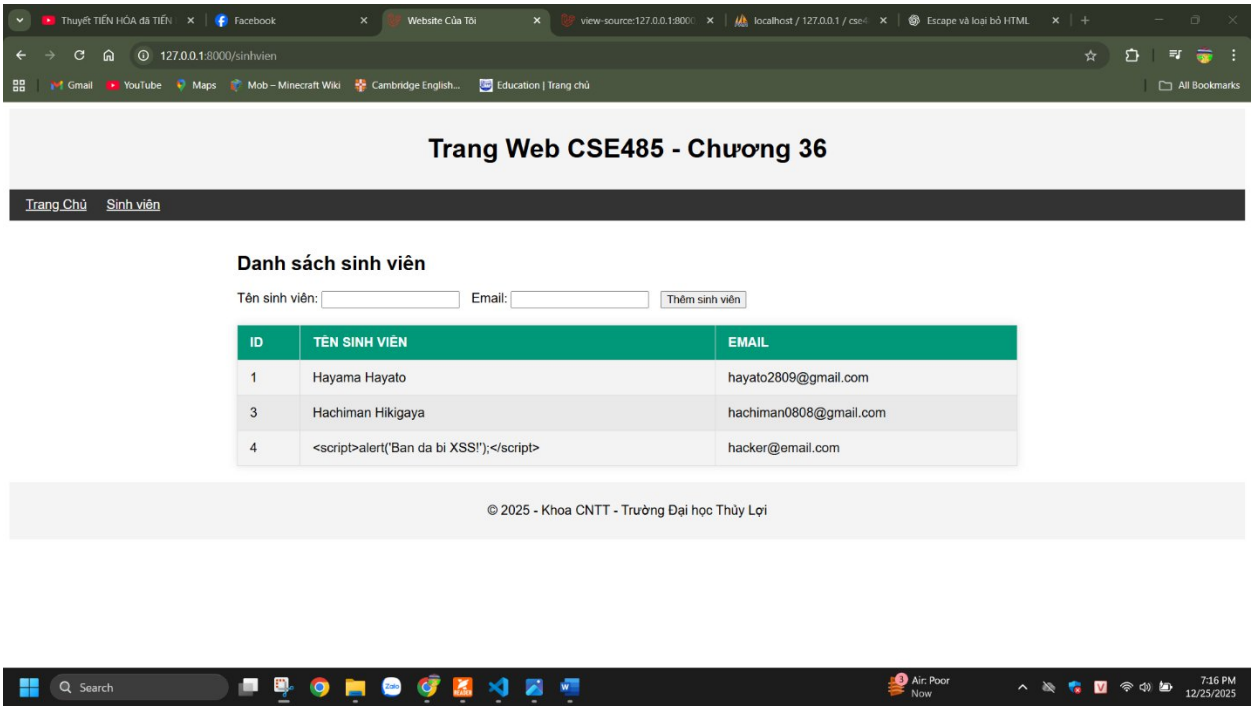
PHIẾU BÀI TẬP 9

Ảnh 1 (Bằng chứng Chống CSRF): Tải trang /sinhvien, **nhấn chuột phải $\rightarrow$**

View Page Source (Xem nguồn trang). Chụp ảnh màn hình mã nguồn HTML, **khoanh tròn** vào thẻ <input type="hidden" name="_token" ...> mà @csrf đã tự động tạo ra.



Ảnh 2 (Bằng chứng Chống XSS): Chụp ảnh màn hình trang /sinhvien **sau khi** bạn đã thêm sinh viên ở (TODO 6 & 7). Ảnh phải cho thấy dòng chữ <script>alert('Ban da bi XSS!');</script> được **in ra dưới dạng text** trên bảng, **chứ KHÔNG CÓ** popup "alert" nào hiện lên.



*Câu hỏi: Sự khác biệt cơ bản giữa **Xác thực (Authentication)** và **Phân quyền (Authorization)** là gì? 2 Trong Bài tập lớn, chức năng 'Đăng nhập' là Authentication hay Authorization? Chức năng 'Chỉ Admin mới thấy trang Quản trị' là gì?*

Câu trả lời: Authentication dùng để xác định người dùng là ai, còn Authorization dùng để xác định người dùng được phép làm gì trong hệ thống. Trong bài tập lớn, chức năng đăng nhập là xác thực, còn việc giới hạn quyền truy cập trang quản trị chỉ dành cho Admin là phân quyền.

Câu hỏi của tôi: Tại sao lại phải dùng @csrf để che đi cái loại của ô input? --> Do em nhìn nhầm thực ra nó là một đoạn mã khác thêm vào

Trả lời:

@csrf trong Laravel hoạt động bằng cách tự động chèn một thẻ input ẩn chứa CSRF token vào form HTML. Token này được dùng để xác minh request được gửi từ chính ứng

dụng, nhằm ngăn chặn tấn công CSRF. Việc sử dụng input hidden chỉ để gửi dữ liệu ngầm, không phải để che giấu hay bảo mật phía client.