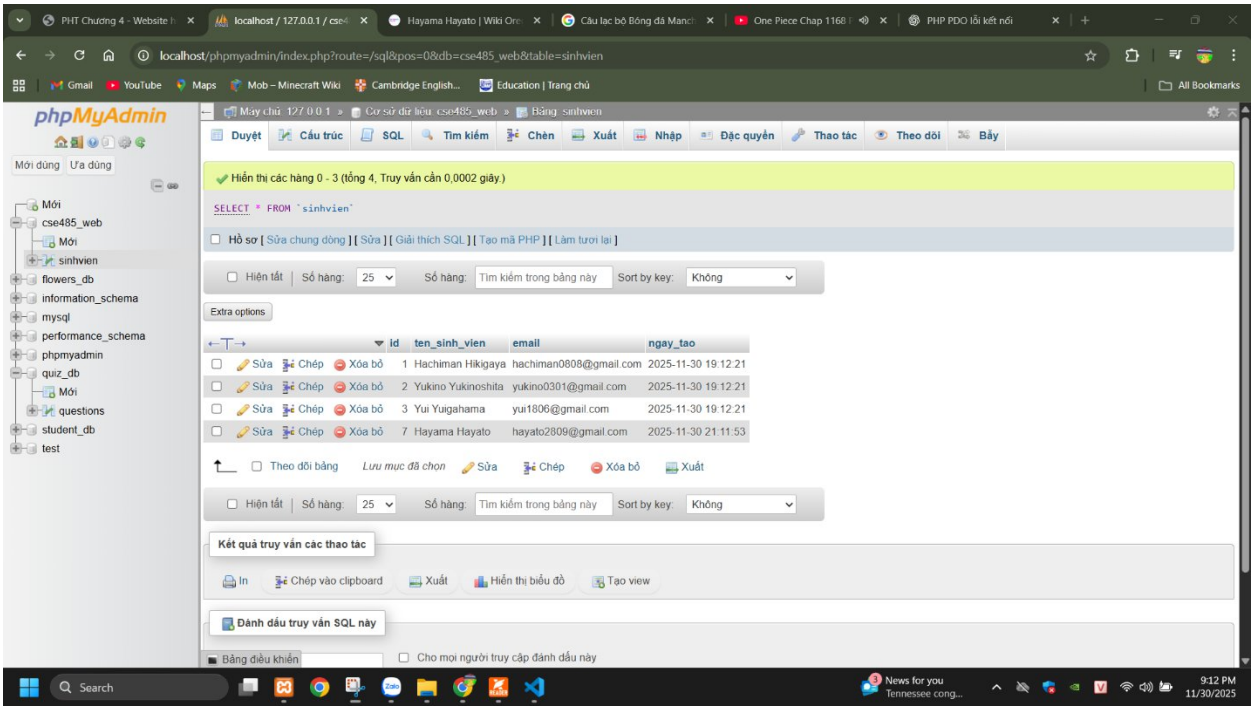
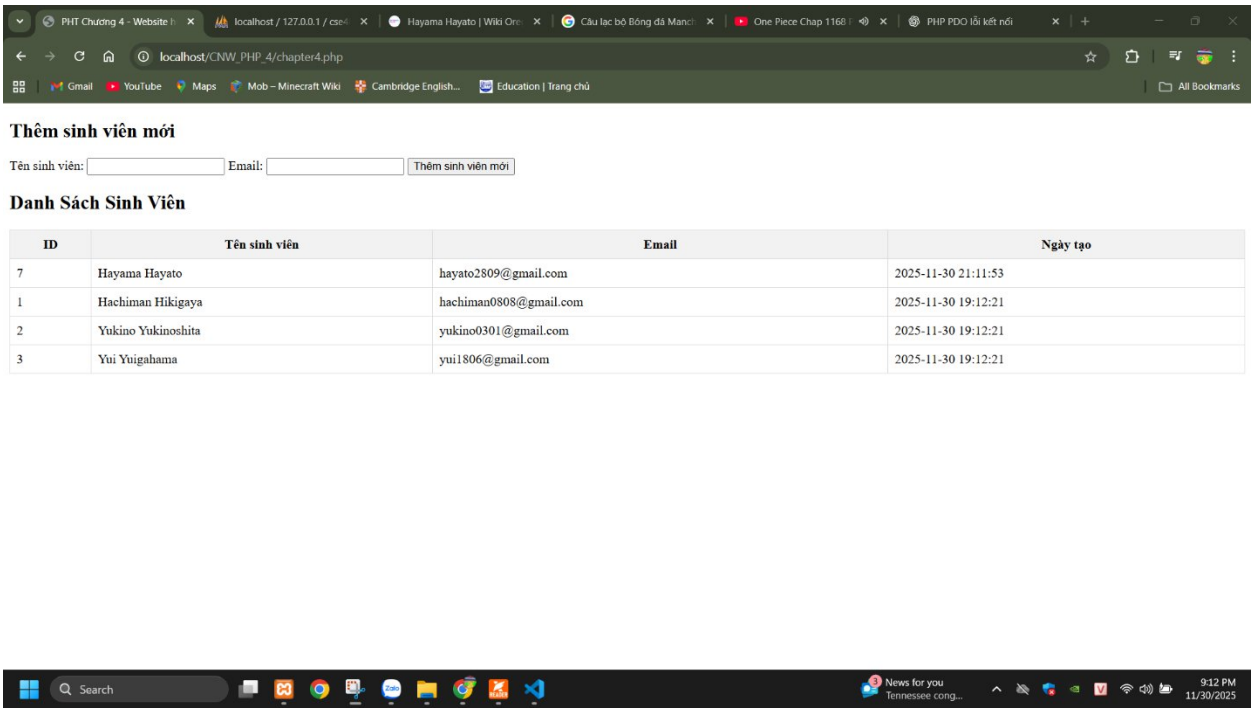
1. Ảnh chụp màn hình kết quả:

1. ẢNH 1 (ảnh tab bảng sinh viên trong phpADMIN)



2. ẢNH 2 (Trình duyệt web)



2. Câu hỏi phản biện (Sinh viên hỏi và thử tìm câu trả lời)

Câu hỏi đến từ câu hỏi 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?

Trả lời:

- Kết nối SQL là một trong các vấn đề đã được dạy ở các môn học sử dụng C# và Java tại trường mình. Trong các môn học thì với tư cách một sinh viên thì em nhận thấy C# và Java cũng có các cấu trúc tương tự:

Ví dụ: C#

```
SqlCommand cmd = new SqlCommand( "INSERT INTO SV (Ten, Email) VALUES (@ten, @email)", conn);

cmd.Parameters.AddWithValue("@ten", ten);

cmd.Parameters.AddWithValue("@email", email);
```

Ví dụ: Java

```
String sql = "INSERT INTO sinhvien (ten, email) VALUES (?, ?)";

PreparedStatement ps = conn.prepareStatement(sql);

ps.setString(1, ten);

ps.setString(2, email);
```

- Nhận xét của ban đầu em khi thấy những cấu trúc này là để ngắn gọn các chuỗi truy vấn có nhiều tham số do sự nhập nhằng trong viết tham số của SQL. Nhưng với câu truy vấn của PHP lại khác, rất gọn. Vậy câu hỏi là vấn đề thực sự cho cách sử dụng của prepareStatement, để tránh bị SQL Injection.

- Những tìm hiểu về SQL Injection ban đầu: Là phương pháp chèn chuỗi SQL để thực hiện truy vấn bất hợp pháp gây phá hoại, chèn thông tin lạ vào cơ sở dữ liệu.

Câu hỏi a: Vậy Hacker thực hiện như thế nào? Tôi thấy rõ ràng là sau tên biến còn các dấu ngoặc đóng nếu thêm vào thì nó sẽ gây lỗi?

- Ví dụ:

```
$sql = "INSERT INTO sinhvien (ten) VALUES ('$ten')";
```

Giả sử nếu $ten được nhập qua 1 input có đầu vào: hacker'); DROP TABLE sinhvien; --
Nó có thể xóa sổ toàn bộ bảng cơ sở dữ liệu đang tương tác. Hacker chỉ cần nhập ký tự để tạm hoàn thành chuỗi truy vấn hiện có, thực hiện một chuỗi sql ngoài ý muốn và comment lại phần bị đứt gãy là đủ để hoàn thành hành vi xấu.

Câu hỏi b: Vậy Prepare Statement đã được thực hiện như thế nào?

- Đơn giản hóa thì là chia thành 2 bước, thực hiện câu lệnh sql trên server trước và sau đó đưa dữ liệu lên sau.

- Và phương pháp kết nối và thực hiện câu lệnh như vậy chính là phương pháp PDO giống như C# vớiSqlCommand + AddWithValue hay Java với PreparedStatement