

## PHIẾU HỌC TẬP CHỦ ĐÔNG (PHT)

Môn học: CSE485: Công nghệ Web

Phùng Minh Anh – 65KTPM – 2351170574

### CHƯƠNG 9: BẢO MẬT ỨNG DỤNG WEB

A. Code đã hoàn thiện:

- khối <form> trong tệp list.blade.php

```
<form action="{{ route('sinhvien.store') }}" method="POST">
    @csrf
    Tên sinh viên: <input type="text" name="ten_sinh_vien" required>
    Email: <input type="email" name="email" required>
    <button type="submit">Thêm</button>
</form>
```

- khối @foreach trong tệp list.blade.php

```
@foreach($danhSachSV as $sv)
    <tr>
        <td>{{ $sv->id }}</td>
        <td>{{ $sv->ten_sinh_vien }}</td>
        <td>{{ $sv->email }}</td>
        <td>{{ $sv->created_at->format('d/m/Y') }}</td>
    </tr>
@endforeach
```

B. Ảnh chụp màn hình Kết quả:

- Bằng chứng chống CSRF

```

39         <a href="/about">Giới thiệu</a>
40     </nav>
41     <div class="container">
42       <h2>DASHBOARD SINH VIÊN</h2>
43       <table>
44         <thead>
45           <th>id</th>
46           <th>Tên sinh viên</th>
47           <th>Email</th>
48           <th>Ngày tạo</th>
49         </thead>
50         <tbody>
51           <tr>
52             <td>1</td>
53             <td>John Doe</td>
54             <td>johndoe@gmail.com</td>
55             <td>08/12/2025</td>
56           </tr>
57           <tr>
58             <td>2</td>
59             <td>Nguyễn Văn A</td>
60             <td>nguyenvana@gmail.com</td>
61             <td>25/12/2025</td>
62           </tr>
63           <tr>
64             <td>3</td>
65             <td>&lt;script&gt;alert('Ban da bi XSS!');&lt;/script&gt;</td>
66             <td>hacker@email.com</td>
67             <td>25/12/2025</td>
68           </tr>
69         </tbody>
70       </table>
71     <h2>FORM SINH VIÊN</h2>
72     <form action="http://127.0.0.1:8000/sinhvien" method="POST">
73       <input type="hidden" name="token" value="0NtzyeXuivyySLxkujli5dElRtdme6Lk1Fs77UC" autocomplete="off">
74       Email: <input type="email" name="email" required>
75       <button type="submit">Thêm</button>
76     </form>
77   </div>
78   <footer><p>© 2025 - Khoa CNTT - Trường Đại học Thủy Lợi</p>
79 </footer>
80 </body>
81 </html>

```

Tên sinh viên: <input type="text" name="ten\_sinh\_vien">

## 2. Bằng chứng chống XSS

The screenshot shows the 'Dashboard Sinh Viên' page. At the top, there's a navigation bar with 'Trang Chủ' and 'Giới Thiệu'. Below it is the main content area:

- DASHBOARD SINH VIÊN**: A table listing three students with their details.
- FORM SINH VIÊN**: A form for adding new students. It has fields for 'Tên sinh viên' (Name) and 'Email', and a 'Thêm' (Add) button.
- Footer**: A copyright notice: '© 2025 - Khoa CNTT - Trường Đại học Thủy Lợi'.

In the 'FORM SINH VIÊN' section, the 'Tên sinh viên' field contains the value '<script>alert("Ban da bi XSS!");</script>'. This is highlighted in red in the original code snippet, indicating it was user input.

| ID | Tên sinh viên                             | Email                | Ngày tạo   |
|----|---|----------------------|------------|
| 1  | John Doe                                  | johndoe@gmail.com    | 08/12/2025 |
| 2  | Nguyễn Văn A                              | nguyenvana@gmail.com | 25/12/2025 |
| 3  | <script>alert('Ban da bi XSS!');</script> | hacker@email.com     | 25/12/2025 |

## C. Câu hỏi phản biện

Câu hỏi của tôi là: mỗi lần gửi form thì @csrf đều tạo một token mới hay nó sẽ chỉ dùng 1 token cho cả session?