

CHƯƠNG 4: WEBSITE HƯỚNG DẪN LIFO

1. Lý thuyết Cốt lõi (Khái niệm)

Để PHP "nói chuyện" với MySQL (hoặc bất kỳ CSDL nào), chúng ta sử dụng một giao diện (interface) chuẩn gọi là **PDO (PHP Data Objects)**.

Luồng làm việc với PDO luôn gồm các bước:

1. **Kết nối (Connect):** Tạo một đối tượng PDO mới, cung cấp cho nó "chuỗi kết nối" (DSN), username và password của CSDL.
2. **Chuẩn bị (Prepare):** Viết câu lệnh SQL (như SELECT * FROM users WHERE id = ?). Dấu ? là một **placeholder** (trình giữ chỗ).
3. **Thực thi (Execute):** "Bind" (gắn) giá trị thật (ví dụ: \$id = 5) vào placeholder ? và thực thi câu lệnh.
4. **Lấy kết quả (Fetch):** Nếu là câu SELECT, dùng fetch() (lấy 1 dòng) hoặc fetchAll() (lấy tất cả) để nhận dữ liệu.

Tại sao dùng "Prepared Statements" (dấu ?)? Đây là cách **bắt buộc** để chống lại một kiểu tấn công cực kỳ phổ biến tên là **SQL Injection**. Tuyệt đối **không bao giờ** viết code bằng cách cộng chuỗi trực tiếp như: \$sql = "SELECT * FROM users WHERE username = '" . \$_POST['user'] . "'"; (CỰC KỲ NGUY HIỂM!)

2. Nhiệm vụ Thực hành (BẮT BUỘC)

Kịch bản: Xây dựng một trang "Danh sách sinh viên" đơn giản. Trang này cho phép bạn:

1. Thêm sinh viên mới vào CSDL (Dùng INSERT).
2. Hiển thị toàn bộ sinh viên đang có trong CSDL (Dùng SELECT).

A. Thiết lập Ban đầu (Bắt buộc)

1. Mở **phpMyAdmin**.
 2. Tạo một CSDL mới tên là **cse485_web**.
 3. Chọn CSDL **cse485_web**, mở tab **SQL** và chạy lệnh sau để tạo bảng: SQL
-

B. Code Khởi đầu (Starter Code):

Tạo 1 tệp chapter4.php trong thư mục htdocs của XAMPP:

PHP

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

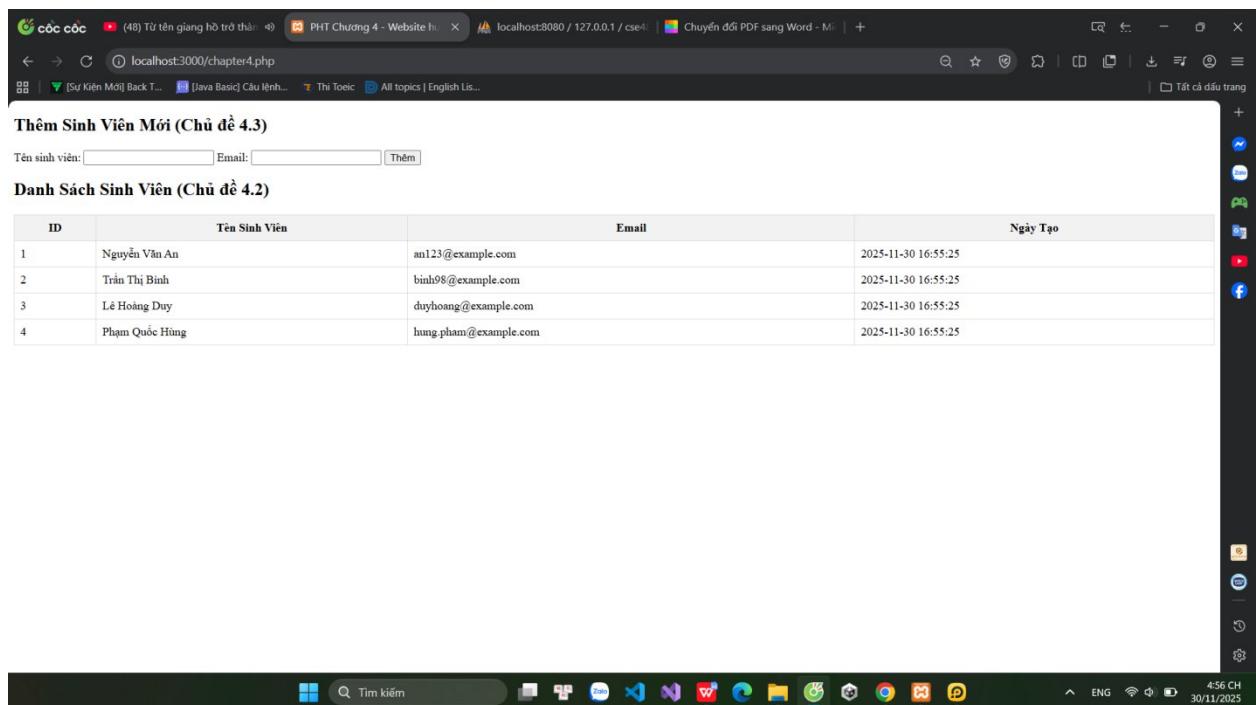
1. **Ảnh 1 (phpMyAdmin):** Chụp màn hình tab "Browse" (Duyệt) của bảng **sinhvien** trong

phpMyAdmin, cho thấy bạn đã INSERT thành công ít nhất 2-3 sinh viên.

The screenshot shows the phpMyAdmin interface on a Windows desktop. The browser tab is 'localhost:8080/phpmyadmin/index.php?route=/sql&pos=0&db=cse485_web&table=sinhvien'. The left sidebar lists databases: Mới dùng, Mới, bai_tap_on_tap_sql, cse485_web, Mới, sinhvien, information_schema, mysql, performance_schema, phpmyadmin, question, test, thi, web1. The main area shows a table named 'sinhvien' with columns: id, ten_sinh_vien, email, ngay_bao. A successful query execution message is displayed: 'Hiển thị các hàng 0 - 3 (tổng 4, Truy vấn cần 0,0007 giây.)' followed by the SQL code: 'SELECT * FROM `sinhvien`' and 'UPDATE `sinhvien` SET `id` = '4' WHERE `sinhvien`.`id` = '13';'. Below the table, there are four rows of data with edit and delete icons. At the bottom, there are buttons for 'In', 'Chép vào clipboard', 'Xuất', 'Hiển thị biểu đồ', and 'Tạo view'. A note says 'Dành dấu truy vấn SQL này'.

	ID	Tên Sinh Viên	Email	Ngày Báo
<input type="checkbox"/> Sửa	1	Nguyễn Văn An	an123@example.com	2025-11-30 16:55:25
<input type="checkbox"/> Sửa	2	Trần Thị Bình	bint98@example.com	2025-11-30 16:55:25
<input type="checkbox"/> Sửa	3	Lê Hoàng Duy	duyhoang@example.com	2025-11-30 16:55:25
<input type="checkbox"/> Sửa	4	Phạm Quốc Hùng	hung.pham@example.com	2025-11-30 16:55:25

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).



(Dán Code A và Ảnh B1, B2 của bạn vào đây)

4. Câu hỏi Phản biện (Bắt buộc)

Sau khi hoàn thành Phần 2 & 3, hãy đặt 01 câu hỏi tư duy.

(Gợi ý: "Hãy giải thích SQL Injection là gì? Tại sao việc cộng chuỗi INSERT INTO sinhvien (ten) VALUES (':ten') lại nguy hiểm, và tại sao cách dùng execute(:ten) (Prepared Statement) lại an toàn hơn?").

Câu hỏi của tôi là: Tại sao phải dùng htmlspecialchars() khi hiển thị dữ liệu sinh viên ra bảng HTML?

5. Kết nối Đánh giá (Rất quan trọng)

Kỹ năng kết nối CSDL bằng **PDO** (bao gồm INSERT và SELECT) là kỹ năng quan trọng nhất trong khối kiến thức PHP thuần.

Bạn sẽ vận dụng trực tiếp PHT này để hoàn thành **Bài tập trên lớp (Phần PHP)**, chiếm 20% tổng điểm, dự kiến vào **Tuần 5**. Nắm vững PDO bây giờ cũng sẽ giúp bạn hiểu tại sao **Eloquent ORM** (Chương 8) lại mạnh mẽ và tiện lợi đến vậy.