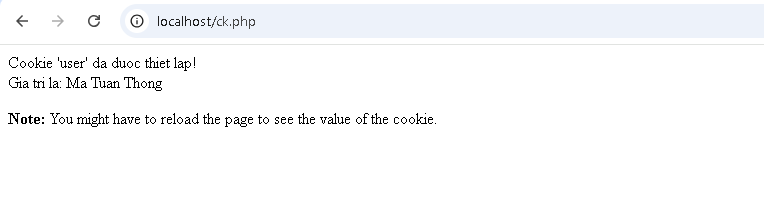
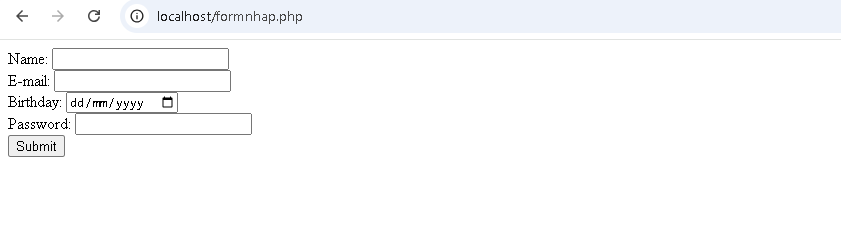
.

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

**Ck.php**



**Formnhap.php**



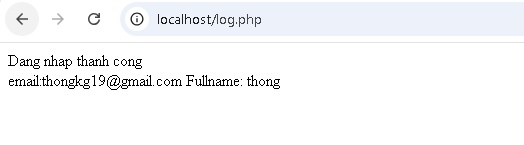
**Luu.php**



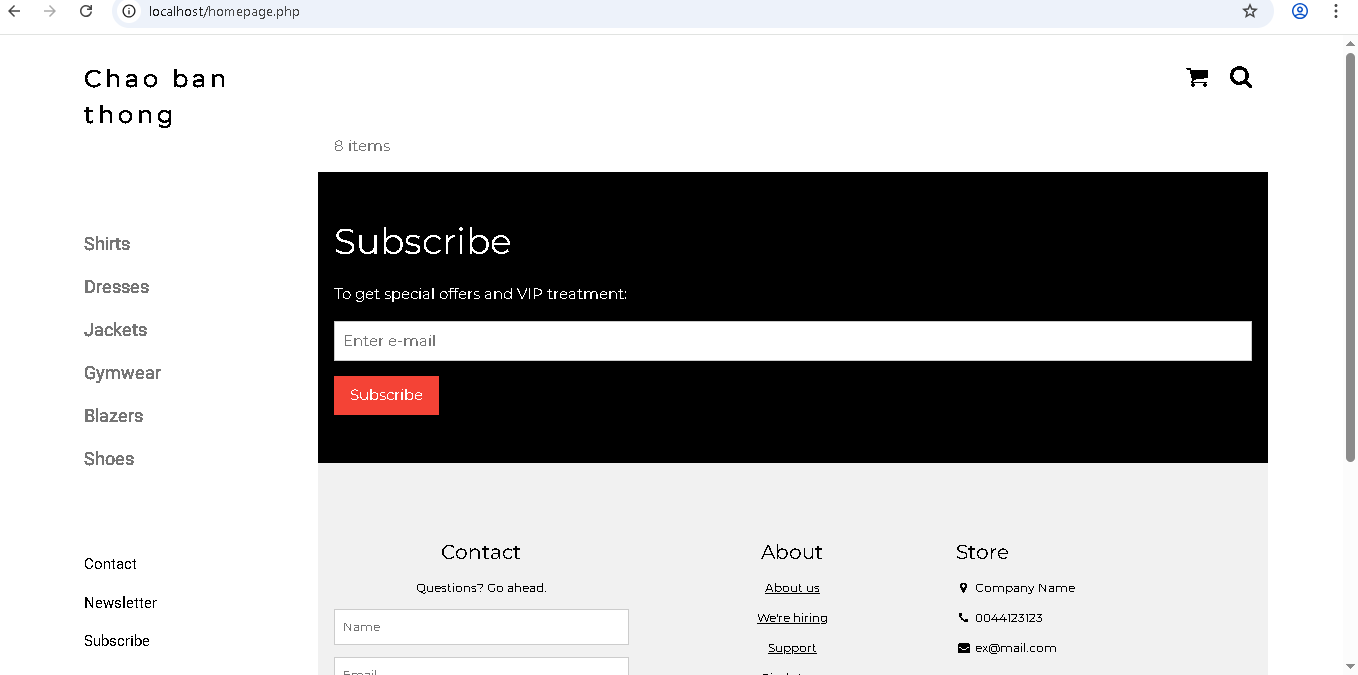
**Login.php**



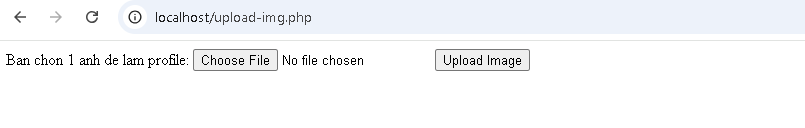
**Log.php**



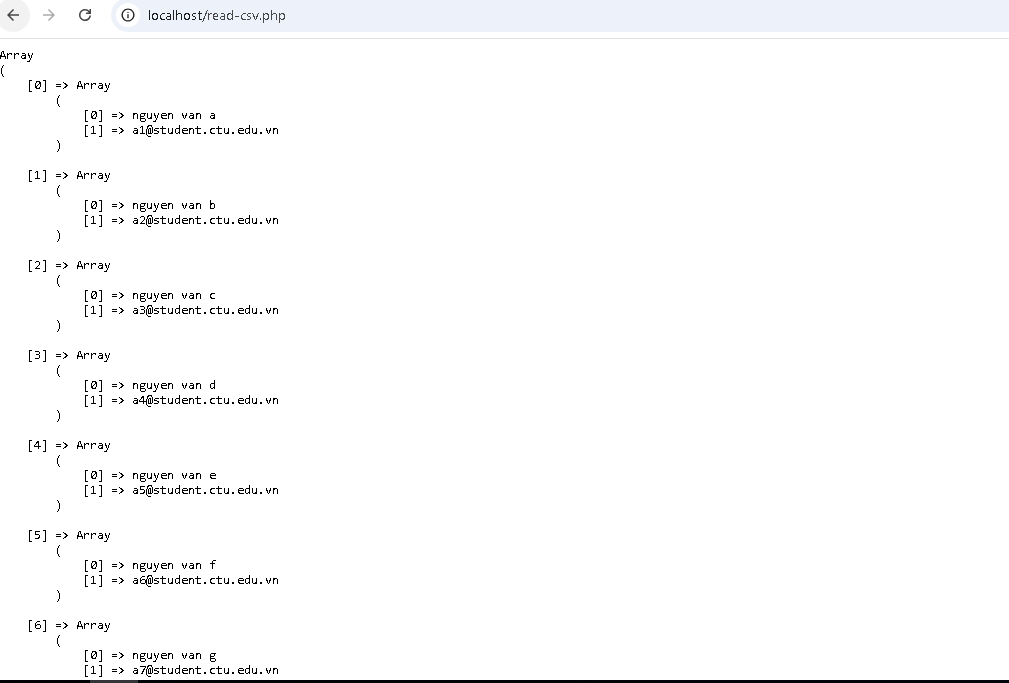
**Homepage.php**



**Upload-img.php**



**Read-csv.php**



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

SQL Injection (viết tắt: SQLi) là một kỹ thuật tấn công phổ biến trong lĩnh vực bảo mật web, trong đó kẻ tấn công **chèn (inject)** các mã SQL độc hại vào các trường nhập liệu (form input) như **tên đăng nhập, mật khẩu, ô tìm kiếm**, v.v. Mục tiêu là để **thay đổi câu truy vấn SQL ban đầu** mà hệ thống thực hiện, từ đó có thể:

* Đăng nhập trái phép.
* Lấy thông tin nhạy cảm trong cơ sở dữ liệu.
* Xóa, sửa, thêm dữ liệu.
* Chiếm quyền điều khiển hệ thống.

3.Dựa vào link, 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 đoạn dữ liệu nhỏ (dạng key-value) được lưu trữ trên **trình duyệt của người dùng** bởi website. Cookie giúp website:

* Ghi nhớ thông tin người dùng (ví dụ: đăng nhập, giỏ hàng, giao diện ưa thích).
* Theo dõi phiên làm việc (session) giữa các lần truy cập.
* Tăng trải nghiệm người dùng (không phải đăng nhập lại, hiển thị cá nhân hóa...).

**Hàm setcookie() trong PHP**

Cú pháp đầy đủ:

php

CopyEdit

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

| **Tham số** | **Ý nghĩa** |
| --- | --- |
| name | Tên của cookie. |
| value | Giá trị của cookie (có thể là chuỗi, mã hóa JSON,...). |
| expire | Thời điểm hết hạn cookie (theo UNIX timestamp – số giây). |
| path | Đường dẫn mà cookie có hiệu lực (thường là / để dùng toàn site). |
| domain | Tên miền cookie được áp dụng (ví dụ: .example.com). |
| secure | Nếu true, cookie chỉ gửi qua HTTPS. |
| httponly | Nếu true, cookie không thể truy cập bằng JavaScript (giúp chống XSS). |

**Lưu giá trị bằng setcookie():**

php

CopyEdit

setcookie("username", "admin", time() + 3600, "/");

→ Tạo cookie tên username, giá trị admin, tồn tại trong 1 giờ.

**Đọc (lấy giá trị) cookie:**

php

CopyEdit

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

echo "Xin chào: " . $\_COOKIE["username"];

}

**Xóa cookie:**

php

CopyEdit

setcookie("username", "", time() - 3600, "/"); // Hết hạn ngay

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

**1. Session là gì?**

**Session** (phiên làm việc) là một **cơ chế lưu trữ tạm thời thông tin người dùng** trên **máy chủ (server)** trong suốt phiên làm việc. Không giống như cookie (lưu trên trình duyệt), session bảo mật hơn vì người dùng **không trực tiếp nhìn thấy hoặc sửa đổi được**.

**🎯 Session dùng để làm gì?**

* Lưu trạng thái đăng nhập của người dùng.
* Lưu thông tin tạm như: giỏ hàng, dữ liệu form, lượt truy cập.
* Tăng cường bảo mật so với Cookie.
* Quản lý thông tin người dùng xuyên suốt các trang trong cùng 1 phiên truy cập.

**🧠 2. Cách sử dụng Session trong PHP**

**✅ a. Khởi tạo session:**

Trước khi dùng session, bạn cần gọi:

php

CopyEdit

session\_start();

Gọi ở **đầu file PHP**, trước bất kỳ mã HTML nào.

**✅ b. Lưu giá trị vào Session:**

php

CopyEdit

session\_start();

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

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

**🔍 c. Lấy (đọc) giá trị từ Session:**

php

CopyEdit

session\_start();

echo $\_SESSION["username"]; // Kết quả: admin

**❌ d. Xóa giá trị trong Session:**

**1. Xóa từng biến:**

php

CopyEdit

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

**2. Xóa toàn bộ session:**

php

CopyEdit

session\_unset(); // Xóa tất cả biến session

session\_destroy(); // Hủy hoàn toàn session hiện tại

5.Bạn hãy so sánh Cookie và Session.

| **Tiêu chí** | **Cookie** | **Session** |
| --- | --- | --- |
| **Lưu trữ ở đâu?** | Trên **trình duyệt** (máy người dùng) | Trên **máy chủ (server)** |
| **Bảo mật** | Kém hơn (dễ bị sửa, xem) | An toàn hơn (người dùng không truy cập trực tiếp) |
| **Dung lượng lưu trữ** | Tối đa khoảng **4KB** | Không giới hạn cụ thể (do lưu ở server) |
| **Thời gian tồn tại** | Có thể tồn tại **lâu dài** (tùy theo thời gian đặt) | Chỉ tồn tại trong **phiên làm việc** (hết khi đóng trình duyệt hoặc logout) |
| **Hiển thị cho người dùng?** | Có thể xem và chỉnh sửa bằng DevTools (trong browser) | Không thể xem trực tiếp |
| **Dễ bị đánh cắp?** | Dễ bị **giả mạo / đánh cắp** nếu không bảo vệ tốt | Ít bị đánh cắp hơn (vì lưu trên server) |
| **Khởi tạo** | Không cần session\_start() | Cần gọi session\_start() |
| **Tác vụ phổ biến** | Ghi nhớ đăng nhập, ngôn ngữ, giỏ hàng nhẹ | Quản lý người dùng đăng nhập, giỏ hàng, bảo mật |
| **Lưu được loại dữ liệu nào?** | Chỉ lưu dạng **chuỗi** | Lưu được **chuỗi, mảng, đối tượng,...** |
| **Gửi kèm mỗi request?** | **Có** – Gửi kèm với mỗi lần tải trang | **Không** – Chỉ xử lý khi PHP cần đọc dữ liệu |

**6.**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.

Homepage.php

<?php

session\_start();

if (!isset($\_SESSION['id'])) {

// Nếu chưa đăng nhập thì chuyển hướng về login

header("Location: login.php");

exit();

}

?>

<!-- Phần HTML bên dưới giữ nguyên, chỉ sửa phần PHP -->

<h3 class="w3-wide"><b>

<?php

echo 'Chào bạn, ' . $\_SESSION['fullname'];

// Lấy ảnh đại diện từ CSDL

$servername = "localhost";

$username = "root";

$password = "";

$dbname = "qlbanhang";

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

if ($conn->connect\_error) {

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

}

$sql = "SELECT img\_profile FROM customers WHERE id = '" . $\_SESSION['id'] . "'";

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

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

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

echo '<img src="./uploads/' . $row['img\_profile'] . '" alt="Ảnh profile">';

}

$conn->close();

?>

</b></h3>

Log.php

<?php

session\_start();

$servername = "localhost";

$username = "root";

$password = "";

$dbname = "qlbanhang";

// Create connection

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

if ($conn->connect\_error) {

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

}

$email = $\_POST["email"];

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

$sql = "SELECT id, fullname, email FROM customers WHERE email = '$email' AND password = '$pass'";

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

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

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

// Lưu thông tin vào SESSION

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

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

$\_SESSION["email"] = $row["email"];

header("Location: homepage.php");

exit();

} else {

echo "Thông tin đăng nhập không hợp lệ.<br>";

header("Refresh: 3;url=login.php");

}

$conn->close();

?>

Thoat.php

<?php

session\_start();

// Xóa toàn bộ biến trong session

session\_unset();

// Hủy phiên làm việc

session\_destroy();

// Nếu có cookie cũ, xóa luôn (dự phòng)

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

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

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

// Chuyển hướng về trang login

header("Location: login.php");

exit();

?>

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

## Cơ chế upload file trong PHP

* Khi người dùng chọn file từ form HTML (dùng <input type="file">) và submit form lên server, PHP sẽ tự động nhận file này và lưu tạm trong một thư mục tạm thời trên server.
* PHP cung cấp một biến toàn cục $\_FILES để truy cập thông tin của file được upload.
* Sau đó, bạn cần di chuyển file từ thư mục tạm tới thư mục đích bằng hàm move\_uploaded\_file().

## Các thành phần chính của $\_FILES

$\_FILES là một mảng siêu toàn cục chứa thông tin về các file upload, ví dụ:

php

CopyEdit

$\_FILES['fileToUpload']['name'] // Tên file gốc trên máy người dùng

$\_FILES['fileToUpload']['type'] // Loại MIME file

$\_FILES['fileToUpload']['tmp\_name'] // Đường dẫn file tạm trên server

$\_FILES['fileToUpload']['error'] // Mã lỗi upload (0 nếu thành công)

$\_FILES['fileToUpload']['size'] // Kích thước file (byte)

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

**Hàm file()**

**Chức năng:**

* Hàm file() đọc toàn bộ nội dung của một file và trả về **một mảng** (array), trong đó mỗi phần tử của mảng tương ứng với một dòng trong file.
* Mỗi dòng trong file bao gồm cả ký tự xuống dòng (newline \n).
* Hàm rất hữu ích khi bạn muốn đọc dữ liệu dòng theo dòng từ một file.

**Cú pháp:**

php

CopyEdit

array file(string $filename, int $flags = 0, resource $context = ?)

**Các tham số:**

1. **$filename** (bắt buộc):
   * Là tên hoặc đường dẫn đến file mà bạn muốn đọc.
2. **$flags** (tùy chọn):
   * Một số tùy chọn để thay đổi cách đọc file, có thể kết hợp nhiều flag bằng cách dùng toán tử OR (|).
   * Các flag phổ biến:
     + FILE\_IGNORE\_NEW\_LINES: loại bỏ ký tự xuống dòng ở cuối mỗi dòng.
     + FILE\_SKIP\_EMPTY\_LINES: bỏ qua những dòng rỗng trong file.
     + FILE\_USE\_INCLUDE\_PATH: tìm file trong đường dẫn include của PHP.
   * Mặc định không có flag nào (giá trị 0).
3. **$context** (tùy chọn):
   * Là một resource context được dùng để thay đổi cách xử lý file, hiếm khi dùng trong trường hợp cơ bản.

10.

Upload-csv

<!DOCTYPE html>

<html>

<body>

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

Chon file CSV de up

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

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

</form>

</body>

</html>

Upload-csdl-csv

<?php

session\_start();

$target\_dir = "upload-csv/";

$target\_file = $target\_dir . basename($\_FILES["fileToUpload"]["name"]);

$uploadOk = 1;

$fileType = strtolower(pathinfo($target\_file, PATHINFO\_EXTENSION));

$allowedMIMEs = ['text/csv', 'application/vnd.ms-excel', 'text/plain'];

if (!in\_array($\_FILES["fileToUpload"]["type"], $allowedMIMEs)) {

    die("❌ Loại tệp không hợp lệ. Chỉ cho phép upload file CSV.");

}

if ($fileType !== "csv") {

    die("❌ File không có phần mở rộng .csv");

}

if (file\_exists($target\_file)) {

    echo "⚠️ File đã tồn tại trên server.<br>";

    $uploadOk = 0;

}

if ($uploadOk == 1) {

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

        echo "✅ File " . htmlspecialchars(basename($\_FILES["fileToUpload"]["name"])) . " đã được tải lên thành công.<br>";

        // Kết nối CSDL

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

        if ($conn->connect\_error) {

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

        }

        // Đọc file CSV từng dòng

        if (($handle = fopen($target\_file, "r")) !== FALSE) {

            $rowCount = 0;

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

                $rowCount++;

                // Bỏ qua dòng đầu tiên nếu là header

                if ($rowCount == 1) {

                    // Giả sử dòng đầu là header, nếu không thì comment dòng này

                    continue;

                }

                // Lấy dữ liệu từng cột, có thể cần kiểm tra số cột

                $id = $conn->real\_escape\_string($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 không cần lấy từ CSV (auto timestamp)

                $password\_raw = $data[5];

                // Nếu password trong CSV chưa mã hóa md5, bạn có thể thay đổi dòng sau:

                // $password = md5($conn->real\_escape\_string($password\_raw));

                $password = $conn->real\_escape\_string($password\_raw);

                // Câu lệnh INSERT, tránh lỗi trùng id bằng cách dùng INSERT IGNORE hoặc REPLACE INTO

                $sql = "INSERT INTO customers (id, fullname, email, Birthday, password) VALUES ('$id', '$fullname', '$email', '$birthday', '$password')";

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

                    echo "Dòng $rowCount: Thêm thành công.<br>";

                } else {

                    echo "Dòng $rowCount: Lỗi khi thêm: " . $conn->error . "<br>";

                }

            }

            fclose($handle);

        } else {

            echo "❌ Không thể mở file CSV để đọc.";

        }

        $conn->close();

        echo '<br><a href="homepage.php">🏠 Quay về trang chủ</a>';

    } else {

        echo "❌ Có lỗi xảy ra khi tải file lên.";

    }

} else {

    echo "❌ Upload thất bại do lỗi kiểm tra.";

}

?>