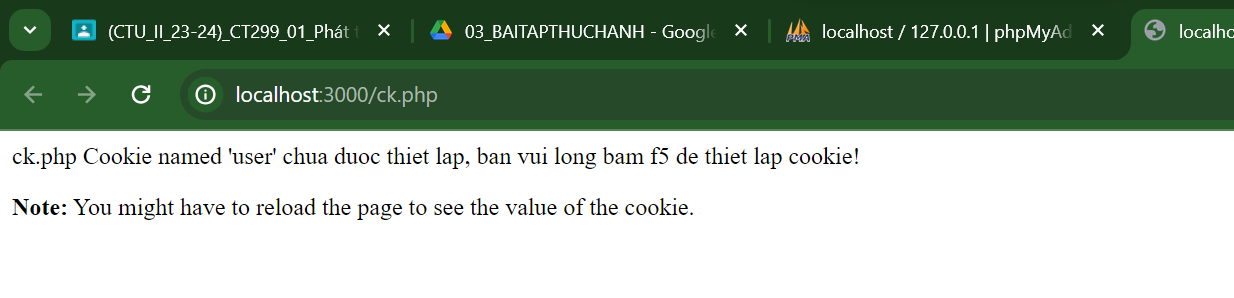
**Danh Thanh Cường**

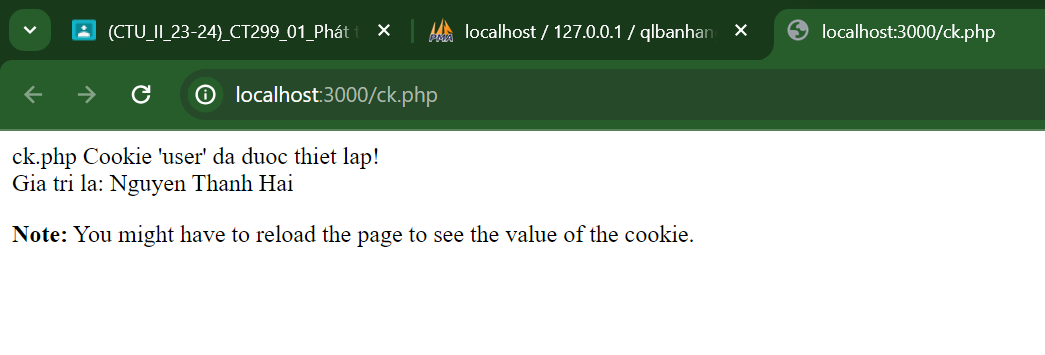
**Mssv: B2110008**

**BÀI THỰC HÀNH 4**

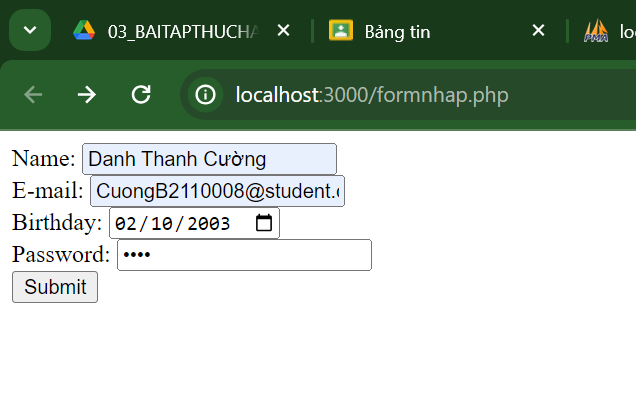
1. Tạo tập tin sử dụng khởi tạo cookies ck.php sau:



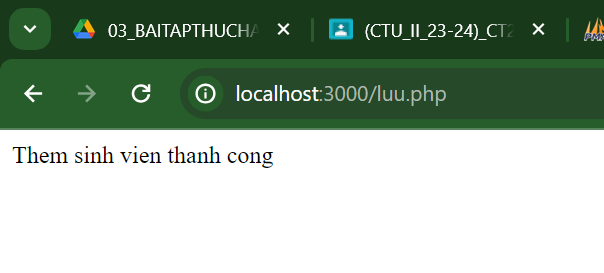
Hình 1 CK.php chưa thiết lập



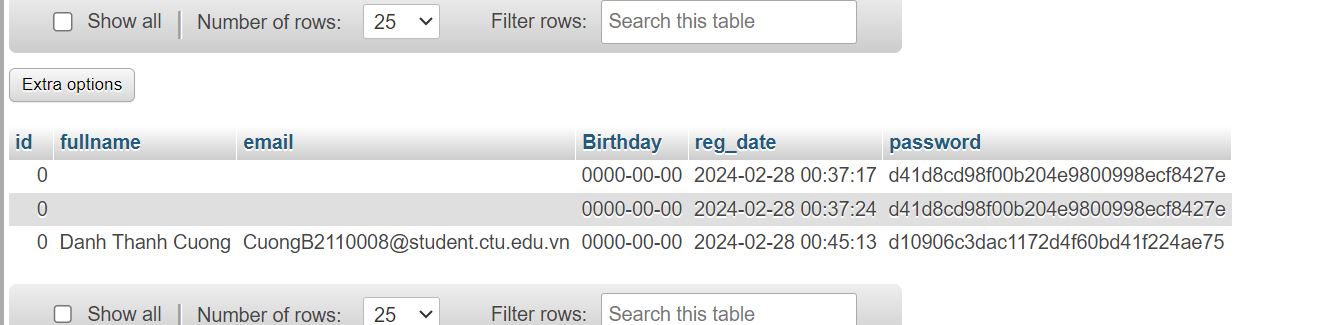
Hình 2 CK.php sau khi đã thiết lập



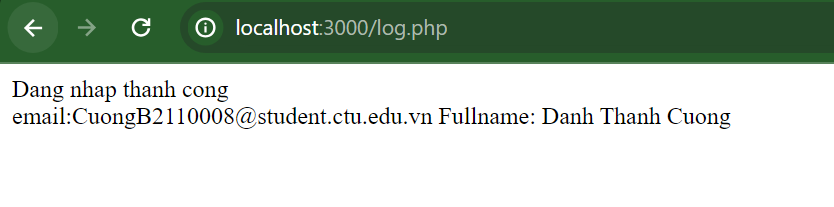
Hình 3 Formnhap.php



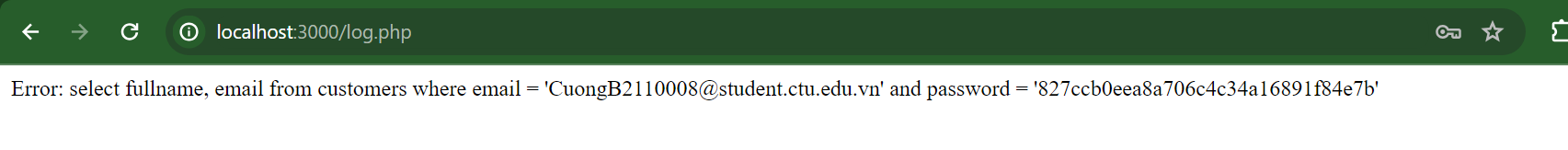
Hình 4 Form luu.php



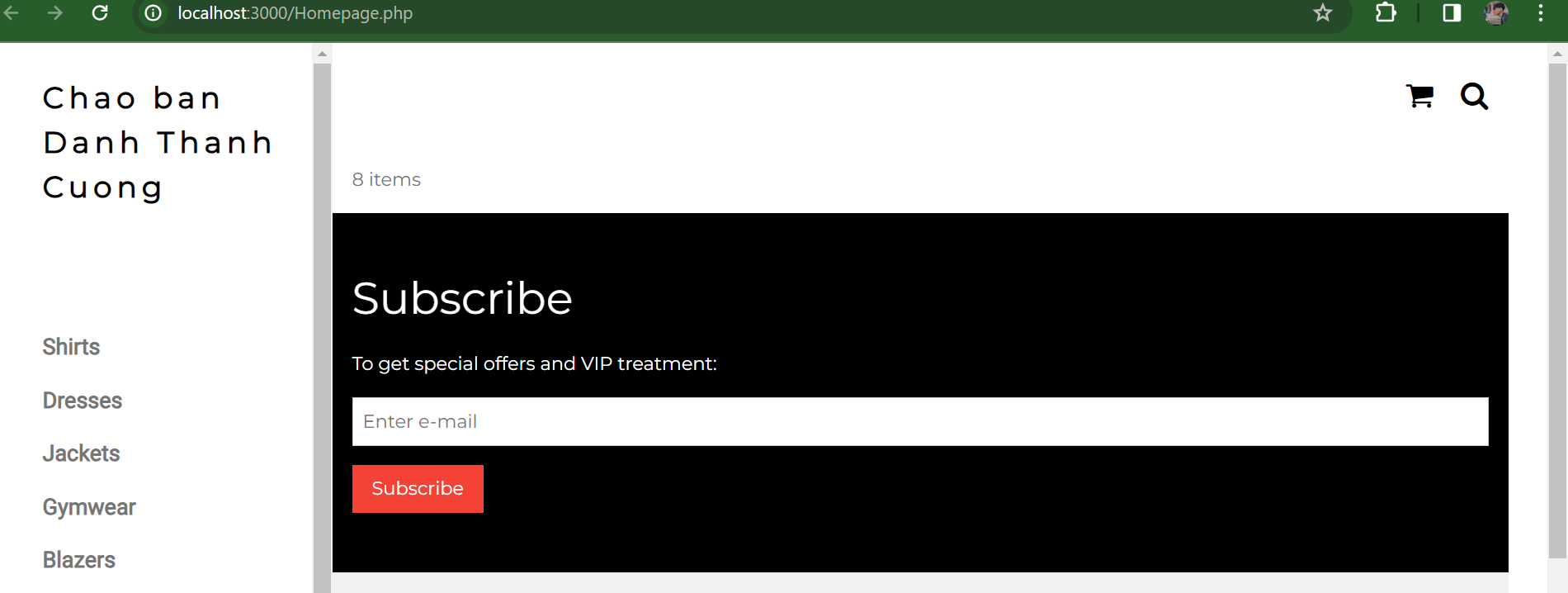
Hình 5 dữ liệu của database qlbanhang



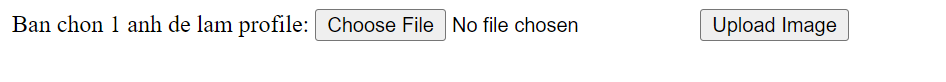
Hình 6 file Log.php khi đăng nhập thành công



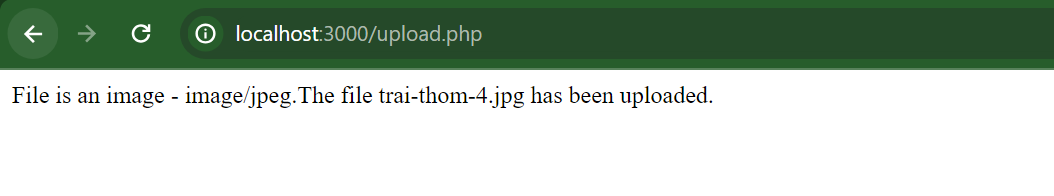
Hình 7 file Log.php khi đăng nhập thất bại



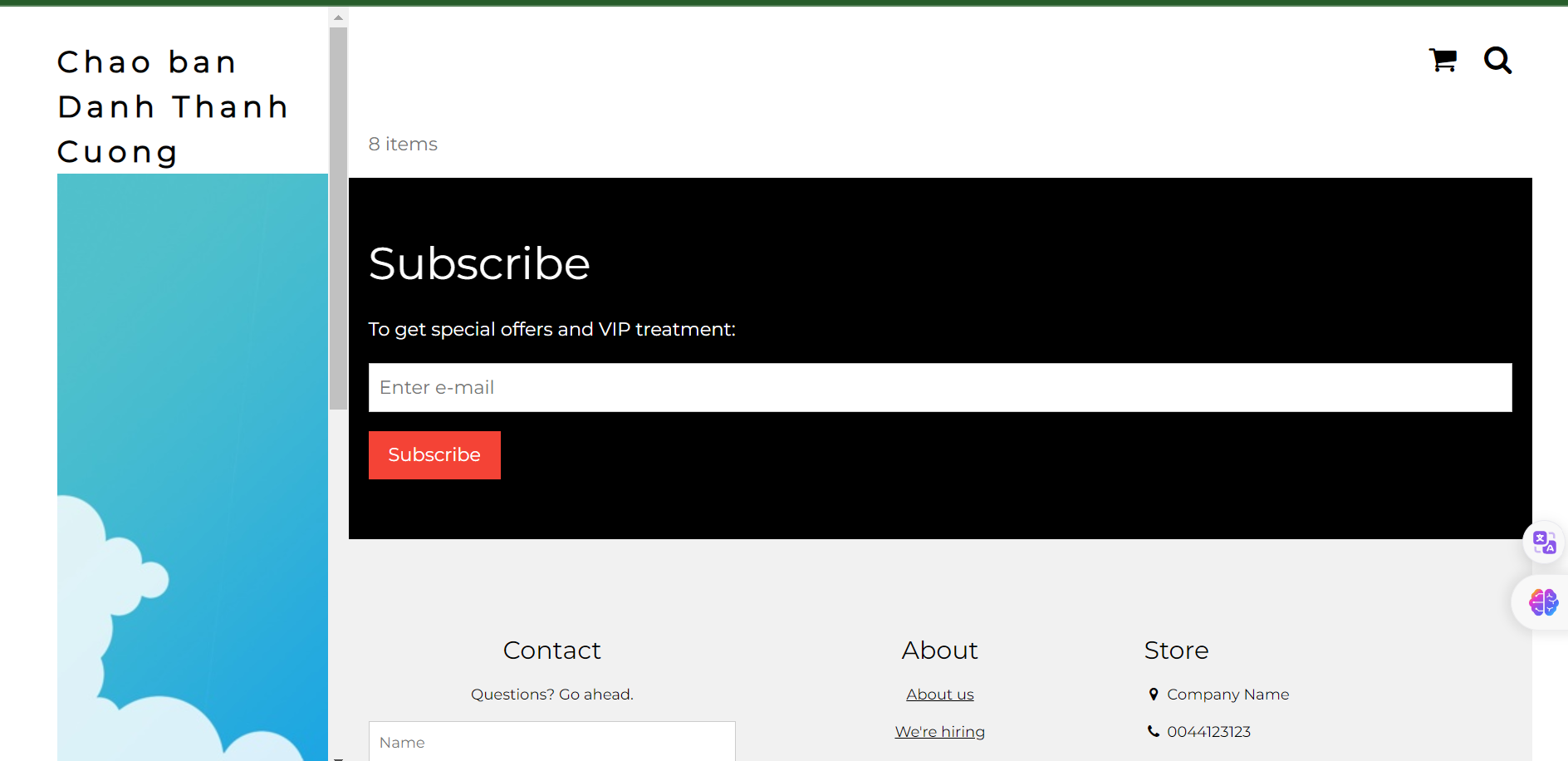
Hình 8 Homepage.php



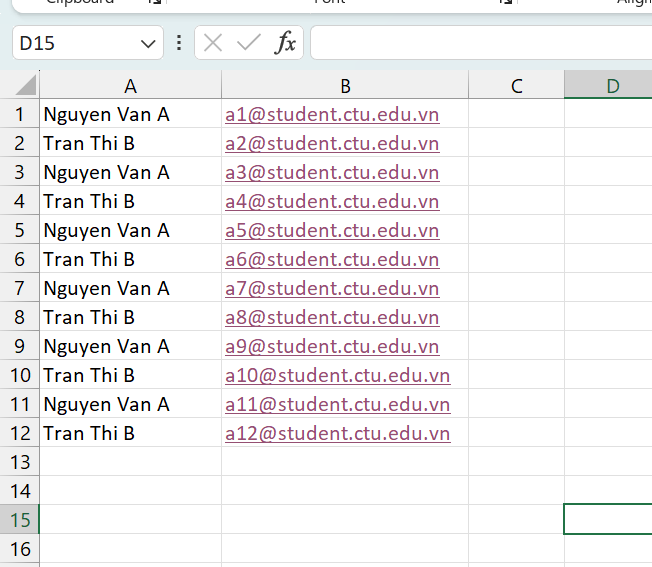
Hình 9 upload-img.php



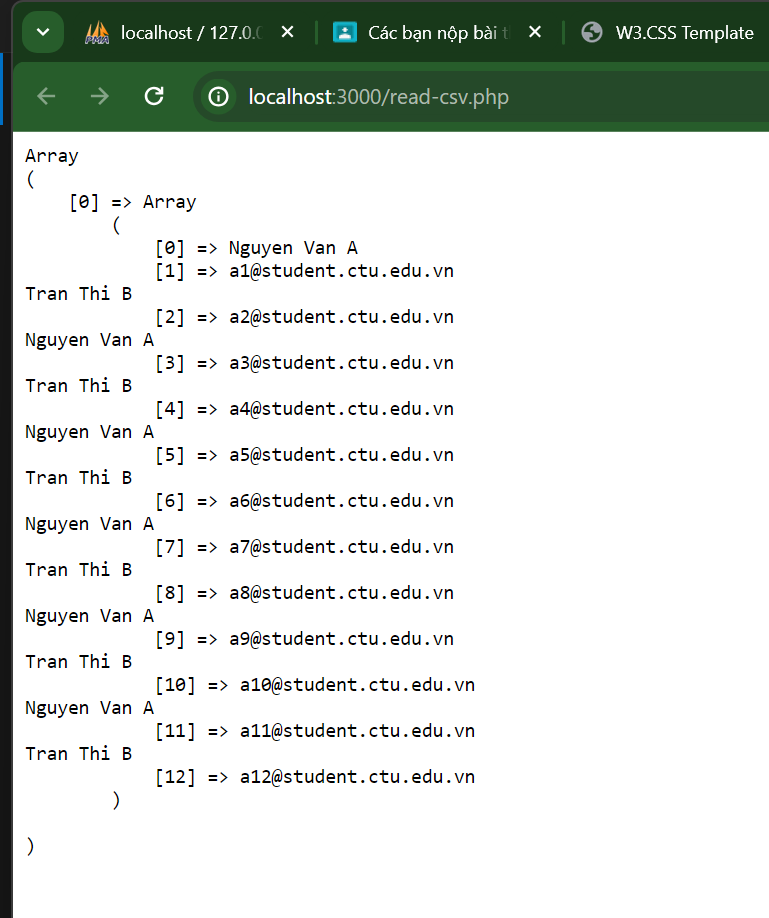
Hình10 Upload tập tin thành công



Hình 11 Upload tập tin làm profile



Hình 12 tập tin cus.csv



Hình 13 read-csv.php

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. Ứng dụng kỹ thuật đó vào trang đăng nhập mà bạn đã tạo, chụp lại các kết quả.

SQL Injection là kỹ thuật tấn công mạng nhắm vào ứng dụng web sử dụng SQL

* 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 việc đặt mã độc trong các câu lệnh SQL, thông qua đầu vào trang web.

Tài liệu tham khảo:<https://www.w3schools.com/sql/sql_injection.asp>

1. Dựa vào link2, 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 một file nhỏ được server gửi đến và lưu trữ ở trình duyệt web (browser) trên máy tính của user. Khi có một request từ browser đến server, những cookie đã tồn tại trên browser cũng sẽ được gửi đến server.

Trong đó :

– **$name** là tên của cookie.

– **$value** là giá trị của cookie được lưu trữ ở browser trên máy tính của user.

– **$expires\_or\_options** là thời gian mà cookie tồn tại (còn được lưu trữ) trên browser.

– **$path** là đường dẫn trên server mà cookie có sẵn. Thường đặt là ‘/’ thì cookie sẽ có sẵn trong toàn bộ tên miền của websitee.

– **$domain** là tên miền hoặc tên miền phụ mà cookie có sẵn.

– **$secure**: nếu được đặt là **true** thì cookie sẽ chỉ được gửi đến client với giao thức **https**.

– **$httponly**: nếu được đặt là **true** thì cookie sẽ chỉ được gửi đến client với giao thức **http**.

Hàm **setcookie()** sẽ trả về **true** nếu cookie được tạo thành công, ngược lại trả về **false**.

Tài liệu tham khảo: <https://gochocit.com/lap-trinh-web/cookie-la-gi-su-dung-cookie-trong-php>

1. Dựa vào link3, bạn hãy cho biết Session dùng để làm gì. Cách lưu, lấy, xóa giá trị trong Session.

* Session là tập tin lưu trữ thông tin về người dùng trên máy chủ trong suốt phiên làm việc của họ.
* Lưu giá trị:

**$\_SESSION["name"] = "value";**

* Lấy giá trị:

**$name = $\_SESSION["name"];**

* Xóa giá trị:

**unset($\_SESSION["name"]);**

1. Bạn hãy so sánh Cookie và Session.

Tài liệu tham khảo:<https://topdev.vn/blog/session-la-gi-cookie-la-gi/>

Bảng so sánh cookie và session:

| **Cookie** | **Session session là gì session là gì** |
| --- | --- |
| **Cookie** được lưu trữ trên trình duyệt của người dùng. | **Session** không được lưu trữ trên trình duyệt. |
| Dữ liệu **cookie** được lưu trữ ở phía client. | Dữ liệu **session** được lưu trữ ở phía server. |
| Dữ liệu **cookie** dễ dàng sửa đổi hoặc đánh cắp khi chúng được lưu trữ ở phía client. | 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 đến khi expired. | Sau khi đóng trình duyệt sẽ hết phiên làm việc (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.

<?php

session\_start();

if (isset($\_SESSION)) {

    session\_unset();

    session\_destroy();

}

echo "đã đăng xuất";

header('Location: formdangnhap');

exit();

?>

* Bị lỗi

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.



Hình 14 sua\_mk.php

* Bị lỗi

1. Bạn đọc trong4 để tìm hiểu và mô tả các cơ chế, các hàm/thủ tục để thực hiện việc upload.

Cơ chế upload file:

* Upload file là quá trình truyền tải file từ máy tính của người dùng lên máy chủ.
* PHP sử dụng $\_FILES biến toàn cục để lưu trữ thông tin về file được upload.

Phương thức upload:

* POST: Phương thức phổ biến nhất, sử dụng form HTML với enctype="multipart/form-data".

Hàm/thủ tục upload file:

* move\_uploaded\_file(): Hàm di chuyển file đã upload đến vị trí mong muốn trên máy chủ.
* is\_uploaded\_file(): Kiểm tra xem file đã được upload hay chưa.
* getimagesize(): Lấy thông tin về kích thước và loại hình ảnh.
* file\_exists(): Kiểm tra xem file có tồn tại hay không.
* unlink(): Xóa file khỏi máy chủ.

1. Bạn hãy đọc5, mô tả chức năng của hàm này và các tham số trong hàm (tham khảo thêm từ read-csv.php).

* Hàm file() trong PHP được sử dụng để đọc toàn bộ nội dung của một tệp và trả về một mảng chứa các dòng trong tệp đó.
* Tham số trong các hàm:

$filename: Đường dẫn đến tệp cần đọc.

$flags: Các cờ để chỉ định cách thức mở tệp. Các giá trị có thể là FILE\_USE\_INCLUDE\_PATH hoặc FILE\_IGNORE\_NEW\_LINES.

$context: Một tài nguyên context được sử dụng khi mở tệp.\

* Giá trị trả về:

Hàm file() trả về một mảng, mỗi phần tử trong mảng là một dòng trong file. Nếu file không tồn tại hoặc không thể mở được hàm sẽ trả về FALSE.

* Chức năng trong hàm:

Đọc tệp: Hàm file() đọc toàn bộ nội dung của tệp được chỉ định và trả về một mảng các dòng trong tệp.

Xử lý context: Có thể cung cấp một context tùy chọn để sử dụng khi mở tệp, chẳng hạn như định cấu hình các tùy chọn cho stream.