## Bài tập chương 9

### A. Code đã hoàn thiện

1. Dán (paste) code của khối form trong tệp list.blade.php (chứng minh bạn đã thêm @csrf).

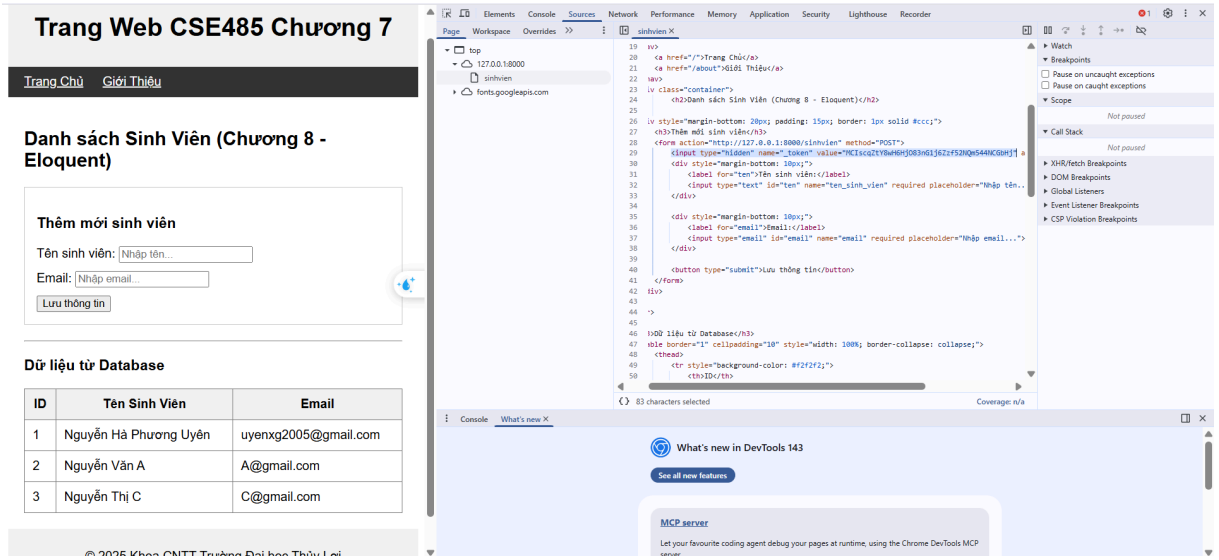
```
<form action="{{ route('sinhvien.store') }}" method="POST">
        @csrf

        <div style="margin-bottom: 10px;">
            <label for="ten">Tên sinh viên:</label>
            <input type="text" id="ten" name="ten_sinh_vien" required
placeholder="Nhập tên...">
        </div>

        <div style="margin-bottom: 10px;">
            <label for="email">Email:</label>
            <input type="email" id="email" name="email" required
placeholder="Nhập email...">
        </div>

        <button type="submit">Lưu thông tin</button>
    </form>
```

2. Dán (paste) code của khối @foreach trong tệp list.blade.php (chứng minh bạn dùng {{ }}).

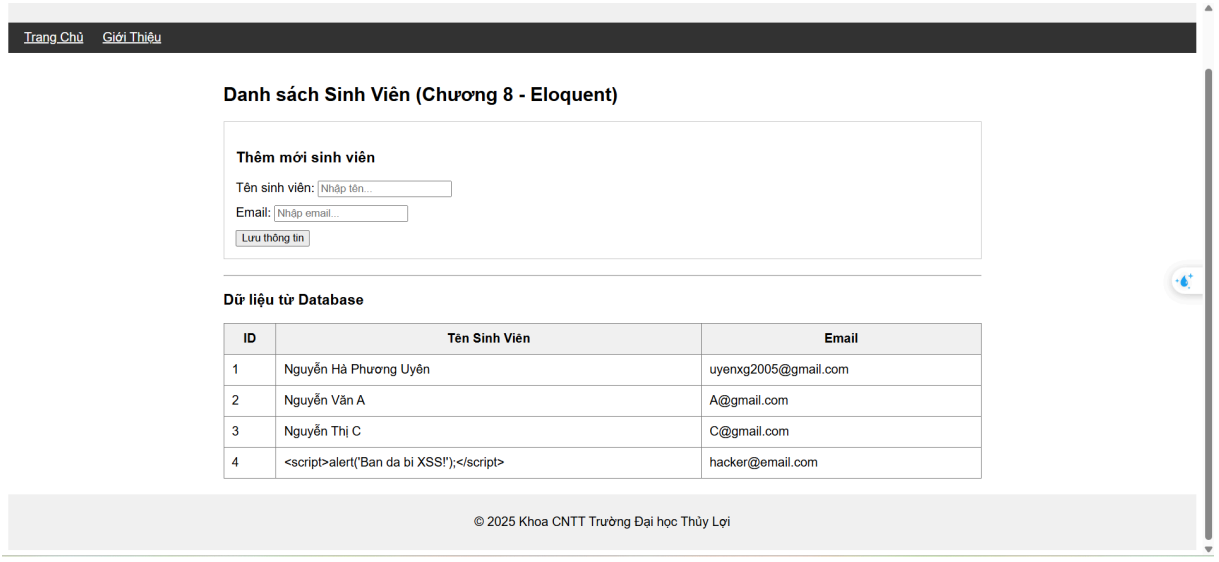
```
@foreach($danhSachSV as $sv)
        <tr>
            <td>{{ $sv->id }}</td>
            <td>{{ $sv->ten_sinh_vien }}</td>
            <td>{{ $sv->email }}</td>
        </tr>
 @endforeach
```

### B. Ảnh chụp màn hình Kết quả:

1. Ảnh 1 (Bằng chứng Chống CSRF): Tải trang /sinhvien, nhấn chuột phải vào View Page Source (Xem nguồn trang). Chụp ảnh màn hình mã nguồn HTML, khoanh tròn vào thẻ mà @csrf đã tự động tạo ra.




2. 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 được in ra dưới dạng text trên bảng, chứ KHÔNG CÓ popup "alert" nào hiện lên.




**Câu hỏi phản biện:**

Cú pháp {{ }} của Blade giúp chống XSS bằng cách chuyển đổi các ký tự đặc biệt thành thực thể HTML (escape). Tuy nhiên, nếu tôi muốn xây dựng một trang web cho phép người dùng viết bài có định dạng (như in đậm, in nghiêng - giống trình soạn thảo Word), tôi phải dùng {!! !!}. Lúc này làm sao để vừa hiển thị được HTML của người dùng vừa ngăn chặn được mã JavaScript độc hại?