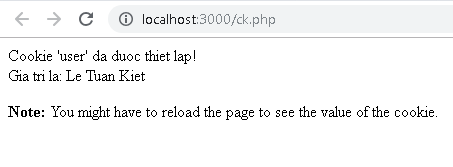
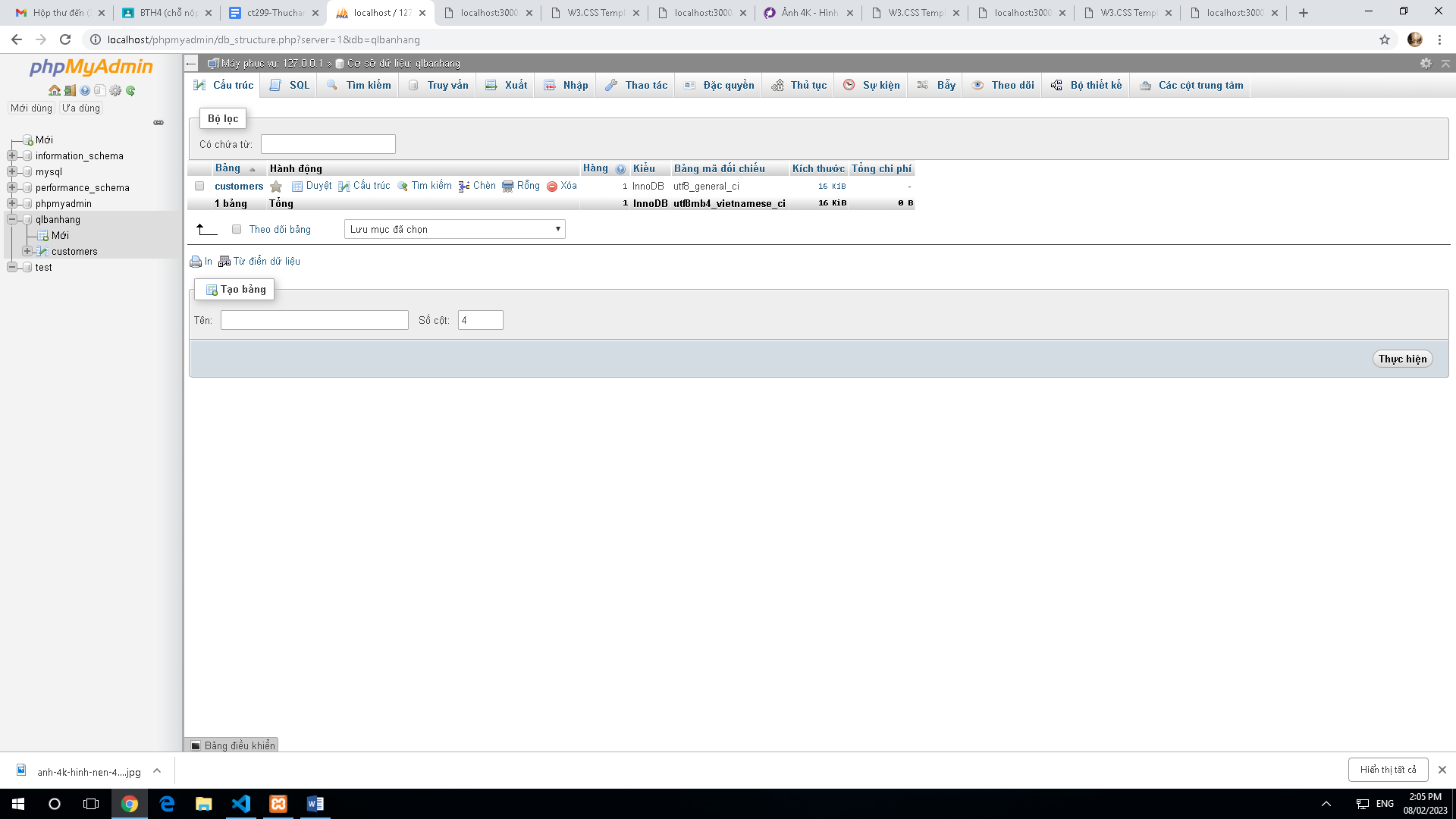
BÀI THỰC HÀNH BUỔI 4

Câu 1:

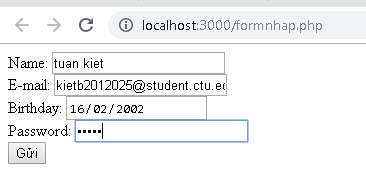
Tạo Cookies:



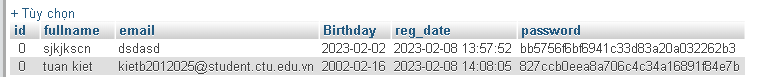
Tạo 1 trang đăng ký người dùng với mật khẩu được mã hóa

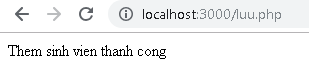


**formnhap.php**



**luu.php**





## Tạo form đăng nhập

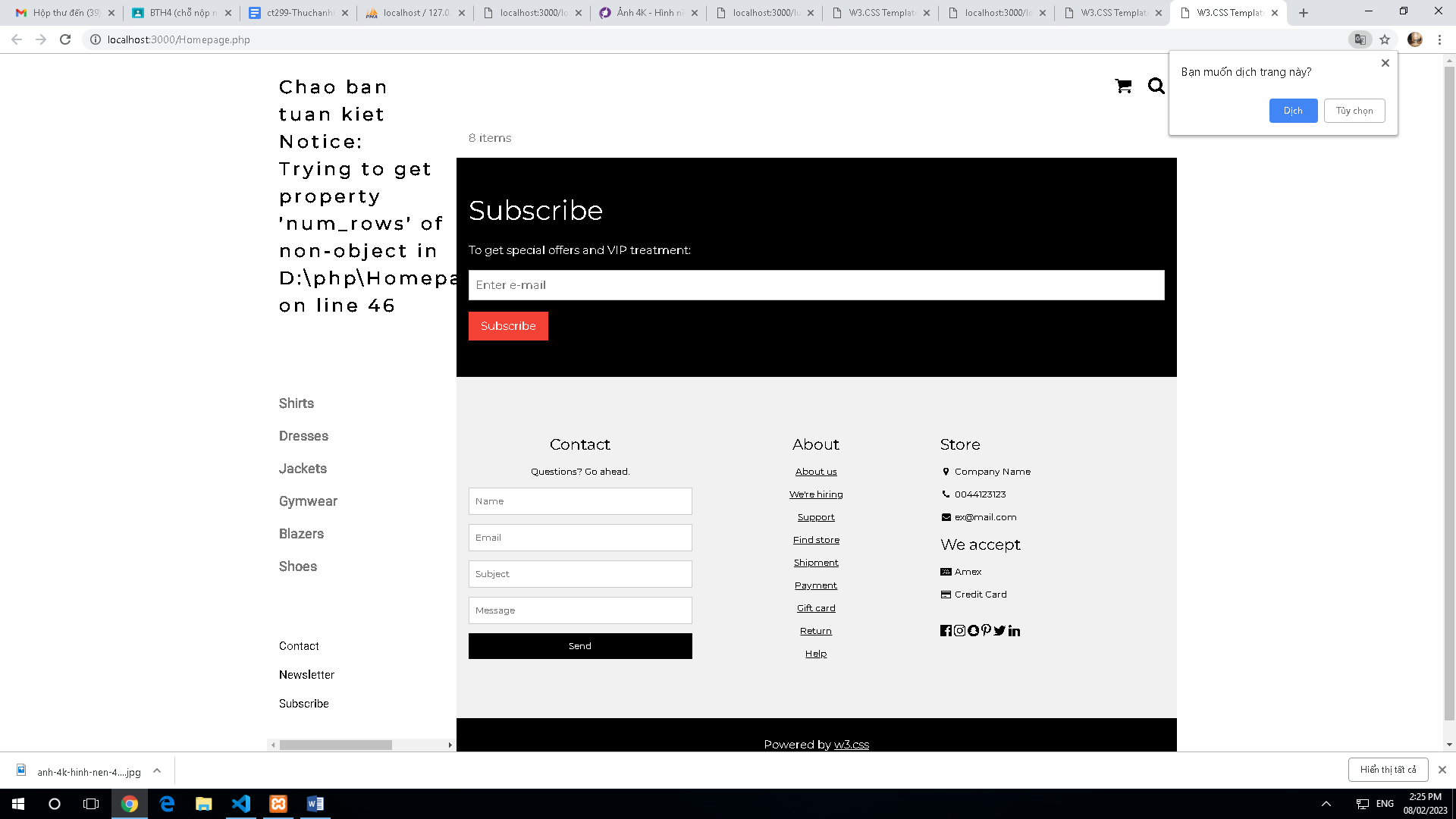
## 

**Log.php**

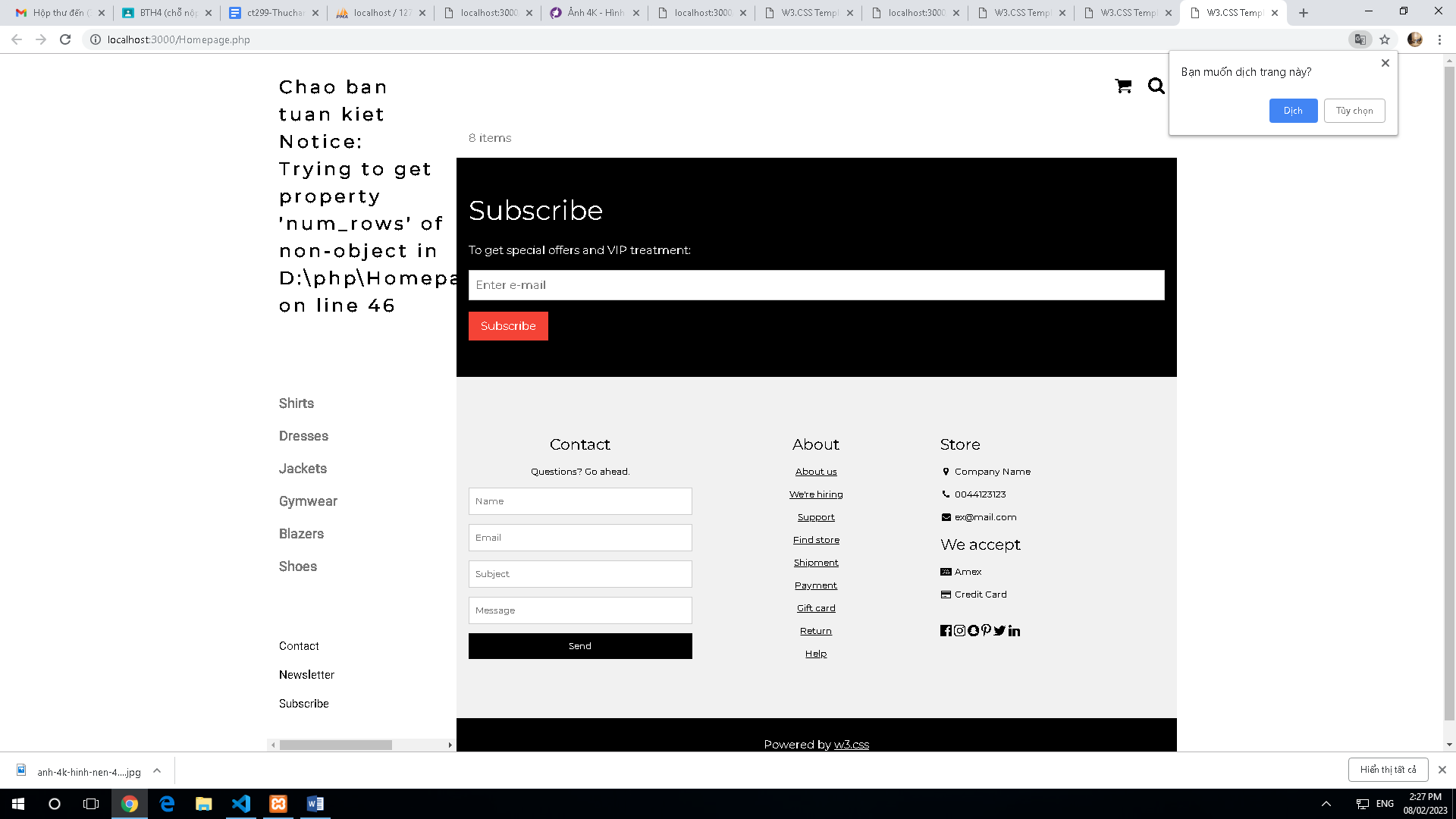


## Dùng Cookies lưu lại tên đăng nhập, email và điều hướng

**Log.php (modified)**



**Homepage.php**



## Upload tập tin

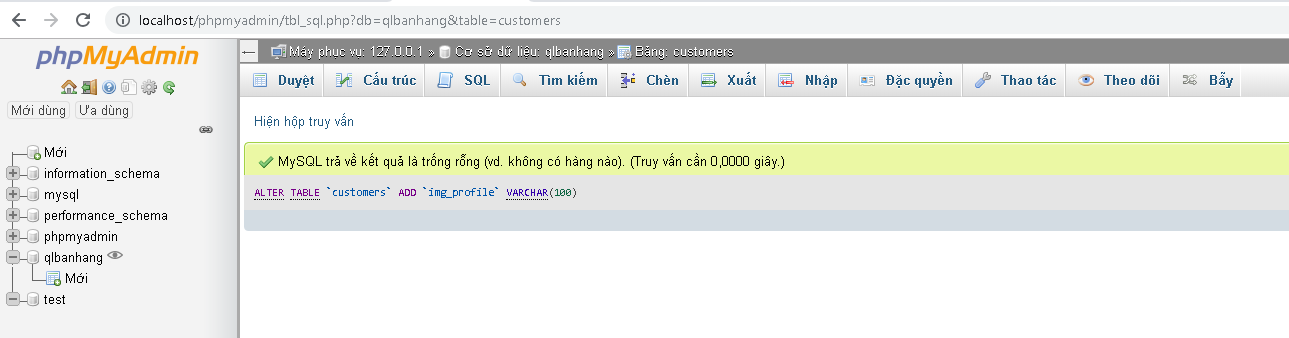
Upload-img.php



**upload.php**

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

**Upload-img.php (modified)**



**Upload-csdl.php**

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

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

## SQL Injection là gì?

**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 một đoạn [SQL](https://topdev.vn/blog/sql-la-gi/) 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 một người quản trị web, trên cơ sở dữ liệu của ứng dụng.

https://topdev.vn/blog/sql-injection/

**Câu 3**:**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.**

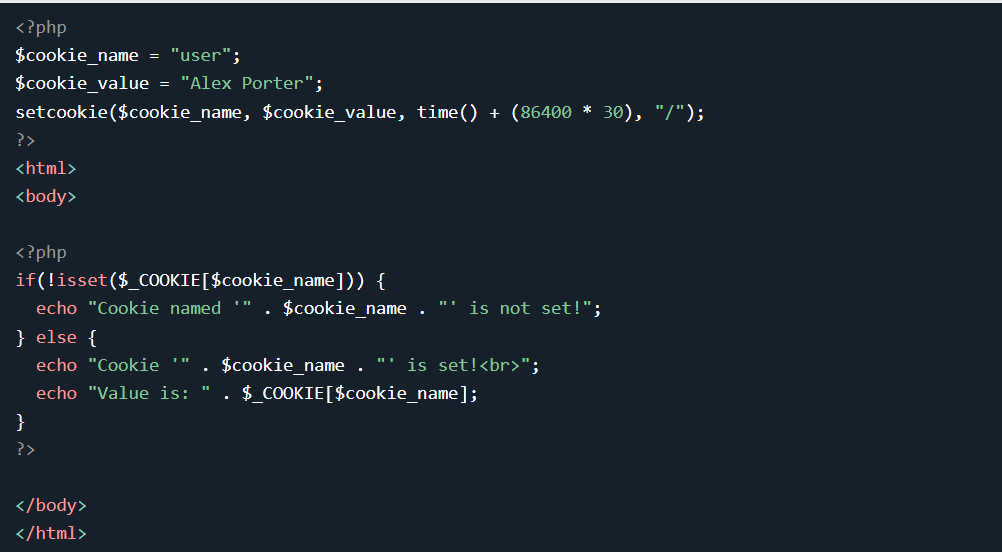
1. Dựa vào link, bạn hãy cho biết Cookie là gì,

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 bằng trình duyệt, nó cũng sẽ gửi cookie. Với PHP, bạn có thể tạo và truy xuất các giá trị cookie.

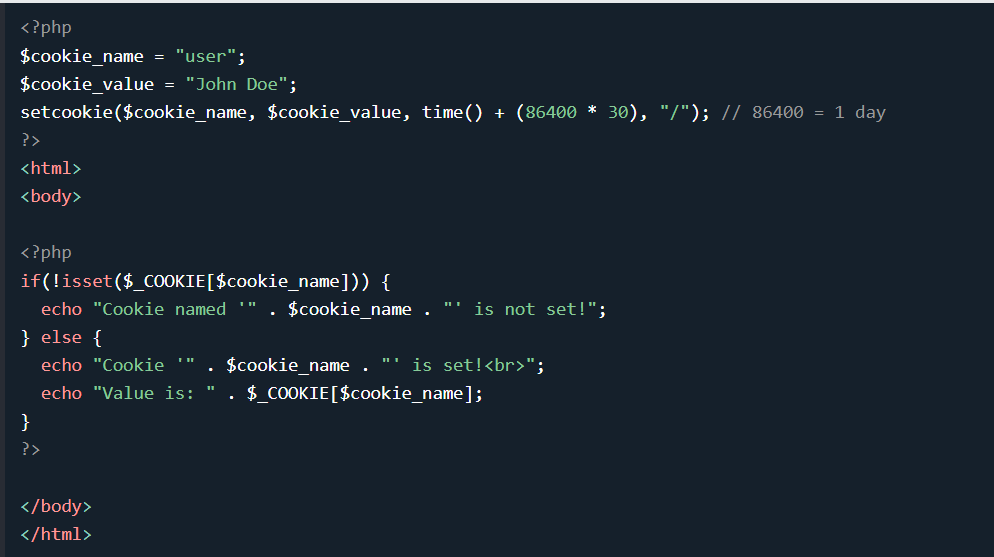
1. Diễn giải ý nghĩa các tham số trong setcookie(). Cách lưu, lấy, xóa giá trị trong cookie.

* 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

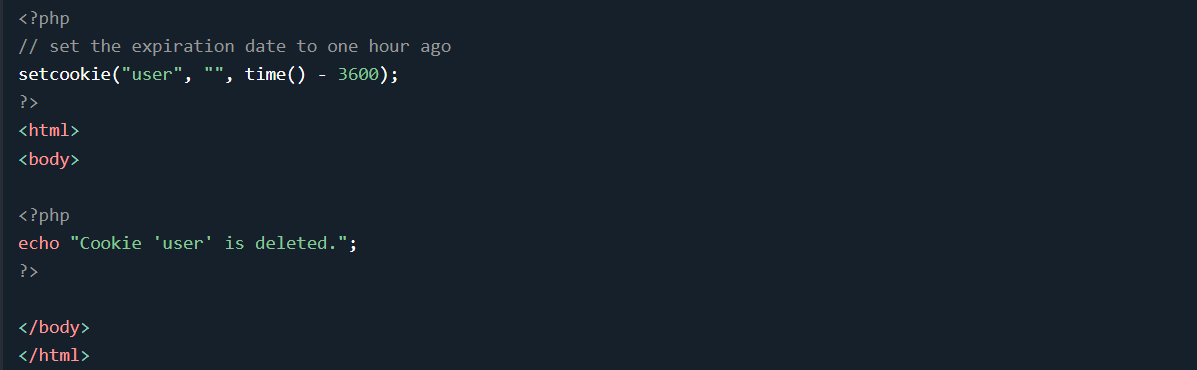
Để sửa đổi cookie, chỉ cần đặt (lại) cookie bằng setcookie()chức năng:



**-Lấy Cookie**



Để xóa cookie, hãy sử dụng **setcookie()** chức năng có ngày hết hạn trong quá khứ:



**Link tham khảo:**[***https://xuanthulab.net/su-dung-session-va-cookie-trong-php.html***](https://xuanthulab.net/su-dung-session-va-cookie-trong-php.html)

**Câu 4:Dựa vào link, bạn hãy cho biết Session dùng để làm gì. Cách lưu, lấy, xóa giá trị trong Session.**

* Dựa vào link, bạn hãy cho biết Session dùng để làm gì.

Khái niệm session là gì không quá xa lạ với các fresher, **Session** là một phiên làm việc là một khái niệm phổ biến được dùng trong lập trình web có kết nối với database. Đặc biệt các chức năng như đăng nhập, đăng xuất người dùng sẽ khó có thể thực hiện được nếu không sử dụng **session**.

* Cách lưu giá trị trong Session:

Tất cả Session được lưu trữ trong biến toàn cục $\_SESSION, vì thể để lưu thêm dữ liệu Session hay là thay đổi dữ liệu của Session thì ta sẽ thao tác trên biến đó. Lưu ý với bạn trước khi dùng phép lấy giá trị Session bạn phải kiểm tra session đó có tồn tại không rồi hãy lấy.

Để lưu một giá trị mới vào Session ta dùng cú pháp như sau:$\_SESSION['session\_name'] = $session\_value

Để lấy giá trị Session ta dùng cú pháp sau: $tenbien = $\_SESSION['session\_name']. Như tôi đề cập ở trên trước khi bạn lấy giá trị Session bạn nên kiểm tra nó có tồn tại không rồi hãy lấy.

* Cách xóa giá trị trong 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.**

| **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 **session** không dễ dàng sửa đổi vì chúng được lưu trữ ở phía máy chủ. | 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**. |

**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.**

$sql = "select img\_profile from customers where id = '".$\_SESSION['fullname']."'";

**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.**

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

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

file\_uploads = On. 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 = "multipart / 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 trên gửi dữ liệu đến một tệp có tên "upload.php", tệp này chúng ta sẽ tạo tiếp theo.

-Tập lệnh PHP giải thích:

* $ 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, kiểm tra xem file ảnh là ảnh thật hay ảnh giả

Lưu ý: Bạn sẽ 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.

-Kiểm tra xem tệp đã tồn tại chưa

* 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:

-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:

-Giới hạn loại tệp

Đoạn mã dưới đây chỉ cho phép người dùng tải lên các tệp JPG, JPEG, PNG và GIF. Tất cả các loại tệp khác đều đưa ra thông báo lỗi trước khi đặt $ uploadOk thành 0:

**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).**

-Tệp () đọc một tệp thành một mảng.

-Mỗi phần tử mảng chứa một dòng từ tệp, với ký tự dòng mới vẫn được đính kèm.

-Cú pháp:

**file(filename, flag, context)**

filename : Yêu cầu. 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 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.

**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 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:**

1. <https://www.w3schools.com/sql/sql_injection.asp> [↑](#footnote-ref-0)
2. <https://www.w3schools.com/php/php_cookies.asp> [↑](#footnote-ref-1)