**Bài tập thực hành 04**

Lập trình PHP nâng cao

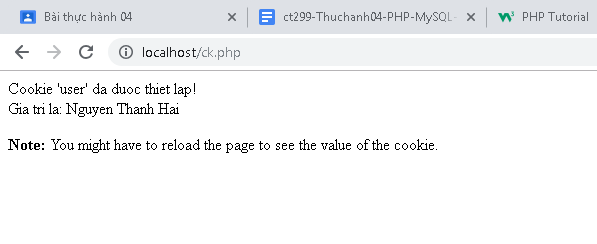
1. Bạn hãy chạy tất cả các lệnh hướng dẫn ở trên và chụp lại màn hình kết quả.

## Tạo Cookies

Cookies và Session hỗ trợ chúng ta quản lý các phiên đăng nhập/đăng nhập, hoạt động của người dùng trên các website

Tạo tập tin sử dụng khởi tạo cookies ck.php sau:

### ck.php



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

Tạo csdl qlbanhang, với bảng customers đầu tiên như sau:

CREATE TABLE `customers` (

`id` int(6) UNSIGNED NOT NULL,

`fullname` varchar(50) CHARACTER SET latin1 NOT NULL,

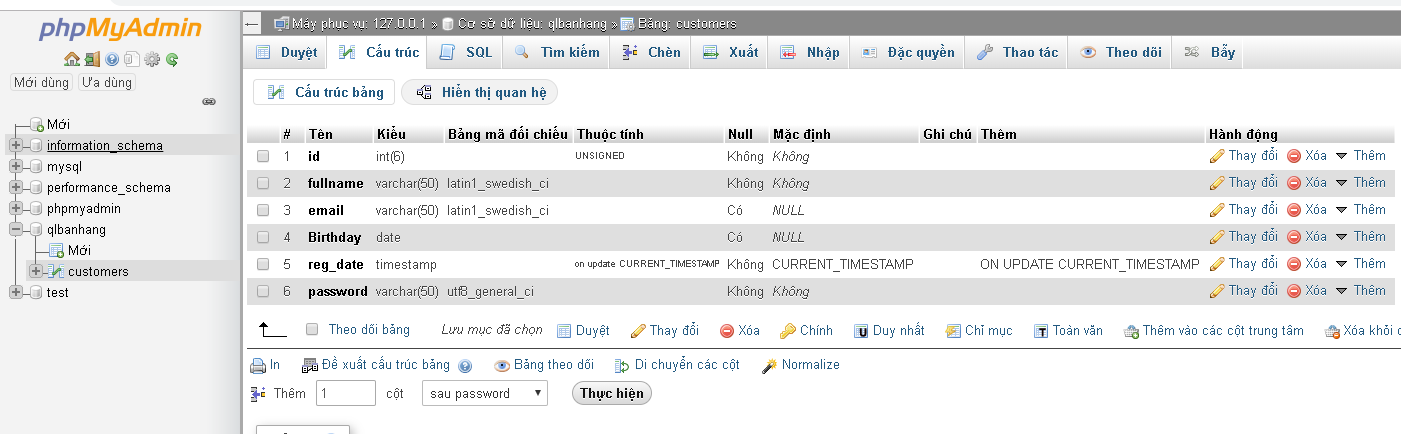
`email` varchar(50) CHARACTER SET latin1 DEFAULT NULL,

`Birthday` date DEFAULT NULL,

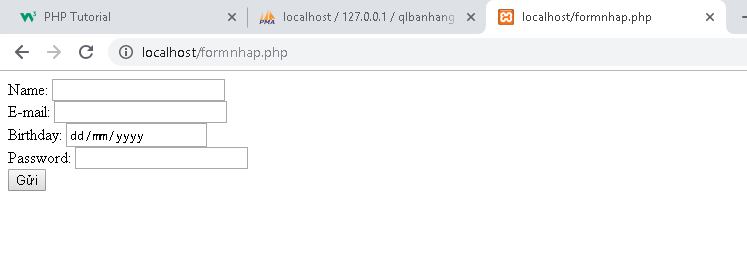
`reg\_date` timestamp NOT NULL DEFAULT current\_timestamp() ON UPDATE current\_timestamp(),

`password` varchar(50) NOT NULL

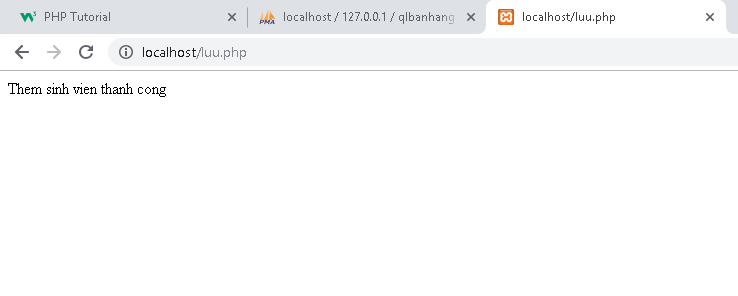
) ENGINE=InnoDB DEFAULT CHARSET=utf8;

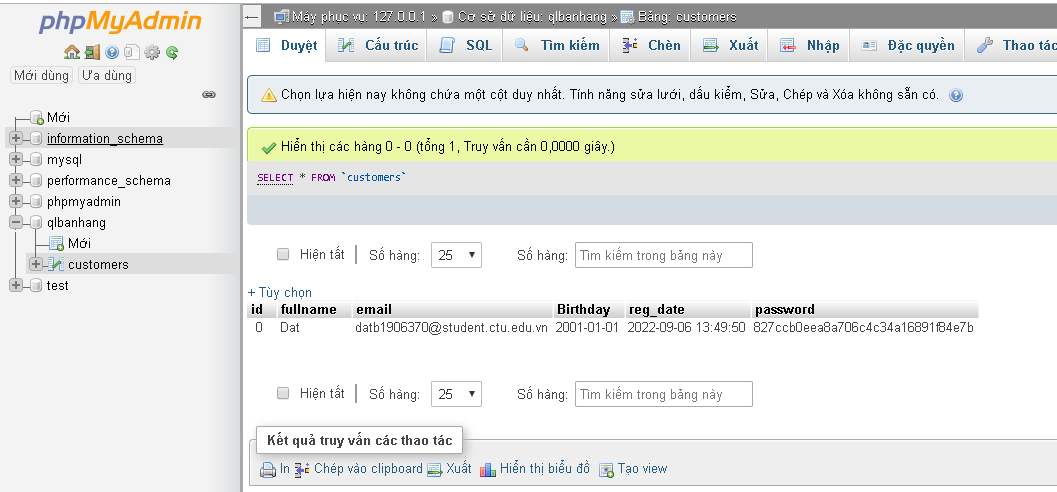


Tạo formnhap.php



### luu.php

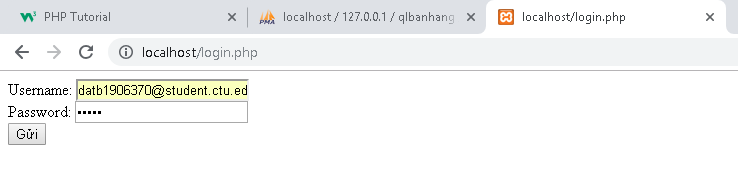




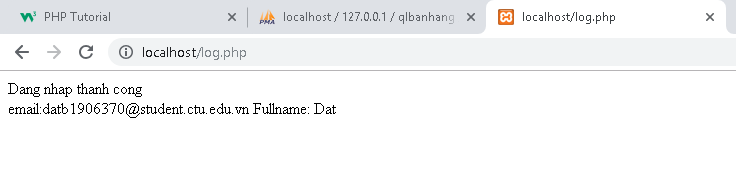
## Tạo form đăng nhập

Sau khi tạo người dùng xong, ta có thể chạy form đăng nhập với username là email và password lấy từ CSDL

### Login.php

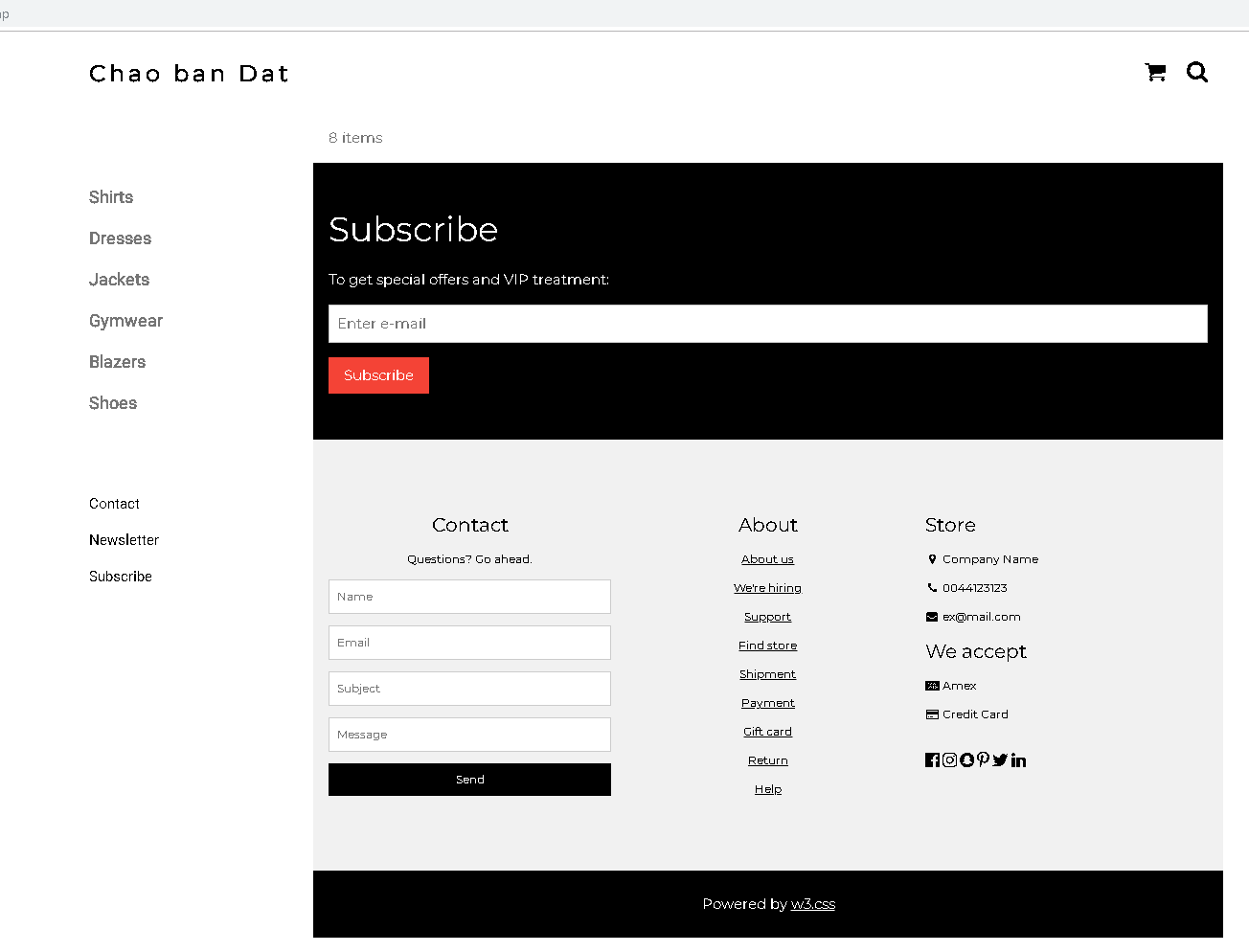


### Log.php



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

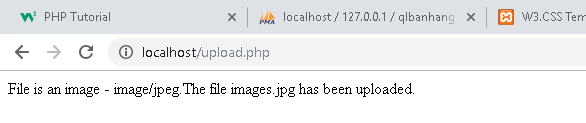
### Homepage.php



## Upload tập tin

Upload file, chúng ta tạo form giao diện để upload file ảnh upload-img.php

### Upload-img.php

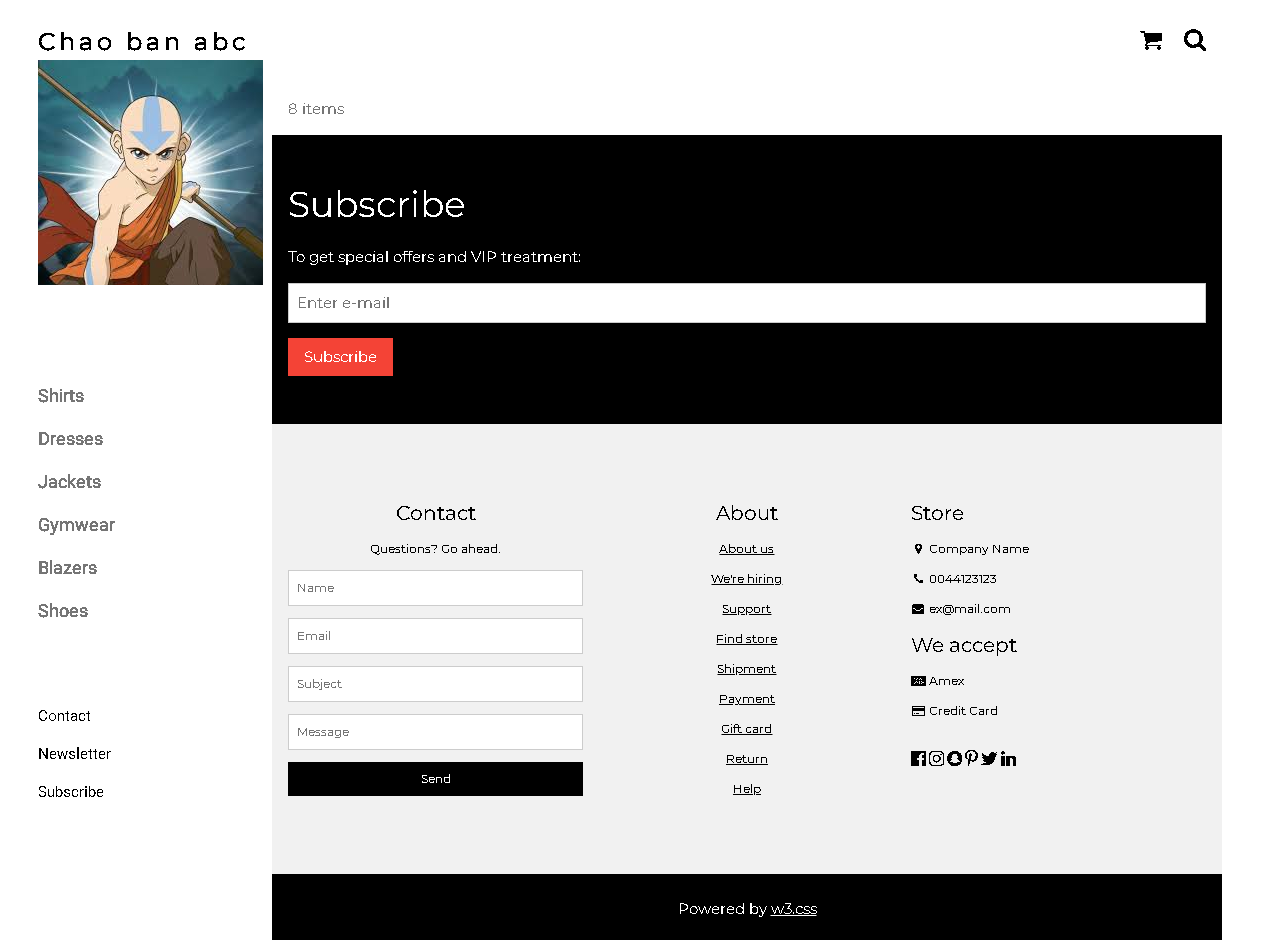


## Upload ảnh và lưu dữ liệu về ảnh trong CSDL

Trong phần này chúng ta minh họa tải tập tin ảnh làm ảnh profile của người dùng

### Upload-img.php (modified)

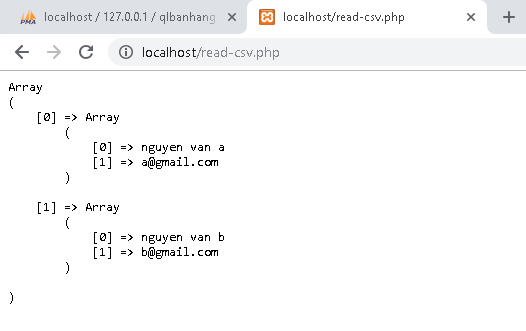
### Homepage.php (modified với ảnh profile)



### Upload file csv và đọc dữ liệu vào mảng

Thao tác đọc dữ liệu từ các tập tin là quan trọng, giúp chúng ta backup dữ liệu và phục hồi hay import dữ liệu từ các hệ thống khác. Ví dụ dưới đây giúp minh họa cho các bạn thao tác đọc dữ liệu từ tập tin csv và từ đó đưa vào mảng để phục vụ cho việc xử lý.

### 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-0). Ứng dụng kỹ thuật đó vào trang đăng nhập mà bạn đã tạo, chụp lại các kết quả.

SQL Injection: là một kỹ thuật lợi dụng những lỗ hổng về câu truy vấn của các ứng dụng. Được thực hiện bằng cách chèn thêm 1 đoạn SQL để làm sai lệnh đi câu truy vấn ban đầu, từ đó có thể khai thác dữ liệu từ database. SQL injection có thể cho phép những kẻ tấn công thực hiện các thao tác như 1 người quản trị web, trên cơ sở dữ liệu của ứng dụng.

1. Dựa vào link[[2]](#footnote-1), 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. Mỗi khi cùng một máy tính yêu cầu một trang có trình duyệt, nó cũng sẽ gửi cookie. Với PHP, bạn có thể vừa tạo và lấy các giá trị cookie.

setcookie($name, $value, $expire, $path, $domain, $security, $httponly);

* name là tên cookie, tên này được sử dụng để truy cập vào biến $\_COOKIE để lấy thông tin
* value gán giá trị cho cookie
* expire là thời điểm hết hạn của cookie, thời gian dạng unix timestamp, có thể dùng hàm time() để lấy unix timestamp. Sau thời điểm này cookie bị hủy lưu trình duyệt. Nếu thiết lập là 0 thì cookie hủy khi đóng trình duyệt.
* path đường dẫn mà cookie hiệu lực.
* domain là tên miền
* security = true nếu sử dụng HTTPS để truyền dữ liệu (mặc định là false)
* httponly mặc định là false, nếu true thì chỉ cho phép cookie với giao thức HTTP

Lưu giá trị

$cookie\_name = “user”;

$cookie\_value = “Dat”

Lấy giá trị:

<?php

$user = $\_COOKIE[‘user’]

echo $user;

?>

Xóa giá trị:

<?php

Setcookie(“user”, “”, time() - 3600);

?>

1. Dựa vào link[[3]](#footnote-2), bạn hãy cho biết Session dùng để làm gì. Cách lưu, lấy, xóa giá trị trong Session.

Session làthông tin về phiên làm việc cho từng khách truy cập, trong PHP nó tạo 1 file trong thư mục tạm để lưu thông tin này, thông tin này được dùng cho tất cả các trang mà khách truy cập. Mỗi khách truy cập dựa vào thông tin trình duyệt gửi lên mà nó tạo hoặc phục hồi 1 session riêng cho khách đó.

Lưu giá trị: sử dụng biến $\_SESSION

<?php

echo "Favorite color is " . $\_SESSION["favcolor"] . ".<br>";

echo "Favorite animal is " . $\_SESSION["favanimal"] . ".";

?>

Xóa giá trị: sử dụng session\_unset() và session\_destroy()

<?php

session\_unset();

session\_destroy();

?>

1. Bạn hãy so sánh Cookie và Session.

|  |  |  |
| --- | --- | --- |
|  | Cookie | Session |
| Vị trí lưu | Lưu trên trình duyệt của client | Lưu trên server |
| Bảo mật | Cookie lưu dưới client nên kém bảo mật hơn | Session lưu trên server nên bảo mật hơn |
| Giới hạn | Lưu có giới hạn | Lưu không giới hạn |

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.
2. 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.
3. Bạn đọc trong[[4]](#footnote-3) để tìm hiểu và mô tả các cơ chế, các hàm/thủ tục để thực hiện việc upload.

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

* Đảm bảo rằng biểu mẫu sử dụng method = "post"
* Biểu mẫu cũng cần thuộc tính sau: enctype = "multiart / form-data". Nó chỉ định loại nội dung sẽ sử dụng khi gửi biểu mẫu
* Nếu không có các yêu cầu ở trên, quá trình tải lên tệp sẽ không hoạt động.
* Thuộc tính type = "file" của thẻ <input> hiển thị trường đầu vào dưới dạng điều khiển chọn tệp, với nút "Duyệt qua" bên cạnh điều khiển đầu vào

Một số câu lệnh php:

* $ 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 tệp chưa được sử dụng (sẽ được sử dụng sau)
* $ uploadOK = 0 tệp đã được sử dụng
* $ imageFileType giữ phần mở rộng tệp của tệp (chữ thường)

Cần tạo một thư mục mới có tên "uploads" trong thư mục chứa tệp "upload.php". Các tệp đã tải lên sẽ được lưu ở đó.

Giới hạn tệp:

* Giới hạn kích thước của tệp: nếu tệp lớn hơn kích thước đã cho, thông báo lỗi và đặt $ uploadOK = 0

if ($\_FILES["fileToUpload"]["size"] > 500000) {

echo "Sorry, your file is too large.";

$uploadOk = 0;

}

* Giới hạn loại tệp: nếu upload tệp loại ngoài các loại đã cho thì báo lỗi và đặt $ uploadOK = 0

if($imageFileType != "jpg" && $imageFileType != "png" && $imageFileType != "jpeg" && $imageFileType != "gif" ) {

echo "Sorry, only JPG, JPEG, PNG & GIF files are allowed.";

$uploadOk = 0;

}

1. Bạn hãy đọc[[5]](#footnote-4), mô tả chức năng của hàm này và các tham số trong hàm (tham khảo thêm từ read-csv.php).

Chức năng hàm file() là đọc 1 tệp thành 1 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 đường dẫn đến tệp để đọc

flag: không bắt buộc, là các hằng số sau:

* FILE\_USE\_INCLUDE\_PATH - Tìm kiếm tệp trong đường dẫn bao gồm (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: Không bắt buộc. Chỉ định ngữ cảnh của xử lý tệp. Ngữ cảnh là một tập hợp các tùy chọn có thể sửa đổi hành vi của một luồng. Có thể được bỏ qua bằng cách sử dụng NULL.

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-5),[[7]](#footnote-6). 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.

1. <https://www.w3schools.com/sql/sql_injection.asp> [↑](#footnote-ref-0)
2. <https://www.w3schools.com/php/php_cookies.asp> [↑](#footnote-ref-1)
3. <https://www.w3schools.com/php/php_sessions.asp> [↑](#footnote-ref-2)
4. <https://www.w3schools.com/php/php_file_upload.asp> [↑](#footnote-ref-3)
5. <https://www.w3schools.com/php/func_filesystem_file.asp> [↑](#footnote-ref-4)
6. <https://www.php.net/manual/en/features.file-upload.post-method.php>, [↑](#footnote-ref-5)
7. https://stackoverflow.com/questions/6654351/check-file-uploaded-is-in-csv-format [↑](#footnote-ref-6)