Bài tập thực hành 04

**MSSV: B2203437**

**Họ và tên sinh viên: Dương Hữu Đan**

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:**

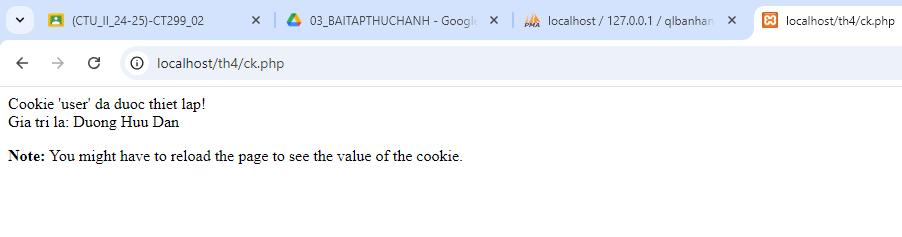
* <https://www.w3schools.com/php/>
* và các nguồn khác mà sinh viên tìm được

# Yêu cầu bài thực hành:

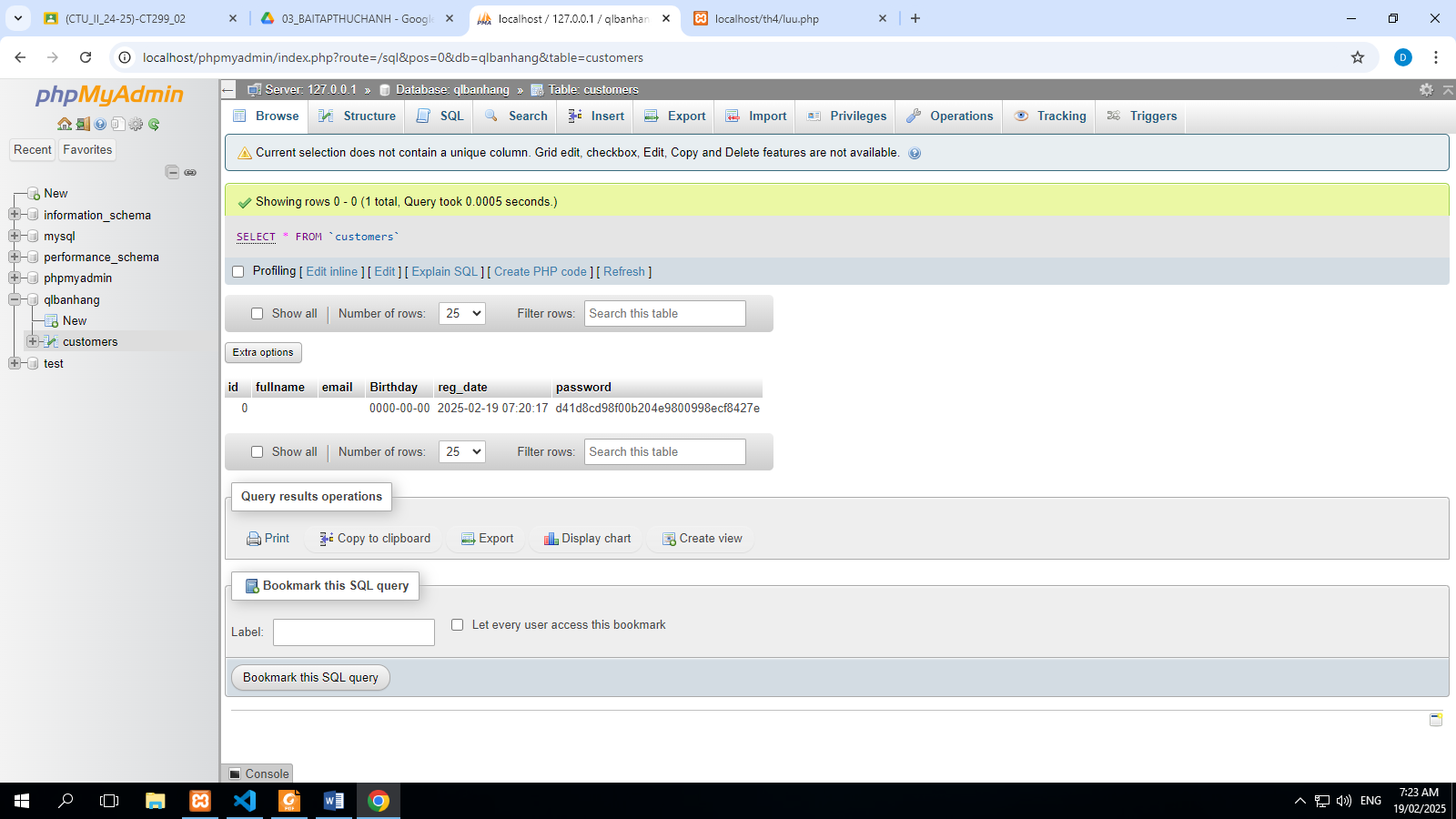
1. Bạn hãy chạy tất cả các lệnh hướng dẫn ở trên và chụp lại màn hình kết quả.

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

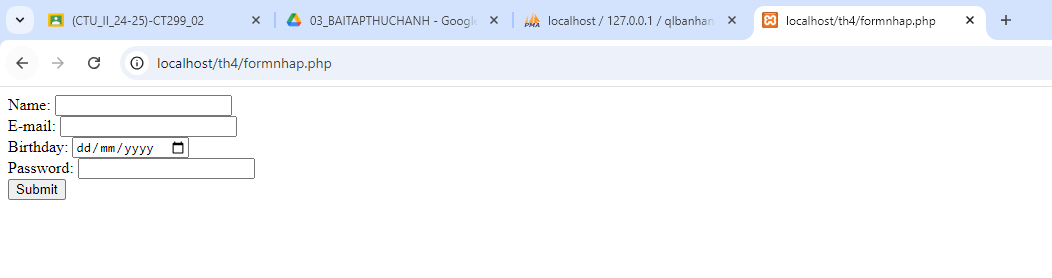
Ck.php

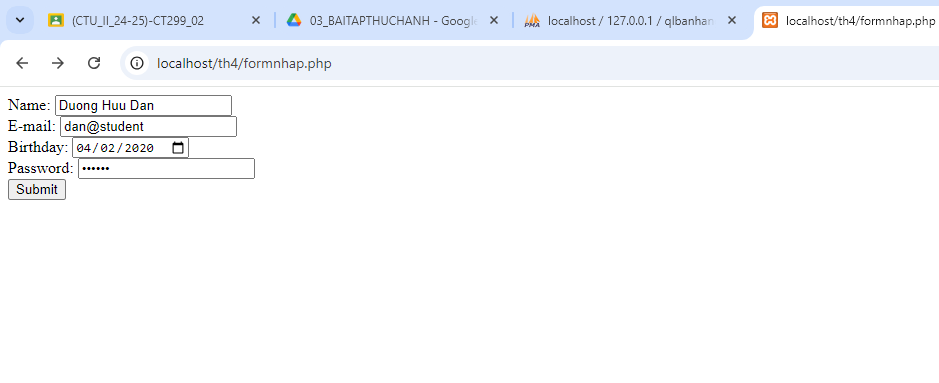


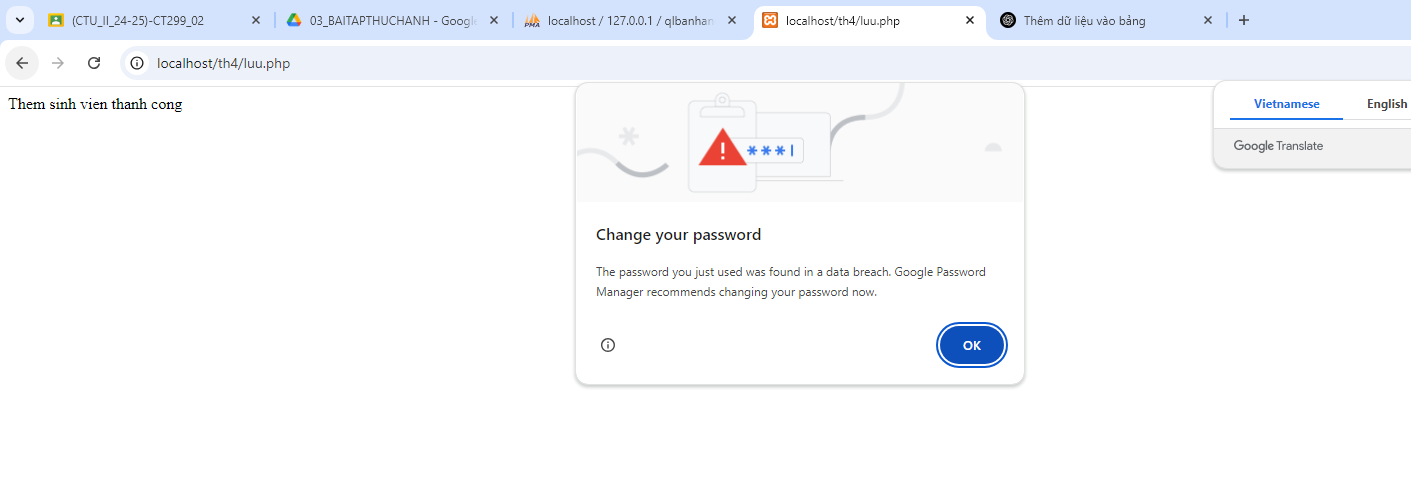
Tạo CSDL



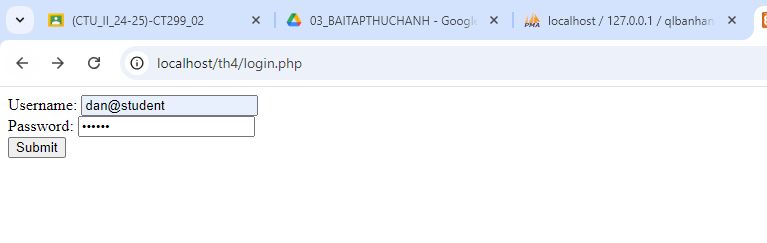
Formnhap.php, luu.php

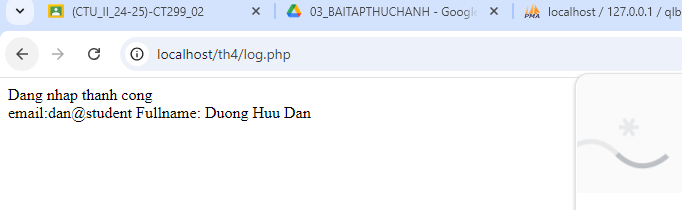






Login.php, log.php

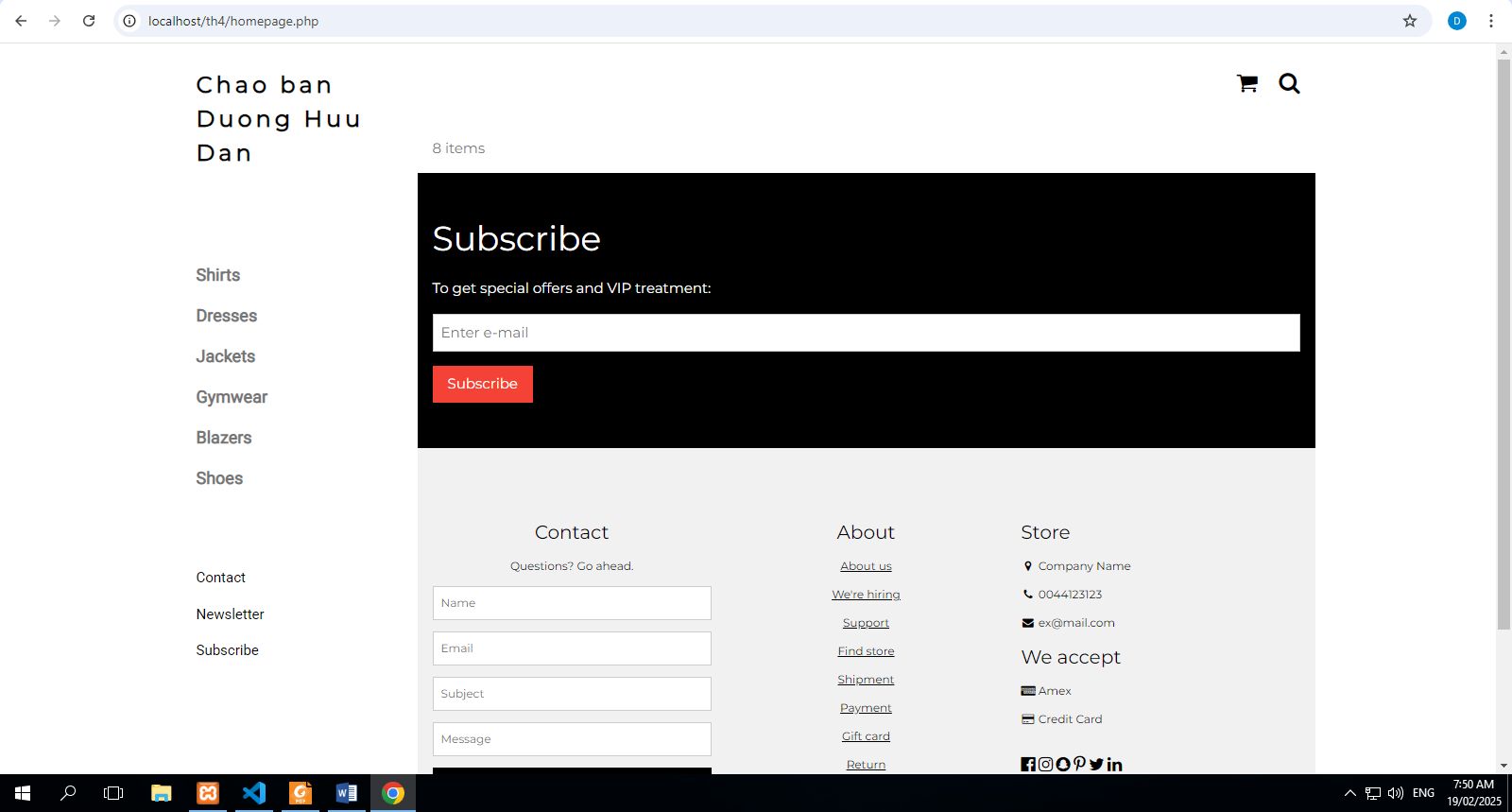


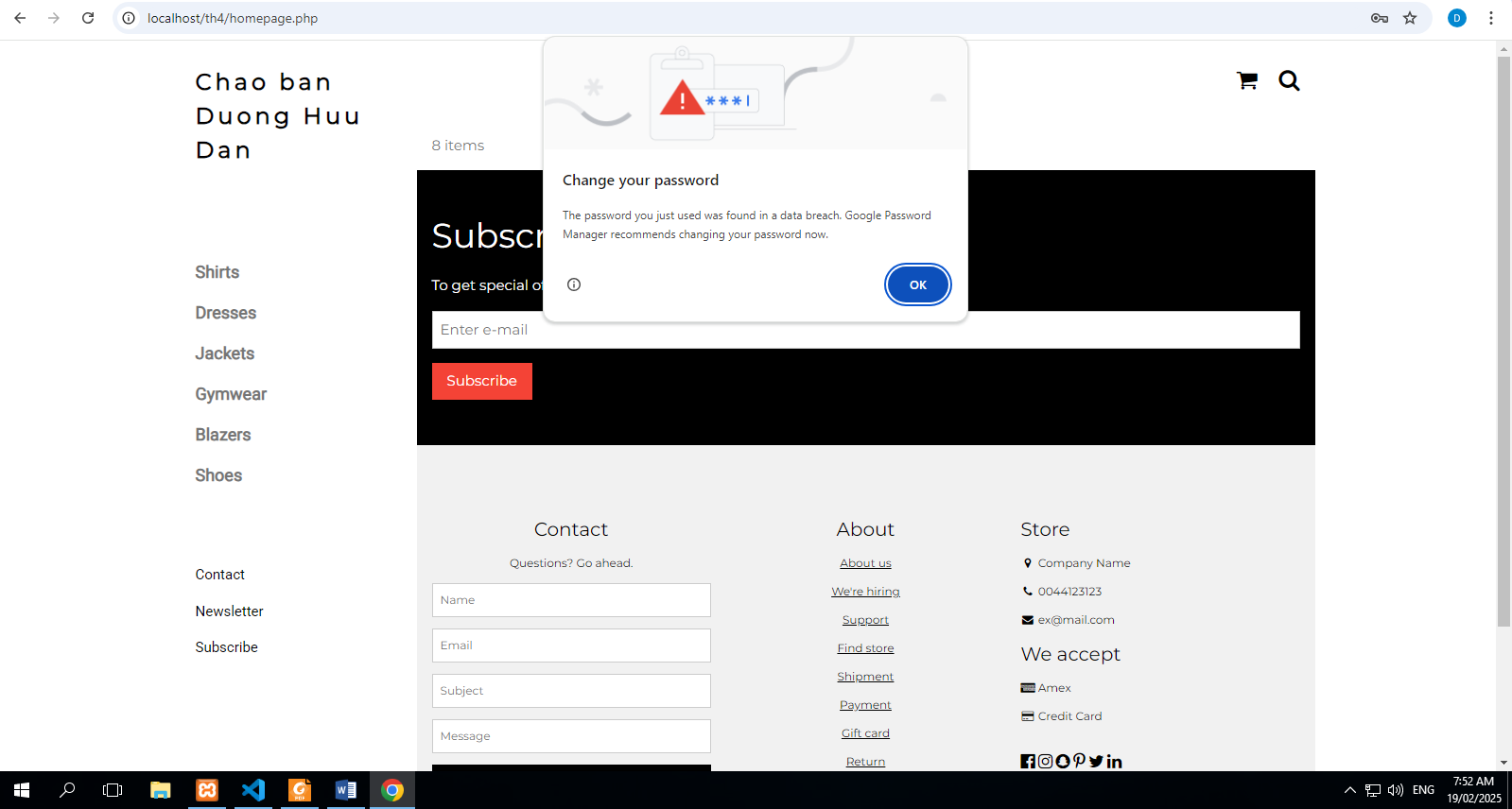
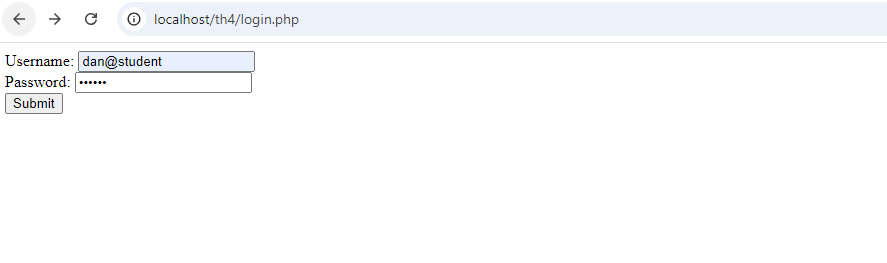


Dùng Cookies lưu lại tên đăng nhập, email và điều hướng

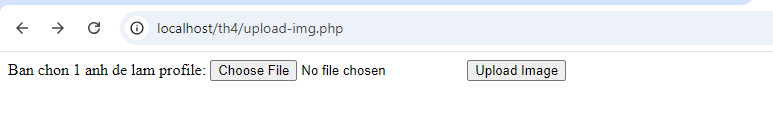
Log.php (modified)

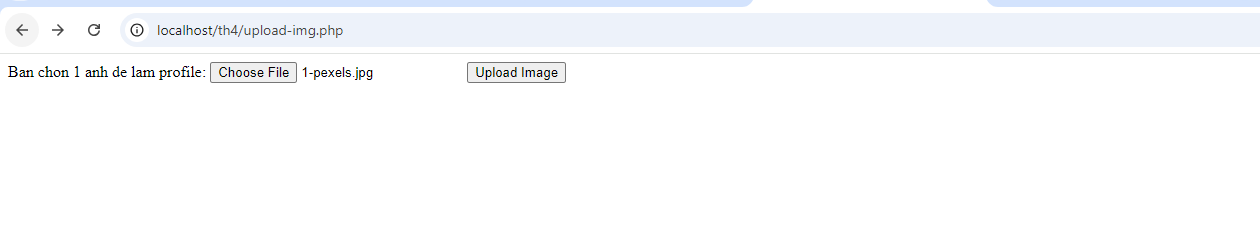
Homepage.php

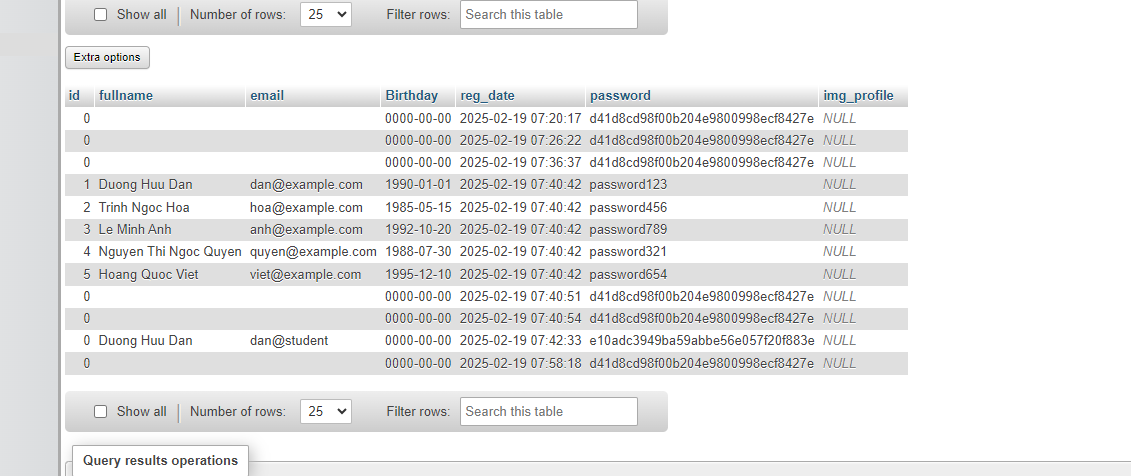




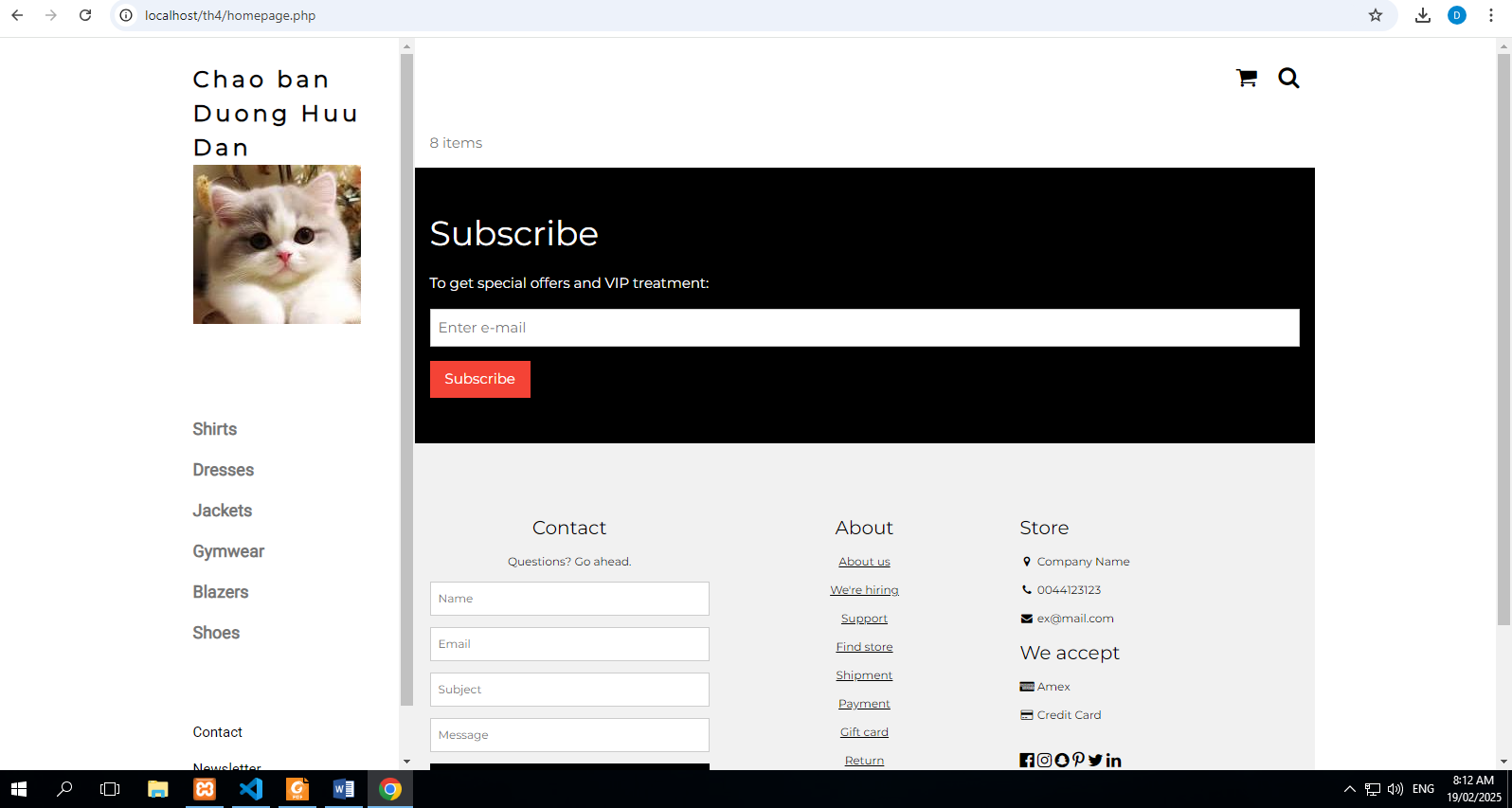
Upload-img.php, upload.php

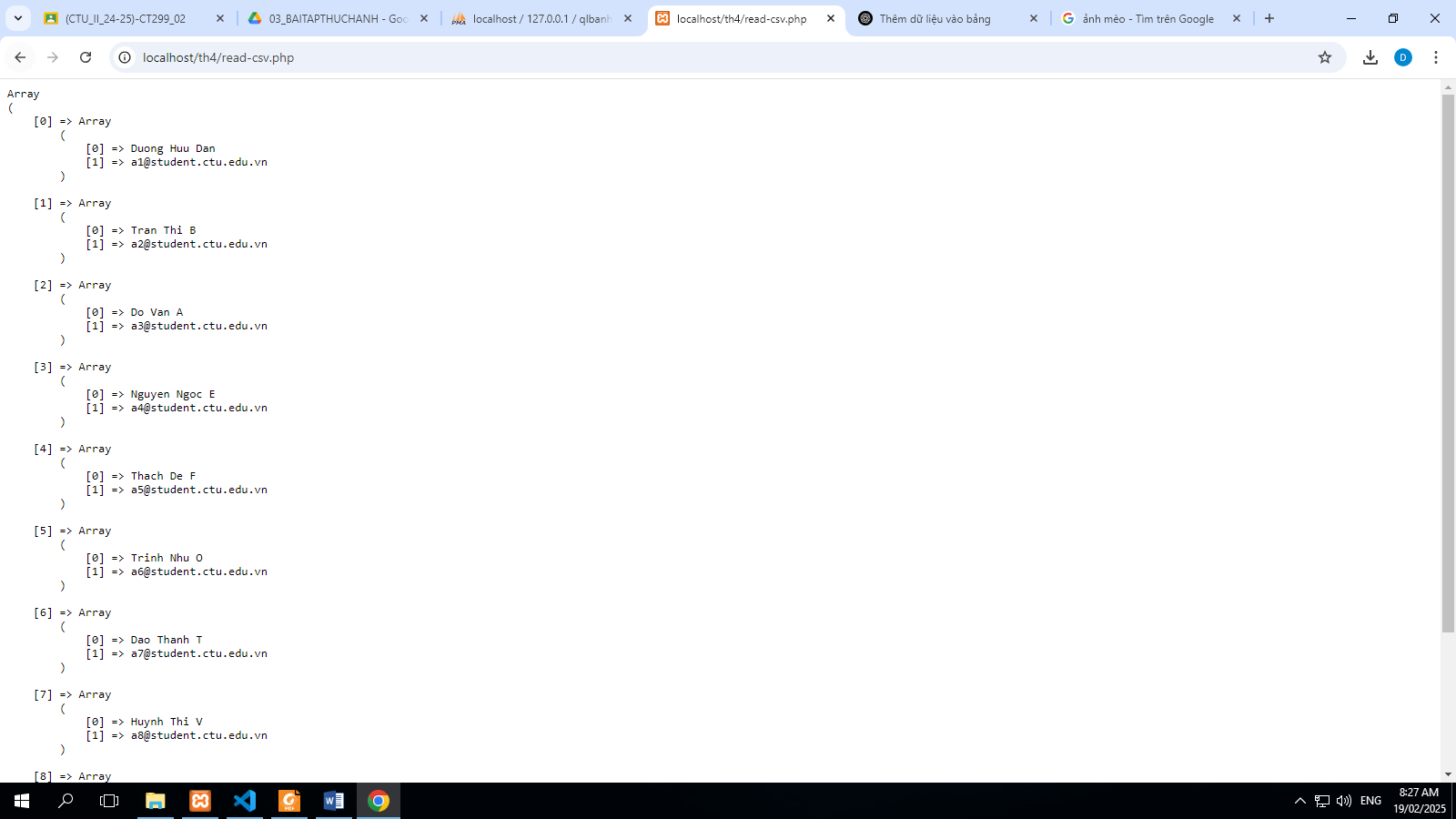






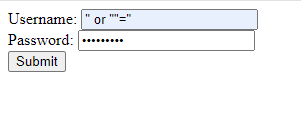
Upload-csdl.php

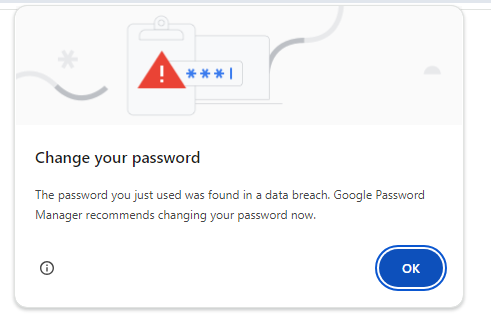
 read-csv.php



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 tấn công mà hacker lợi dụng các lỗ hổng trong ứng dụng web, đặc biệt là khi ứng dụng không kiểm tra hoặc làm sạch dữ liệu đầu vào từ người dùng. Hacker có thể chèn mã SQL độc hại vào truy vấn SQL và làm gián đoạn hoặc thao túng cơ sở dữ liệu.





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** là một đoạn dữ liệu nhỏ được lưu trên trình duyệt của người dùng, giúp lưu trữ thông tin trạng thái của người dùng giữa các lần truy cập. Cookie thường dùng để lưu thông tin đăng nhập, tùy chọn người dùng, hoặc theo dõi hoạt động của người dùng.
* Các tham số trong setcookie(name, value, expire, path, domain, secure, httponly);

1. name: Tên của cookie.
2. value: Giá trị của cookie.
3. expire: Thời gian hết hạn (tính bằng giây từ thời điểm hiện tại).
4. path: Đường dẫn trên server nơi cookie có thể truy cập.
5. domain: Domain mà cookie sẽ được gửi tới.
6. secure: Nếu là true, cookie chỉ được gửi qua HTTPS.
7. httponly: Nếu là true, cookie chỉ có thể được truy cập thông qua HTTP, không thể truy cập từ JavaScript.

* Lưu cookie

setcookie("username", "john\_doe", time() + 3600, "/");

* Lấy cookie

echo $\_COOKIE['username'];

* Xóa cookie

setcookie("username", "", time() - 3600, "/");

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** là một cơ chế giúp lưu trữ thông tin về người dùng trên server trong suốt quá trình sử dụng ứng dụng, và thông tin này có thể được truy cập trong các yêu cầu tiếp theo của người dùng.
* Lưu

session\_start();

$\_SESSION['username'] = 'john\_doe';

* Lấy

echo $\_SESSION['username'];

* Xóa

unset($\_SESSION['username']);

* Hủy toàn bộ

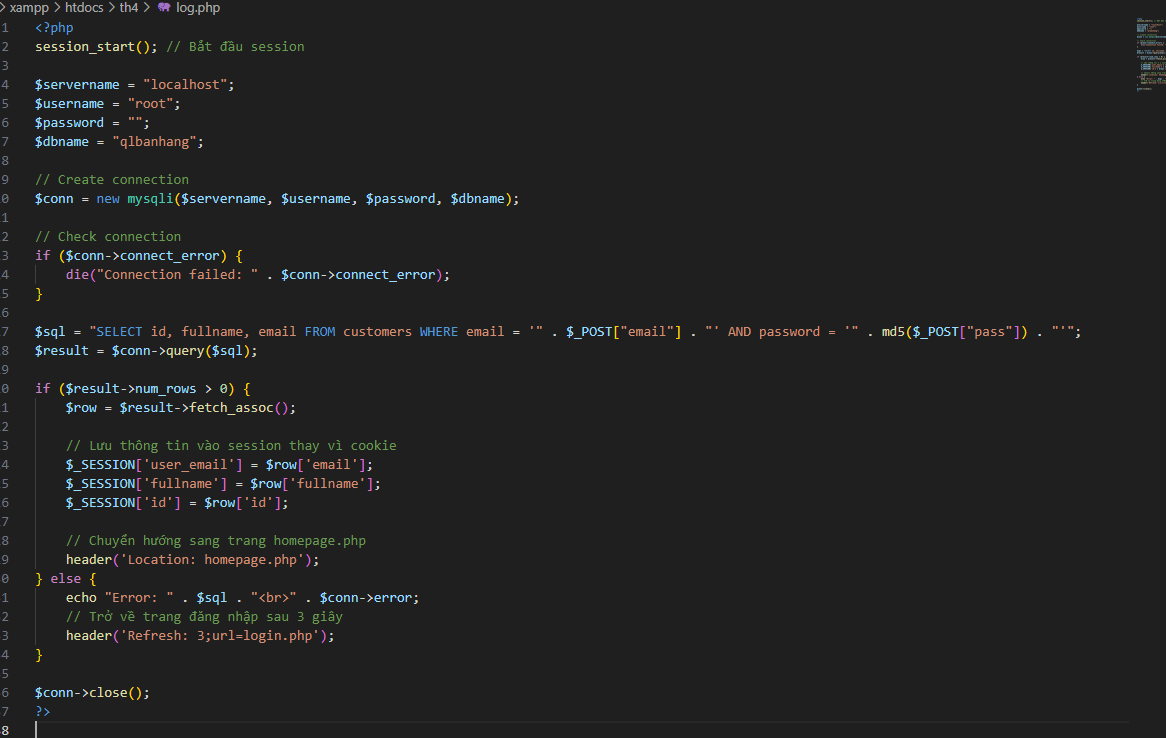
session\_destroy();

1. Bạn hãy so sánh Cookie và Session.

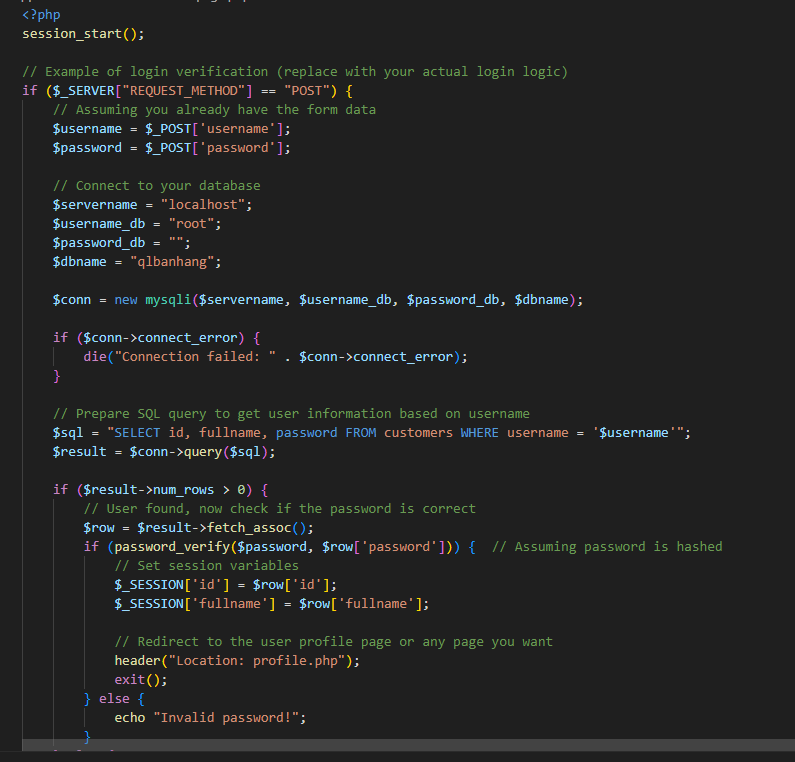
|  |  |  |
| --- | --- | --- |
| Tiêu chí | Cookie | Session |
| Lưu trữ | Lưu trên trình duyệt của người dùng. | Lưu trên server. |
| Kích thước | Lượng dữ liệu nhỏ (thường dưới 4KB). | Không giới hạn (tùy vào cấu hình server). |
| Thời gian sống | Có thể được thiết lập thời gian hết hạn (expire). | Duy trì cho đến khi phiên làm việc kết thúc hoặc hủy. |
| Bảo mật | Dễ bị giả mạo nếu không mã hóa, có thể bị đánh cắp. | An toàn hơn, chỉ có thể truy cập từ server. |
| Tính di động | Di động, cookie sẽ được gửi cùng với các yêu cầu HTTP. | Không di động, chỉ có thể sử dụng trong phiên hiện tại. |

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.

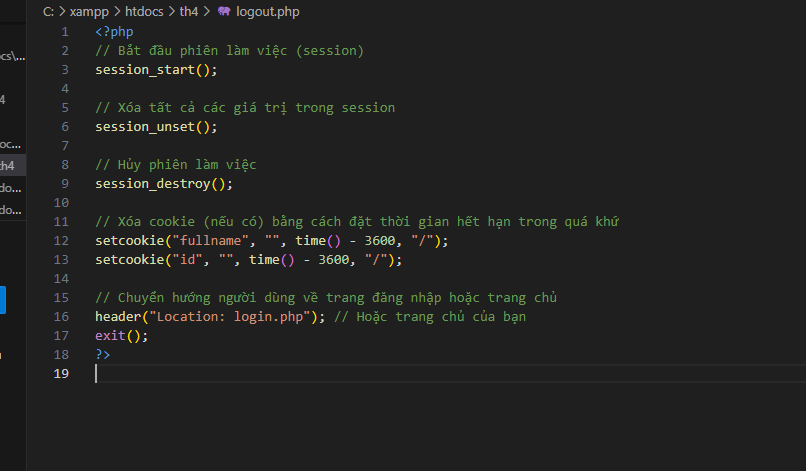
Log.php



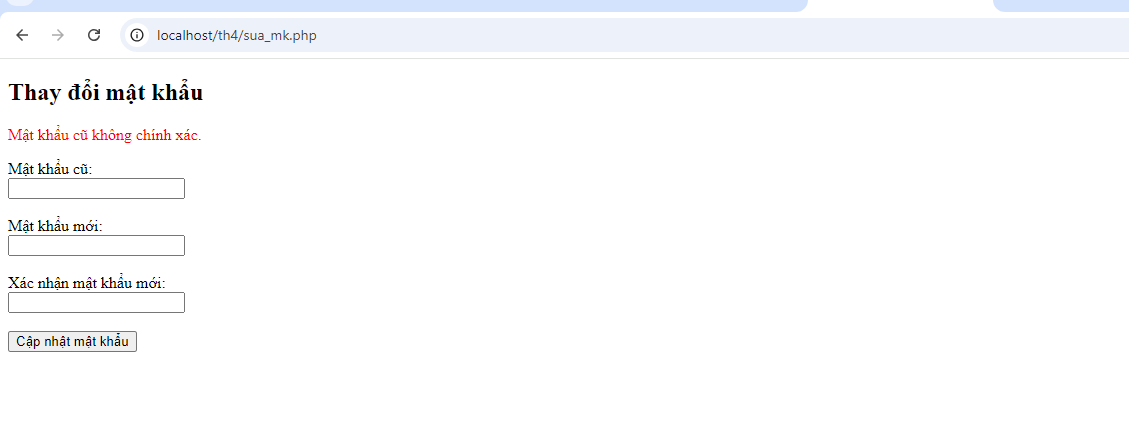
Homepage.php



Logout.php



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.



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.

* Để thực hiện việc **upload tệp tin** trong PHP, bạn có thể làm theo các bước sau:

1. Tạo Biểu Mẫu HTML
2. Xử Lý Tệp Tin Trong PHP

* Các hàm và thủ tục
* $\_FILES: Biến siêu toàn cục trong PHP, chứa thông tin về tệp tin được upload, bao gồm:
  + $\_FILES["fileToUpload"]["name"]: Tên gốc của tệp tin.
  + $\_FILES["fileToUpload"]["tmp\_name"]: Đường dẫn tạm thời của tệp tin trên server.
  + $\_FILES["fileToUpload"]["size"]: Kích thước của tệp tin (tính bằng byte).
  + $\_FILES["fileToUpload"]["error"]: Mã lỗi nếu có sự cố khi upload.
* getimagesize(): Kiểm tra xem tệp tin có phải là hình ảnh hay không bằng cách trả về kích thước và loại MIME của hình ảnh.
* move\_uploaded\_file(): Di chuyển tệp tin từ vị trí tạm thời đến thư mục đích trên server. Đây là bước quan trọng để lưu trữ tệp tin một cách an toàn.
* pathinfo(): Trả về thông tin về đường dẫn tệp tin, bao gồm phần mở rộng của tệp tin, giúp xác định loại tệp tin.

1. 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).

**Hàm file() trong PHP**

* Hàm file() trong PHP được sử dụng để đọc toàn bộ nội dung của một tệp và lưu mỗi dòng vào một phần tử của một mảng. Mỗi phần tử trong mảng đại diện cho một dòng của tệp, bao gồm cả ký tự xuống dòng nếu có.

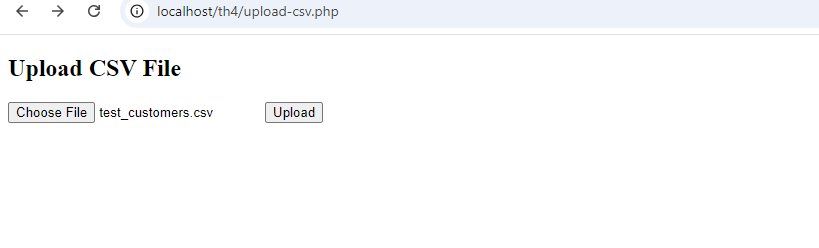
Cú pháp:

array file ( string $filename [, int $flags = 0 [, resource $context ]] )

### Tham số:

* $filename: Đường dẫn đến tệp cần đọc.
* $flags (tùy chọn): Các cờ ảnh hưởng đến cách đọc tệp:
  + FILE\_USE\_INCLUDE\_PATH: Tìm kiếm tệp trong include\_path.
  + FILE\_IGNORE\_NEW\_LINES: Bỏ qua ký tự xuống dòng ở cuối mỗi dòng.
  + FILE\_SKIP\_EMPTY\_LINES: Bỏ qua các dòng trống trong tệp.
* $context (tùy chọn): Ngữ cảnh của tệp, cung cấp các tùy chọn và thiết lập khi làm việc với tệp.

1. 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)