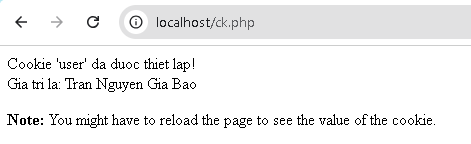
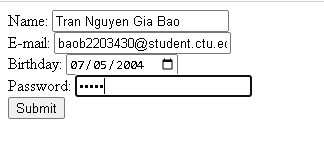
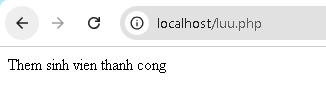
**1.Bạn hãy chạy tất cả các lệnh hướng dẫn ở trên và chụp lại màn hình kết quả.**

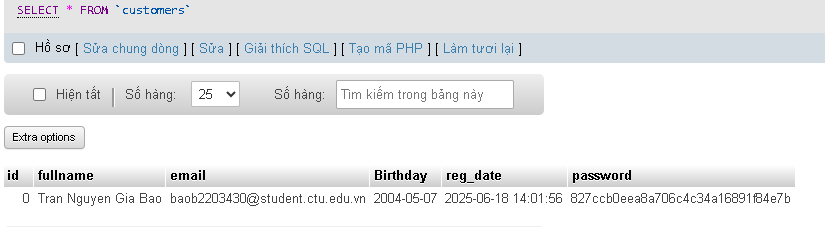
**Tạo cookie**

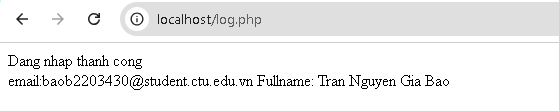


**Tạo 1 trang đăng ký người dùng với mật khẩu được mã hóa**

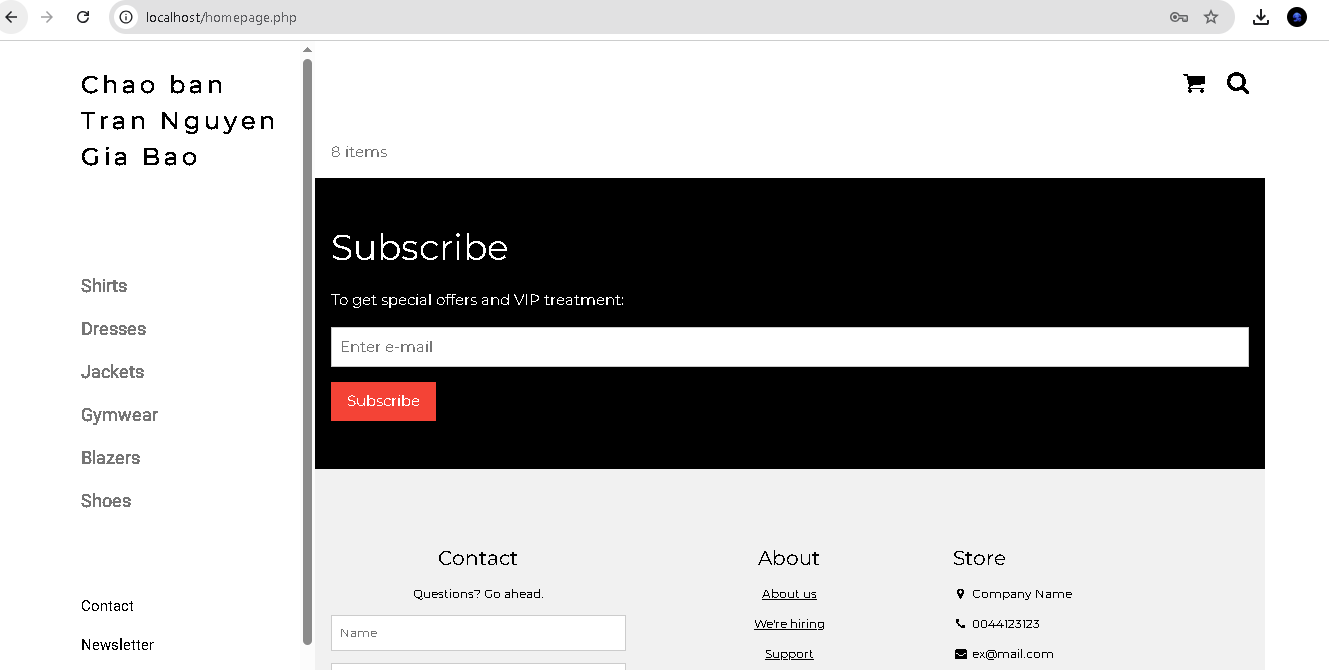




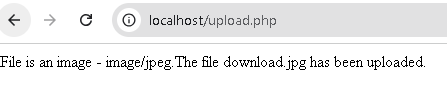




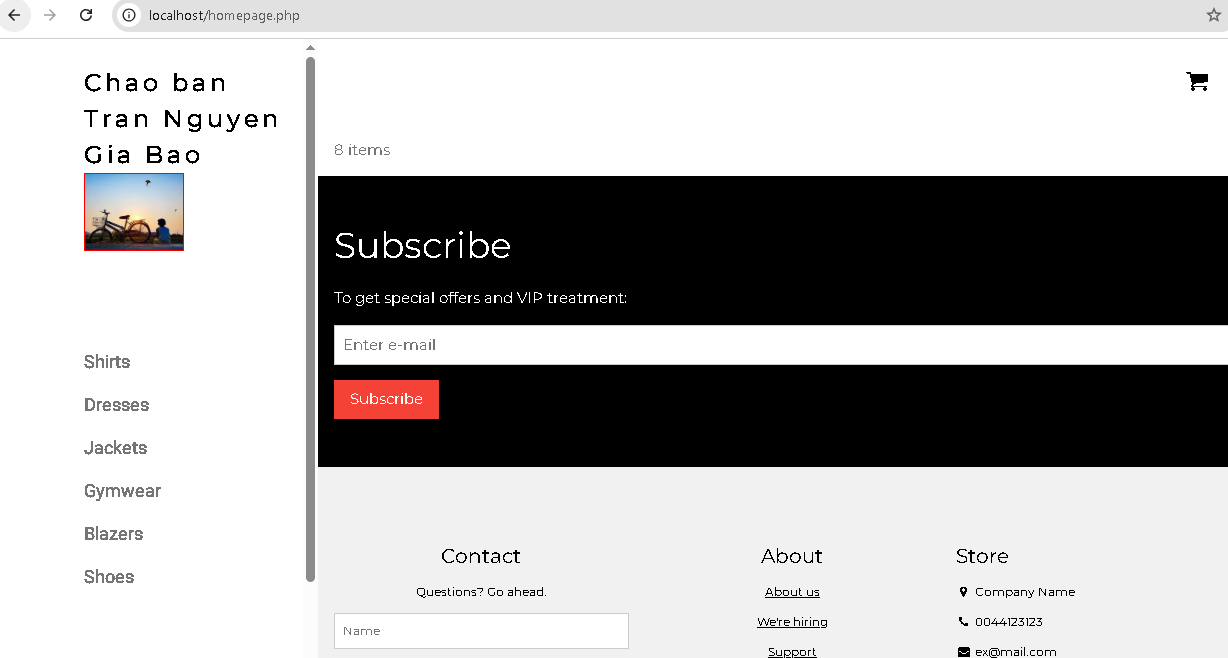
## Dùng Cookies lưu lại tên đăng nhập, email và điều hướng



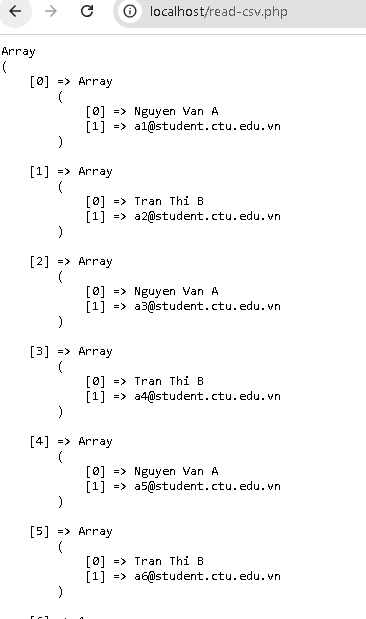
**Upload tập tin**



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



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



**2.Trong vài trường hợp, hacker có thể sử dụng các kỹ thuật SQL Injection để hack hệ**

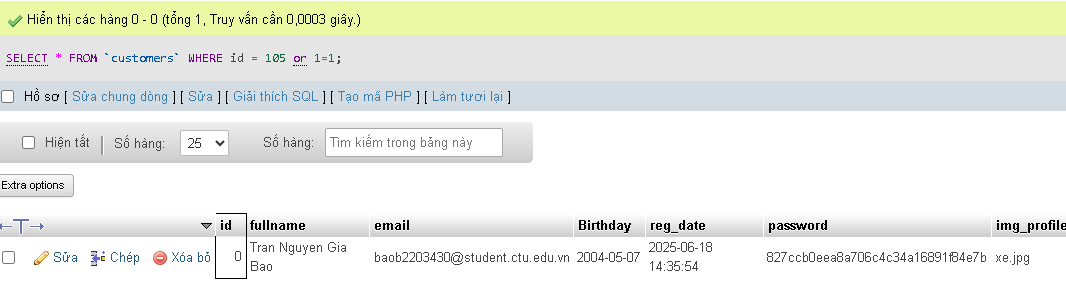
**thống của bạn. Bạn hãy trình bày SQL Injection là gì và thử các ví dụ trình bày trong 1. Ứng dụng kỹ thuật đó vào trang đăng nhập mà bạn đã tạo, chụp lại các kết quả.**

SQL Injection (tiêm nhiễm SQL) là một dạng tấn công bảo mật cho phép kẻ tấn công chèn mã SQL độc hại vào các truy vấn mà ứng dụng gửi đến cơ sở dữ liệu. Từ đó, kẻ tấn công có thể:

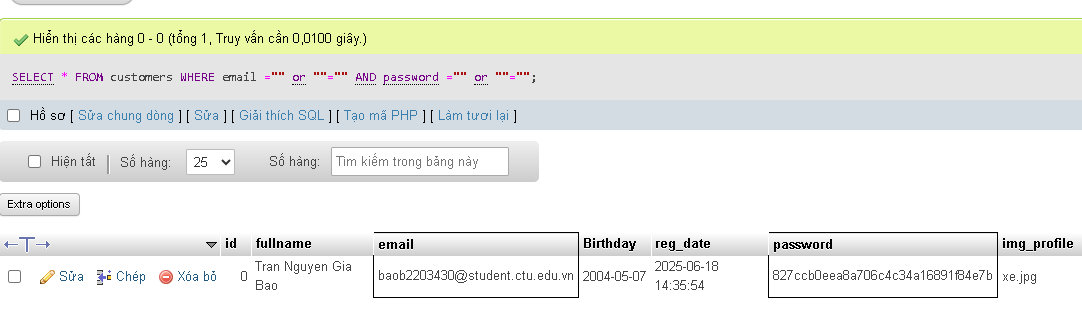
* Lấy cắp dữ liệu (ví dụ: tài khoản, mật khẩu)
* Xem thông tin nhạy cảm
* Chèn, sửa, xóa dữ liệu
* Thậm chí điều khiển toàn bộ hệ thống

**Ví dụ:**

* Hacker chỉ cần chọn id = 105 or 1=1 là sẽ truy vấn được toàn bộ bảng khách hàng vì 1=1 luôn đúng



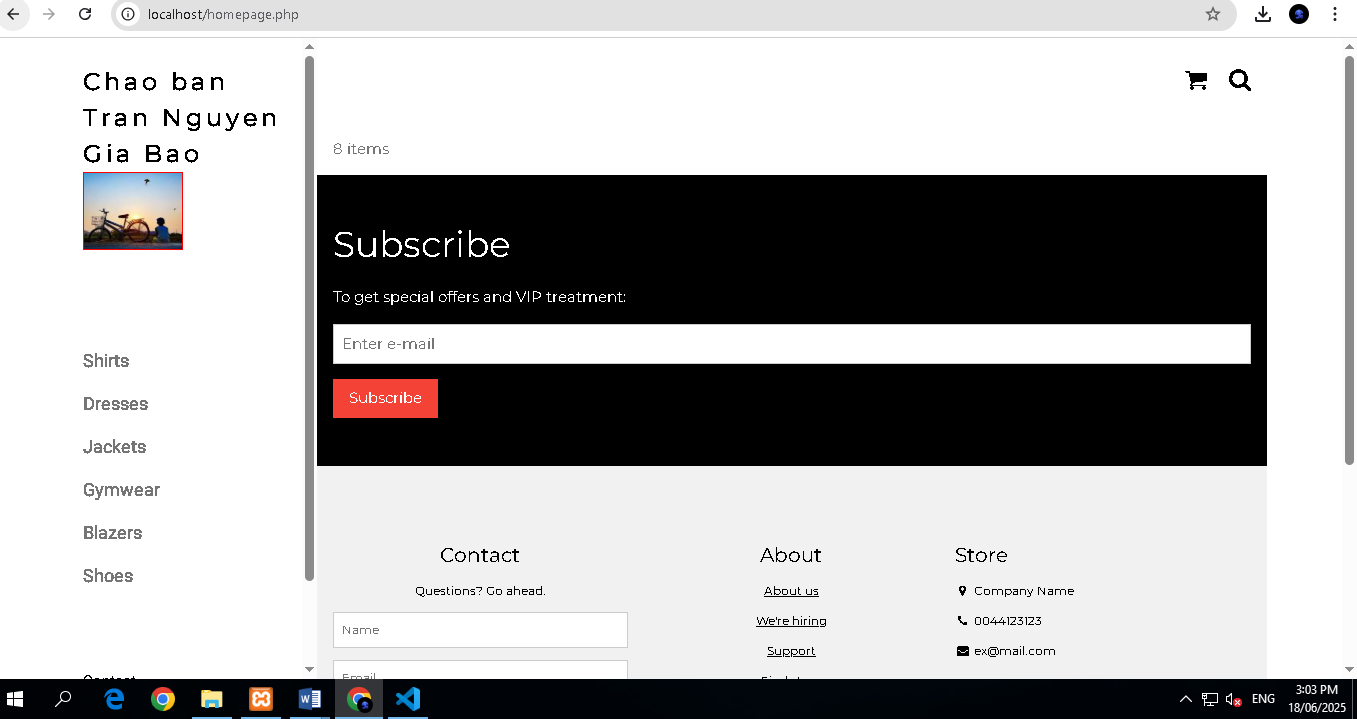
**Hoặc hacker có thể truy bằng email and password:**



**Đăng nhập bằng lỗi an toàn hệ thống:**



**Vào được trang**



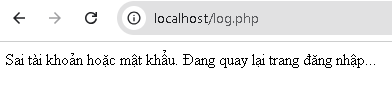
**Sử dụng prepared statement để tránh SQL Injection**

**$sql = "SELECT id, fullname, email FROM customers WHERE email = ? AND password = ?";**

**$stmt = $conn->prepare($sql);**

**$stmt->bind\_param("ss", $email, $pass);**

**$stmt->execute();**



**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 tệp nhỏ được lưu trên máy tính người dùng bởi trình duyệt, cho phép lưu thông tin tạm thời như:

* Tên đăng nhập
* Trạng thái đăng nhập
* Giỏ hàng
* Ngôn ngữ người dùng chọn

Cookie được gửi kèm mỗi khi trình duyệt gọi lại đến cùng server.

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

name Tên của cookie

value Giá trị cần lưu

expire Thời điểm hết hạn (timestamp). Ví dụ: `time() + 3600` là 1 giờ

path Đường dẫn áp dụng cookie (thường là `'/'` để áp dụng toàn bộ web)

domain Tên miền áp dụng cookie

secure : true: chỉ gửi cookie khi kết nối HTTPS

httponly: true: cookie không thể truy cập từ JavaScript (tăng bảo mật)

Lưu giá trị Cookie: setcookie("ten", "giatri", time()+...);

Lấy giá trị Cookie: $\_COOKIE["ten"]

Xóa giá trị Cookie: setcookie("ten", "", time()-3600);

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

Session là một cơ chế lưu trữ thông tin tạm thời trên server cho từng người dùng. Không như cookie (lưu ở máy người dùng), session lưu trên server → bảo mật hơn. Mỗi người dùng sẽ có một Session ID duy nhất (được lưu trong cookie).

**Lưu giá trị trong Session:**

$\_SESSION["username"] = "B2203430";

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

**Lấy giá trị trong Session:**echo $\_SESSION["username"];

**Xóa giá trị trong Session:**unset($\_SESSION["username"]);

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

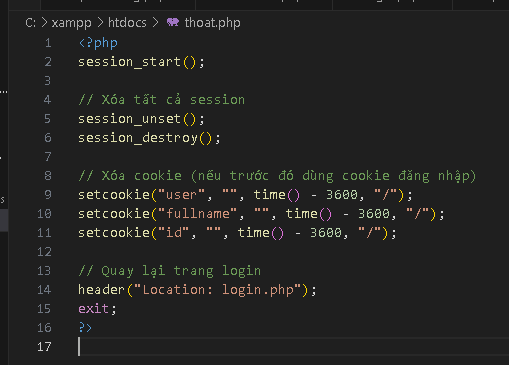
**Cookie:** Lưu bằng trình duyệt, dung lượng và bảo mật thấp, cài được thời gian hết hạn.

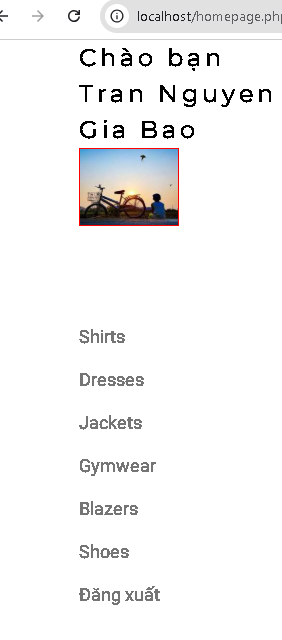
**Session:** Lưu ở server, dung lượng và độ bảo mật cao hơn nhiều so với cookie, sẽ mặc định hết hạn khi đóng trình duyệt.

**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,**

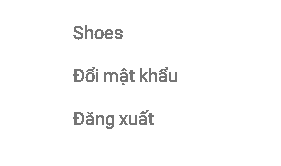
**cookie thực hiện chức năng log out khỏi hệ thống.**





**7. 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.**

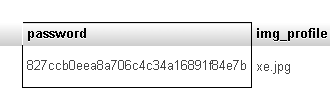
Chèn thêm nút đổi mật khẩu:



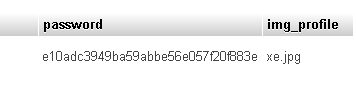
**Đổi mật khẩu từ: 12345 -> 123456**



**Mã băm cũ:**



**Mã băm sau khi đổi mật khẩu:**



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

**upload.**

**Cơ chế:**

Người dùng chọn file từ máy tính → gửi thông tin lên server thông qua form HTML (<form enctype="multipart/form-data">).

PHP nhận file qua biến $\_FILES.

File tạm được lưu vào thư mục tạm thời trên server (thường /tmp).

Ta cần di chuyển file tạm đến thư mục đích (như uploads/) bằng hàm move\_uploaded\_file().

**Để upload file (như ảnh đại diện, tài liệu...) trong PHP, ta sử dụng một số cơ chế và hàm chuẩn của ngôn ngữ:**

- move\_uploaded\_file(tmp, dest)

- is\_uploaded\_file()

- pathinfo()

- filesize()

- mime\_content\_type()

**9. Bạn hãy đọc 5 , mô tả chức năng của hàm này và các tham số trong hàm (tham khảo**

**thêm từ read-csv.php).**

Hàm file() trong PHP dùng để đọc toàn bộ nội dung của một file văn bản vào thành một mảng, trong đó mỗi phần tử là một dòng của file.

**Các tham số trong hàm:**

**$filename:** Đường dẫn đến tập tin cần đọc

**$flags**: Thêm các tùy chọn, ví dụ như FILE\_IGNORE\_NEW\_LINES, FILE\_SKIP\_EMPTY\_LINES

**$context :** Bối cảnh dòng (network/stream) nếu đọc qua giao thức như FTP, HTTP

**10. 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 , 7 . 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.**





