

Bài tập chương 9

A. Code đã hoàn thiện

- Dán (paste) code của khôi 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>
```

- Dán (paste) code của khôi @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:

- 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.

The screenshot shows a web browser window with the title "Trang Web CSE485 Chương 7". Below the title, there's a navigation bar with "Trang Chủ" and "Giới Thiệu". The main content area has a heading "Danh sách Sinh Viên (Chương 8 - Eloquent)". Below it is a form titled "Thêm mới sinh viên" with fields for "Tên sinh viên" and "Email", and a "Lưu thông tin" button. To the right of the form is a table titled "Dữ liệu từ Database" with columns "ID", "Tên Sinh Viên", and "Email". The table contains three rows of data. At the bottom of the page is a copyright notice: "© 2025 Khoa CNTT Trường Đại học Thủy Lợi". On the right side of the browser, the Chrome DevTools developer console is open. The "Sources" tab is selected, showing the HTML source code of the page. Line 49 of the code contains an "alert" statement: "<script>alert('Ban da bi XSS!');</script>". This line is highlighted in red, indicating a syntax error or highlighting by the developer tools.

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.

This screenshot shows the same web browser window as the previous one, but after a student has been added. The database table now has four rows. The fourth row's 'Tên Sinh Viên' field contains the value "<script>alert('Ban da bi XSS!');</script>". The rest of the page, including the form and the rest of the table, appears normal. The copyright notice at the bottom is also present.

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?