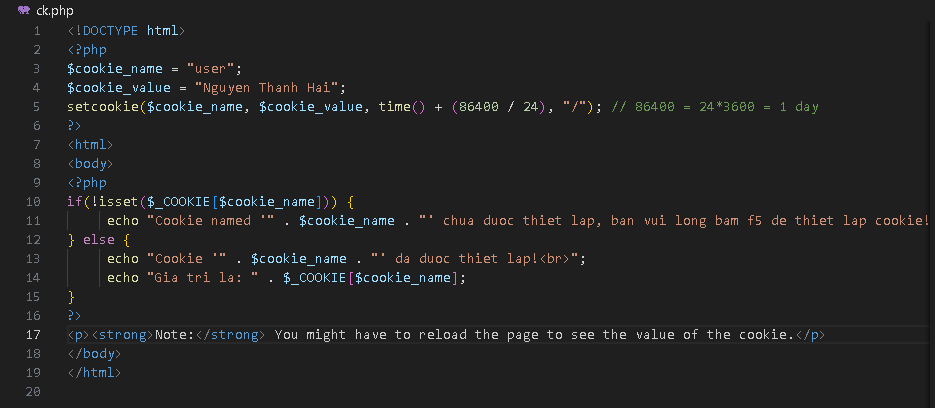
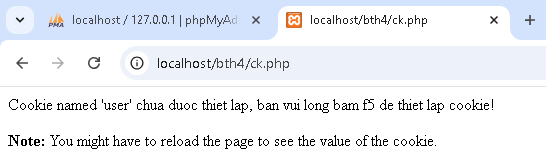
**1.**

ck.php

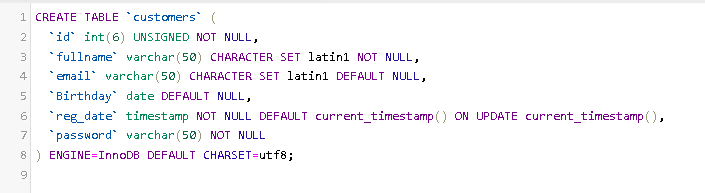


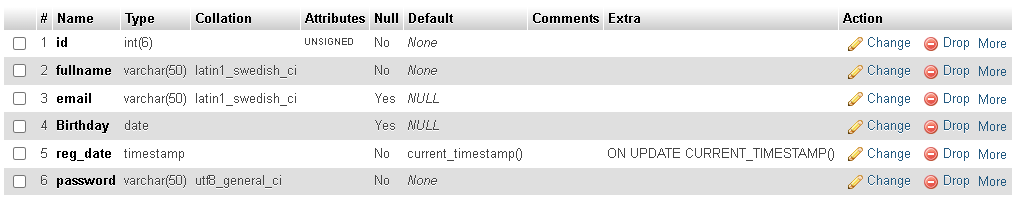
Kết quả file ck.php



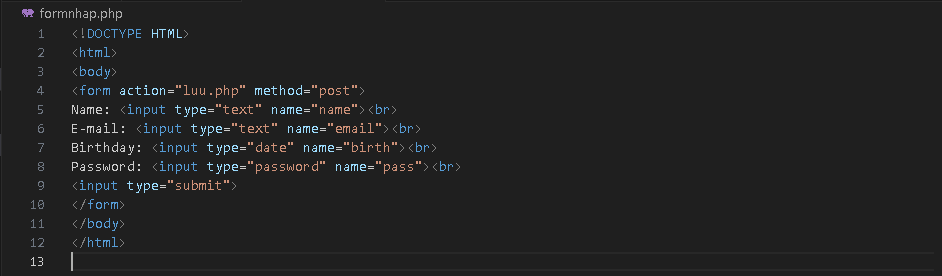
Tạo csdl qlbanhang



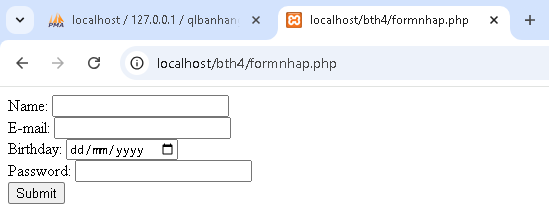
Kết quả tạo csdl



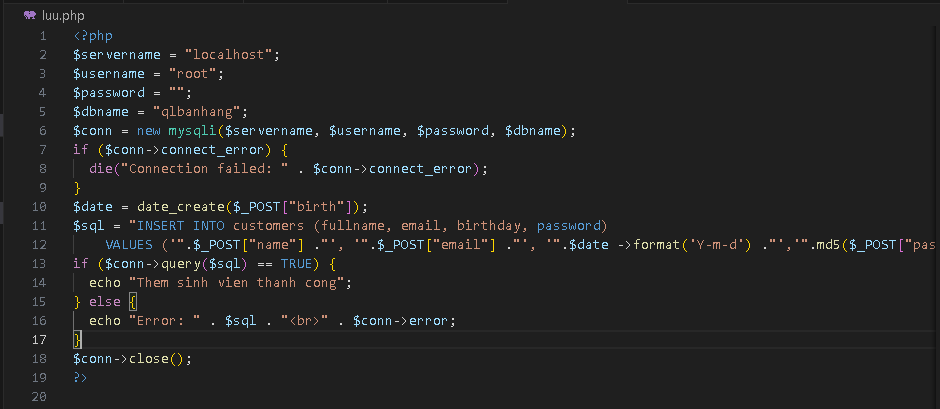
formnhap.php



Kết quả file formnhap.php



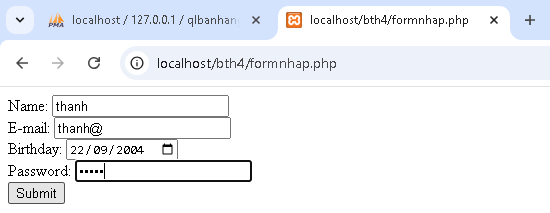
luu.php

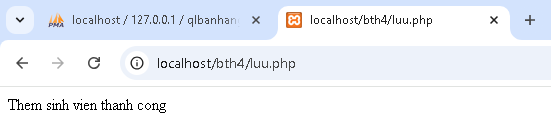


Thêm ràng buộc



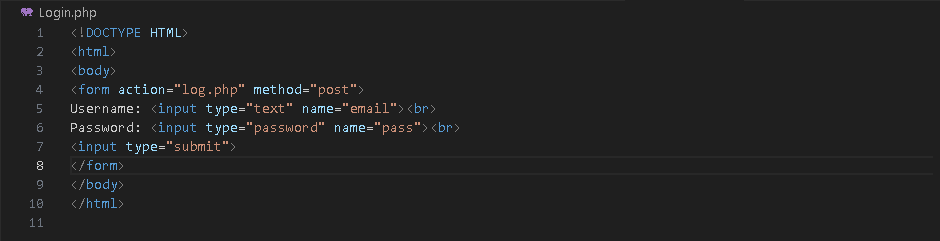
Kết quả sau khi thêm file luu.php



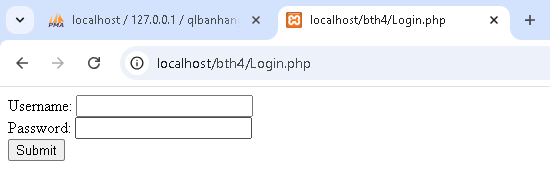




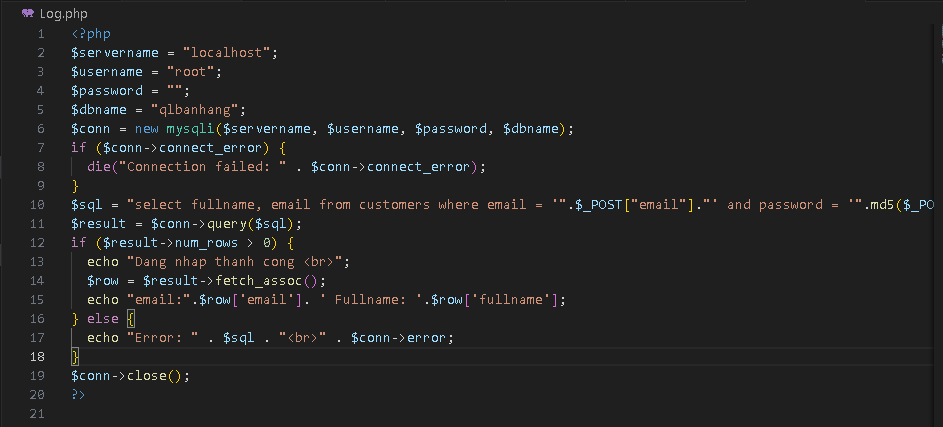
Login.php



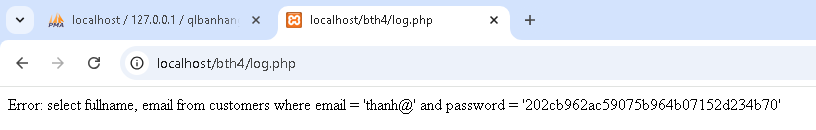
Kết quả file Login.php

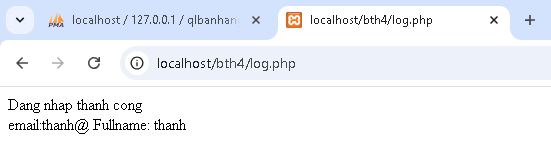


Log.php



Kết quả sau khi thêm file Log.php

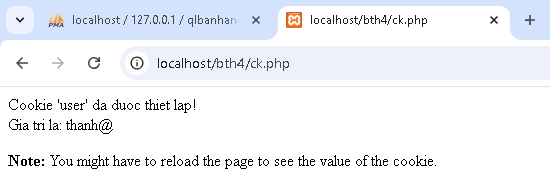




Log.php (modified)

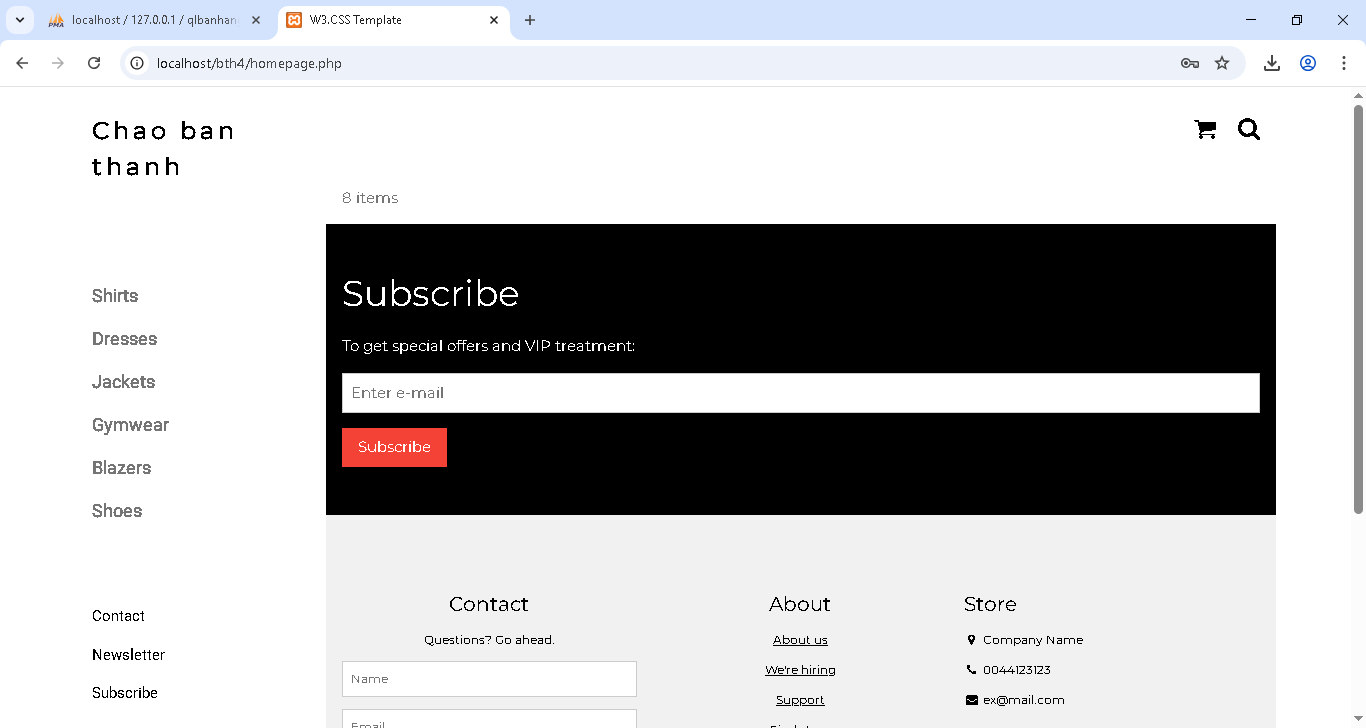


Kết quả sau hki sửa file Log.php

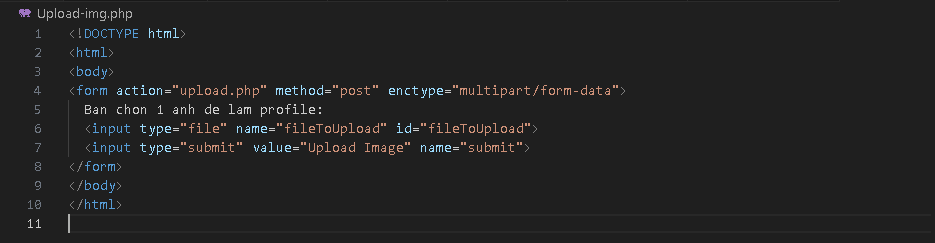


Homepage.php

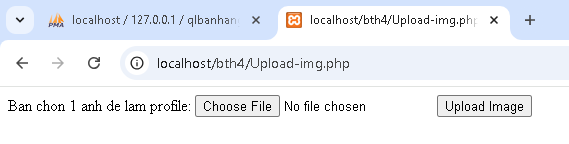
Kết quả sau khi thêm file Homepage.php



Upload-img.php

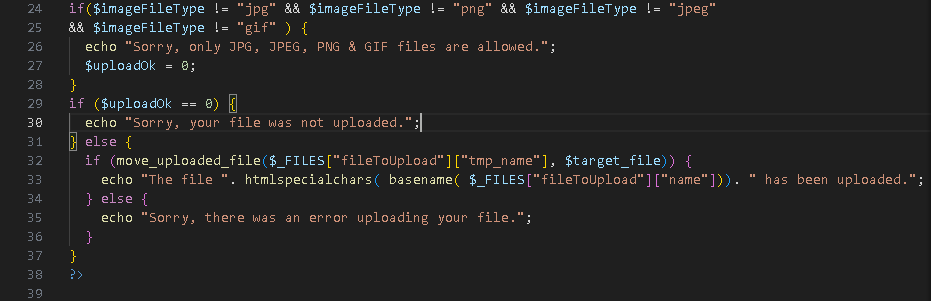


Kết quả file Upload-img.php

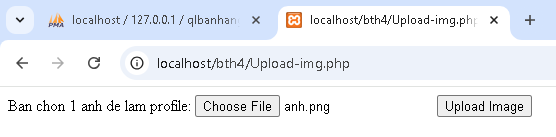


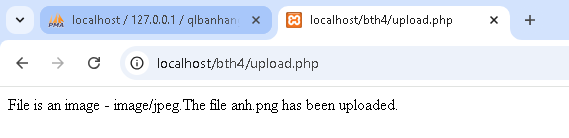
upload.php

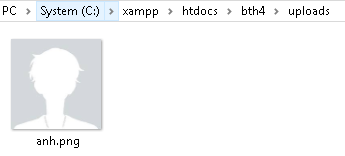




Kết quả sau khi thêm file upload.php







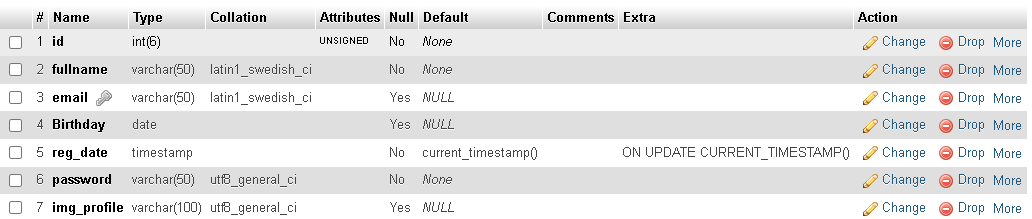
Upload-img.php (modified)



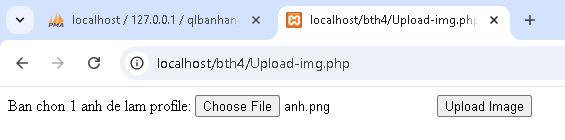
Thêm cột mới

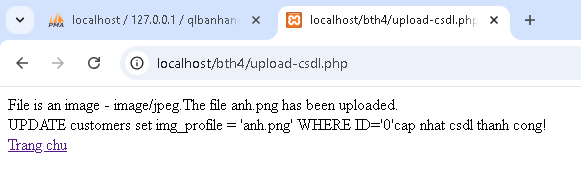


Kết quả thêm cột mới



Kết quả sau khi sửa file Upload-img.php

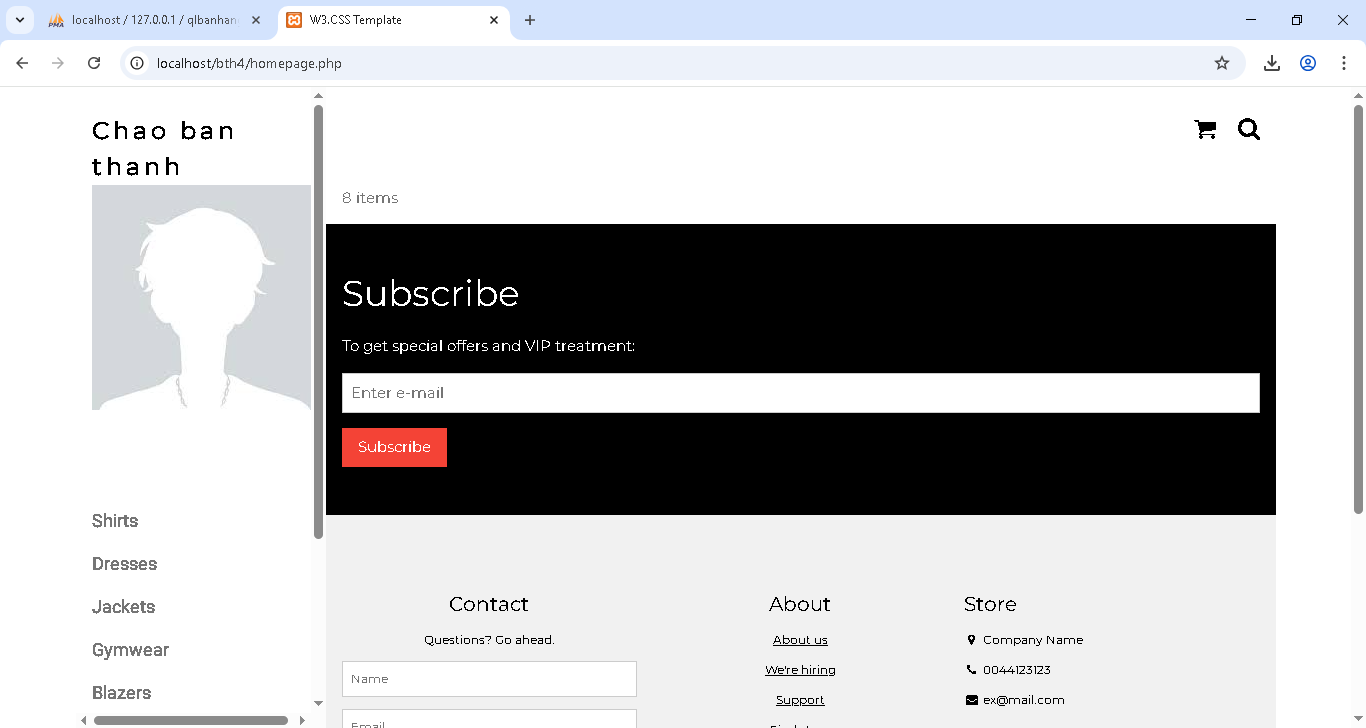




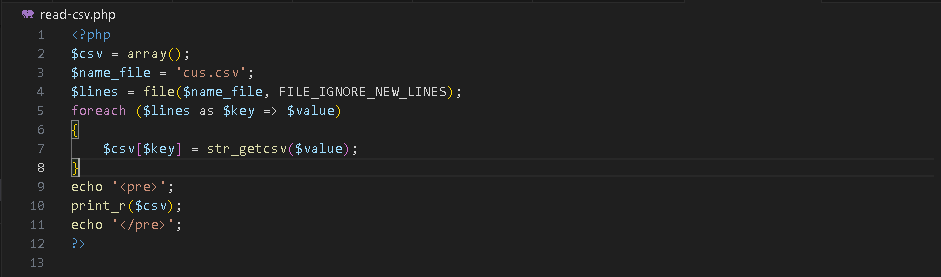


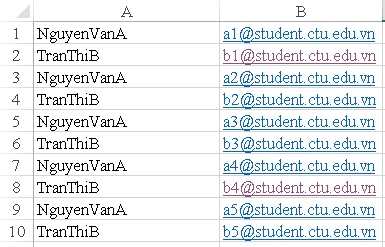
Homepage.php (modified)

Kết quả sau khi sửa file Homepage.php

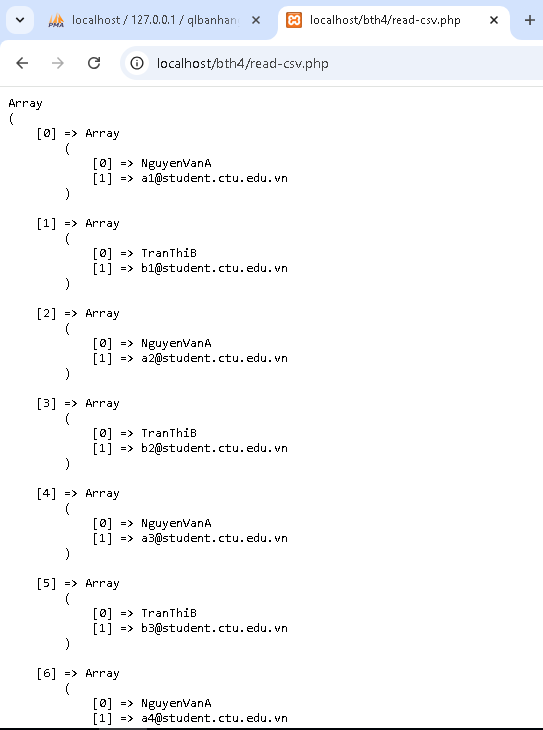


read-csv.php





Kết quả chạy file read-csv.php



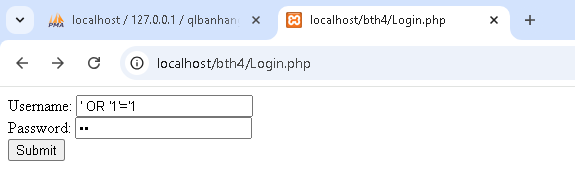
**2.**

**- SQL Injection** là một kỹ thuật tấn công bảo mật mà kẻ tấn công **chèn mã SQL độc hại** vào các đầu vào của ứng dụng (thường là form đăng nhập hoặc URL), nhằm can thiệp vào câu truy vấn cơ sở dữ liệu.

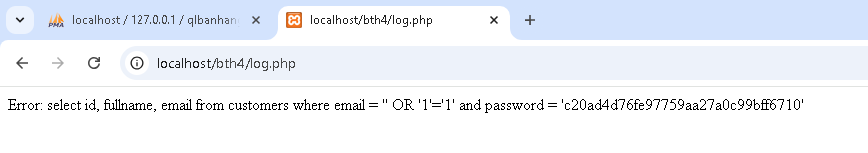
- Kẻ tấn công có thể:

* Truy cập trái phép tài khoản người dùng
* Xem, sửa hoặc xóa dữ liệu.
* Ghi đè mật khẩu.
* Gây hỏng hóc hệ thống.

- Áp dụng



Kết quả



**3.**

**Cookie** là một **tệp nhỏ** được lưu trữ trên **máy tính của người dùng** bởi **trình duyệt**, chứa thông tin mà **trang web có thể ghi nhớ** giữa các lần truy cập.

| **Tham số** | **Ý nghĩa** |
| --- | --- |
| name | Tên cookie (bắt buộc) |
| value | Giá trị cần lưu (bắt buộc, dạng chuỗi) |
| expire | Thời gian hết hạn (UNIX timestamp). Mặc định là **cookie phiên**, sẽ bị xóa khi đóng trình duyệt |
| path | Đường dẫn mà cookie có hiệu lực (mặc định là /) |
| domain | Tên miền có thể truy cập cookie. VD: .example.com |
| secure | Chỉ gửi cookie qua HTTPS nếu là true |
| httponly | Ngăn JavaScript truy cập cookie nếu là true (bảo vệ khỏi XSS) |

Lưu cookie:

setcookie("username", "admin", time() + 86400, "/");

Lấy cookie:

if (isset($\_COOKIE["username"])) {

echo "Hello " . $\_COOKIE["username"];

} else {

echo "Cookie chưa được thiết lập.";

}

Xóa cookie:

setcookie("username", "", time() - 3600, "/");

**4.**

**Session** là cơ chế lưu trữ **dữ liệu tạm thời trên server** để theo dõi **người dùng trong suốt quá trình truy cập website** (trên nhiều trang).

Lưu sesion:

$\_SESSION["username"] = "admin";

$\_SESSION["email"] = "admin@example.com";

Lấy session:

echo $\_SESSION["username"];

Xóa 1 session cụ thể:

unset($\_SESSION["username"]);

Xóa tất cả session:

session\_unset();

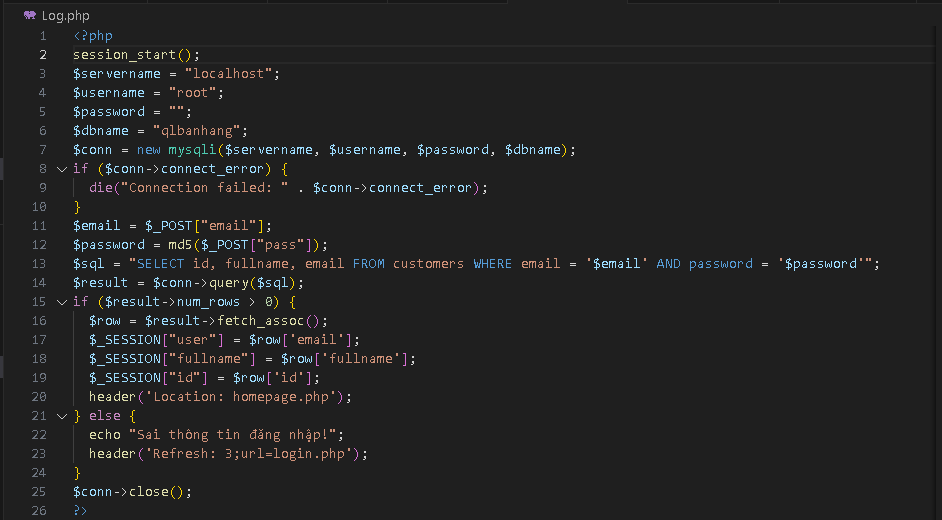
session\_destroy();

**5.**

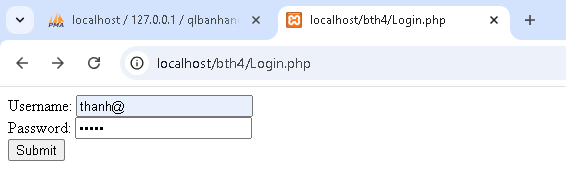
|  |  |  |
| --- | --- | --- |
| Tiêu chí | cookie | session |
| Vị trí lưu trữ | Trình duyệt | Server |
| Dung lượng | ~4kb | Tùy thuộc server |
| Thời gian tồn tại | Lâu dài | Tồn tại trong phiên truy cập hoặc đến khi bị xóa |
| Bảo mật | Kém | Tốt |
| Khả năng bị tấn công | Dễ bị tấn công XSS, giả mạo cookie | Có thể bị đánh cắp session ID |
| Khởi tạo | Không cần gọi hàm | Cần gọi hàm |
| Tuy xuất dữ liệu | $\_COOKIE[“name”] | $\_SESSION[“name”] |
| Tốc độ xử lý | Nhanh | Chậm hơn một chút |
| Khi nào nên dùng | Cần lưu thông tin lâu dài,không nhạy cảm | Cần bảo mật cao |

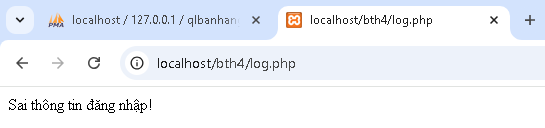
**6.**

Log.php

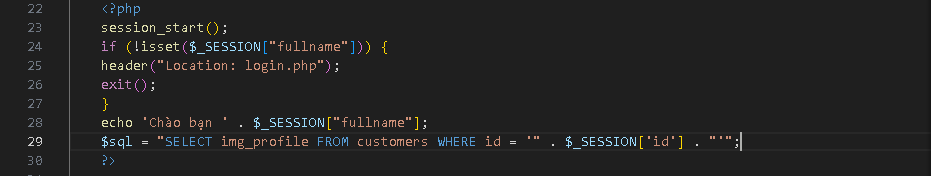


Kết quả sau khi chỉnh sửa file Log.php

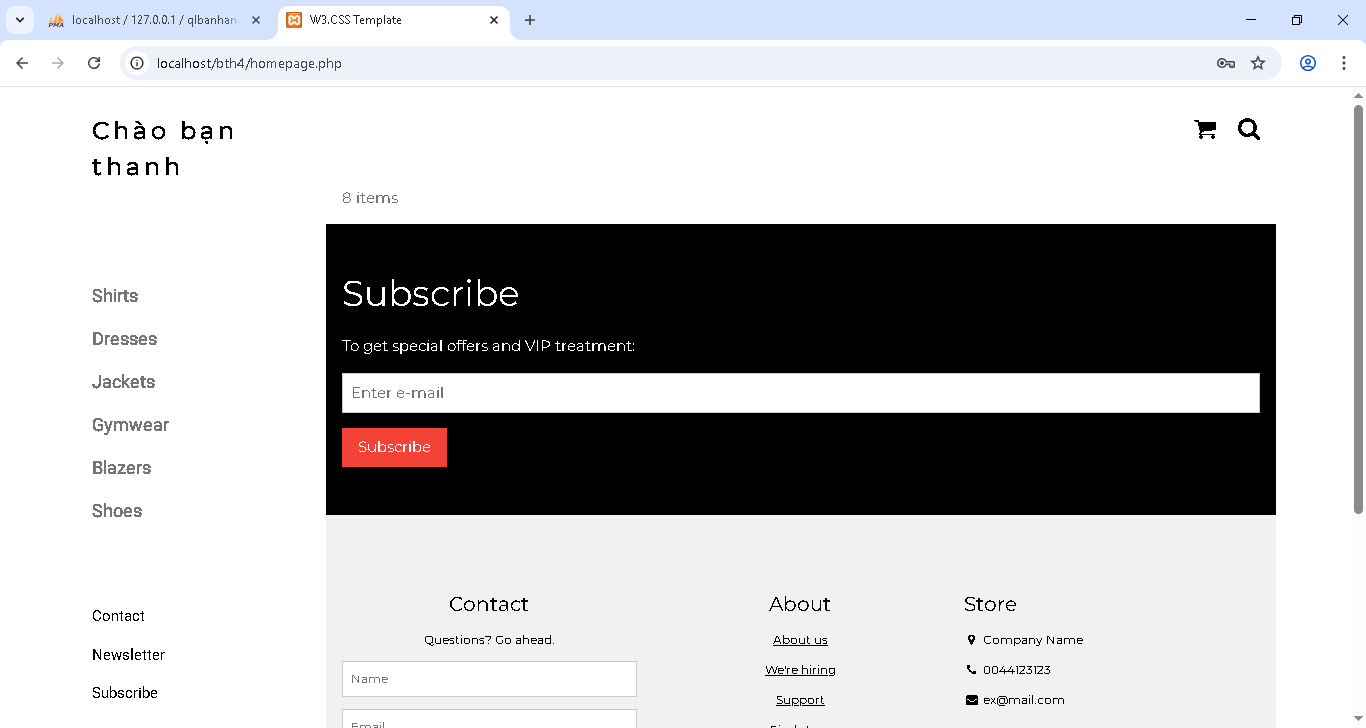




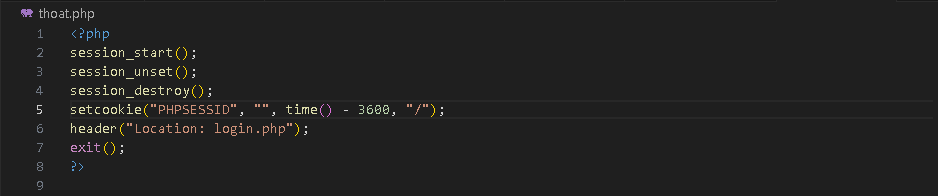
Sửa file Homepage.php



Kết quả sau khi sửa file Homepage.php



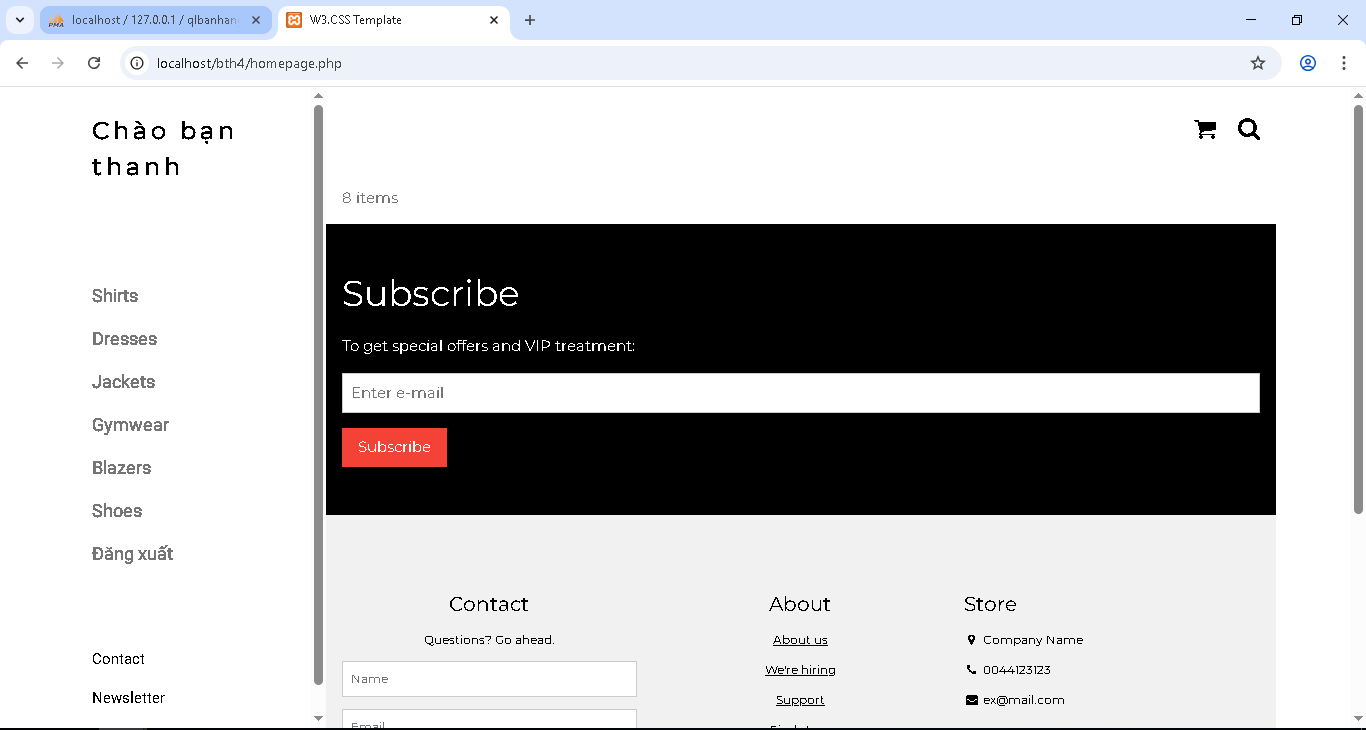
thoat.php

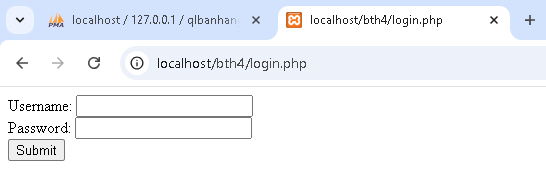


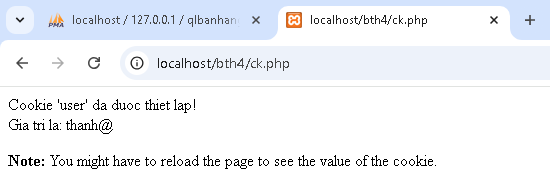
Thêm đường dẫn vào file Homepage.php

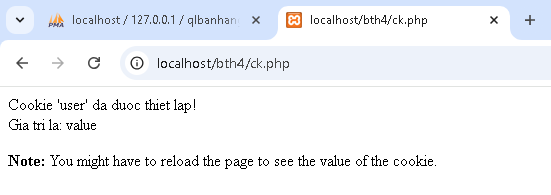


Kết quả sau khi hoàn thành







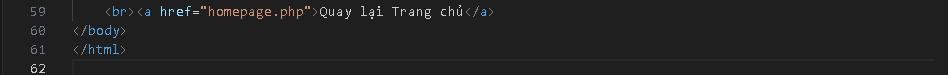


**7.**

sua\_mk.php



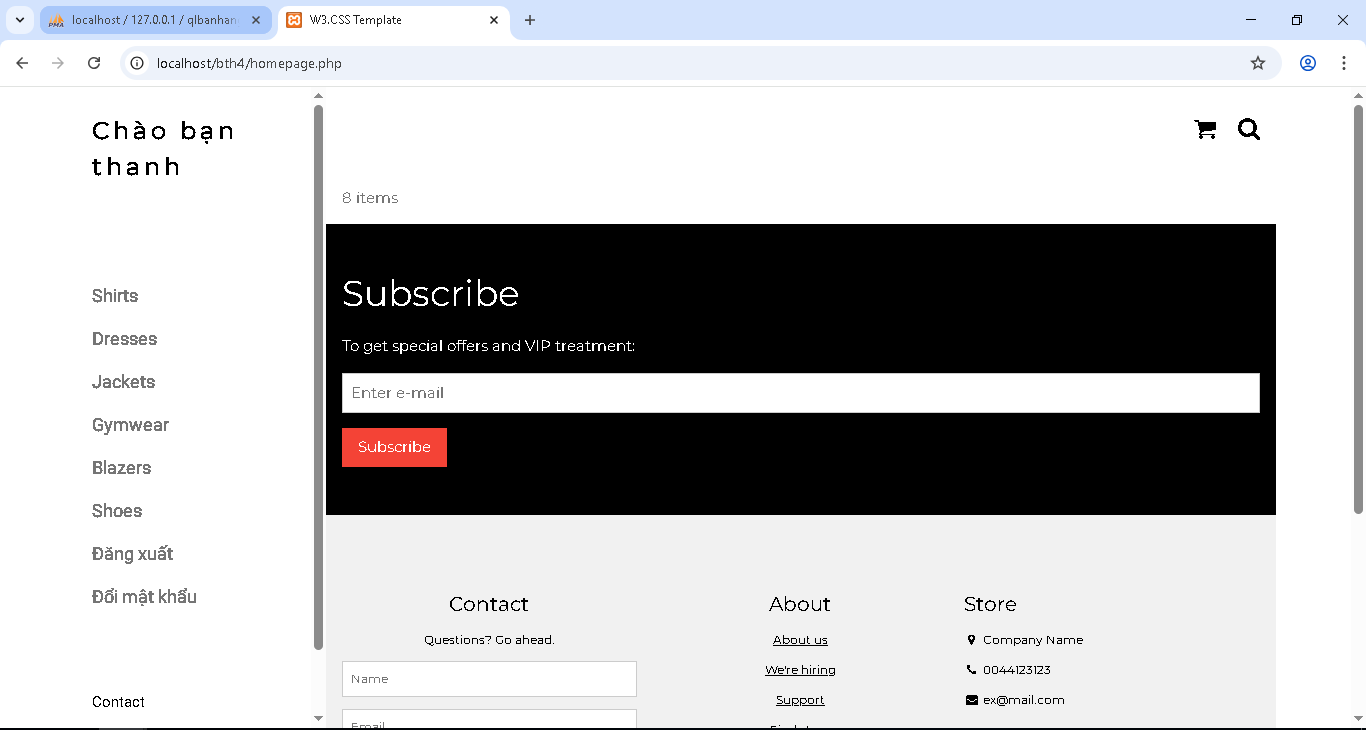


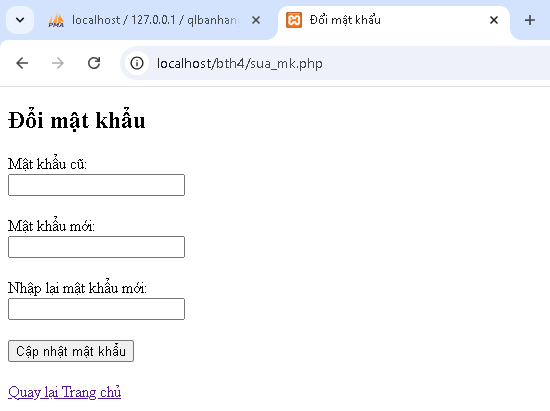


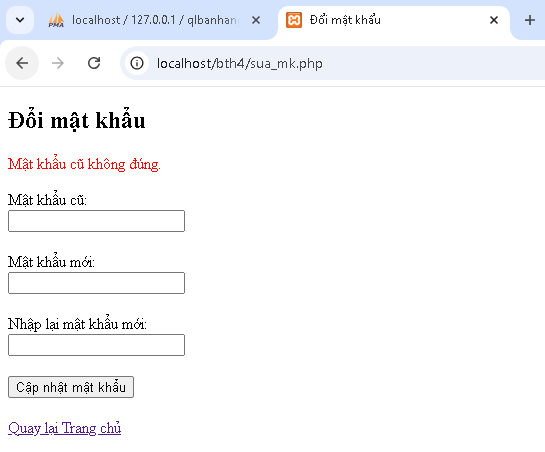
Thêm đường dẫn vào file Homepage.php



Kết quả sau khi hoàn thành







\

**8.**

Cơ chế hoạt động upload file trong PHP

* Khi người dùng gửi một file từ form HTML, PHP sẽ xử lý file đó qua biến $\_FILES.
* Tập tin sẽ được lưu tạm thời trên server tại thư mục tạm (tmp), sau đó bạn cần di chuyển file đến thư mục đích.

|  |  |
| --- | --- |
| Move\_uploaded\_file() | Di chuyển file từ thư mục tạm sang thư mục đích |
| Is\_uploaded\_file() | Kiểm tra xem file có phải là upload hợp lệ từ client không |
| File\_exists() | Kiểm tra xem file đã tồn tại trong thư mục đích chưa |
| Pathinfo() | Lấy phần mở rộng hoặc tên file |

**9.**

Hàm file() dùng để:**Đọc toàn bộ nội dung của một tập tin và lưu từng dòng vào một mảng.**

Tham số

|  |  |
| --- | --- |
| filename | Đường dẫn đến file cần đọc. |
| flags | Các cờ để điều chỉnh cách đọc file |
| context | Dùng khi bạn muốn tùy chỉnh hành vi stream |

**10.**

upload-csv.php

<?php

if ($\_SERVER["REQUEST\_METHOD"] == "POST" && isset($\_FILES["csvfile"])) {

    $file = $\_FILES["csvfile"]["tmp\_name"];

    $handle = fopen($file, "r");

    $conn = new mysqli("localhost", "root", "", "qlbanhang");

    if ($conn->connect\_error) {

        die("Kết nối thất bại: " . $conn->connect\_error);

    }

    $success = 0;

    $fail = 0;

    while (($data = fgetcsv($handle, 1000, ",")) !== FALSE) {

        $id = (int)$data[0];

        $fullname = $conn->real\_escape\_string($data[1]);

        $email = $conn->real\_escape\_string($data[2]);

        $birthday = $conn->real\_escape\_string($data[3]);

        $reg\_date = $conn->real\_escape\_string($data[4]);

        $password = md5($data[5]);

        $img\_profile = $conn->real\_escape\_string($data[6]);

        $check\_sql = "SELECT id FROM customers WHERE id = $id OR email = '$email'";

        $check\_result = $conn->query($check\_sql);

        if ($check\_result->num\_rows > 0) {

            $fail++;

            continue;

        }

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

                VALUES ($id, '$fullname', '$email', '$birthday', '$reg\_date', '$password', '$img\_profile')";

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

            $success++;

        } else {

            echo "Lỗi khi thêm ID $id: " . $conn->error . "<br>";

            $fail++;

        }

    }

    fclose($handle);

    $conn->close();

    echo "<p>Đã thêm $success dòng thành công.</p>";}

?>

<!DOCTYPE html>

<html>

<head>

    <title>Upload CSV</title>

</head>

<body>

    <h2>Upload CSV </h2>

    <form method="POST" enctype="multipart/form-data">

        Chọn file CSV:

        <input type="file" name="csvfile" accept=".csv" required><br><br>

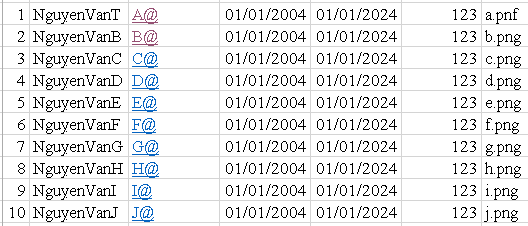
        <input type="submit" value="Upload & Import">

    </form>

</body>

</html>





Kết quả file upload-csv.php

