Bài tập thực hành 04

**MSSV: B2110034**

**Họ và tên sinh viên: Võ Minh Trí**

Lập trình PHP nâng cao

**Mục tiêu cần đạt**:

Sau buổi các bạn cần nắm thao tác sử dụng PHP nâng cao

* Hiểu và biết cách dùng Cookies và Session
* Tạo form đăng nhập và dùng cookies, session để quản lý các đăng nhập, thực hiện chức năng log out (thoát) khỏi hệ thống
* Biết về SQL Injection.
* Upload file, lưu thông tin về tập tin trong CSDL
* Đọc, và xử lý nội dung trong tập tin

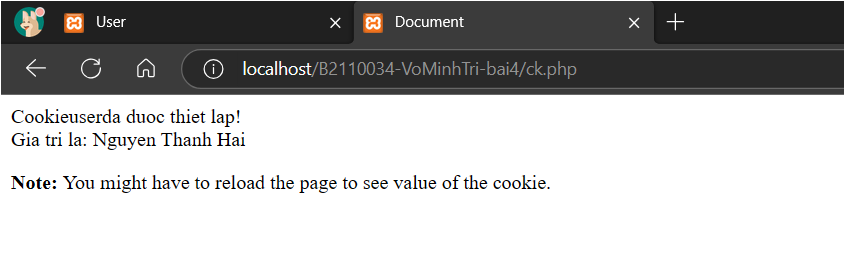
Các bạn đọc và thực hiện viết code như hướng dẫn để làm quen, sau đó đọc trả lời các **Yêu cầu** ở dưới bài hướng dẫn để thực hiện yêu cầu bài thực hành.

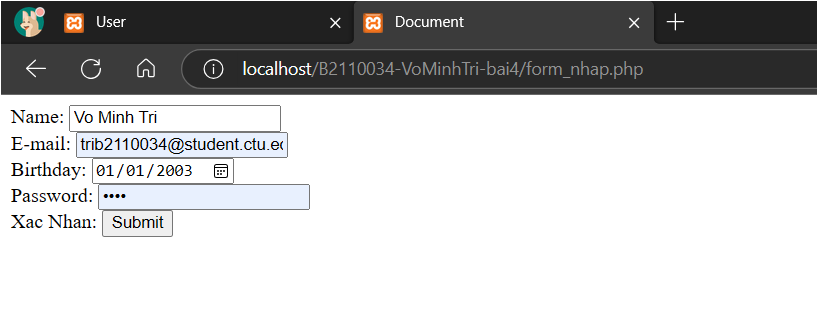
**Gợi ý Tham khảo:**

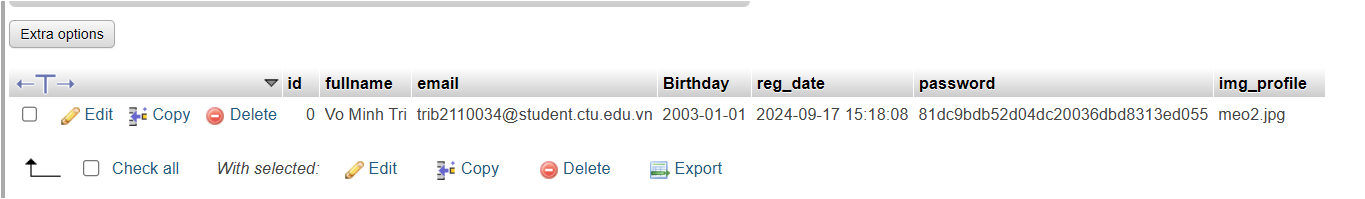
* <https://www.w3schools.com/php/>
* và các nguồn khác mà sinh viên tìm được

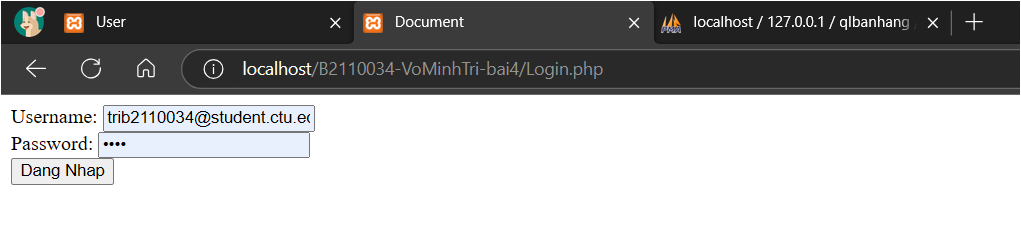
# Yêu cầu bài thực hành:

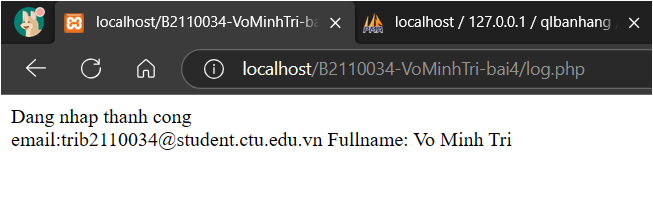
1. Bạn hãy chạy tất cả các lệnh hướng dẫn ở trên và chụp lại màn hình kết quả.



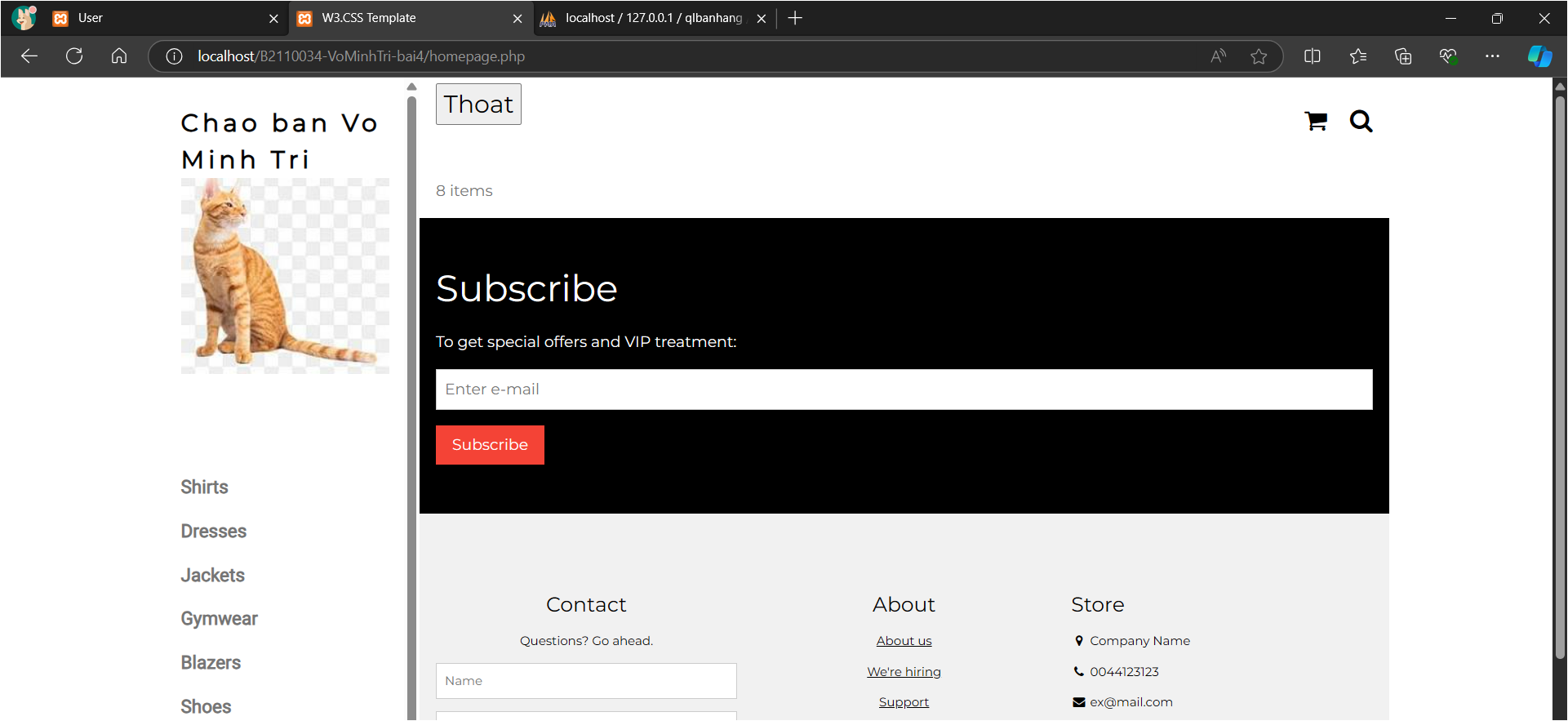


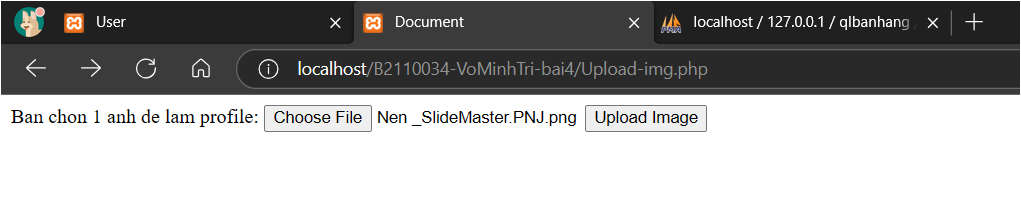


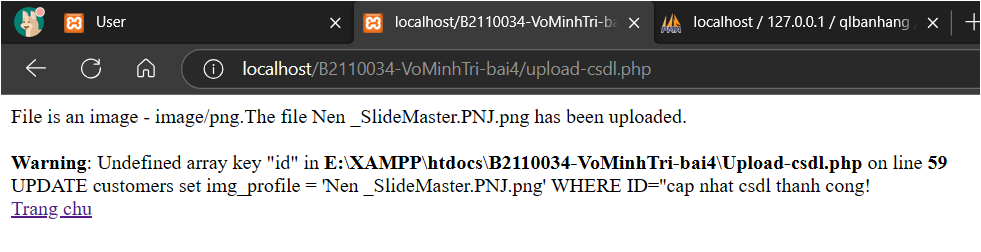


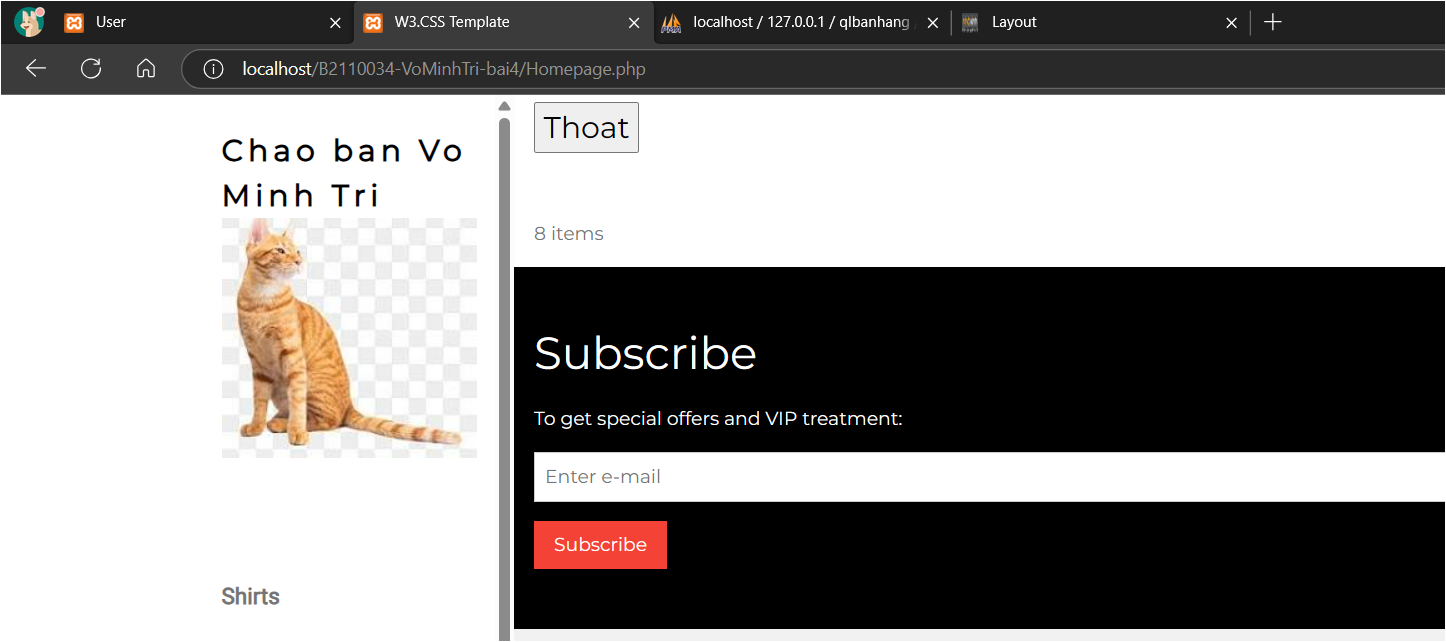


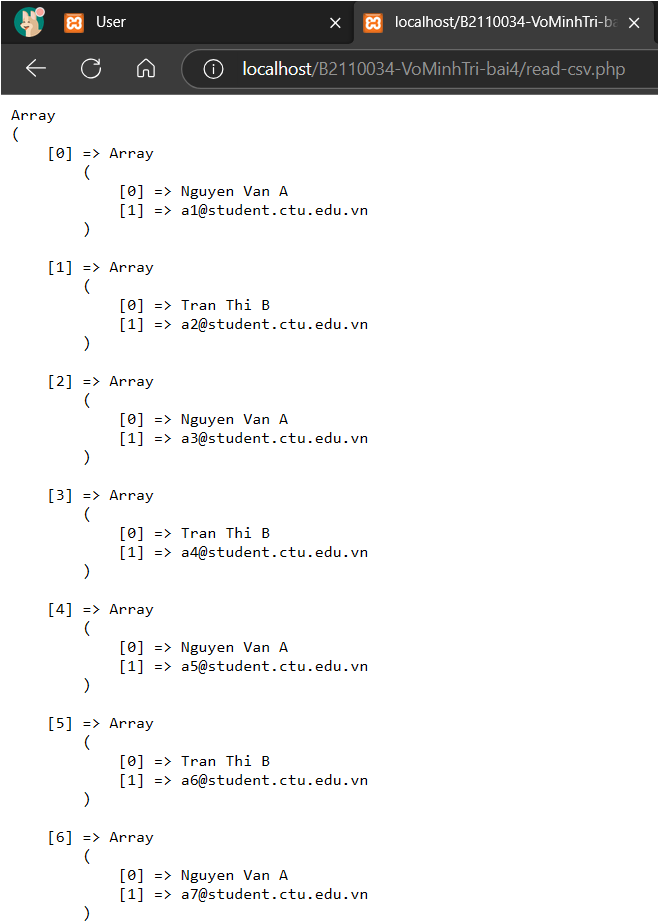
* Sau khi chỉnh sửa file log để điều hướng qua trang homepage







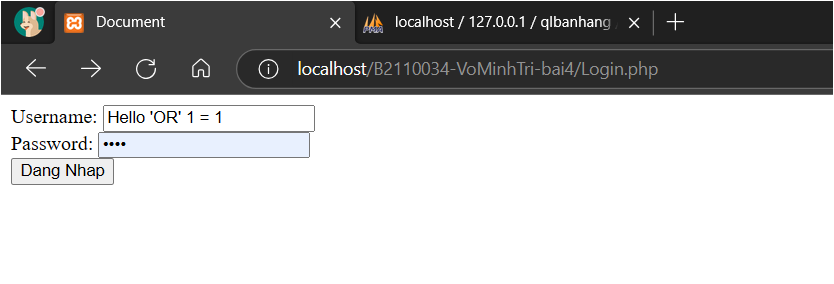




1. Trong vài trường hợp, hacker có thể sử dụng các kỹ thuật SQL Injection để hack hệ thống của bạn. Bạn hãy trình bày SQL Injection là gì và thử các ví dụ trình bày trong [[1]](#footnote-1). Ứng dụng kỹ thuật đó vào trang đăng nhập mà bạn đã tạo, chụp lại các kết quả.

- SQL injection là một kỹ thuật cho phép những kẻ tấn công lợi dụng lỗ hổng của việc kiểm tra dữ liệu đầu vào để inject và thi hành các câu lệnh SQL bất hợp pháp.

Ví dụ: Khi ta đăng nhập vào tài khoản [trib2110034@student.ctu.edu.vn](mailto:trib2110034@student.ctu.edu.vn) (có mật khẩu là 1234)



Ta sẽ để username là Hello ' OR ' 1=1, kết quả chạy như sau :

- Giải thích cơ chế hack :

Thực chất, khi ta đăng nhập ở trang login.php, khi đăng nhập xong sẽ chuyển qua trang log.php. Tại đây sẽ xác nhận tài khoản và mật khẩu nhập vào rồi mới quyết định việc có cho người dùng vào hệ thống hay không. Tuy nhiên, trong code của log.php có đoạn như sau :

Hacker có thể lợi dụng kẻ hở nơi username nhập vào và chèn đoạn « Hehe ' OR ' 1=1 »

Lúc này, câu lệnh truy vấn sẽ bị đổi thành

« select id, fullname, email from customers where email = *Hello OR 1=1* and password = 1234.

Vì 1=1 luôn là kết quả TRUE nên câu lệnh truy vấn trên luôn hợp lệ=>Đăng nhập vào hệ thống thành công.

Link Tham Khảo: <https://www.w3schools.com/sql/sql_injection.asp>

1. Dựa vào link[[2]](#footnote-2), 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 xác định người dùng. Cookie là một tệp nhỏ mà máy chủ nhúng vào máy tính của người dùng.

setcookie(name, value, expire, path, domain, secure, httponly): name là bắt buộc, các tham số khác là tùy chọn

- Diễn giải các tham số trong hàm setcookie:

+ name: tên.

+ value: giá trị.

+ expire: thời hạn.

+ path: đường dẫn.

+ domain: tên miền.

+ secure: true nếu sử dụng HTTPS để truyền dữ liệu (mặc định false).

+ httponly: mặc định là false, nếu true thì chỉ cho phép cookie với giao thức HTTP.

- Lưu: từ PHP có thể thiết lập Cookie bằng hàm setcookie (phải xuất hiện trước thẻ html).

- Lấy: dùng biến $\_COOKIE để truy cập thông tin cookie (có thể dùng isset() để kiểm tra sự tồn tại của COOKIE).

- Xóa: sử dụng chính hàm setcookie với thủ thuật đặt thời gian đã hết hạn.

VD: setcookie( "$cookie\_name", "$cookie\_value", time() -60 , "/","", 0);

Link Tham Khảo: <https://www.w3schools.com/php/php_cookies.asp>

1. Dựa vào link[[3]](#footnote-3), bạn hãy cho biết Session dùng để làm gì. Cách lưu, lấy, xóa giá trị trong Session.

- Session dùng để lưu trữ thông tin (trong các biến) sẽ được sử dụng trên nhiều trang. Không giống như cookie, thông tin không được lưu trữ trên máy tính của người dùng.

- Lưu: một phiên được bắt đầu với session\_start() chức năng. Các biến session được đặt bằng biến toàn cục PHP: $\_SESSION.

- Lấy: dùng biến $\_SESSION để truy cập thông tin session.

- Xóa: để xóa session sử dụng hàm session\_unset() và session\_destroy() .

Link Tham Khảo: <https://www.w3schools.com/php/php_sessions.asp>

1. Bạn hãy so sánh Cookie và Session.

- Về Cookie:

+ Cookie được lưu trữ trên trình duyệt người dùng.

+ Cookie dược lưu trữ ở phía máy khách.

+ Cookie dễ dàng sửa đổi vì được lưu trữ ở phía máy khách.

+ Dữ liệu có sẵn trong trình duyệt chạy đến khi hết hạn.

- Về Session:

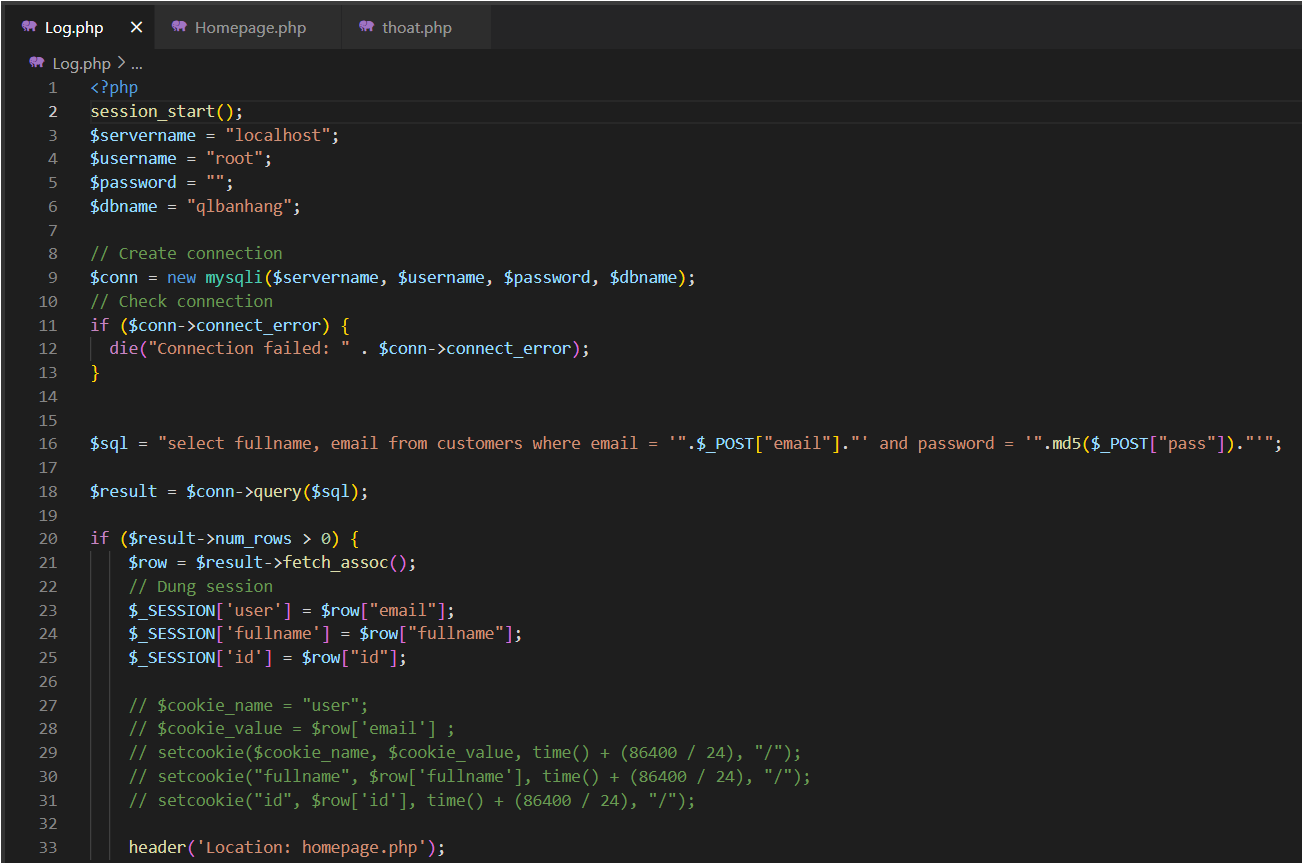
+ Session không được lưu trữ trên trình duyệt người dùng.

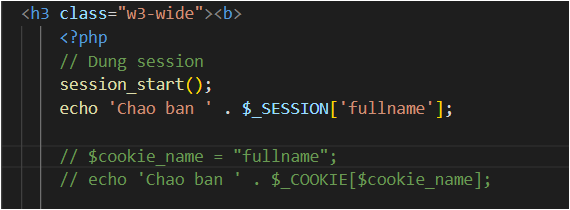
+ Session được lưu trữ ở phía máy chủ.

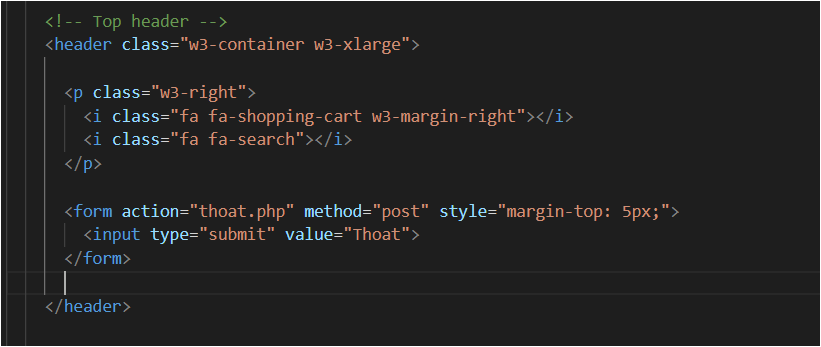
+ Session không dễ dàng sửa đổi vì được lưu trữ ở phía máy chủ.

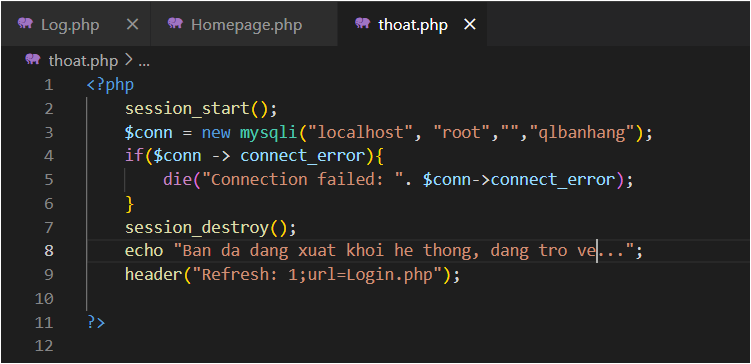
+ Dữ liệu có sẵn cho trình duyệt chạy, sẽ mất thông tin session khi đóng trình duy

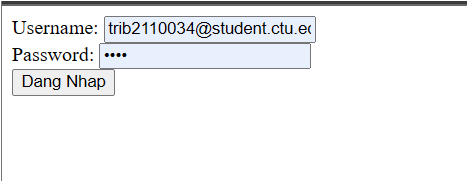
1. Chỉnh sửa các đoạn gán, khởi tạo, lấy giá trị cookie trong log.php và homepage.php thay bằng cách dùng Session. Tạo tập tin thoat.php để xóa các giá trị trong session, cookie thực hiện chức năng log out khỏi hệ thống.

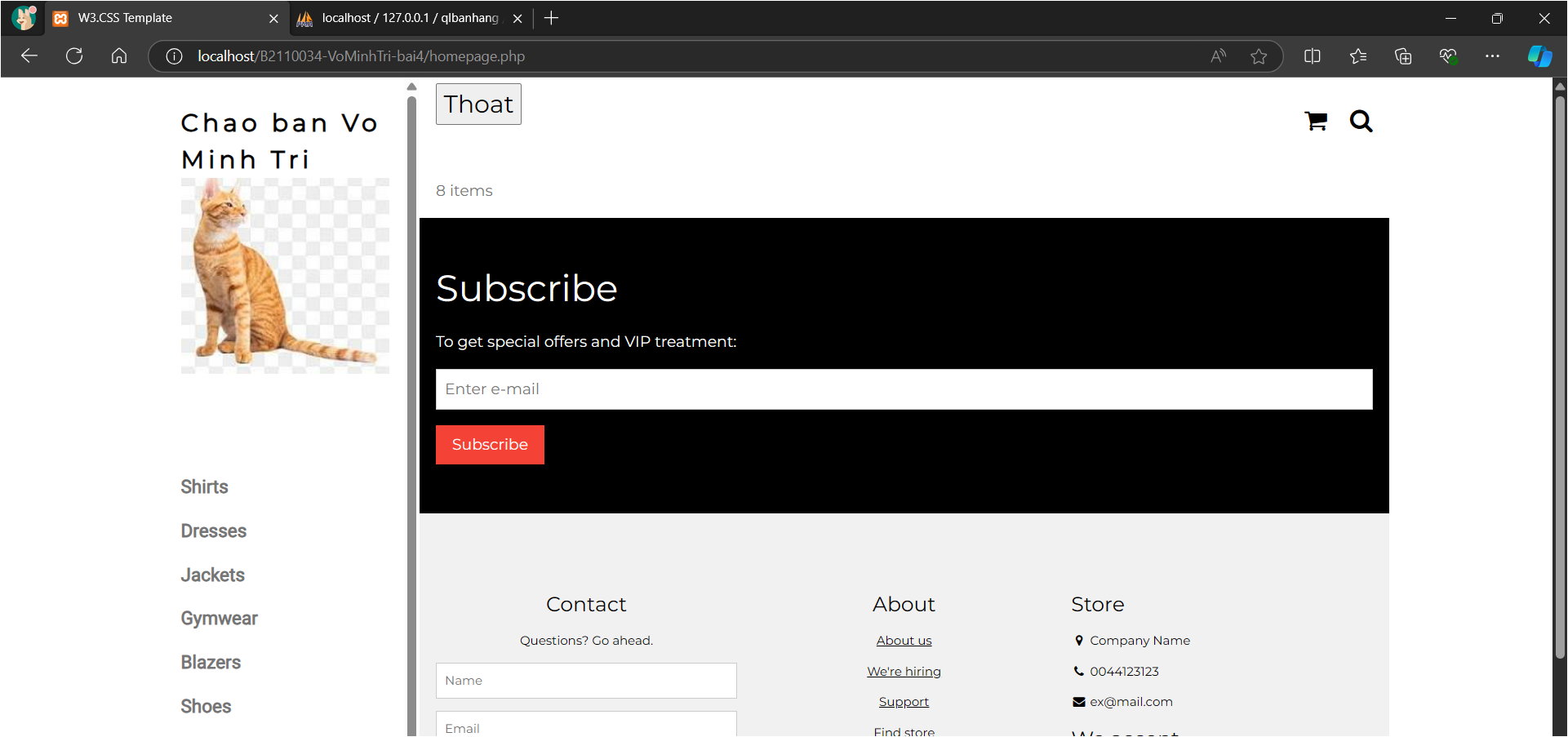


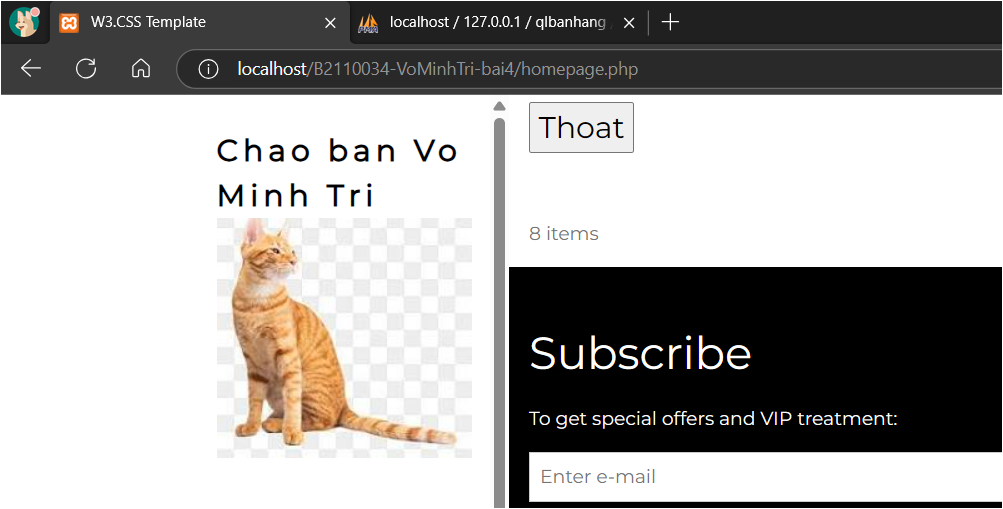




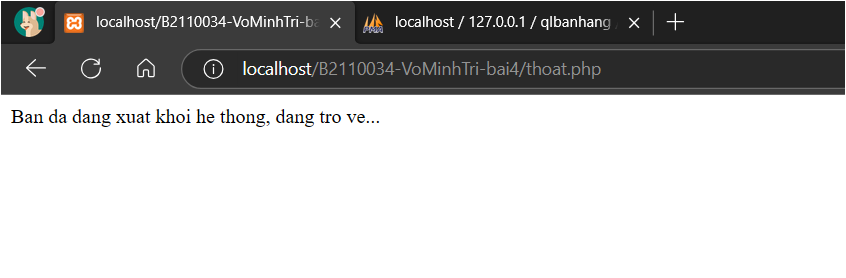




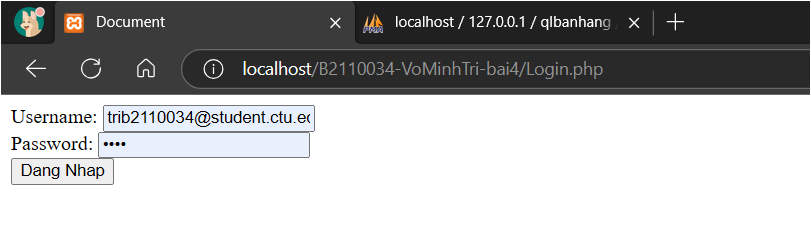




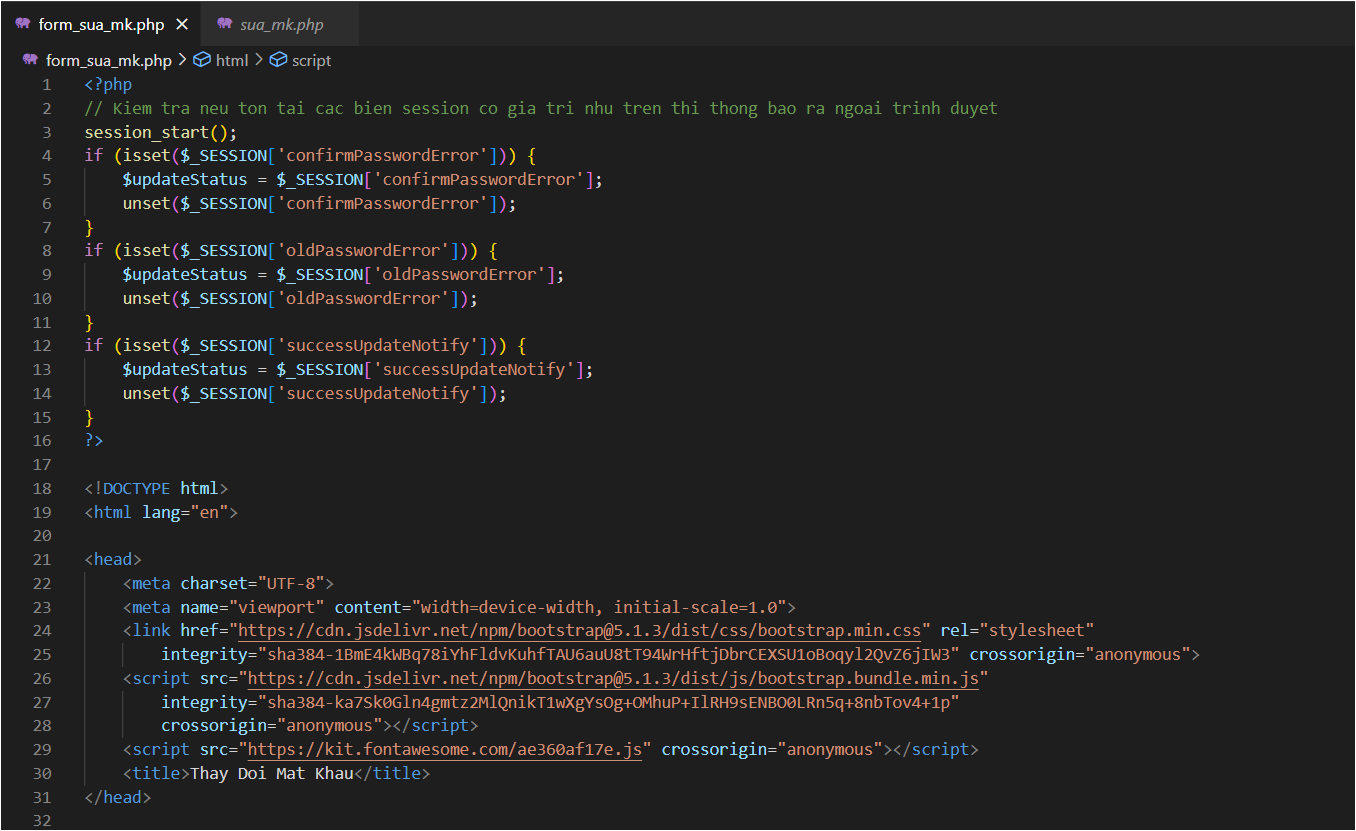
* Sau khi click vào nút thoát

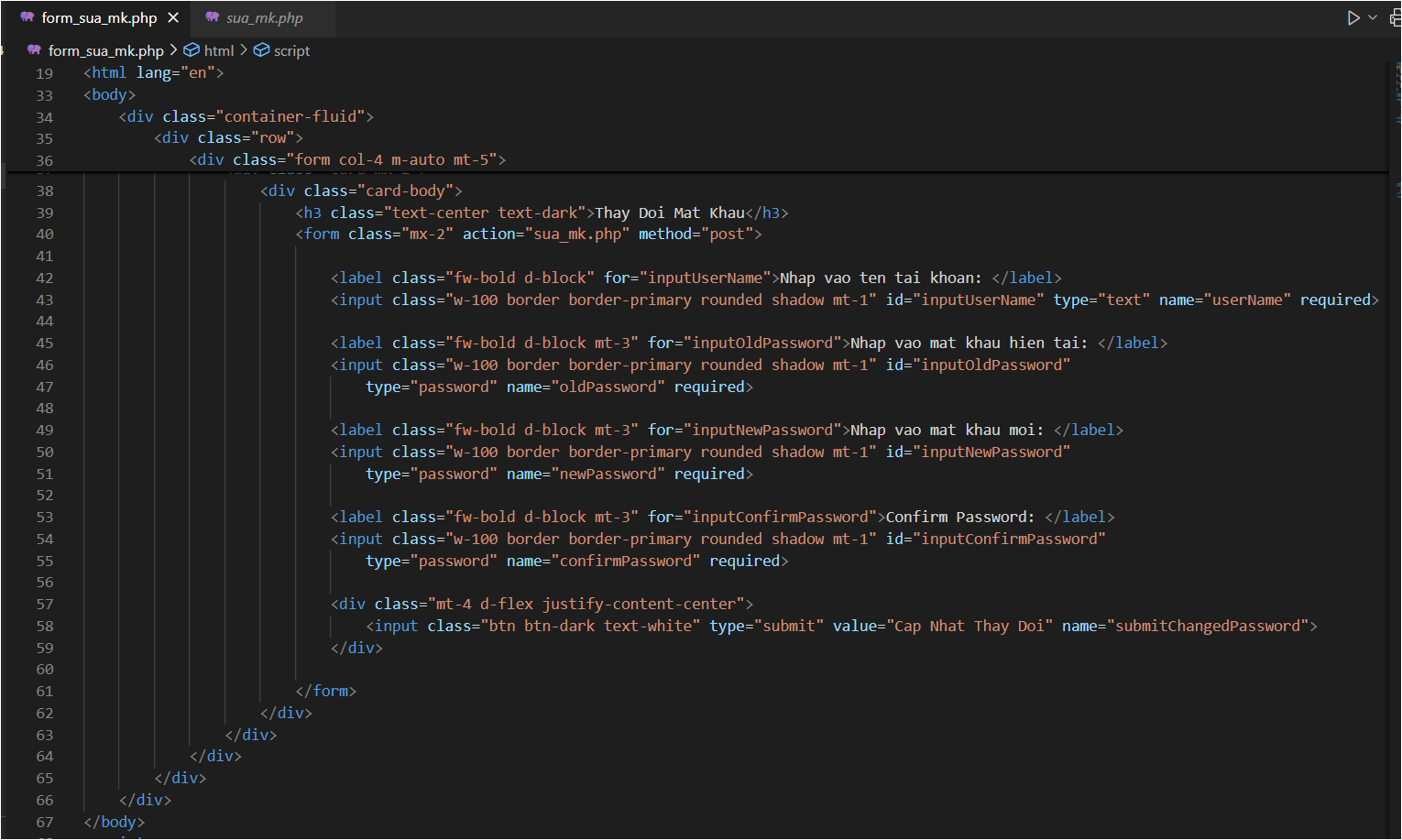


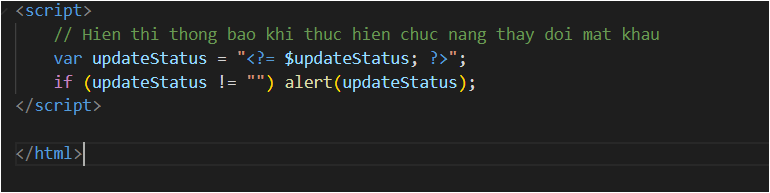
* Sau khi thoát sẽ trở về trang đăng nhập

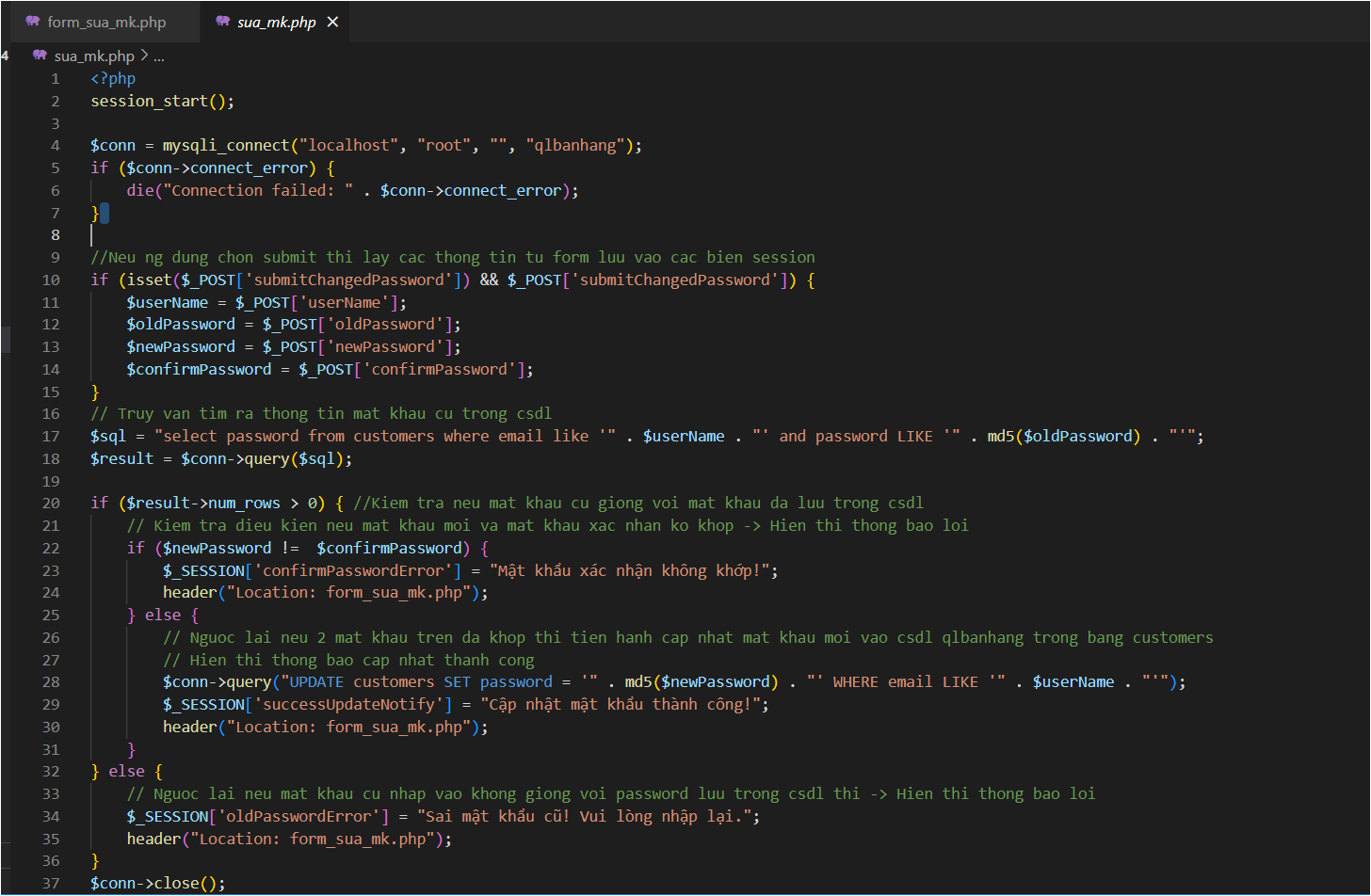


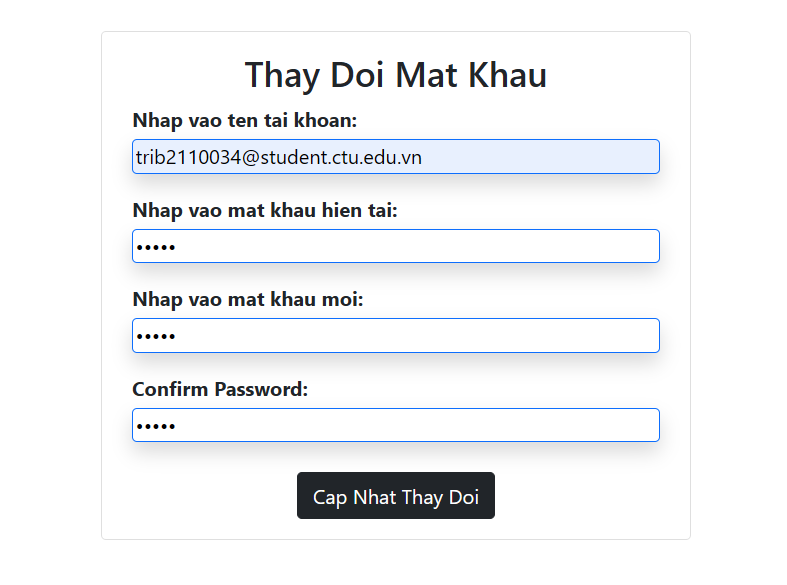
1. Bạn hãy tạo form sua\_mk.php cho phép người dùng chỉnh sửa mật khẩu sau khi đăng nhập. Yêu cầu gồm 3 input: ô để nhập mật khẩu cũ, 1 ô để nhập mật khẩu mới, 1 ô cho phép nhập mật lại mật khẩu mới. Khi nhập xong cần đảm bảo: mật khẩu cũ là khớp với CSDL đang lưu, 2 ô nhập mật khẩu mới phải khớp với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



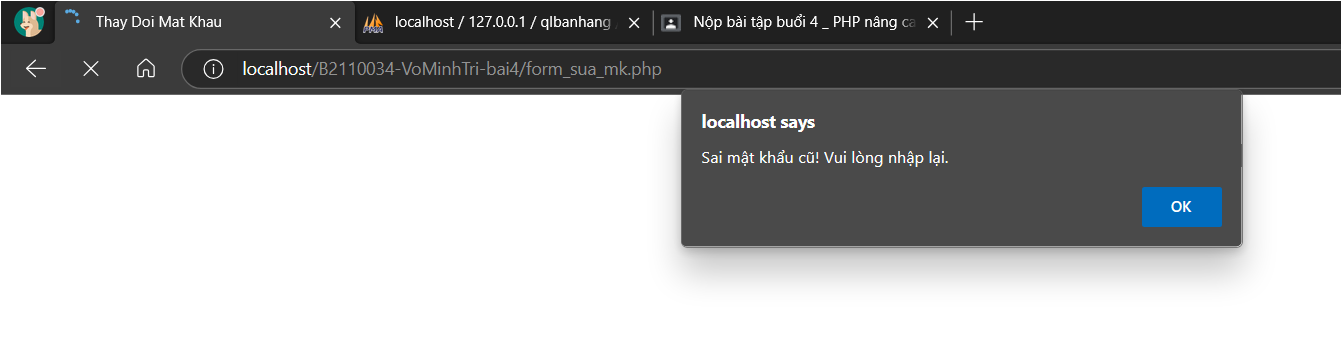




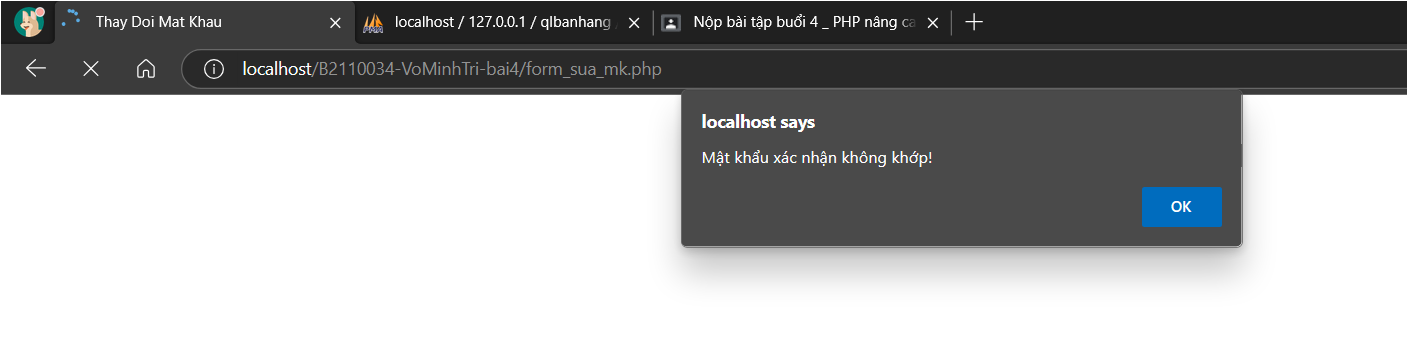




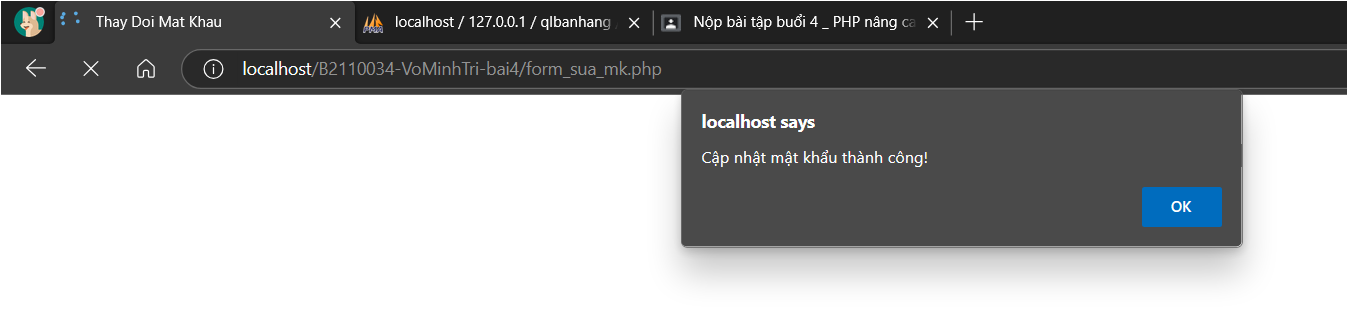
* Trường hợp nhập mật khẩu hiện tại sai



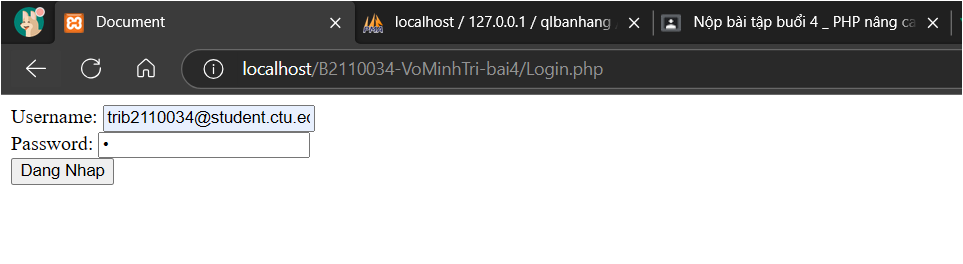
* Trường hợp nhập mật khẩu xác nhận sai



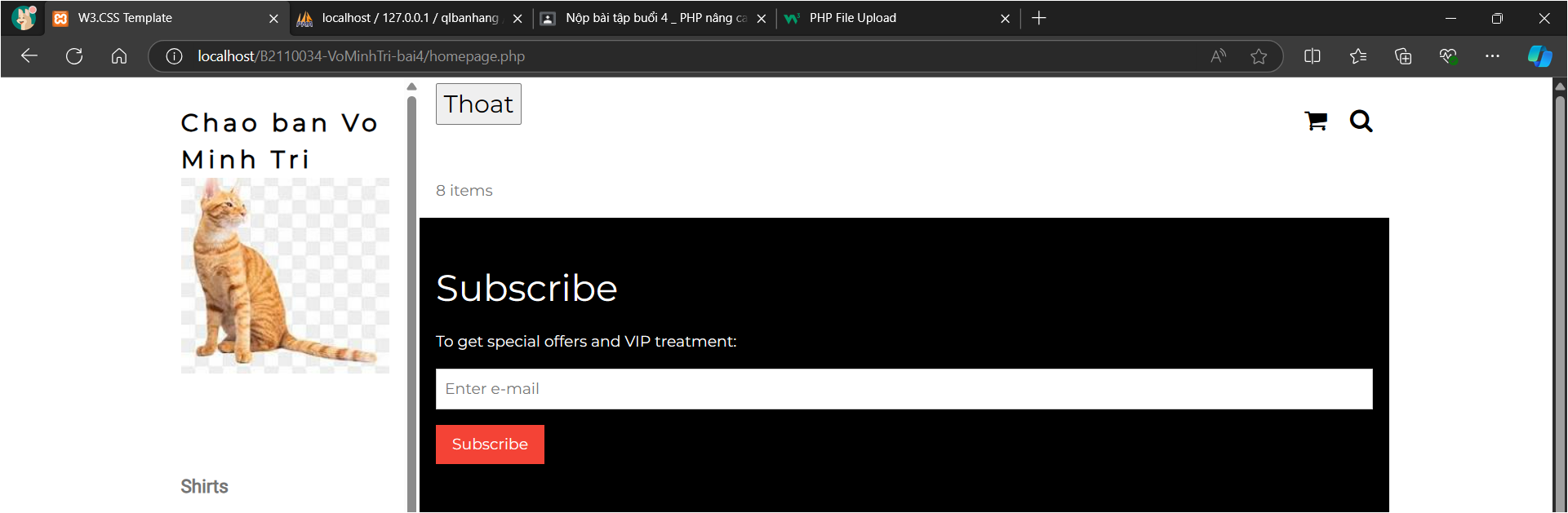
* Trường hợp cập nhật thành công



* Đăng nhập lại với mật khẩu mới



* Đăng Nhập Thành Công



1. Bạn đọc trong[[4]](#footnote-4) để tìm hiểu và mô tả các cơ chế, các hàm/thủ tục để thực hiện việc upload.
2. Bạn hãy đọc[[5]](#footnote-5), mô tả chức năng của hàm này và các tham số trong hàm (tham khảo thêm từ read-csv.php).
3. 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]](#footnote-6),[[7]](#footnote-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.

**Chú ý:**

* Các bạn nộp file word: Quy tắc đặt tên file: **<mssv>-<hoten>-<bai><stt\_bai thực hành>.docx** nộp lên Classroom (VD: **B123456-NguyenVanA-bai1.docx**), kèm với các file khác được yêu cầu như phần câu hỏi đã nêu. **Ngoại trừ file word trả lời câu hỏi, các file còn lại các bạn nén vào 1 file zip**. File zip đặt tên như file word.
* Mỗi câu các bạn trả lời bằng hình hoặc dạng text tùy vào yêu cầu của câu hỏi và **TRẢ LỜI THEO ĐÚNG THỨ TỰ CÂU HỎI**. Nếu câu nào không trả lời được các bạn cứ để số thứ tự câu hỏi và bỏ trống phần trả lời.
* Các câu trả lời có tham khảo trên Internet phải trích dẫn link/nguồn.
* *Vi phạm 1 trong các điều sau đây bài thực hành sẽ bị 0 điểm:*
  + Đặt tên KHÔNG ĐÚNG quy tắc được yêu cầu.
  + Bài không đủ các thành phần (word, code+data (nếu có),...) đã được yêu cầu.
  + Bài không thực hiện đúng yêu cầu “**Ngoại trừ file word trả lời câu hỏi, các file còn lại các bạn nén vào 1 file .zip”**
  + Bị phát hiện copy, sao chép từ các bạn khác
  + Phần trả lời không ghi rõ trả lời cho câu nào
  + Thứ tự câu trả lời không đúng thứ tự câu hỏi

1. <https://www.w3schools.com/sql/sql_injection.asp> [↑](#footnote-ref-1)
2. <https://www.w3schools.com/php/php_cookies.asp> [↑](#footnote-ref-2)
3. <https://www.w3schools.com/php/php_sessions.asp> [↑](#footnote-ref-3)
4. <https://www.w3schools.com/php/php_file_upload.asp> [↑](#footnote-ref-4)
5. <https://www.w3schools.com/php/func_filesystem_file.asp> [↑](#footnote-ref-5)
6. <https://www.php.net/manual/en/features.file-upload.post-method.php>, [↑](#footnote-ref-6)
7. https://stackoverflow.com/questions/6654351/check-file-uploaded-is-in-csv-format [↑](#footnote-ref-7)