

A. Code đã hoàn thiện

```
.chapter4.php
1  <?php
2  |     $host = "127.0.0.1";
3  |     $dbname = "cse485_web";
4  |     $username = "root";
5  |     $password = "";
6  |     $dsn = "mysql:host=$host;dbname=$dbname;charset=utf8mb4";
7  |     try
8  |     {
9  |         $pdo = new PDO(dsn: $dsn, username: $username, password: $password);
10 |         $pdo->setAttribute(attribute: PDO::ATTR_ERRMODE, value: PDO::ERRMODE_EXCEPTION);
11 |         echo "Connected";
12 |     }
13 |     catch (PDOException $e)
14 |     {
15 |         die("Connection failed: " . $e->getMessage());
16 |     }
17 |
18 |     if (isset($_POST["ten_sinh_vien"]) && isset($_POST["email"]))
19 |     {
20 |         $ten = $_POST["ten_sinh_vien"];
21 |         $email = $_POST["email"];
22 |         $sql = "INSERT INTO sinhvien (ten_sinh_vien, email) VALUES (?, ?)";
23 |         $stmt = $pdo->prepare(query: $sql);
24 |         $stmt->execute(params: [$ten, $email]);
25 |         // echo "Added " . $ten . " with email " . $email;
26 |         header(header: "Location: chapter4.php");
27 |         exit;
28 |     }
29 |     $sql_select = "SELECT * FROM sinhvien";
30 |     $stmt_select = $pdo->query(query: $sql_select);
31 | ?>
32 | <!DOCTYPE html>
33 | <html lang="vi">
34 |
35 | <head>
36 |     <meta charset="UTF-8">
37 |     <title>PHT Chương 4 - Website hướng dẫn liệu</title>
38 |     <style>
39 |         table {
40 |             width: 100%;
41 |             border-collapse: collapse;
42 |         }
43 |
44 |         th,
45 |         td {
46 |             border: 1px solid #ddd;
47 |             padding: 8px;
48 |         }

```

```
50  v |     th {
51  |     |     background-color: #f2f2f2;
52  |     }
53  |   </style>
54  | </head>
55
56 v <body>
57   <h2>Thêm Sinh Viên Mới (Chủ đề 4.3)</h2>
58 v   <form action="chapter4.php" method="POST">
59   |     Tên sinh viên: <input type="text" name="ten_sinh_vien" required>
60   |     Email: <input type="email" name="email" required><button type="submit">Thêm</button>
61   | </form>
62   <h2>Danh Sách Sinh Viên (Chủ đề 4.2)</h2>
63 v   <table>
64 v     <tr>
65   |       <th>ID</th>
66   |       <th>Tên Sinh Viên</th>
67   |       <th>Email</th>
68   |       <th>Ngày Tạo</th>
69   |     </tr>
70 v     <?php
71   |     // TODO 9: Dùng vòng lặp (ví dụ: while) để duyệt qua kết quả
72   |     // Gợi ý: while ($row = $stmt_select->fetch(PDO::FETCH_ASSOC)) { ... }
73 v     while ($row = $stmt_select->fetch(mode: PDO::FETCH_ASSOC))
74     {
75       echo "<tr>";
76       echo "<td>" . htmlspecialchars(string: $row['id']) . "</td>";
77       echo "<td>" . htmlspecialchars(string: $row['ten_sinh_vien']) . "</td>";
78       echo "<td>" . htmlspecialchars(string: $row['email']) . "</td>";
79       echo "<td>" . htmlspecialchars(string: $row['ngay_tao']) . "</td>";
80       echo "</tr>";
81     }
82 v     // TODO 10: In (echo) các dòng <tr> và <td> chứa dữ liệu $row
83     // Gợi ý: echo "<tr>";
84     // Gợi ý: echo "<td>" . htmlspecialchars($row['id']) . "</td>";
85     // (htmlspecialchars là để bảo mật, tránh lỗi XSS - sẽ học ở Chương 9)
86     // Đóng vòng lặp
87     ?>
88   </table>
89 </body>
90
91 </html>
```

B. Kết quả

The screenshot shows the phpMyAdmin interface for the 'cse485_web' database, specifically the 'sinhvien' table. The table contains 4 rows of data:

ID	Tên Sinh Viên	Email	Ngày Tạo
1	Nguyễn Văn A	abc@gmail.com	2025-11-30 17:16:03
2	a	ad@gmail.com	2025-11-30 17:16:09
3	a	ad@gmail.com	2025-11-30 17:16:26
4	a	abc@gmail.com	2025-11-30 17:16:43

Below the table, a browser window displays a form titled 'Thêm Sinh Viên Mới (Chủ đề 4.3)'. The form has fields for 'Tên sinh viên' (Name), 'Email', and a 'Thêm' (Add) button.

The browser's address bar shows the URL: `localhost/cse485/chapter4/chapter4.php`.

C. Câu hỏi phản biện

- Tại sao Prepared Statement với PDO lại có thể ngăn chặn hoàn toàn SQL Injection trong khi việc ghép chuỗi trực tiếp (string concatenation) lại cực kỳ nguy hiểm?