

## A. Code đã hoàn thiện:

### 1. Dán (paste) code của khôi <form> trong tệp list.blade.php

```
<form action="{{ route('sinh-vien.store') }}" method="POST">
    @csrf
    <div>
        <label for="ten_sinh_vien">Ten sinh vien: </label>
        <input type="text"
            name="ten_sinh_vien"
            value="{{ old('ten_sinh_vien') }}" required>
    </div>
    <div>
        <label for="email">Email: </label>
        <input type="text"
            name="email"
            value="{{ old('email') }}" required>
    </div>
    <div>
        <button type="submit">Submit</button>
    </div>
    <div>
        <div class="student-list">
            @foreach($dsSinhvien as $sinhvien)
                <tr>
                    <td>{{ $sinhvien->id }}</td>
                    <td>{{ $sinhvien->ten_sinh_vien }}</td>
                    <td>{{ $sinhvien->email }}</td>
                    <br>
                </tr>
            @endforeach
        </div>
    </div>
</form>
```

### 2. Dán (paste) code của khôi @foreach trong tệp list.blade.php

```
@foreach($dsSinhvien as $sinhvien)
    <tr>
        <td>{{ $sinhvien->id }}</td>
        <td>{{ $sinhvien->ten_sinh_vien }}</td>
        <td>{{ $sinhvien->email }}</td>
        <br>
    </tr>
@endforeach
```

## B. Ảnh chụp màn hình Kết quả (BẮT BUỘC 2 ẢNH):

1. 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.

The screenshot shows a browser window with the URL `127.0.0.1:8000/sinhvien`. The page title is "Trang Web CSE485 - Chương 9". Below the title is a form with fields for "Ten sinh vien:" and "Email:", both containing placeholder text. A "Submit" button is present. To the right of the form, the browser's developer tools are open, specifically the "Elements" tab. The HTML source code is displayed, showing the structure of the page. A red box highlights a specific line of code: `<input type="hidden" name="_token" value="fweEskQoqYTBnMCnvkpaiemtkLcOjyGCVBn3" autocomplete="off">`. This line represents the automatically generated CSRF token.

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 `<script>alert('Ban da bi XSS!');</script>` được in ra dưới dạng text trên bảng, chứ KHÔNG CÓ popup "alert" nào hiện lên.

The screenshot shows a browser window with the URL `127.0.0.1:8000/sinhvien`. The page title is "Trang Web CSE485 - Chương 9". Below the title is a form with fields for "Ten sinh vien:" and "Email:", both containing placeholder text. A "Submit" button is present. To the right of the form, the browser's developer tools are open, specifically the "Elements" tab. The HTML source code is displayed, showing the structure of the page. A red box highlights a specific line of code: `<script>alert('Ban da bi XSS!');</script>`. This line represents the reflected XSS payload. The browser's main content area displays the text "1 tung tttt@gmail.com", "2 ninhbeo tung.2@hihihaha", "5 baobao gv@test.com", and "6 <script>alert('Ban da bi XSS!');</script> hacker@email.com". The last line contains the reflected script, which is intended to trigger an alert but does not actually do so because the browser is in developer mode.

## **Câu hỏi Phản biện**

**Câu hỏi của tôi là:** Vì csrf yêu cầu 1 token được sinh ra trong mỗi phiên làm việc, liệu có rủi ro mà hacker lấy được token từ session của người dùng từ đó qua mặt được hệ thống bảo vệ của Laravel không ?