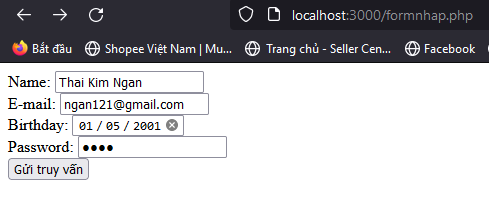
**B1906386 - Thái Kim Ngân**

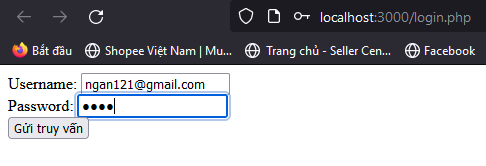
**Bài tập thực hành 04**

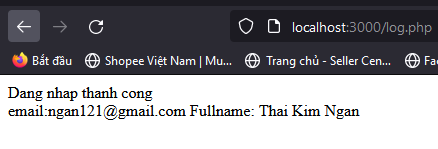
Lập trình PHP nâng cao

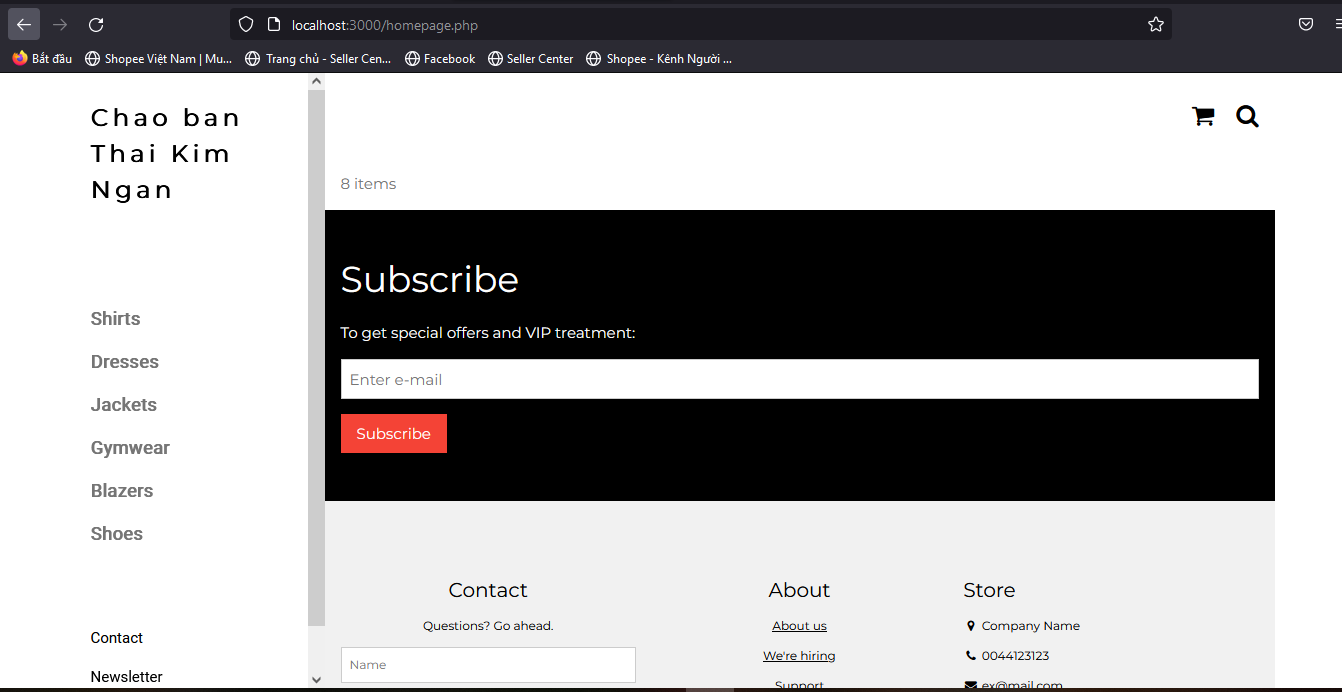
# Yêu cầu bài thực hành:

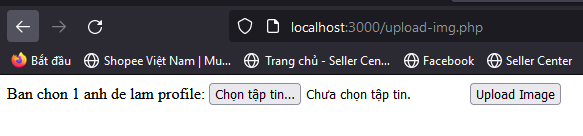
1. Bạn hãy chạy tất cả các lệnh hướng dẫn ở trên và chụp lại màn hình kết quả.

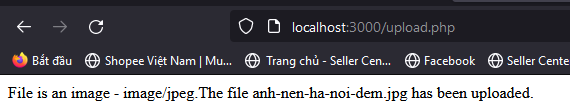


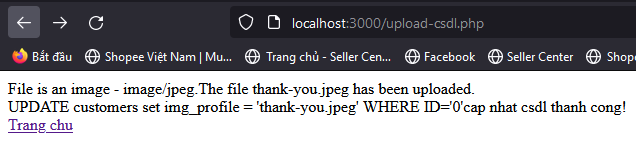


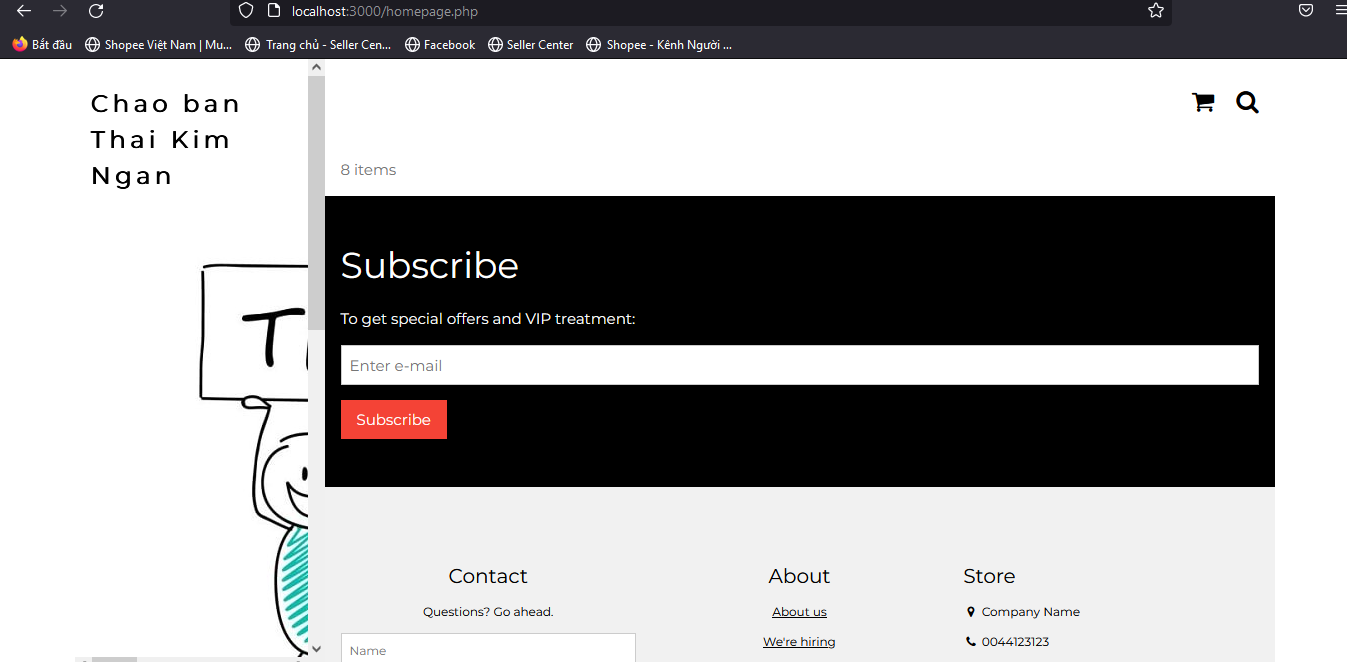












1. Trong vài trường hợp, hacker có thể sử dụng các kỹ thuật SQL Injection để hack hệ thống của bạn. Bạn hãy trình bày SQL Injection là gì và thử các ví dụ trình bày trong [[1]](#footnote-0). Ứng dụng kỹ thuật đó vào trang đăng nhập mà bạn đã tạo, chụp lại các kết quả.

Trả lời:

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

1. 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.

Trả lời: 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.

Ý nghĩa các tham số trong setcookie(name, value, expire, path, domain, secure, httponly) là

Lấy giá trị trong cookie:

<?php

$cookie\_name = "user";

$cookie\_value = "Kim Ngan";

setcookie($cookie\_name, $cookie\_value, time() + (86400 \* 30), "/"); // 86400 = 1 day

?>

<html>

<body>

<?php

if(!isset($\_COOKIE[$cookie\_name])) {

echo "Cookie named '" . $cookie\_name . "' is not set!";

} else {

echo "Cookie '" . $cookie\_name . "' is set!<br>";

echo "Value is: " . $\_COOKIE[$cookie\_name];

}

?>

</body>

</html>

Lưu giá trị trong cookie:

Xóa giá trị trong cookie:

<?php

// set the expiration date to one hour ago

setcookie("user", "", time() - 3600);

?>

<html>

<body>

<?php

echo "Cookie 'user' is deleted.";

?>

</body>

</html>

1. Dựa vào link[[3]](#footnote-2), bạn hãy cho biết Session dùng để làm gì. Cách lưu, lấy, xóa giá trị trong Session.

Trả lời:

Session dùng để lưu trữ thông tin để sử dụng trên nhiều trang, thông tin này không được lưu trữ trên máy tính của người dùng.

Lưu giá trị trong Session:

Lấy giá trị trong Session:

<?php

session\_start();

?>

<!DOCTYPE html>

<html>

<body>

<?php

// Echo session variables that were set on previous page

echo "Favorite color is " . $\_SESSION["favcolor"] . ".<br>";

echo "Favorite animal is " . $\_SESSION["favanimal"] . ".";

?>

</body>

</html>

Xóa giá trị trong Session:

<?php

session\_start();

?>

<!DOCTYPE html>

<html>

<body>

<?php

// remove all session variables

session\_unset();

// destroy the session

session\_destroy();

?>

</body>

</html>

1. Bạn hãy so sánh Cookie và Session.

Vị trí lưu:

- Sesion: Lưu trên server.

- Cookie: Lưu trên trình duyệt của client.

Bảo mật:

- Sesion: Session lưu trên server nên bảo mật.

- Cookie: Cookie lưu dưới client nên kém bảo mật hơn.

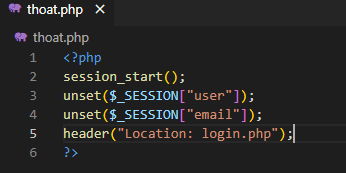
Giới hạn:

- Sesion: Lưu không giới hạn.

- Cookie: Lưu có giới hạn.

( Nguồn: viblo.asia )

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.



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.
2. Bạn đọc trong[[4]](#footnote-3) để tìm hiểu và mô tả các cơ chế, các hàm/thủ tục để thực hiện việc upload.

Mô tả: Để upload được file chúng ta cần có input file với type =”file” và trên form upload chúng ta cần chỉ định thuộc tính enctype = "multipart/form-data". Khi người dùng submit form, file sẽ được upload lên thư mục tạm của webserver và tên của file đã upload cũng là một tên tạm thời do webserver sinh ra, do đó để di chuyển nó đến thư mục được chỉ định trên webserver.

1. Bạn hãy đọc[[5]](#footnote-4), mô tả chức năng của hàm này và các tham số trong hàm (tham khảo thêm từ read-csv.php).

Mô tả chức năng của hàm file(): đọc một tệp thành một mảng.

Chức năng của tham số filename: Bắt buộc. Chỉ định đường dẫn đến tệp để đọc.

Chức năng của tham số flag: Không bắt buộc. Có thể dùng một hoặc nhiều hằng số sau: FILE\_USE\_INCLUDE\_PATH, FILE\_IGNORE\_NEW\_LINES, FILE\_SKIP\_EMPTY\_LINES

Chức năng của tham số context: Không bắt buộc. Chỉ định ngữ cảnh của xử lý tệp. 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-5),[[7]](#footnote-6). 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-0)
2. <https://www.w3schools.com/php/php_cookies.asp> [↑](#footnote-ref-1)
3. <https://www.w3schools.com/php/php_sessions.asp> [↑](#footnote-ref-2)
4. <https://www.w3schools.com/php/php_file_upload.asp> [↑](#footnote-ref-3)
5. <https://www.w3schools.com/php/func_filesystem_file.asp> [↑](#footnote-ref-4)
6. <https://www.php.net/manual/en/features.file-upload.post-method.php>, [↑](#footnote-ref-5)
7. https://stackoverflow.com/questions/6654351/check-file-uploaded-is-in-csv-format [↑](#footnote-ref-6)