**BÀI THỰC HÀNH 4**

**YÊU CẦU BÀI THỰC HÀNH**

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

**ck.php**

<!DOCTYPE html>

<?php

    $cookie\_name = "user";

    $cookie\_value = "Phung Cao My Quynh";

    setcookie($cookie\_name, $cookie\_value, time() + (86400 / 24), "/"); // 86400 = 24\*3600 = 1 day

?>

<html>

    <body>

        <?php

            if(!isset($\_COOKIE[$cookie\_name])) {

                echo "Cookie named '" . $cookie\_name . "' chua duoc thiet lap, ban vui long bam f5 de thiet lap cookie!";

            }else{

                    echo "Cookie '" . $cookie\_name . "' da duoc thiet lap!<br>";

                    echo "Gia tri la: " . $\_COOKIE[$cookie\_name];

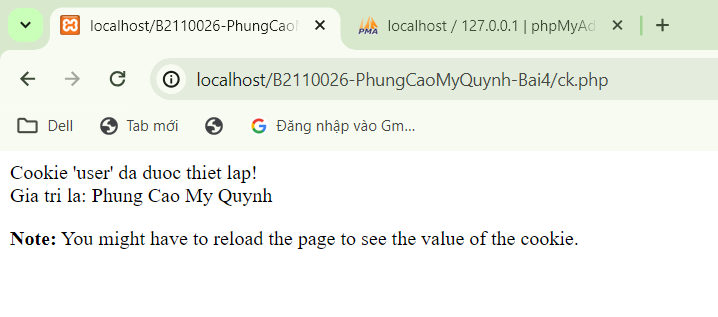
                }

        ?>

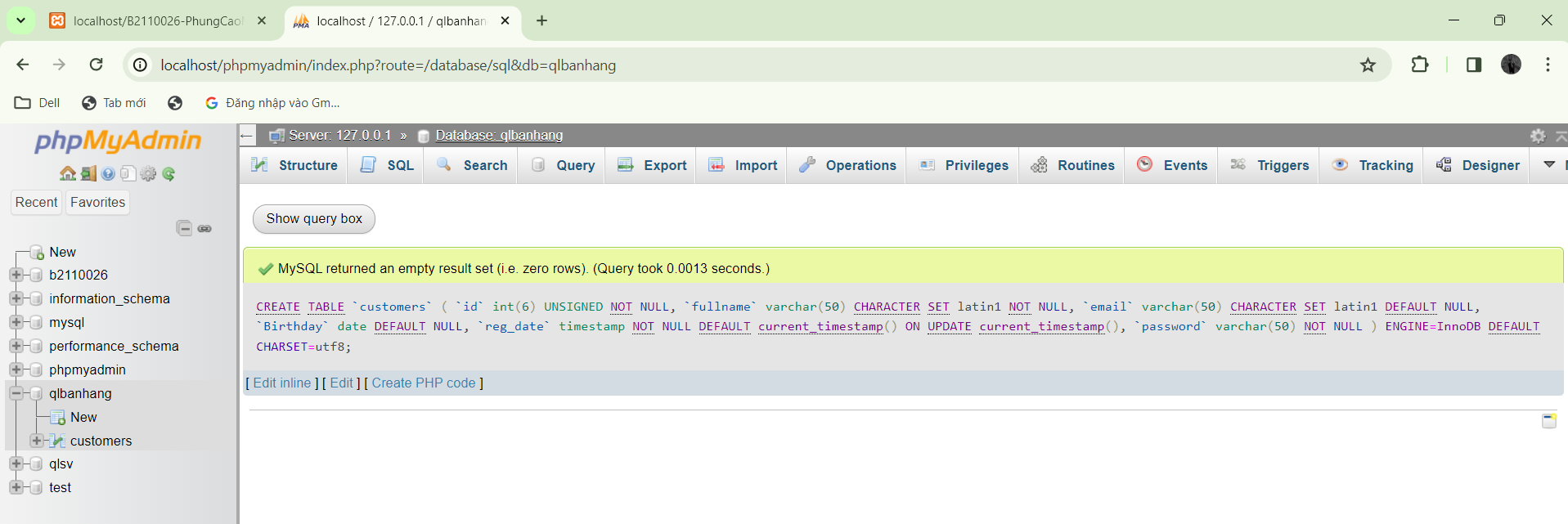
    <p><strong>Note:</strong> You might have to reload the page to see the value of the cookie.</p>

</body>

</html>

****

**Tạo csdl qlbanhang, với bảng customers đầu tiên như sau:**

****

**formnhap.php**

<!DOCTYPE HTML>

<html>

<body>

    <form action="luu.php" method="post">

        Name: <input type="text" name="name"><br>

        E-mail: <input type="text" name="email"><br>

        Birthday: <input type="date" name="birth"><br>

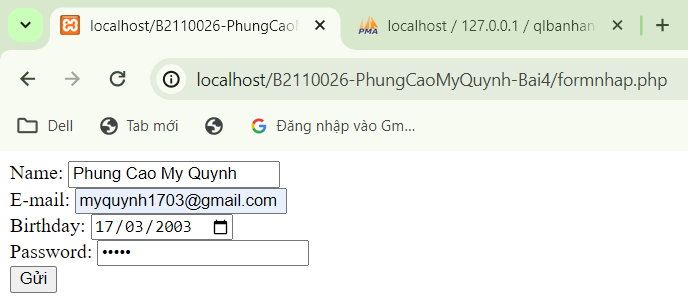
        Password: <input type="password" name="pass"><br>

        <input type="submit">

    </form>

</body>

</html>

****

**luu.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);

}

$date = date\_create($\_POST["birth"]);

$sql = "INSERT INTO customers (fullname, email, birthday, password)

VALUES ('".$\_POST["name"] ."', '".$\_POST["email"] ."', '".$date ->format('Y-m-

d') ."','".md5($\_POST["pass"])."' )";

if ($conn->query($sql) == TRUE) {

echo "Them sinh vien thanh cong";

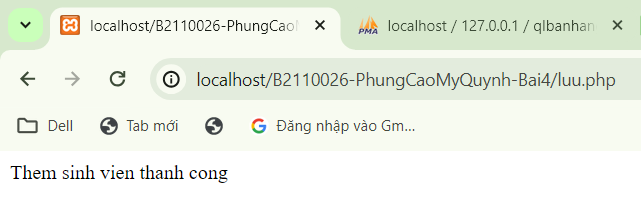
} else {

echo "Error: " . $sql . "<br>" . $conn->error;

}

$conn->close();

?>

****

**login.php**

<!DOCTYPE HTML>

<html>

<body>

    <form action="log.php" method="post">

        Username: <input type="text" name="email"><br>

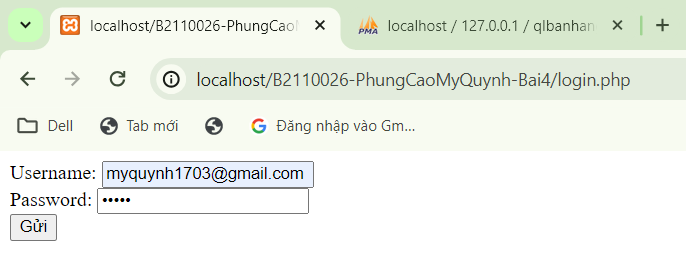
        Password: <input type="password" name="pass"><br>

        <input type="submit">

    </form>

</body>

</html>



**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);

}

$sql = "select fullname, email from customers where email = '".$\_POST["email"]."' and

password = '".md5($\_POST["pass"])."'";

$result = $conn->query($sql);

if ($result->num\_rows > 0) {

echo "Dang nhap thanh cong <br>";

$row = $result->fetch\_assoc();

echo "email:".$row['email']. ' Fullname: '.$row['fullname'];

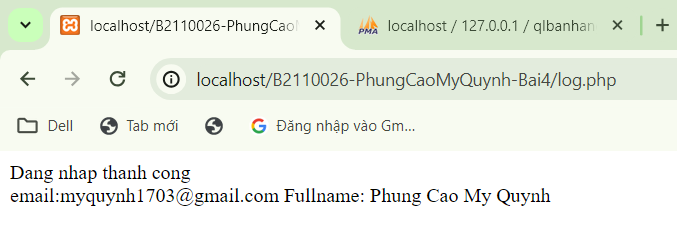
} else {

echo "Error: " . $sql . "<br>" . $conn->error;

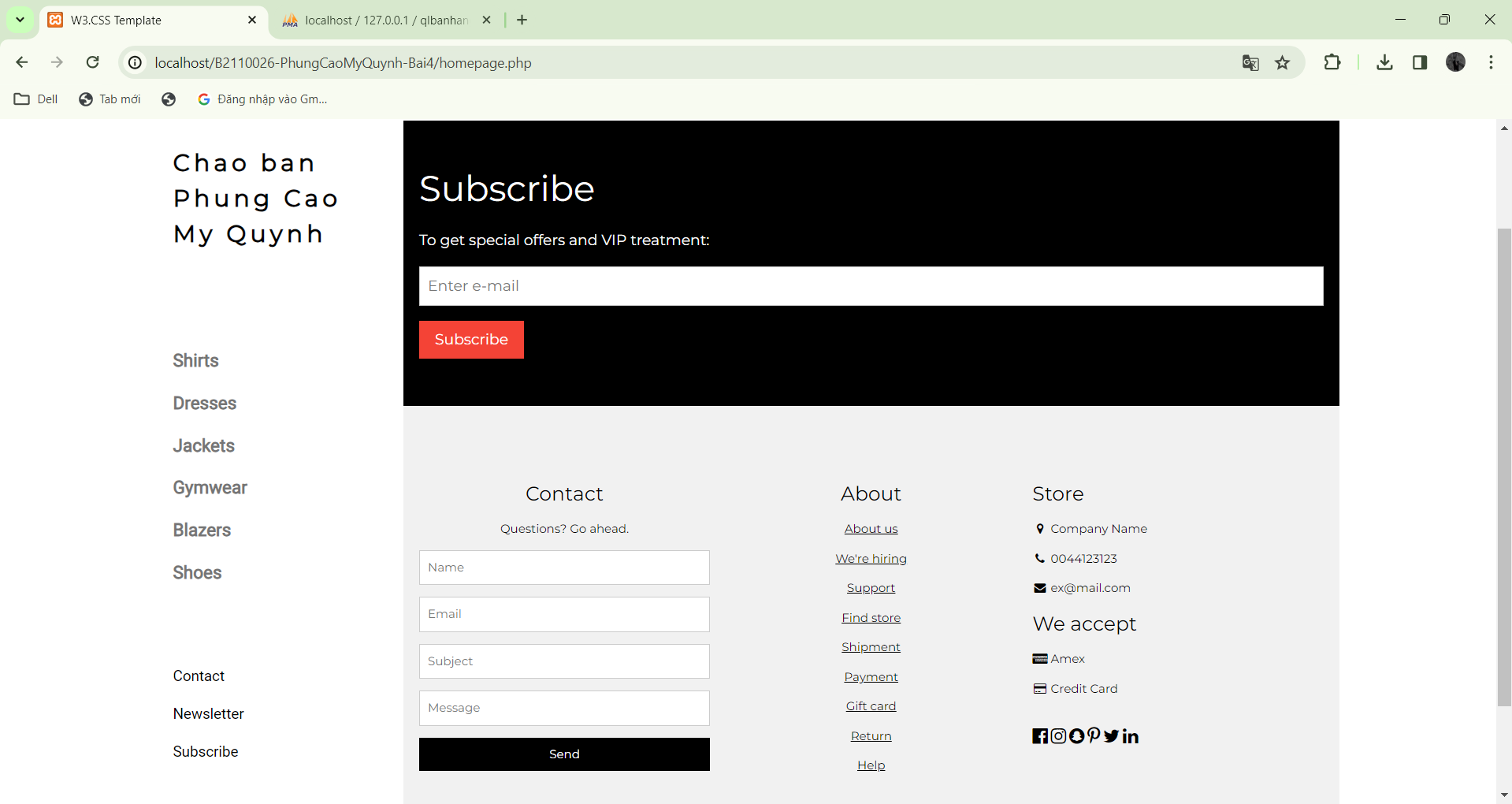
}

$conn->close();

?>



**homepage.php**

****

**upload\_img.php**

<!DOCTYPE html>

<html>

<body>

    <form action="upload.php" method="post" enctype="multipart/form-data">

        Ban chon 1 anh de lam profile:

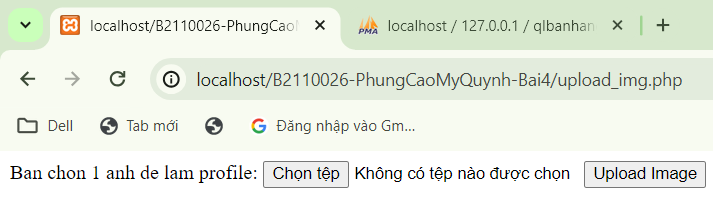
        <input type="file" name="fileToUpload" id="fileToUpload">

        <input type="submit" value="Upload Image" name="submit">

    </form>

</body>

</html>



**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.";

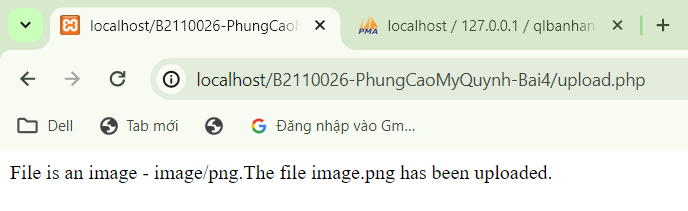
} else {

echo "Sorry, there was an error uploading your file.";

}

}

?>

****

**upload\_csdl.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.";

echo '<br>';

$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);

}

$id = $\_COOKIE['id'];

$sql = "UPDATE customers set img\_profile = '".$\_FILES["fileToUpload"]["name"]."'";

$sql = $sql. " WHERE ID='".$id."'";

echo $sql;

if ($conn->query($sql) == TRUE) {

echo 'cap nhat csdl thanh cong!<br>';

echo '<a href="homepage.php">Trang chu</a>';

} else {

echo "Error: " . $sql . "<br>" . $conn->error;

}

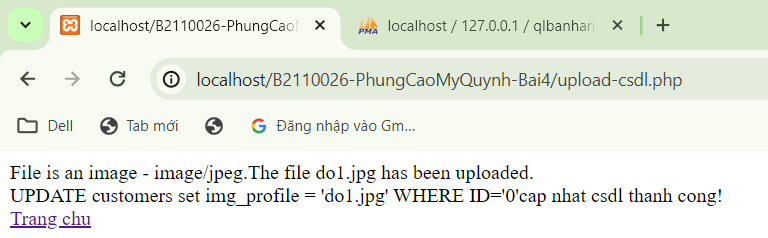
} else {

echo "Sorry, there was an error uploading your file.";

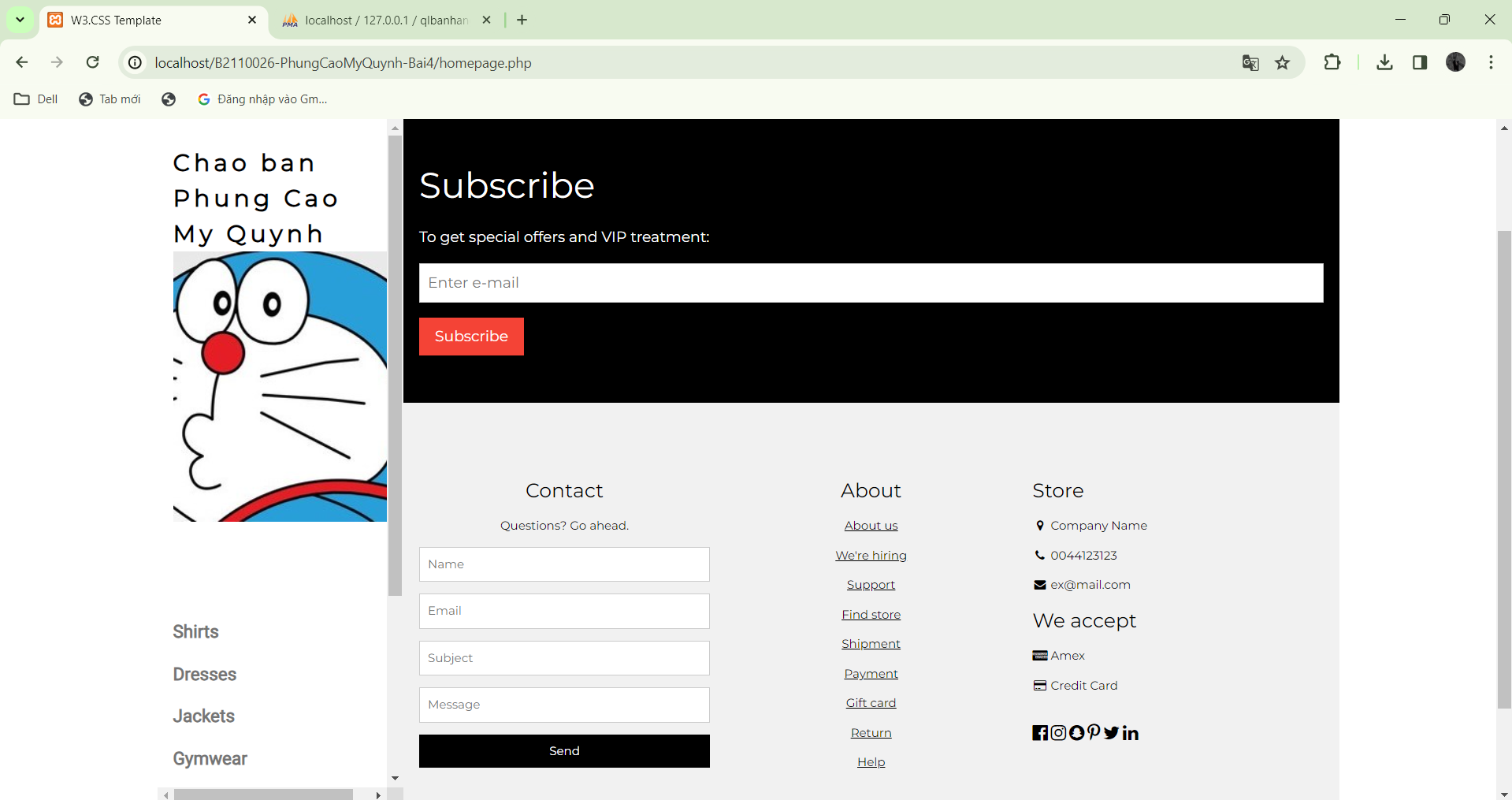
}

}

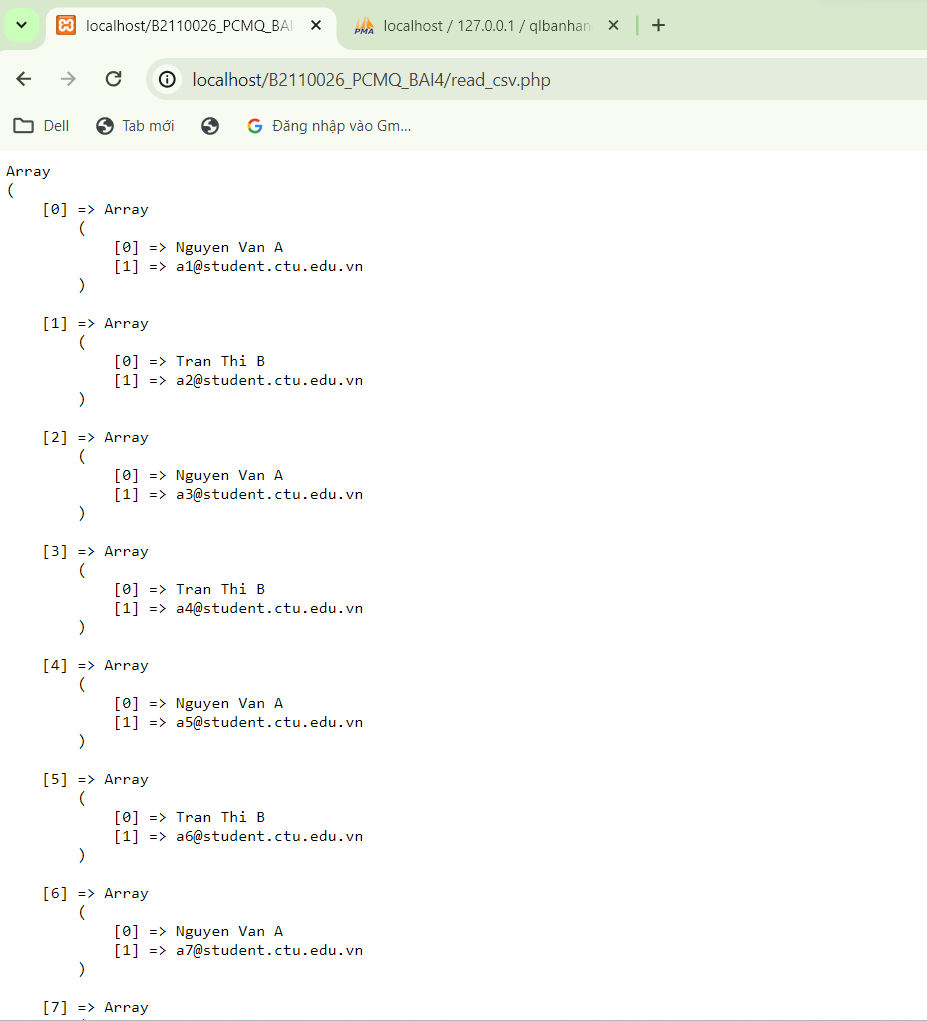
?>



**homepage.php (modified với ảnh profile)**

****

**read\_csv.php**

****

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. Ứng dụng kỹ thuật đó vào trang đăng nhập mà bạn đã tạo, chụp lại các kết quả.**

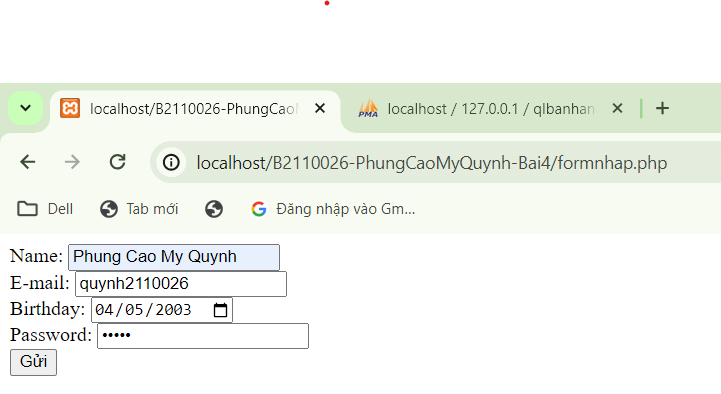
* SQL Injection là một kỹ thuật tấn công phổ biến trong lập trình web, trong đó kẻ tấn công chèn các đoạn mã SQL bất hợp pháp vào các truy vấn SQL được tạo bởi ứng dụng web. Khi ứng dụng không kiểm tra hoặc xác nhận đầu vào của người dùng đúng cách, hacker có thể chèn các câu lệnh SQL độc hại vào các trường dữ liệu của form và thực hiện các hành động không được phép như truy xuất, sửa đổi, xóa dữ liệu hoặc thậm chí là kiểm soát toàn bộ hệ thống.
* Các ví dụ:
* Sử dụng câu lệnh SQL Injection để xóa bảng:

**$sql = "SELECT id, firstname, lastname FROM MyGuests WHERE lastname = 'Doe'";**

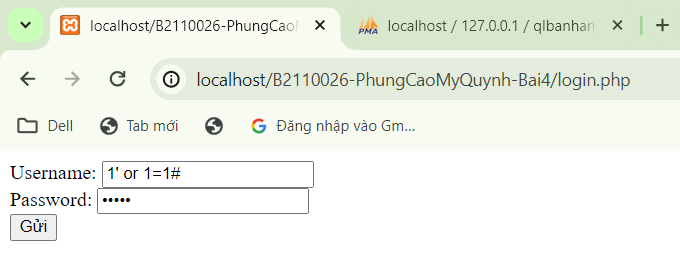
* Sử dụng câu lệnh SQL Injection để truy xuất dữ liệu bảng nhật ký đăng nhập:

**$sql = "SELECT id, username FROM users WHERE username = '$username' AND password = '$password'";**

* Ứng dụng vào trang đăng nhập (với email = ‘quynh2110026’ , pass =’12345’)

****

* Đăng nhập vào trang login với mật khẩu bất kỳ cùng key “1’ or 1=1 #”

****

1. **Dựa vào link2, 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 phần nhỏ dữ liệu được lưu trữ trên máy tính của người dùng bởi trình duyệt web. Cookie được sử dụng để lưu trữ thông tin về người dùng và sử dụng nó trong các yêu cầu sau này, giúp website nhận biết và theo dõi người dùng.
* Ý nghĩa các tham số trong setcookie():

**name**: Tên của cookie

**value**: Giá trị của cookie

**expire**: Thời gian hết hạn của cookie, được biểu diễn dưới dạng timestamp. Nếu không được cung cấp, cookie sẽ hết hạn khi trình duyệt đóng.

**part:** Đường dẫn của cookie. Cookie sẽ chỉ được gửi đến các trang trong đường dẫn này.

**domain:** Miền của cookie. Cookie sẽ chỉ được gửi đến miền này

secure: Xác định liệu cookie có chỉ được gửi qua kết nối an toàn (HTTPS) hay không

**httponly**: Đặt cookie như một “HTTTP only” cookie, không thể được truy cập bằng JavaScript. Điều này giúp ngăn chặn các cuộc tấn công Cross-Site Scripting (XSS).

* Cách lưu, lấy, xóa giá trị trong cookie

Lưu giá trị trong cookie

**setcookie("user", "", time() + 3600, "/");**

Lấy giá trị trong cookie

**$user = $\_COOKIE[‘user’];**

**echo “Welcome $user!”;**

Xóa giá trị trong cookie

**setcookie("user", "", time() - 3600, "/");**

1. **Dựa vào link3, bạn hãy cho biết Session dùng để làm gì. Cách lưu, lấy, xóa giá trị trong Session.**

* Session là một cách để lưu trữ thông tin phiên làm việc của người dùng trên máy chủ. Mỗi phiên làm việc có một ID duy nhất được gắn với nó, và thông tin trong session này có thể được lưu trữ và truy cập trong suốt phiên làm việc đó
* Cách lưu giá trị trong session: Để lưu giá trị trong session sử dụng hàm

**`$\_SESSION [‘key’] = value;`**

* Cách lấy giá trị trong session, ta chỉ cần truy cập vào khóa tương ứng trong mảng **`$\_SESSION`**
* Cách xóa giá trị trong session: Để xóa giá trị trong session, bạn có thể sủ dụng hàm `unset()` hoặc hàm `session\_unset()`

1. **Bạn hãy so sánh Cookie và Session.**

* **Bản chất:**
* **Cookie:** là một dạng dữ liệu được lưu trữ trên máy tính của người dùng dưới dạng văn bản thông qua trình duyệt web. Cookie được gửi từ máy chủ đến trình duyệt và được lưu trữ tại đó.
* **Session:** là một cách để lưu trữ thông tin trên máy chủ. Mỗi phiên làm việc của người dùng được gắn với một ID phiên duy nhất, và thông tin trong session được lưu trữ trên máy chủ.
* **Thời gian lưu trữ**
* **Cookie:** có thể được lưu trữ trong một khoảng thời gian cụ thể, xác định bởi thời gian sống của cookie hoặc cho đến khi người dùng xóa cookie hoặc hết hạn.
* **Session:** thông tin trong session thường chỉ tồn tại trong suốt phiên làm việc của người dùng. Khi phiên làm việc kết thúc, thông tin trong session sẽ bị xóa.
* **Bảo mật:**
* **Cookie:** dữ liệu trong cookie được lưu trữ trên máy tính của người dùng và có thể bị tiết lộ nếu bị hack. Tuy nhiên, có thể sử dụng các tùy chọn bảo mật như mã hóa để bảo vệ dữ liệu.
* **Session:** thông tin session được lưu trữ trên máy chủ và không bị tiết lộ cho người dùng, điều này làm cho session an toàn hơn so với cookie trong một số trường hợp.
* **Sử dụng:**
* **Cookie:** thường được sử dụng để lưu trữ thông tin như thông tin đăng nhập, tùy chọn người dùng, và các dữ liệu như giỏ hàng trong các trang mua sắm trực tuyến.
* **Session:** thường được sử dụng để lưu trữ thông tin phiên làm việc của người dùng, như thông tin đăng nhập, danh sách sản phẩm được chọn trong một phiên mua sắm, và các thông tin tạm thời khác.
* **Dung lượng lưu trữ:**
* **Cookie:** có giới hạn về dung lượng ( thường khoảng vài KB dến vài MB).
* **Session:** dung lượng lưu trữ phụ thuộc vào cấu hình máy chủ và không có giới hạn cụ thể, nhưng quản trị viên cần cân nhắc để tránh quá tải máy chủ với nhiều thông tin session.

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.**

**Sửa file log.php**

session\_start();

$session\_name = "user";

$session\_value = $row['email'];

$\_SESSION['fullname'] = $row['fullname'];

$\_SESSION['id'] = $row['id'];

$\_SESSION['$session\_name'] = $row['session\_value'];

//

header('Location: homepage.php');

**Sửa file homepage.php**

session\_start();

$session\_name = "fullname";

echo 'Chao ban '.$\_SESSION[$session\_name];





**Tập tin thoat.php**

<?php

    session\_start();

    session\_destroy();

    header('Location: login.php');

?>

1. **Bạn hãy tạo form sua\_mk.php cho phép người dùng chỉnh sửa mật khẩu sau khi đăngnnhập. 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.**

**sua\_mk.php**

<!DOCTYPE HTML>

<html>

    <body>

        <form action="luu\_mk.php" method="post">

            Password: <input type="password" name="pass"><br>

            New Password: <input type="password" name="newpass"><br>

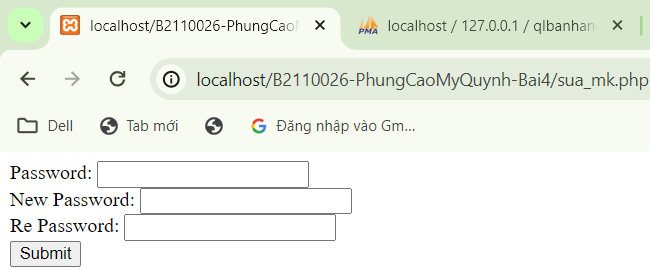
            Re Password: <input type="password" name="newpass2"><br>

            <input type="submit">

        </form>

    </body>

</html>

****

**luu\_mk.php**

<?php

session\_start();

$severname = "localhost";

$username = "root";

$password = "";

$dbname = "qlbanhang";

$id = $\_SESSION['id'];

$conn = new mysqli($severname, $username, $password, $dbname);

if ($conn->connect\_error) {

    die("Connection failed: " . $conn->connect\_error);

}

$sql = "SELECT \* FROM `customers` WHERE `password` = '".md5($\_POST["pass"])."'";

$result = $conn->query($sql);

if ($result->num\_rows > 0) {

    if ($\_POST["newpass"] != $\_POST["newpass2"]) {

        echo "Error: Passwords do not match";

        header('Refresh: 3;url=sua\_mk.php');

    }else{

        $sql = "UPDATE `customers` SET `password` = '".md5($\_POST["newpass"])."' WHERE id = " .$id;

        $conn->query($sql);

        echo "Success: changed password successfully";

        header('Refresh: 3;url=homepage.php');

    }

}else{

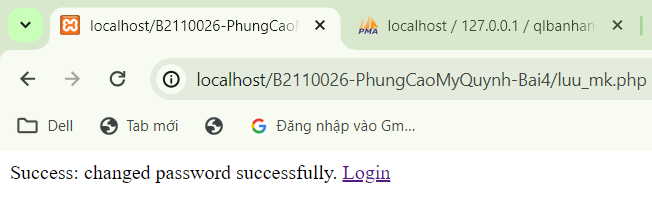
    echo "Error: wrong password!";

    header('Refresh: 3;url=sua\_mk.php');

}

$conn->close();

?>



1. **Bạn đọc trong 4 để tìm hiểu và mô tả các cơ chế, các hàm/thủ tục để thực hiện việc upload.**

* **From HTML:** để cho phép người dùng tải tệp lên, cần sử dụng một mẫu HTML `<from>` với thuộc tính `enctype = “multipart/from-data” `để cho phép tải lên tệp. Ví dụ:

**<form action="upload.php" method="post" enctype="multipart/form-data">**

**Select image to upload:**

**<input type="file" name="fileToUpload" id="fileToUpload">**

**<input type="submit" value="Upload Image" name="submit">**

**</form>**

* **PHP Upload File:** trang web cung cấp một ví dụ về cách thực hiện việc xử lý tệp được tải lên trong PHP. Đoạn mã này bao gồm các bước sau:
* Kiểm tra xem tệp đã được chọn và được tải lên thành công không
* Kiểm tra kích thước của tệp để đảm bảo rằng nó không quá lớn
* Kiểm tra loại tệp đã đảm bảo rằng nó là loại tệp hợp lệ
* Di chuyển tệp từ thư mục tạm thời đến thư mục mục tiêu
* **Hàm PHP cụ thể:**
* ` move\_uploaded\_file() `: được sử dụng để di chuyển tệp tải lên từ thư mục tạm thời sang một vị trí mới. Ví dụ:

**move\_uploaded\_file($\_FILES["fileToUpload"]["tmp\_name"], $target\_file);**

* **Biến siêu toàn cục ` $\_FILES `:** trong PHP, các tệp được tải lên thông qua một mảng gọi là ` $\_FILES `. Trong ví dụ, ` $\_FILES[“fileToUpload”][“tmp\_name”] ` được sử dụng để tham chiếu đến tệp tạm thời đã được tải lên.
* **Xử lý lỗi:** trang web cũng cung cấp một số mã để xử lý lỗi có thể xảy ra trong quá trình tải tệp lên, chẳng hạn như kiểm tra kích thước tệp quá lớn hoặc loại tệp không được phép
* **Bảo mật:** ngoài các hướng dẫn cơ bản, trang web cũng cung cấp một số gợi ý về bảo mật, chẳng hạn như kiểm tra loại tệp và mô phỏng việc tải lên tệp trong một thư mục không công khai.

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

* Mô tả chức năng của một số hàm quan trọng và các tham số tương ứng trong hàm đó:
* **` file\_exists($filename) `** : Kiểm tra xem một tập tin có tồn tại hay không

- **` $filename `** : Tên hoặc đường dẫn tới tệp tin cần kiểm tra

- Trả về ` true ` nếu tập tin tồn tại, ngược lại trả về ` false `

* **` is\_file($filename) `** : Kiểm tra xem một tệp tin có phải là một tệp tin hay không

- **` $filename `** : Tên hoặc đường dẫn tới tệp tin cần kiểm tra

- Trả về ` true ` nếu tập tin tồn tại, ngược lại trả về ` false `

* **` file\_get\_contents($filename) `** : Đọc nội dung của một tệp tin và trả về dưới dạng một chuỗi

- **` $filename `** : Tên hoặc đường dẫn tới tệp tin cần đọc

- Trả về nội dung của tệp tin dưới dạng chuỗi, hoặc` false ` nếu có lỗi xảy ra

* **` fopen($filename, $mode) `** : Mở một tệp tin hoặc URL

- **` $filename `:** Tên hoặc đường dẫn tới tệp tin cần mở

- ` $mode ` : Chế độ mở tệp tin, ví dụ “r” (mở tệp tin chỉ để đọc), “w” (mở tập tin để ghi, xóa nội dung cũ), “a” (mở tệp tin để ghi, giữ nội dung cũ).

- Trả về một con trỏ tệp tin (file pointer) hoặc ` false ` nếu có lỗi xảy ra

* **` fgets($file) ` và ` fgetcsv($file) `** : Đọc một dòng từ tệp tin

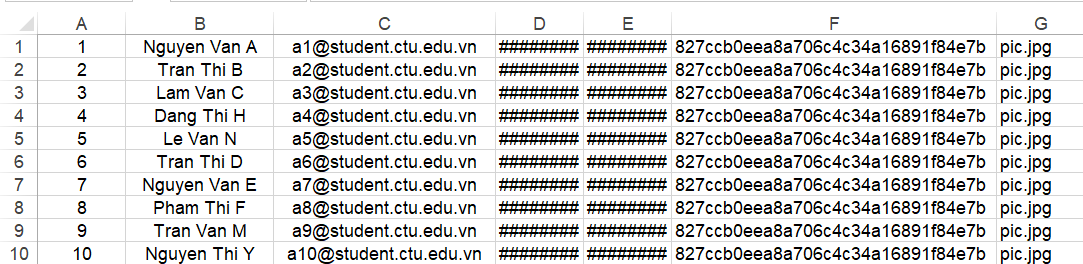
- ` $file ` : con trỏ tệp tin trả về từ hàm ` fopen() `

- ` fgets($file) ` : Đọc một dòng từ tệp tin và trả về dưới dạng một chuỗi

- ` fgetcsv($file) ` : Đọc một dòng từ tệp tin và trả về dưới dạng một mảng chứa các giá trị được phân tách bằng dấu phẩy ( dùng cho đọc tệp tin CSV ) .

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.**

**Tạo file csv ít nhất 10 dòng dữ liệu**

****

**upload\_csv.php**

<!DOCTYPE html>

<html>

<body>

    <form action="upload-csv-processing.php" method="post" enctype="multipart/form-data">

        Ban chon 1 file csv de upload:

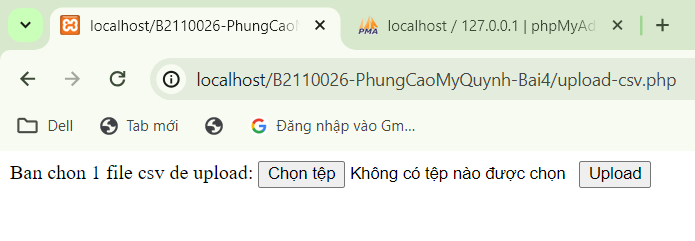
        <input type="file" name="csv\_file">

        <input type="submit" value="Upload">

    </form>

</body>

</html>



**upload\_csv\_processing.php**

<?php

if ($\_SERVER["REQUEST\_METHOD"] == "POST" ) {

    if (isset($\_FILES["csv\_file"]) && $\_FILES["csv\_file"][error] == UPLOAD\_ERR\_OK) {

        $csv\_file = $\_FILES["csv\_file"]["tmp\_name"];

        $file\_info = pathinfo($\_FILES["csv\_file"]["name"]);

        //

        if (strtolower($file\_info["extension"]) == "csv") {

            //

            $csv = array();

            $lines = file($csv\_file, FILE\_IGNORE\_NEW\_LINES);

            foreach ($lines as $key => $value) {

                $csv[$key] = str\_getcsv($value);

            }

            //

            $servername = "localhost";

            $username = "root";

            $password = "";

            $dbname = "qlbanhang";

            $conn = new mysqli($servername, $username, $password, $dbname);

            if ($conn->connect\_error) {

                die ("Connection failed: " . $conn->connect\_error);

            }

            //

            foreach ($csv as $row) {

                $column1 = $row[0];

                $column2 = $row[1];

                $column3 = $row[2];

                $column4 = $row[3];

                $column5 = $row[4];

                $column6 = $row[5];

                $column7 = $row[6];

                $sql = "INSERT INTO customers (id , fullname , email , Birthday, reg\_date , password, img\_profile)

                VALUES ('$column1', '$column2', '$column3', '$column4', '$column5', '$column6', '$column7')";

                if ($conn->query($sql) === TRUE) {

                    echo "Inserted data: $column1, $column2, $column3, $column4, $column5, $column6, $column7<br>";

                }else {

                    echo "Error inserting data: " . $conn->error . "<br> ";

                }

            }

            $conn->close();

        }else {

            echo "Only CSV files are allowed";

        }

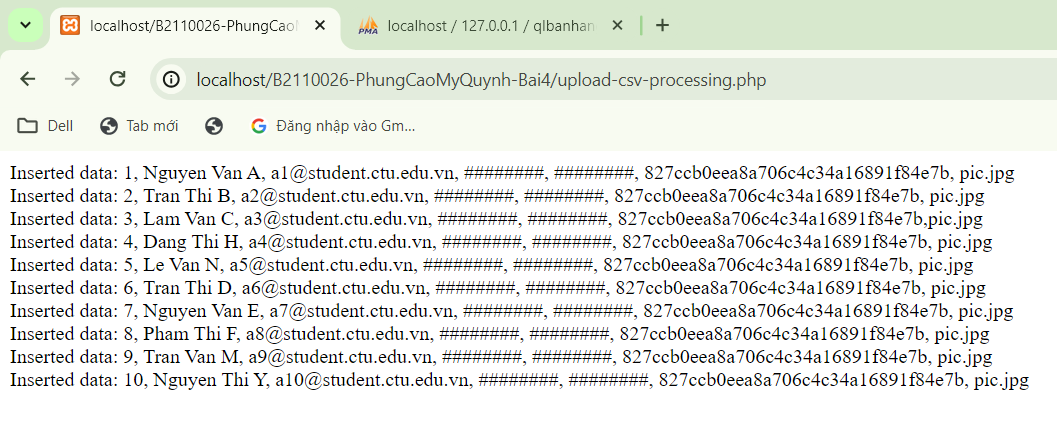
    }else {

        echo "Error uploading file.";

    }

}

?>

****