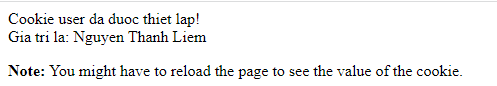
**B2003790**

**Nguyễn Thanh Liêm**

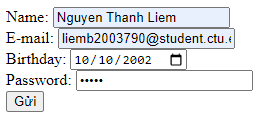
**Lập trình PHP nâng cao**

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

File ck.php

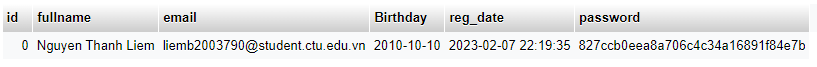


File formnhap.php

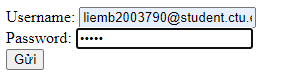


File luu.php





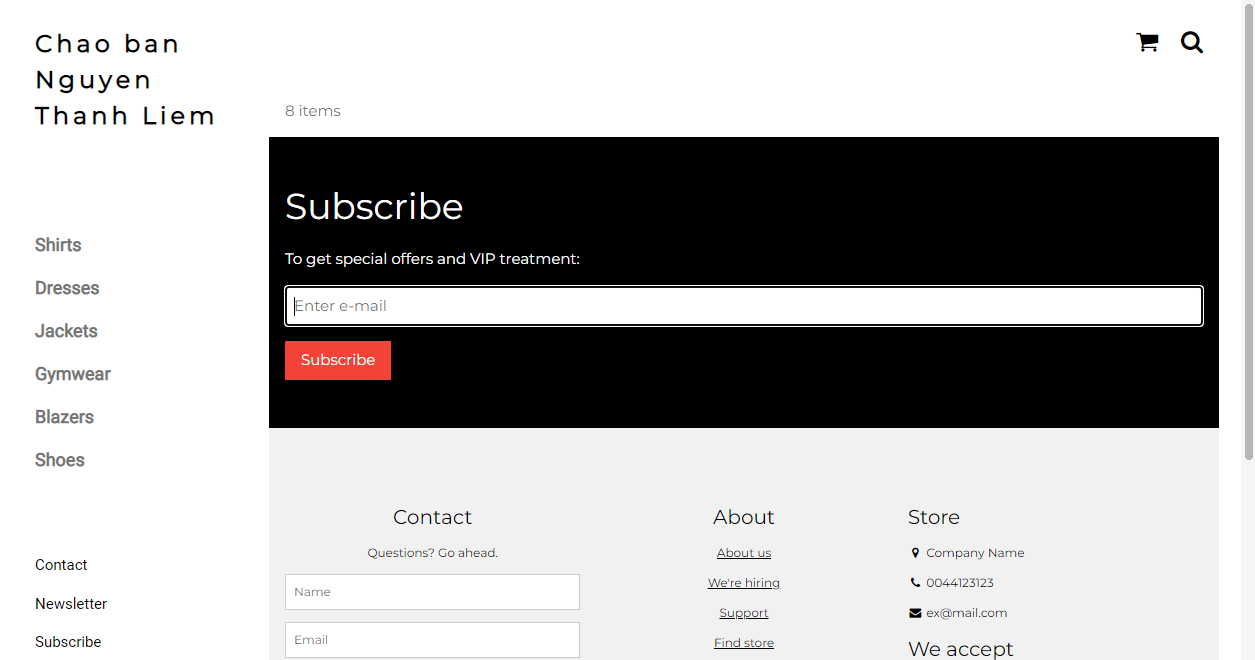
File login.php



File log.php



File homepage.php



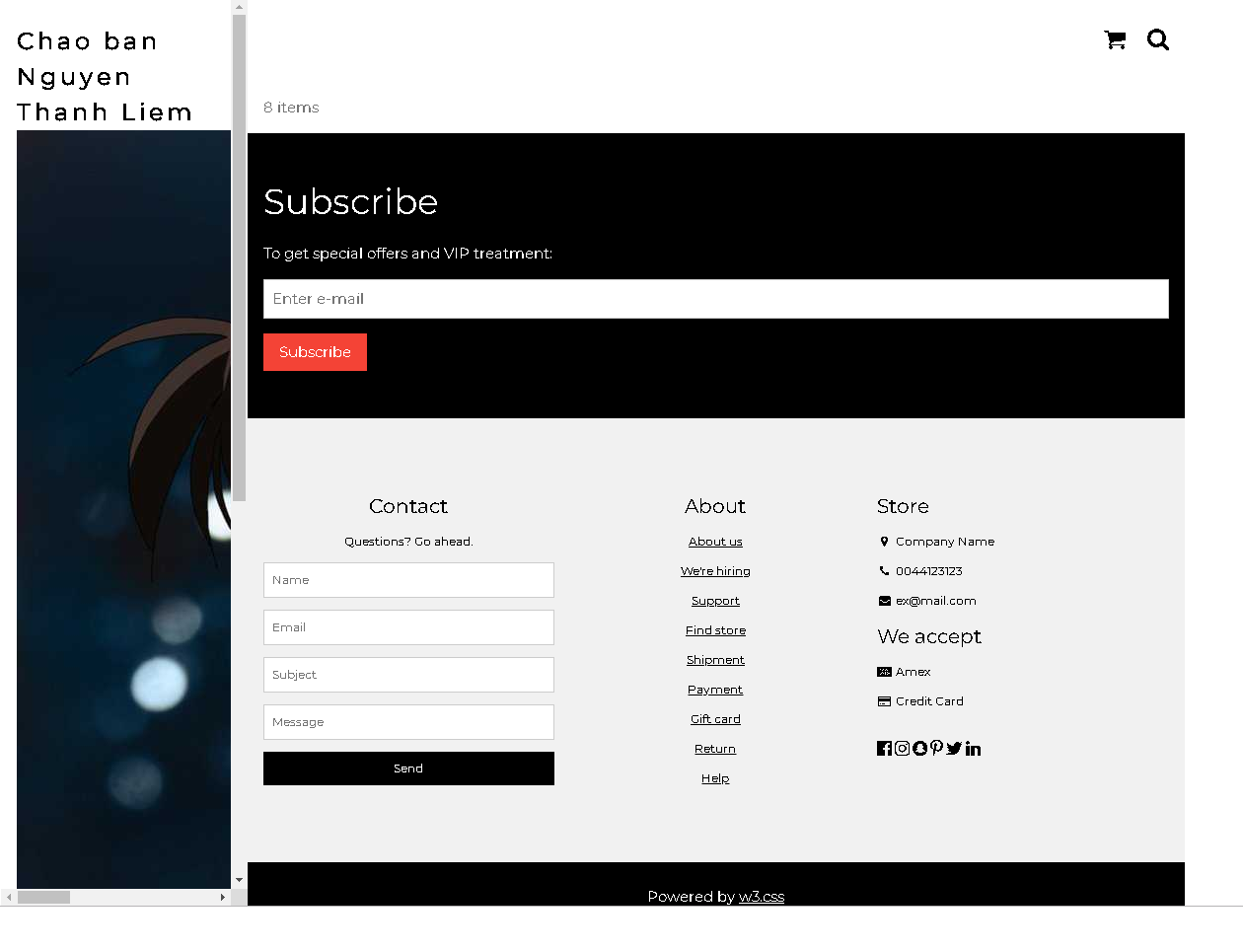
File upload.php



File upload.php



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

* SQL Injection là một kỹ thuật chèn mã có thể phá hủy một cơ sở dữ liệu. Là một trong những ký thuật hack wed phổ biến nhất hiện nay. Là vị trí của mã độc hại trong câu lệnh SQL thông qua đầu vào của trang wed

1. ***Dựa vào link[[2]](#footnote-2), 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 tệp nhỏ mà máy chủ nhúng vòa máy tính người dùng. Mỗi khi máy tính yêu cầu một trang bằng trình duyệt, nó cũng sẽ gửi cookie. Cookie thường được sử dụng để xác định người dùng.
* Ý nghĩa các tham số trong setcookie()

(https://xuanthulab.net/su-dung-session-va-cookie-trong-php.html)

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

*name:* 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, có thể dùng hàm time() để lấy Unix timestamp. Sau thời gian này cookie bị hủy lưu tại trình duyệt. Nếu thiết lập là 0 thì cookie hủy ngay khi đóng trình duyệt.

path: đường dẫn cookie có hiệu lực. nếu để giá trị mặc định thì có giá trị theo đường dẫn hiện tại.

domain: tên miền.

secure: bằng true nếu sử dụng https để truyền dữ liệu (mặc định là false)

httponly: mặc định là false, nếu true thì chỉ cho phép cookie với giao thức http.

* Lưu cookie: Tạo ra một cookie với setcookie()

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

* Lấy cookie: sử dụng isset() để kiểm tra xem cookie có tồn tại hay không
* Xóa cookie: đặt giá trị của expire hết hạn trước đó một thời điểm

setcookie("user", "", time() - 3600);

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

* Session được dùng để lưu trữ thông tin người dùng trong các biến và được sử dụng trên nhiều trang.
* Lưu session: tạo session session\_start(); và sẽ được lưu trong mảng $\_SESSION[]
* Lấy session: sử dụng isset() kiểm tra session tồn tại trong mảng hay $\_SESSION[] không, rồi truy cập vào
* Xóa session: dùng lệnh session\_unset(); hoặc session\_destroy();

1. ***Bạn hãy so sánh Cookie và Session.***

|  |  |
| --- | --- |
| **Cookie** | **Session** |
| * Lưu trữ trên trình duyệt người dùng * Dữ liệu được lưu trữ máy khách * Dễ dàng sửa đổi, có thể bị đánh cấp hoặc xóa * Có sẵn trên trình duyệt đến khi hết hạn | * Không được lưu trữ trong trình duyệt người dùng * Dữ liệu được lưu trữ ở phía máy chủ * Không dễ dàng sữa đổi hay can thiệp đến dữ liệu * Khi đóng một trình duyệt thì bị mất thông tin 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.
2. 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.
3. ***Bạn đọc trong[[4]](#footnote-4) để tìm hiểu và mô tả các cơ chế, các hàm/thủ tục để thực hiện việc upload.***

* Tạo biểu mẫu cho phép người dùng chọn ảnh upload (Đảm bảo rằng biểu mẫu sử dụng method="post" và enctype="multipart/form-data" thuộc tính type của thẻ input phải là file
* Tạo tập tin upload.php để tải tệp lên

<?php  
$target\_dir = "uploads/";  
$target\_file = $target\_dir . basename($\_FILES["fileToUpload"]["name"]);  
$uploadOk = 1;  
$imageFileType = strtolower(pathinfo($target\_file,PATHINFO\_EXTENSION));  
// Check if image file is a actual image or fake image  
if(isset($\_POST["submit"])) {  
  $check = getimagesize($\_FILES["fileToUpload"]["tmp\_name"]);  
  if($check !== false) {  
    echo "File is an image - " . $check["mime"] . ".";  
    $uploadOk = 1;  
  } else {  
    echo "File is not an image.";  
    $uploadOk = 0;  
  }  
}  
?>

* $ 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 sử dụng sau)
* $imageFileType giữ phần mở rộng tệp của tệp (ở dạng chữ thường)
* Tiếp theo, kiểm tra xem tệp hình ảnh là hình ảnh thật hay hình ảnh giả mạo
* Kiểm tra xem tệp đã tồn tại hay chưa: nếu có thì thông báo lỗi và $uploadOk=0;

// Check if file already exists  
if (file\_exists($target\_file)) {  
  echo "Sorry, file already exists.";  
  $uploadOk = 0;  
}

* Giới hạn kích thước tệp: Nếu kích thước lớn hơn 500KB thì thông báo lỗi và $uploadOk=0;

// Check file size  
if ($\_FILES["fileToUpload"]["size"] > 500000) {  
  echo "Sorry, your file is too large.";  
  $uploadOk = 0;  
}

* Giới hạn loại tệp: cho phép người dùng tải lên các tệp JPG, JPEG, PNG và GIF, tất cả các tệp khác sẽ thông báo lỗi trước kho đặt $uploadOk=0;

// Allow certain file formats  
if($imageFileType != "jpg" && $imageFileType != "png" && $imageFileType != "jpeg"  
&& $imageFileType != "gif" ) {  
  echo "Sorry, only JPG, JPEG, PNG & GIF files are allowed.";  
  $uploadOk = 0;  
}

1. ***Bạn hãy đọc[[5]](#footnote-5), mô tả chức năng của hàm này và các tham số trong hàm (tham khảo thêm từ read-csv.php).***
2. <?php
3. $csv = array();
4. $name\_file = 'cus.csv';
5. $lines = file($name\_file, FILE\_IGNORE\_NEW\_LINES);
6. //dua du lieu tu file csv vao mang:
7. foreach ($lines as $key => $value)
8. {
9. $csv[$key] = str\_getcsv($value);
10. }
11. //in mang
12. echo '<pre>';
13. print\_r($csv);
14. echo '</pre>';
15. ?>

Hàm này dùng để đọc dữ liệu từ file

Khai báo một biến có kiểu mảng

File() đọc một tập tin thành một mảng.

Lines lưu tập tin từ file cus.csv

Foreach: cho chạy vòng lặp từng lines trên các key dữ liệu

Str\_getcsv(): Phân tích chuỗi csv thành mảng

In mảng ra

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-6),[[7]](#footnote-7). 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-1)
2. <https://www.w3schools.com/php/php_cookies.asp> [↑](#footnote-ref-2)
3. <https://www.w3schools.com/php/php_sessions.asp> [↑](#footnote-ref-3)
4. <https://www.w3schools.com/php/php_file_upload.asp> [↑](#footnote-ref-4)
5. <https://www.w3schools.com/php/func_filesystem_file.asp> [↑](#footnote-ref-5)
6. <https://www.php.net/manual/en/features.file-upload.post-method.php>, [↑](#footnote-ref-6)
7. https://stackoverflow.com/questions/6654351/check-file-uploaded-is-in-csv-format [↑](#footnote-ref-7)