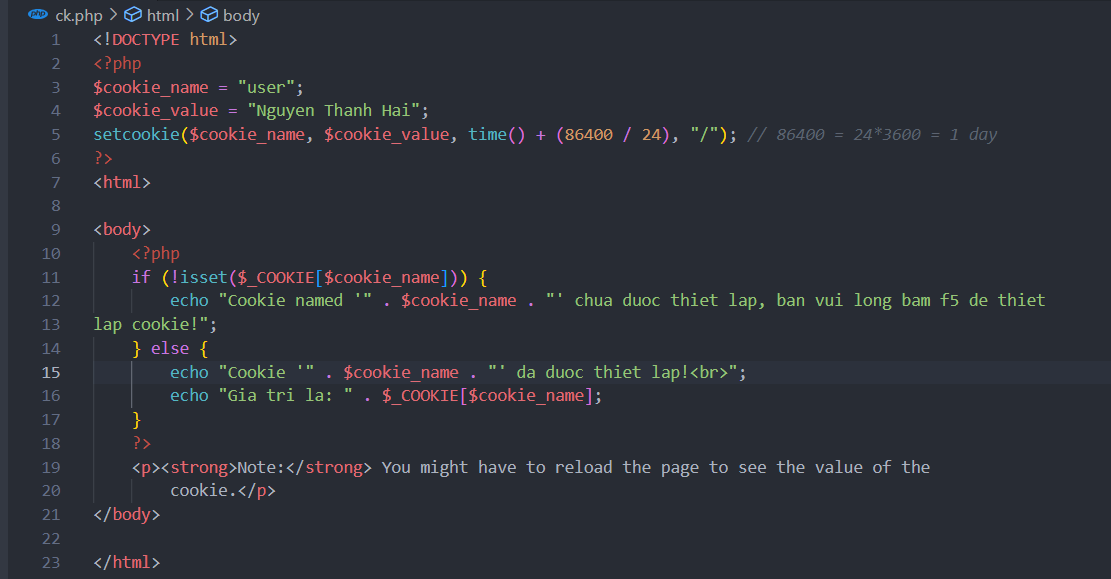
Họ tên: Nguyễn Hoàng Hồng Nhung

MSSV: B2205950

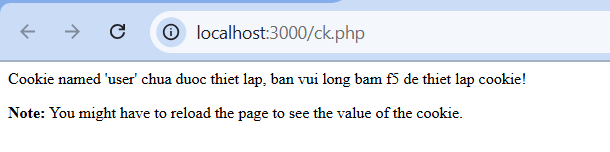
# Bạn hãy chạy tất cả các lệnh hướng dẫn ở trên và chụp lại màn hình kết quả.

* 1. Tạo cookies

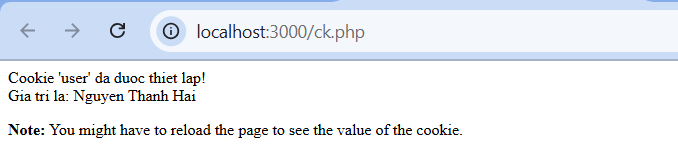
ck.php



Chạy lần đầu

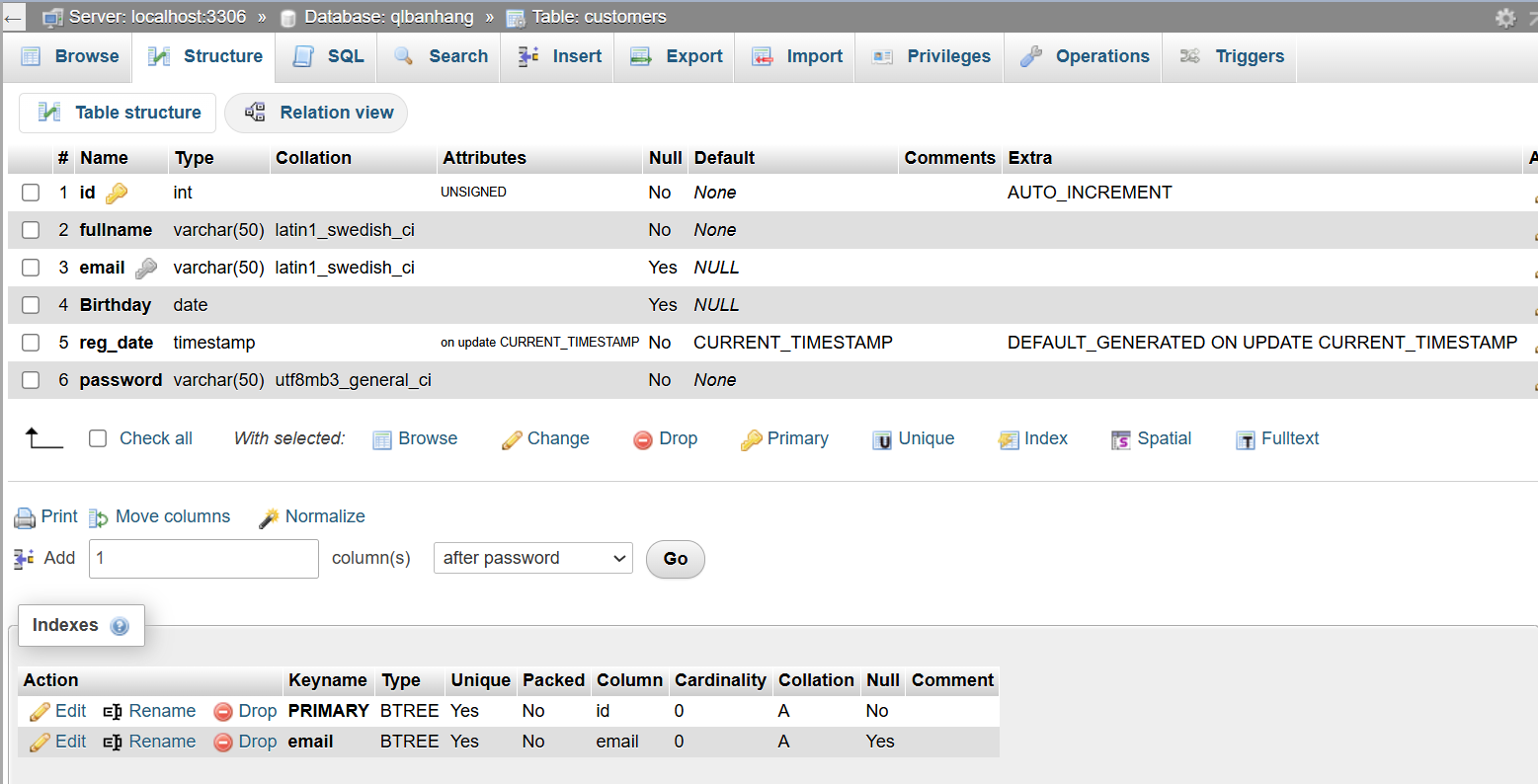


Sau khi reload

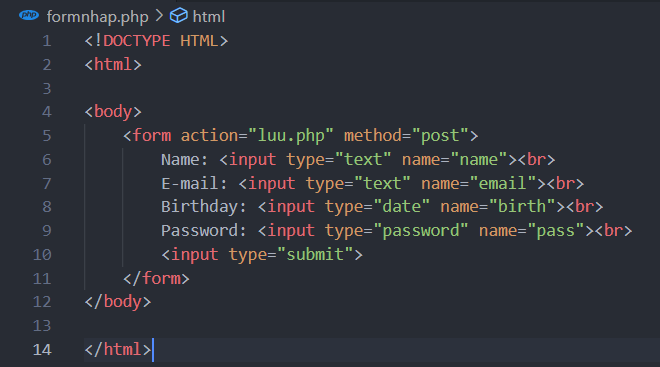


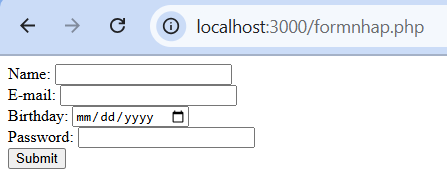
b. Tạo 1 trang đăng ký người dùng với mật khẩu được mã hóa:

* Cấu trúc bảng customers



* Formnhap.php





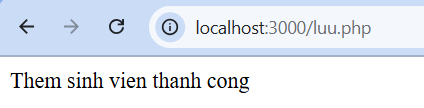
Form sau khi nhập



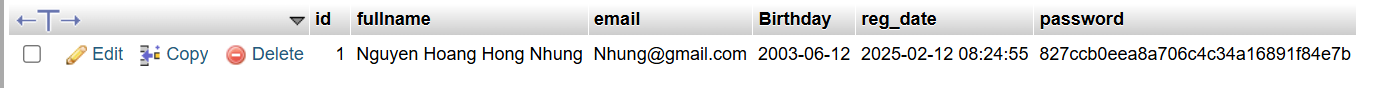
* luu.php



Sau khi chạy

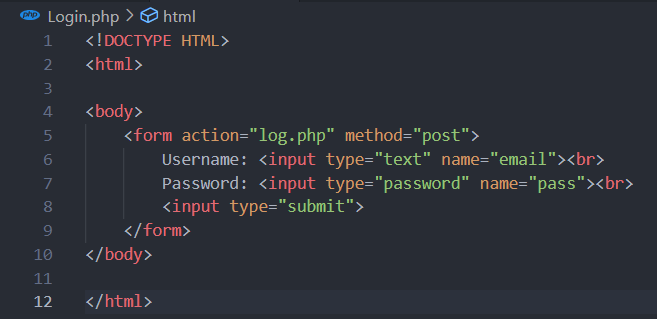


Kết quả trong csdl

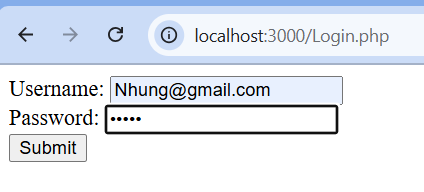


1. Tạo form đăng nhập

* Login.php



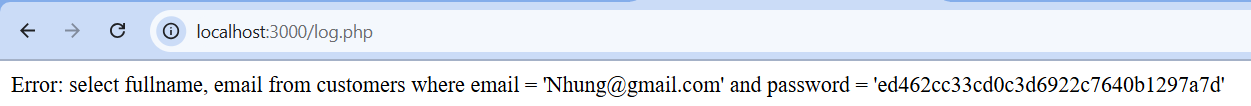
Nhập form đúng



Kết quả



Kết quả khi nhập form sai



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

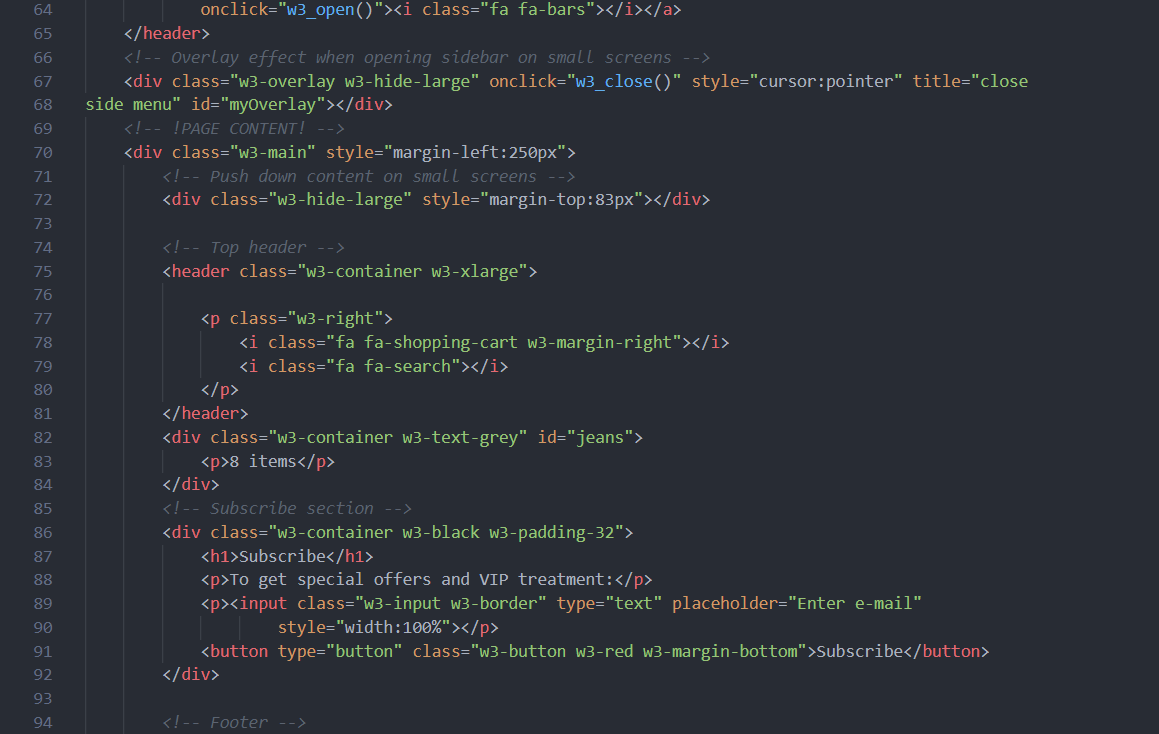
* Log.php được chỉnh sửa

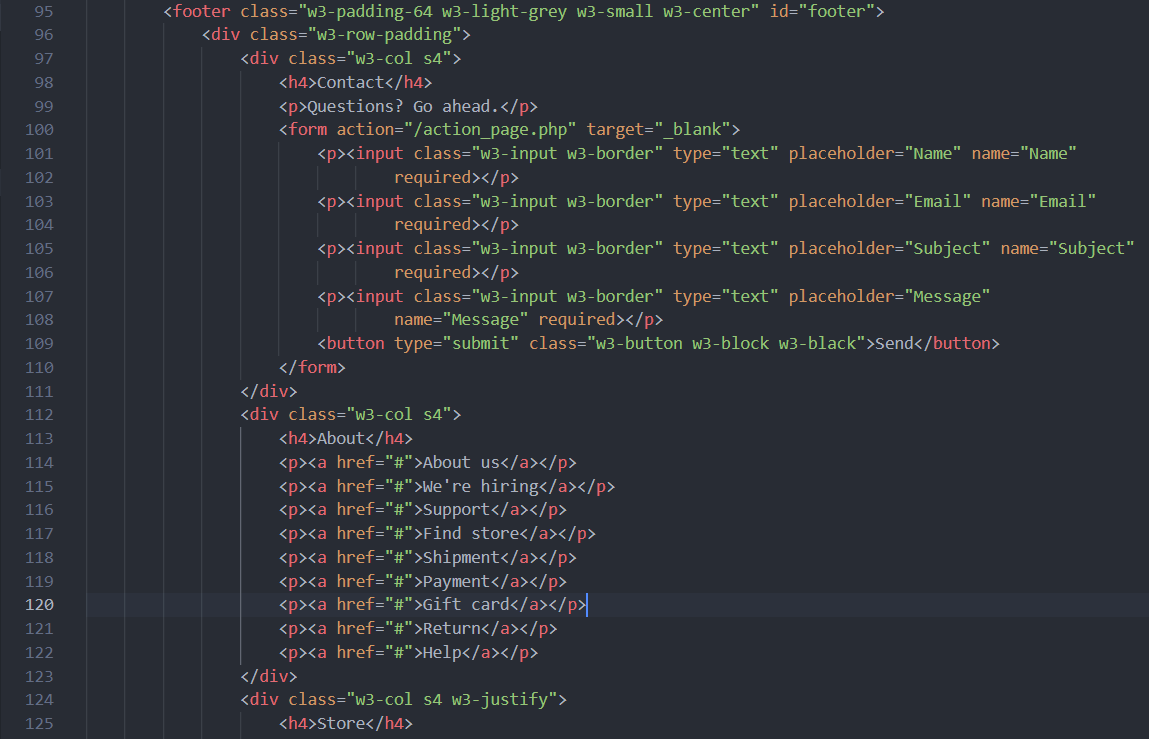


* Homepage.php

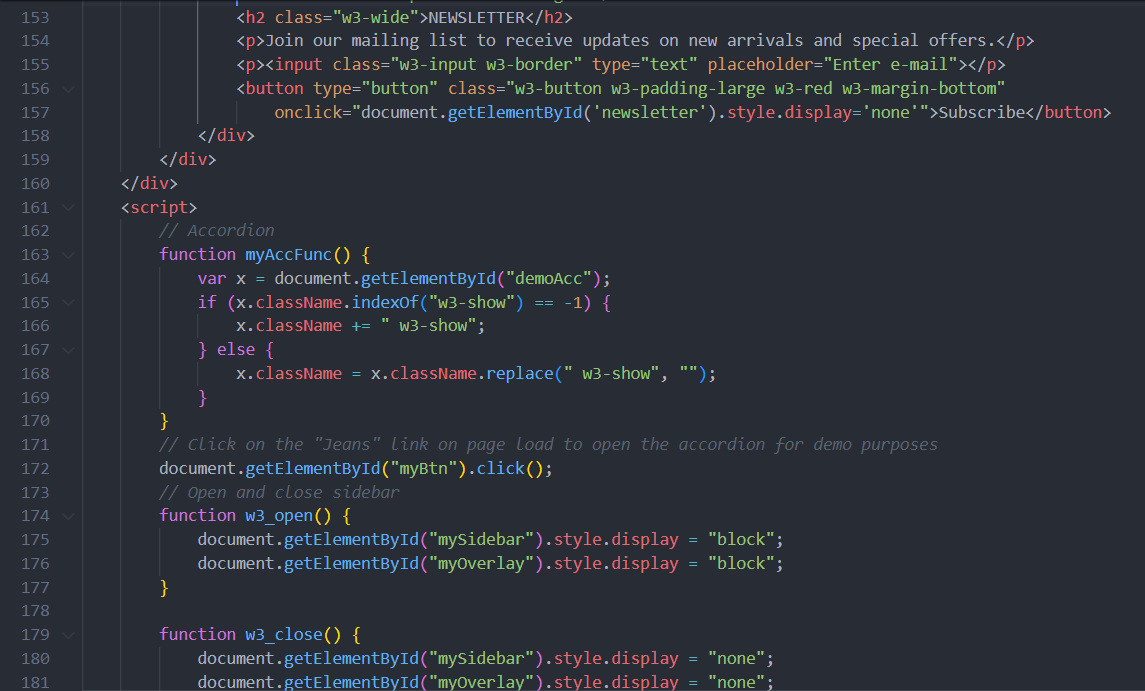






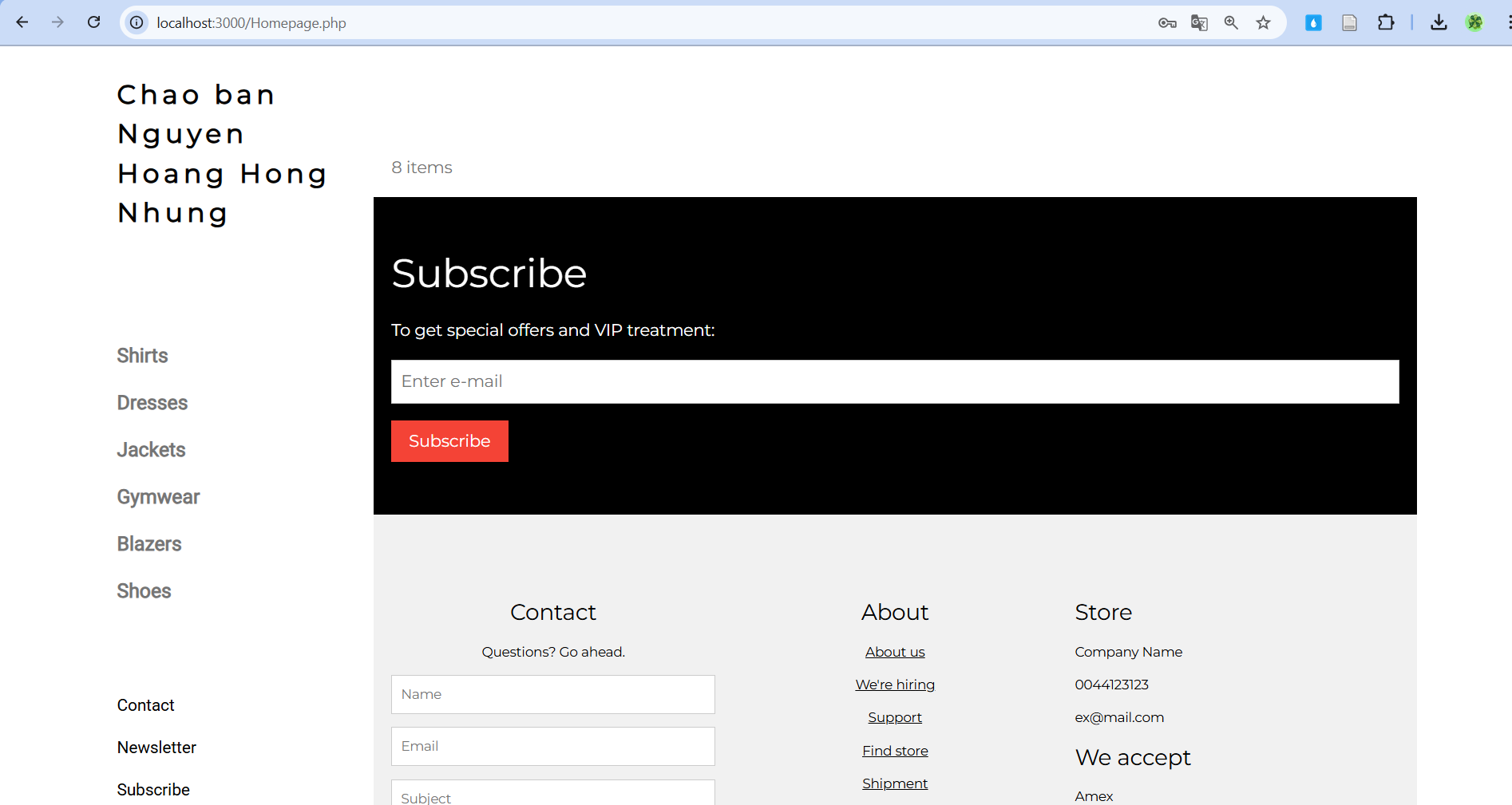






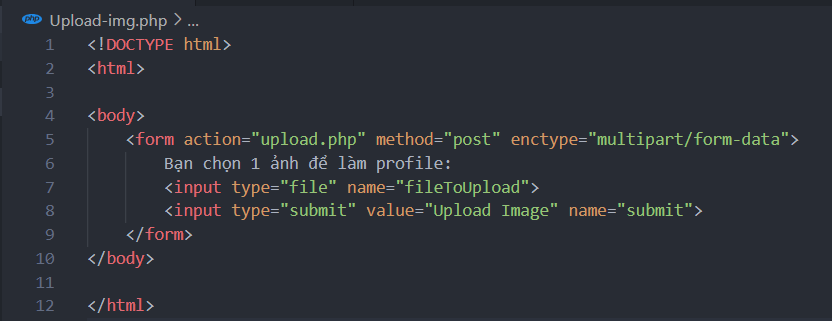


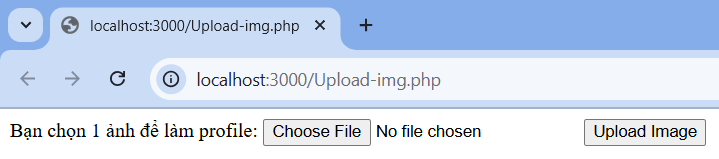
* Kết quả khi nhập đúng



1. Upload tập tin

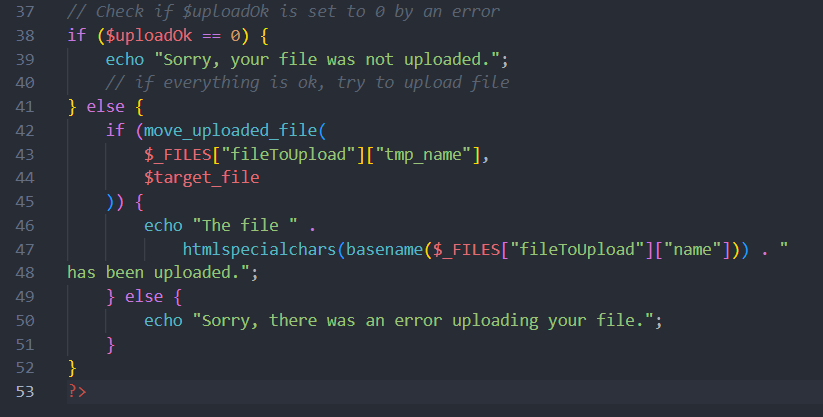
* Upload-img.php





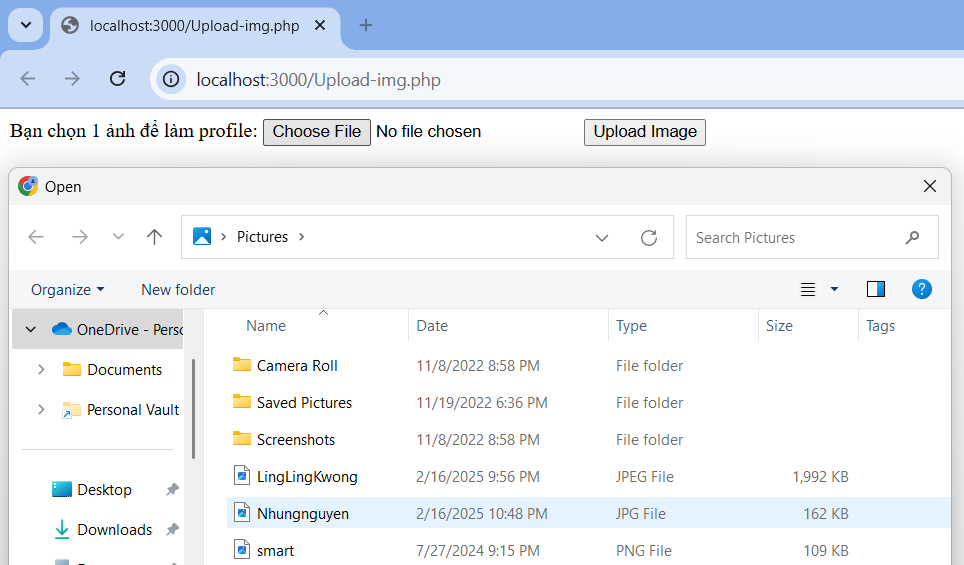
* upload.php

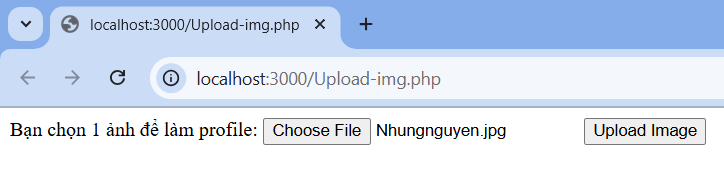


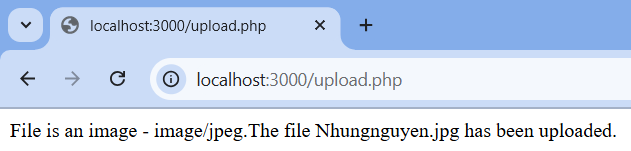


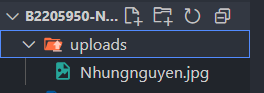
Kết quả test 1 (file đúng quy định):

Upload file Nhungnguyen.jpg



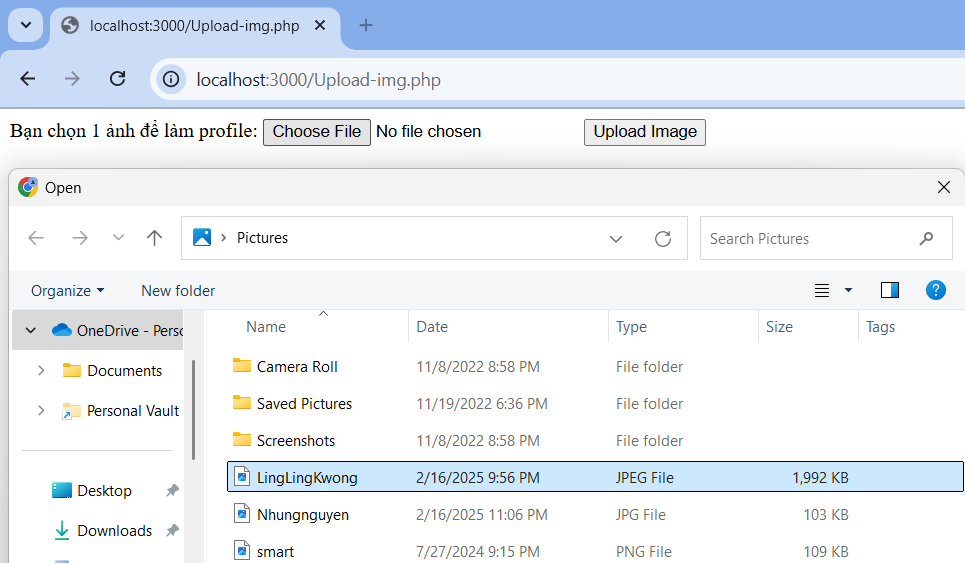


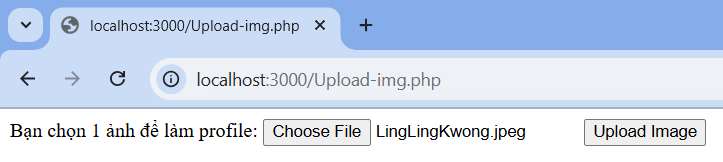


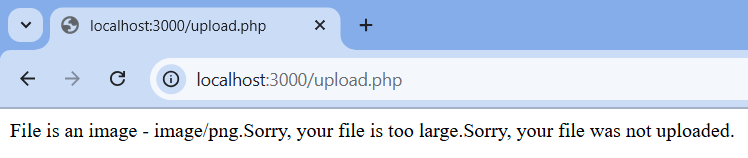


Kết quả test 2 (file lớn):

Upload file LingLingKwong.jpeg

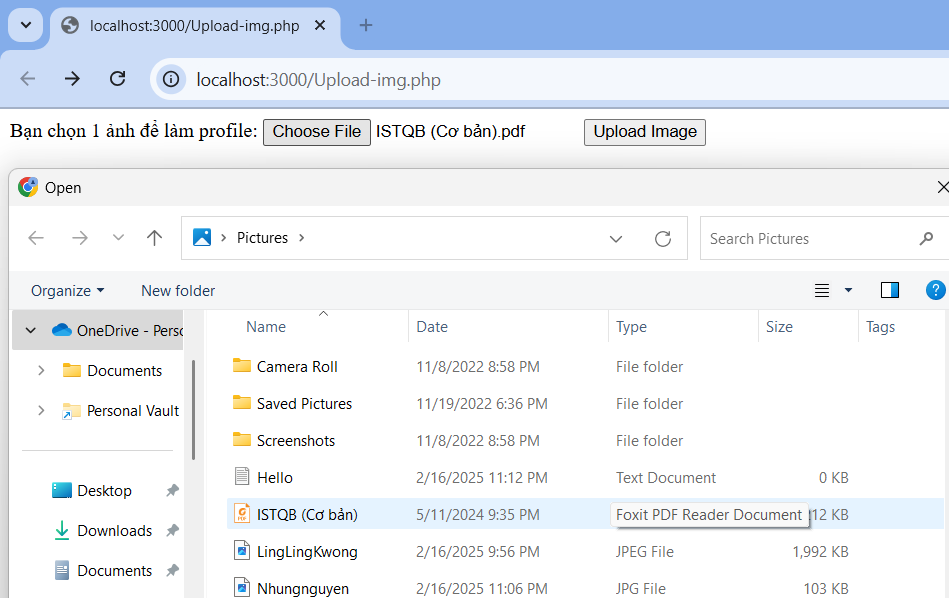


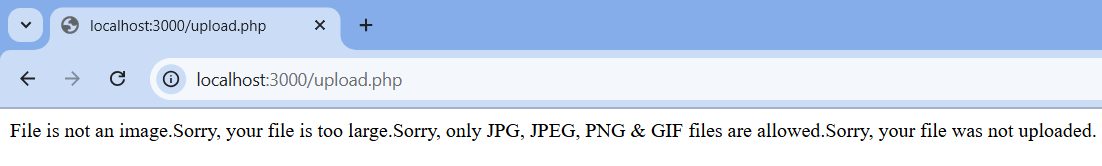




Kết quả test 3 (file khác định dạng cho phép):

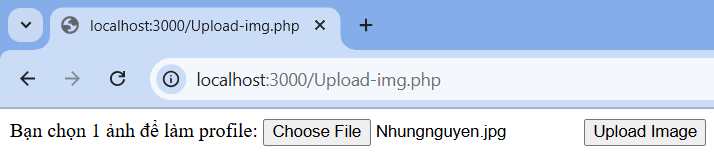
Upload file ISTQB (Cơ bản).pdf

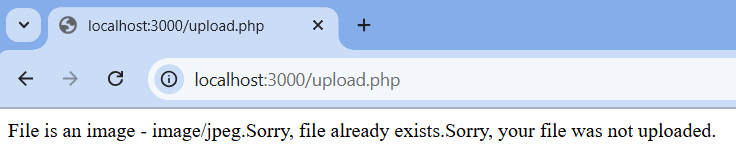




Kết quả test 4 (file đã tồn tại):

Upload file Nhungnguyen.jpg



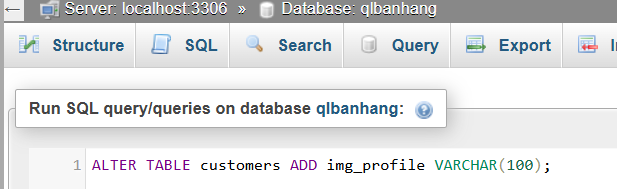


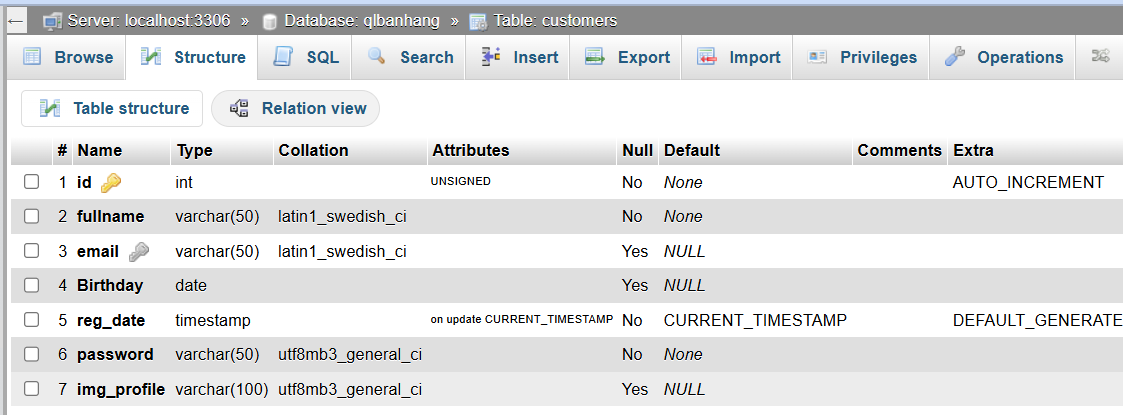
1. Upload ảnh và lưu dữ liệu về ảnh trong CSDL

* Upload-img.php (modified)

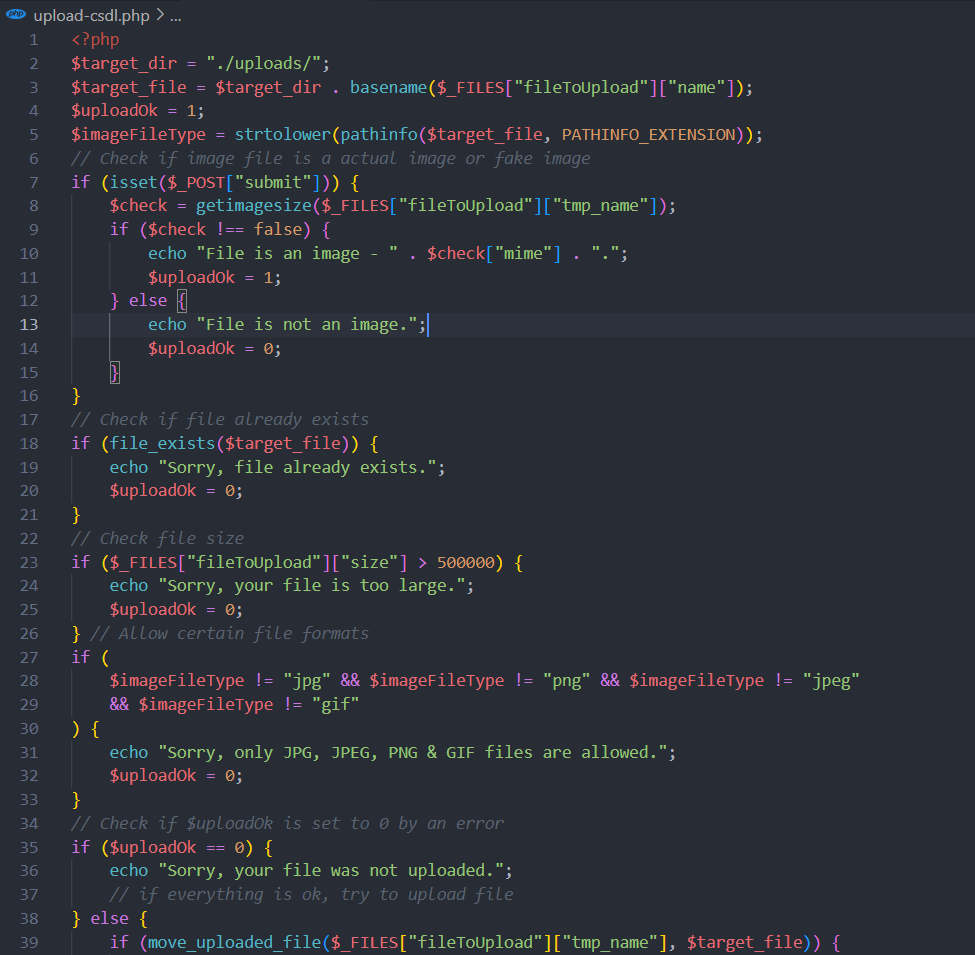
****

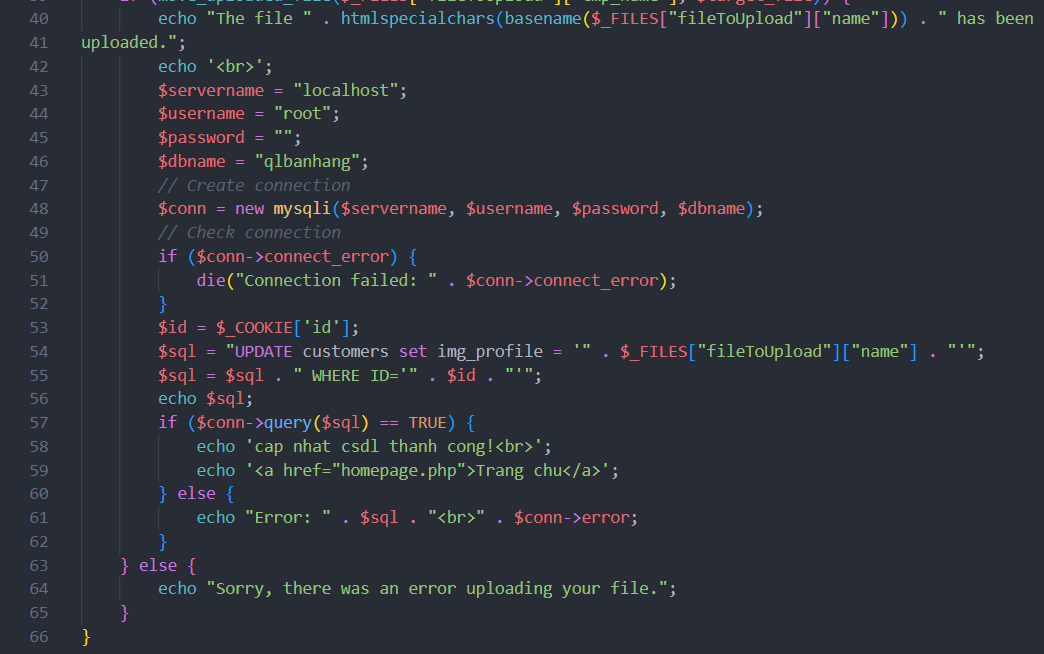
Tạo cột mới trong bảng customer



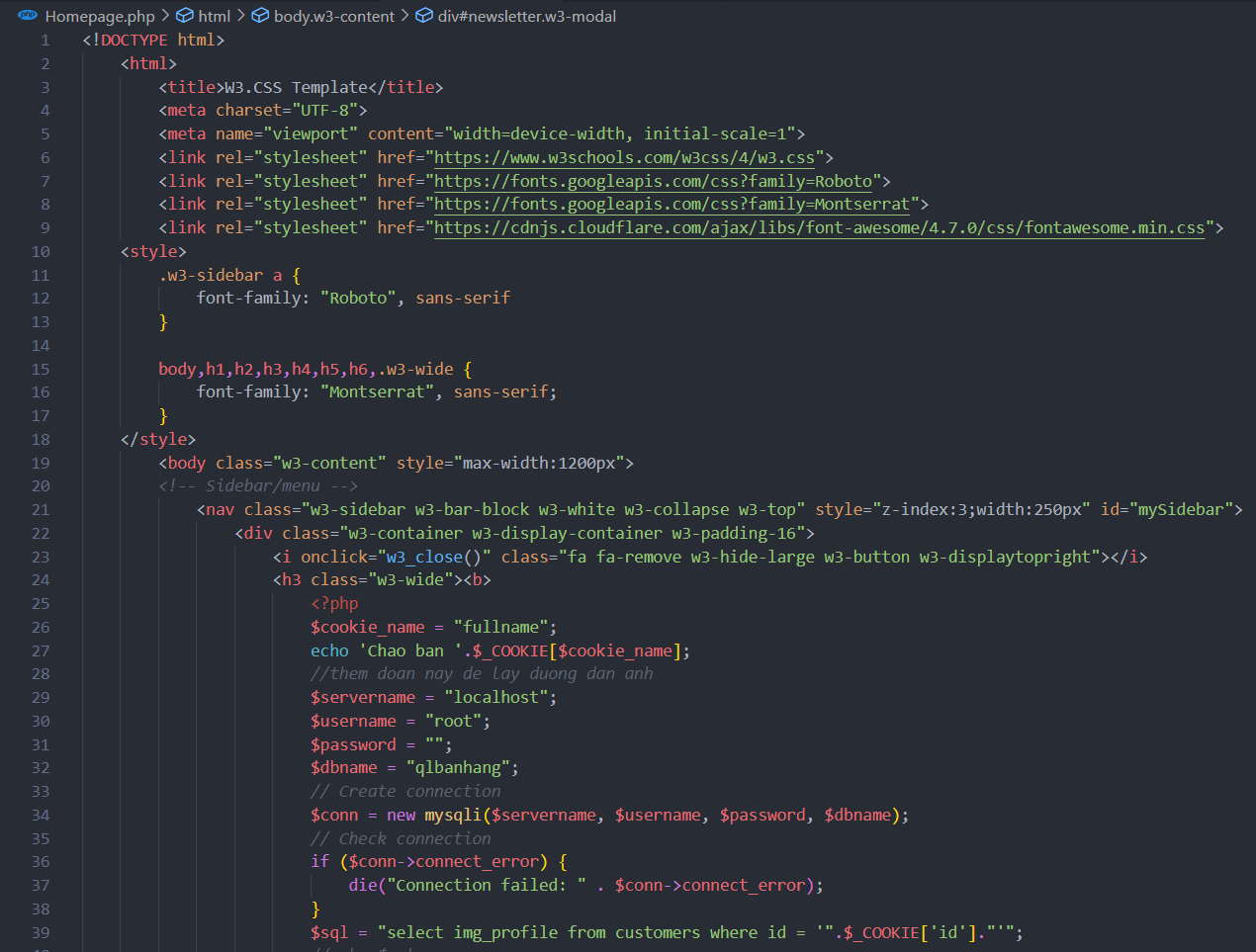


upload-csdl.php

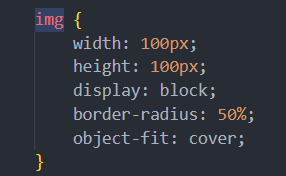




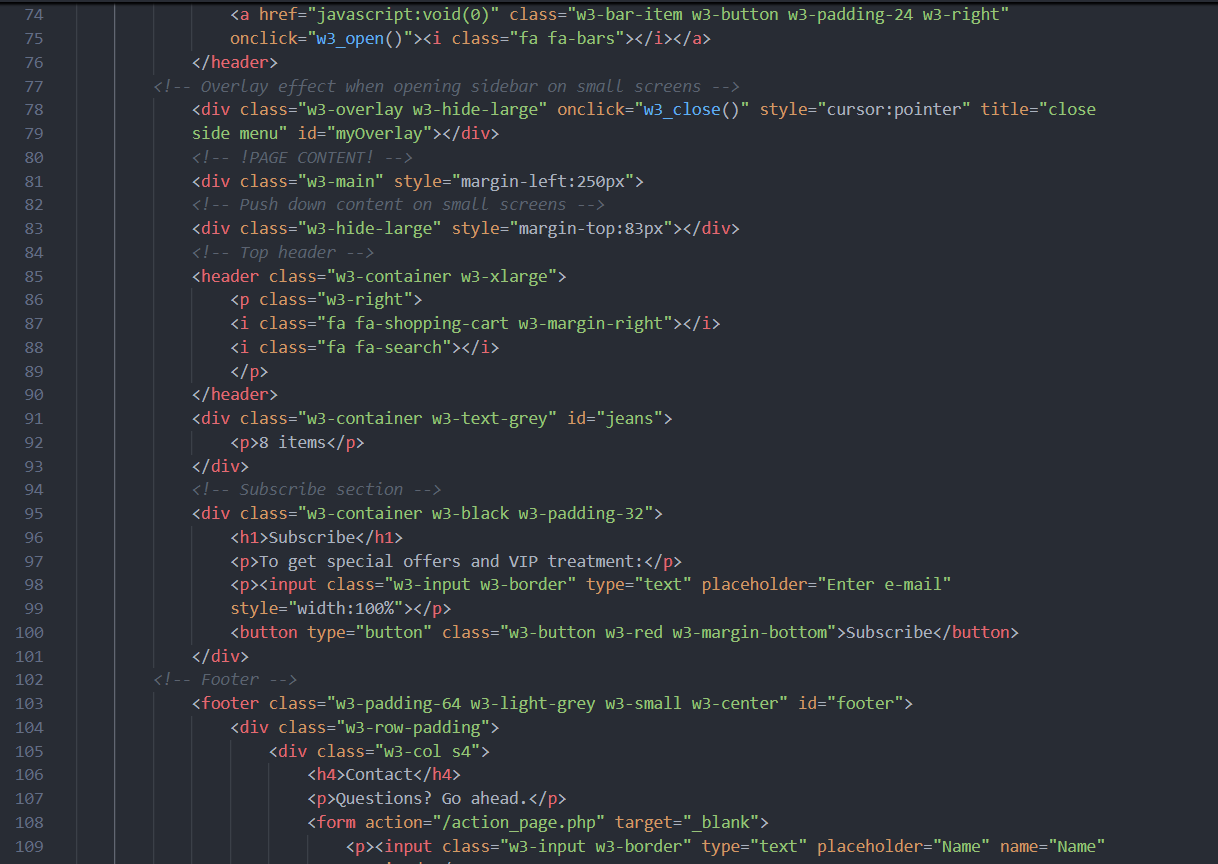
Homepage.php (modified với ảnh profile)

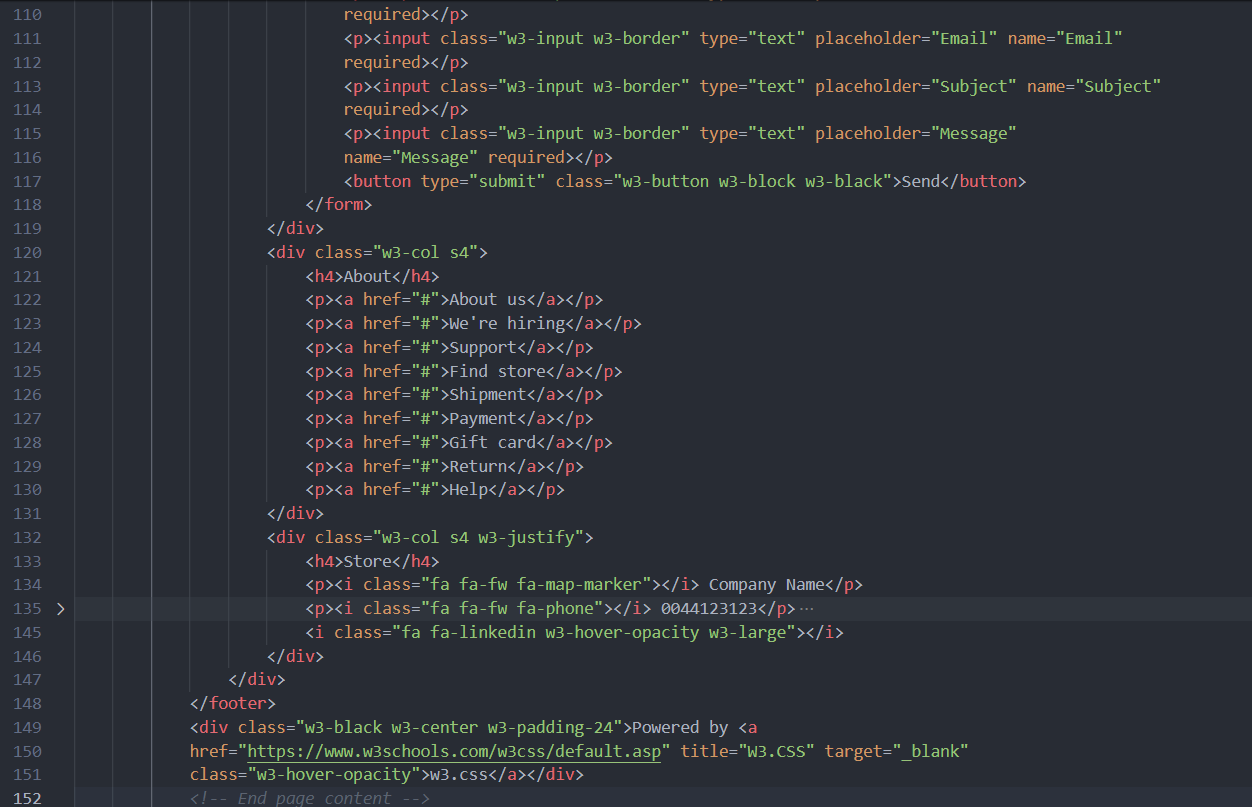


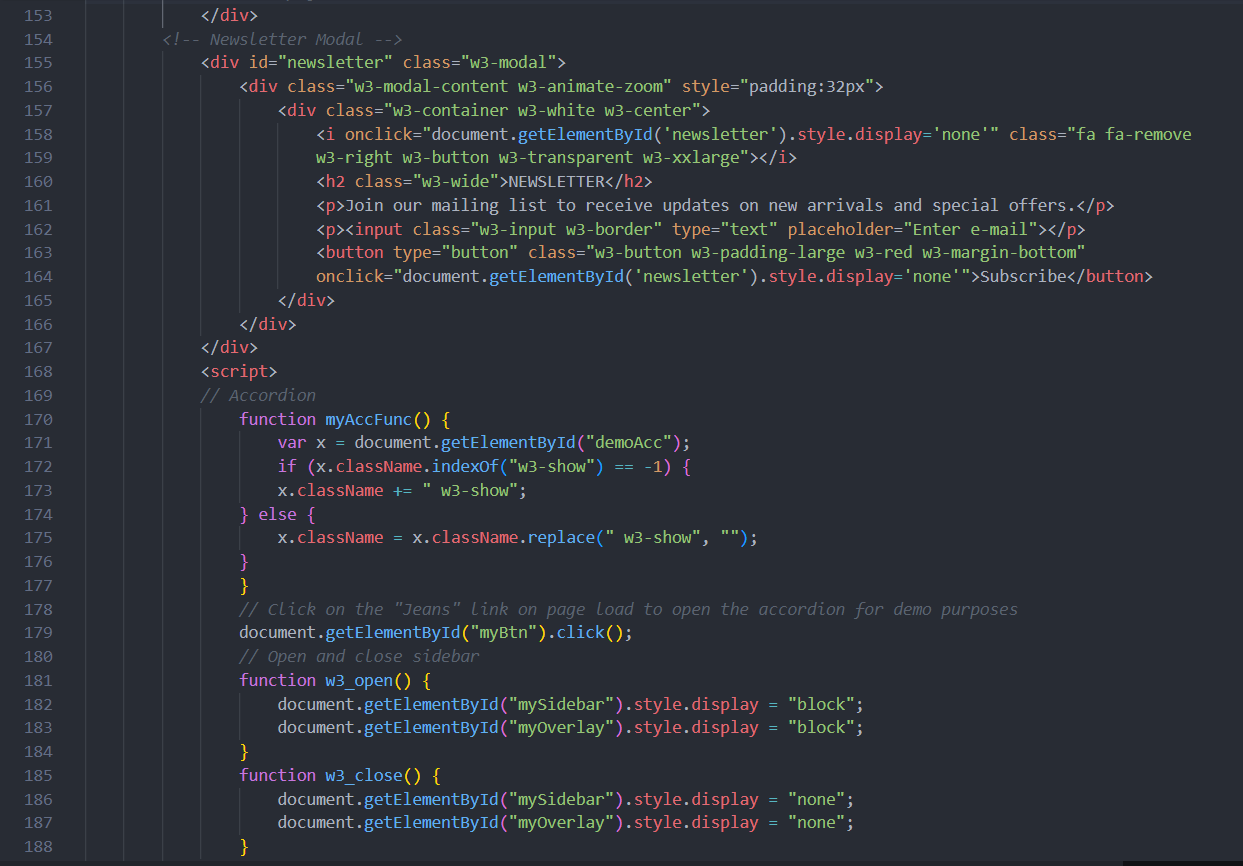
Thêm code chỉnh sửa ảnh avatar

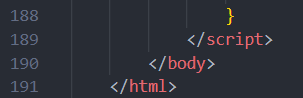




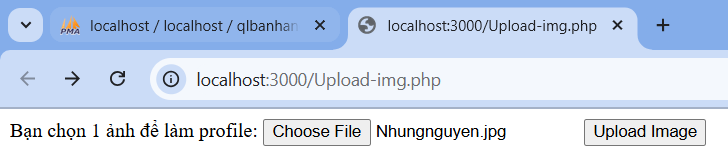


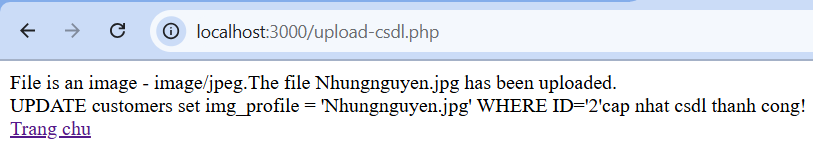


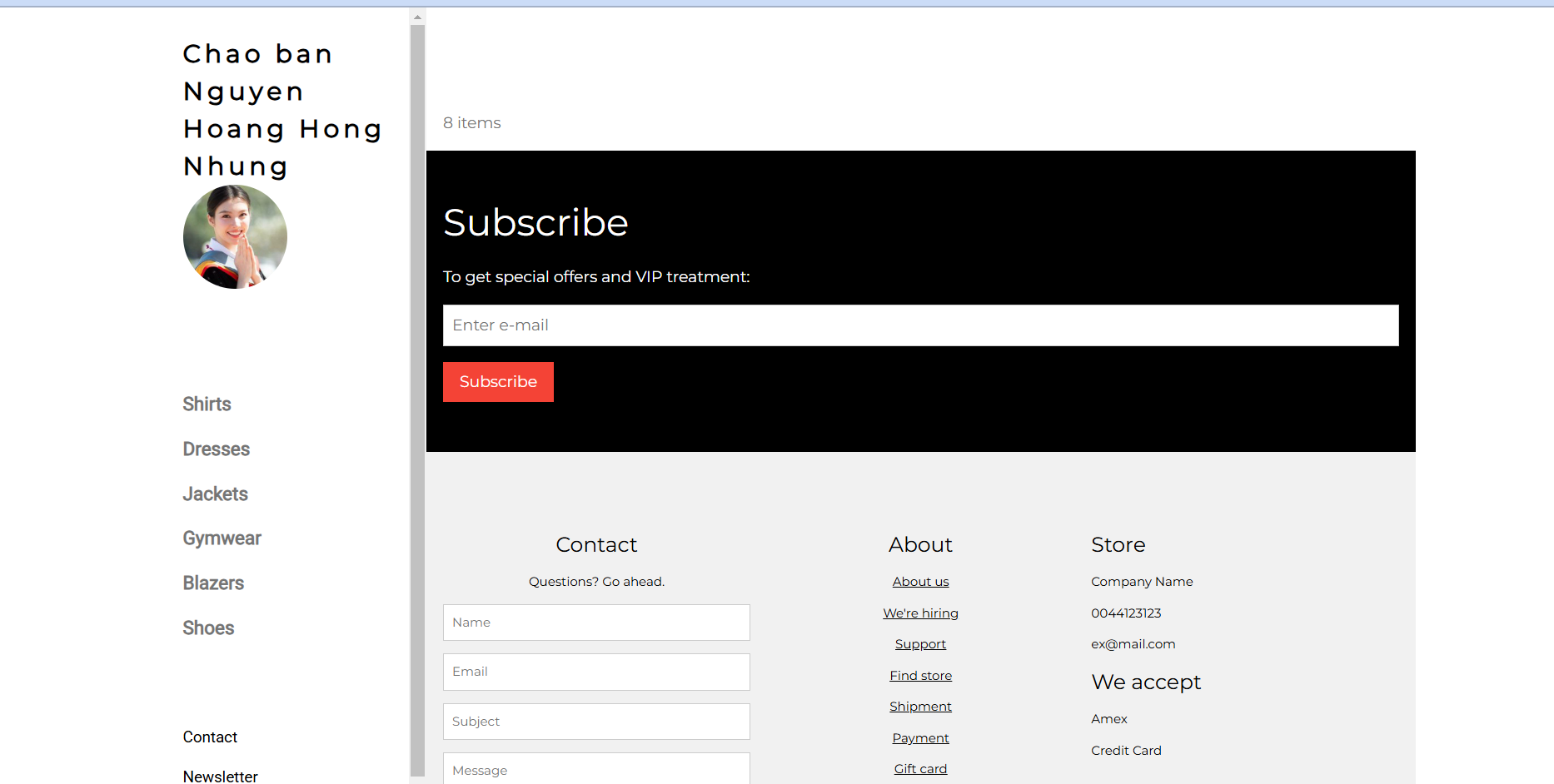




Kết quả khi upload file Nhungnguyen.jpg





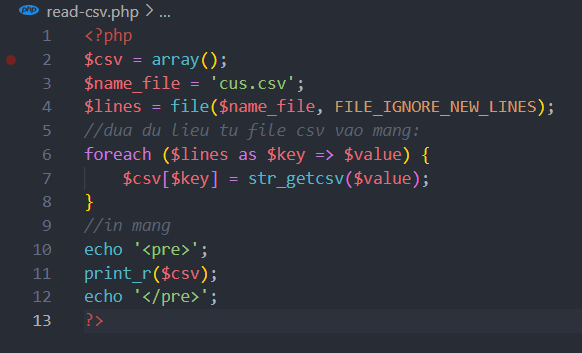


Thông tin trong csdl

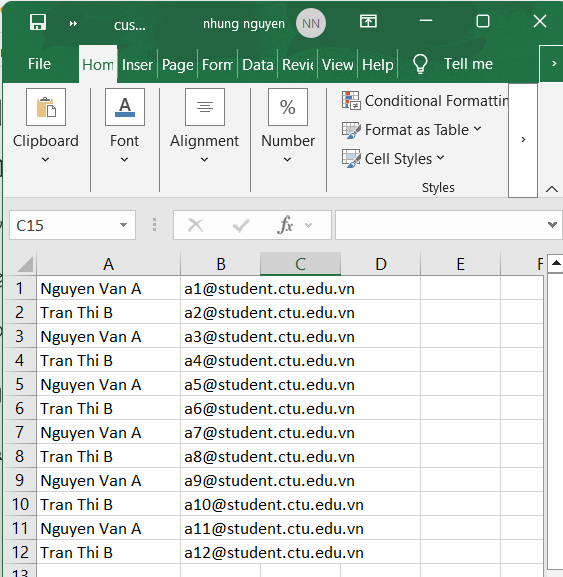


1. Upload file csv và đọc dữ liệu vào mảng

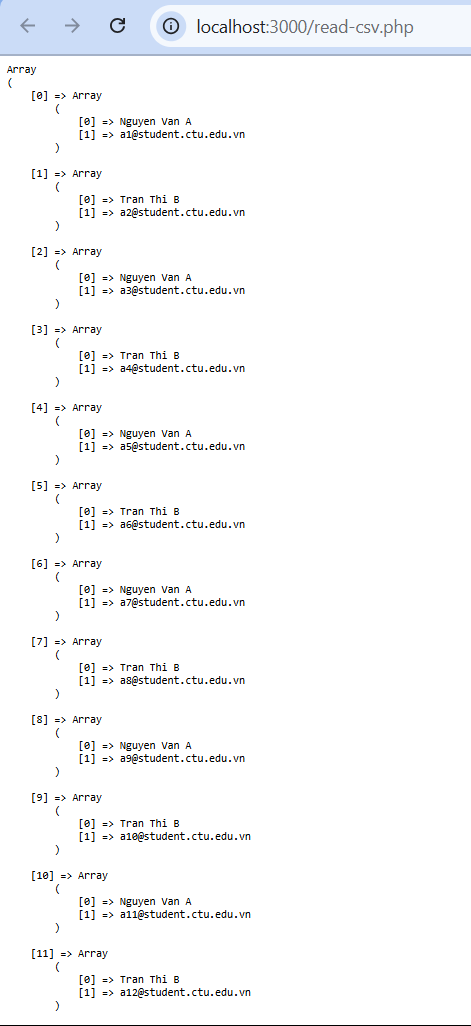
read-csv.php



Tạo file cus.csv



Kết quả



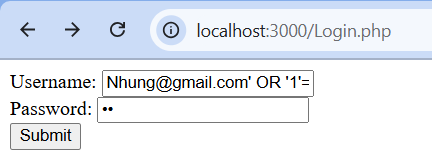
# 2. Trong vài trường hợp, hacker có thể sử dụng các kỹ thuật SQL Injection để hack hệ thống của bạn. Bạn hãy trình bày SQL Injection là gì và thử các ví dụ trình bày trong 1. Ứng dụng kỹ thuật đó vào trang đăng nhập mà bạn đã tạo, chụp lại các kết quả.

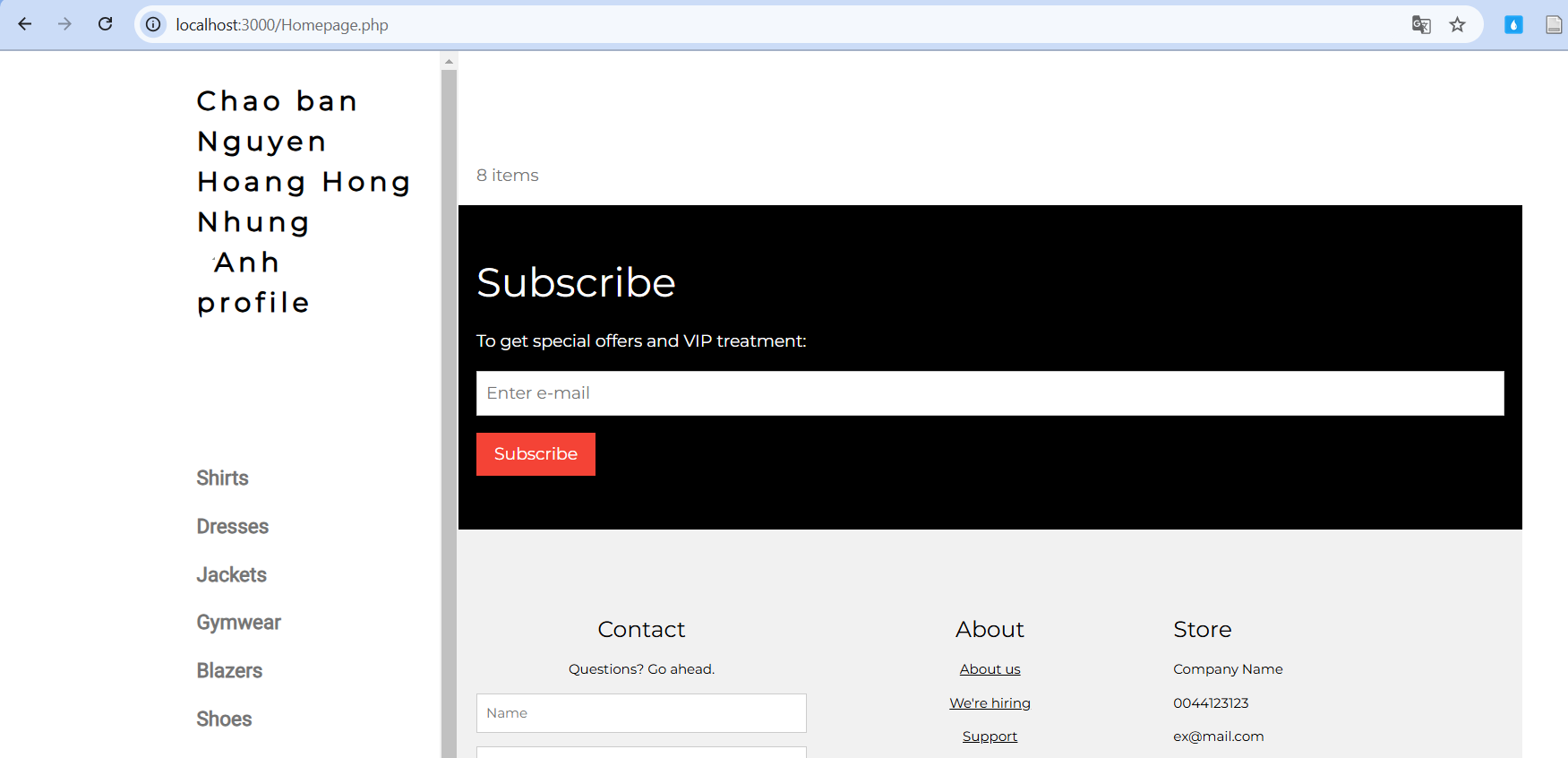
SQL injection là một kỹ thuật tiêm mã có thể phá hủy cơ sở dữ liệu của bạn, là một trong những kỹ thuật hack web phổ biến nhất. Là việc đặt mã độc hại vào các câu lệnh SQL, thông qua đầu vào trang web.[1]

Thử vào trang Login.php và Log.php

Nhập vào username: Nhung@gmail.com' OR '1'='1

Password: bỏ trống hoặc nhập bất kỳ



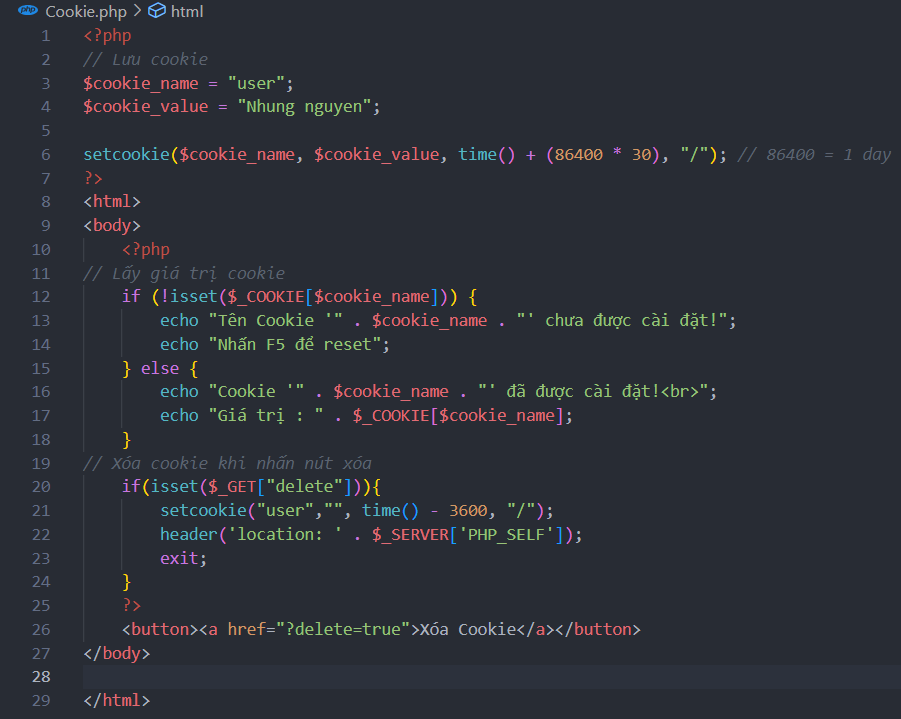


# 3. Dựa vào link2, bạn hãy cho biết Cookie là gì, diễn giải ý nghĩa các tham số trong setcookie(). Cách lưu, lấy, xóa giá trị trong cookie.

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 cùng một máy tính yêu cầu một trang bằng trình duyệt, nó cũng sẽ gửi cookie. Với PHP, bạn có thể tạo và truy xuất giá trị cookie.[2]

* Ý nghĩa các tham số trong setcookie(name, value, expire, path, domain, secure, httponly);
* Name: Tên của cookie bạn muốn tạo
* Value: Giá trị bạn muốn lưu trữ trong cookie
* Expire: Thời gian cookie sẽ tồn tại trên máy tính của người dùng
* Path: Đường dẫn mà cookie sẽ được sử dụng
* Domain: Tên miền mà cookie sẽ được sử dụng
* Secure: Nếu true, cookie chỉ được gửi qua HTTPS
* Httponly: Nếu true, cookie chỉ có thể truy cập bằng HTTP (không thể truy cập qua JavaScript, giúp bảo mật hơn)
* Lưu giá trị, Lấy giá trị và xóa cookie trong setcookie():

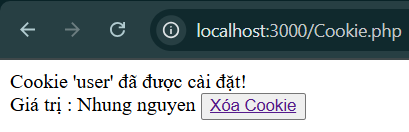
Cookie.php



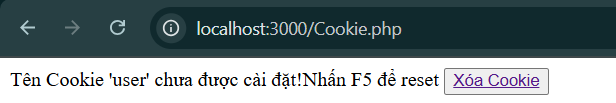
Lúc đầu



Sau khi nhấp F5



Sau khi xóa



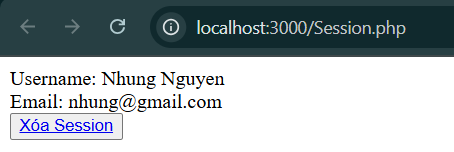
# 4. Dựa vào link3, bạn hãy cho biết Session dùng để làm gì. Cách lưu, lấy, xóa giá trị trong Session.

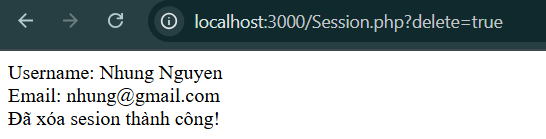
Session là một cách lưu trữ thông tin (trong các biến) để sử dụng trên nhiều trang. Không giống như cookie, thông tin không được lưu trữ trên máy tính của người dùng. Session được lưu trữ trên server [3]

* Cách lưu, lấy, xóa giá trị trong Session.

Session.php







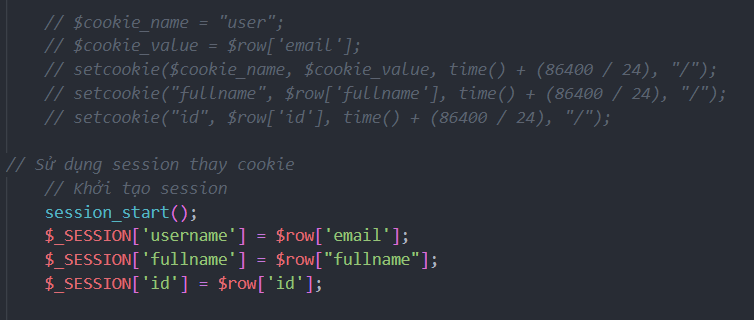
# 5. Bạn hãy so sánh Cookie và Session.

|  |  |  |
| --- | --- | --- |
| **Tiêu chí** | **Cookie** | **Session** |
| Lưu trữ | Lưu trữ trên trình duyệt (máy khách) | Lưu trữ trên máy chủ |
| Bảo mật | Được lưu trữ trên trình duyệt của người dùng, nên bảo mật kém hơn | Được lưu trữ trong máy chủ, nên bảo mật tốt hơn |
| Truy cập dữ liệu | Dữ liệu cookie dễ dàng sửa đổi khi chúng được lưu trữ ở phía khách hàng. | Dữ liệu session không dễ dàng sửa đổi vì chúng được lưu trữ ở phía máy chủ. |
| Thời gian | Dữ liệu cookie có sẵn trong trình duyệt của chúng ta đến khi hết hạn. | Dữ liệu session có sẵn cho trình duyệt chạy. Sau khi đóng trình duyệt sẽ mất thông tin session. |

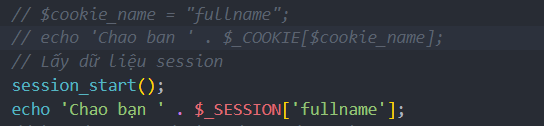
[4]

# 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.

log.php được sửa như sau

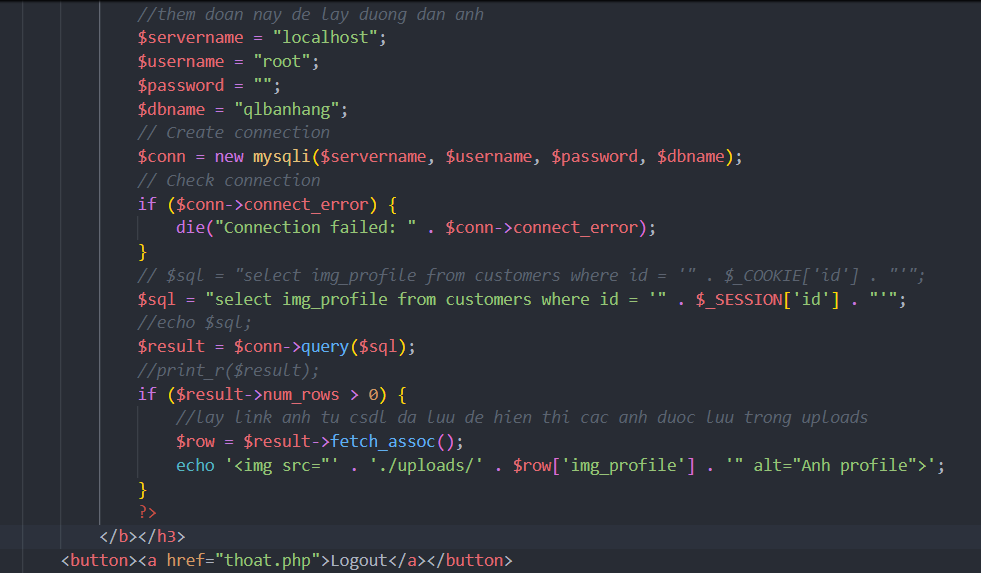


homepage.php được sửa như sau

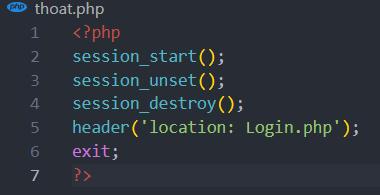


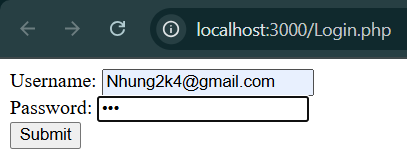


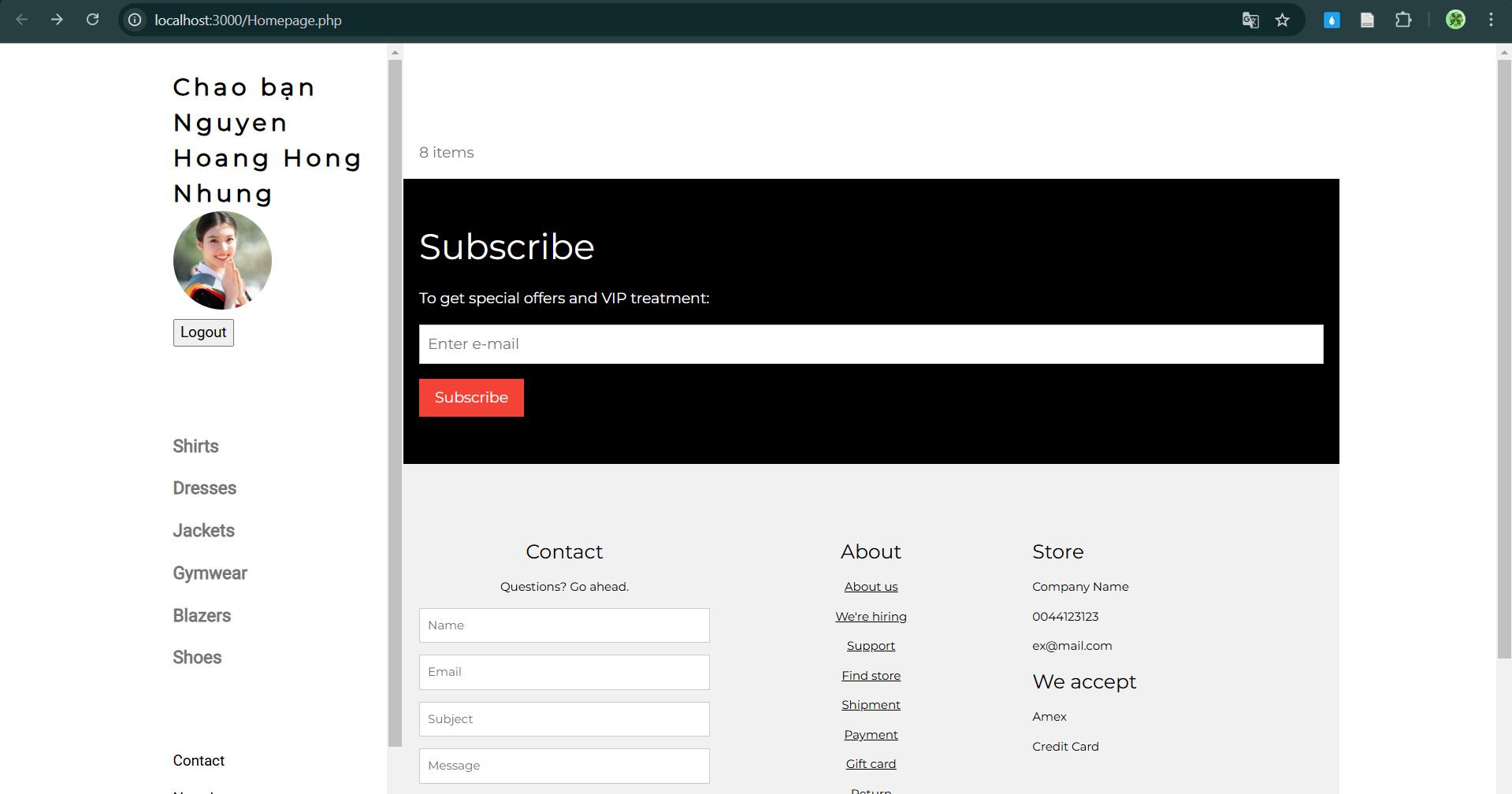
Thêm nút logout



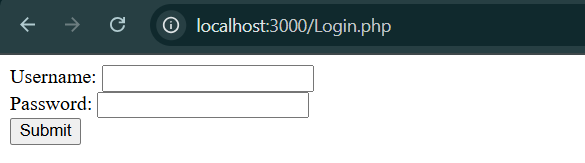
thoat.php



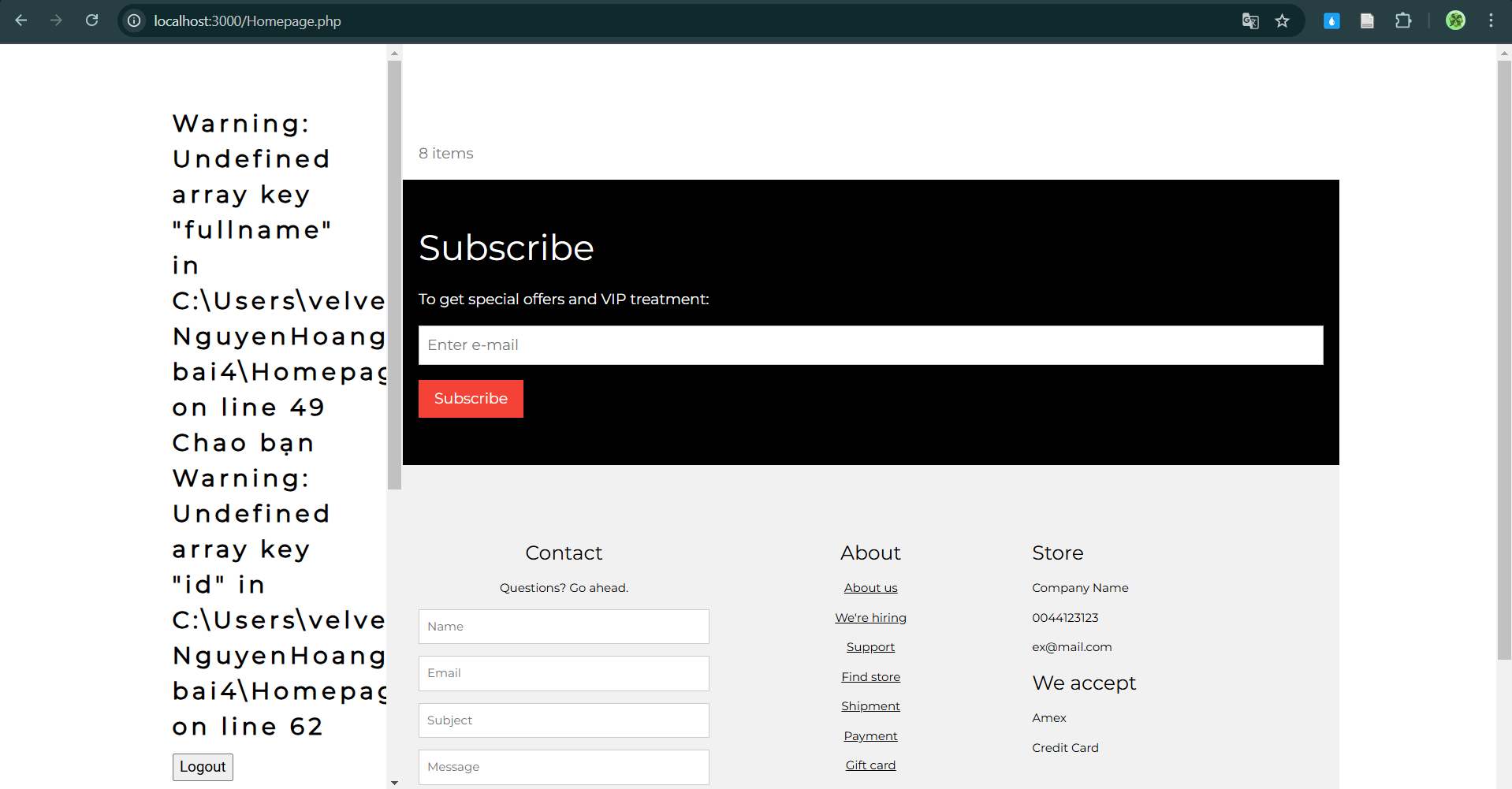




Sau khi nhấn logout



Thử vào bằng homepage.php

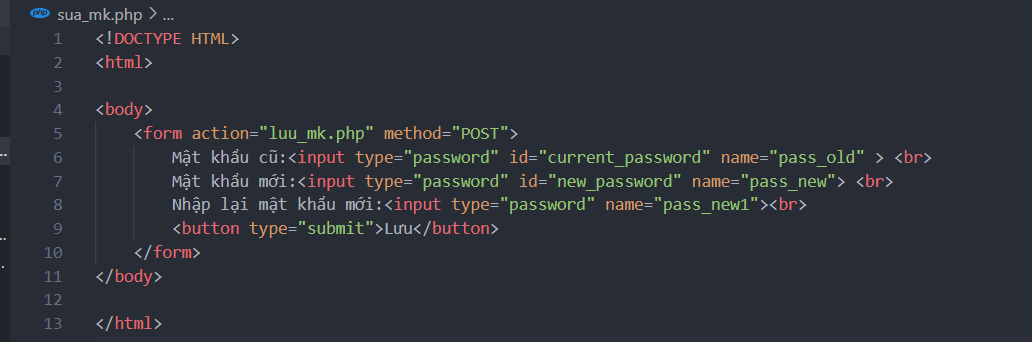


# 7. Bạn hãy tạo form sua\_mk.php cho phép người dùng chỉnh sửa mật khẩu sau khi đăng nhập. Yêu cầu gồm 3 input: ô để nhập mật khẩu cũ, 1 ô để nhập mật khẩu mới, 1 ô cho phép nhập mật lại mật khẩu mới. Khi nhập xong cần đảm bảo: mật khẩu cũ là khớp với CSDL đang lưu, 2 ô nhập mật khẩu mới phải khớp với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

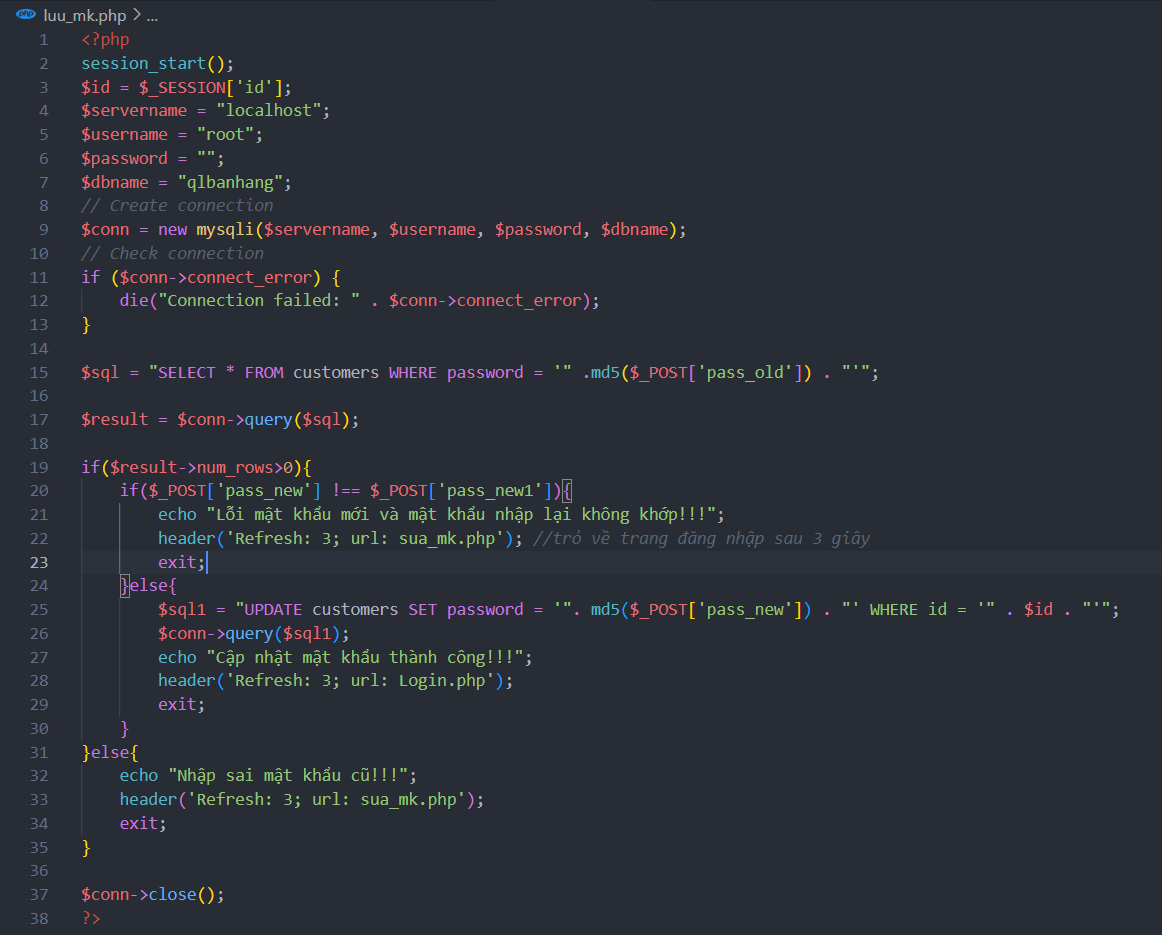
Tạo thêm nút change password trong trang homepage.php



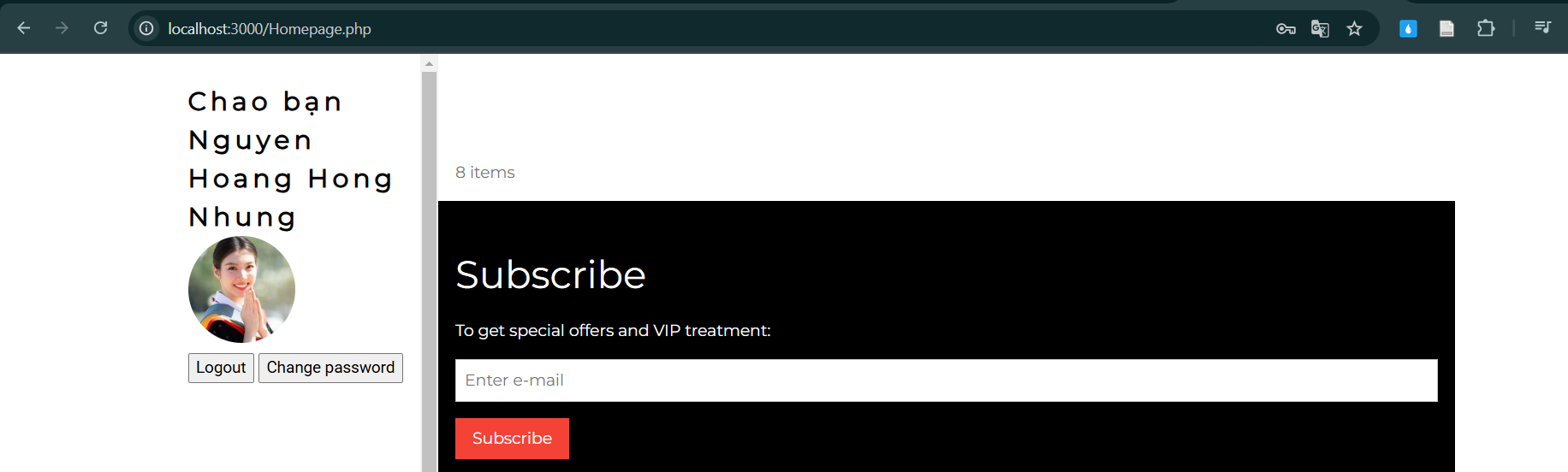
sua\_mk.php

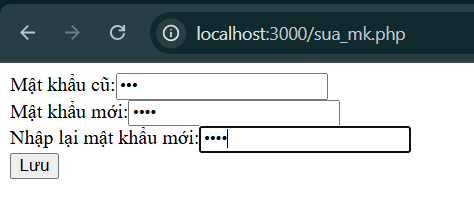


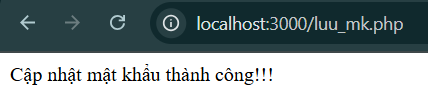
luu\_mk.php



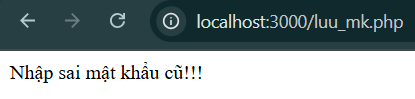
Kết quả:



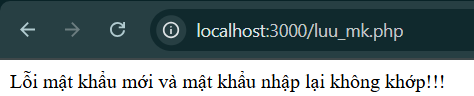




Nếu nhập mật khẩu của sai



Khi nhập mật khẩu mới và mật khẩu nhập lại không đúng



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

Mô tả các hàm/thủ tục để thực hiện việc upload



Đảm bảo form phải có  method="post" enctype="multipart/form-data" thì mới tải tệp lên được

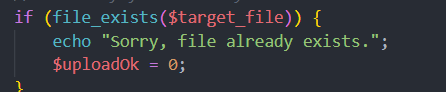


$target\_dir = "./uploads/" - chỉ định thư mục nơi tệp sẽ được đặt

$target\_file chỉ định đường dẫn của tệp sẽ được tải lên

$uploadOk=1 chưa được sử dụng (sẽ được sử dụng sau)

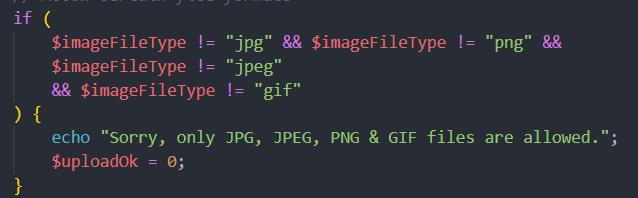
$imageFileType giữ phần mở rộng của tệp (ở dạng chữ thường)



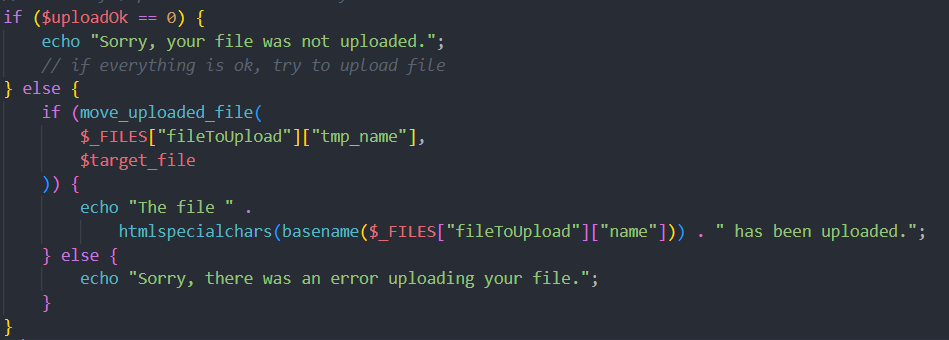
Kiểm tra xem tệp đã tồn tại trong thư mục "uploads" chưa. Nếu có, một thông báo lỗi sẽ được hiển thị và $uploadOk = 0



Kiểm tra kích thước tệp. Nếu tệp lớn hơn 500KB, thông báo lỗi sẽ hiển thị và $uploadOk = 0



Kiểm tra định dạng của tệp,  chỉ cho phép người dùng tải lên các tệp JPG, JPEG, PNG và GIF. Tất cả các loại tệp khác đều hiển thị thông báo lỗi trước khi đặt $uploadOk = 0



Kiểm tra biến $uploadOK có bằng 0 hay không, Nếu bằng 0 thì tệp không được upload. Nếu khác 0 thì kiểm tra tệp được lưu chưa. Nếu rồi được hiện thông báo ngược lại hiện thông báo lỗi.

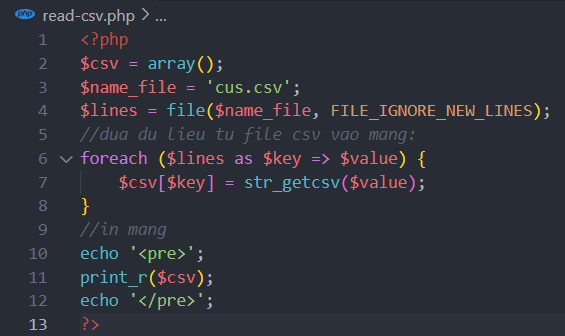
move\_uploaded\_file(): Di chuyển tệp tin từ vị trí tạm thời đến thư mục đích trên server.

$\_FILES["fileToUpload"]["tmp\_name"]: Lưu trữ đường dẫn tạm thời của tệp tin khi được tải lên.

$target\_file: đường dẫn đích nơi tệp tin sẽ được di chuyển đến

# 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).

Mô tả chức năng của hàm này và các tham số trong hàm: [5]



Hàm file() đọc một tệp vào một mảng. Cú pháp 

Filename: Đây là tên hoặc đường dẫn đến tệp mà bạn muốn đọc

Flag: Đây là một tham số tùy chọn xác định cách thức mở tệp.

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

Context: Đây là một tham số tùy chọn. Chỉ định ngữ cảnh của tệp xử lý. 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.

str\_getcsv($value) là một hàm trong PHP dùng để phân tách một chuỗi (dòng văn bản) thành một mảng con theo định dạng CSV (Comma-Separated Values).

print\_r($csv) sẽ in ra nội dung của mảng $csv. Sau khi xử lý xong, mảng này sẽ chứa các mảng con (mỗi mảng con đại diện cho một dòng trong tệp CSV).

# 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.**

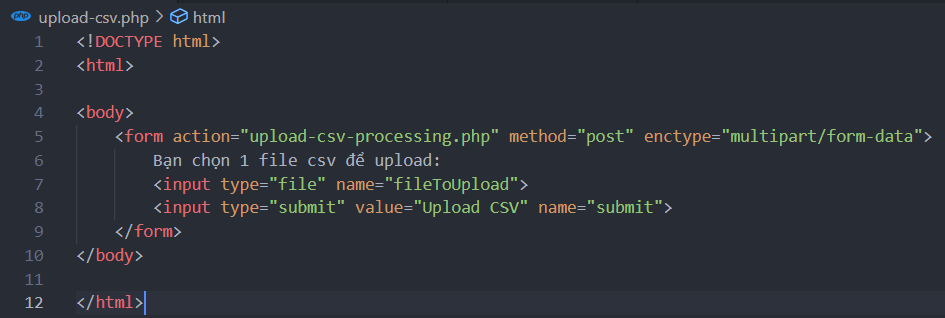
**○ Tham khảo upload-img.php để thiết kế giao diện upload file**

**○ 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.**

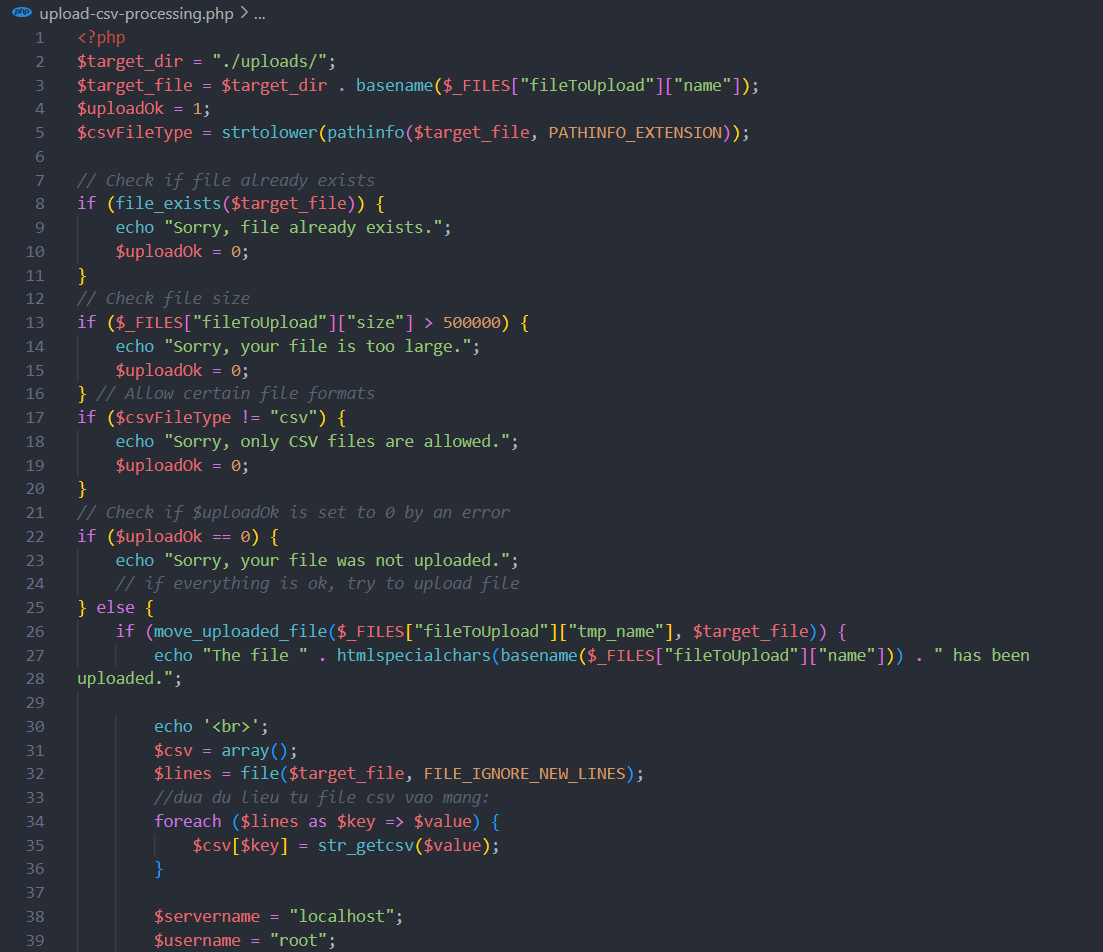
Customers.csv

****

upload-csv.php

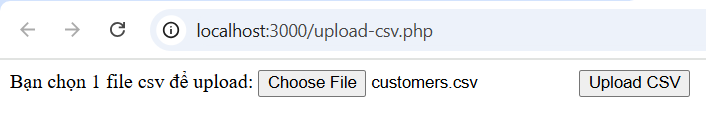
****

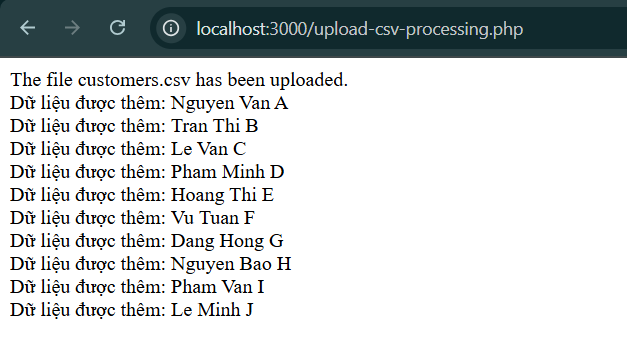
upload-csv-processing.php

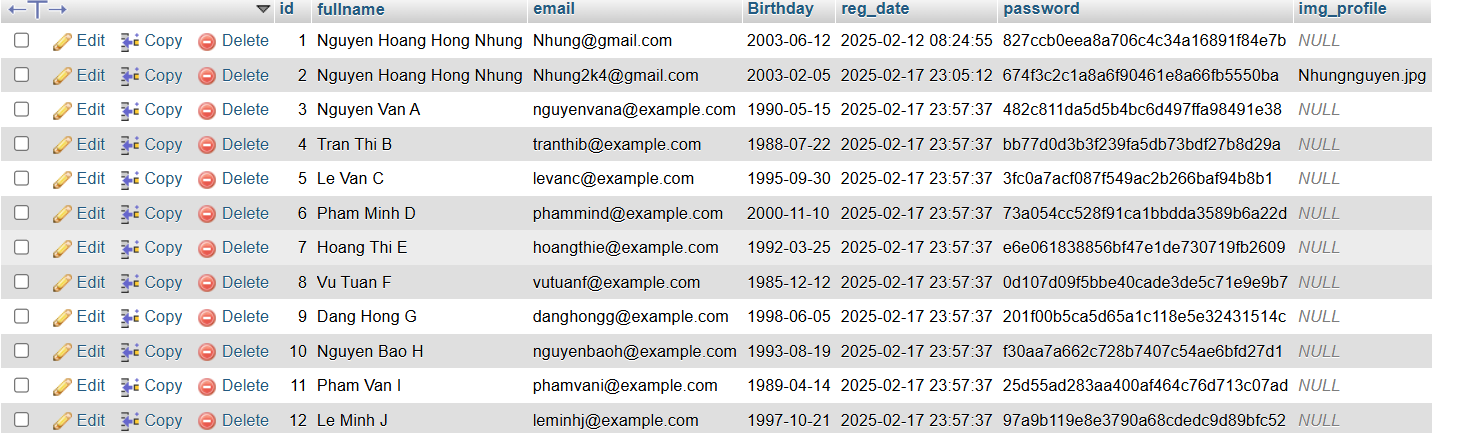
****

****

Kết quả:

****

****

****

**Tham Khảo**

1. SQL Injection, https://www.w3schools.com/sql/sql\_injection.asp

2. PHP Cookies, https://www.w3schools.com/php/php\_cookies.asp

3. PHP Sessions, https://www.w3schools.com/php/php\_sessions.asp

4. Cookie và Session, https://viblo.asia/p/cookie-va-session-07LKXEvEZV4

5. PHP file() Function, https://www.w3schools.com/php/func\_filesystem\_file.asp