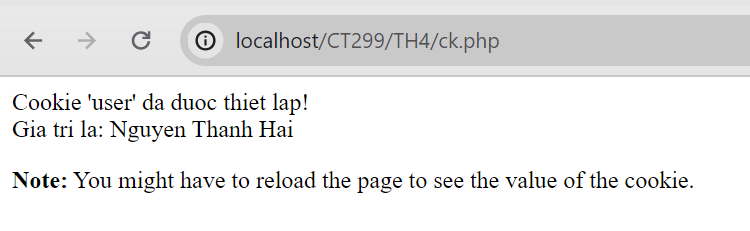
THỰC HÀNH 4.

Nguyễn Hoàng Gia – B2110041 – CT299 – Nhóm 2.

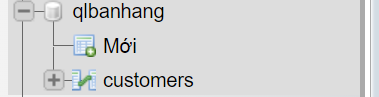
**Câu 1:**

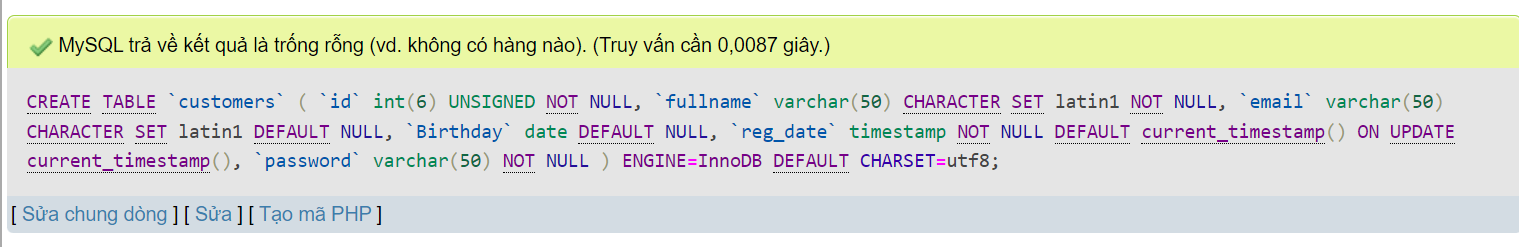
**Tạo cookies:**



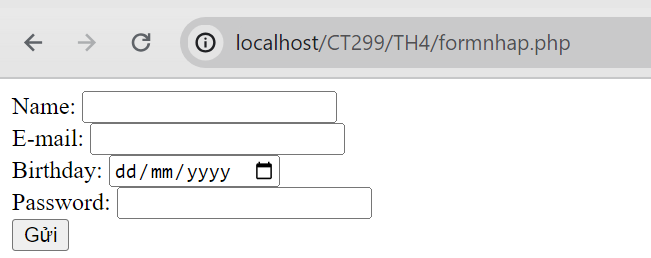
**Tạo 1 trang đăng kí người dùng với mật khẩu được mã hóa**

* Tạo database qlbanhang và table customers.

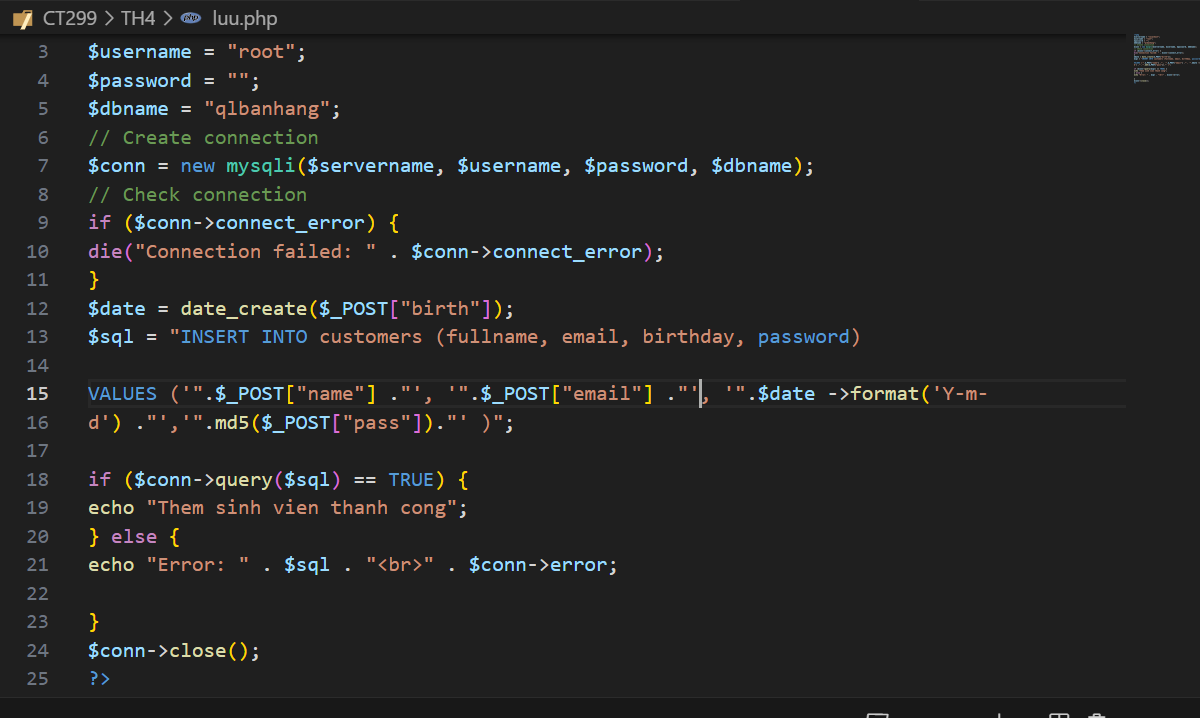




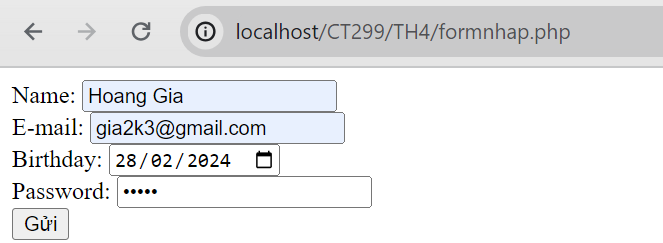
* Tạo formnhap.php

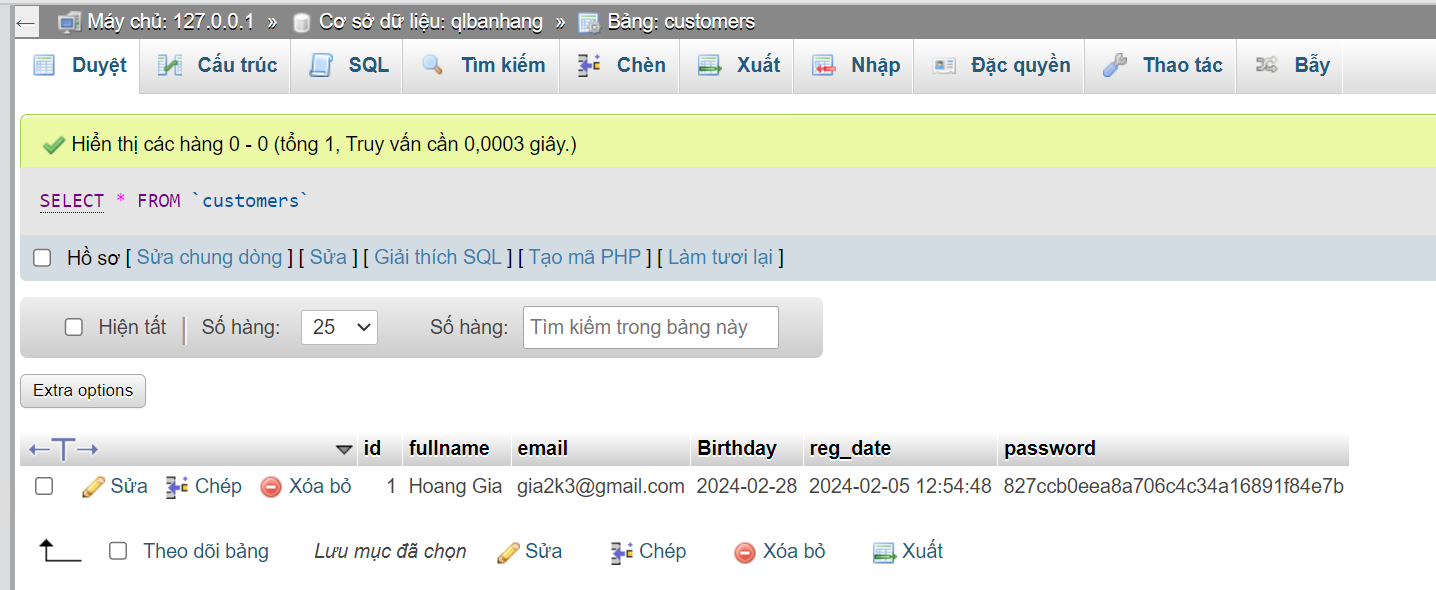


* Tạo luu.php

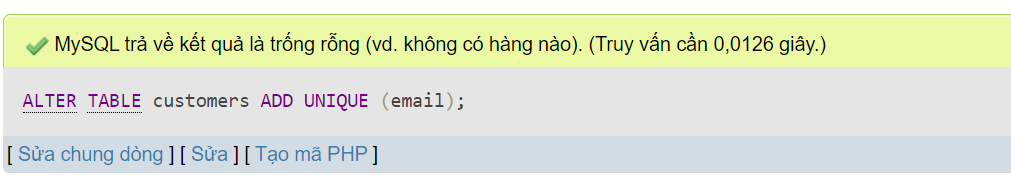


* Nhập dữ liệu



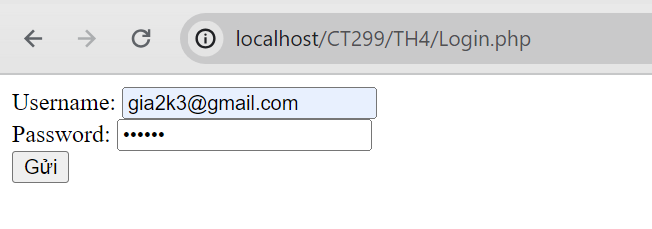


* Chọn email là unique



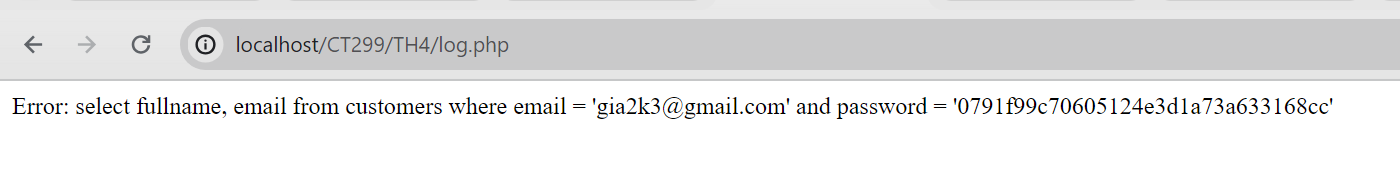
**Tạo form đăng nhập**

* Form Login.php



* Form Log.php

+ Khi nhập Username và Password sai:

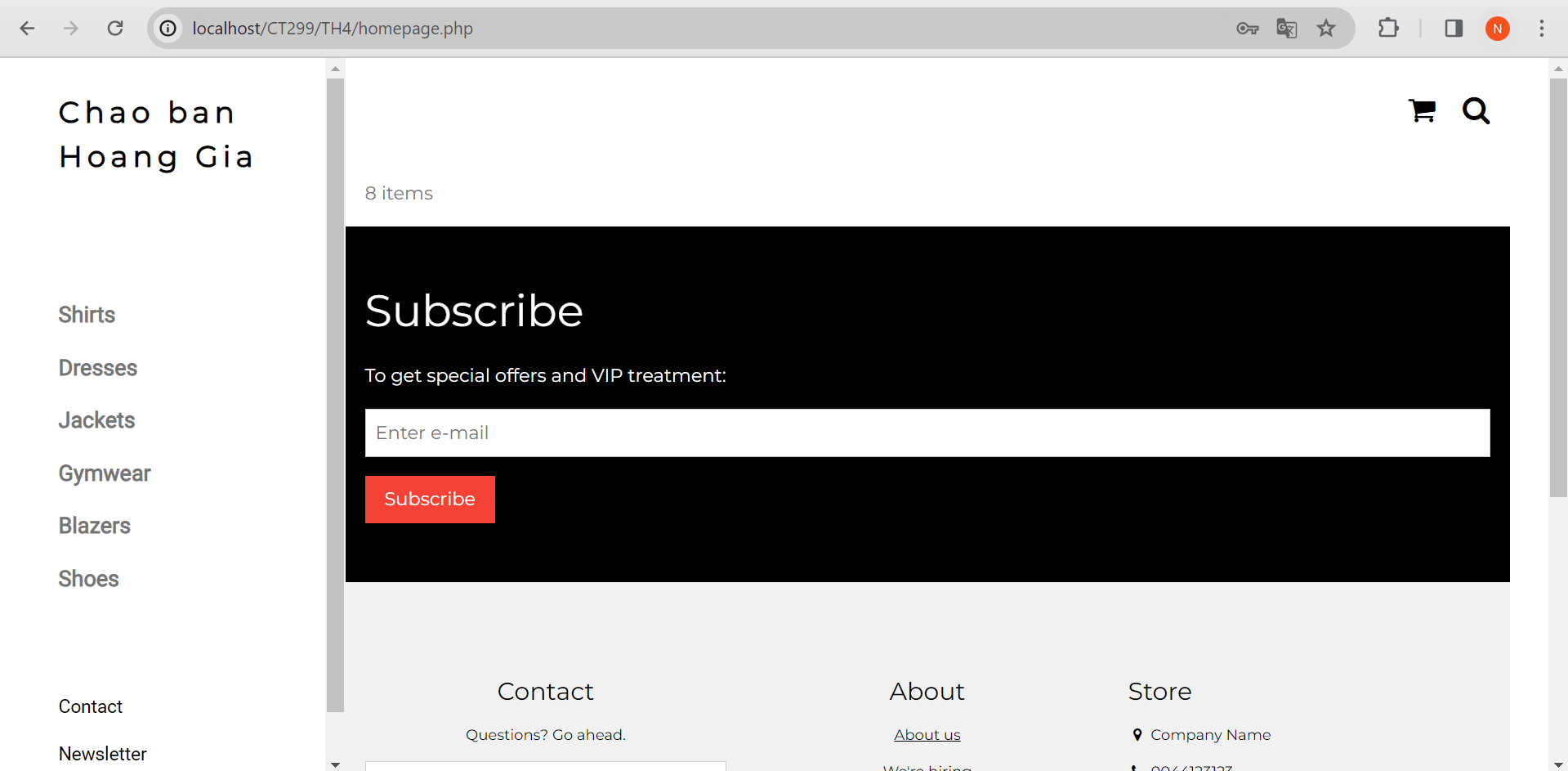


+ Khi nhập đúng:



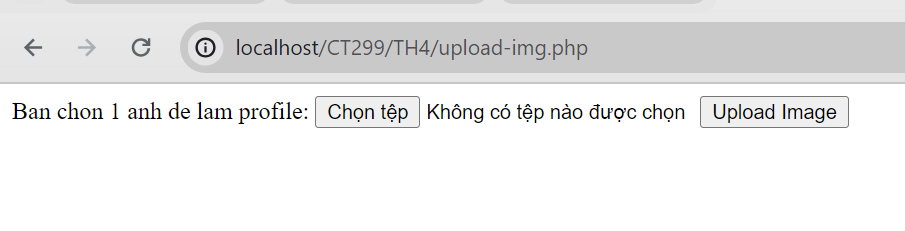
**Dùng cookies lưu lại tên đăng nhập, email và điều hướng**

* Chỉnh sửa lại Log.php
* <?php
* $servername = "localhost";
* $username = "root";
* $password = "";
* $dbname = "qlbanhang";
* // Create connection
* $conn = new mysqli($servername, $username, $password, $dbname);
* // Check connection
* if ($conn->connect\_error) {
* die("Connection failed: " . $conn->connect\_error);
* }
* $sql = "select id, fullname, email from customers where email = '".$\_POST["email"]."' and
* password = '".md5($\_POST["pass"])."'";
* $result = $conn->query($sql);
* if ($result->num\_rows > 0) {
* $row = $result->fetch\_assoc();
* $cookie\_name = "user";
* $cookie\_value = $row['email'] ;
* setcookie($cookie\_name, $cookie\_value, time() + (86400 / 24), "/");
* setcookie("fullname", $row['fullname'], time() + (86400 / 24), "/");
* setcookie("id", $row['id'], time() + (86400 / 24), "/");
* header('Location: homepage.php');
* } else {
* echo "Error: " . $sql . "<br>" . $conn->error;
* //Tro ve trang dang nhap sau 3 giay
* header('Refresh: 3;url=login.php');
* }
* $conn->close();
* ?>
* Và đăng nhập:

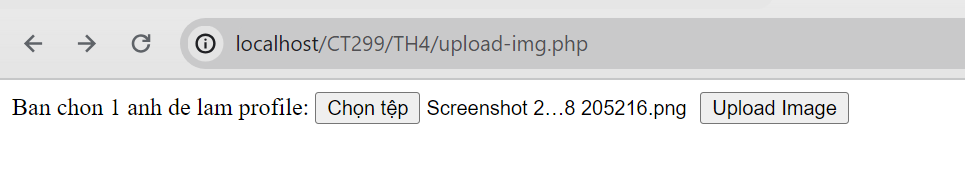


**Upload tập tin**

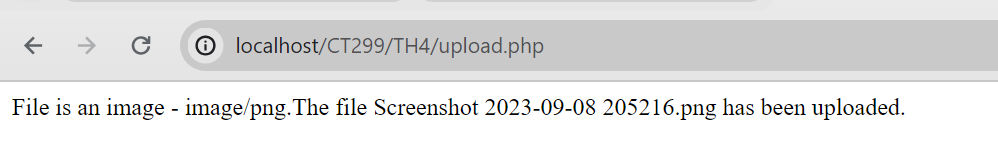
* Form Upload-img.php



* Form upload.php
* <?php
* $target\_dir = "uploads/";
* $target\_file = $target\_dir .
* basename($\_FILES["fileToUpload"]["name"]);
* $uploadOk = 1;
* $imageFileType =
* strtolower(pathinfo($target\_file,PATHINFO\_EXTENSION));
* // Check if image file is a actual image or fake image
* if(isset($\_POST["submit"])) {
* $check = getimagesize($\_FILES["fileToUpload"]["tmp\_name"]);
* if($check !== false) {
* echo "File is an image - " . $check["mime"] . ".";
* $uploadOk = 1;
* } else {
* echo "File is not an image.";
* $uploadOk = 0;
* }
* }
* // Check if file already exists
* if (file\_exists($target\_file)) {
* echo "Sorry, file already exists.";
* $uploadOk = 0;
* }
* // Check file size
* if ($\_FILES["fileToUpload"]["size"] > 500000) {
* echo "Sorry, your file is too large.";
* $uploadOk = 0;
* }
* // Allow certain file formats
* if($imageFileType != "jpg" && $imageFileType != "png" &&
* $imageFileType != "jpeg"
* && $imageFileType != "gif" ) {
* echo "Sorry, only JPG, JPEG, PNG & GIF files are allowed.";
* $uploadOk = 0;
* }
* // Check if $uploadOk is set to 0 by an error
* if ($uploadOk == 0) {
* echo "Sorry, your file was not uploaded.";
* // if everything is ok, try to upload file
* } else {
* if (move\_uploaded\_file($\_FILES["fileToUpload"]["tmp\_name"],
* $target\_file)) {
* echo "The file ".
* htmlspecialchars( basename( $\_FILES["fileToUpload"]["name"])). "
* has been uploaded.";
* } else {
* echo "Sorry, there was an error uploading your file.";
* }
* }
* ?>
* Chọn ảnh để upload:

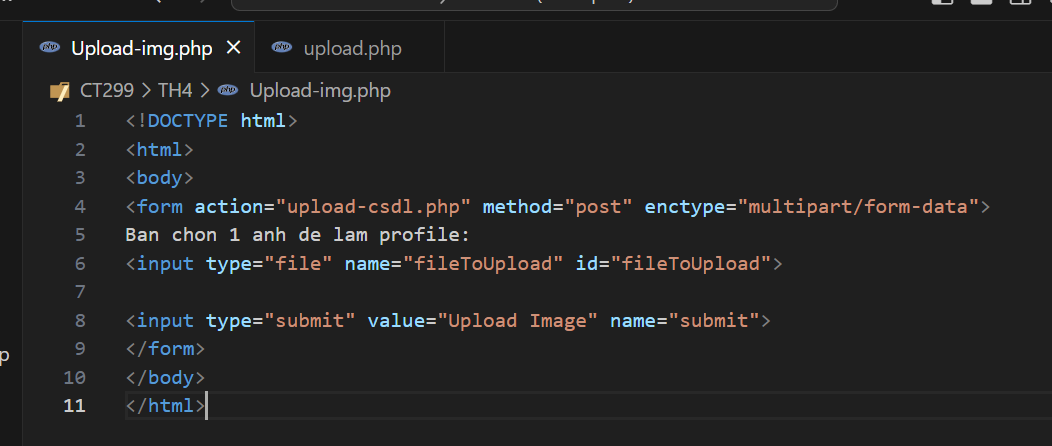


* Ảnh đã được upload:

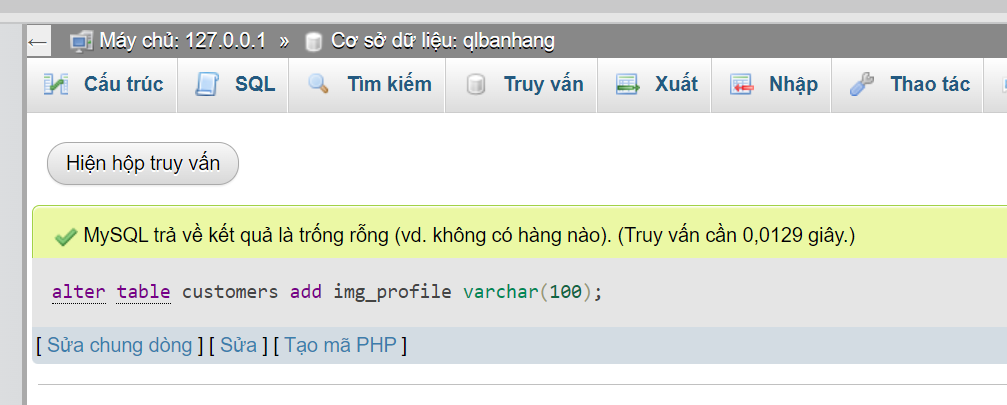


**Upload ảnh và lưu dữ liệu về ảnh trong CSDL**

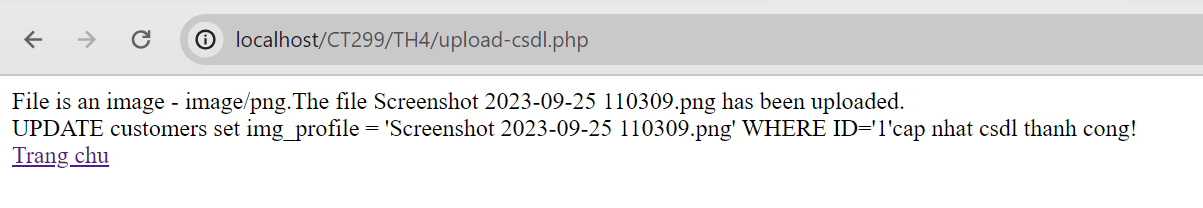
* Sửa upload-img.php

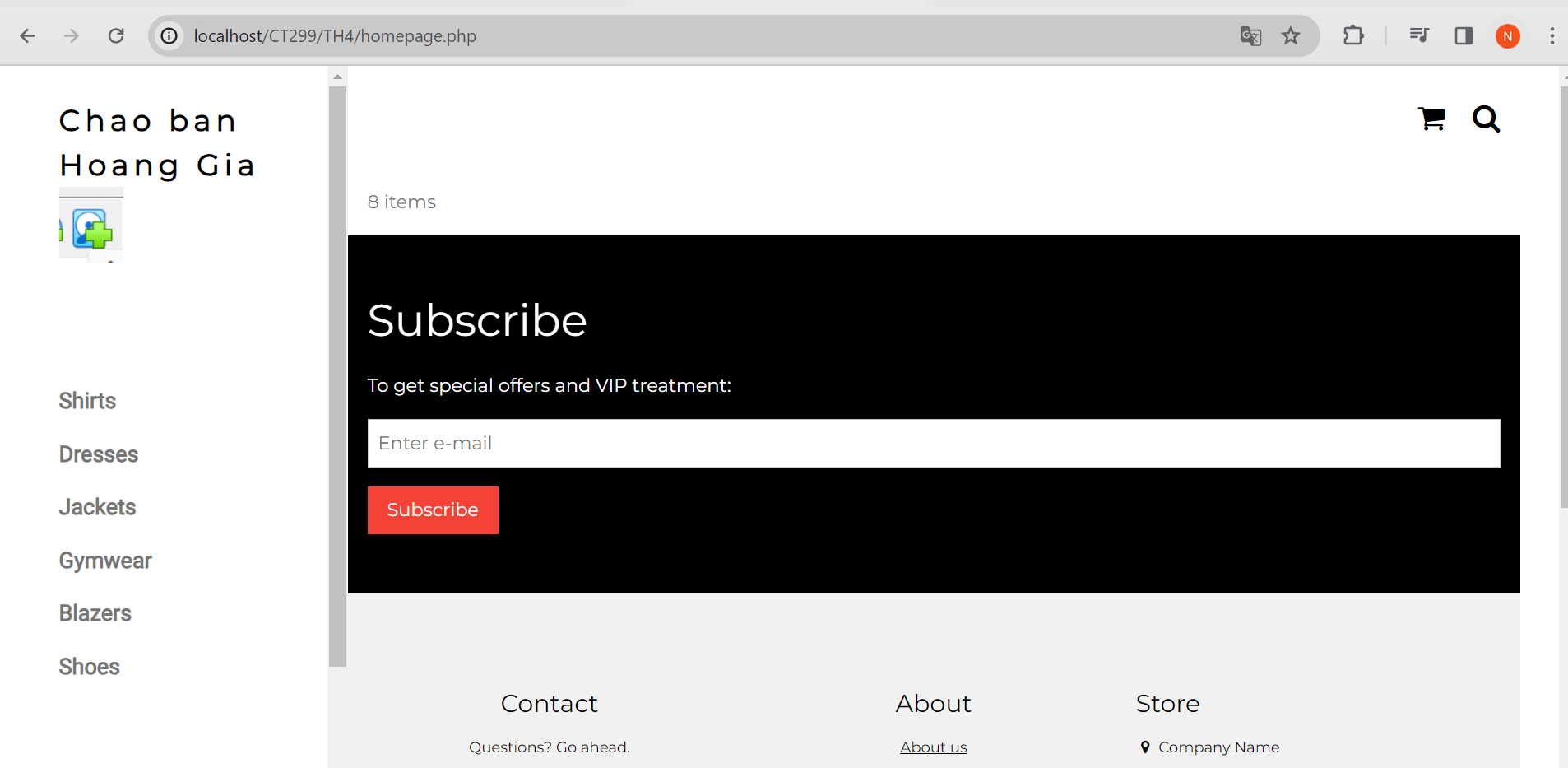


Thêm cột để lưu đường dẫn ảnh:

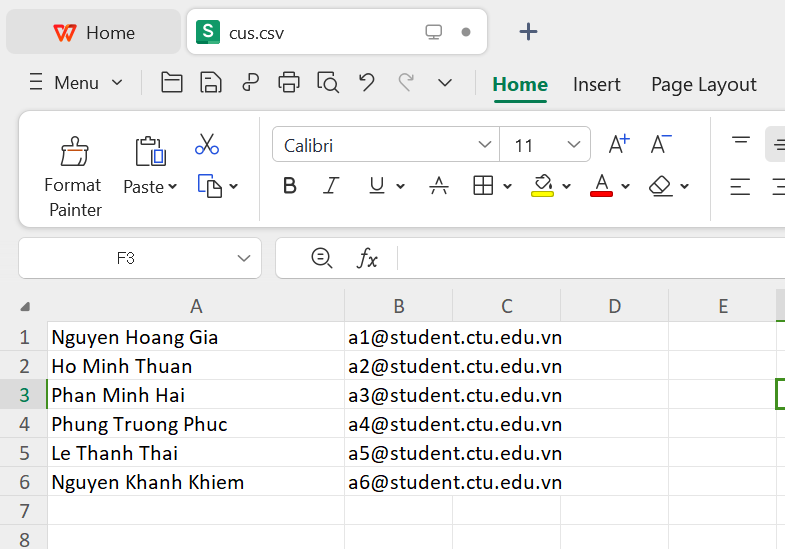


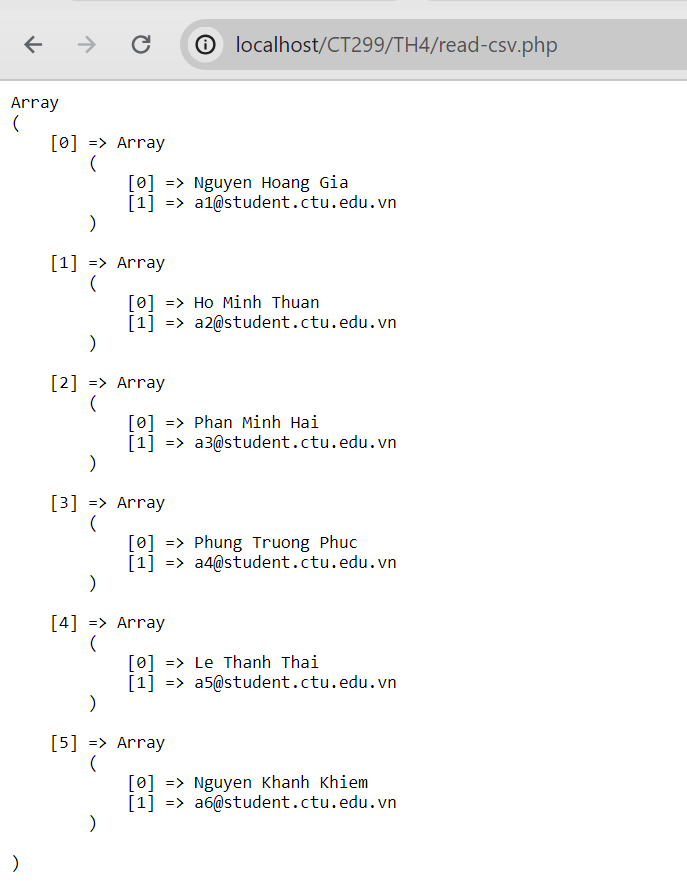
Upload-csdl.php





**Upload file CSV và đọc dữ liệu vào mảng**





Câu 2:

* SQL injection[[1]](#footnote-1):

SQL Injection là một kỹ thuật cho phép những kẻ tấn công lợi dụng lỗ hổng của việc kiểm tra dữ liệu đầu vào trong các ứng dụng web và các thông báo lỗi của hệ quản trị cơ sở dữ liệu trả về để inject (tiêm vào) và thi hành các câu lệnh SQL bất hợp pháp.

SQL injection có thể cho phép những kẻ tấn công thực hiện các thao tác trên cơ sở dữ liệu của ứng dụng, thậm chí là server mà ứng dụng đó đang chạy.

Hiểu đơn giản:

+ là một kỹ thuật chèn mã có thể phá hủy cơ sở dữ liệu của bạn.

+ là một trong những kỹ thuật hack web phổ biến nhất.

+ injection là việc đặt mã độc vào câu lệnh SQL thông qua đầu vào trang web.

Tùy vào mức độ tinh vi, SQL injection có thể cho phép kẻ tấn công:

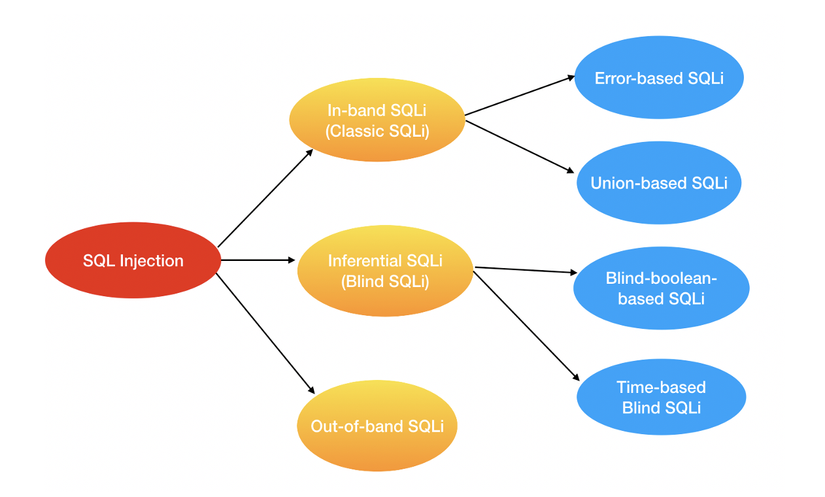
+ Vượt qua các khâu xác thực người dùng.

+ Chèn, xóa hoặc sửa đổi dữ liệu.

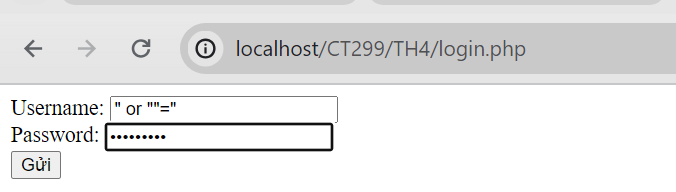
+ Đánh cắp thông tin trong CSDL.

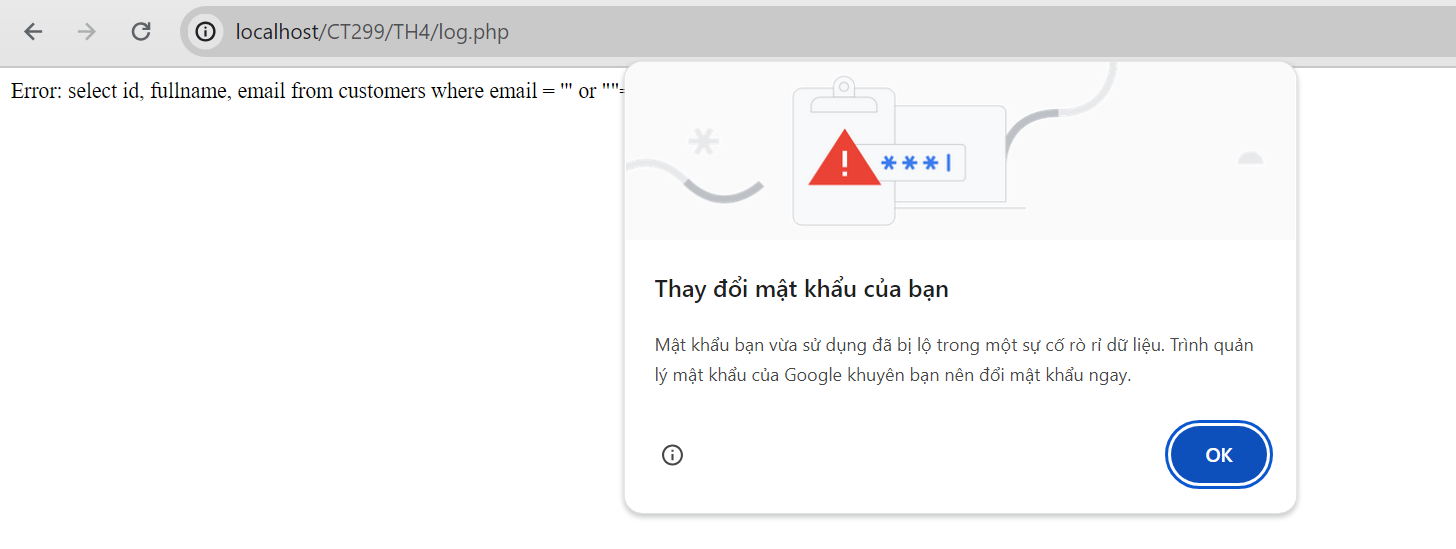
+ Chiếm quyền điều khiển hệ thống.

* SQL Injection có thể chia làm các loại sau:



Tin tặc có thể có quyền truy cập vào tên người dùng và mật khẩu trong cơ sở dữ liệu bằng cách chèn " OR ""=" vào hộp văn bản tên người dùng hoặc mật khẩu:



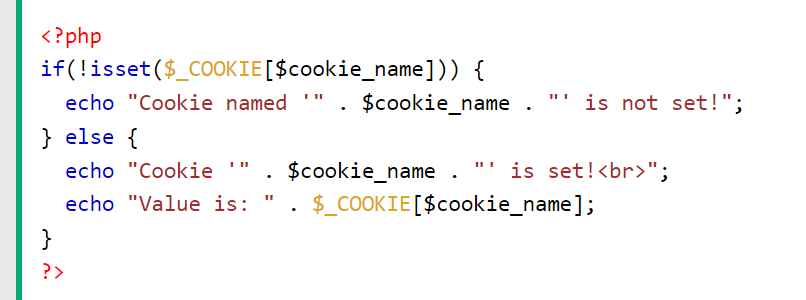


**Câu 3:**

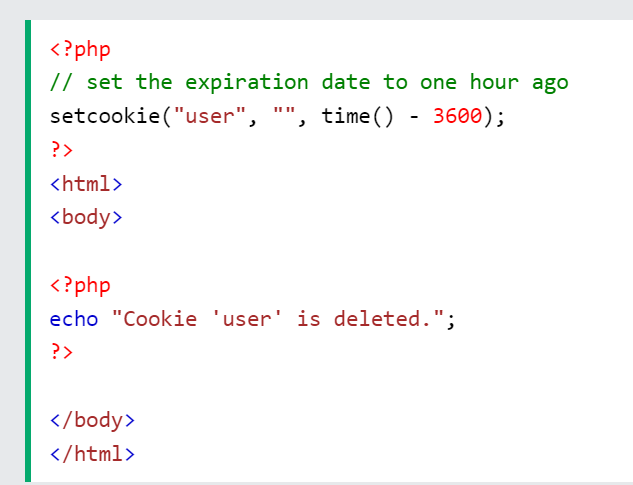
Cookie thường được sử dụng để nhận dạng người dùng. Cookie là một tệp nhỏ mà máy chủ nhúng vào máy tính của người dùng. Mỗi lần máy tính đó yêu cầu một trang bằng trình duyệt, nó cũng sẽ gửi cookie. Với PHP, bạn có thể vừa tạo vừa truy xuất các giá trị cookie.

setcookie(name, value, expire, path, domain, secure, httponly);

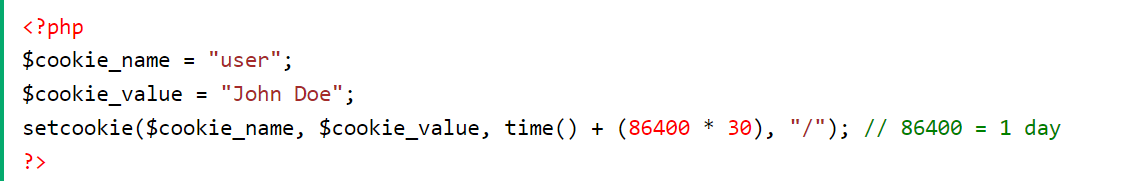
* Name: tên của cookies mà bạn muốn thiết lập
* Value: giá trị của cookies
* Expire: thời gian hết hạn của cookies
* Path: đường dẫn trên máy chủ mà cookies có sẵn. Mặc định là ‘/’. Điều này có nghĩa là cookies sẽ có sẵn cho tất cả trang trong tên miền.
* Domain: Tên miền nơi cookies có sẵn. Mặc định là rỗng, có nghĩa là cookies chỉ có sẵn trên tên miền hiện tại.
* Secure: Xác định cookies có được gửi qua HTTPS hay không. Nếu được thì đặt thành `true`, cookies sẽ chỉ được gửi qua HTTPS. Giá trị mặc định là `false`.
* Httponly: Xác định cookies có được thông qua Javascripts hay không. Nếu được đặt thành `true`, cookies sẽ không thể được truy cập bằng cách sử dụng Javascripts. Điều này giúp bảo vệ cookies khỏi các cuộc tấn công Cross-site Scripting(XSS). Giá trị mặc định là `false`.
* Lấy giá trị cookies:



* Xóa cookies:



* Lưu cookies:



**Câu 4:**

Sessions là gì?

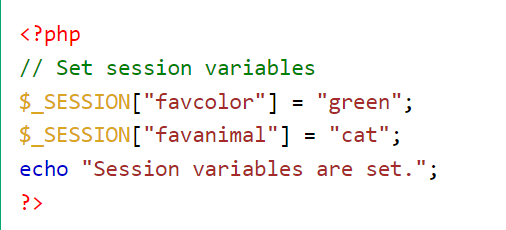
Sessions là một cách lưu trữ thông tin (theo biến) để sử dụng trên nhiều trang.

Không giống như cookie, thông tin không được lưu trữ trên máy tính của người dùng.

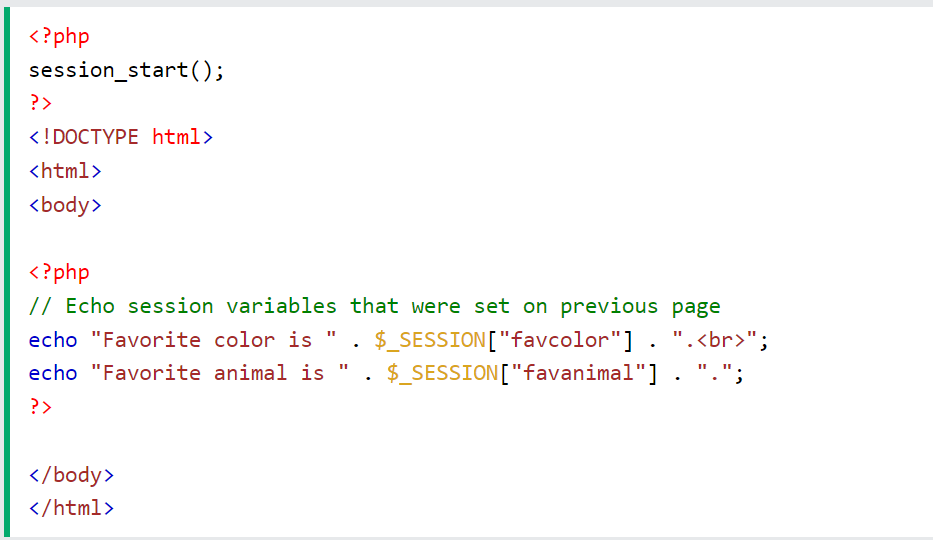
 Trên internet có một vấn đề: máy chủ web không biết bạn là ai hoặc bạn làm gì, vì địa chỉ HTTP không duy trì trạng thái.

Biến sessions giải quyết vấn đề này bằng cách lưu trữ thông tin người dùng sẽ được sử dụng trên nhiều trang (ví dụ: tên người dùng, màu yêu thích, v.v.). Theo mặc định, các biến sessions kéo dài cho đến khi người dùng đóng trình duyệt.

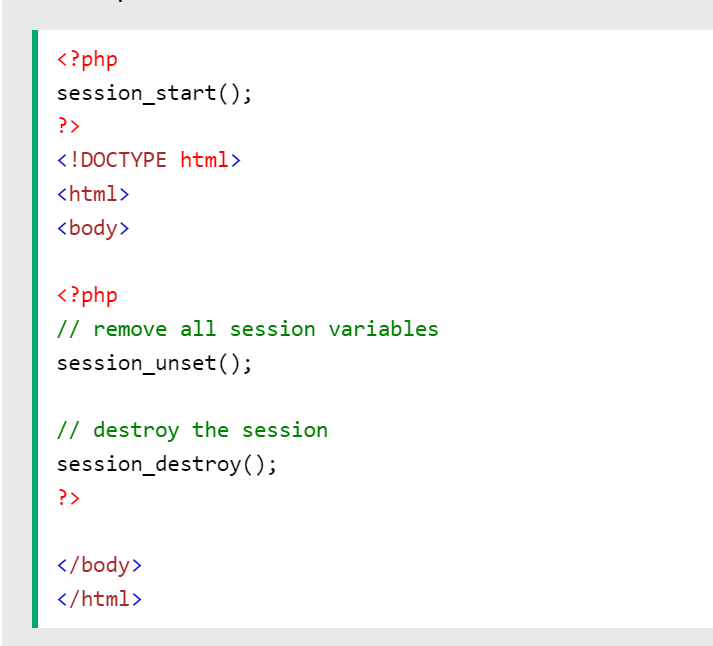
* Lưu sessions:



* Lấy giá trị sessions:



* Xóa sessions:

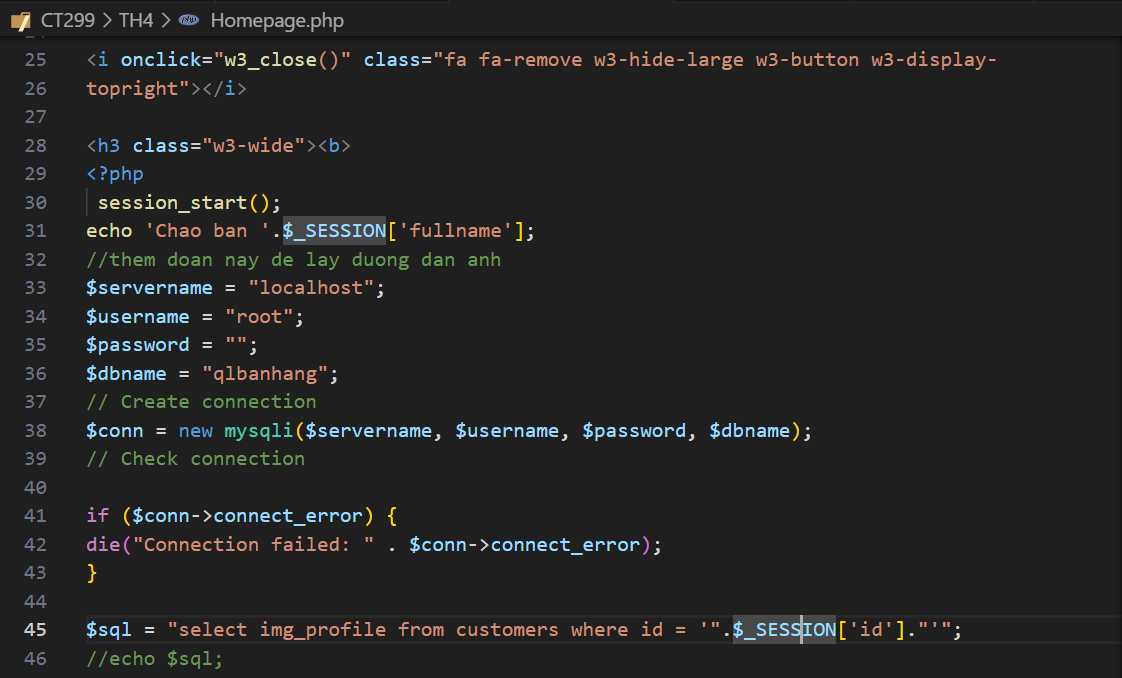


**Câu 5: So sánh giữa Cookies và Sessions [[2]](#footnote-2)**

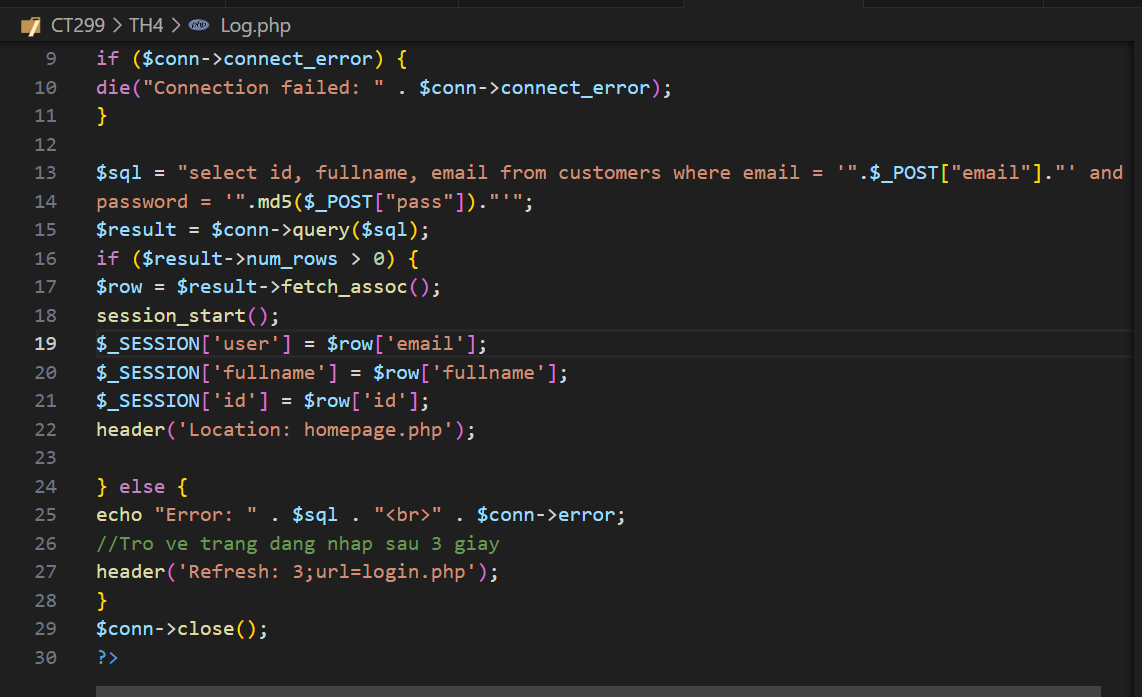


**Câu 6:**

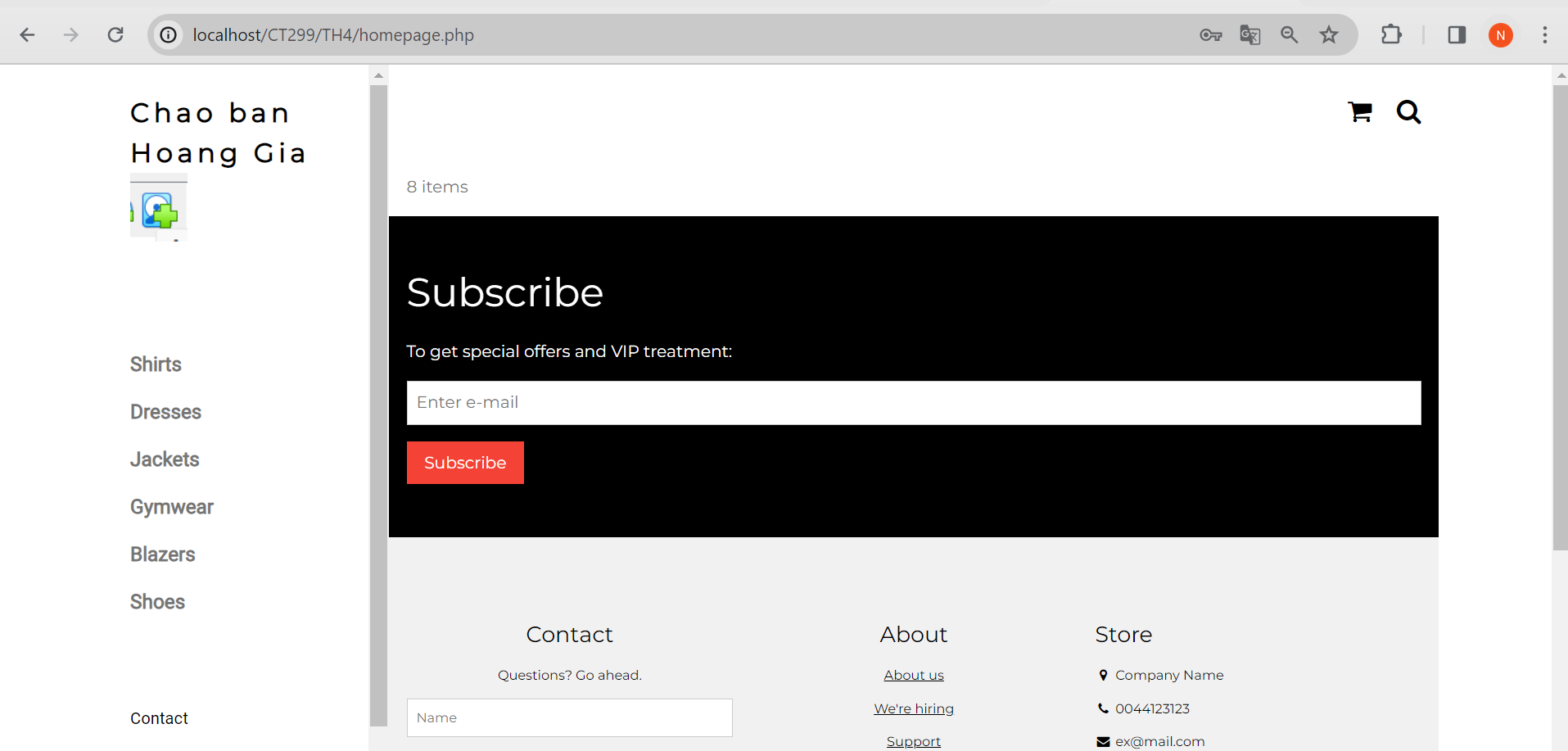
* Homepage.php ( sửa từ cookies thành sessions )



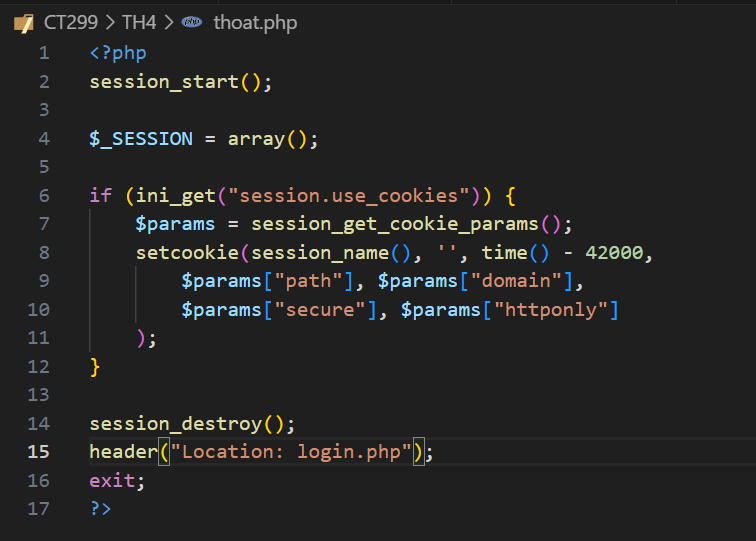
* Log.php ( sửa từ cookies sang sessions)



* Đăng nhập thử

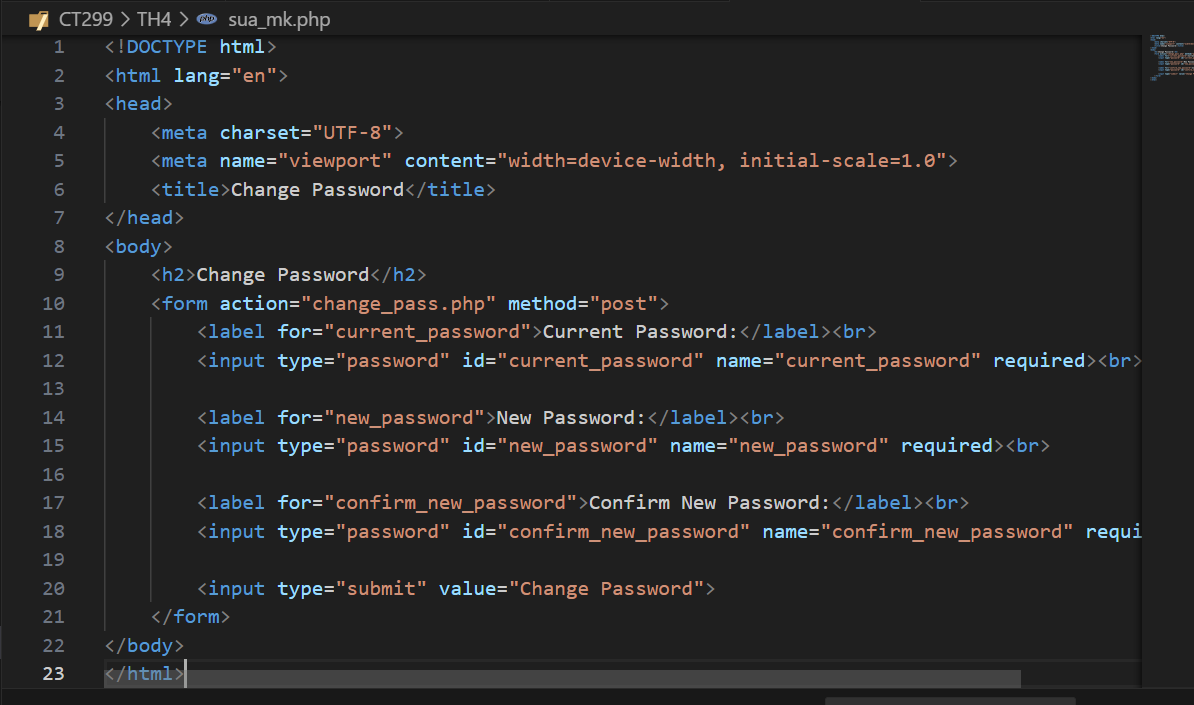


* Thoat.php

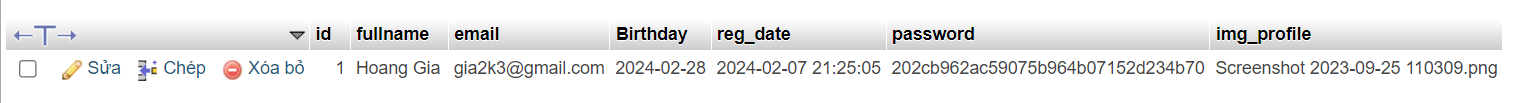


**Câu 7:**

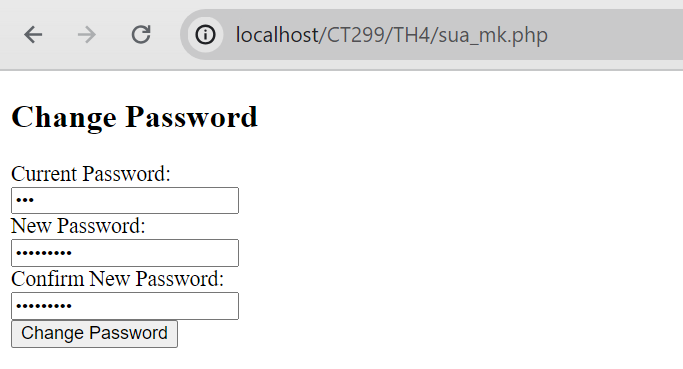
* Tạo sua\_mk.php

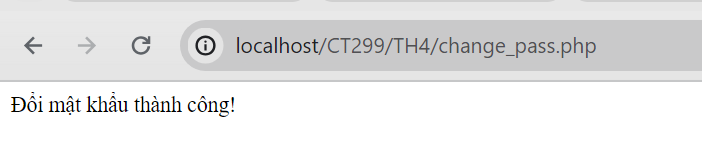


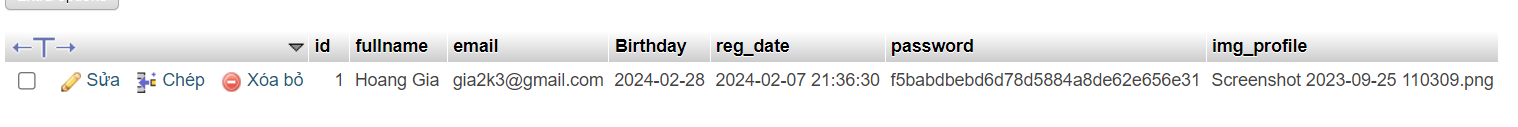
* Change\_pass.php
* <?php
* $servername = "localhost";
* $username = "root";
* $password = "";
* $dbname = "qlbanhang";
* $conn = new mysqli($servername, $username, $password, $dbname);
* if ($conn->connect\_error) {
* die("Kết nối đến cơ sở dữ liệu thất bại: " . $conn->connect\_error);
* }
* if ($\_SERVER["REQUEST\_METHOD"] == "POST") {
* $current\_password = md5($\_POST['current\_password']);
* $new\_password = md5($\_POST['new\_password']);
* $confirm\_new\_password = md5($\_POST['confirm\_new\_password']);
* session\_start();
* $username = $\_SESSION['fullname'];
* $sql = "SELECT password FROM customers WHERE fullname='$username'";
* $result = $conn->query($sql);
* if ($result->num\_rows > 0) {
* $row = $result->fetch\_assoc();
* $current\_password\_db = $row["password"];
* if ($current\_password !== $current\_password\_db) {
* echo "Mật khẩu hiện tại không chính xác.";
* } else if ($new\_password === $current\_password) {
* echo "Mật khẩu mới không được giống mật khẩu cũ.";
* } else if ($new\_password !== $confirm\_new\_password) {
* echo "Mật khẩu mới và xác nhận mật khẩu mới không khớp.";
* } else {
* $update\_sql = "UPDATE customers SET password='$new\_password' WHERE fullname='$username'";
* if ($conn->query($update\_sql) === TRUE) {
* echo "Đổi mật khẩu thành công!";
* } else {
* echo "Lỗi khi cập nhật mật khẩu: " . $conn->error;
* }
* }
* } else {
* echo "Không tìm thấy người dùng với tên người dùng này trong cơ sở dữ liệu.";
* }
* }
* $conn->close();
* ?>
* Mật khẩu ban đầu:



* Mật khẩu sau khi thay đổi:





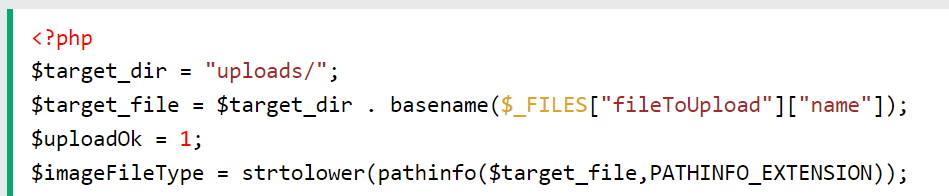


**Câu 8:**

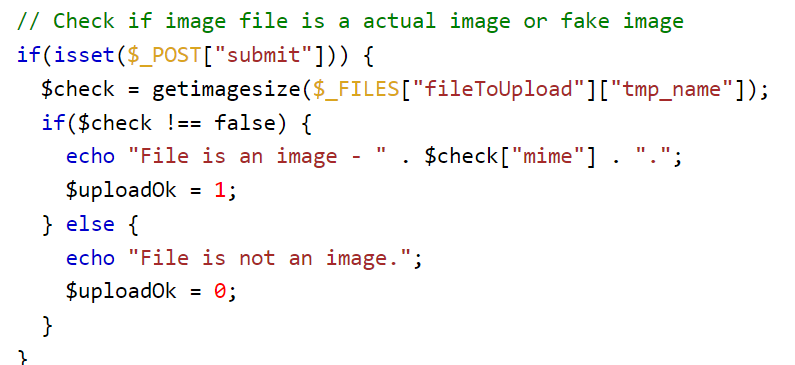
* Tạo biểu mẫu HTML



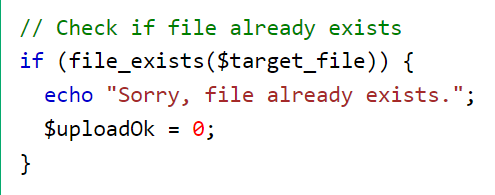
* Tệp "upload.php" chứa mã để tải tệp lên:



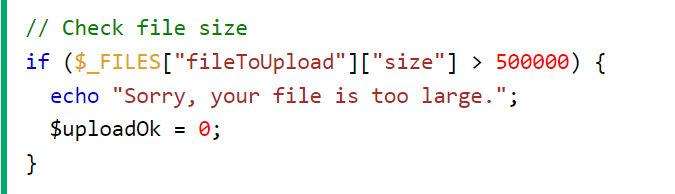
* Kiểm tra file ảnh là ảnh thật hay ảnh giả:



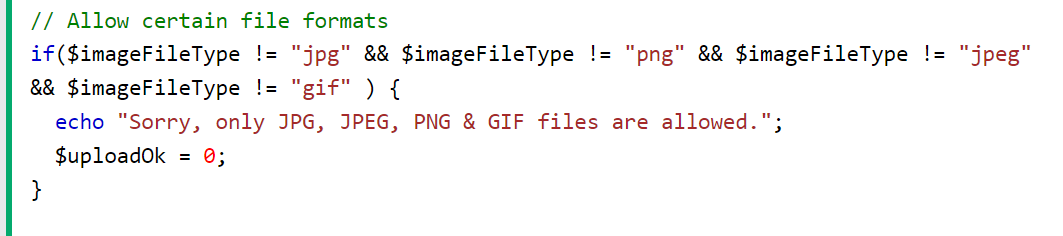
* Kiểm tra xem tệp đã tồn tại chưa:



* Giới hạn kích thước file:



* Giới hạn loại file:



* Kiểm tra file có tải lên được hay không:



**Câu 9:**

Cú pháp:

file(*filename*, *flag*, *context*)

* Filename: chỉ định đường dẫn đến file cần đọc.
* Flag: Không bắt buộc. có thể là một trong nhiều hằng số sau:

+ FILE\_USE\_INCLUDE\_PATH: Tìm kiếm file trong include\_path

+ FILE\_IGNORE\_NEW\_LINES: Bỏ qua dòng mới ở cuối phần tử mảng

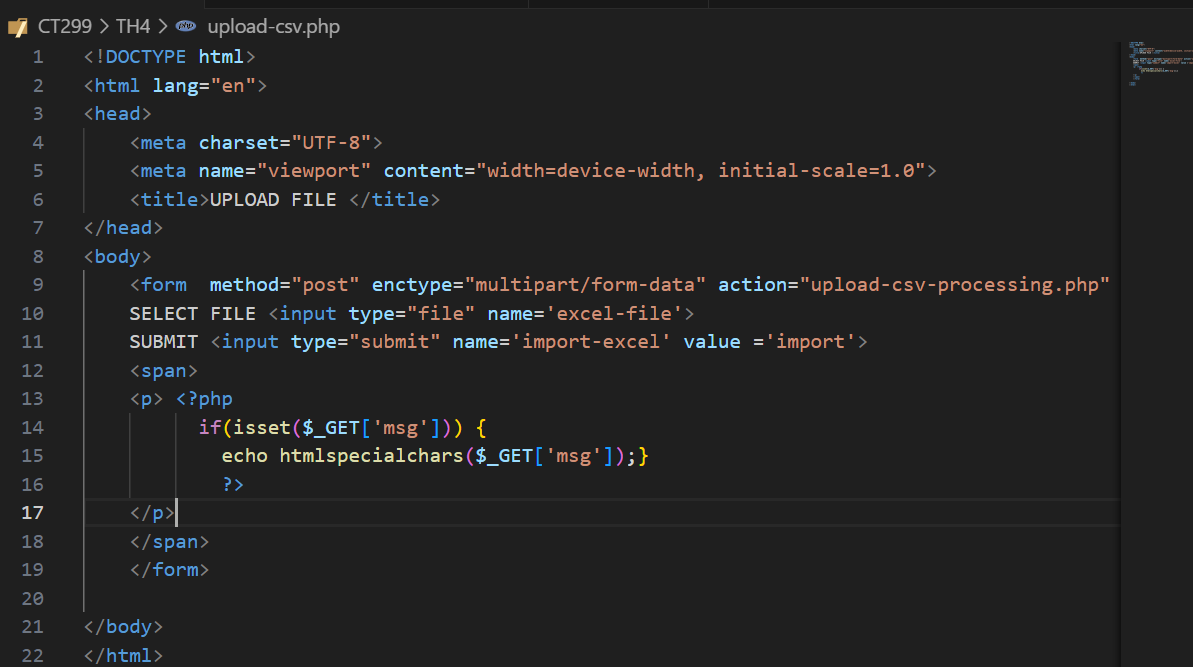
+ FILE\_SKIP\_EMPTY\_LINES: Bỏ qua các dòng trống trong file

* Context: Không bắt buộc. Chỉ định ngữ cảnh xử lí file. Ngữ cảnh là tập hợp các tùy chọn có thể sửa đổi hành vi của luồng. Có thể bỏ qua bằng cách sử dụng NULL.

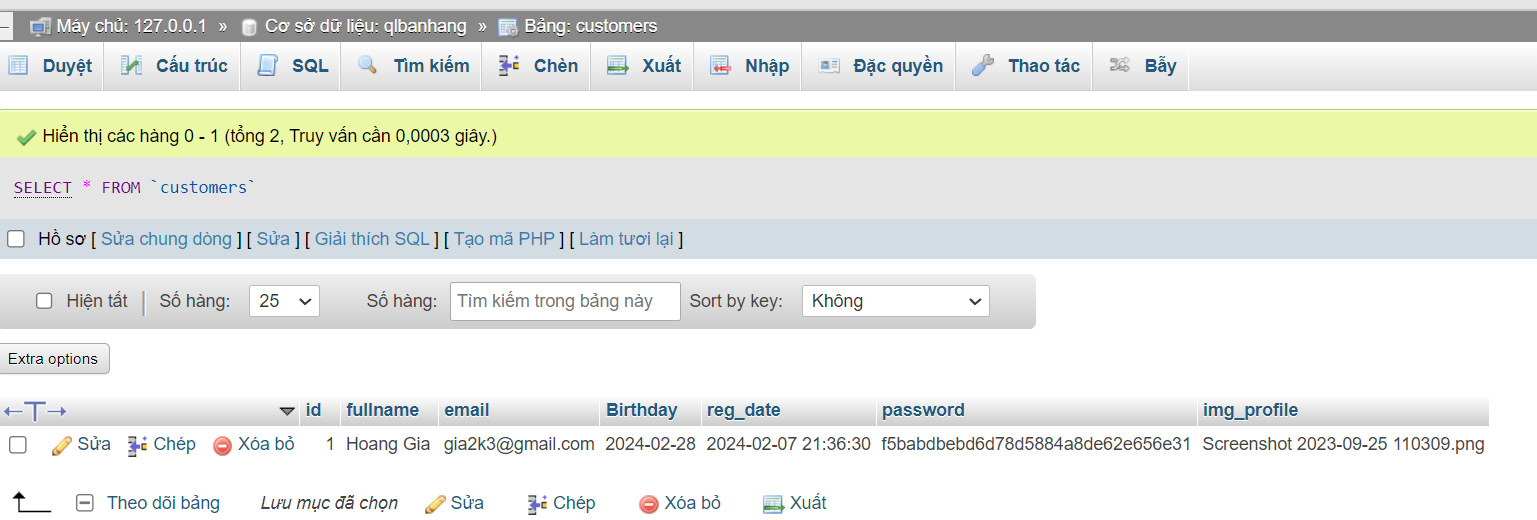
Hàm này sẽ trả về một mảng chứa nội dung của tệp tin. Mỗi phần tử trong mảng sẽ là một dòng trong tệp tin. Nếu có lỗi xảy ra trong quá trình đọc tệp tin, hàm sẽ trả về `false`.

**Câu 10:**

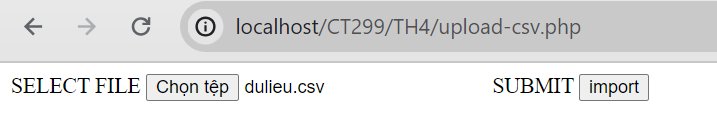
* Upload-csv.php

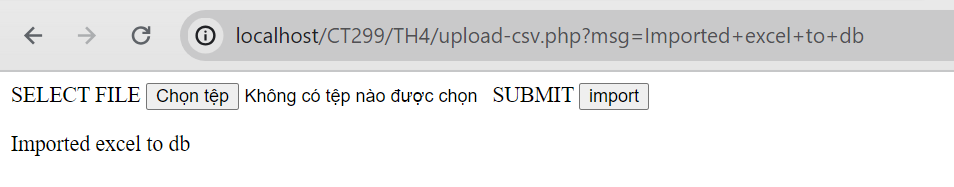


* Dữ liệu ban đầu:

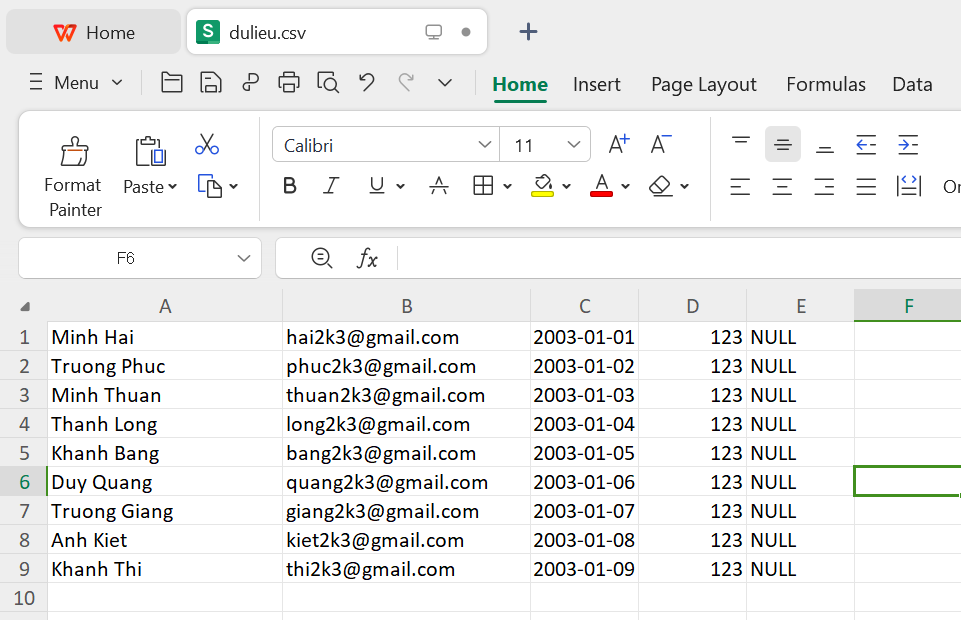


* Upload file:

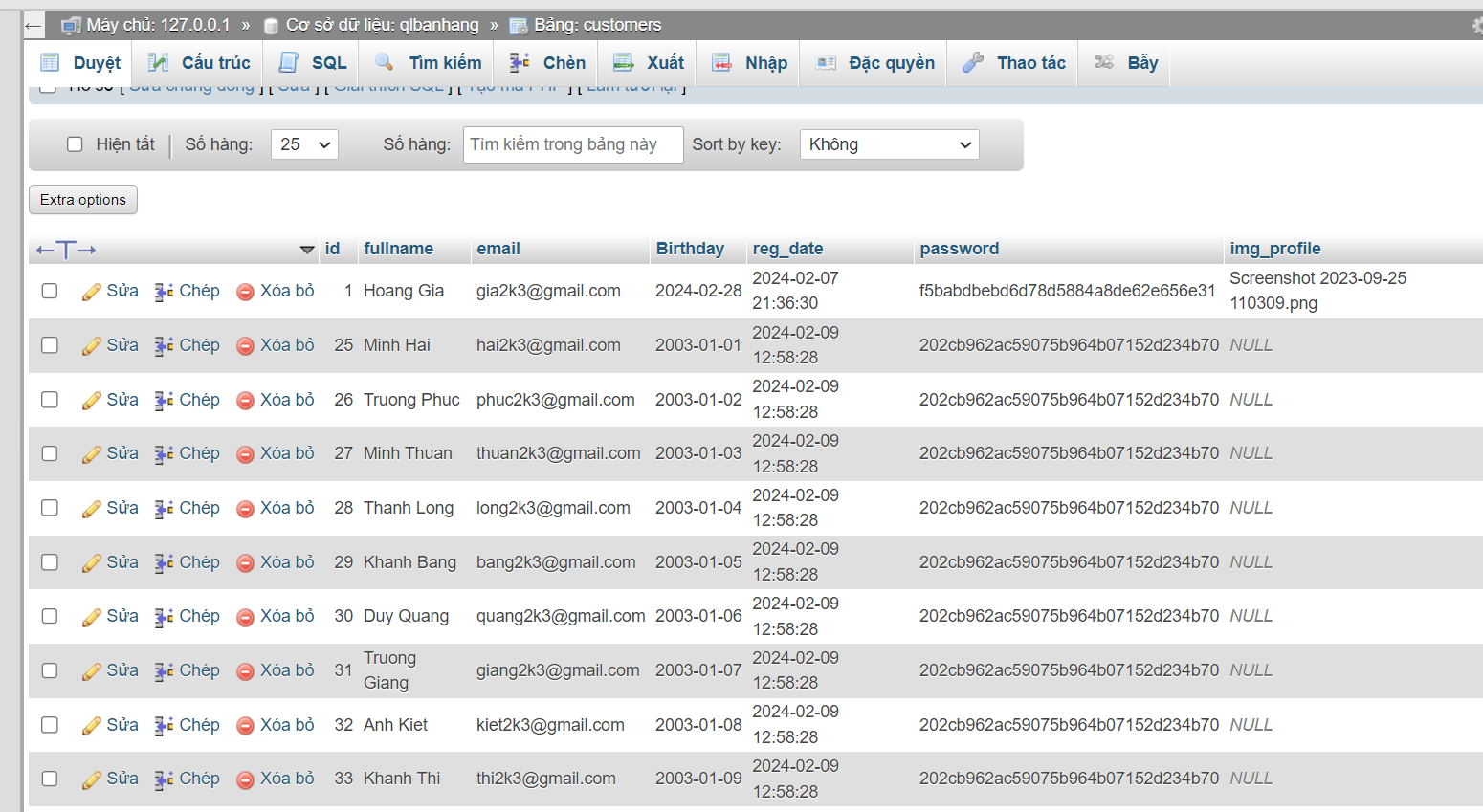




* Upload-csv-processing.php
* <?php
* include 'connect.php';
* require 'vendor/autoload.php';
* use PhpOffice\PhpSpreadsheet\Spreadsheet;
* use PhpOffice\PhpSpreadsheet\Writer\Xlsx;
* if(isset($\_REQUEST['import-excel'])){
* $file = $\_FILES['excel-file']['tmp\_name'];
* $extension = pathinfo($\_FILES['excel-file']['name'],PATHINFO\_EXTENSION);
* if($extension == 'xlsx' || $extension == 'xls' || $extension == 'csv'){
* $obj = PhpOffice\PhpSpreadsheet\IOFACTORY::load($file);
* $data = $obj->getActiveSheet()->toArray();
* foreach($data as $row){
* $name = $row['0'];
* $email = $row['1'];
* $Birthday = $row['2'];
* $password = $row['3'];
* $insert\_query =mysqli\_query($conn, "INSERT INTO customers set fullname = '$name', email='$email',Birthday='$Birthday', password= '".md5($password)."'");
* if($insert\_query){
* $msg = 'Imported excel to db';
* }
* else {
* $msg = 'Not imported';
* }
* }
* }
* else {
* $msg = 'Invalid file';
* }
* header('Location: upload-csv.php?msg=' . urlencode($msg));
* exit();
* }
* ?>
* File CSV:



* Dữ liệu của table custormers sau khi đọc file:



1. https://viblo.asia/p/sql-injection-la-gi-co-bao-nhieu-kieu-tan-cong-sql-injection-m68Z0QnMlkG [↑](#footnote-ref-1)
2. https://viblo.asia/p/cookie-va-session-07LKXEvEZV4 [↑](#footnote-ref-2)