**Bài tập thực hành 04**

MSSV: B1906361

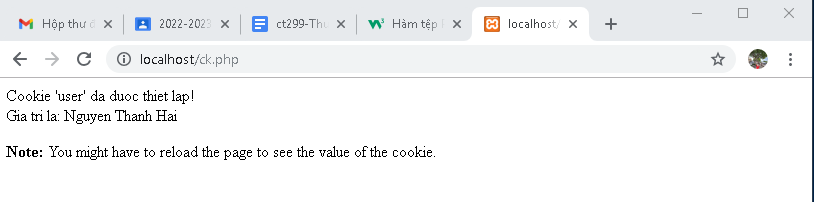
Họ & tên: Hồ Thị Như Ý

Lập trình PHP nâng cao

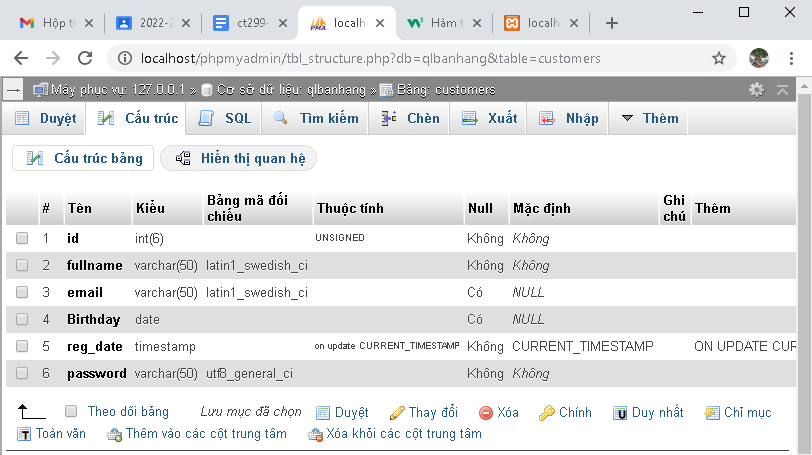
Yêu cầu bài thực hành:

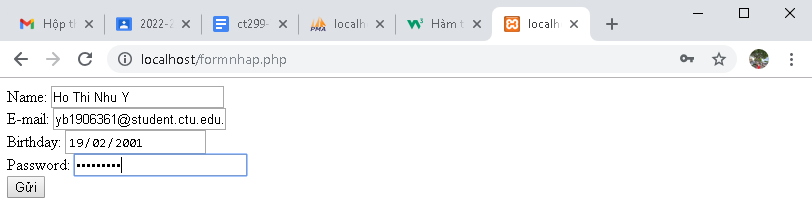
1. Bạn hãy chạy tất cả các lệnh hướng dẫn ở trên và chụp lại màn hình kết quả.

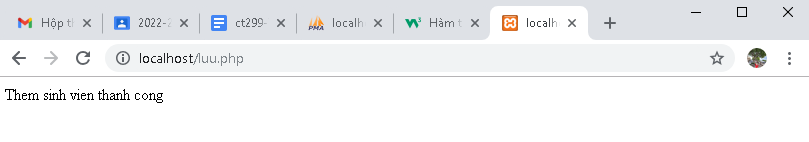
* **Tạo Cookies**

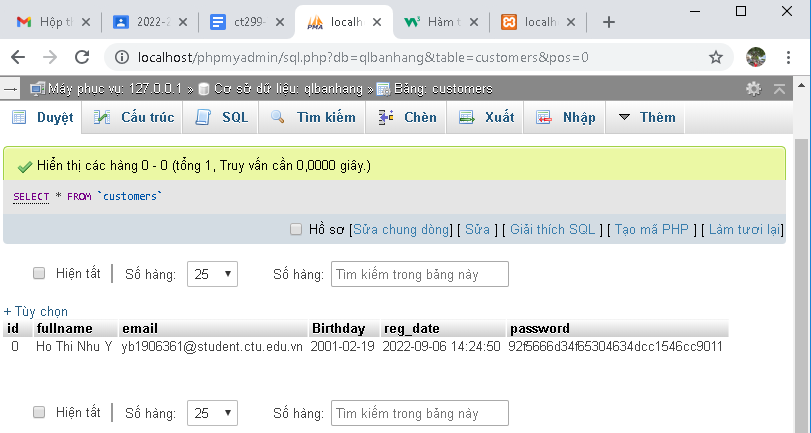


* **Tạo 1 trang đăng ký người dùng với mật khẩu được mã hóa**

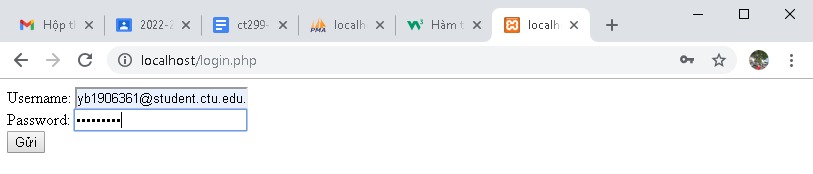


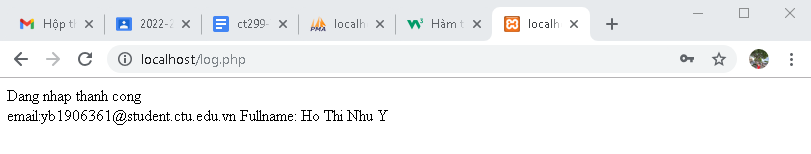




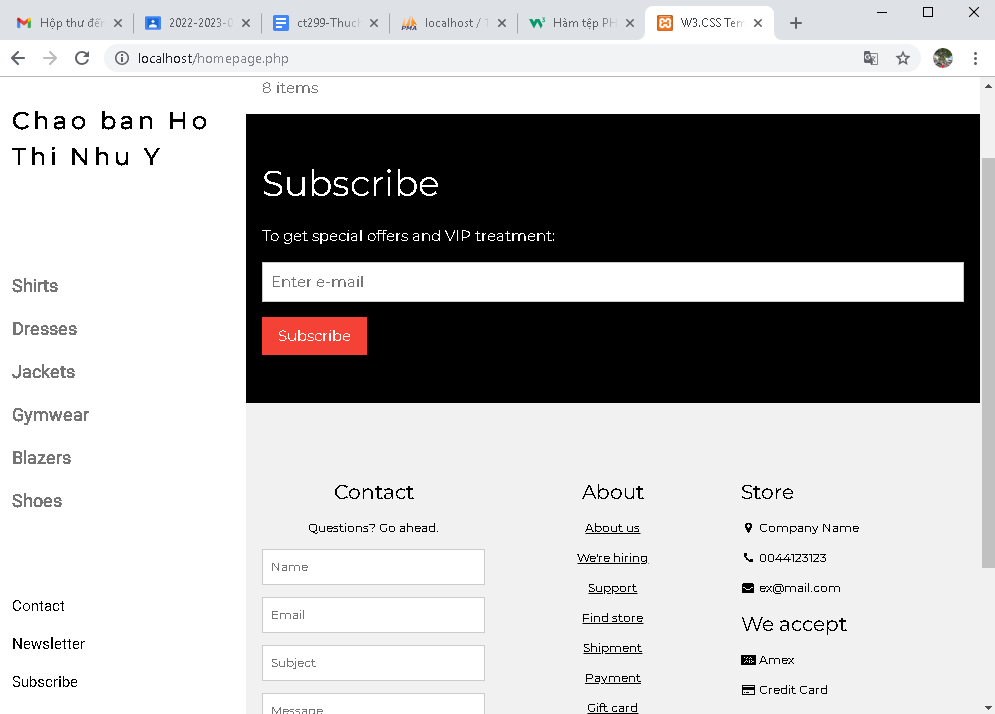


* **Tạo form đăng nhập**

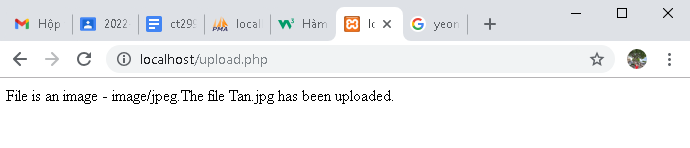




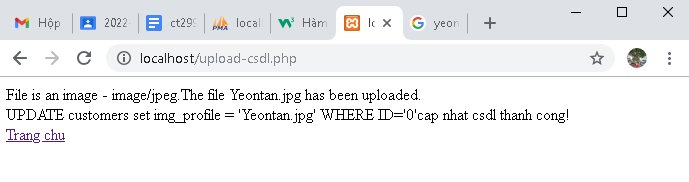
* **Dùng Cookies lưu lại tên đăng nhập, email và điều hướng**

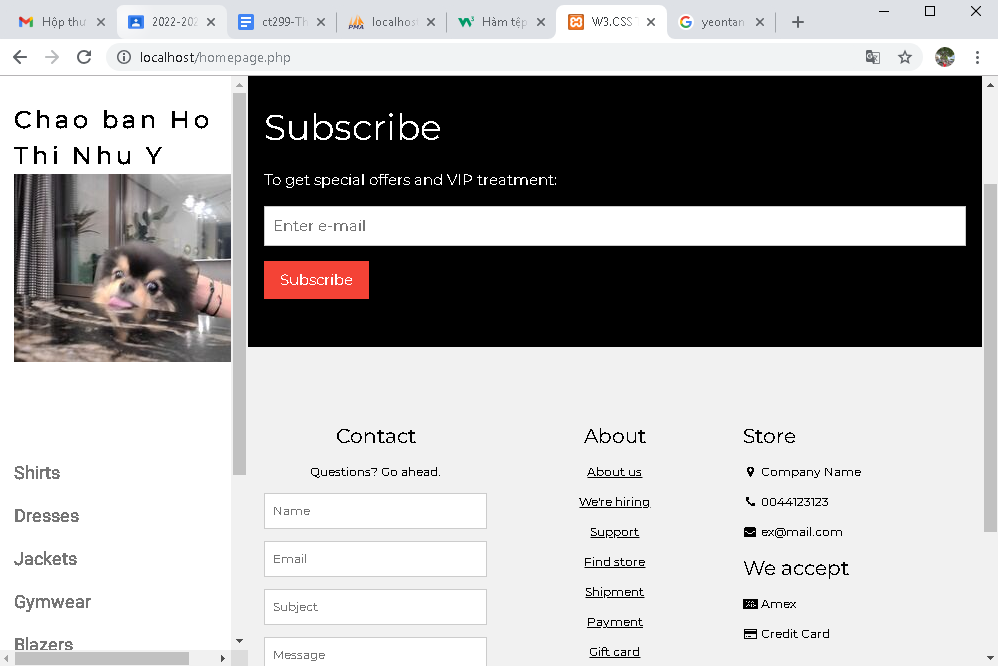


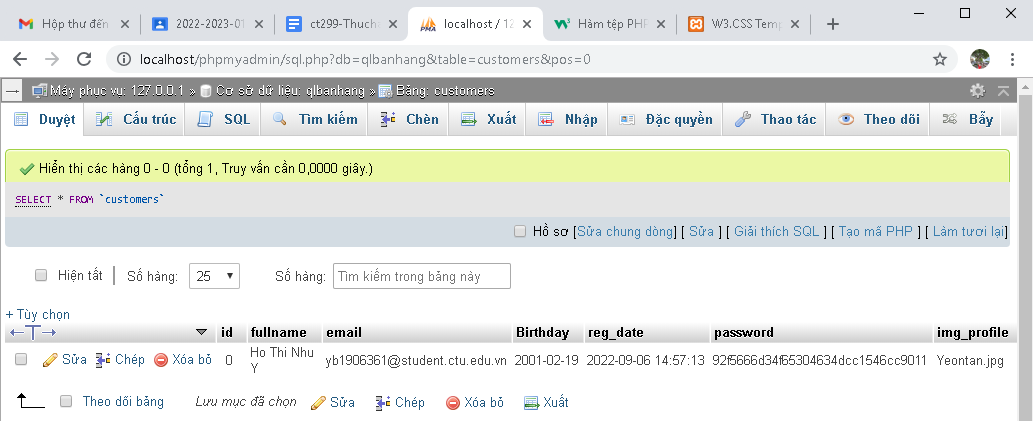
* **Upload tập tin**



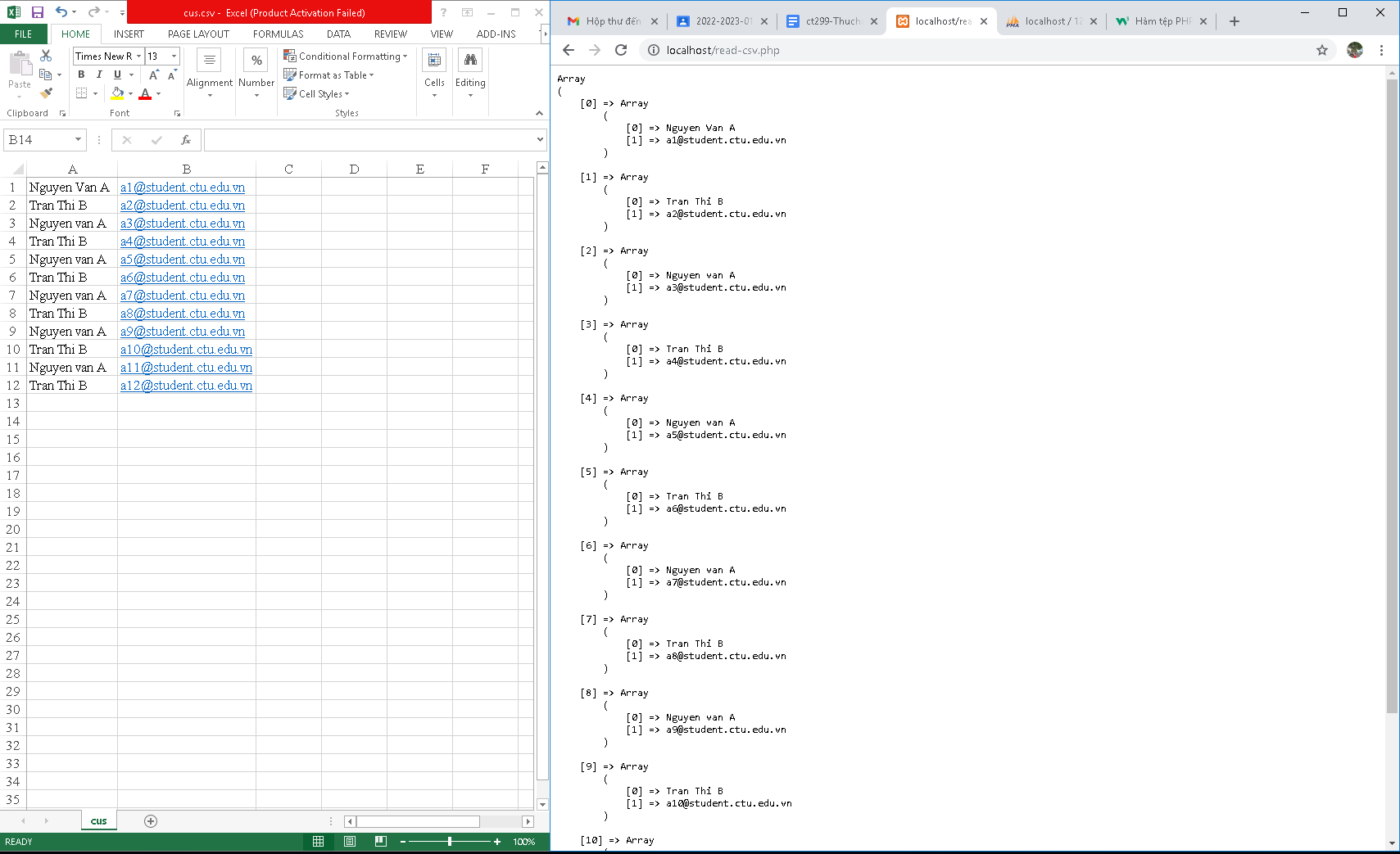
* **Upload ảnh và lưu dữ liệu về ảnh trong CSDL**







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



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 chèn mã có thể phá hủy cơ sở dữ liệu của bạn, là một trong những kỹ thuật hack web phổ biến nhất, là vị trí của mã độc hại trong các câu lệnh SQL, thông qua đầu vào trang web.

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.

( <https://xuanthulab.net/su-dung-session-va-cookie-trong-php.html#luu-sookie> ).

* Cookie là một tệp nhỏ được lưu ở máy tính của người dùng (cụ thể là tại Browser, trình duyệt) để theo dõi, lưu lại hoạt động truy cập.
* Các tham số trong setcookie():
* name: tên của cookie, đây là tham số bắt buộc. Tên này được sử dụng để truy cập vào biến $\_COOKIE để lấy thông tin.
* value: giá trị gán cho cookie.
* expire: Thời điểm hết hạn (hủy) của cookie, thời gian dạng Unix timestamp. Sau thời gian này cookie bị hủy lưu tại trình duyệt. Nếu thiết lập là 0 thì cookie hủy khi đóng trình duyệt.
* path: chỉ định đường dẫn trên máy chủ mà cookie sẽ có hiệu lực. Nếu được đặt thành / , cookie sẽ có sẵn trong toàn bộ domain, nếu thiết lập là /foo/ thì cookie chỉ có hiệu lực với các URL dạng /foo/ và các con của nó như /foo/abc/… Nếu để giá trị mặc định thì có hiệu lực theo đường dẫn hiện tại.
* domain: chỉ định tên miền mà cookie có hiệu lực.
* 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.
* Cách lưu cookie:

<?php

setcookie(“name”, “THU”, time() + 600, “/”);

echo “Set cookie”;

?>

Đoạn mã trên lưu Cookie với tên là name, giá trị là THU, hết hạn sau 600 giây.

* Cách lấy cookie: sử dụng biến toàn cục $\_COOKIE để truy xuất giá trị của cookie. ( vd: echo $\_COOKIE[“username”]; )
* Cách xóa cookie: sử dụng setcookie() với thủ thuật đặt thời gian đã hết hạn. (vd: setcookie( “name”, “”, time()- 60, “/”, “”, 0); ).

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

( <https://xuanthulab.net/su-dung-session-va-cookie-trong-php.html#luu-sookie> ).

* Session dùng để lưu trữ thông tin người dùng (trong các biến) để sử dụng trên nhiều trang.
* Cách lưu và lấy giá trị trong Session: biến toàn cục $\_SESSION: kiểu mảng là nơi Session lưu trữ thông tin – cũng là dữ liệu phục hồi được giữa các trang, truy cập biến này trong suốt vòng đời của Session để lấy, lưu trữ thông tin.
* Cách xóa giá trị trong Session: sử dụng lệnh unset() để hủy một biến và sử dụng lệnh session\_destroy() để hủy toàn bộ Session.

1. Bạn hãy so sánh Cookie và Session.

( <https://khacnhaugiua.vn/session-va-cookie-khac-nhau-nhu-the-nao/> ).

* Cookie: được lưu trữ trên máy tính của người dùng. Dữ liệu Cookie có sẵn trong trình duyệt của người dùng khi hết hạn.
* Session: thông tin không được lưu trữ trên máy tính của người dùng. Dữ liệu Session có sẵn cho trình duyệt chạy, sau khi đóng trình duyệt sẽ mất thông tin Session.

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-4) để tìm hiểu và mô tả các cơ chế, các hàm/thủ tục để thực hiện việc upload.

* Cơ chế để thực hiện việc upload:
* Định cấu hình tệp “php.ini”: trong tệp “php.ini”, tìm kiếm lệnh file\_uploads và đặt thành Bật: file\_uploads = On
* Tạo biểu mẫu HTML để cho phép người dùng chọn tệp hình ảnh muốn tải lên:
* Đảm bảo biểu mẫu sử dụng method=”post”
* Biểu mẫu cần thuộc tính: enctype = “multiart/form-data”. Nó chỉ định loại nội dung sẽ sử dụng khi gửi biểu mẫu.

<!DOCTYPE html>  
<html>  
<body>  
  
<form action="upload.php" method="post" enctype="multipart/form-data">  
  Select image to upload:  
  <input type="file" name="fileToUpload" id="fileToUpload">  
  <input type="submit" value="Upload Image" name="submit">  
</form>  
  
</body>  
</html>

* Tạo tập lệnh PHP tải lên
* Kiểm tra xem tệp đã tồn tại chưa

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

* Giới hạn kích thước tệp: nếu tệp lớn hơn 500KB, hiển thị thông báo lỗi.

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

* Giới hạn loại tệp: đoạn mã này chỉ cho phép tải lên các tệp JPG, JPEG, PNG và GIF.

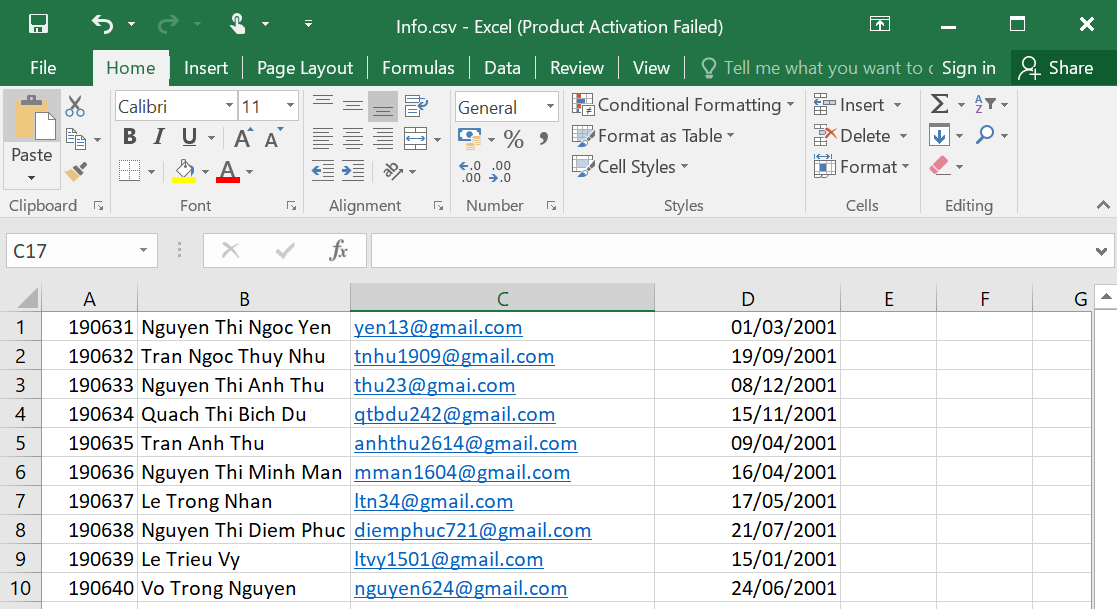
// Allow certain file formats  
if($imageFileType != "jpg" && $imageFileType != "png" && $imageFileType != "jpeg"  
&& $imageFileType != "gif" ) {  
  echo "Sorry, only JPG, JPEG, PNG & GIF files are allowed.";  
  $uploadOk = 0;  
}

* Hoàn thành tải lên tập tin PHP Script.

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() đọc một tệp thành một mảng, mỗi phần tử mảng chứa một dòng từ tệp.
* Các tham số trong hàm:
* filename: tên tệp, đây là tham số bắt buộc. Chỉ định đường dẫn đến tệp để đọc.
* flag: cờ, tham số tùy chọn. Có thể là một hoặc nhiều hằng số sau:
* 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: ngữ cảnh, tham số tùy chọn. 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-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.

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)