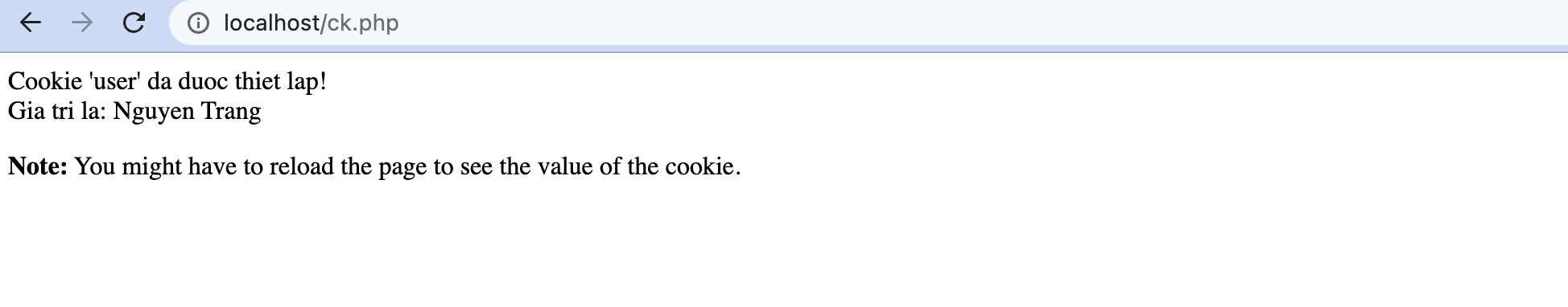
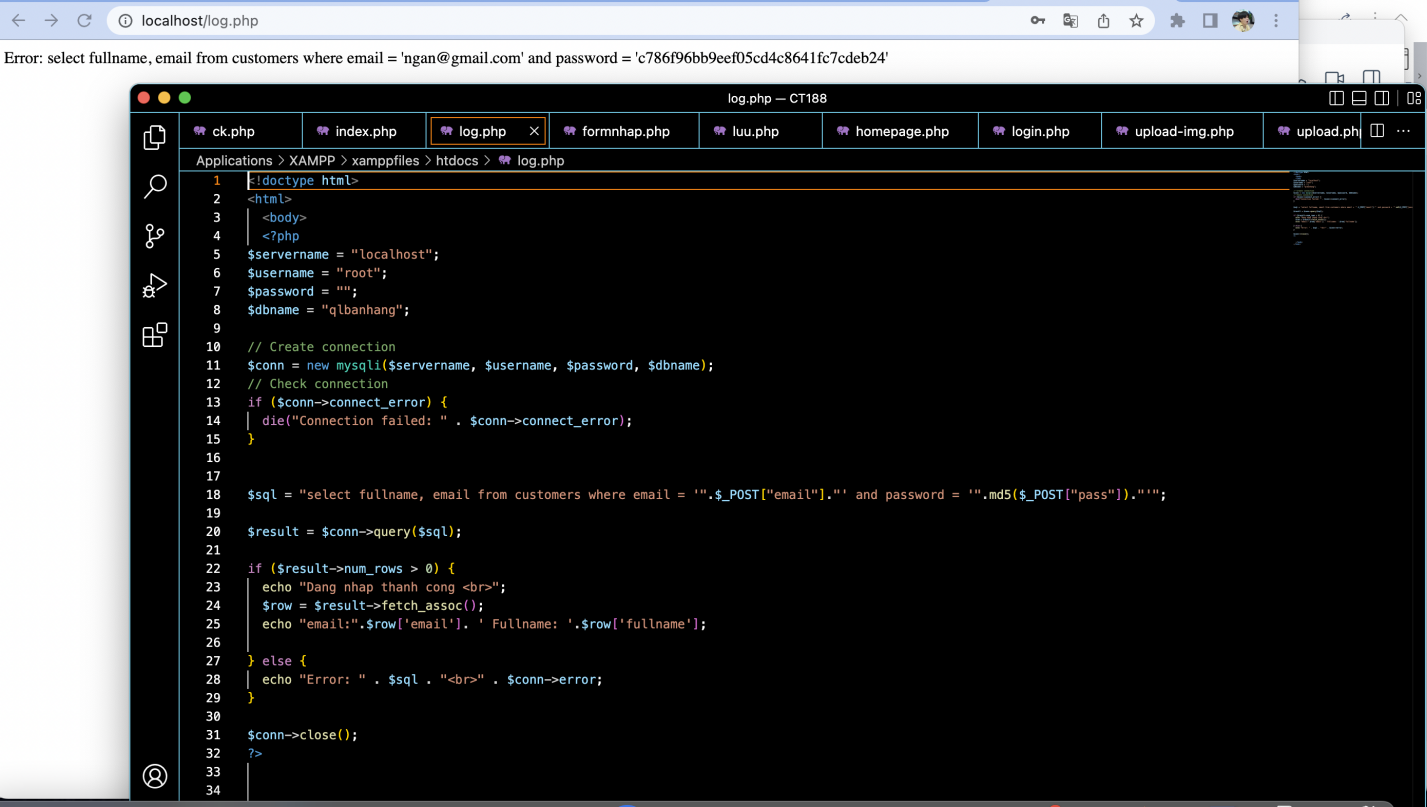
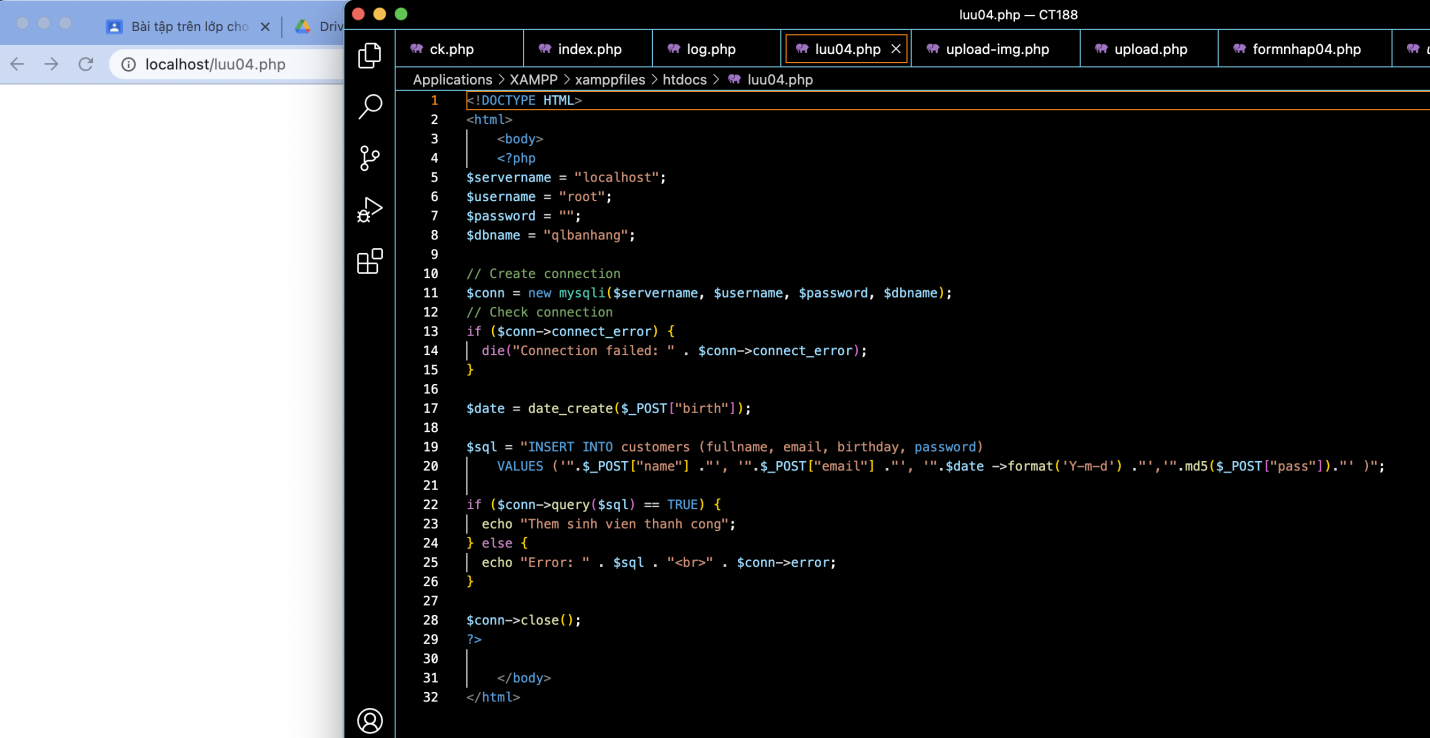
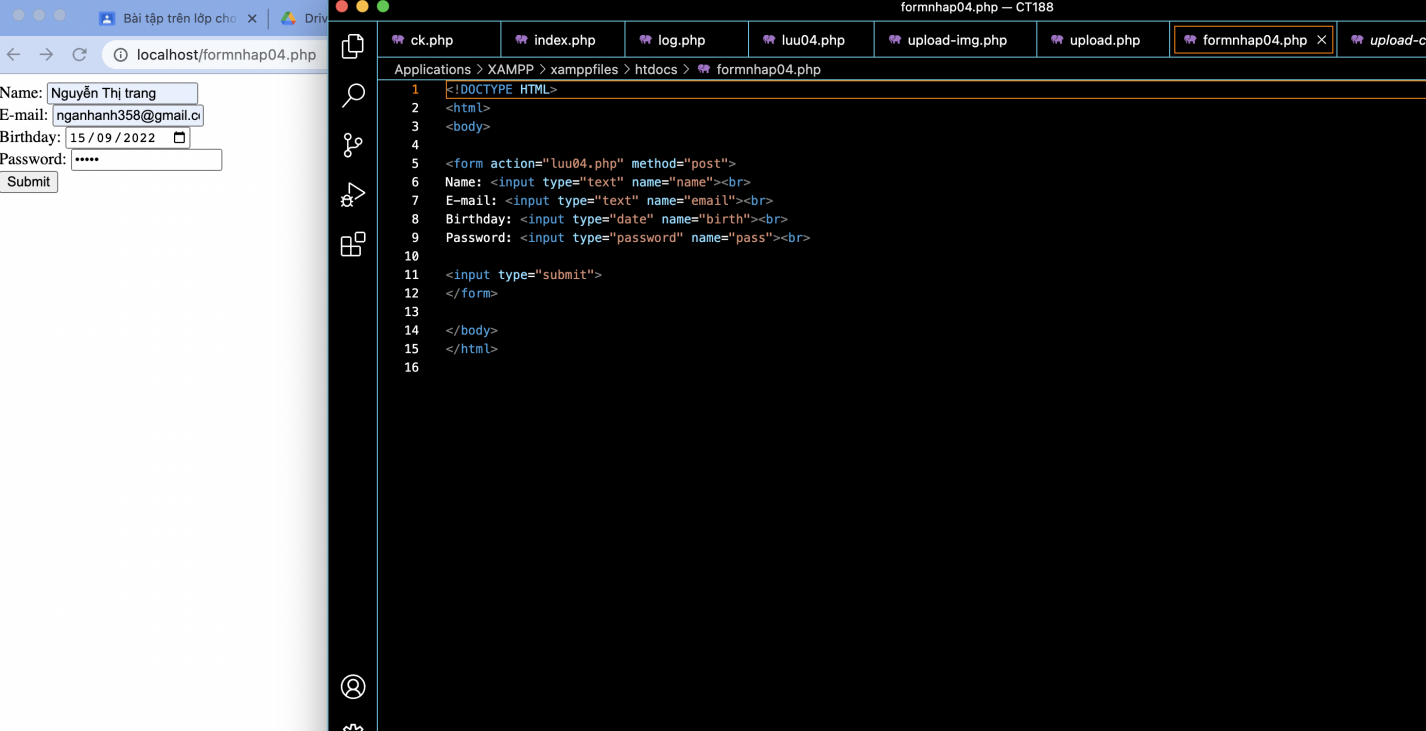
**Bài tập thực hành 04**

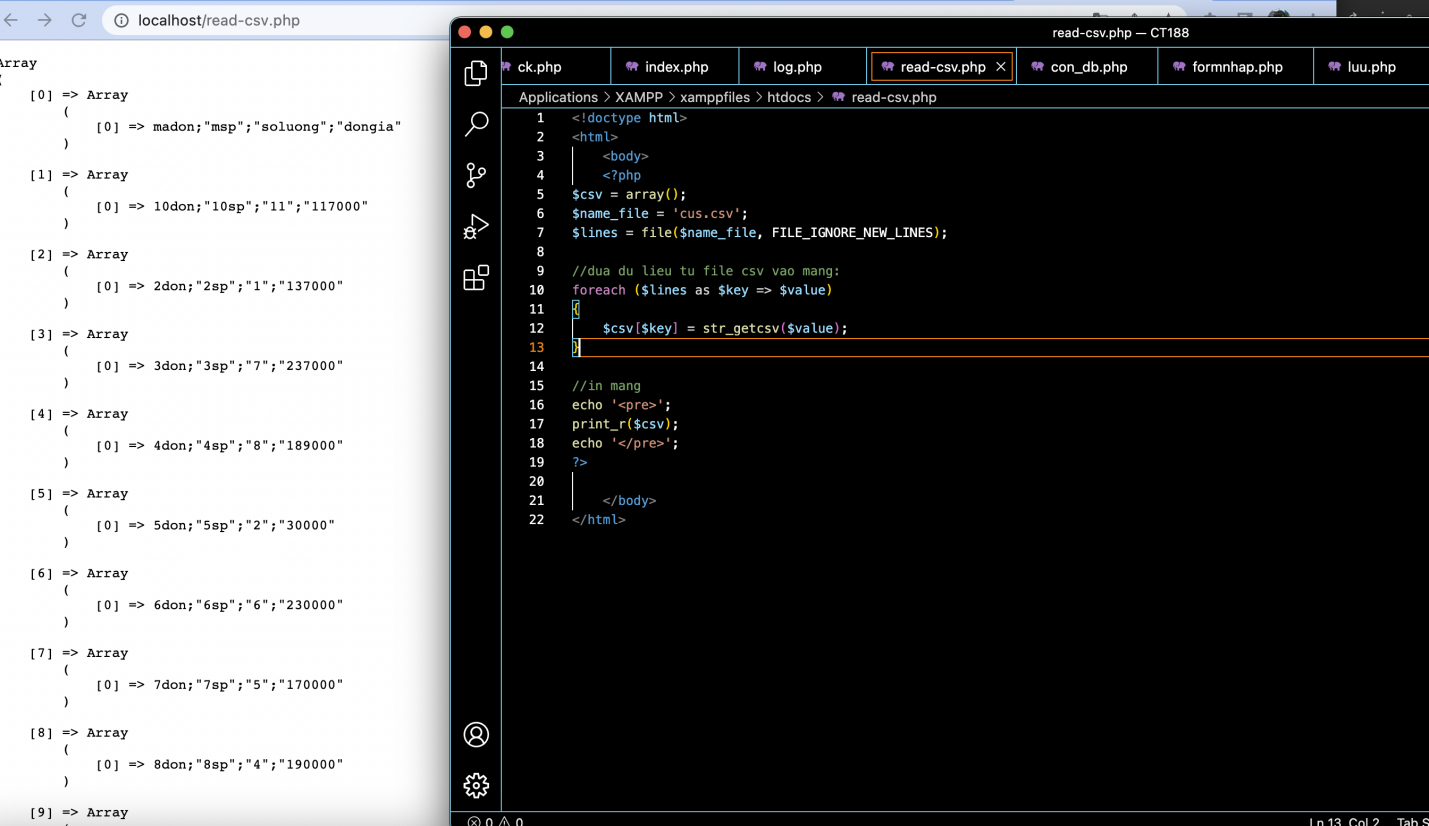
**Lập trình PHP nâng cao**

# Yêu cầu bài thực hành:

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

****

****

****

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 chèn mã có thể phá hủy cơ sở dữ liệu của bạn, là một trong những kỹ thuật hack web phổ biến nhất.

Ví dụ:

## SQL Injection dựa trên 1 = 1 luôn đúng

Mục đích ban đầu của mã là tạo một câu lệnh SQL để chọn một người dùng, với một id người dùng nhất định.

Nếu không có gì ngăn người dùng nhập "sai" đầu vào, người dùng có thể nhập một số đầu vào "thông minh" như sau:

Tên người dùng:105 OR 1=1

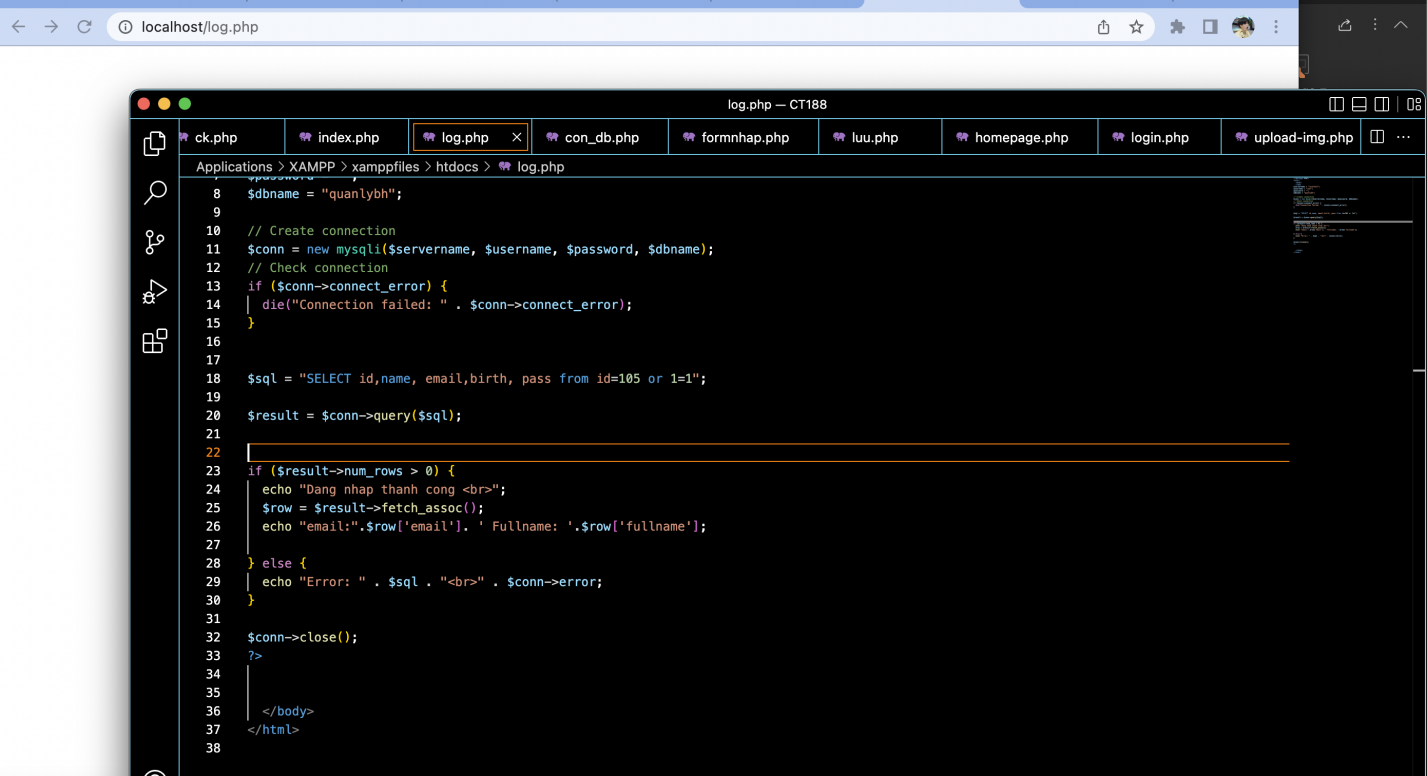
Sau đó, câu lệnh SQL sẽ giống như sau:

SELECT \* FROM Users WHERE UserId = 105 OR 1=1;

SQL ở trên là hợp lệ và sẽ trả về TẤT CẢ các hàng từ bảng "Người dùng", vì ****OR 1 = 1**** luôn là TRUE.

SELECT UserId, Name, Password FROM Users WHERE UserId = 105 or 1=1;

Một tin tặc có thể có quyền truy cập vào tất cả tên người dùng và mật khẩu trong cơ sở dữ liệu, bằng cách chỉ cần chèn 105 OR 1 = 1 vào trường đầu vào.



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, secure, httponly*);

Name: tên của coolie

Value: giá trị của cookie, được lưu trữ trên máy khách

*Expire: thời gian cookie hết*

*Path: đường dẫn trên máy chủ mà cookie sẽ có sẵn*

*Domain: miền phụ mà cookie có sẵn(có hiệu lực)*

*Secure: cho biết cookie chỉ nên được truyền qqua kết nối https an toàn từ máy khách*

*Httponly: khi truecookie sẽ được thực hiện chỉcos thể truy câp thông qua giao thức*

Chỉ tham số *tên* là bắt buộc. Tất cả các thông số khác là tùy chọn.

Lấy giá trị cookie: Biến toàn cục $\_COOKIE là nơi lưu thông tin của COOKIE.Dựa theo tên của cookie để truy xuất và lấy giá trị.

Sửa giá trị cookie: chỉ cần đặt (lại) cookie bằng setcookie()

Xoá giá trị cookie: ta cập nhật thời gian sống bằng một thời gian trong quá khứ

<http://hocweb123.com/huong-dan-lam-viec-voi-cookie-trong-php.html>

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

Sessoion là một cách để lưu trữ thông tin (trong các biến) được sử dụng trên nhiều trang.

Lưu giá trị session: $\_SESSION[‘session\_name]=$sesion\_value

Xoá giá trị session: sử dụng hàm unset($bien)

Lấy giá trị sesion: $bien=$\_SESSION[‘session\_name’]

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

|  |  |
| --- | --- |
| **Cookie** | **Session** |
| Cookie được lưu trữ trên trình duyệt của người dùng. | Session không được lưu trữ trong trình duyệt của người dùng. |
| Dữ liệu cookie được lưu trữ ở phía máy khách. | Dữ liệu session được lưu trữ ở phía máy chủ. |
| 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. |
| 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. |

<https://viblo.asia/p/cookie-va-session-07LKXEvEZV4>

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.**

Trong tệp "php.ini" của bạn, hãy tìm kiếm lệnh file\_uploadsvà đặt nó thành Bật:

file\_uploads = On

Sau đó tạo một biểu mẫu HTML cho phép người dùng chọn tệp hình ảnh mà họ muốn tải lên. 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

Biểu mẫu ở trên gửi dữ liệu đến một tệp có tên "upload.php". và có một số mục sau:

* $ 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 tệp của tệp (chữ thường)
* Tiếp theo, hãy kiểm tra xem file ảnh là ảnh thật hay ảnh giả

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.

// Check if file already exists  
if (file\_exists($target\_file)) {  
  echo "Sorry, file already exists.";  
  $uploadOk = 0;  
}

## Giới hạn kích thước tệp

// Check file size  
if ($\_FILES["fileToUpload"]["size"] > 500000) {  
  echo "Sorry, your file is too large.";  
  $uploadOk = 0;  
}

## Giới hạn loại tệp

// Allow certain file formats  
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).**

file(filename,flag,context)

Trong đó:

Filename: tên tệp cần đọc

Flag: là tham số không bắt buộc, mang một trong các giá trị sau:

FILE\_USE\_INCLUDE\_PATH : tìm kiếm file trong [include\_path](https://freetuts.net/ham-file-trong-php-4800.html" \o " " \t "/Users/trang/Documents\\x/_blank).

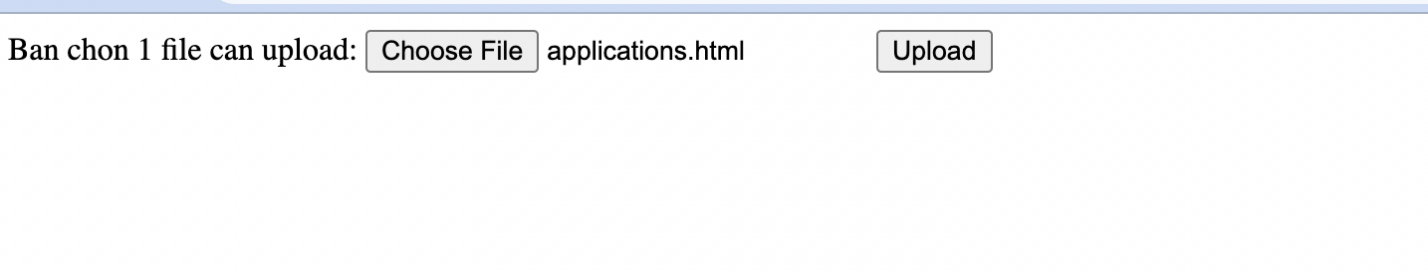
FILE\_IGNORE\_NEW\_LINES : không thêm dòng mới vào cuối mỗi phần tử của mảng.

FILE\_SKIP\_EMPTY\_LINES : bỏ qua những dòngtrống.

Context: không bắt buộc,định nghĩa ngử cảnh xử lý tệp, có thể bỏ qua hoặc null.

Chức năng: đọc một tệp thành mảng

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)