CHƯƠNG 4: WEBSITE HƯỚNG DỮ LIỆU

2. Nhiệm vụ Thực hành (BẮT BUỘC)

3. Yêu cầu Bằng chứng (Proof of Work)

Bạn phải nộp lại 2 bằng chứng sau:

A. **Code đã hoàn thiện:** Dán (paste) toàn bộ code của tệp chapter4.php mà bạn đã hoàn thiện.

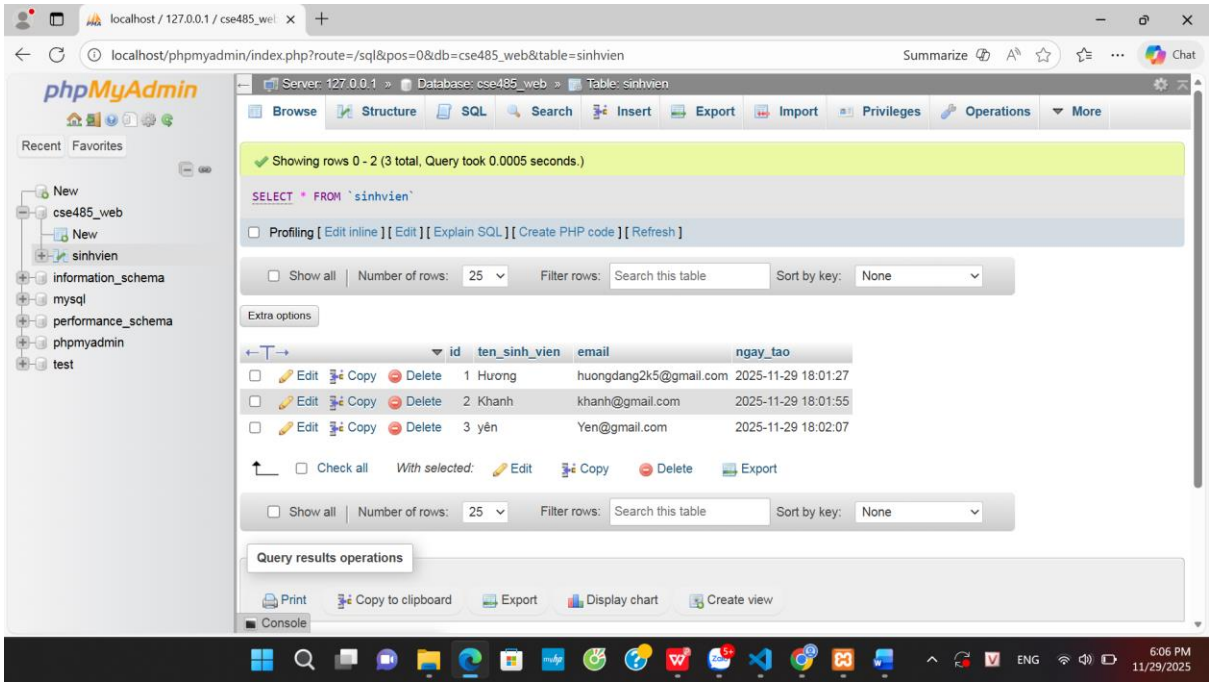
```
B. <?php
C. // === THIẾT LẬP KẾT NỐI PDO ===
D. $host = '127.0.0.1'; // hoặc localhost
E. $dbname = 'cse485_web'; // Tên CSDL bạn vừa tạo
F. $username = 'root'; // Username mặc định của XAMPP
G. $password = ''; // Password mặc định của XAMPP (rỗng)
H. $dsn = "mysql:host=$host;dbname=$dbname;charset=utf8mb4";
I. try {
J.  // TODO 1: Tạo đối tượng PDO để kết nối CSDL
K.  // Gợi ý: $pdo = new PDO(...);
L.  $pdo = new PDO($dsn, $username, $password);
M.  $pdo->setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION);
N.  // echo "Kết nối thành công!"; // (Bỏ comment để test)
O. } catch (PDOException $e) {
P.  die("Kết nối thất bại: " . $e->getMessage());
Q. }
R. // === LOGIC THÊM SINH VIÊN (XỬ LÝ FORM POST) ===
S. // TODO 2: Kiểm tra xem form đã được gửi đi (method POST) và có
   'ten_sinh_vien' không
T. // Gợi ý: Dùng isset($_POST['...'])
U. if ( isset($_POST['ten_sinh_vien']) && isset($_POST['email'])) {
V.
W.  // TODO 3: Lấy dữ liệu 'ten_sinh_vien' và 'email' từ $_POST
X.  $ten = $_POST['ten_sinh_vien'];
Y.  $email = $_POST['email'];
Z.  // TODO 4: Viết câu lệnh SQL INSERT với Prepared Statement (dùng dấu
   ?)
AA. $sql = "INSERT INTO sinhvien (ten_sinh_vien, email) VALUES (?, ?)";
BB.
CC. // TODO 5: Chuẩn bị (prepare) và thực thi (execute) câu lệnh
DD. // Gợi ý: $stmt = $pdo->prepare($sql);
EE. // Gợi ý: $stmt->execute([$ten, $email]);
FF. $stmt = $pdo->prepare($sql);
GG.$stmt->execute([$ten, $email]);
HH. // TODO 6: (Tùy chọn) Chuyển hướng về chính trang này để "làm mới"
II. // Gợi ý: Dùng header('Location: chapter4.php');
JJ. header("Location: chapter4.php");
KK. exit;
LL.}
```

```php
// === LOGIC LẤY DANH SÁCH SINH VIÊN (SELECT) ===
// TODO 7: Viết câu lệnh SQL SELECT *
$sql_select = "SELECT * FROM sinhvien ORDER BY ngay_tao DESC";
// TODO 8: Thực thi câu lệnh SELECT (không cần prepare vì không có tham số)
// Gợi ý: $stmt_select = $pdo->query($sql_select);
$stmt_select = $pdo->query($sql_select);
?>
<!DOCTYPE html>
<html lang="vi">
<head>
 <meta charset="UTF-8">
 <title>PHT Chương 4 - Website hướng dữ liệu</title>
 <style>
 table { width: 100%; border-collapse: collapse; }
        th, td { border: 1px solid #ddd; padding: 8px; }
        th { background-color: #f2f2f2; }
        </style>
      </head>
      <body>
        <h2>Thêm Sinh Viên Mới (Chủ đề 4.3)</h2>
        <form action="chapter4.php" method="POST">
        Tên sinh viên: <input type="text" name="ten_sinh_vien" required>
        Email: <input type="email" name="email" required>
        <button type="submit">Thêm</button>
        </form>
        <h2>Danh Sách Sinh Viên (Chủ đề 4.2)</h2>
        <table>
        <tr>
        <th>ID</th>
        <th>Tên Sinh Viên</th>
        <th>Email</th>
        <th>Ngày Tạo</th>
        </tr>
        <?php
        // TODO 9: Dùng vòng lặp (ví dụ: while) để duyệt qua kết quả $stmt_select
        // Gợi ý: while ($row = $stmt_select->fetch(PDO::FETCH_ASSOC)) { ... }
        while ($row = $stmt_select->fetch(PDO::FETCH_ASSOC)){
            // TODO 10: In (echo) các dòng <tr> và <td> chứa dữ liệu $row
            // Gợi ý: echo "<tr>";
            // Gợi ý: echo "<td>" . htmlspecialchars($row['id']) . "</td>";
            // (htmlspecialchars là để bảo mật, tránh lỗi XSS - sẽ học ở Chương 9)
            echo "<tr>";
            echo "<td>". htmlspecialchars($row['id']) . "</td>";
```

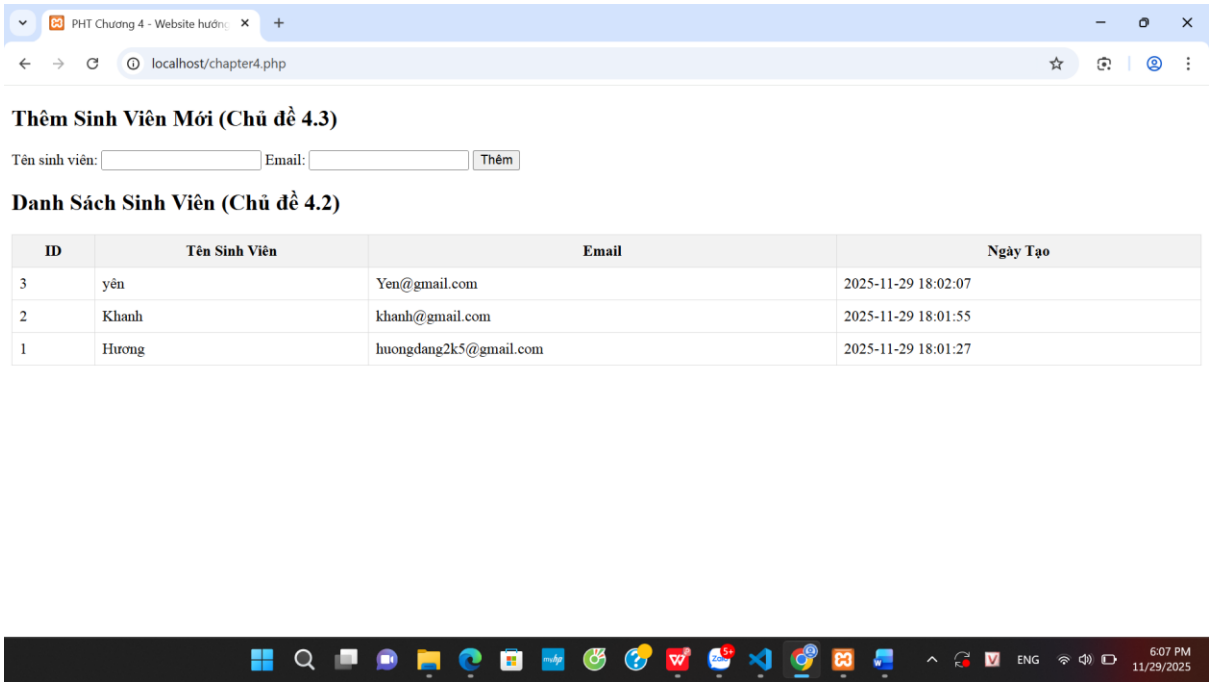
```
DDDD.         echo "<td>". htmlspecialchars($row['ten_sinh_vien']) .
   "</td>";
EEEE.         echo "<td>". htmlspecialchars($row['email']) . "</td>";
FFFF.         echo "<td>". htmlspecialchars($row['ngay_tao']) . "</td>";
GGGG.         echo "</tr>";
HHHH.      }
IIII.      // Đóng vòng lặp
JJJJ.      ?>
KKKK.      </table>
LLLL.     </body>
MMMM.     </html>
```

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

1. **Ảnh 1 (phpMyAdmin):** Chụp màn hình tab "Browse" (Duyệt) của bảng sinhvien trong phpMyAdmin, cho thấy bạn đã INSERT thành công ít nhất 2-3 sinh viên.



2. Ảnh 2 (Trình duyệt Web): Chụp ảnh màn hình trang chapter4.php của bạn, hiển thị đúng 2-3 sinh viên mà bạn vừa thêm (chứng minh SELECT thành công).



4. Câu hỏi Phản biện (Bắt buộc)

Câu hỏi của tôi là: Khi người dùng gửi dữ liệu qua form HTML, tại sao chúng ta nên dùng hàm htmlspecialchars() khi hiển thị lại dữ liệu lên trình duyệt? Hãy giải thích nếu không dùng hàm này thì trang web có thể gặp rủi ro bảo mật gì..