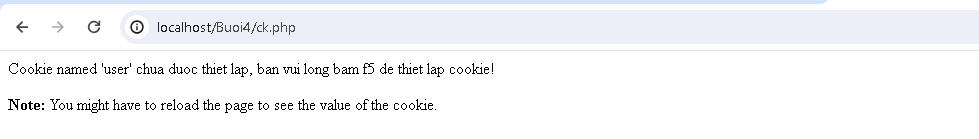
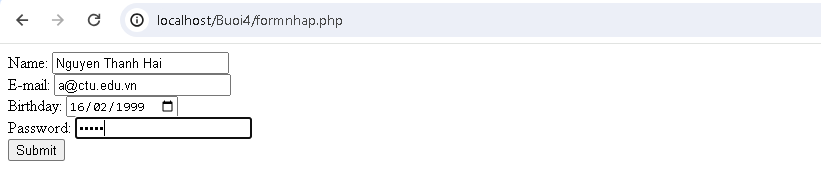
Câu 1:

* ck.php



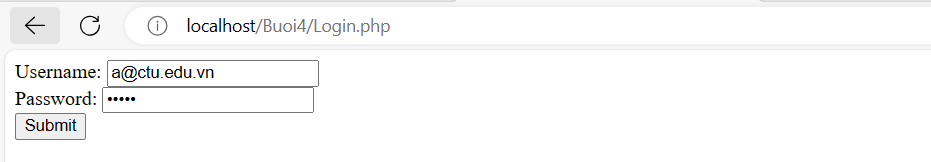
* formnhap.php



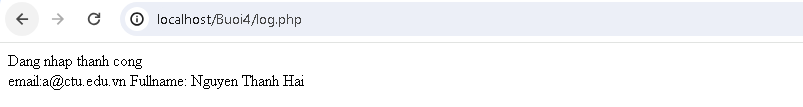
* luu.php



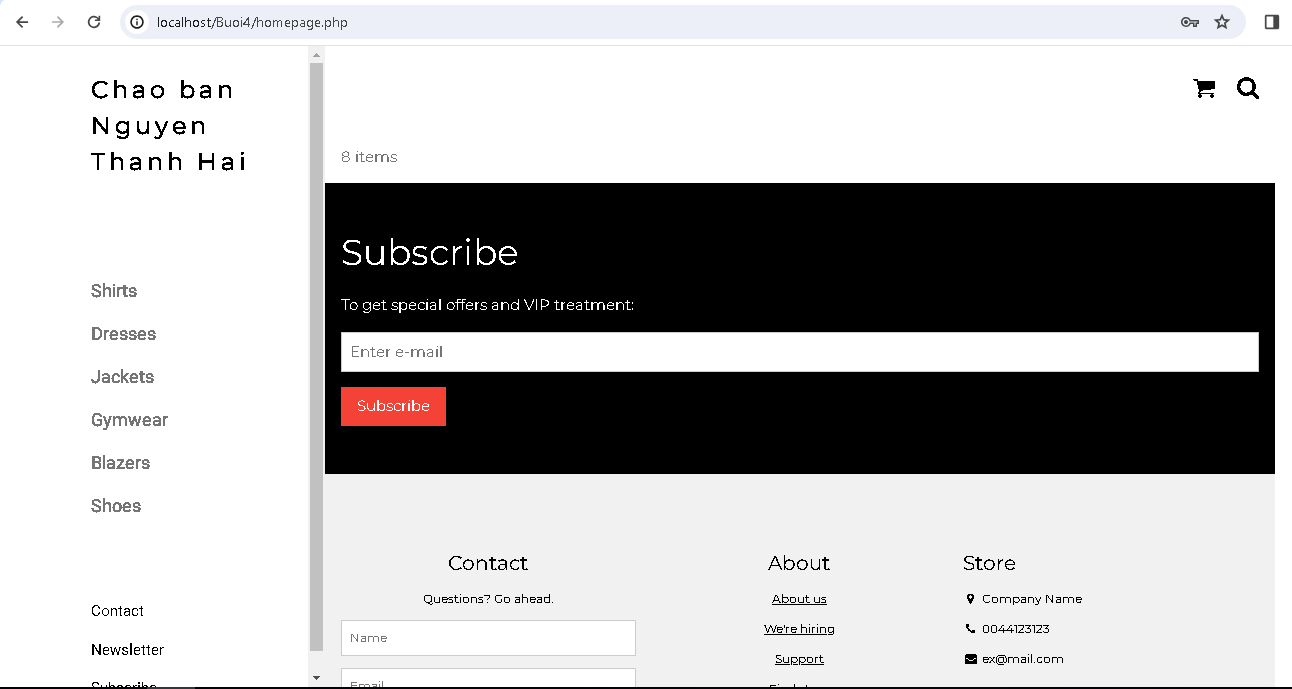
* Login.php



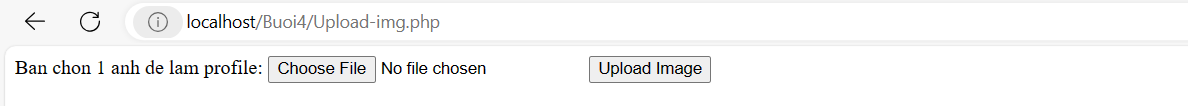
* log.php



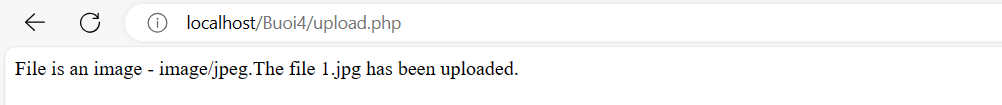
* homepage.php

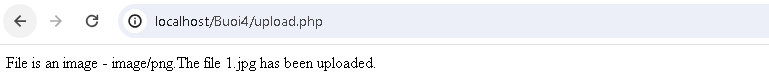


* Upload-img.php

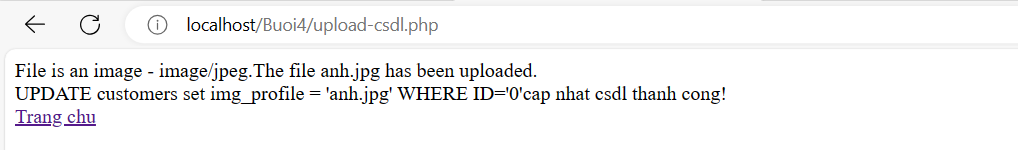


* upload.php

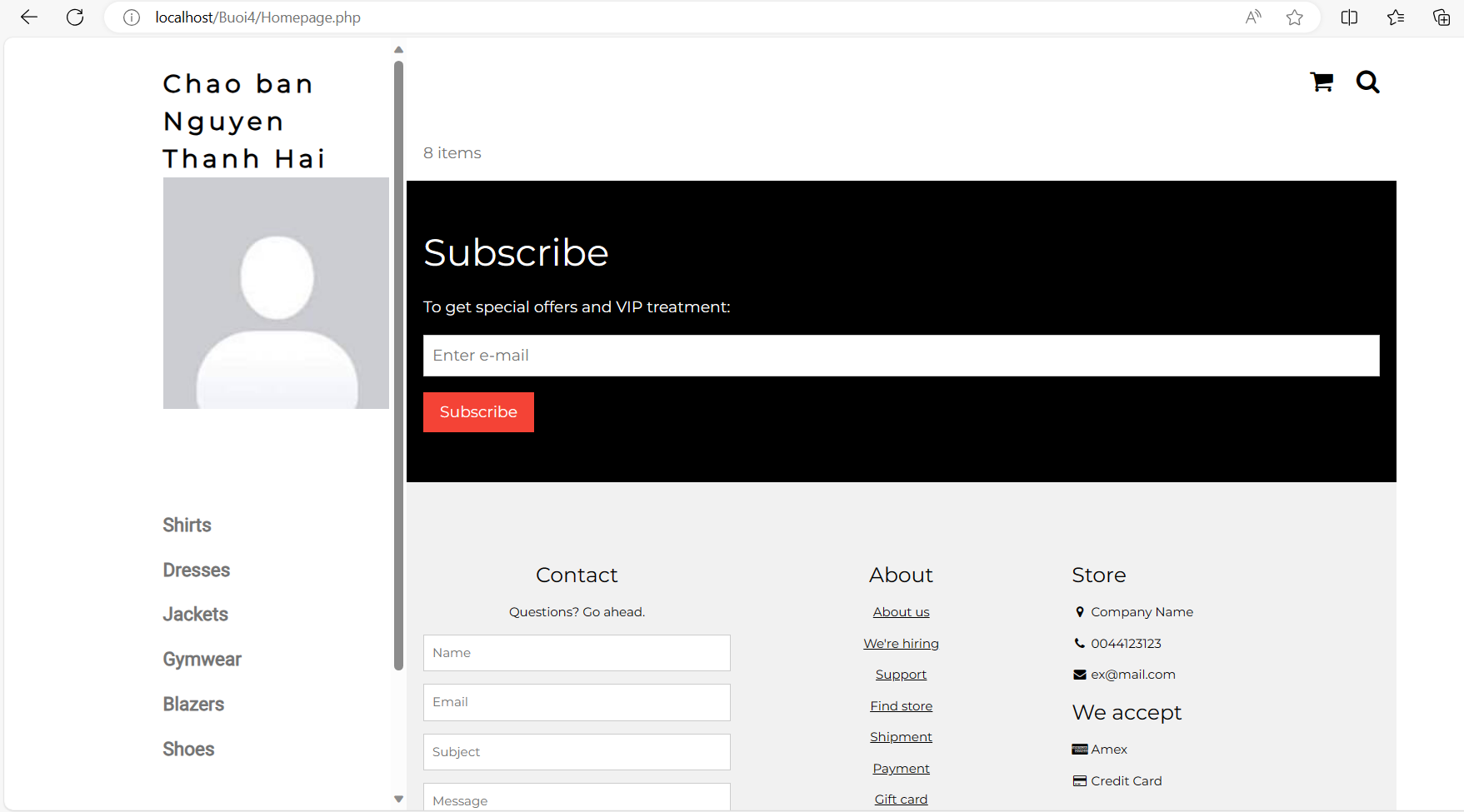




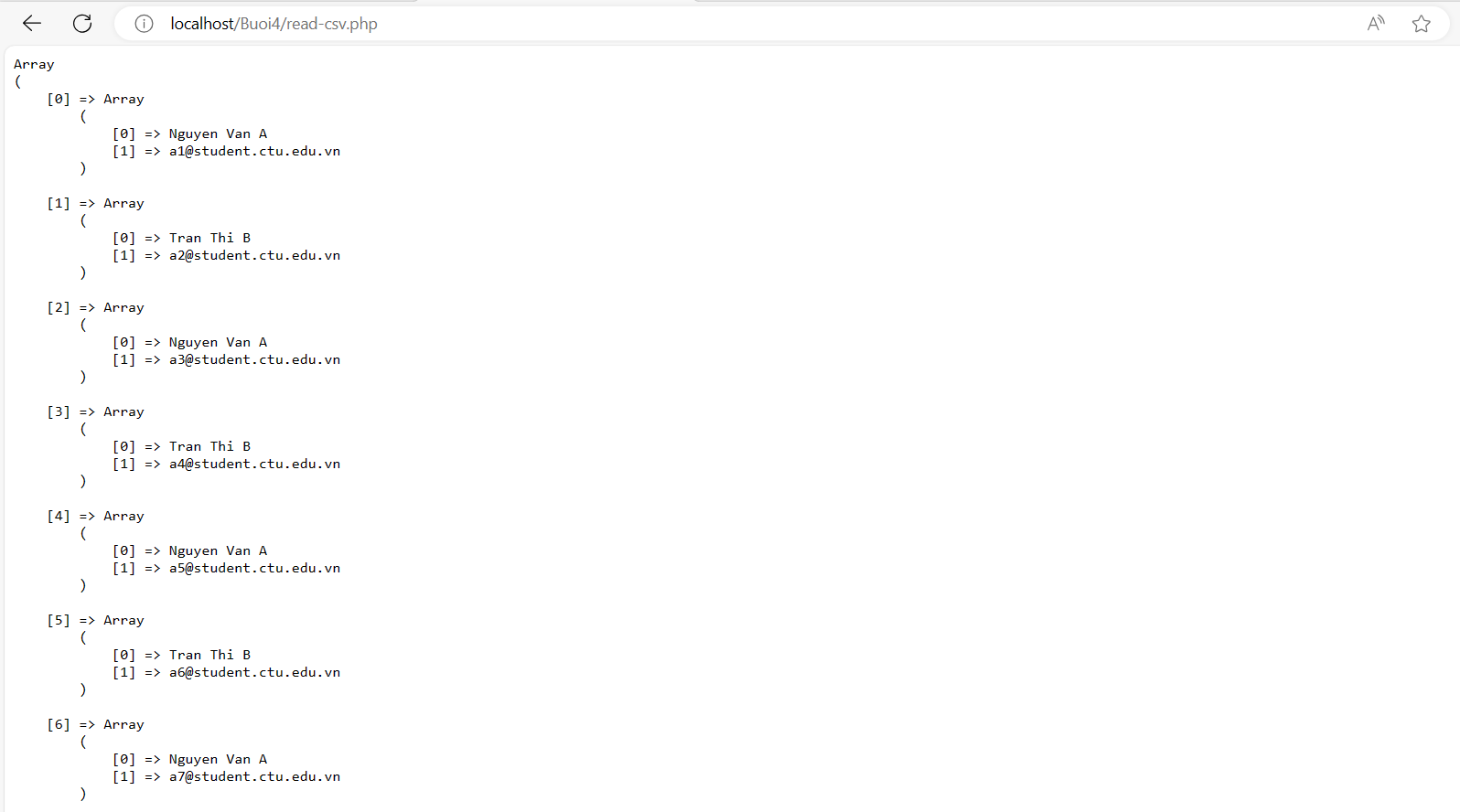
* upload-csdl



* Homepage.php

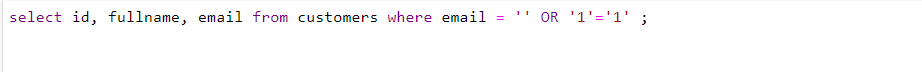


* read-csv

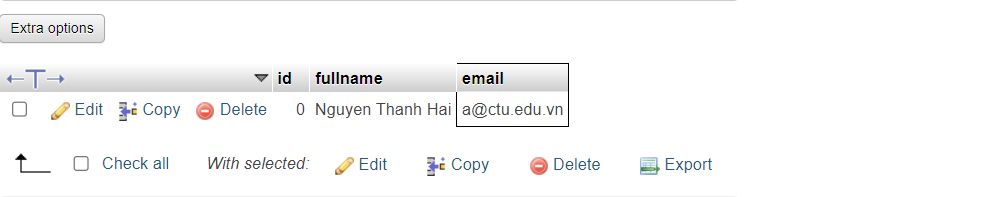


Câu 2:

* SQL Injection là một kỹ thuật tấn công mà kẻ tấn công sử dụng để lạm dụng lỗ hổng bảo mật trong ứng dụng web hoặc ứng dụng cơ sở dữ liệu. Kỹ thuật này cho phép kẻ tấn công chèn các đoạn mã SQL độc hại vào các trường nhập liệu của ứng dụng, từ đó thực hiện các thao tác gian lận, truy xuất hay thậm chí thay đổi cơ sở dữ liệu. Khi thành công, SQL Injection có thể cho phép kẻ tấn công truy xuất, thay đổi hoặc xóa dữ liệu từ cơ sở dữ liệu, thực hiện các hành động không được ủy quyền và thậm chí kiểm soát toàn bộ hệ thống. Điều này có thể gây ra hậu quả nghiêm trọng đối với tính bảo mật và tính toàn vẹn của ứng dụng và cơ sở dữ liệu.
* Truy vấn sql:

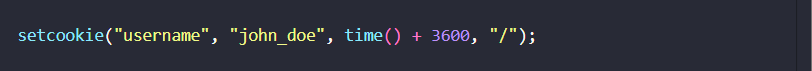


* Kết quả:



Câu 3:

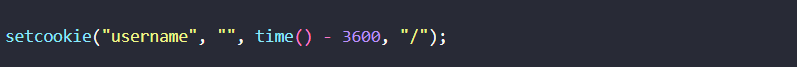
* Cookie là các đoạn thông tin được lưu trữ trên máy tính của người dùng khi họ truy cập các trang web. Cookies thường được sử dụng để lưu trữ thông tin về phiên làm việc, thông tin đăng nhập, sở thích của người dùng, cài đặt ngôn ngữ, giỏ hàng mua sắm, hoặc các dữ liệu khác liên quan đến tương tác trên trang web.
* setcookie(name, value, expire, path, domain, secure, httponly)
* Name: Tên của cookie.
* Value: Giá trị của cookie.
* Expire: Thời gian hết hạn của cookie, có thể là timestamp hoặc 0 nếu muốn cookie hết hạn khi phiên làm việc kết thúc.
* Path: Đường dẫn trên server mà cookie có thể truy cập được.
* Domain: Miền mà cookie có thể truy cập được.
* Secure: Nếu được thiết lập là true, cookie chỉ được gửi qua kết nối an toàn (HTTPS).
* Httponly: Nếu được thiết lập là true, cookies chỉ có thể được truy cập thông qua HTTP.
* Lưu giá trị



* Lấy giá trị:



* Xóa giá trị:



Câu 4:

* Session là một khái niệm trong lập trình web được sử dụng để lưu trữ thông tin phiên làm việc của người dùng trên máy chủ web. Mỗi phiên làm việc được tạo ra khi người dùng truy cập vào trang web và được duy trì cho đến khi người dùng đăng xuất hoặc quá thời gian hết hạn của phiên làm việc.
* Lưu giá trị:



* Lấy giá trị:



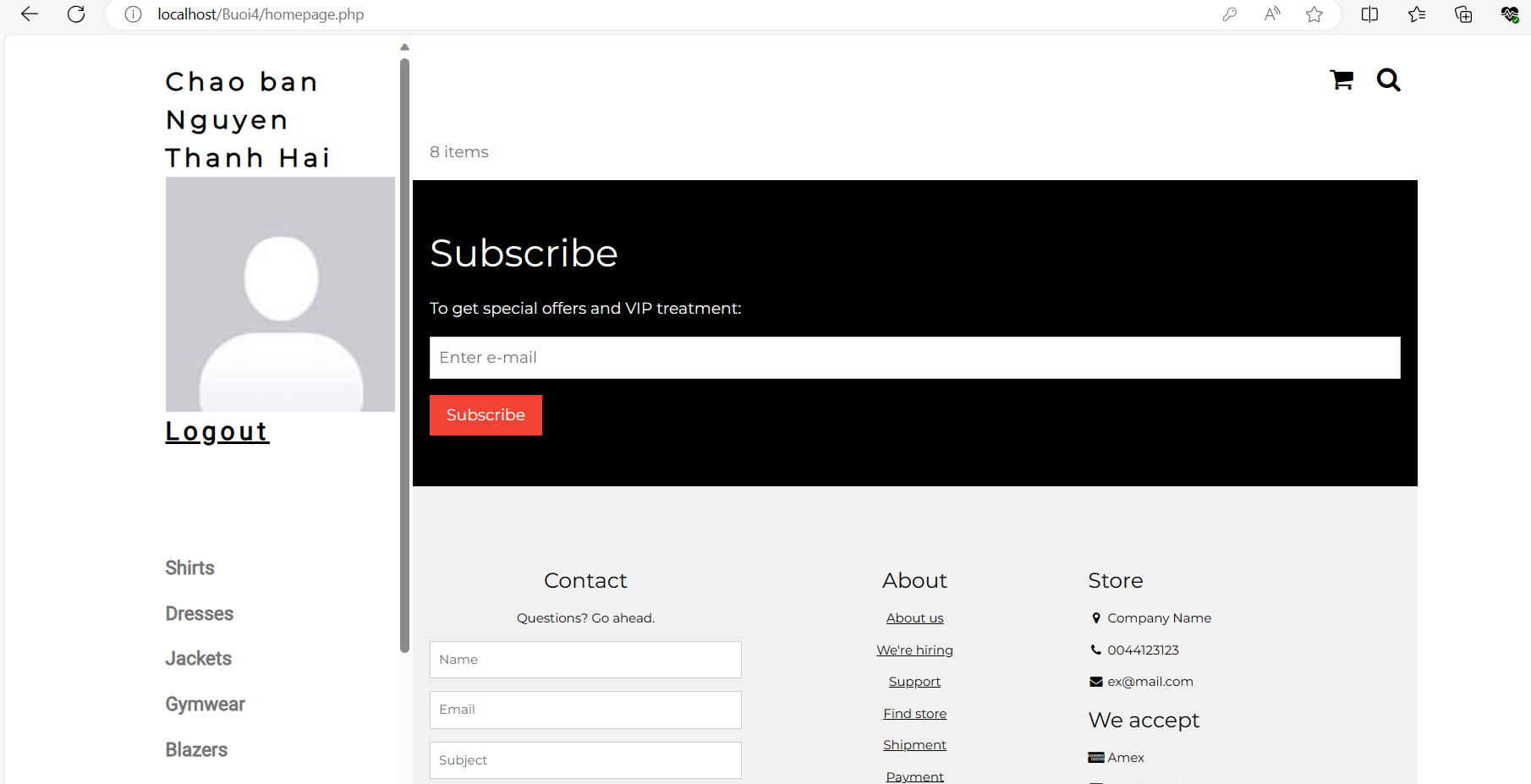
* Xóa giá trị:



Câu 5:

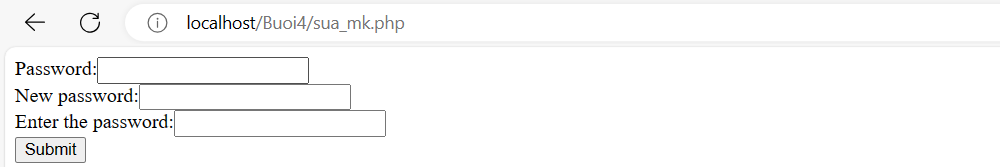
* Cookie:
* Lưu trữ vị trí: Được lưu trữ trên máy tính của người dùng dưới dạng file văn bản. Cookie có thể lưu trữ trên máy tính của người dùng và được gửi đi mỗi khi truy cập vào trang web mà nó thuộc về.
* Bảo mật: Có thể bị đánh cắp hoặc sửa đổi bởi người dùng hoặc bên thứ ba, do đó cần phải được sử dụng cẩn thận khi lưu trữ thông tin nhạy cảm.
* Thời gian lưu trữ: Có thể thiết lập thời gian sống cụ thể, từ vài phút đến vài năm, tùy thuộc vào cấu hình của cookie.
* Dùng để lưu trữ: Thường được sử dụng để lưu trữ thông tin đăng nhập, sở thích của người dùng, theo dõi hoạt động trên website.
* Chuyển thông giữa các trang: Cookie cần được chuyển giữa các trang.
* Session:
* Lưu trữ vị trí: Thông tin session được lưu trữ trên máy chủ và chỉ có một ID phiên làm việc được lưu trữ trên trình duyệt của người dùng dưới dạng cookie.
* Bảo mật: Thông tin session được lưu trữ trên máy chủ, do đó tốt hơn về mặt bảo mật so với Cookie.
* Thời gian lưu trữ: Thông tin session tồn tại cho đến khi người dùng đăng xuất hoặc hết thời gian định nghĩa cho phiên làm việc.
* Dùng để lưu trữ: Được sử dụng để lưu trữ thông tin phiên làm việc, thông tin đăng nhập và các thông tin liên quan đến trạng thái của người dùng trên ứng dụng web.
* Chuyển đổi giữa các trang: session không cần vì dữ liệu được lưu trữ trên máy chủ.

Câu 6:

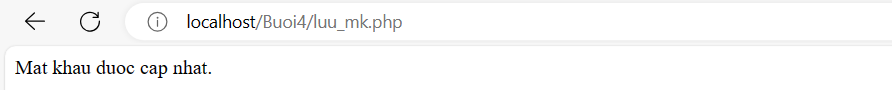


Câu 7:

* sua\_mk.php

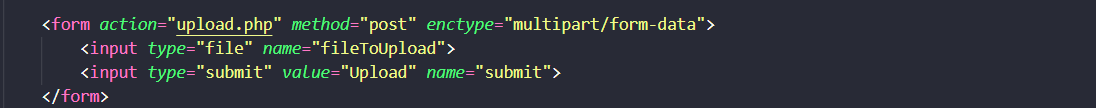


* luu\_mk.php

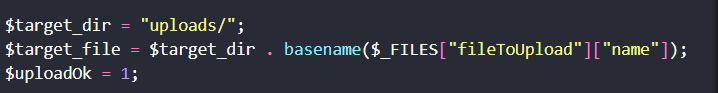


Câu 8:

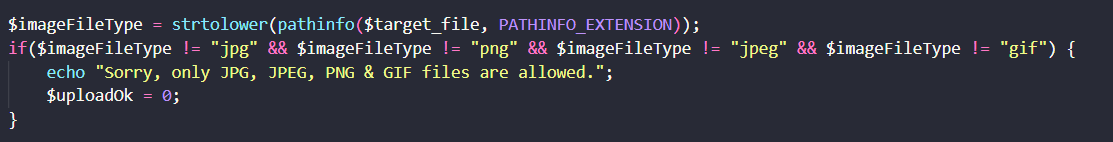
* Để thực hiện việc tải lên (upload) tập tin trong môi trường web, có một số cơ chế và thủ tục cơ bản có thể được sử dụng, phổ biến nhất là thông qua ngôn ngữ lập trình PHP và các thư viện kết hợp.
* 1. HTML Form:
* Để cho phép người dùng tải lên tập tin từ trình duyệt, bạn cần tạo một form HTML với thuộc tính "enctype" được đặt là "multipart/form-data" để cho phép tải lên các tập tin.
* action: Đường dẫn tới script xử lý việc upload.
* method: Phương thức gửi dữ liệu, thường là post.
* enctype="multipart/form-data": Quan trọng để hỗ trợ upload file.
* Ví dụ:



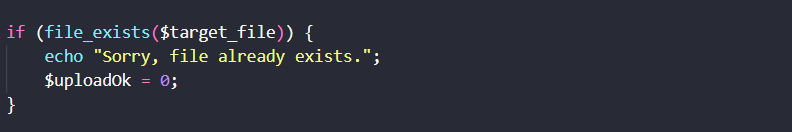
* 2. PHP Upload Function: Trong file PHP được đặt trong thuộc tính action của form, bạn sẽ xử lý quá trình upload. Các bước chính bao gồm:
* Kiểm tra sự tồn tại của tệp tin và thư mục đích để lưu trữ:



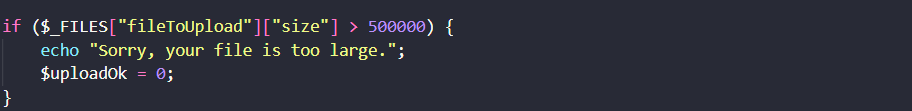
* Kiểm tra kiểu file:



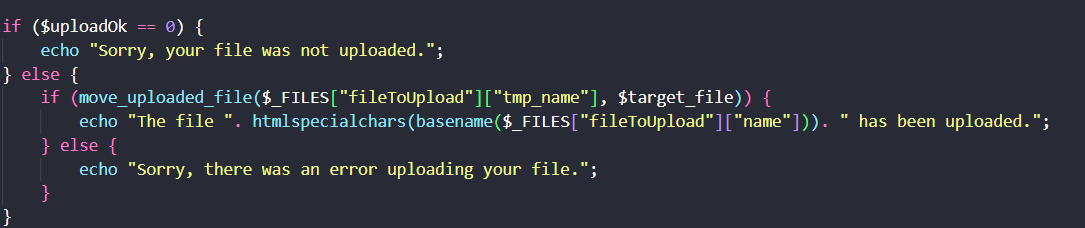
* Kiểm tra file đã tồn tại hay chưa:



* Kiểm tra dung lượng file:



* Thực hiện upload nếu không có lỗi:



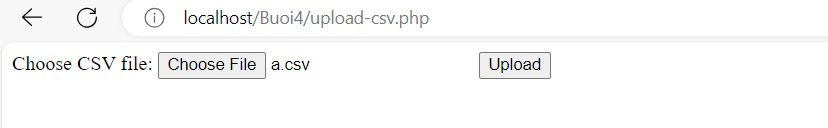
* Các hàm/thủ tục chính:
* Move\_uploaded\_file(): Di chuyển file từ thư mục tạm thời đến thư mục đích trên máy chủ.
* basename(): Trả về phần tên file từ một đường dẫn.
* file\_exists(): Kiểm tra xem file đã tồn tại hay chưa.
* strtolower() và pathinfo(): Lấy thông tin về đường dẫn file, bao gồm cả phần mở rộng của file.
* $\_FILES superglobal: Một mảng chứa thông tin về file đã được tải lên.
* enctype="multipart/form-data": Đặt thuộc tính enctype trong thẻ <form> để hỗ trợ upload file

Câu 9:

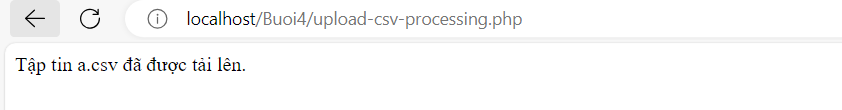
* file\_exists($filename): được sử dụng để kiểm tra xem một tập tin hoặc thư mục có tồn tại hay không.
* Đường dẫn tới tập tin hoặc thư mục mà bạn muốn kiểm tra.
* is\_file($filename): được sử dụng để kiểm tra xem một đường dẫn tới một tập tin có tồn tại và đúng là một tập tin không.
* Đường dẫn tới tập tin hoặc thư mục mà bạn muốn kiểm tra.
* Str\_getcsv(): được sử dụng để phân tích một chuỗi chứa dữ liệu CSV và trả về một mảng.
* $input (bắt buộc): Chuỗi chứa dữ liệu CSV cần phân tích.
* $delimiter (tùy chọn): Ký tự phân cách giữa các trường (mặc định là ,).
* $enclosure (tùy chọn): Ký tự bao quanh các trường (mặc định là ").
* escape (tùy chọn): Ký tự escape (mặc định là \).
* file(): được sử dụng để đọc toàn bộ nội dung của một tập tin và trả về một mảng, với mỗi phần tử của mảng là một dòng trong tập tin.
* $filename (bắt buộc): Tên của tập tin cần đọc.
* $flags (tùy chọn): Các cờ kiểm soát cách hàm sẽ hoạt động. Trong đoạn mã, FILE\_IGNORE\_NEW\_LINES được sử dụng để loại bỏ ký tự mới (\n) từ cuối mỗi dòng.
* file\_get\_contents(): được sử dụng để đọc toàn bộ nội dung của một tập tin và trả về nội dung đó dưới dạng một chuỗi.
* $filename (bắt buộc): Đường dẫn tới tập tin cần đọc.
* $use\_include\_path (tùy chọn): Nếu được đặt là TRUE, hàm sẽ tìm kiếm file trong các đường dẫn include\_path nếu không tìm thấy trong đường dẫn cụ thể.
* $context (tùy chọn): Một nguồn ngữ cảnh (context) cung cấp nhiều tùy chọn cho hàm, thường được sử dụng để xử lý quyền truy cập file.
* $offset (tùy chọn): Bắt đầu đọc từ vị trí này trong file. Được sử dụng nếu bạn muốn bắt đầu đọc từ một vị trí cụ thể trong file.
* $maxlen (tùy chọn): Số lượng ký tự tối đa bạn muốn đọc. Nếu không được chỉ định, hàm sẽ đọc toàn bộ file.
* fopen(): được sử dụng để mở một tập tin hoặc URL.
* $filename (bắt buộc): Đường dẫn tới tập tin hoặc URL cần mở.
* $mode (bắt buộc): Chế độ mở tập tin. Điều này xác định liệu tập tin sẽ được mở để đọc, ghi, hoặc các hoạt động khác.
* $use\_include\_path (tùy chọn): Nếu được đặt là TRUE, hàm sẽ tìm kiếm tập tin trong các đường dẫn include\_path.
* $context (tùy chọn): Một nguồn ngữ cảnh (context) cung cấp nhiều tùy chọn cho hàm, thường được sử dụng để xử lý quyền truy cập tập tin.
* fgets(): được sử dụng để đọc một dòng từ tập tin.
* $handle (bắt buộc): Con trỏ tới tập tin đã mở bằng fopen().
* $length (tùy chọn): Số ký tự tối đa bạn muốn đọc.

Câu 10:

* upload-csv



* upload-csv-processing



* read-csv.php

