**Bài tập thực hành 04**

**B2003785  
Đinh Thái Hợp**

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.

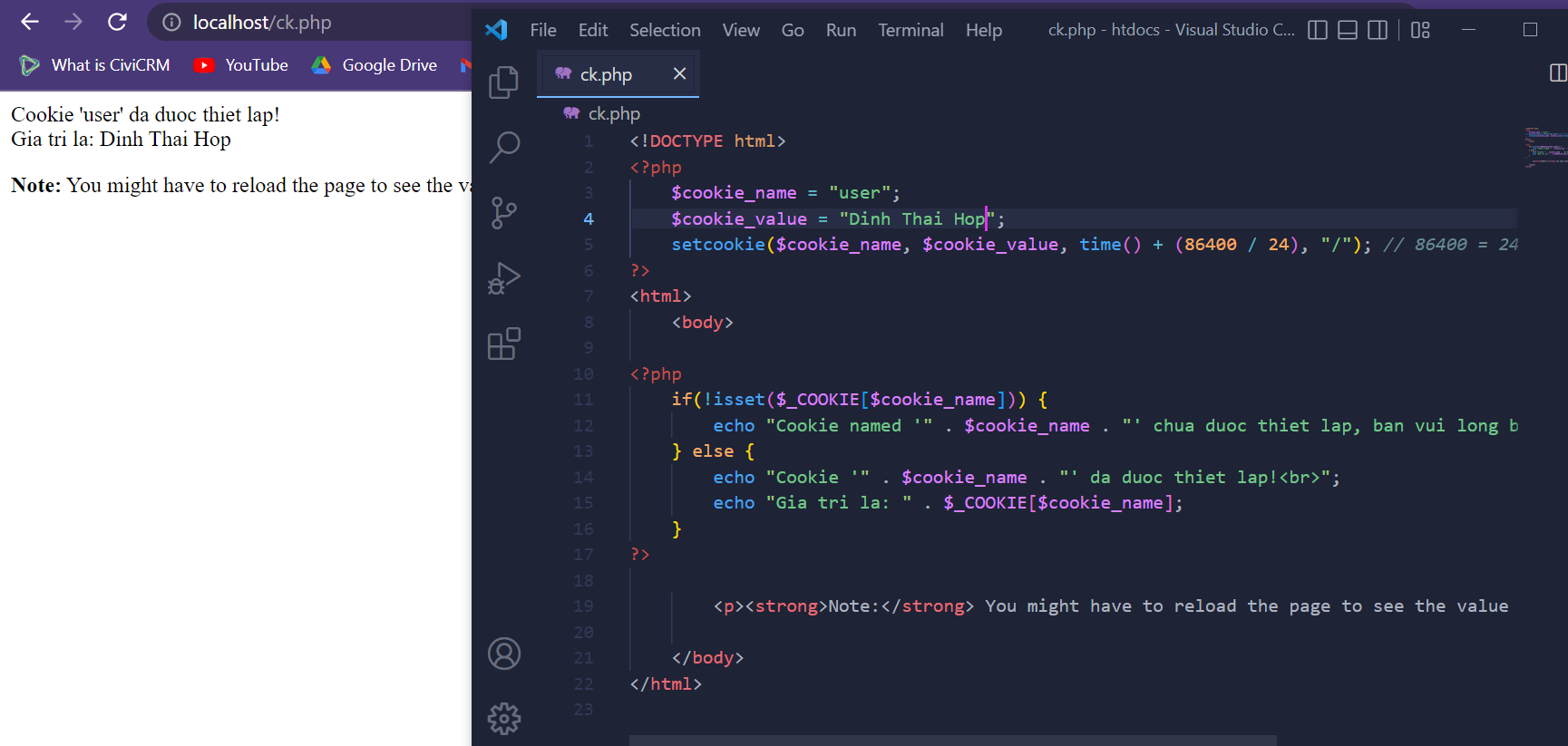
**Gợi ý Tham khảo:**

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

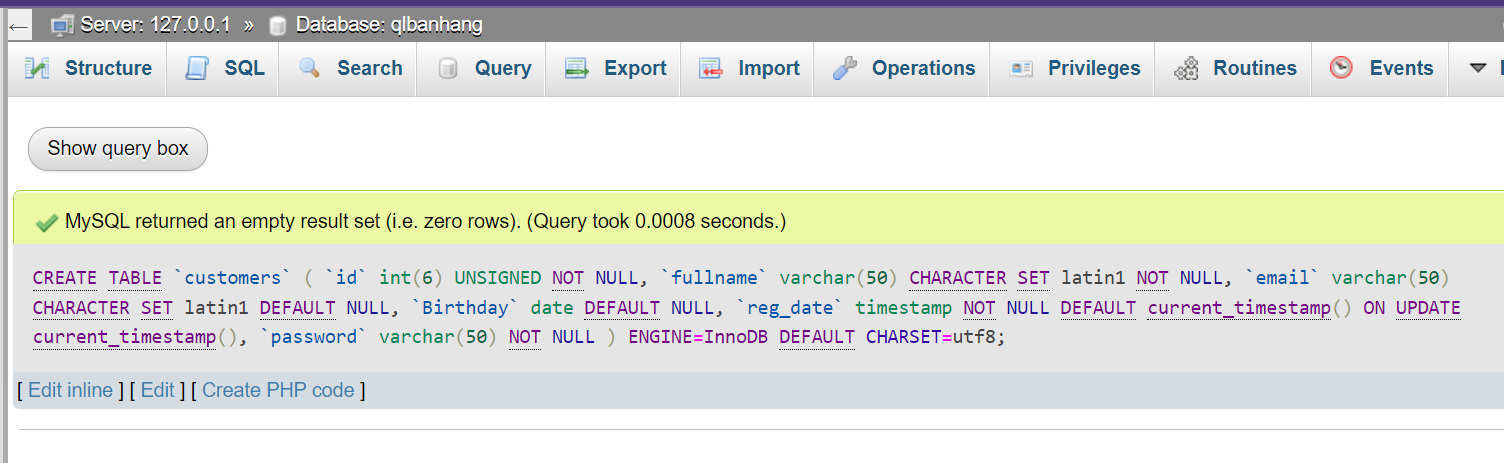
Yêu cầu bài thực hành:

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

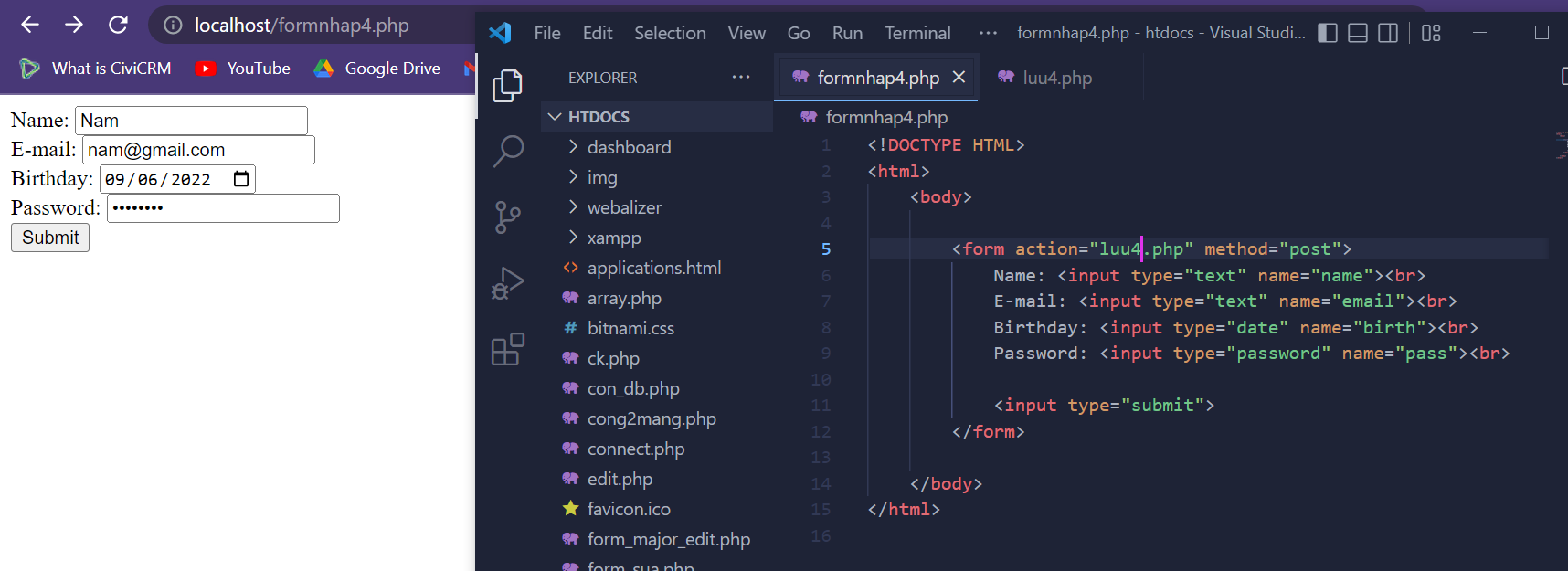
Ck.php



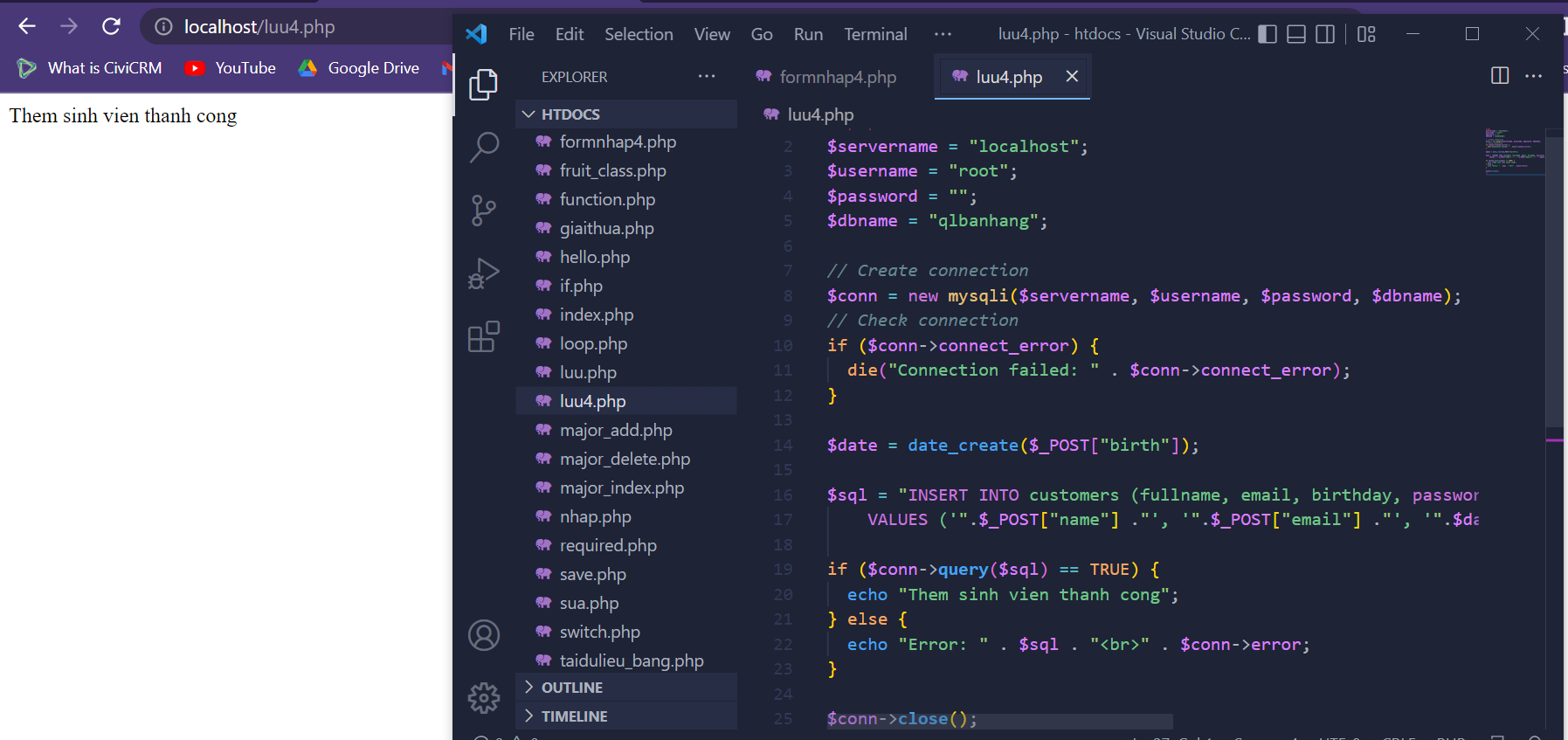
Csdl qlbanhang, với bảng customers



Formnhap4.php



Luu4.php



Trong trường hợp chúng ta muốn dùng email là username để đăng nhập ta nên đảm bảo 2 student không có email trùng nhau. Để đảm bảo điều này ta có thể chọn email là unique key (vì ta đã chọn id la primary key, và 1 bảng không thể có 2 khóa chính)

Graphical user interface, application, Word

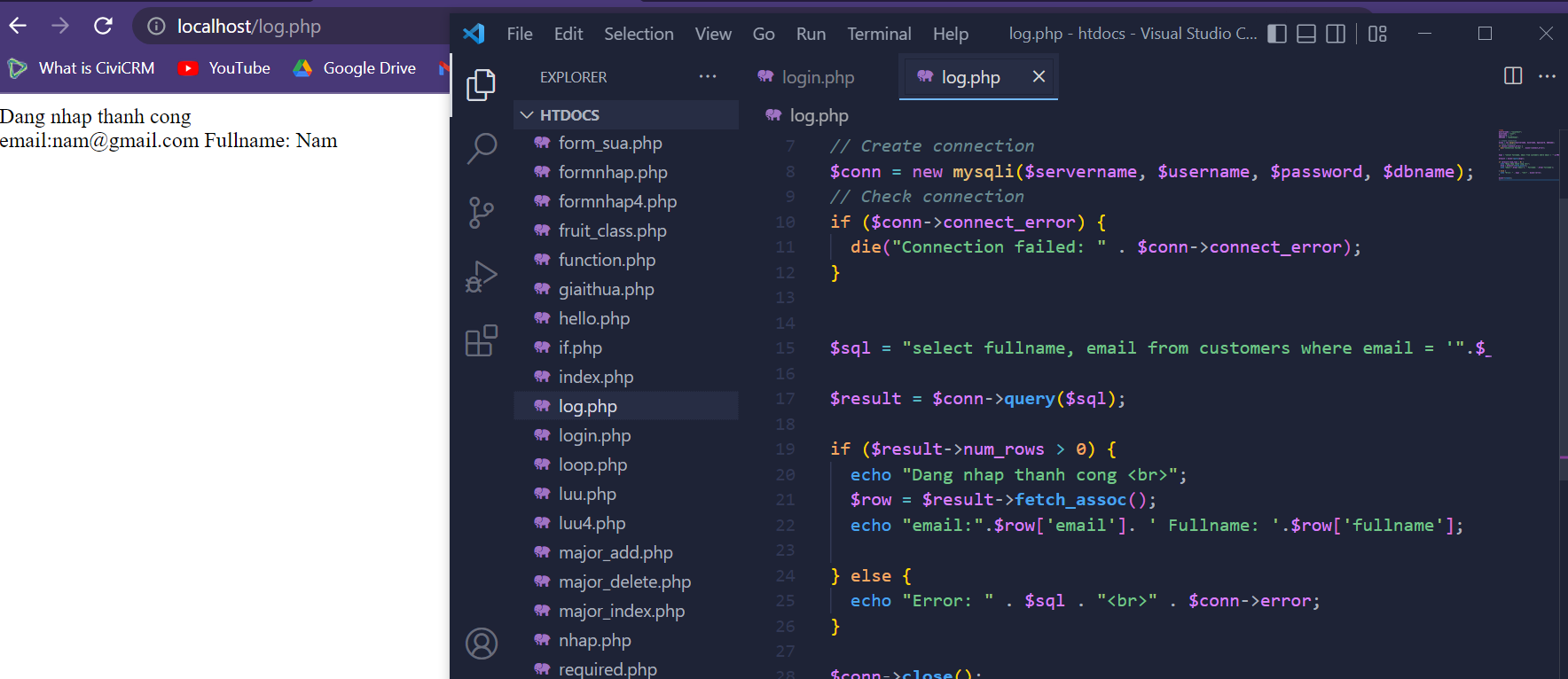
Description automatically generated

Login.php

Text

Description automatically generated

Log.php

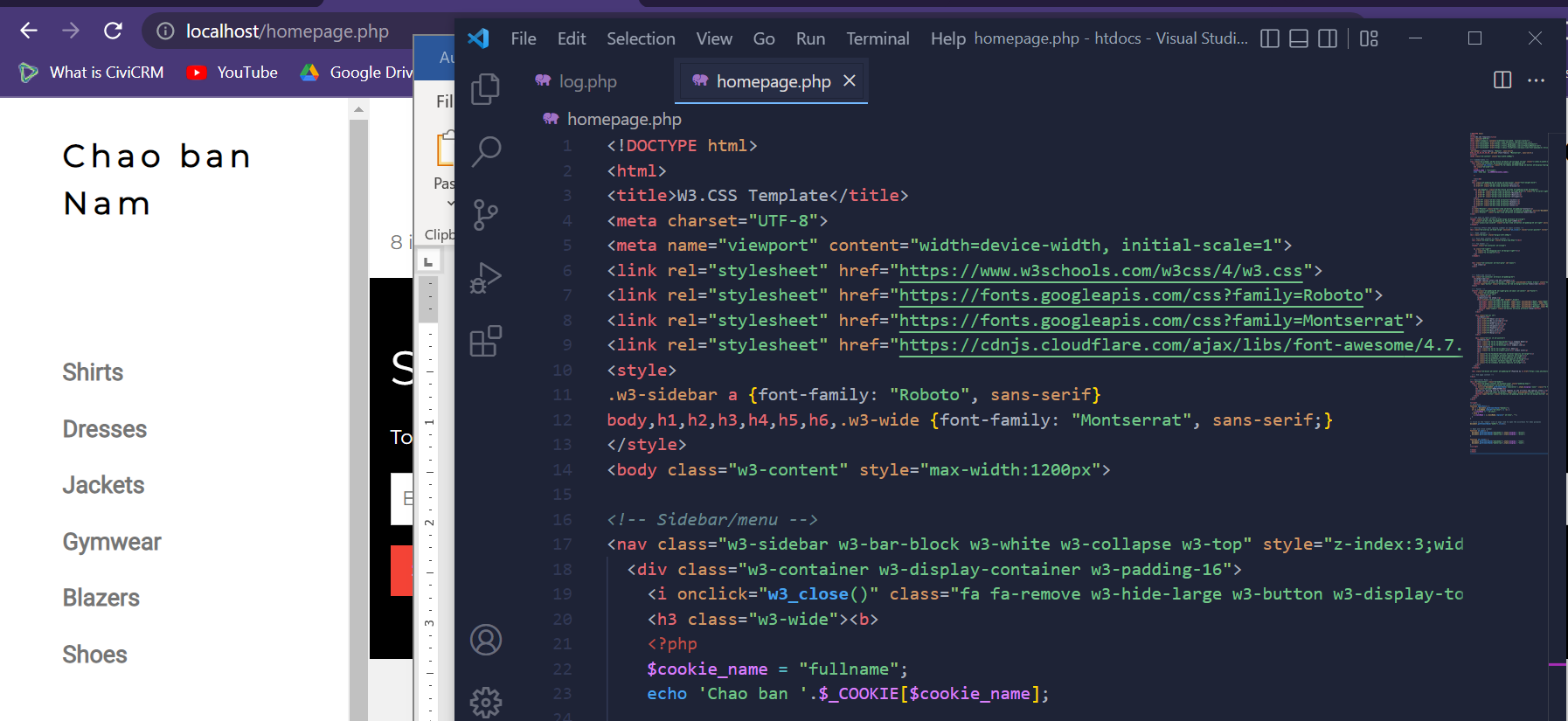


Log.php update

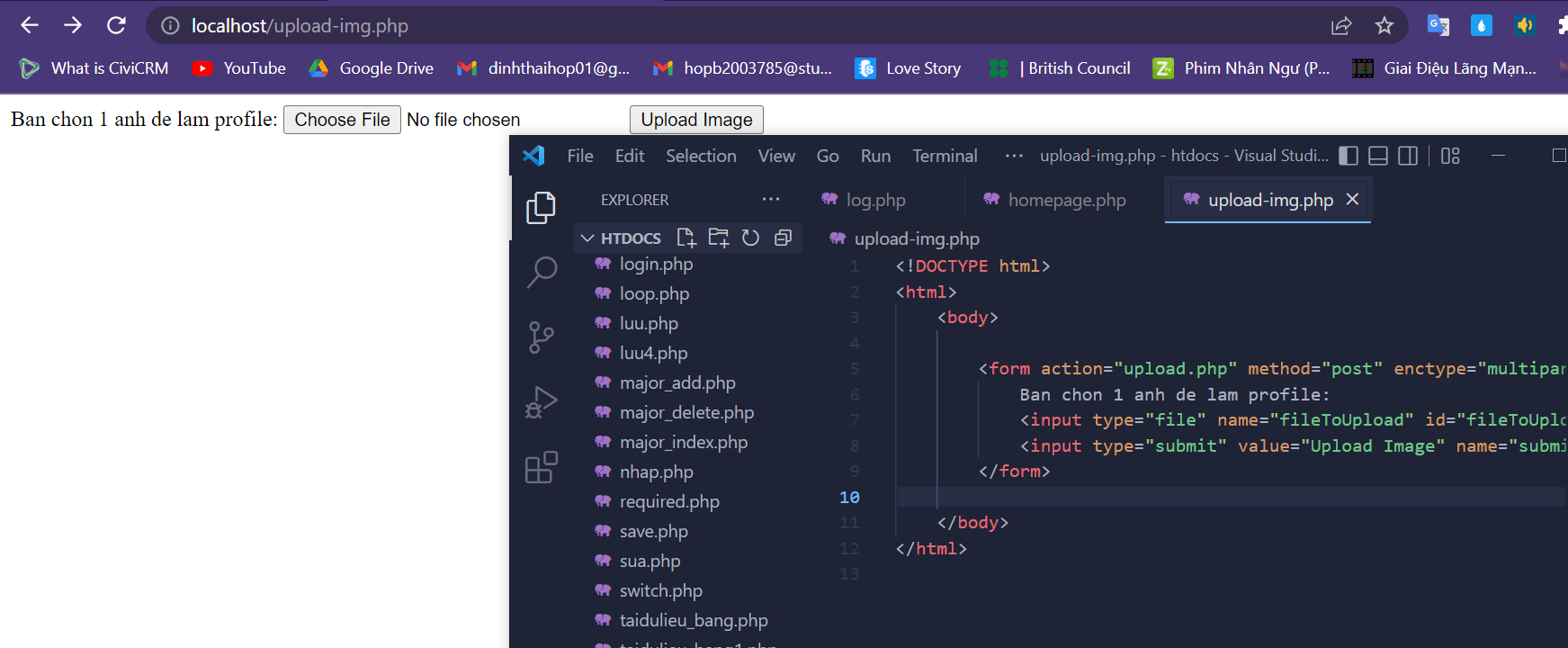
Text

Description automatically generated

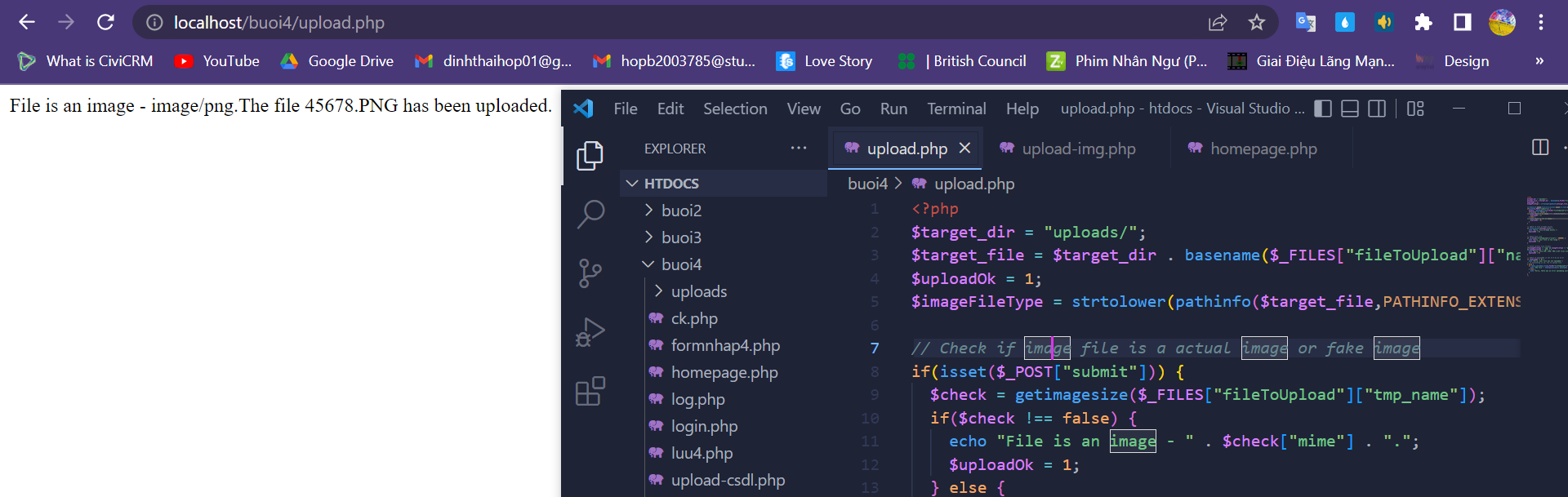
Homepage.php



Upload-img.php



Upload.php



Upload-csdl.php modìied

Graphical user interface, application

Description automatically generated

Homepage.php modified

Graphical user interface, text, website

Description automatically generated

Read-csv.php

Graphical user interface, text, application

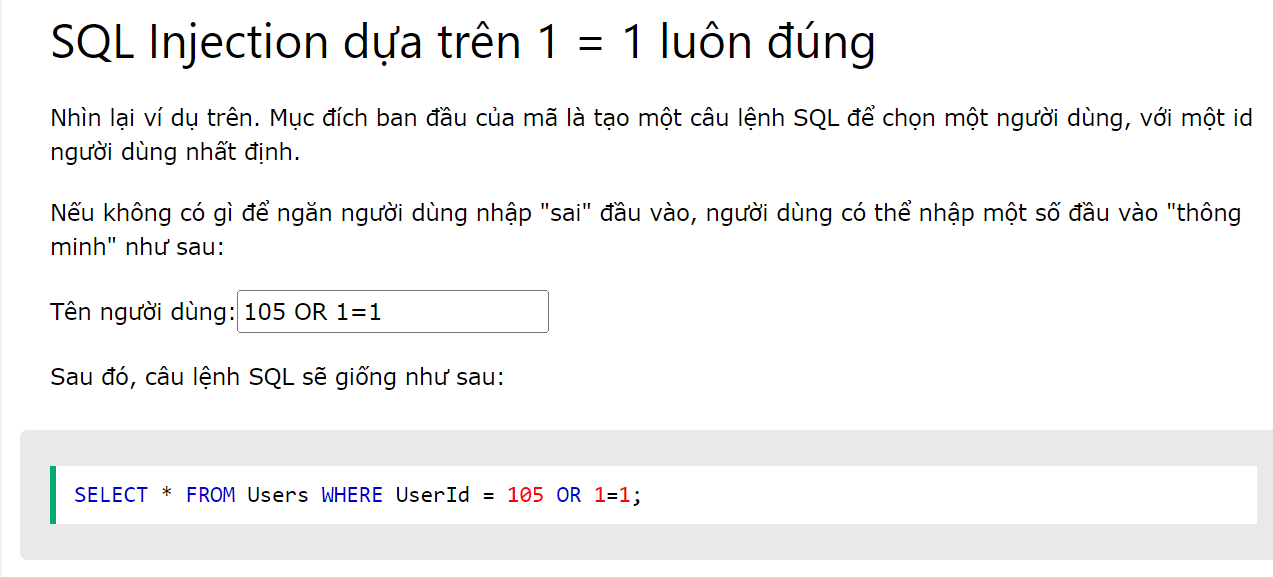
Description automatically generated

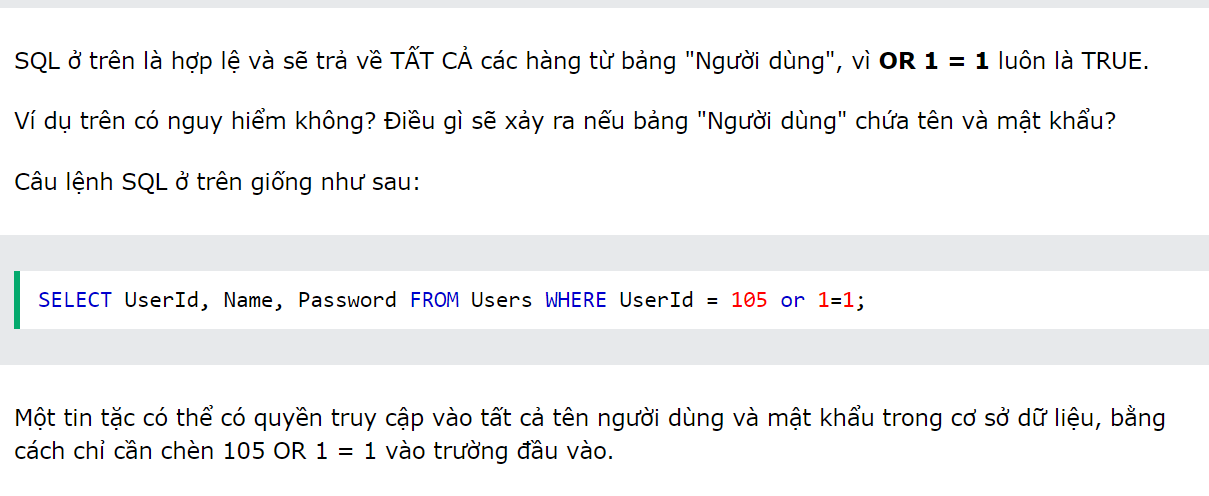
1. Trong vài trường hợp, hacker có thể sử dụng các kỹ thuật SQL Injection để hack hệ thống của bạn. Bạn hãy trình bày SQL Injection là gì và thử các ví dụ trình bày trong . Ứng dụng kỹ thuật đó vào trang đăng nhập mà bạn đã tạo, chụp lại các kết quả.

***SQL Injection***

SQL injection là một kỹ thuật chèn mã có thể phá hủy cơ sở dữ liệu của bạn.

SQL injection là một trong những kỹ thuật hack web phổ biến nhất.

SQL injection là vị trí của mã độc hại trong các câu lệnh SQL, thông qua đầu vào trang web.  




Graphical user interface, text, application, email

Description automatically generated

https://www.w3schools.com/sql/sql\_injection.asp

1. Dựa vào link, 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.

Cú pháp

setcookie(name, value, expire, path, domain, secure, httponly);

name: tên

value: giá trị

expire: hết hạn

path: đường dẫn

domain: miền

secure: bảo mật

httponly: /

**PHP Tạo / Lấy và lưu Cookie**

Ví dụ sau tạo một cookie có tên "người dùng" với giá trị "John Doe". Cookie sẽ hết hạn sau 30 ngày (86400 \* 30). "/" Có nghĩa là cookie có sẵn trong toàn bộ trang web (nếu không, hãy chọn thư mục bạn thích).

Sau đó, chúng tôi truy xuất giá trị của cookie "người dùng" (sử dụng biến toàn cục **$ \_COOKIE**). Chúng tôi cũng sử dụng **isset()** chức năng để tìm hiểu xem cookie có được đặt hay không

Graphical user interface, text, application, email

Description automatically generated

Xóa cookie

Graphical user interface, text, application, email

Description automatically generated

1. Dựa vào link, bạn hãy cho biết Session dùng để làm gì. Cách lưu, lấy, xóa giá trị trong Session.

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

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application, Word

Description automatically generated

Xóa session

Graphical user interface, text, application

Description automatically generated

1. Bạn hãy so sánh Cookie và Session.

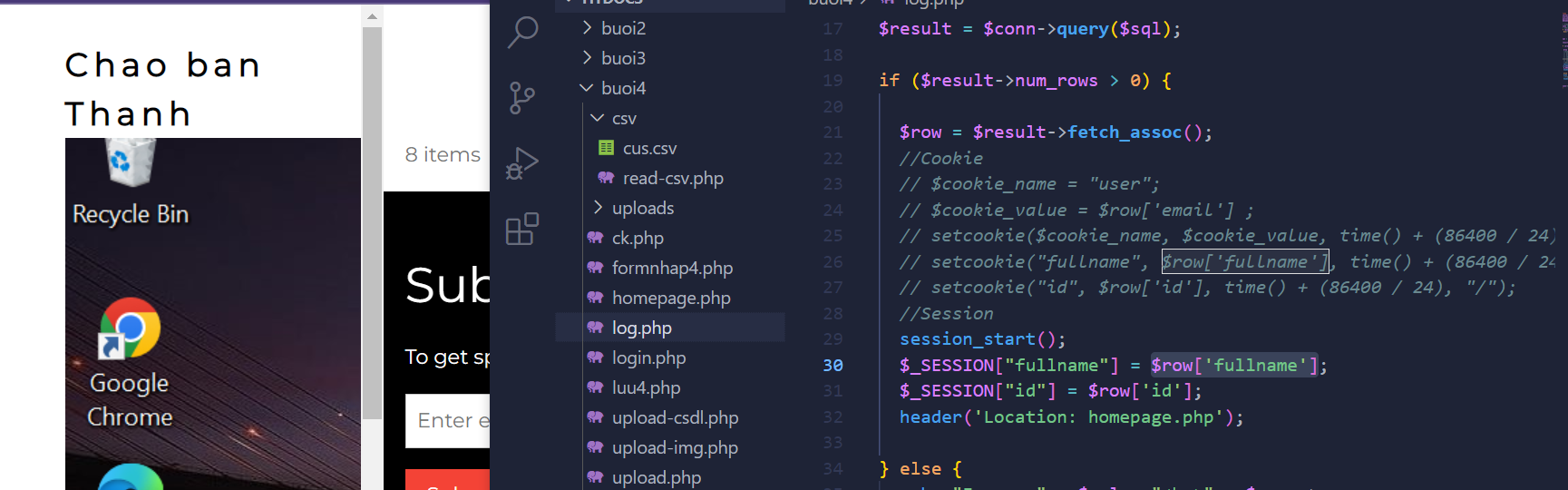
Đối với Cookie thông tin được lưu trên máy tính người dùng còn Session thì không(lưu trên các biến).

Các hàm phải đặt trước thẻ <html>

Hàm: session thì không có tham số bên trong còn cookie thì phải có tham số bên trong.

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 updated



Homepage.php updated

Text

Description automatically generated

Thoat.php

Text

Description automatically generated

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.

Text

Description automatically generated

1. Bạn đọc trong để tìm hiểu và mô tả các cơ chế, các hàm/thủ tục để thực hiện việc upload.

Đầu tiên, hãy đảm bảo rằng PHP được định cấu hình để cho phép tải tệp lên.

Tiếp theo, tạo một biểu mẫu HTML cho phép người dùng chọn tệp hình ảnh mà họ muốn tải lên.

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.

Những điều khác cần lưu ý:

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

Biểu mẫu ở trên gửi dữ liệu đến một tệp có tên "upload.php", tệp này chúng ta sẽ tạo tiếp theo

Text

Description automatically generated

$ 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. Nếu có, một thông báo lỗi sẽ hiển thị và $ uploadOk được đặt thành 0:

Text

Description automatically generated

Giới hạn kích thước tệp

Trường nhập tệp trong biểu mẫu HTML của chúng tôi ở trên được đặt tên là "fileToUpload".

Bây giờ, chúng tôi muốn kiểm tra kích thước của tệp. Nếu tệp lớn hơn 500KB, một thông báo lỗi sẽ hiển thị và $ uploadOk được đặt thành 0:

Graphical user interface, text, application

Description automatically generated

Cho phép các tệp giống định dạng được tải lên

Graphical user interface

Description automatically generated with medium confidence

Nếu không có lỗi xảy ra thì tệp được upload ngược lại thì hiển thị lỗi

Graphical user interface, text, application

Description automatically generated

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

file(filename, flag, context)

Đọc một tệp thành một mảng.

Filename: Chỉ định đường dẫn đến tệp để đọc.

Flag: Không bắt buộc. Có thể là một hoặc nhiều hằng số sau: FILE\_USE\_INCLUDE\_PATH - Tìm kiếm tệp trong đường dẫn include (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: ,. 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: Đặt tên file: <mssv><hoten><bai4>.docx nộp lên classroom, kèm với các file code đã tạo (**ngoại trừ file word trả lời câu hỏi, các file còn lại các bạn nén vào file .zip**).
* Mỗi câu các bạn trả lời bằng hình/trả lời dạng text tùy vào yêu cầu của câu hỏi, và ghi rõ số thứ tự câu hỏi mà bạn trả lời.
* Các bài phát hiện copy từ các bài của bạn khác sẽ không được tính điểm.
* *Chú ý: Các câu trả lời có tham khảo trên Internet phải trích dẫn link*