Bài tập thực hành 04

**MSSV: B2203465**

**Họ và tên sinh viên: Nguyễn Thị Ngọc Quyển**

Lập trình PHP nâng cao

**Mục tiêu cần đạt**:

Sau buổi các bạn cần nắm thao tác sử dụng PHP nâng cao

* Hiểu và biết cách dùng Cookies và Session
* Tạo form đăng nhập và dùng cookies, session để quản lý các đăng nhập, thực hiện chức năng log out (thoát) khỏi hệ thống
* Biết về SQL Injection.
* Upload file, lưu thông tin về tập tin trong CSDL
* Đọc, và xử lý nội dung trong tập tin

Các bạn đọc và thực hiện viết code như hướng dẫn để làm quen, sau đó đọc trả lời các **Yêu cầu** ở dưới bài hướng dẫn để thực hiện yêu cầu bài thực hành.

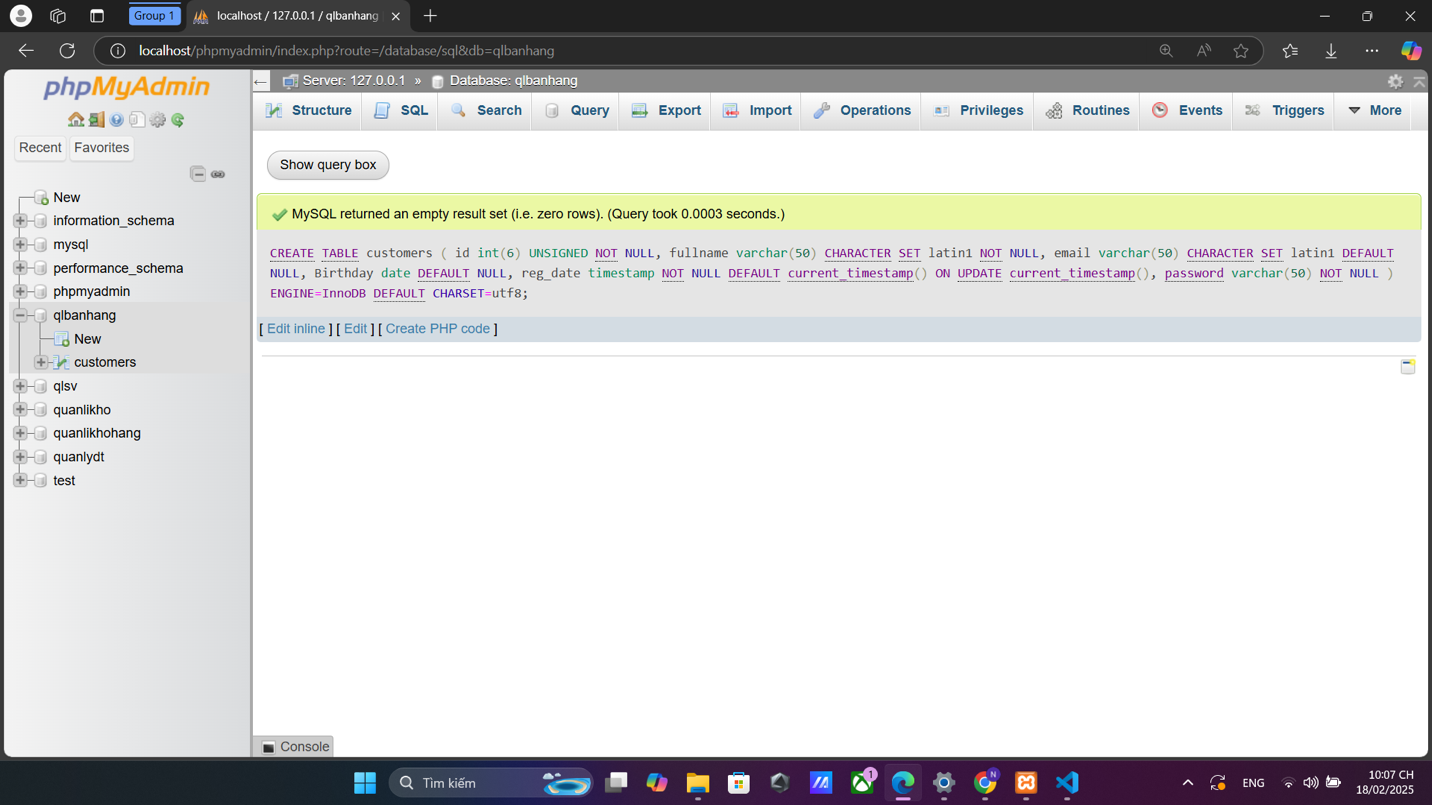
**Gợi ý Tham khảo:**

* <https://www.w3schools.com/php/>
* và các nguồn khác mà sinh viên tìm được

# Yêu cầu bài thực hành:

1. Bạn hãy chạy tất cả các lệnh hướng dẫn ở trên và chụp lại màn hình kết quả.

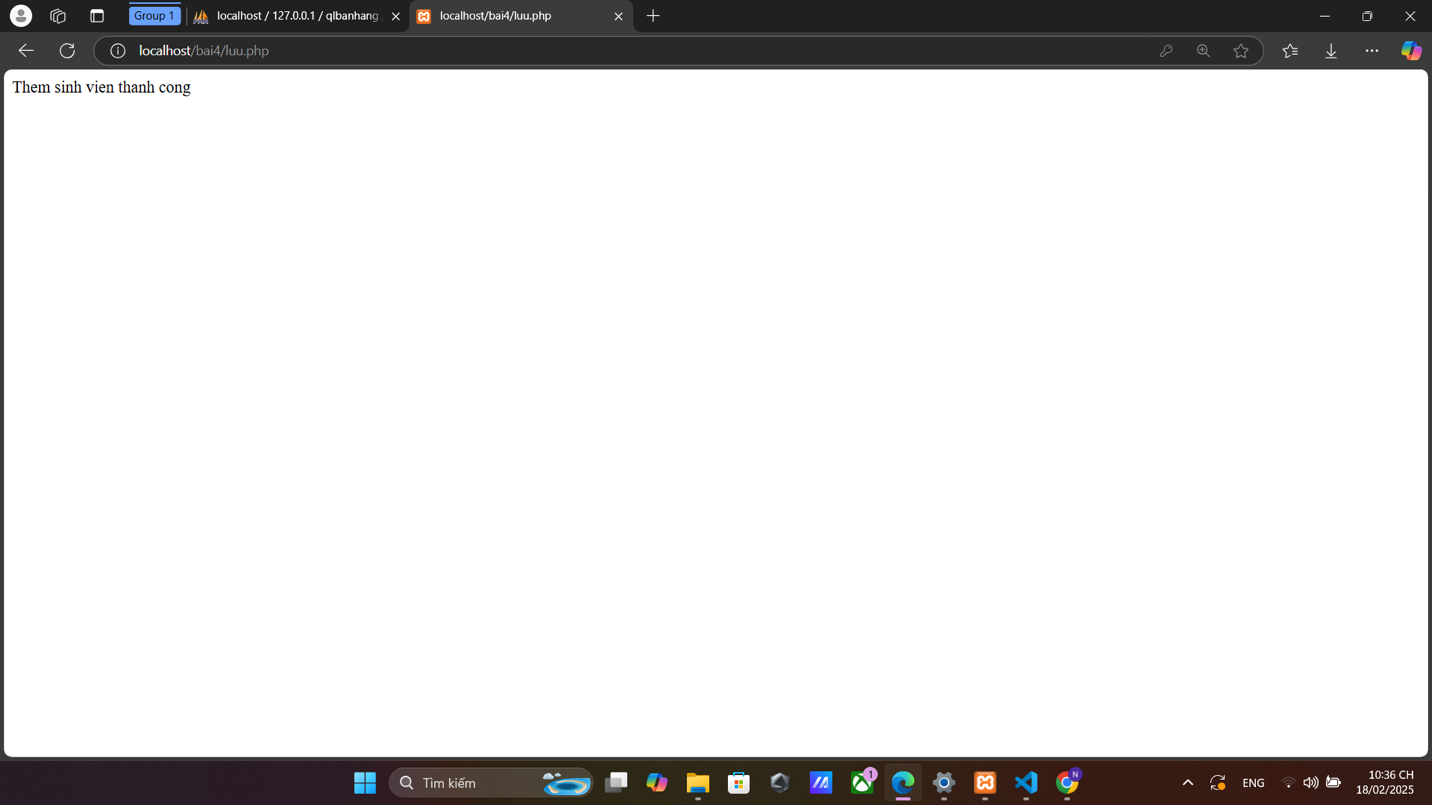
-Tạo bảng customer:



-Thêm sinh viên mới:

A screenshot of a computer

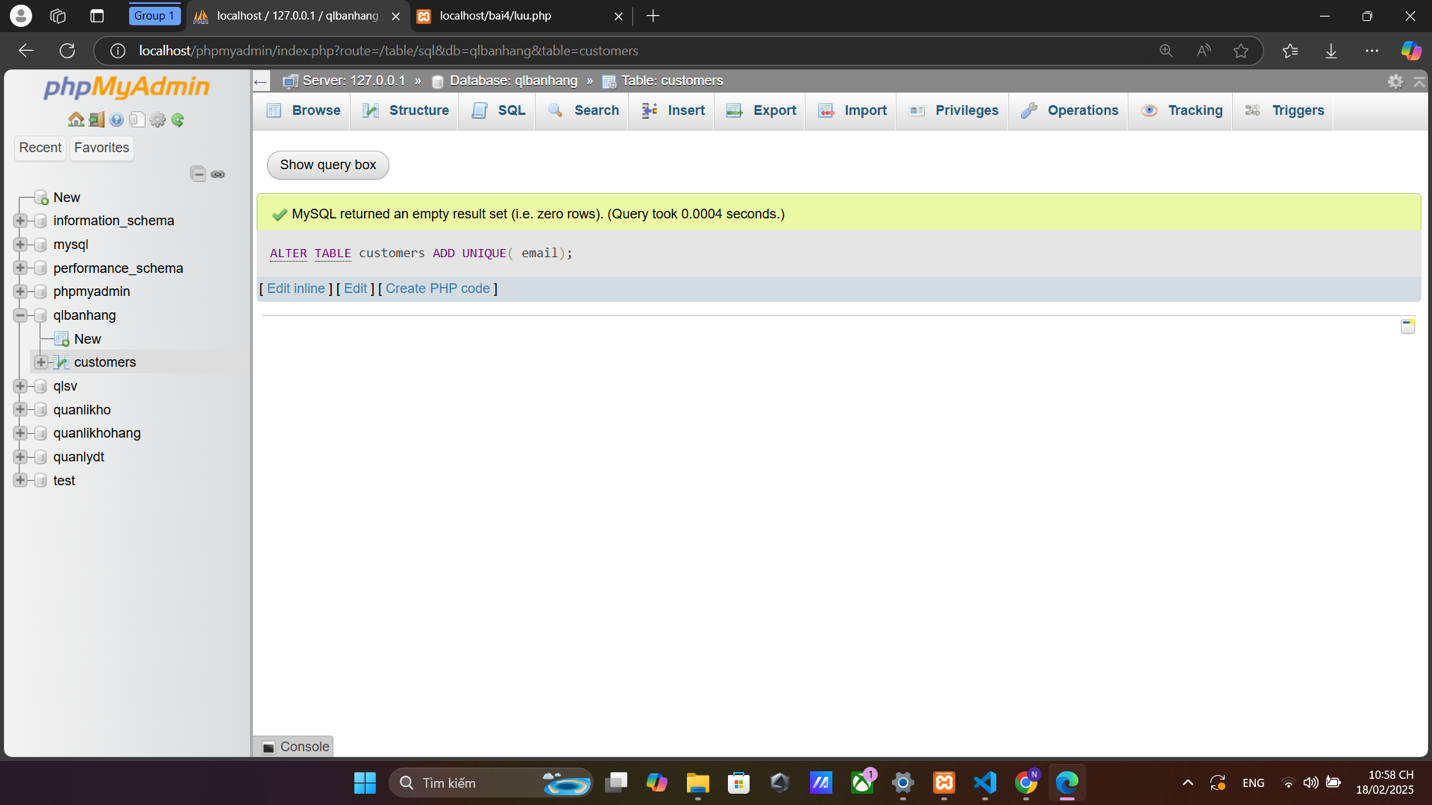
Description automatically generated

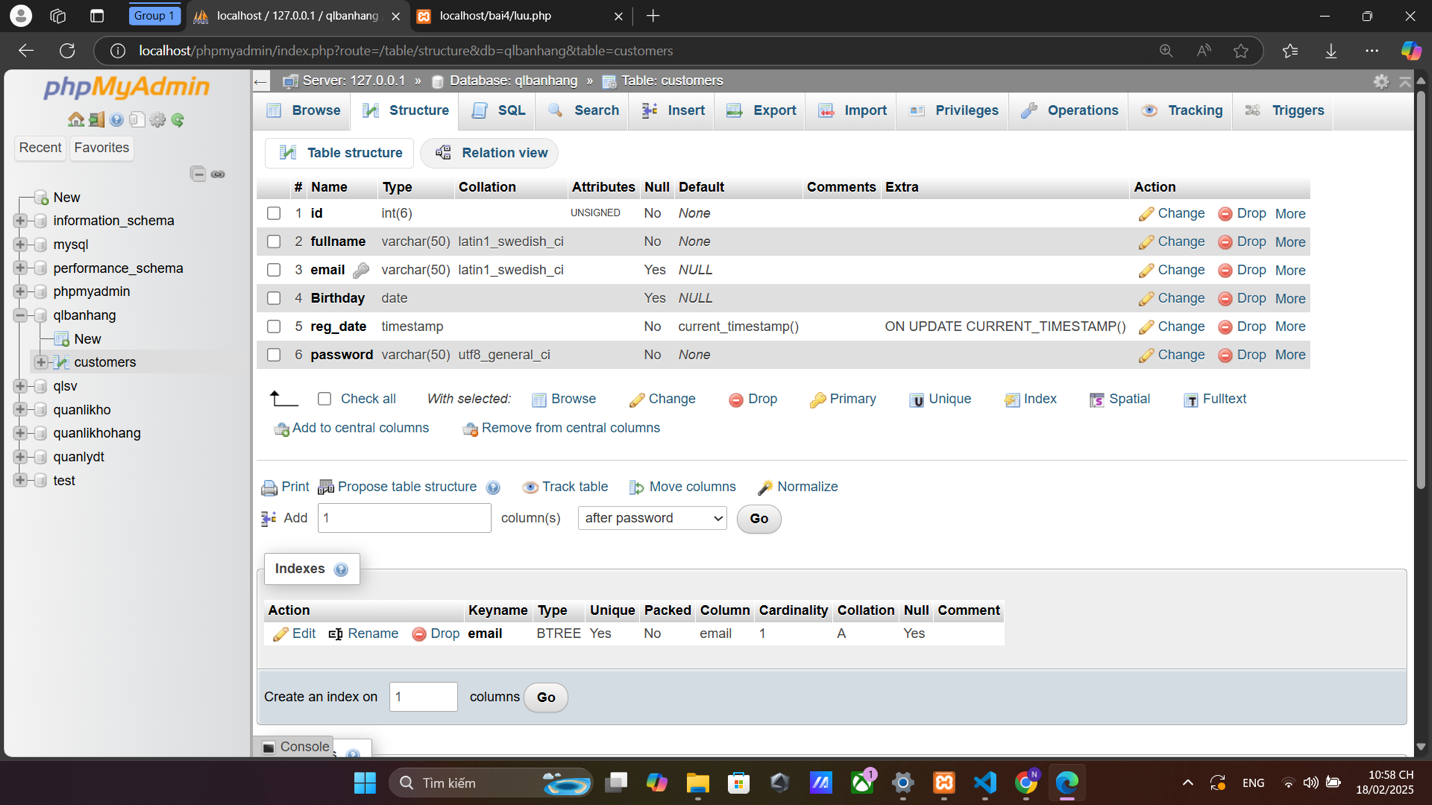


A screenshot of a computer

Description automatically generated

-Sửa cột email:



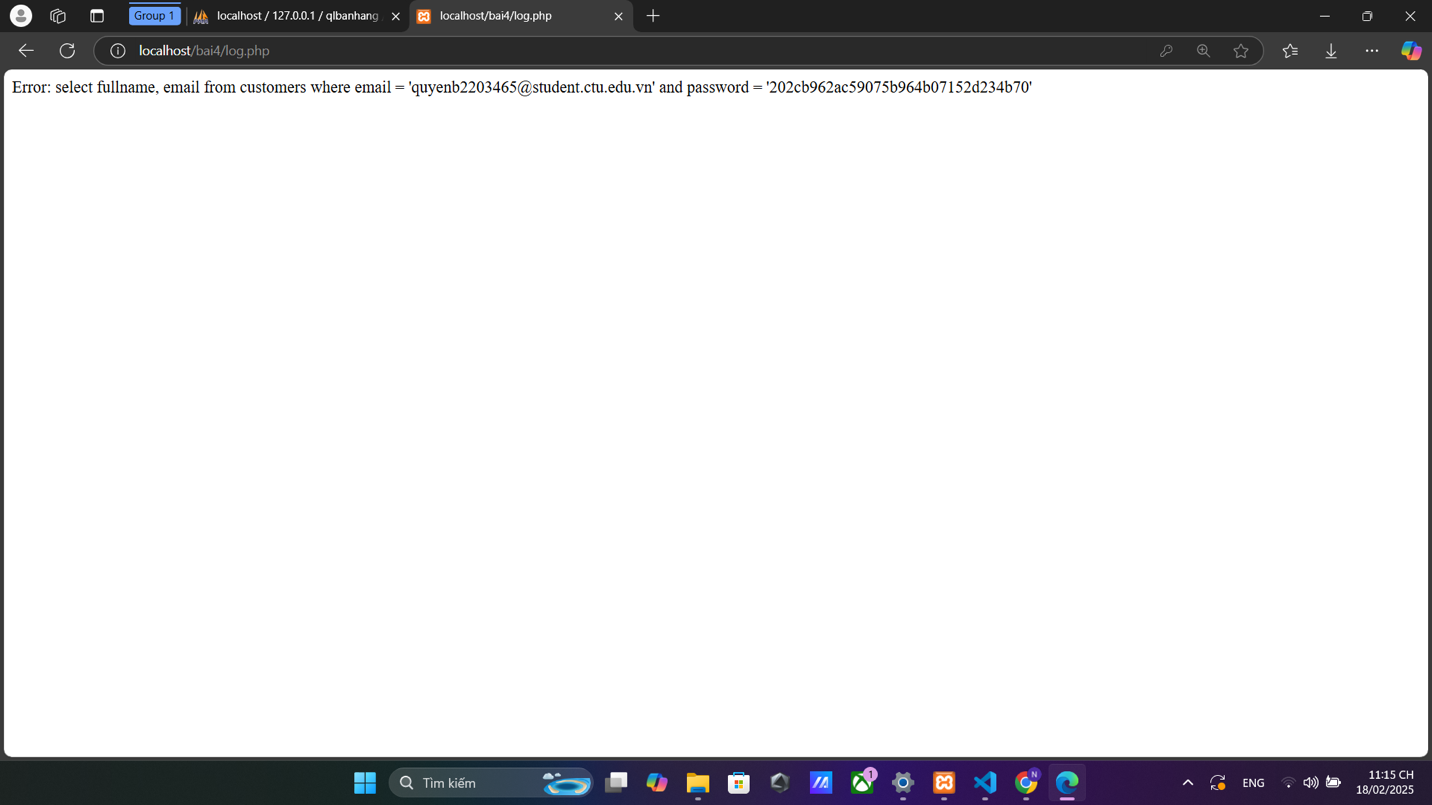


-Form nhập email:

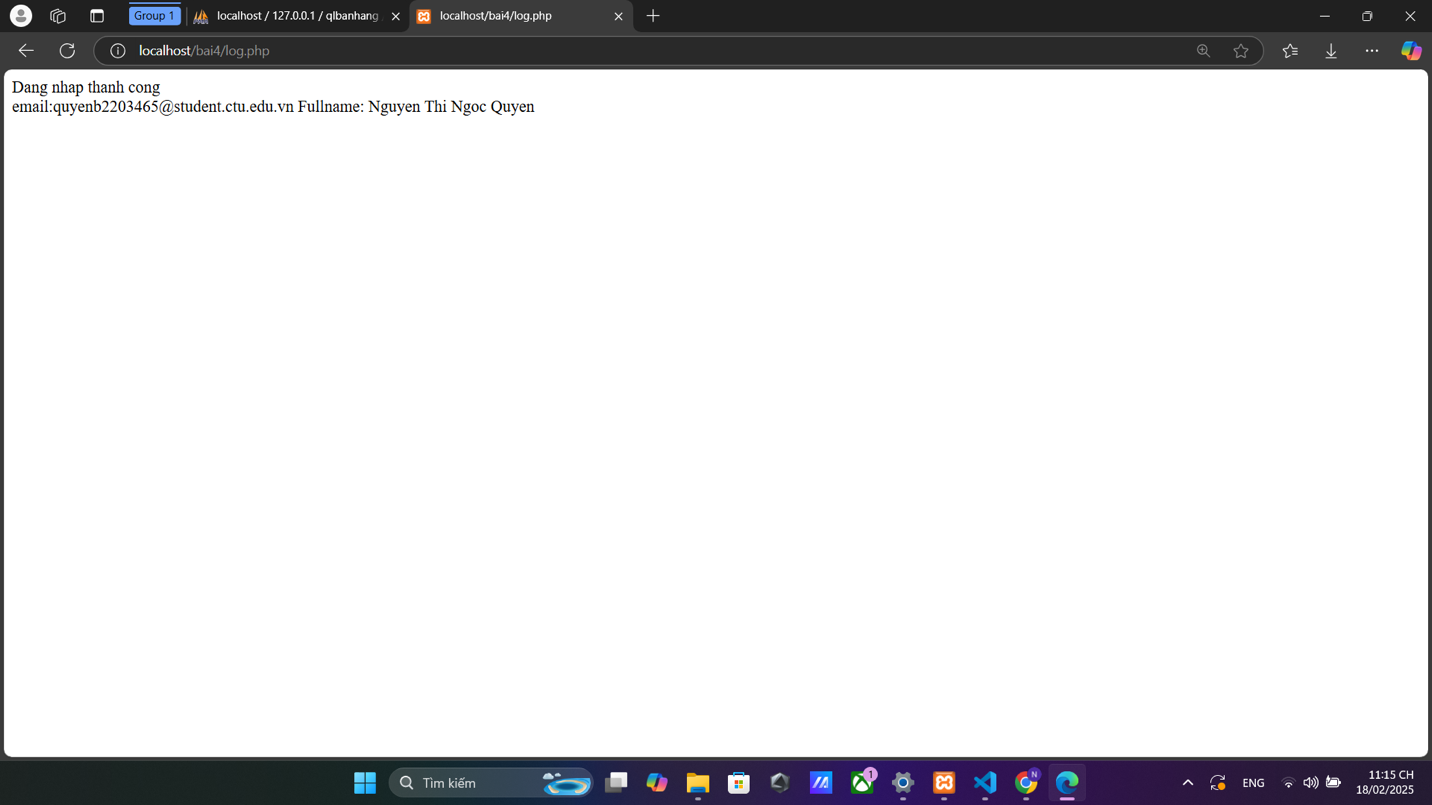
A screenshot of a computer

Description automatically generated

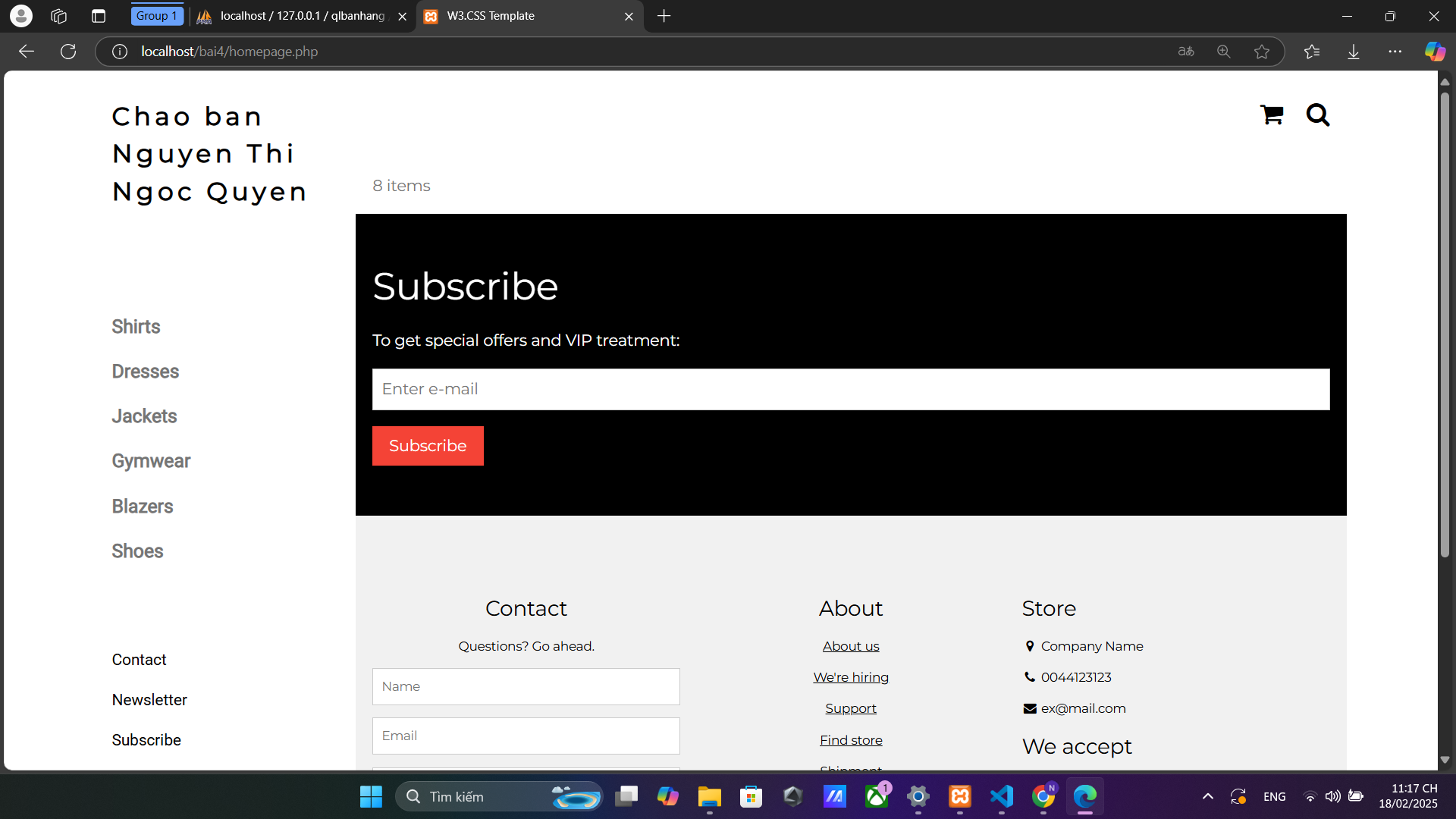
-Nếu nhập sai sẽ hiện thị lỗi:



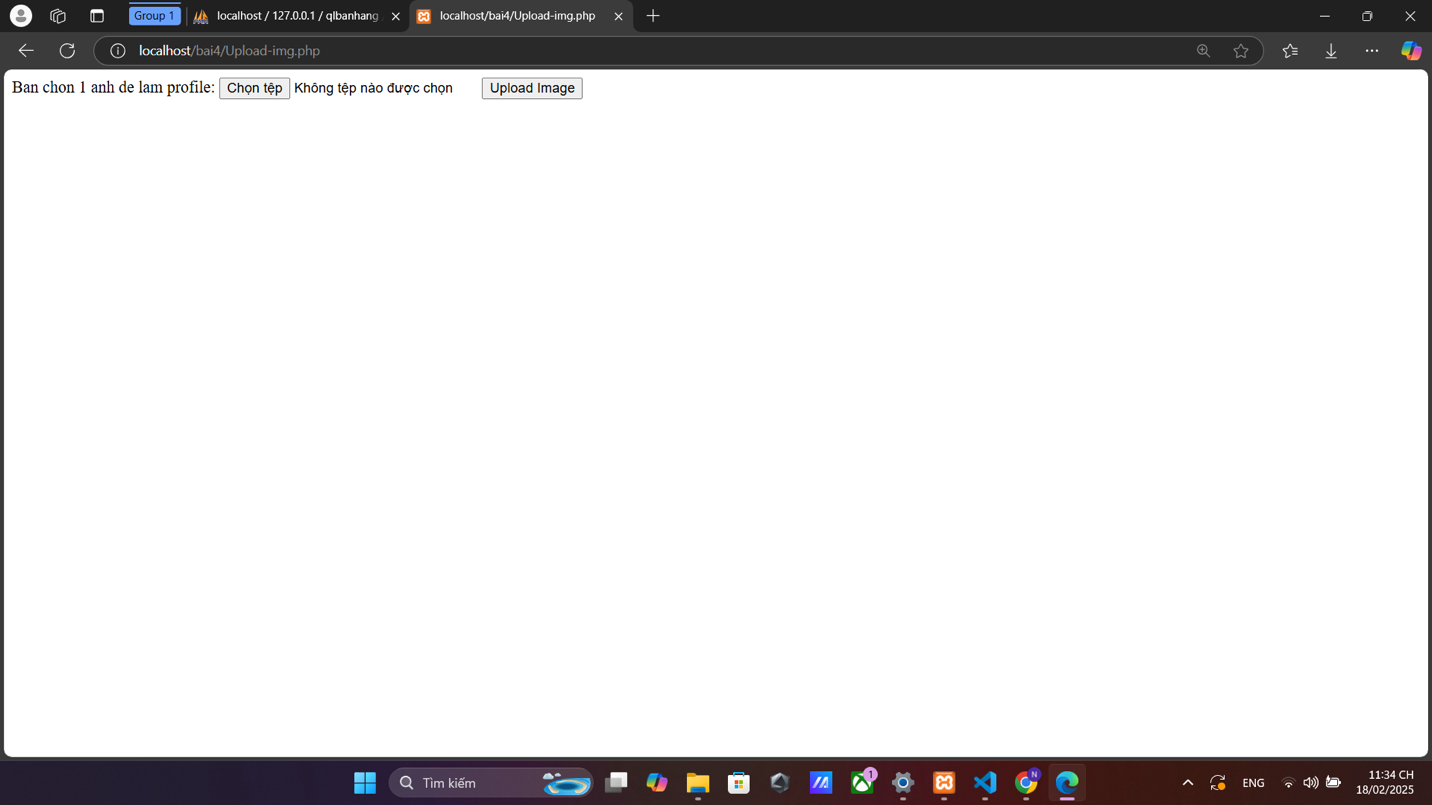
-Đăng nhập thành công:



-Trang Homepage:



-Form Upload-image:



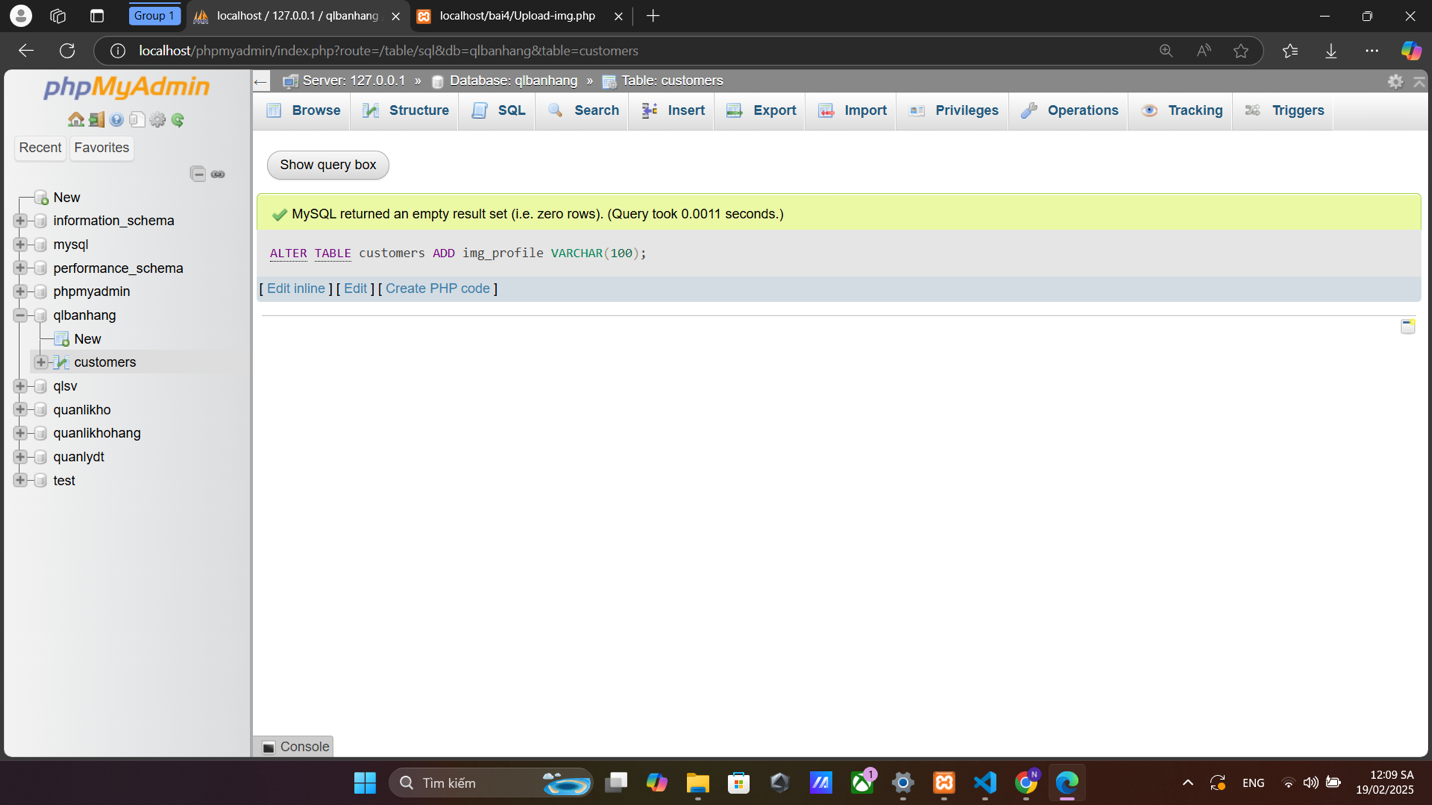
A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

-Thêm cột img\_profile vào bảng custommer:





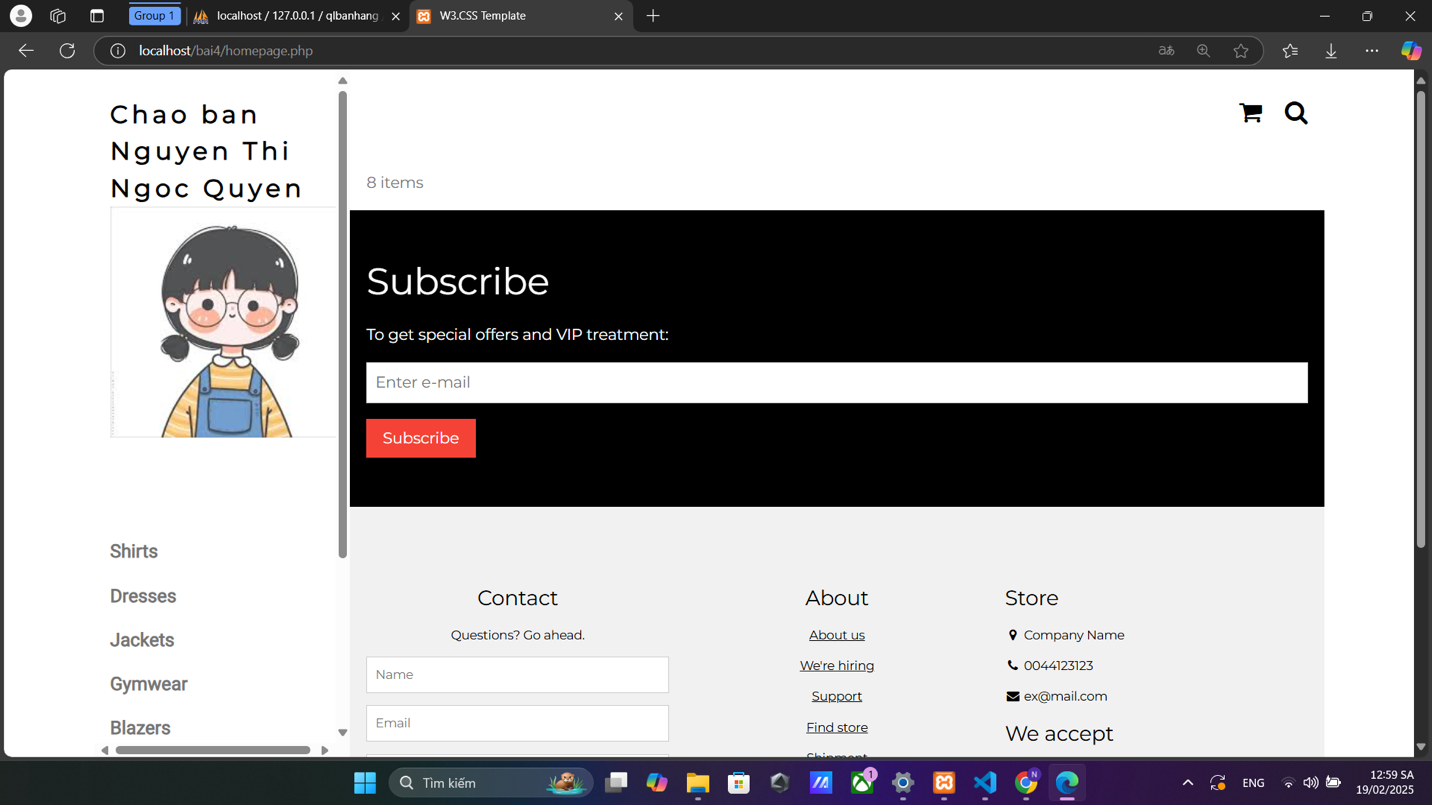
-Form Upload image lên CSDL:

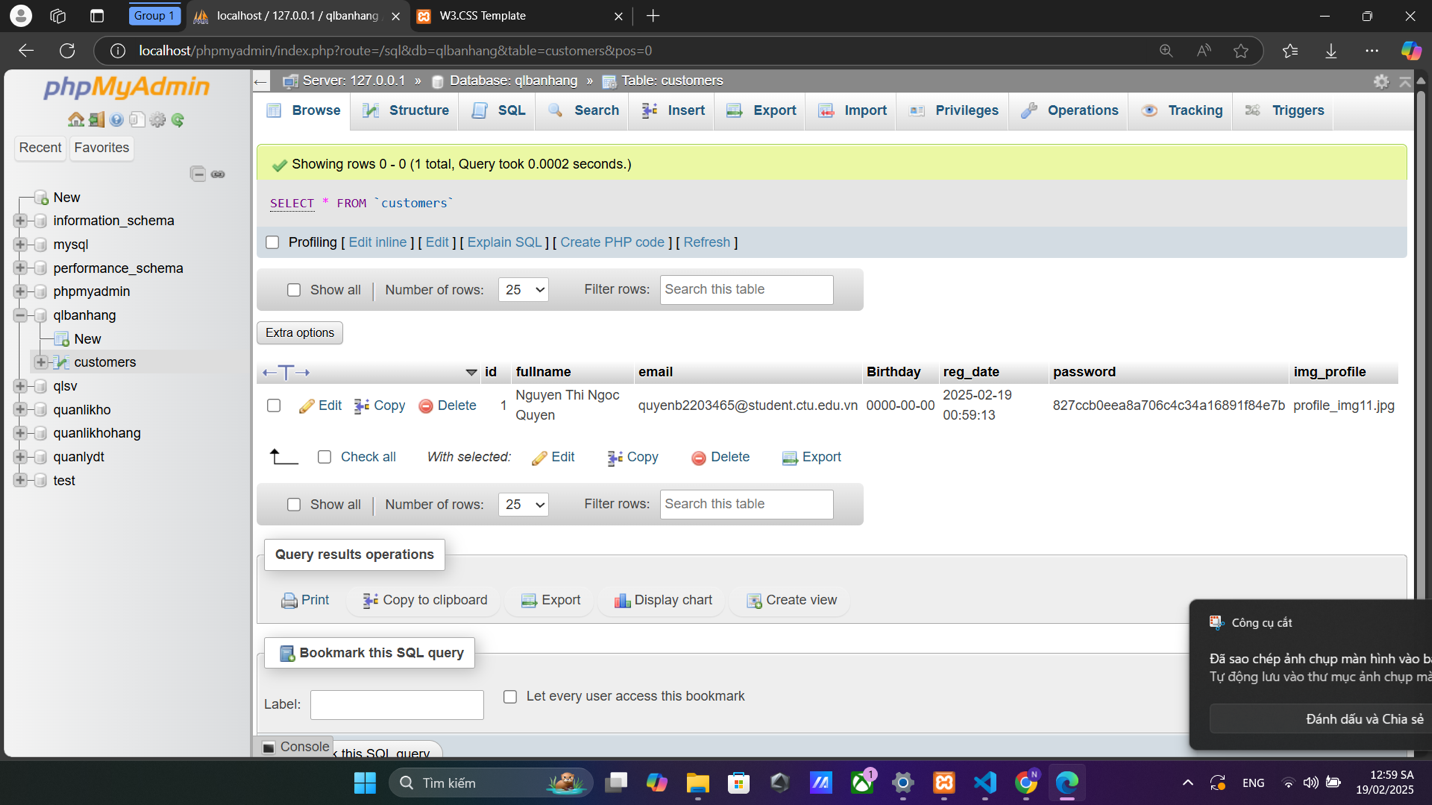
A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated





-Tạo file cus.csv:

A screenshot of a computer

Description automatically generated

-Đọc file csv:

A screenshot of a computer

Description automatically generated

1. Trong vài trường hợp, hacker có thể sử dụng các kỹ thuật SQL Injection để hack hệ thống của bạn. Bạn hãy trình bày SQL Injection là gì và thử các ví dụ trình bày trong [[1]](#footnote-0). Ứng dụng kỹ thuật đó vào trang đăng nhập mà bạn đã tạo, chụp lại các kết quả.

SQL Injection là một kỹ thuật tấn công vào cơ sở dữ liệu bằng cách chèn các câu lệnh SQL độc hại vào đầu vào của ứng dụng web. Điều này có thể cho phép kẻ tấn công truy xuất, thay đổi hoặc xóa dữ liệu từ cơ sở dữ liệu của bạn.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. Dựa vào link[[2]](#footnote-1), bạn hãy cho biết Cookie là gì, diễn giải ý nghĩa các tham số trong setcookie(). Cách lưu, lấy, xóa giá trị trong cookie.

Cookie là một tệp nhỏ được lưu trữ trên trình duyệt của người dùng để lưu thông tin giữa các phiên truy cập. Nó thường được sử dụng để lưu trạng thái đăng nhập, tùy chỉnh giao diện, hoặc theo dõi hành vi người dùng.

| | **Tham số** |  | | --- | --- | | |  | **Ý nghĩa** | | --- | --- | |
| --- | --- | --- | --- | --- | --- |
| | Name | | --- | | | Tên của cookie. | | --- | |
| | Value |  | | --- | --- | | |  | Giá trị được lưu trữ (chuỗi). | | --- | --- | |
| | Expire |  | | --- | --- | | |  | Thời gian hết hạn (tính bằng giây từ thời điểm hiện tại). Nếu không có, cookie sẽ bị xóa khi đóng trình duyệt. | | --- | --- | |
| | Path |  | | --- | --- | | |  | Đường dẫn mà cookie có hiệu lực (mặc định là /, áp dụng cho toàn bộ trang web). | | --- | --- | |
| Domain | | Miền mà cookie có hiệu lực (ví dụ: .example.com để áp dụng cho tất cả subdomain). | | --- | |
| Secure | |  | Nếu là true, cookie chỉ được gửi qua kết nối **HTTPS**. | | --- | --- | |
| |  | Httponly | | --- | --- | | |  | Nếu là true, cookie chỉ có thể được truy cập qua **HTTP**, không thể bị truy xuất bởi JavaScript. | | --- | --- | |

**Cách lưu, lấy và xóa Cookie trong PHP:**

Lưu giá trị vào: Cookie setcookie("username", "JohnDoe", time() + 3600, "/");

Lấy giá trị từ: Cookie if(isset($\_COOKIE["username"])) { echo "User: " . $\_COOKIE["username"]; } else { echo "Cookie 'username' không tồn tại."; }

Xóa Cookie: setcookie("username", "", time() - 3600, "/"); tạo lại khác chút coi

1. Dựa vào link[[3]](#footnote-2), bạn hãy cho biết Session dùng để làm gì. Cách lưu, lấy, xóa giá trị trong Session.

| **Cách sử dụng Session trong PHP** | |
| --- | --- |
| Bắt đầu một Session | session\_start(); |
| Lưu giá trị vào Session | $\_SESSION["username"] = "JohnDoe";  $\_SESSION["role"] = "admin"; |
| Lấy giá trị từ Session | session\_start();  if(isset($\_SESSION["username"])) {      echo "User: " . $\_SESSION["username"];  } else {      echo "Session chưa được thiết lập.";  } |
| Xóa giá trị trong Session | Xóa một biến: unset($\_SESSION["username"]); |
| Xóa toàn bộ: session\_destroy(); |

1. Bạn hãy so sánh Cookie và Session.

**Lưu trữ:**

**Session:** Dữ liệu được lưu trữ trên **máy chủ**.

**Cookie:** Dữ liệu được lưu trữ trên **trình duyệt** của người dùng.

**Bảo mật:**

**Session:** Bảo mật cao hơn vì dữ liệu không được lưu trên phía client, giảm nguy cơ bị đánh cắp hoặc sửa đổi.

**Cookie:** Dễ bị đánh cắp hoặc sửa đổi nếu không được bảo vệ đúng cách, vì dữ liệu nằm trên phía client.

**Thời gian sống:**

**Session:** Thường tồn tại trong suốt phiên làm việc và sẽ mất khi người dùng đóng trình duyệt hoặc khi hết thời gian timeout được thiết lập trên máy chủ.

**Cookie:** Có thể tồn tại lâu hơn tùy thuộc vào thời gian hết hạn được thiết lập; nếu không đặt thời gian hết hạn, cookie sẽ bị xóa khi đóng trình duyệt.

1. Chỉnh sửa các đoạn gán, khởi tạo, lấy giá trị cookie trong log.php và homepage.php thay bằng cách dùng Session. Tạo tập tin thoat.php để xóa các giá trị trong session, cookie thực hiện chức năng log out khỏi hệ thống.

A screenshot of a computer

Description automatically generated

-Khi chọn đăng xuất sẽ quay về form đăng nhập:

A screenshot of a computer

Description automatically generated

1. Bạn hãy tạo form sua\_mk.php cho phép người dùng chỉnh sửa mật khẩu sau khi đăng nhập. Yêu cầu gồm 3 input: ô để nhập mật khẩu cũ, 1 ô để nhập mật khẩu mới, 1 ô cho phép nhập mật lại mật khẩu mới. Khi nhập xong cần đảm bảo: mật khẩu cũ là khớp với CSDL đang lưu, 2 ô nhập mật khẩu mới phải khớp với nhau và không giống với mật khẩu cũ, nếu đáp ứng điều kiện thì tiến hành băm mật khẩu với md5 và lưu mật khẩu mới vào CSDL.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. Bạn đọc trong[[4]](#footnote-3) để tìm hiểu và mô tả các cơ chế, các hàm/thủ tục để thực hiện việc upload.

Việc upload file trong PHP bao gồm các bước sau:

1. Tạo form upload
2. Xử lý dữ liệu file khi được gửi
3. Kiểm tra file hợp lệ (kích thước, loại file, bảo mật, v.v.)
4. Di chuyển file vào thư mục lưu trữ trên server

| **Hàm** | **Mô tả** |
| --- | --- |
| $\_FILES | Mảng chứa thông tin file upload |
| pathinfo($filename, PATHINFO\_EXTENSION) | Lấy phần mở rộng của file |
| getimagesize($filename) | Kiểm tra file có phải là ảnh hợp lệ |
| move\_uploaded\_file($tmp\_name, $destination) | Di chuyển file từ thư mục tạm vào thư mục đích |
| file\_exists($filename) | Kiểm tra file có tồn tại hay không |
| filesize($filename) | Lấy kích thước file |
| mime\_content\_type($filename) | Lấy loại MIME của file |

1. Bạn hãy đọc[[5]](#footnote-4), mô tả chức năng của hàm này và các tham số trong hàm (tham khảo thêm từ read-csv.php).

Hàm file() trong PHP được sử dụng để đọc toàn bộ nội dung của một tệp và lưu từng dòng vào một mảng. Mỗi phần tử của mảng là một dòng trong tệp.

Cú pháp: array file(string $filename, int $flags = 0)

| Tham số | Mô tả |
| --- | --- |
| $filename | Đường dẫn đến tệp cần đọc. |
| $flags *(Tùy chọn)* | Có thể sử dụng một hoặc nhiều cờ (flags) để thay đổi cách đọc file. |

Các giá trị trả về:

+ Nếu thành công, file() trả về một mảng, trong đó mỗi phần tử là một dòng từ file.

+ Nếu có lỗi, hàm trả về false.

| Giá trị cờ | Mô tả |
| --- | --- |
| FILE\_IGNORE\_NEW\_LINES | Loại bỏ ký tự xuống dòng (\n, \r) ở cuối mỗi dòng. |
| FILE\_SKIP\_EMPTY\_LINES | Bỏ qua các dòng trống. |
| FILE\_USE\_INCLUDE\_PATH | Kiểm tra cả trong include\_path khi tìm file |

1. Bạn hãy tạo 1 tập tin csv ít nhất 10 dòng dữ liệu với các cột dữ liệu như bảng customer trong csdl qlbanhang. Tạo tập tin upload-csv.php với giao diện cho phép upload các tập tin csv, và tập tin upload-csv-processing để xử lý nút xử lý sự kiện upload file csv và đưa dữ liệu vào bảng customers trong CSDL. Gợi ý:
   * Xem cấu trúc của bảng customer, mở excel và nhập liệu lưu lại với định dạng CSV.
   * Tham khảo upload-img.php để thiết kế giao diện upload file
   * Tham khảo upload-csdl.php để thiết kế action xử lý việc upload file, chú ý chỉnh sửa loại tập tin chấp nhận các file csv. Tham khảo: [[6]](#footnote-5),[[7]](#footnote-6). Ở đoạn sau khi upload thành công, bạn lấy tên file vừa upload đưa vào hàm đọc tập tin. Bạn tham khảo read-csv.php chỉnh sửa đọc dữ liệu từ csv đưa vào mảng để lần lượt thực hiện insert từng dòng dữ liệu trong csv vào CSDL.

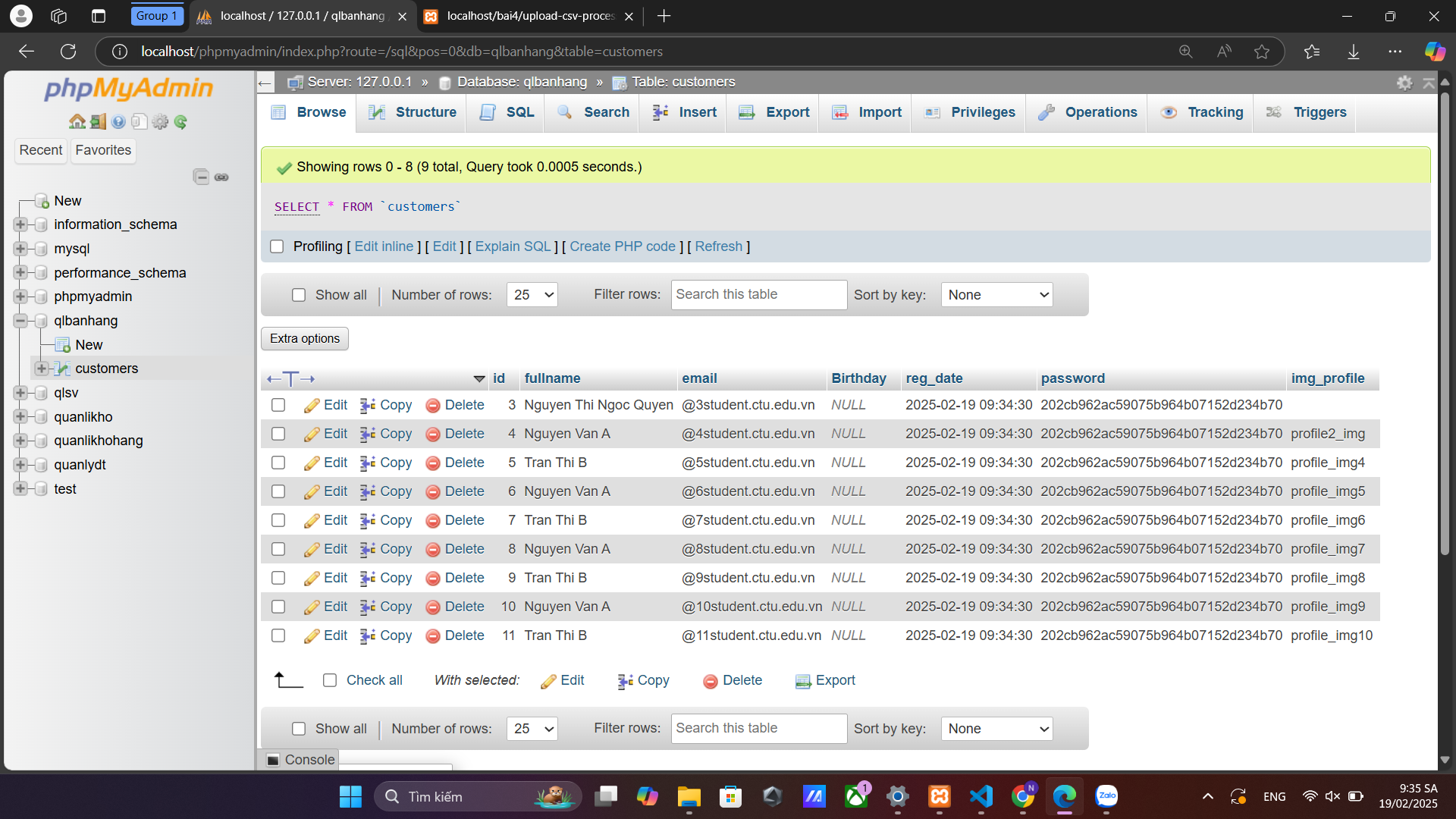
-Form upload file csv:

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated



**Chú ý:**

* Các bạn nộp file word: Quy tắc đặt tên file: **<mssv>-<hoten>-<bai><stt\_bai thực hành>.docx** nộp lên Classroom (VD: **B123456-NguyenVanA-bai1.docx**), kèm với các file khác được yêu cầu như phần câu hỏi đã nêu. **Ngoại trừ file word trả lời câu hỏi, các file còn lại các bạn nén vào 1 file zip**. File zip đặt tên như file word.
* Mỗi câu các bạn trả lời bằng hình hoặc dạng text tùy vào yêu cầu của câu hỏi và **TRẢ LỜI THEO ĐÚNG THỨ TỰ CÂU HỎI**. Nếu câu nào không trả lời được các bạn cứ để số thứ tự câu hỏi và bỏ trống phần trả lời.
* Các câu trả lời có tham khảo trên Internet phải trích dẫn link/nguồn.
* *Vi phạm 1 trong các điều sau đây bài thực hành sẽ bị 0 điểm:*
  + Đặt tên KHÔNG ĐÚNG quy tắc được yêu cầu.
  + Bài không đủ các thành phần (word, code+data (nếu có),...) đã được yêu cầu.
  + Bài không thực hiện đúng yêu cầu “**Ngoại trừ file word trả lời câu hỏi, các file còn lại các bạn nén vào 1 file .zip”**
  + Bị phát hiện copy, sao chép từ các bạn khác
  + Phần trả lời không ghi rõ trả lời cho câu nào
  + Thứ tự câu trả lời không đúng thứ tự câu hỏi

1. <https://www.w3schools.com/sql/sql_injection.asp> [↑](#footnote-ref-0)
2. <https://www.w3schools.com/php/php_cookies.asp> [↑](#footnote-ref-1)
3. <https://www.w3schools.com/php/php_sessions.asp> [↑](#footnote-ref-2)
4. <https://www.w3schools.com/php/php_file_upload.asp> [↑](#footnote-ref-3)
5. <https://www.w3schools.com/php/func_filesystem_file.asp> [↑](#footnote-ref-4)
6. <https://www.php.net/manual/en/features.file-upload.post-method.php>, [↑](#footnote-ref-5)
7. https://stackoverflow.com/questions/6654351/check-file-uploaded-is-in-csv-format [↑](#footnote-ref-6)