**Bài tập thực hành 04**

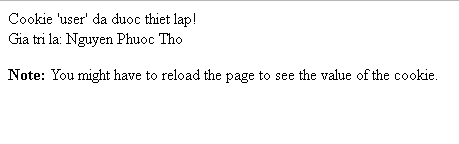
**Nguyễn Phước Thọ**

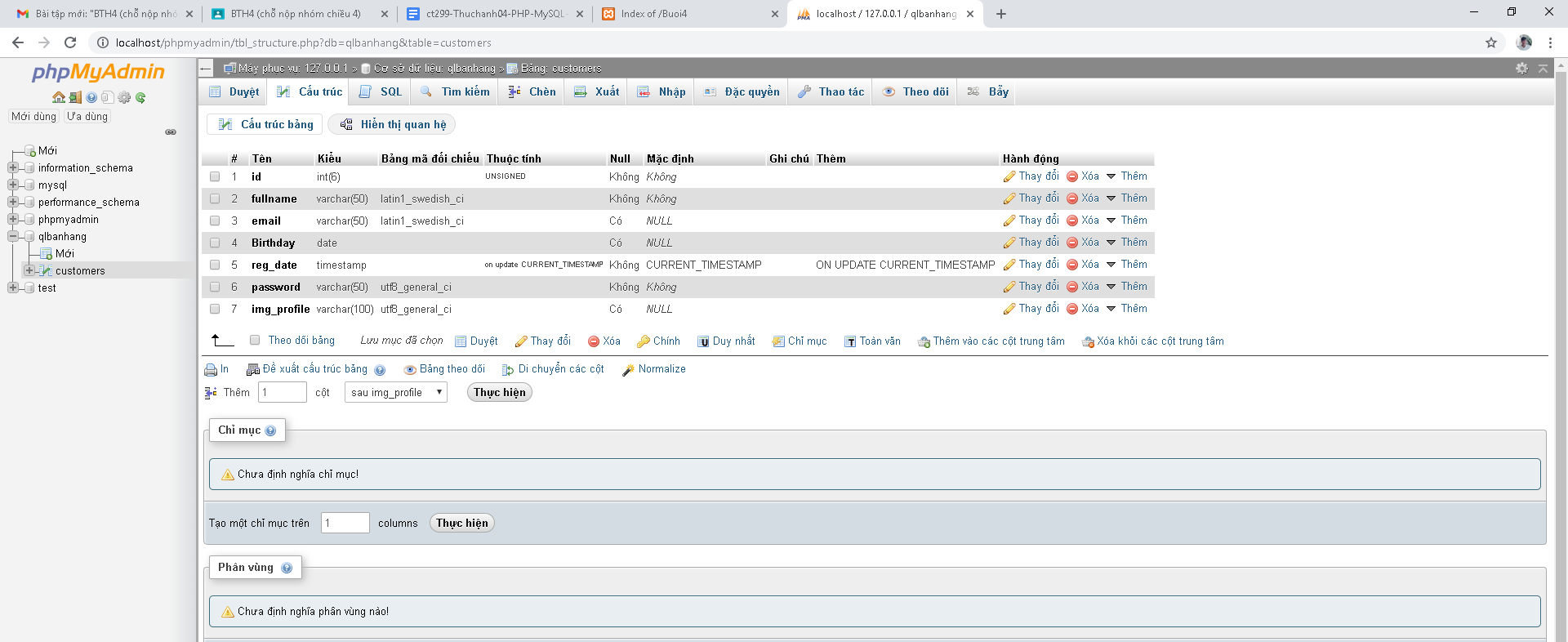
**B2003809**

**Lập trình PHP nâng cao**

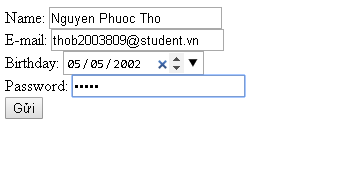
**Câu 1:**

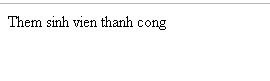
Tạo cookie

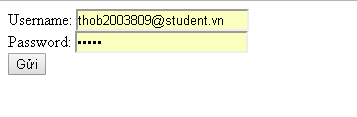




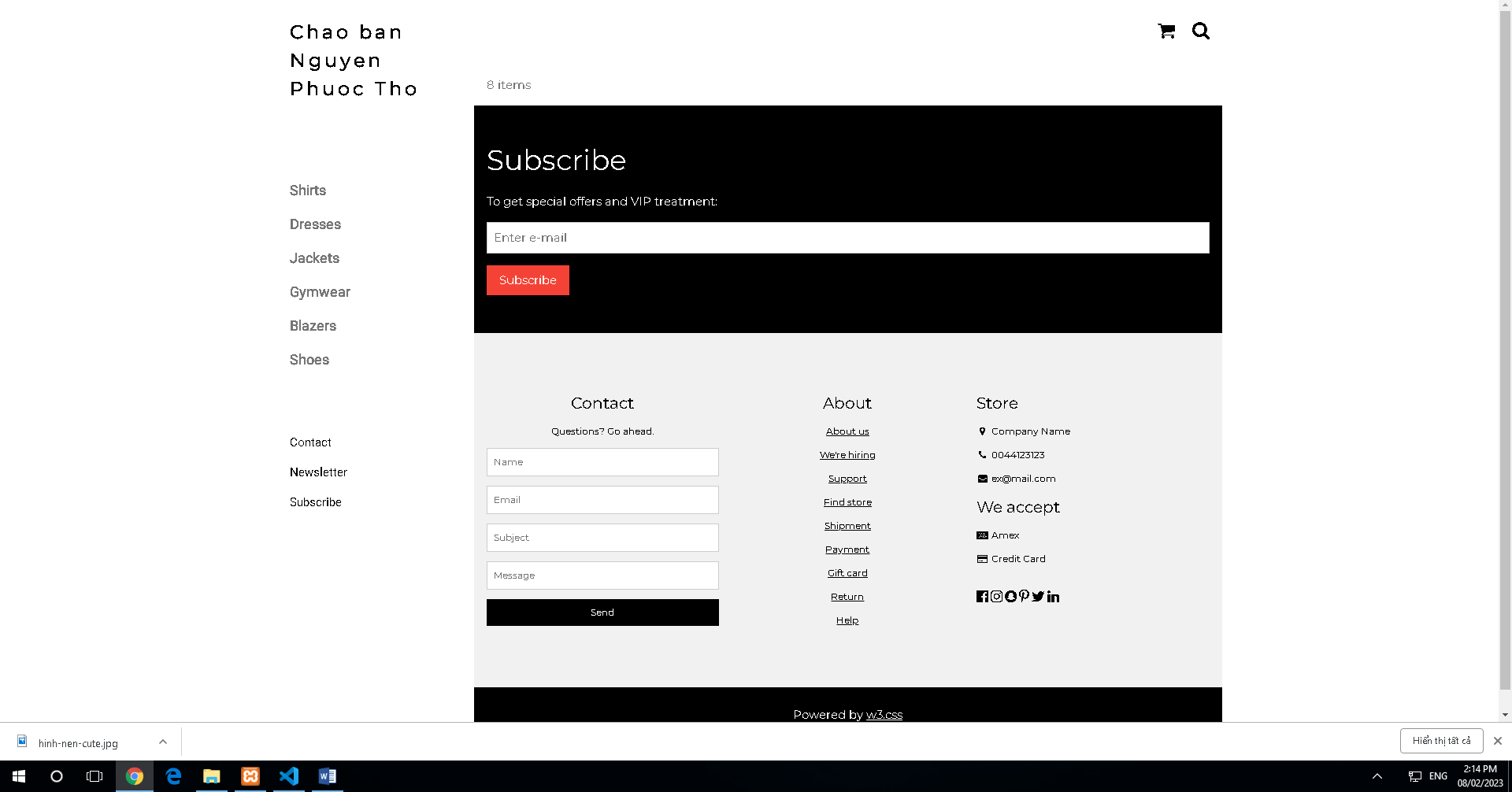
Tạo formnhap.php



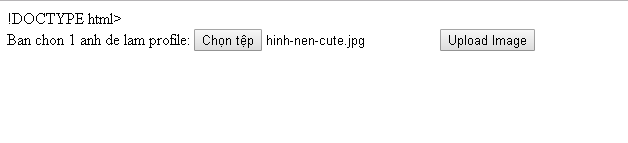




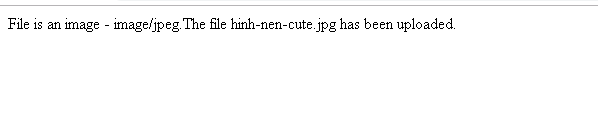
Homepage.php

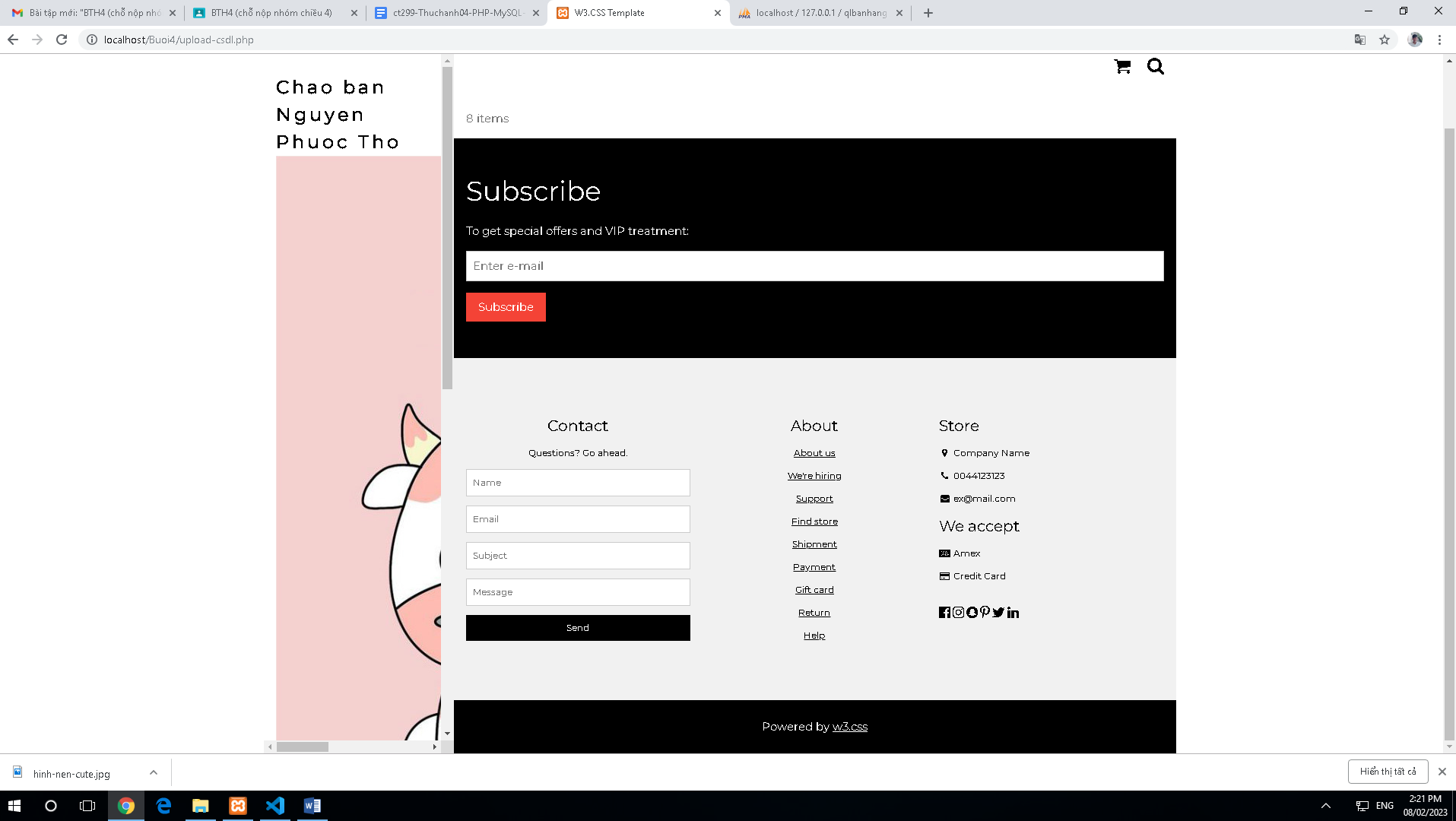


Upload-img.php



Upload thành công





**Câu 2:**

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.

**Câu 3:**

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 là mẩu tin nhỏ được lưu ở máy người dùng (cụ thể là tại Browser, trình duyệt), Cookie sử dụng với mục đích để theo dõi, lưu lại hoạt động truy cập

-Từ PHP có thể thiết lập Cookie bằng hàm setcookie (nhớ phải gọi trước các dòng code xuất html).

setcookie($name, $value, $expire = 0, $path="", $domain = "", $security = false, $httponly = false);

\* name là tên cookie, 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](https://xuanthulab.net/unix-timestamp-chuyen-doi-thoi-gian-unix.html), có thể dùng hàm time() để lấy Unix timestamp. Sau thời điểm này Cookie bị hủy lưu tại trình duyệt. Nếu thiết lập là 0 thì cookie hủy khi đóng trình duyệt

\*path đường dẫn mà cookie có hiệu lực. Sử dụng / cho biết cookie có hiệu lực ở cấp độ domain - mọi URL thuộc 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 tên miền

\*security = 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

Dùng biến $\_COOKIE là một mảng để truy cập thông tin cookie do trình duyệt gửi lên. Giống như Session bạn nên dùng isset() để kiểm tra sự tồn tại của COOKIE.

Xóa cookie

Để yêu cầu trình duyệt xóa cookie bạn sử dụng chính hàm setcookie với thủ thuật đặt thời gian đã hết hạn. Ví dụ:

**\*setcookie**( "name", "", **time**()- 60, "/","", 0);

**Câu 4:**

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

-Khái niệm về Session

Để trao đổi dữ liệu từ trang này qua trang khác (giữa 2 request) thì làm như thế nào? Ví dụ nếu người dùng đã đăng nhập, thì thông tin đăng nhập được lưu lại và chuyển cho các trang khác nhau trong phiên làm việc để tránh mỗi lần gửi request lại phải đăng nhập, hay người dùng chọn đựa mặt hàng vào giỏ hàng thì phải nhớ để chuyển đến trang thanh toán ... PHP có cơ chế để làm việc này đó chính là SESSION

**Session** là thông tin về phiên làm việc cho từng khách truy cập, trong PHP nó tạo một file trong thư mục tạm (thư mục này cài đặt ở php.ini : session.save\_path) để lưu thông tin này, thông tin này được dùng chung cho tất cả các trang mà khách truy cập. Mỗi khách truy cập, dựa vào thông tin trình duyệt gửi lên nó tạo (hoặc phục hồi) một Session riêng cho khách đó.

-Sự làm việc của Session có thể vắn tắt như sau:

Khi khách lần đầu truy cập, PHP tự động tạo ra một định danh duy nhất cho khách đó, định danh này là một chuỗi ngẫu nhiên - duy nhất. Nó là tham số để xác định tên file dữ liệu session.

Một mẩu tin nhỏ Cookie gọi là PHPSESSID (là ánh xạ đến định danh ở trên) sẽ được gửi đến trình duyệt và trình duyệt lưu giữ PHPSESSID này, để sau đó mỗi lần trình duyệt truy cập nó gửi lại PHPSESSID cho PHP.

PHP dựa vào PHPSESSID gửi đến để phục hồi - lấy lại dữ liệu từ file là thông tin của SESSION.

Session bị hủy - mất khi trình duyệt bị đóng lại, thông thường PHP cũng có tham số ấn định thời gian tồn tại của SESSION, ví dụ như 30 phút.

Như vậy SESSION là cơ chế lưu trữ và phục hồi thông tin cho phiên làm việc (truy cập) của khách, nhằm trao đổi thông tin khi duyệt từ page này sang page khác. Để Session hoạt động thì còn liên quan tới hỗ trợ COOKIE từ trình duyệt. Ví dụ trong Chrome bạn block Cookie từ facebook, thì bạn không thể đăng nhập được facebook.

-Chạy Session - Lưu trữ và lấy thông tin

Session trong PHP bắt đầu hoạt động sau khi bạn gọi hàm session\_start(), hàm này sẽ phục hồi dữ liệu SESSION nếu đã có, nếu chưa nó sẽ tạo ra SESSION mới cho bạn. Để sử dụng khuyên nên gọi hàm này ngay khi bắt đầu của Page. Một cách khác mà không cần quan tâm đến gọi session\_start() đó là thiết lập cho PHP tự động chạy hàm này bàng cách session.auto\_start = 1 trong php.ini

Khi mà hệ thống session trong PHP được chạy, mặc định nó sẽ gửi về trình duyệt một Cookie với tiền tố PHPSESSID, tất nhiên có thể thay đổi tiền tố này trong php.ini

Ví dụ trang chạy thử Session

startsession.php

<?php

**if** (**session\_id**() === '') **session\_start**();

**echo** "Session đang chạy";

Kiểm tra bạn thấy có Cookie gửi về, cookie này dùng để phục hồi dữ liệu Session

-Hủy Session

Bạn có thể hủy một biến, giá trị ... đã lưu vào Session:

Để hủy một biến nào đó lưu trữ trong Session thì dùng lệnh unset ví dụ unset($\_SESSION['counter']);

Để hủy toàn bộ Session thì dùng lệnh session\_destroy()

**Câu 5:**

Bạn hãy so sánh Cookie và Session.

Session là các tệp chứa thông tin người dùng ở máy chủ.

- Không được lưu trên trình duyệt

- Dữ liệu được lưu ở sever

-Dữ liệu của session được lưu ở máy chủ nên rất khó can thiệp hay sửa đổi

-Hết phiên làm việc (session) khi người dùng đóng trình duyệt

-Không hạn chế. Giới hạn bộ nhớ tối đa mà tập lệnh có thể tiêu thụ cùng lúc là 128MB theo mặc định

-Một session sẽ phụ thuộc vào cookie

Cookie là các tệp chứa thông tin người dùng ở phía máy khách.

-Lưu trữ ngay trên trình duyệt của người dùng

-Dữ liệu được lưu trên trình duyệt của client (người dùng)

-Dữ liệu của cookie được lưu ở thiết bị của người dùng nên rất dễ bị xâm nhập và sửa đổi

-Luôn được lưu trữ trong trình duyệt cho đến khi expired

-Tối đa là 4KB

-Một cookie không bị phụ thuộc bởi session

**Câu 6:**

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.

**Câu 7:**

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.

**Câu 8:**

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

Mảng biến $\_FILES khi var\_dump có cấu trúc dạng như sau:

array (size=1)

'myfile' =>

array (size=5)

'name' => string 'somefile.txt' (length=12)

'type' => string 'text/plain' (length=10)

'tmp\_name' => string '/tmp/phpDC66.tmp' (length=16)

'error' => int 0

'size' => int 18

-Các thành phần đó là:

myfile : chỉ số mảng tương ứng với tên phần tử input, upload file.

name : tên gốc (ban đầu) của file.

type : kiểu file (tùy phần mở rộng có thể là text/plain, image/jpg, image/png ...)

tmp\_name : nơi lưu tạm file upload lên, nếu muốn di chuyển nó ra khỏi thư mục tạm dùng hàm move\_uploaded\_file.

error : mã lỗi, nếu mã này bằng 0 là không lỗi.

size : cỡ file (byte).

Bằng việc đọc $\_FILES bạn sẽ biết các thông tin về file được upload, nơi file đang lưu tạm, bạn cần phải xử lý bằng các hàm PHP để di chuyển file ra một vị trí theo cấu trúc thư mục của ứng dụng.

Nếu sau khi upload vào thư mục tạm một thời gian (như trên là /tmp/) một thời gian (do cấu hình hệ thống) mà bạn không di chuyển nó đến vị trí thích hợp, nó sẽ tự xóa.

**Câu 9:**

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

**Câu 10:**

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