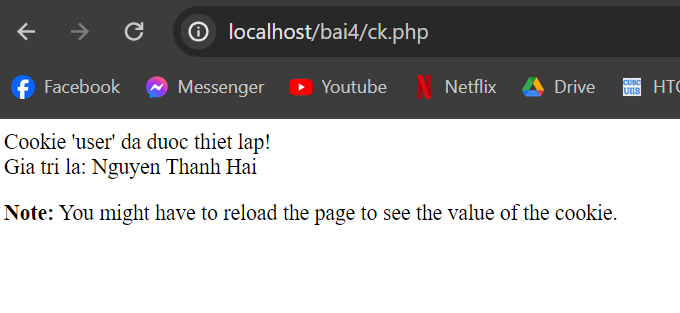
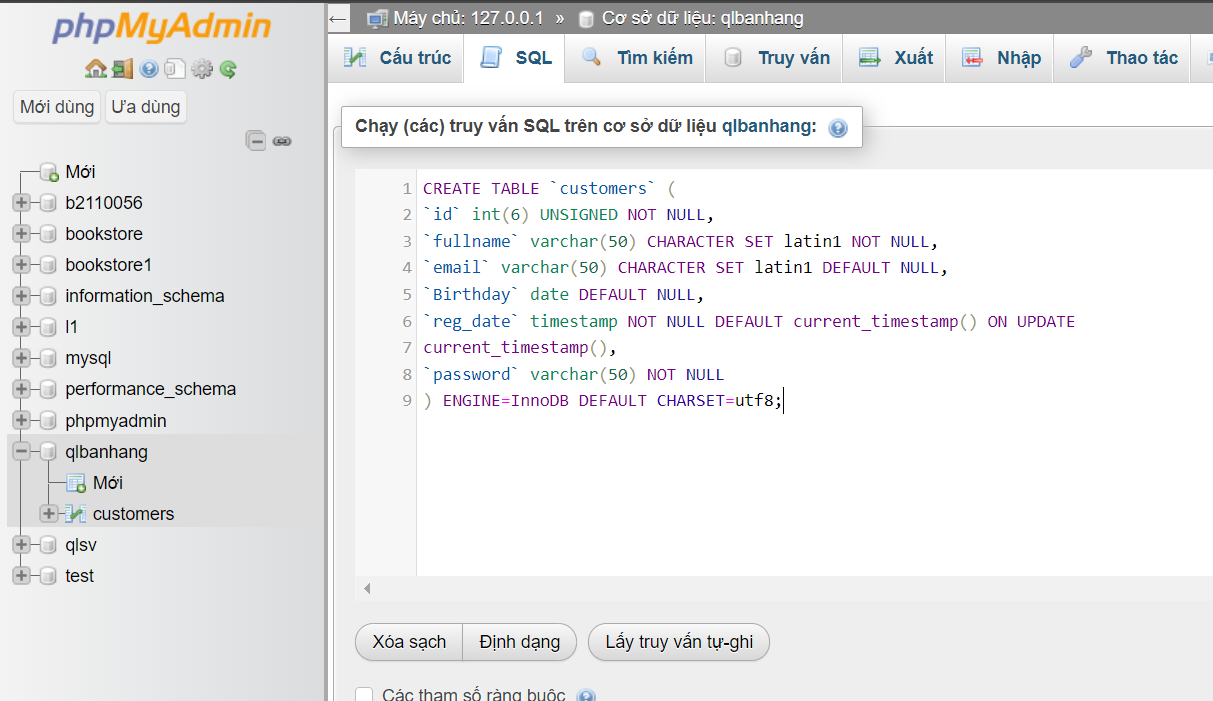
**1. Bạn hãy chạy tất cả các lệnh hướng dẫn ở trên và chụp lại màn hình kết quả.**

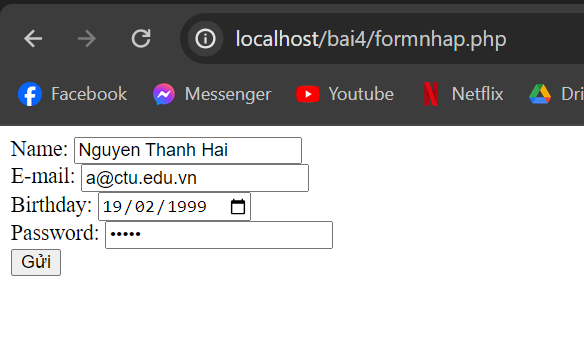
Tạo cookies ck.php

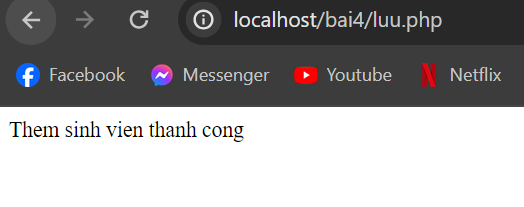


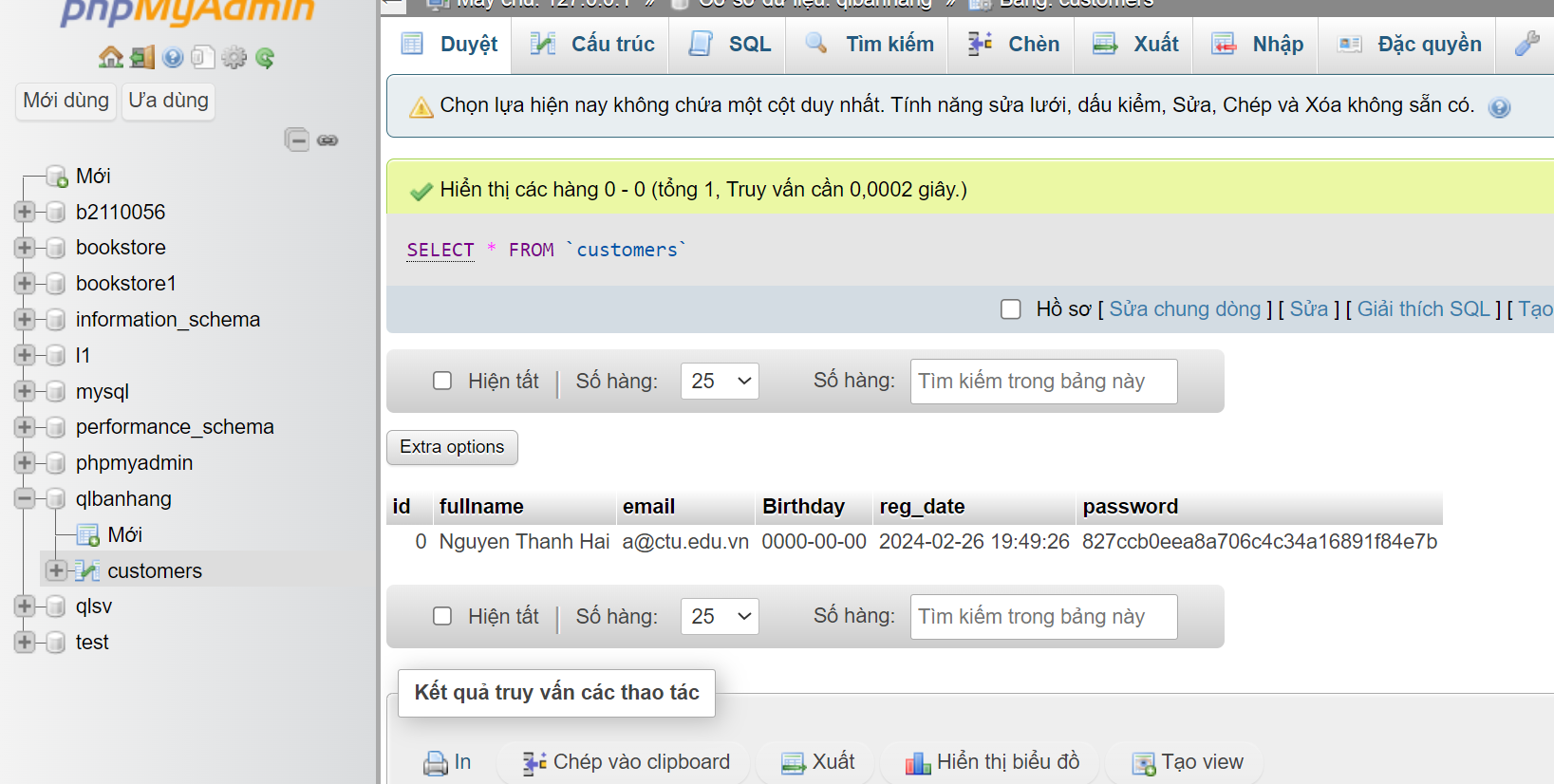
Tạo 1 trang đăng ký người dùng với mật khẩu được mã hóa



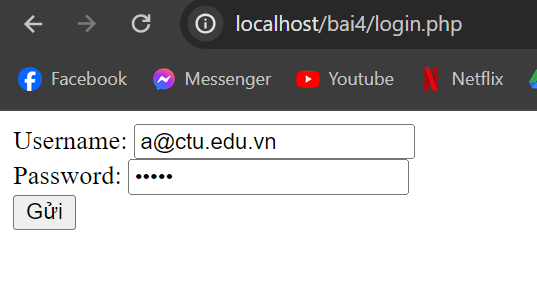
formnhap.php



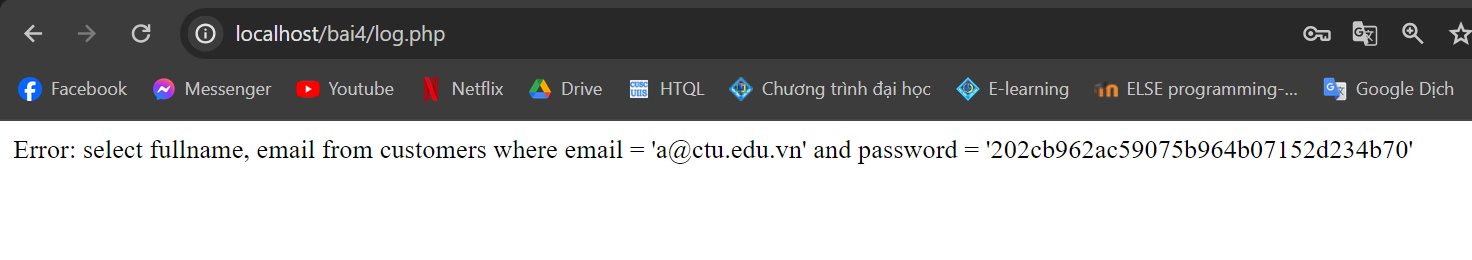


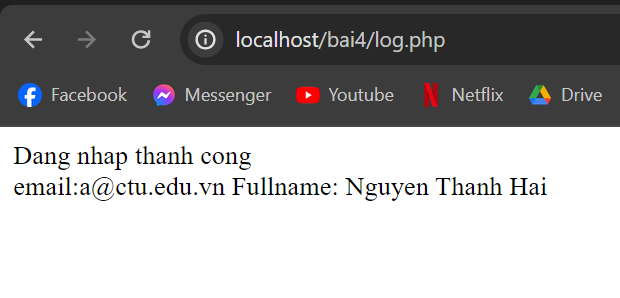
luu.php

login.php

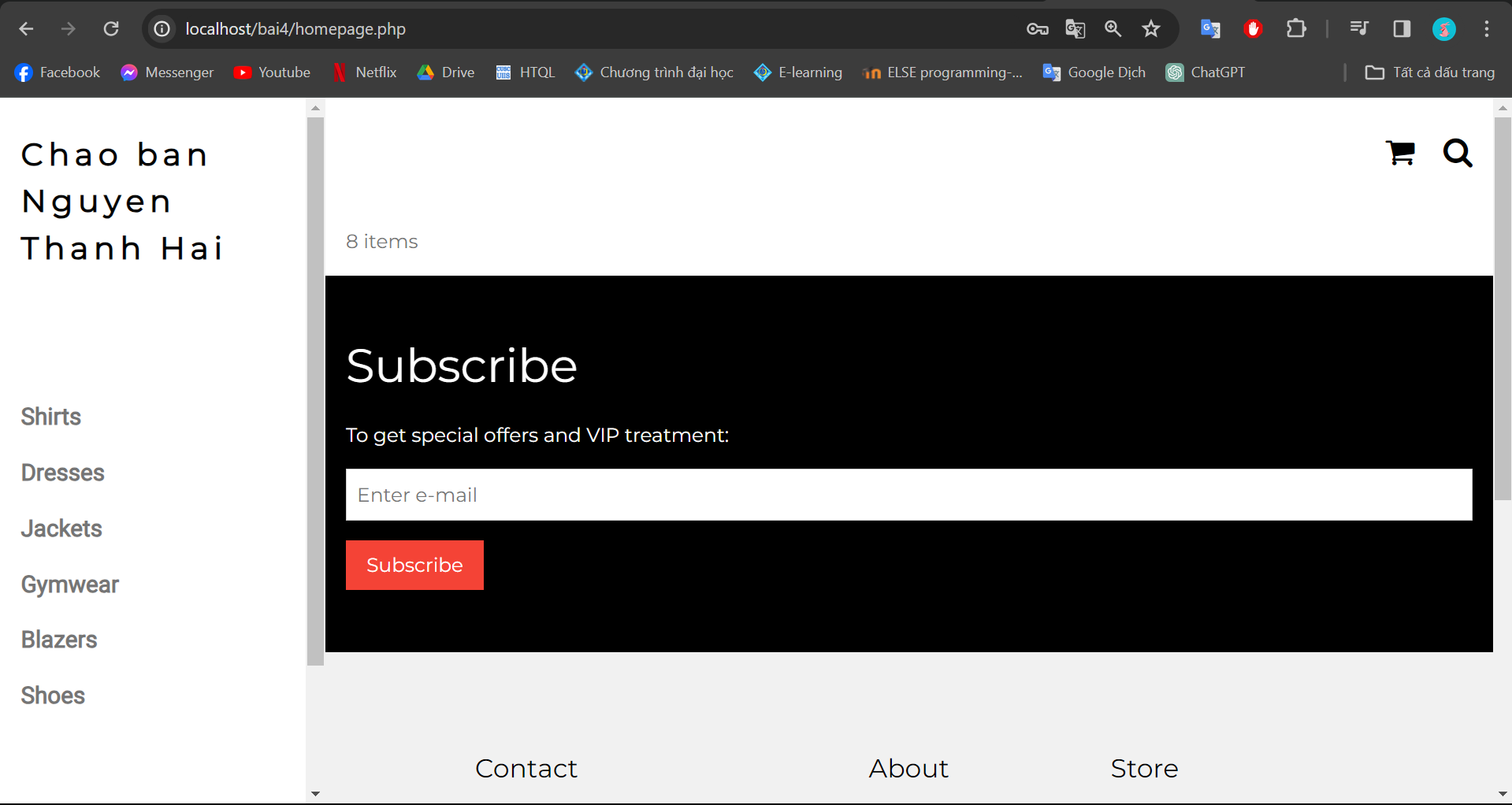


log.php

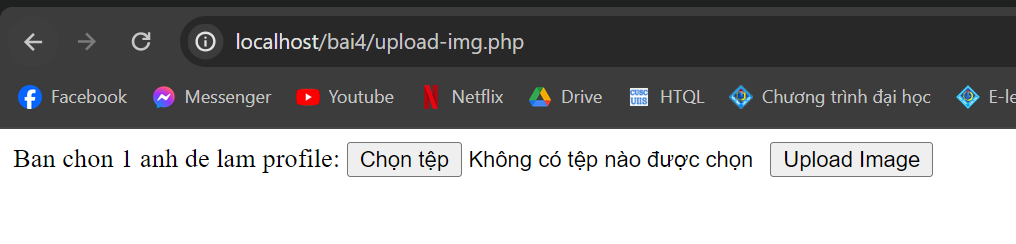




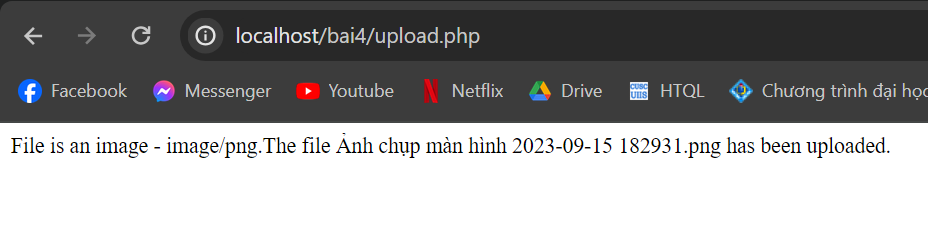
homepage.php



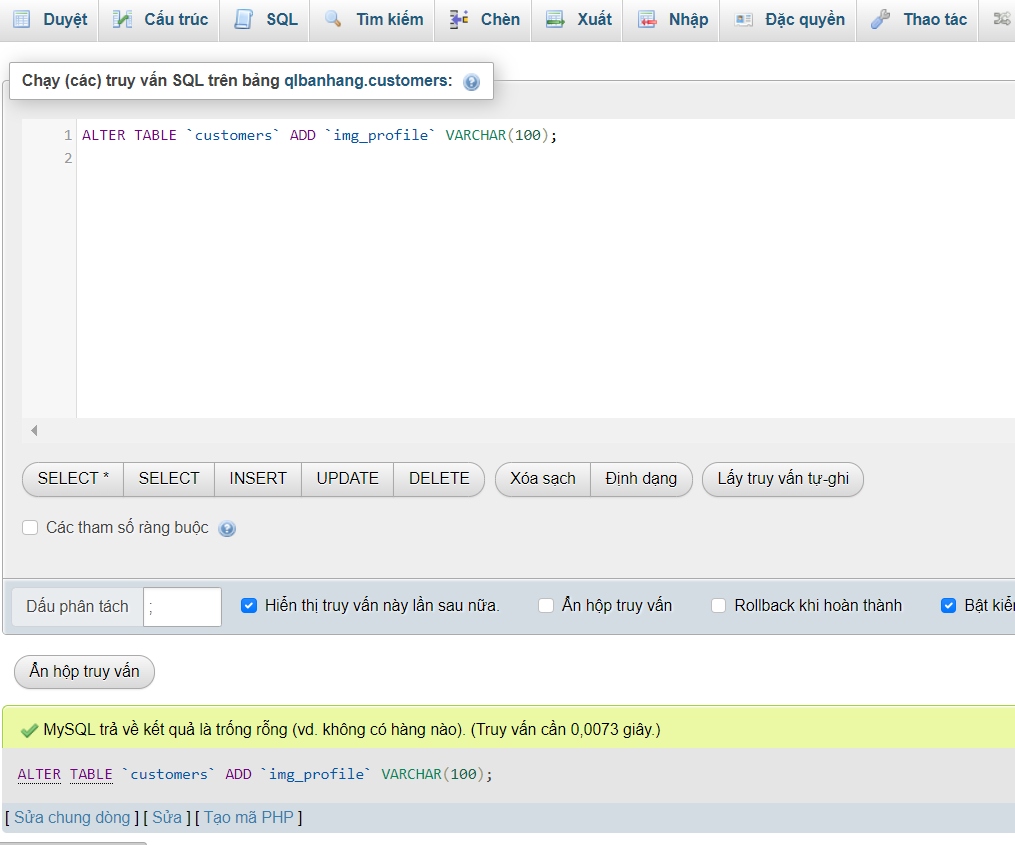
upload-img.php



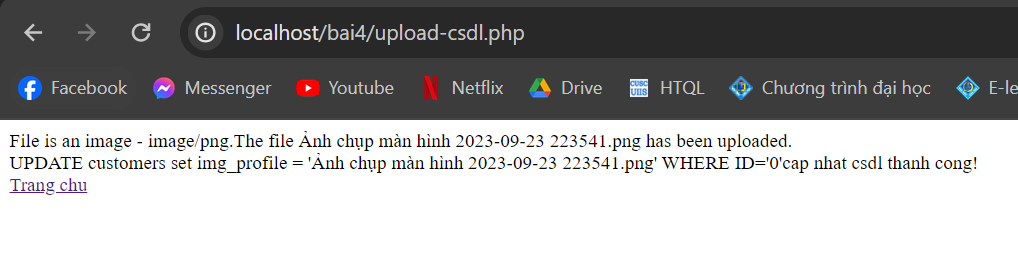
upload.php

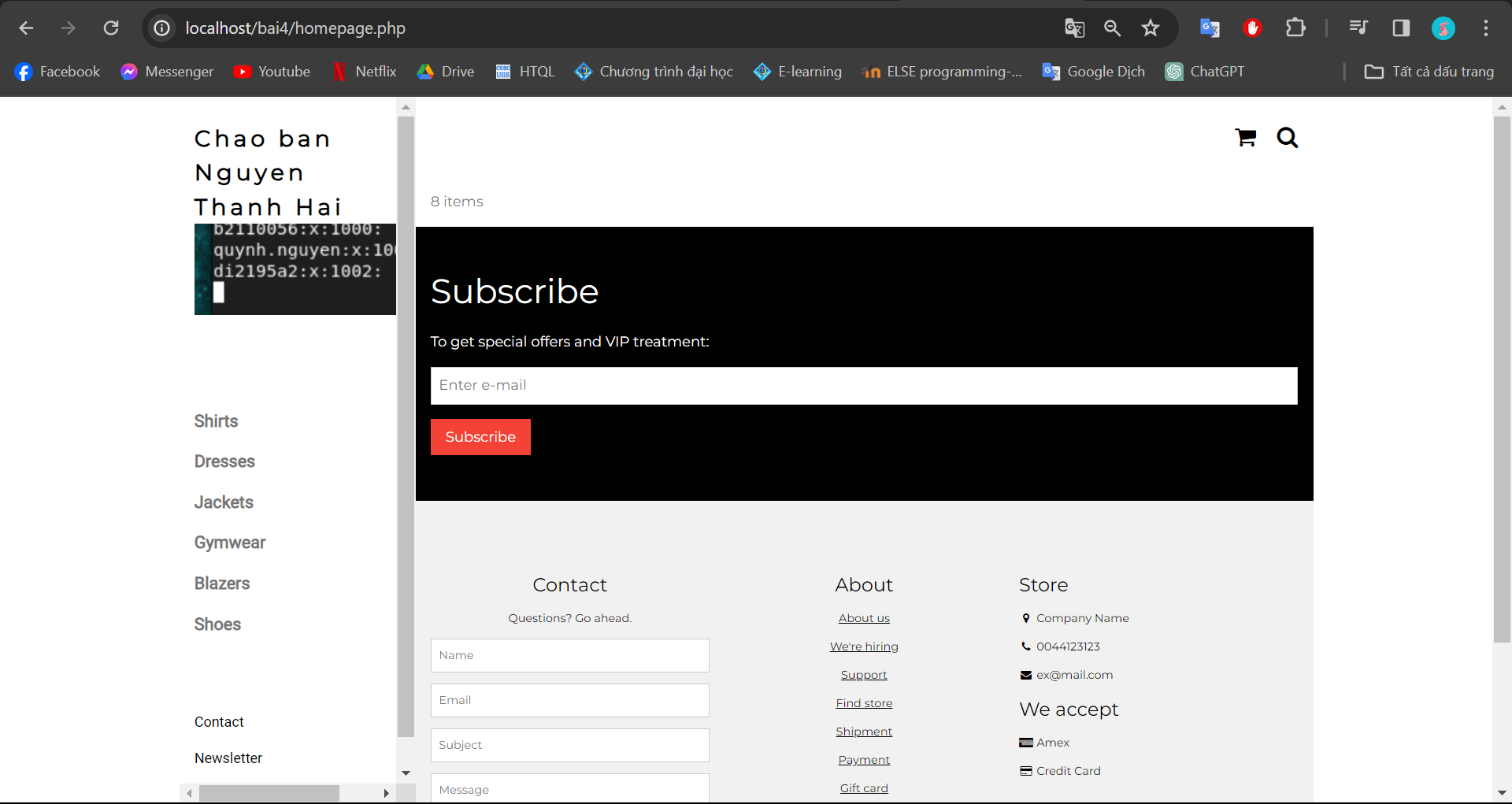


upload-img.php(modified)

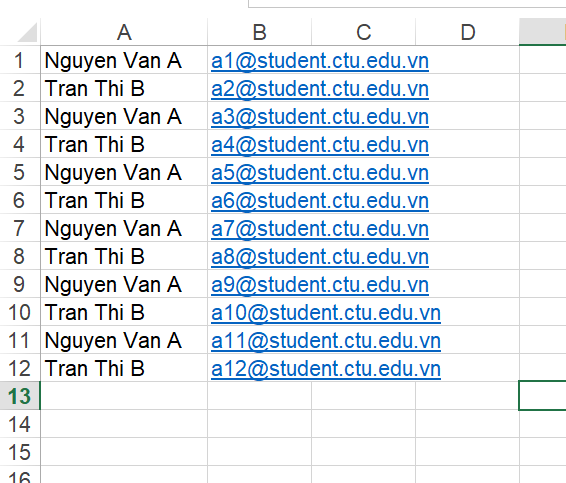


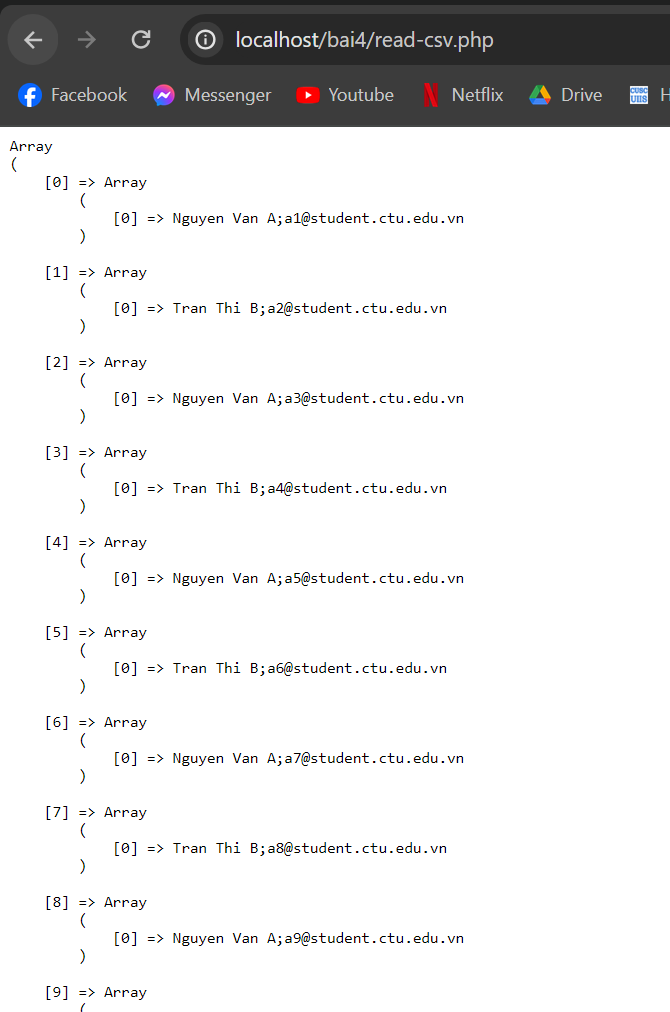
upload-csdl.php

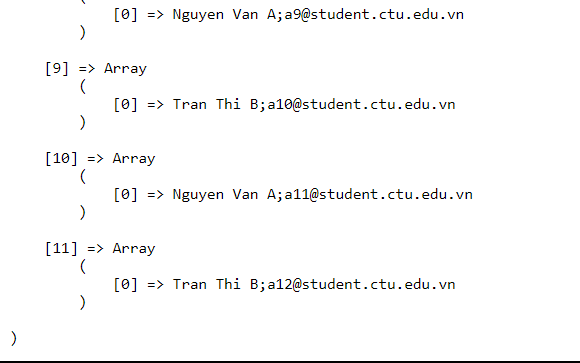




read-csv.php







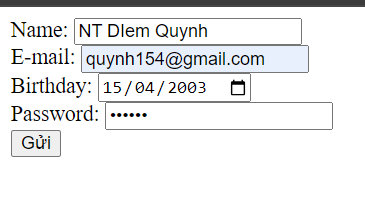
**2. Trong vài trường hợp, hacker có thể sử dụng các kỹ thuật SQL Injection để hack hệ thống của bạn. Bạn hãy trình bày SQL Injection là gì và thử các ví dụ trình bày trong 1. Ứng dụng kỹ thuật đó vào trang đăng nhập mà bạn đã tạo, chụp lại các kết quả.**

SQL Injection là một kỹ thuật chèn mã có thể phá hủy cơ sở dữ liệu của bạn.

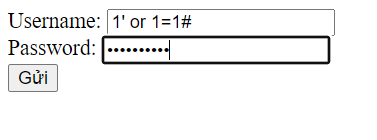
SQL Injection là một trong những kỹ thuật hack web phổ biến nhất.

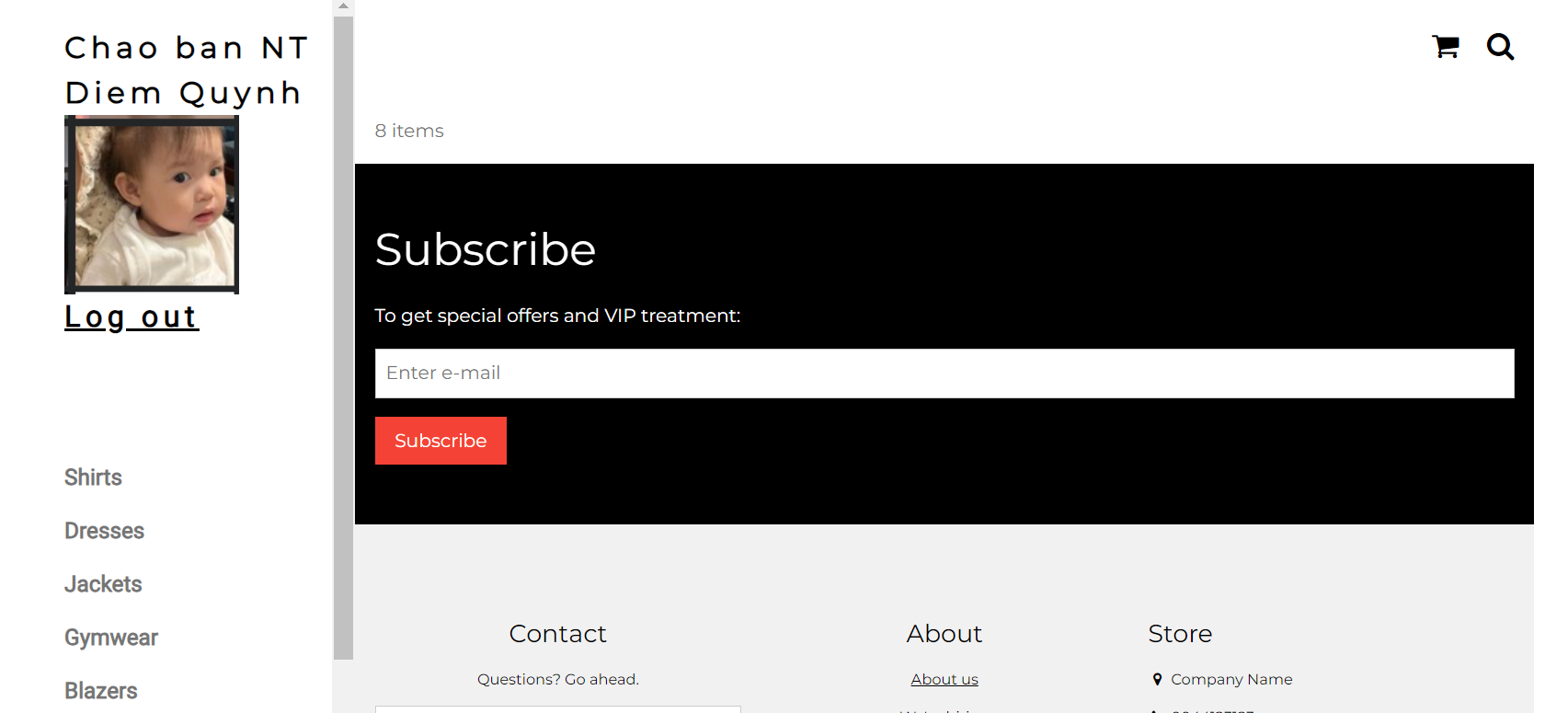
SQL Injection là việc đặt mã độc vào câu lệnh SQL thông qua đầu vào trang web.

Ứng dụng vào trang đăng nhập:



Đăng nhập vào trang login với tài khoản và mật khẩu cùng key “1’ or 1=1 #”





**3.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 thường được sử dụng để nhận dạng người dùng. Cookie là một tệp nhỏ mà máy chủ nhúng vào máy tính của người dùng. Mỗi lần máy tính đó yêu cầu một trang bằng trình duyệt, nó cũng sẽ gửi cookie. Với PHP, bạn có thể vừa tạo vừa truy xuất các giá trị cookie.

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

name: Tên của cookie.

value: Giá trị của cookie. Đây là dữ liệu bạn muốn lưu trữ trong cookie.

expire: Thời gian hết hạn của cookie, được biểu diễn dưới dạng timestamp Unix (số giây tính từ 1/1/1970). Cookie sẽ tự động hết hạn sau khoảng thời gian này. Nếu bạn đặt expire thành 0, cookie sẽ hết hạn khi phiên duyệt kết thúc.

path: Đường dẫn trong đó cookie có thể được truy cập. Nếu bạn đặt path, cookie chỉ có thể được truy cập từ các trang có đường dẫn bắt đầu bằng giá trị path này.

domain: Tên miền mà cookie áp dụng. Cookie sẽ được gửi đến máy chủ chỉ định bởi tên miền này. Mặc định là tên miền của trang web hiện tại.

secure: Xác định liệu cookie có sử dụng kết nối bảo mật (HTTPS) hay không. Nếu secure được đặt thành true, cookie sẽ chỉ được gửi qua kết nối bảo mật.

httponly: Nếu được đặt thành true, cookie sẽ chỉ được truy cập thông qua giao thức HTTP và không thể truy cập bằng JavaScript. Điều này giúp ngăn chặn các cuộc tấn công Cross-Site Scripting (XSS) mà có thể lấy thông tin cookie của người dùng.

Ví dụ:

-Cách lưu trong cookie.

<?php

$cookie\_name = "user";

$cookie\_value = "Nguyen Thanh Hai";

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

?>

-Cách lấy giá trị trong cookie

<?php

echo $\_COOKIE["username"];

?>

-Cách xóa giá trị trong cookie

<?php

// Thiết lập thời gian hết hạn của cookie thành một thời điểm trong quá khứ

$expire = time() - 3600; // 1 giờ trước đây

setcookie("user", "", $expire, "/");

?>

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

Session trong PHP được sử dụng để lưu trữ thông tin của người dùng qua các trang web trong suốt phiên làm việc (session). Phiên làm việc bắt đầu khi người dùng truy cập vào trang web và kết thúc khi họ đóng trình duyệt hoặc phiên làm việc hết hạn do thiết lập.

Cách lưu giá trị trong Session

session\_start();

$\_SESSION['user'] = 'John Doe';

Cách lấy giá trị trong Session

echo "Welcome back " . $\_SESSION["user"] . ".";

Cách xóa giá trị trong Session

// xóa tất cả các Session

session\_unset();

//Hủy các session

session\_destroy();

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

Cookie và Session là hai cách để lưu trữ thông tin của người dùng trên web. Một số điểm khác biệt chính là:

•Cookie là tệp nhỏ được lưu trữ trên máy khách, còn Session là biến toàn cục được lưu trữ trên máy chủ.

•Session phụ thuộc vào Cookie, nhưng Cookie không phụ thuộc vào Session.

•Session kết thúc khi người dùng đóng trình duyệt hoặc đăng xuất khỏi ứng dụng, còn Cookie hết hạn tùy thuộc vào thời gian bạn đặt cho nó.

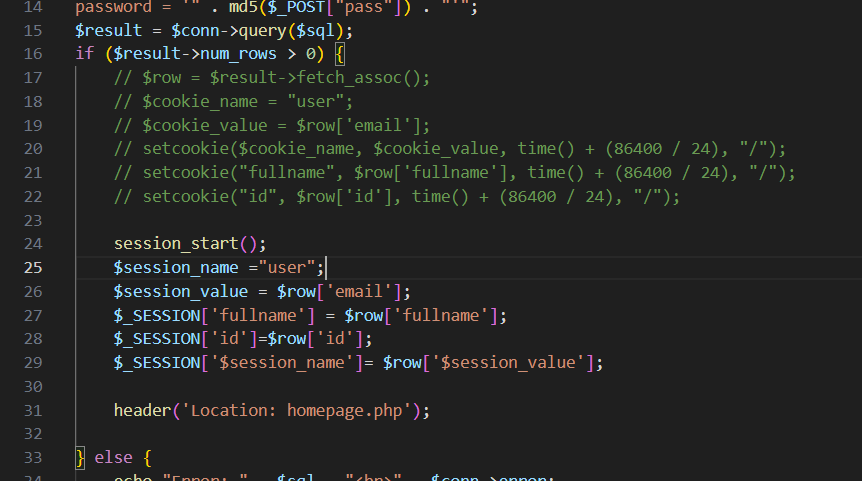
•Session có thể lưu trữ nhiều dữ liệu như người dùng muốn, còn Cookie có kích thước giới hạn là 4KB.

•Session lưu trữ dữ liệu dưới dạng mã hóa, còn Cookie lưu trữ dữ liệu dưới dạng văn bản.

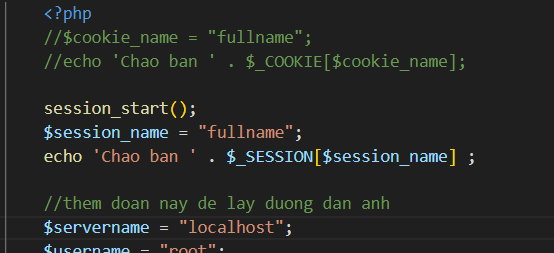
•Session an toàn hơn Cookie.

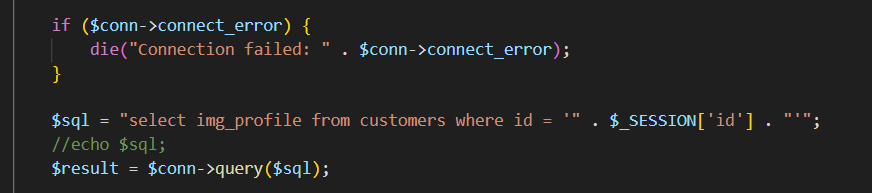
**6. Chỉnh sửa các đoạn gán, khởi tạo, lấy giá trị cookie trong log.php và homepage.php thay bằng cách dùng Session. Tạo tập tin thoat.php để xóa các giá trị trong session, cookie thực hiện chức năng log out khỏi hệ thống.**

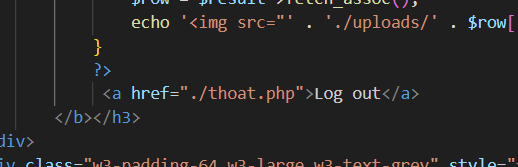
Chỉnh sửa trong log.php



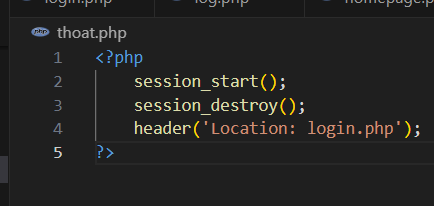
Chỉnh sửa trong homepage.php

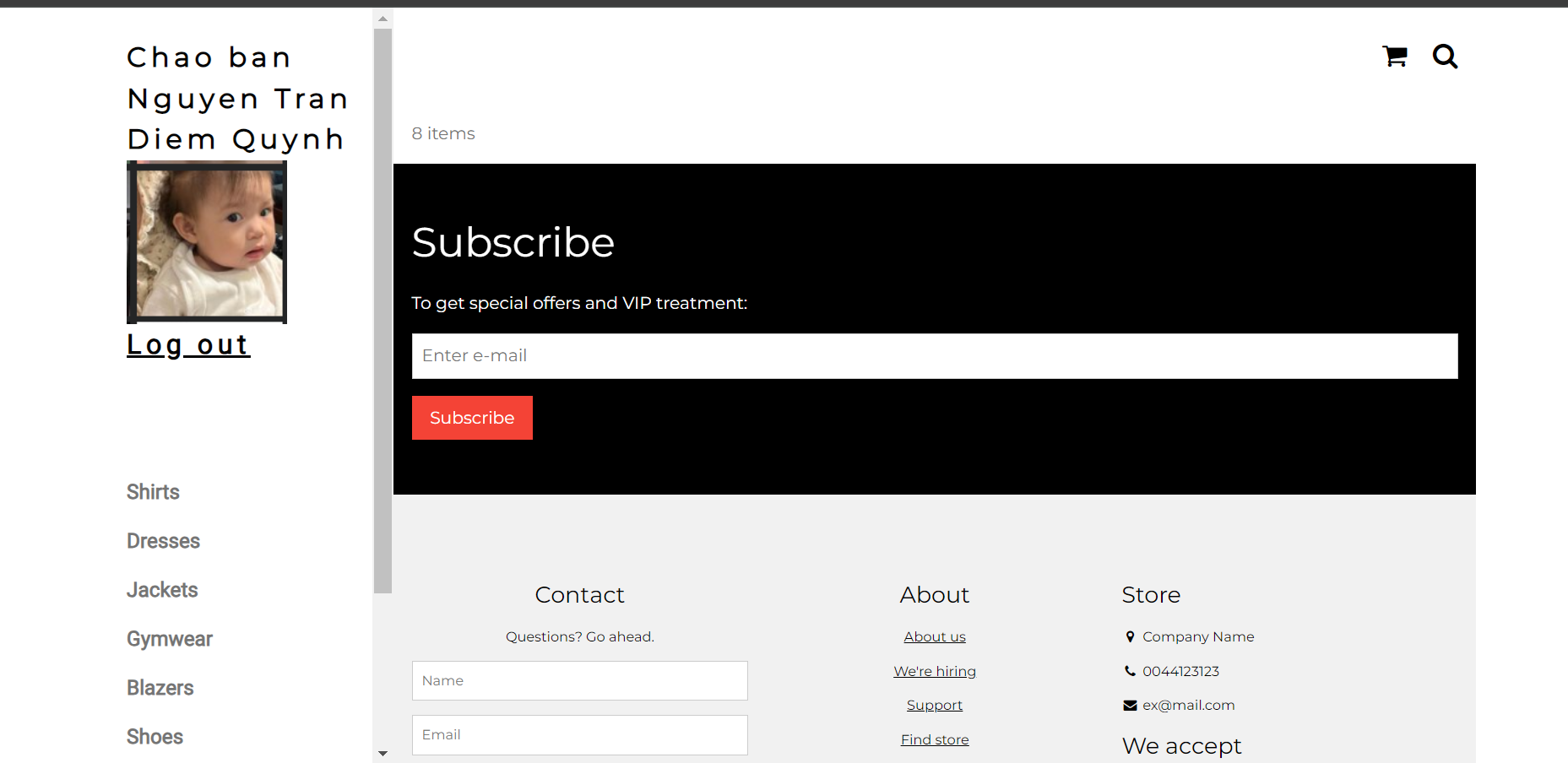






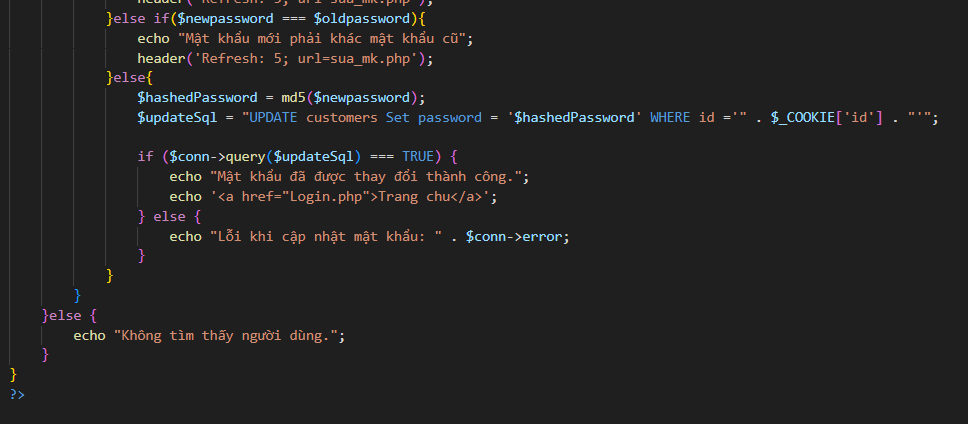
Thoat.php

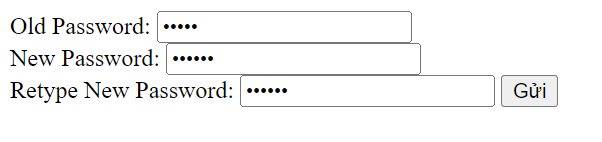




**7. Bạn hãy tạo form sua\_mk.php cho phép người dùng chỉnh sửa mật khẩu sau khi đăng nhập. Yêu cầu gồm 3 input: ô để nhập mật khẩu cũ, 1 ô để nhập mật khẩu mới, 1 ô cho phép nhập mật lại mật khẩu mới. Khi nhập xong cần đảm bảo: mật khẩu cũ là khớp với CSDL đang lưu, 2 ô nhập mật khẩu mới phải khớp với 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.**

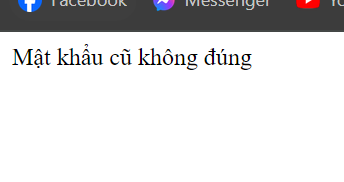
sua\_mk.php



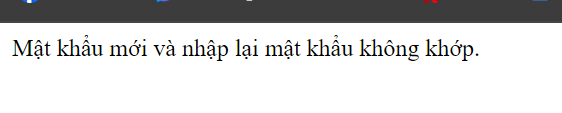


Thử các trường hợp

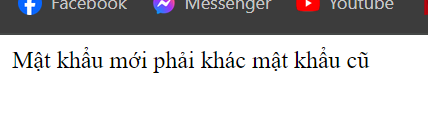
* Mật khẩu cũ Không khớp với CSDL đang lưu



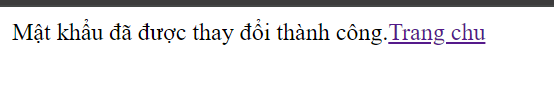
* 2 ô nhập mật khẩu mới phải khớp với nhau



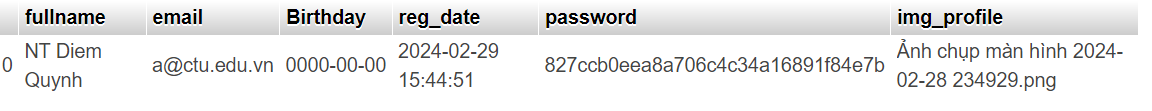
* Không được giống với mật khẩu cũ



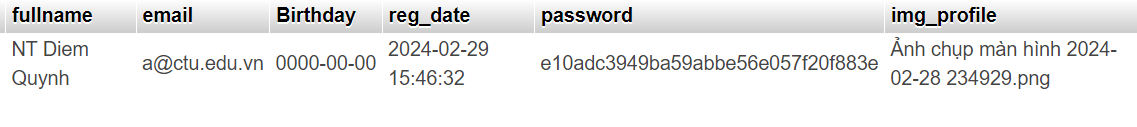
Thành công:



Mã băm trước khi đổi mật khẩu



Mã băm sau khi đổi mật khẩu



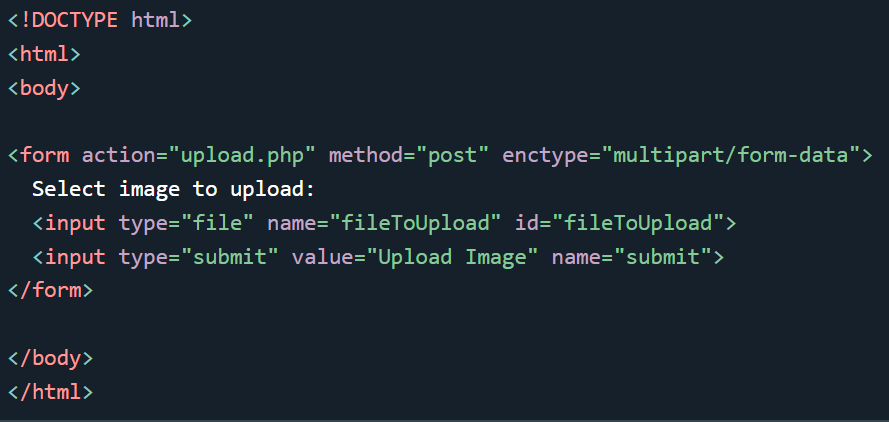
**8. Bạn đọc trong 4 để tìm hiểu và mô tả các cơ chế, các hàm/thủ tục để thực hiện việc upload.**

**Cấu hình tệp ‘php.ini’**

Trước tiên, hãy đảm bảo rằng PHP được cấu hình để cho phép tải tệp lên. Trong tệp "php.ini" của bạn, hãy tìm kiếm lệnh file\_uploads và đặt thành Bật:



**Tạo biểu mẫu HTML**

****

Một số quy tắc cần tuân theo đối với biểu mẫu HTML ở trên:

+Đảm bảo rằng biểu mẫu sử dụng phương thức = "post"

+Biểu mẫu cũng cần thuộc tính sau: enctype="multipart/form-data".Nó chỉ định loại nội dung nào sẽ sử dụng khi gửi biểu mẫu

Nếu không có các yêu cầu trên thì việc tải file lên sẽ không thành công.

Những điều khác cần chú ý:

Thuộc tính type="file" của thẻ <input> hiển thị trường đầu vào dưới dạng điều khiển chọn tệp, với nút "Duyệt" bên cạnh điều khiển đầu vào.

Biểu mẫu ở trên gửi dữ liệu đến một tệp có tên "upload.php", mà chúng ta sẽ tạo tiếp theo.

**Tạo file upload**

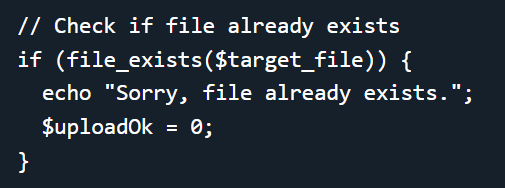
****

Tập lệnh PHP đã giải thích:

* $target\_dir = "uploads/" - chỉ định thư mục nơi tệp sẽ được đặt
* $target\_file chỉ định đường dẫn của tệp sẽ được tải lên
* $uploadOk=1 chưa được sử dụng (sẽ được sử dụng sau)
* $imageFileType chứa phần mở rộng tệp của tệp (viết thường)
* Tiếp theo kiểm tra file ảnh là ảnh thật hay ảnh giả

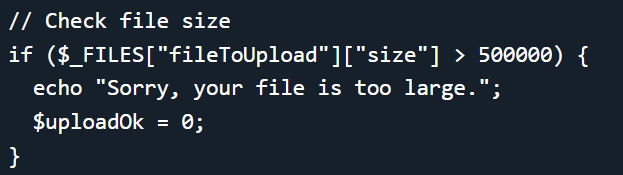
**Kiểm tra xem tệp đã tồn tại chưa**

Bây giờ chúng ta có thể thêm một số hạn chế. Đầu tiên, chúng tôi sẽ kiểm tra xem tệp đã tồn tại trong thư mục "tải lên" hay chưa. Nếu đúng như vậy, một thông báo lỗi sẽ hiển thị và $uploadOk được đặt thành 0:



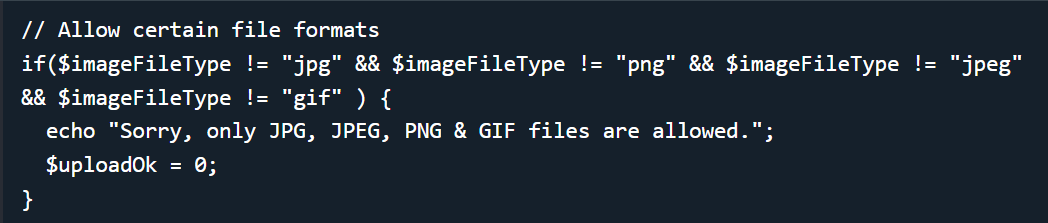
**Giới hạn kích thước tệp**

Trường nhập tệp trong biểu mẫu HTML của chúng tôi ở trên có tên là "fileToUpload". Bây giờ, chúng tôi muốn kiểm tra kích thước của tập tin. Nếu tệp lớn hơn 500KB, thông báo lỗi sẽ hiển thị và $uploadOk được đặt thành 0:



**Giới hạn loại tệp**

Mã bên dưới chỉ cho phép người dùng tải lên các tệp JPG, JPEG, PNG và GIF. Tất cả các loại tệp khác đều đưa ra thông báo lỗi trước khi đặt $uploadOk thành 0:

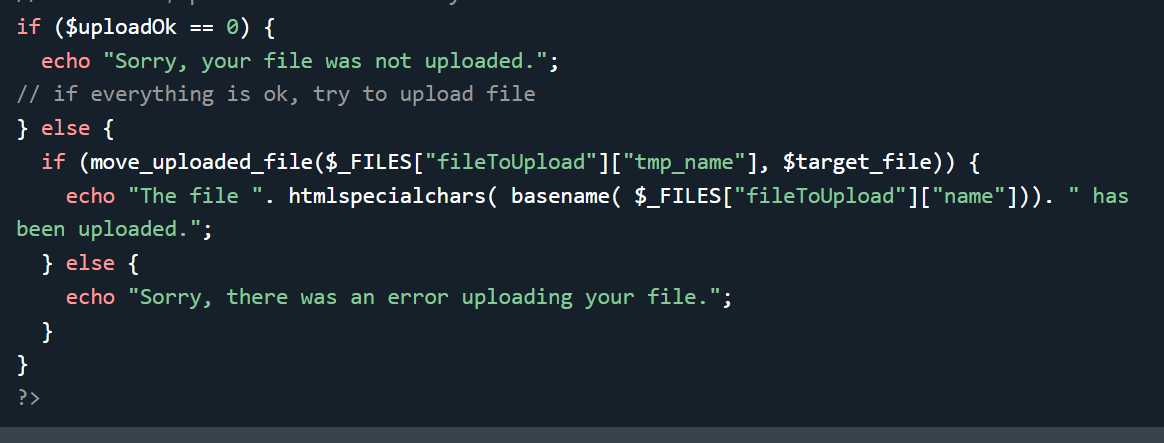


**Kiểm tra nếu $uploadOk =0**

Nếu $uploadOk bằng 0, điều này ngụ ý rằng có lỗi xảy ra trong quá trình xác thực tệp (chẳng hạn như loại tệp không được phép, kích thước tệp vượt quá giới hạn, v.v.). Trong trường hợp này, mã sẽ in ra "Sorry, your file was not uploaded." và không tiến hành bất kỳ thao tác tải lên nào.

Nếu $uploadOk không phải là 0, điều này ngụ ý rằng không có lỗi xảy ra và tệp có thể được tải lên. Mã tiếp tục vào một câu lệnh điều kiện khác để thực hiện thao tác tải lên.

Nó sử dụng hàm move\_uploaded\_file() để di chuyển tệp tạm thời từ vị trí tạm thời lưu trữ đến vị trí cụ thể mà bạn muốn tệp được lưu trữ (được chỉ định bởi ‘$target\_file’). Nếu thao tác di chuyển tệp thành công, mã sẽ in ra một thông báo xác nhận "The file [tên tệp] has been uploaded." với tên tệp đã được tải lên. Nếu thao tác di chuyển tệp không thành công, mã sẽ in ra "Sorry, there was an error uploading your file."



**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() đọc một tập tin vào một mảng. Mỗi phần tử mảng chứa một dòng từ tệp, với ký tự dòng mới vẫn được đính kèm.

**file(*filename*, *flag*, *context*)**

filename: Bắt buộc. Chỉ định đường dẫn tới file cần đọc

flag: Tùy chọn. Có thể là một hoặc nhiều hằng số sau:

* FILE\_USE\_INCLUDE\_PATH - Tìm kiếm tệp trong include\_path (trong php.ini)
* FILE\_IGNORE\_NEW\_LINES - Bỏ qua dòng mới ở cuối mỗi phần tử mảng
* FILE\_SKIP\_EMPTY\_LINES - Bỏ qua các dòng trống trong tệp bối cảnh Tùy chọn. Chỉ định ngữ cảnh của việc xử lý tập tin.

context: Tùy chọn. Chỉ định ngữ cảnh của việc xử lý tập tin. Ngữ cảnh là một tập hợp các tùy chọn có thể sửa đổi hành vi của luồng. Có thể bỏ qua bằng cách sử dụng NULL

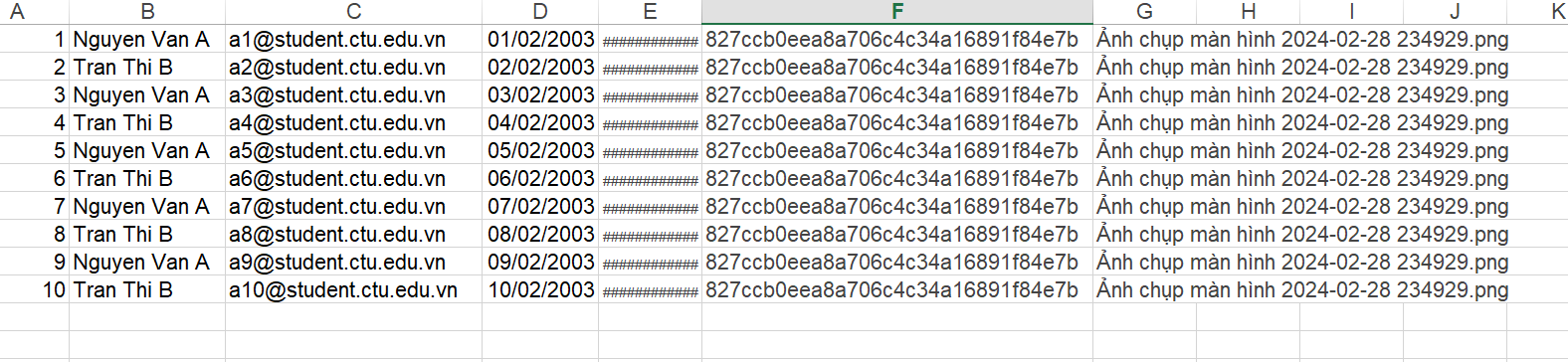
**10. Bạn hãy tạo 1 tập tin csv ít nhất 10 dòng dữ liệu với các cột dữ liệu như bảng customer trong csdl qlbanhang. Tạo tập tin upload-csv.php với giao diện cho phép upload các tập tin csv, và tập tin upload-csv-processing để xử lý nút xử lý sự kiện upload file csv và đưa dữ liệu vào bảng customers trong CSDL. Gợi ý:**

**○ Xem cấu trúc của bảng customer, mở excel và nhập liệu lưu lại với định dạng CSV.**

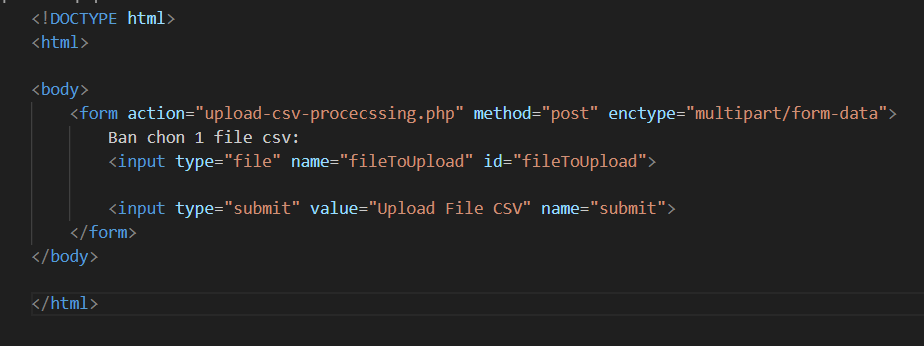
**○ Tham khảo upload-img.php để thiết kế giao diện upload file**

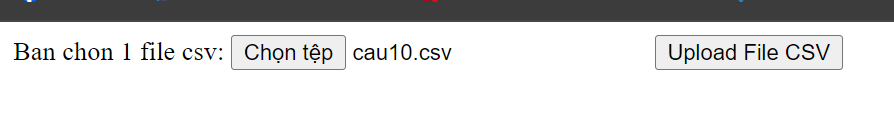
**○ Tham khảo upload-csdl.php để thiết kế action xử lý việc upload file, chú ý chỉnh sửa loại tập tin chấp nhận các file csv. Tham khảo: 6,7. Ở đoạn sau khi upload thành công,** bạn lấy tên file vừa upload đưa vào hàm đọc tập tin**. Bạn tham khảo read-csv.php chỉnh sửa đọc dữ liệu từ csv đưa vào mảng để lần lượt thực hiện insert từng dòng dữ liệu trong csv vào CSDL.**

cau10.csv



upload-csv.php





upload-csv-processing.php

