**Bài tập thực hành 04**

Lập trình PHP nâng cao

**Mục tiêu cần đạt**:

Sau buổi các bạn cần nắm thao tác sử dụng PHP nâng cao

* Hiểu và biết cách dùng Cookies và Session
* Tạo form đăng nhập và dùng cookies, session để quản lý các đăng nhập, thực hiện chức năng log out (thoát) khỏi hệ thống
* Biết về SQL Injection.
* Upload file, lưu thông tin về tập tin trong CSDL
* Đọc, và xử lý nội dung trong tập tin

Các bạn đọc và thực hiện viết code như hướng dẫn để làm quen, sau đó đọc trả lời các **Yêu cầu** ở dưới bài hướng dẫn để thực hiện yêu cầu bài thực hành.

**Gợi ý Tham khảo:**

* <https://www.w3schools.com/php/>
* và các nguồn khác mà sinh viên tìm được

## Tạo Cookies

Cookies và Session hỗ trợ chúng ta quản lý các phiên đăng nhập/đăng nhập, hoạt động của người dùng trên các website

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

### ck.php

<!DOCTYPE html>

<?php

$cookie\_name = "user";

$cookie\_value = "Nguyen Thanh Hai";

setcookie($cookie\_name, $cookie\_value, time() + (86400 / 24), "/"); // 86400 = 24\*3600 = 1 day

?>

<html>

<body>

<?php

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

echo "Cookie named '" . $cookie\_name . "' chua duoc thiet lap, ban vui long bam f5 de thiet lap cookie!";

} else {

echo "Cookie '" . $cookie\_name . "' da duoc thiet lap!<br>";

echo "Gia tri la: " . $\_COOKIE[$cookie\_name];

}

?>

<p><strong>Note:</strong> You might have to reload the page to see the value of the cookie.</p>

</body>

</html>

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

Tạo csdl qlbanhang, với bảng customers đầu tiên như sau:

CREATE TABLE `customers` (

`id` int(6) UNSIGNED NOT NULL,

`fullname` varchar(50) CHARACTER SET latin1 NOT NULL,

`email` varchar(50) CHARACTER SET latin1 DEFAULT NULL,

`Birthday` date DEFAULT NULL,

`reg\_date` timestamp NOT NULL DEFAULT current\_timestamp() ON UPDATE current\_timestamp(),

`password` varchar(50) NOT NULL

) ENGINE=InnoDB DEFAULT CHARSET=utf8;

Tạo formnhap.php

### formnhap.php

<!DOCTYPE HTML>

<html>

<body>

<form action="luu.php" method="post">

Name: <input type="text" name="name"><br>

E-mail: <input type="text" name="email"><br>

Birthday: <input type="date" name="birth"><br>

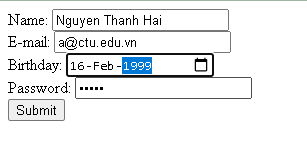
Password: <input type="password" name="pass"><br>

<input type="submit">

</form>

</body>

</html>



Và luu.php, chú ý lúc này chúng ta sẽ mã hóa mật khẩu với giải thuật md5 để bảo mật mật khẩu:

### luu.php

<?php

$servername = "localhost";

$username = "root";

$password = "";

$dbname = "qlbanhang";

// Create connection

$conn = new mysqli($servername, $username, $password, $dbname);

// Check connection

if ($conn->connect\_error) {

die("Connection failed: " . $conn->connect\_error);

}

$date = date\_create($\_POST["birth"]);

$sql = "INSERT INTO customers (fullname, email, birthday, password)

VALUES ('".$\_POST["name"] ."', '".$\_POST["email"] ."', '".$date ->format('Y-m-d') ."','".md5($\_POST["pass"])."' )";

if ($conn->query($sql) == TRUE) {

echo "Them sinh vien thanh cong";

} else {

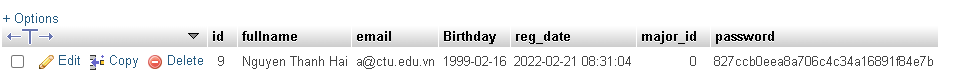
echo "Error: " . $sql . "<br>" . $conn->error;

}

$conn->close();

?>

Sau khi chúng ta nhập xong mật khẩu với 12345 nhưng khi quan sát trong CSDL ta sẽ thấy mật khẩu đã được mã hóa ra chuỗi 827ccb0eea8a706c4c34a16891f84e7b:



Trong trường hợp chúng ta muốn dùng email là username để đăng nhập ta nên đảm bảo 2 student không có email trùng nhau. Để đảm bảo điều này ta có thể chọn email là unique key (vì ta đã chọn id la primary key, và 1 bảng không thể có 2 khóa chính)

[ALTER](http://localhost/phpmyadmin/url.php?url=https://dev.mysql.com/doc/refman/5.5/en/alter-table.html) [TABLE](http://localhost/phpmyadmin/url.php?url=https://dev.mysql.com/doc/refman/5.5/en/alter-table.html) `customers` ADD UNIQUE( `email`);

## Tạo form đăng nhập

Sau khi tạo người dùng xong, ta có thể chạy form đăng nhập với username là email và password lấy từ CSDL

### Login.php

<!DOCTYPE HTML>

<html>

<body>

<form action="log.php" method="post">

Username: <input type="text" name="email"><br>

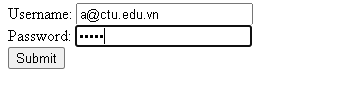
Password: <input type="password" name="pass"><br>

<input type="submit">

</form>

</body>

</html>



### Log.php

<?php

$servername = "localhost";

$username = "root";

$password = "";

$dbname = "qlbanhang";

// Create connection

$conn = new mysqli($servername, $username, $password, $dbname);

// Check connection

if ($conn->connect\_error) {

die("Connection failed: " . $conn->connect\_error);

}

$sql = "select fullname, email from customers where email = '".$\_POST["email"]."' and password = '".md5($\_POST["pass"])."'";

$result = $conn->query($sql);

if ($result->num\_rows > 0) {

echo "Dang nhap thanh cong <br>";

$row = $result->fetch\_assoc();

echo "email:".$row['email']. ' Fullname: '.$row['fullname'];

} else {

echo "Error: " . $sql . "<br>" . $conn->error;

}

$conn->close();

?>

Khi chúng ta nhập sai, nhìn vào thông báo lỗi ta thấy



Mật khẩu đã cho không khớp với mã đã băm

Khi ta nhập đúng



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

Chỉnh sửa lại log.php với code sau để khi đăng nhập thành công chuyển sang 1 trang chủ, còn nếu không đúng thì trở lại trang đăng nhập

### Log.php (modified)

<?php

$servername = "localhost";

$username = "root";

$password = "";

$dbname = "qlbanhang";

// Create connection

$conn = new mysqli($servername, $username, $password, $dbname);

// Check connection

if ($conn->connect\_error) {

die("Connection failed: " . $conn->connect\_error);

}

$sql = "select id, fullname, email from customers where email = '".$\_POST["email"]."' and password = '".md5($\_POST["pass"])."'";

$result = $conn->query($sql);

if ($result->num\_rows > 0) {

$row = $result->fetch\_assoc();

$cookie\_name = "user";

$cookie\_value = $row['email'] ;

setcookie($cookie\_name, $cookie\_value, time() + (86400 / 24), "/");

setcookie("fullname", $row['fullname'], time() + (86400 / 24), "/");

setcookie("id", $row['id'], time() + (86400 / 24), "/");

header('Location: homepage.php');

} else {

echo "Error: " . $sql . "<br>" . $conn->error;

//Tro ve trang dang nhap sau 3 giay

header('Refresh: 3;url=login.php');

}

$conn->close();

?>

Tạo 1 trang chủ để khi đăng nhập thành công chuyển qua trang chủ này:

### Homepage.php

<!DOCTYPE html>

<html>

<title>W3.CSS Template</title>

<meta charset="UTF-8">

<meta name="viewport" content="width=device-width, initial-scale=1">

<link rel="stylesheet" href="https://www.w3schools.com/w3css/4/w3.css">

<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Roboto">

<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Montserrat">

<link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.min.css">

<style>

.w3-sidebar a {font-family: "Roboto", sans-serif}

body,h1,h2,h3,h4,h5,h6,.w3-wide {font-family: "Montserrat", sans-serif;}

</style>

<body class="w3-content" style="max-width:1200px">

<!-- Sidebar/menu -->

<nav class="w3-sidebar w3-bar-block w3-white w3-collapse w3-top" style="z-index:3;width:250px" id="mySidebar">

<div class="w3-container w3-display-container w3-padding-16">

<i onclick="w3\_close()" class="fa fa-remove w3-hide-large w3-button w3-display-topright"></i>

<h3 class="w3-wide"><b>

<?php

$cookie\_name = "**fullname**";

echo 'Chao ban '.$\_COOKIE[$cookie\_name];

?>

</b></h3>

</div>

<div class="w3-padding-64 w3-large w3-text-grey" style="font-weight:bold">

<a href="#" class="w3-bar-item w3-button">Shirts</a>

<a href="#" class="w3-bar-item w3-button">Dresses</a>

<div id="demoAcc" class="w3-bar-block w3-hide w3-padding-large w3-medium">

<a href="#" class="w3-bar-item w3-button w3-light-grey"><i class="fa fa-caret-right w3-margin-right"></i>Skinny</a>

<a href="#" class="w3-bar-item w3-button">Relaxed</a>

<a href="#" class="w3-bar-item w3-button">Bootcut</a>

<a href="#" class="w3-bar-item w3-button">Straight</a>

</div>

<a href="#" class="w3-bar-item w3-button">Jackets</a>

<a href="#" class="w3-bar-item w3-button">Gymwear</a>

<a href="#" class="w3-bar-item w3-button">Blazers</a>

<a href="#" class="w3-bar-item w3-button">Shoes</a>

</div>

<a href="#footer" class="w3-bar-item w3-button w3-padding">Contact</a>

<a href="javascript:void(0)" class="w3-bar-item w3-button w3-padding" onclick="document.getElementById('newsletter').style.display='block'">Newsletter</a>

<a href="#footer" class="w3-bar-item w3-button w3-padding">Subscribe</a>

</nav>

<!-- Top menu on small screens -->

<header class="w3-bar w3-top w3-hide-large w3-black w3-xlarge">

<div class="w3-bar-item w3-padding-24 w3-wide">LOGO</div>

<a href="javascript:void(0)" class="w3-bar-item w3-button w3-padding-24 w3-right" onclick="w3\_open()"><i class="fa fa-bars"></i></a>

</header>

<!-- Overlay effect when opening sidebar on small screens -->

<div class="w3-overlay w3-hide-large" onclick="w3\_close()" style="cursor:pointer" title="close side menu" id="myOverlay"></div>

<!-- !PAGE CONTENT! -->

<div class="w3-main" style="margin-left:250px">

<!-- Push down content on small screens -->

<div class="w3-hide-large" style="margin-top:83px"></div>

<!-- Top header -->

<header class="w3-container w3-xlarge">

<p class="w3-right">

<i class="fa fa-shopping-cart w3-margin-right"></i>

<i class="fa fa-search"></i>

</p>

</header>

<div class="w3-container w3-text-grey" id="jeans">

<p>8 items</p>

</div>

<!-- Subscribe section -->

<div class="w3-container w3-black w3-padding-32">

<h1>Subscribe</h1>

<p>To get special offers and VIP treatment:</p>

<p><input class="w3-input w3-border" type="text" placeholder="Enter e-mail" style="width:100%"></p>

<button type="button" class="w3-button w3-red w3-margin-bottom">Subscribe</button>

</div>

<!-- Footer -->

<footer class="w3-padding-64 w3-light-grey w3-small w3-center" id="footer">

<div class="w3-row-padding">

<div class="w3-col s4">

<h4>Contact</h4>

<p>Questions? Go ahead.</p>

<form action="/action\_page.php" target="\_blank">

<p><input class="w3-input w3-border" type="text" placeholder="Name" name="Name" required></p>

<p><input class="w3-input w3-border" type="text" placeholder="Email" name="Email" required></p>

<p><input class="w3-input w3-border" type="text" placeholder="Subject" name="Subject" required></p>

<p><input class="w3-input w3-border" type="text" placeholder="Message" name="Message" required></p>

<button type="submit" class="w3-button w3-block w3-black">Send</button>

</form>

</div>

<div class="w3-col s4">

<h4>About</h4>

<p><a href="#">About us</a></p>

<p><a href="#">We're hiring</a></p>

<p><a href="#">Support</a></p>

<p><a href="#">Find store</a></p>

<p><a href="#">Shipment</a></p>

<p><a href="#">Payment</a></p>

<p><a href="#">Gift card</a></p>

<p><a href="#">Return</a></p>

<p><a href="#">Help</a></p>

</div>

<div class="w3-col s4 w3-justify">

<h4>Store</h4>

<p><i class="fa fa-fw fa-map-marker"></i> Company Name</p>

<p><i class="fa fa-fw fa-phone"></i> 0044123123</p>

<p><i class="fa fa-fw fa-envelope"></i> ex@mail.com</p>

<h4>We accept</h4>

<p><i class="fa fa-fw fa-cc-amex"></i> Amex</p>

<p><i class="fa fa-fw fa-credit-card"></i> Credit Card</p>

<br>

<i class="fa fa-facebook-official w3-hover-opacity w3-large"></i>

<i class="fa fa-instagram w3-hover-opacity w3-large"></i>

<i class="fa fa-snapchat w3-hover-opacity w3-large"></i>

<i class="fa fa-pinterest-p w3-hover-opacity w3-large"></i>

<i class="fa fa-twitter w3-hover-opacity w3-large"></i>

<i class="fa fa-linkedin w3-hover-opacity w3-large"></i>

</div>

</div>

</footer>

<div class="w3-black w3-center w3-padding-24">Powered by <a href="https://www.w3schools.com/w3css/default.asp" title="W3.CSS" target="\_blank" class="w3-hover-opacity">w3.css</a></div>

<!-- End page content -->

</div>

<!-- Newsletter Modal -->

<div id="newsletter" class="w3-modal">

<div class="w3-modal-content w3-animate-zoom" style="padding:32px">

<div class="w3-container w3-white w3-center">

<i onclick="document.getElementById('newsletter').style.display='none'" class="fa fa-remove w3-right w3-button w3-transparent w3-xxlarge"></i>

<h2 class="w3-wide">NEWSLETTER</h2>

<p>Join our mailing list to receive updates on new arrivals and special offers.</p>

<p><input class="w3-input w3-border" type="text" placeholder="Enter e-mail"></p>

<button type="button" class="w3-button w3-padding-large w3-red w3-margin-bottom" onclick="document.getElementById('newsletter').style.display='none'">Subscribe</button>

</div>

</div>

</div>

<script>

// Accordion

function myAccFunc() {

var x = document.getElementById("demoAcc");

if (x.className.indexOf("w3-show") == -1) {

x.className += " w3-show";

} else {

x.className = x.className.replace(" w3-show", "");

}

}

// Click on the "Jeans" link on page load to open the accordion for demo purposes

document.getElementById("myBtn").click();

// Open and close sidebar

function w3\_open() {

document.getElementById("mySidebar").style.display = "block";

document.getElementById("myOverlay").style.display = "block";

}

function w3\_close() {

document.getElementById("mySidebar").style.display = "none";

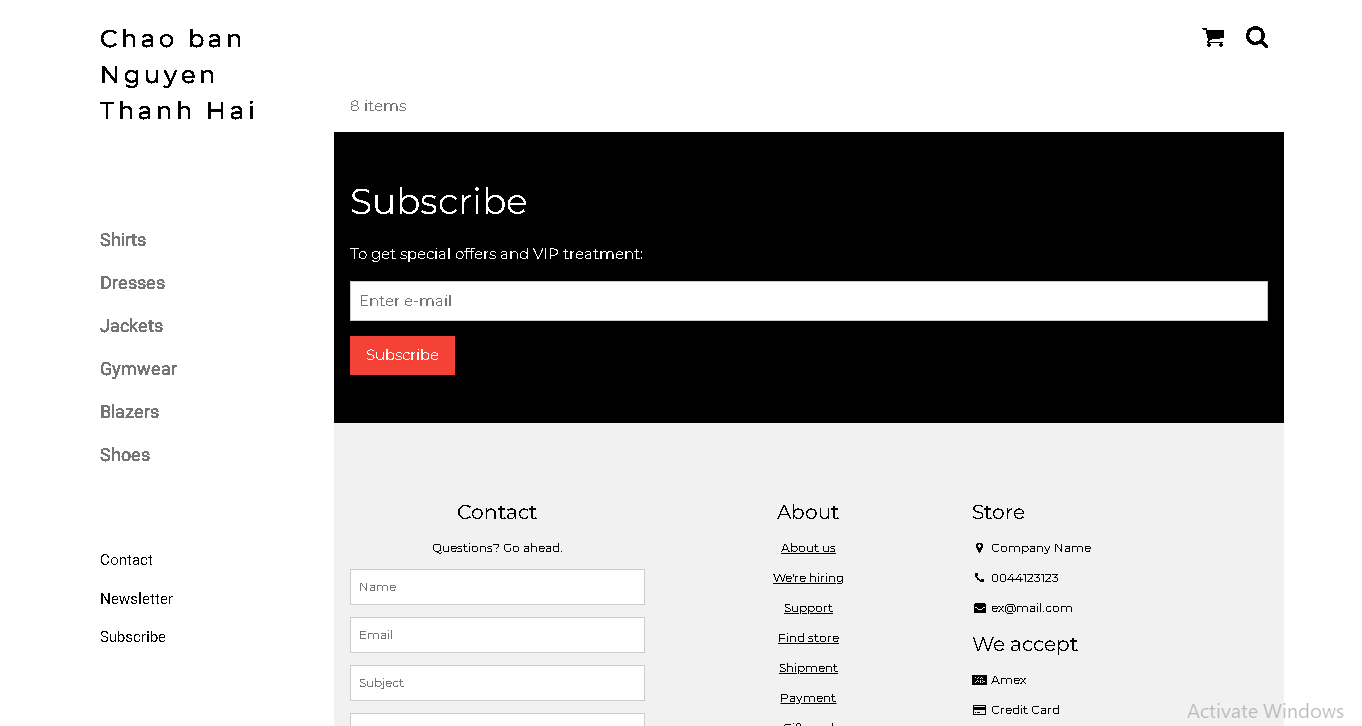
document.getElementById("myOverlay").style.display = "none";

}

</script>

</body>

</html>



## Upload tập tin

Upload file, chúng ta tạo form giao diện để upload file ảnh upload-img.php

### Upload-img.php

<!DOCTYPE html>

<html>

<body>

<form action="upload.php" method="post" enctype="multipart/form-data">

Ban chon 1 anh de lam profile:

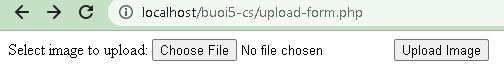
<input type="file" name="fileToUpload" id="fileToUpload">

<input type="submit" value="Upload Image" name="submit">

</form>

</body>

</html>



Tập tin upload.php xử lý hành động

### upload.php

<?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;

}

}

// Check if file already exists

if (file\_exists($target\_file)) {

echo "Sorry, file already exists.";

$uploadOk = 0;

}

// Check file size

if ($\_FILES["fileToUpload"]["size"] > 500000) {

echo "Sorry, your file is too large.";

$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;

}

// Check if $uploadOk is set to 0 by an error

if ($uploadOk == 0) {

echo "Sorry, your file was not uploaded.";

// if everything is ok, try to upload file

} else {

if (move\_uploaded\_file($\_FILES["fileToUpload"]["tmp\_name"], $target\_file)) {

echo "The file ". htmlspecialchars( basename( $\_FILES["fileToUpload"]["name"])). " has been uploaded.";

} else {

echo "Sorry, there was an error uploading your file.";

}

}

?>

Sau khi chúng ta upload thành công giao diện sau sẽ hiển thị



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

Trong phần này chúng ta minh họa tải tập tin ảnh làm ảnh profile của người dùng

### Upload-img.php (modified)

<!DOCTYPE html>

<html>

<body>

<form action="upload-csdl.php" method="post" enctype="multipart/form-data">

Ban chon 1 anh de lam profile:

<input type="file" name="fileToUpload" id="fileToUpload">

<input type="submit" value="Upload Image" name="submit">

</form>

</body>

</html>

Thêm cột để lưu đường dẫn ảnh:

[ALTER](http://localhost/phpmyadmin/url.php?url=https://dev.mysql.com/doc/refman/5.5/en/alter-table.html) [TABLE](http://localhost/phpmyadmin/url.php?url=https://dev.mysql.com/doc/refman/5.5/en/alter-table.html) `customers` ADD `img\_profile` [VARCHAR](http://localhost/phpmyadmin/url.php?url=https://dev.mysql.com/doc/refman/5.5/en/string-types.html)(100);

### Upload-csdl.php

<?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;

}

}

// Check if file already exists

if (file\_exists($target\_file)) {

echo "Sorry, file already exists.";

$uploadOk = 0;

}

// Check file size

if ($\_FILES["fileToUpload"]["size"] > 500000) {

echo "Sorry, your file is too large.";

$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;

}

// Check if $uploadOk is set to 0 by an error

if ($uploadOk == 0) {

echo "Sorry, your file was not uploaded.";

// if everything is ok, try to upload file

} else {

if (move\_uploaded\_file($\_FILES["fileToUpload"]["tmp\_name"], $target\_file)) {

echo "The file ". htmlspecialchars( basename( $\_FILES["fileToUpload"]["name"])). " has been uploaded.";

echo '<br>';

$servername = "localhost";

$username = "root";

$password = "";

$dbname = "qlbanhang";

// Create connection

$conn = new mysqli($servername, $username, $password, $dbname);

// Check connection

if ($conn->connect\_error) {

die("Connection failed: " . $conn->connect\_error);

}

$id = $\_COOKIE['id'];

$sql = "UPDATE customers set img\_profile = '".$\_FILES["fileToUpload"]["name"]."'";

$sql = $sql. " WHERE ID='".$id."'";

echo $sql;

if ($conn->query($sql) == TRUE) {

echo 'cap nhat csdl thanh cong!<br>';

echo '<a href="homepage.php">Trang chu</a>';

} else {

echo "Error: " . $sql . "<br>" . $conn->error;

}

} else {

echo "Sorry, there was an error uploading your file.";

}

}

?>

### Homepage.php (modified với ảnh profile)

<!DOCTYPE html>

<html>

<title>W3.CSS Template</title>

<meta charset="UTF-8">

<meta name="viewport" content="width=device-width, initial-scale=1">

<link rel="stylesheet" href="https://www.w3schools.com/w3css/4/w3.css">

<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Roboto">

<link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Montserrat">

<link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-awesome.min.css">

<style>

.w3-sidebar a {font-family: "Roboto", sans-serif}

body,h1,h2,h3,h4,h5,h6,.w3-wide {font-family: "Montserrat", sans-serif;}

</style>

<body class="w3-content" style="max-width:1200px">

<!-- Sidebar/menu -->

<nav class="w3-sidebar w3-bar-block w3-white w3-collapse w3-top" style="z-index:3;width:250px" id="mySidebar">

<div class="w3-container w3-display-container w3-padding-16">

<i onclick="w3\_close()" class="fa fa-remove w3-hide-large w3-button w3-display-topright"></i>

<h3 class="w3-wide"><b>

<?php

$cookie\_name = "fullname";

echo 'Chao ban '.$\_COOKIE[$cookie\_name];

//them doan nay de lay duong dan anh

$servername = "localhost";

$username = "root";

$password = "";

$dbname = "qlbanhang";

// Create connection

$conn = new mysqli($servername, $username, $password, $dbname);

// Check connection

if ($conn->connect\_error) {

die("Connection failed: " . $conn->connect\_error);

}

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

//echo $sql;

$result = $conn->query($sql);

//print\_r($result);

if ( $result->num\_rows > 0) {

//lay link anh tu csdl da luu de hien thi cac anh duoc luu trong uploads

$row = $result->fetch\_assoc();

echo '<img src="'.'./uploads/'.$row['img\_profile'].'" alt="Anh profile">';

}

?>

</b></h3>

</div>

<div class="w3-padding-64 w3-large w3-text-grey" style="font-weight:bold">

<a href="#" class="w3-bar-item w3-button">Shirts</a>

<a href="#" class="w3-bar-item w3-button">Dresses</a>

<div id="demoAcc" class="w3-bar-block w3-hide w3-padding-large w3-medium">

<a href="#" class="w3-bar-item w3-button w3-light-grey"><i class="fa fa-caret-right w3-margin-right"></i>Skinny</a>

<a href="#" class="w3-bar-item w3-button">Relaxed</a>

<a href="#" class="w3-bar-item w3-button">Bootcut</a>

<a href="#" class="w3-bar-item w3-button">Straight</a>

</div>

<a href="#" class="w3-bar-item w3-button">Jackets</a>

<a href="#" class="w3-bar-item w3-button">Gymwear</a>

<a href="#" class="w3-bar-item w3-button">Blazers</a>

<a href="#" class="w3-bar-item w3-button">Shoes</a>

</div>

<a href="#footer" class="w3-bar-item w3-button w3-padding">Contact</a>

<a href="javascript:void(0)" class="w3-bar-item w3-button w3-padding" onclick="document.getElementById('newsletter').style.display='block'">Newsletter</a>

<a href="#footer" class="w3-bar-item w3-button w3-padding">Subscribe</a>

</nav>

<!-- Top menu on small screens -->

<header class="w3-bar w3-top w3-hide-large w3-black w3-xlarge">

<div class="w3-bar-item w3-padding-24 w3-wide">LOGO</div>

<a href="javascript:void(0)" class="w3-bar-item w3-button w3-padding-24 w3-right" onclick="w3\_open()"><i class="fa fa-bars"></i></a>

</header>

<!-- Overlay effect when opening sidebar on small screens -->

<div class="w3-overlay w3-hide-large" onclick="w3\_close()" style="cursor:pointer" title="close side menu" id="myOverlay"></div>

<!-- !PAGE CONTENT! -->

<div class="w3-main" style="margin-left:250px">

<!-- Push down content on small screens -->

<div class="w3-hide-large" style="margin-top:83px"></div>

<!-- Top header -->

<header class="w3-container w3-xlarge">

<p class="w3-right">

<i class="fa fa-shopping-cart w3-margin-right"></i>

<i class="fa fa-search"></i>

</p>

</header>

<div class="w3-container w3-text-grey" id="jeans">

<p>8 items</p>

</div>

<!-- Subscribe section -->

<div class="w3-container w3-black w3-padding-32">

<h1>Subscribe</h1>

<p>To get special offers and VIP treatment:</p>

<p><input class="w3-input w3-border" type="text" placeholder="Enter e-mail" style="width:100%"></p>

<button type="button" class="w3-button w3-red w3-margin-bottom">Subscribe</button>

</div>

<!-- Footer -->

<footer class="w3-padding-64 w3-light-grey w3-small w3-center" id="footer">

<div class="w3-row-padding">

<div class="w3-col s4">

<h4>Contact</h4>

<p>Questions? Go ahead.</p>

<form action="/action\_page.php" target="\_blank">

<p><input class="w3-input w3-border" type="text" placeholder="Name" name="Name" required></p>

<p><input class="w3-input w3-border" type="text" placeholder="Email" name="Email" required></p>

<p><input class="w3-input w3-border" type="text" placeholder="Subject" name="Subject" required></p>

<p><input class="w3-input w3-border" type="text" placeholder="Message" name="Message" required></p>

<button type="submit" class="w3-button w3-block w3-black">Send</button>

</form>

</div>

<div class="w3-col s4">

<h4>About</h4>

<p><a href="#">About us</a></p>

<p><a href="#">We're hiring</a></p>

<p><a href="#">Support</a></p>

<p><a href="#">Find store</a></p>

<p><a href="#">Shipment</a></p>

<p><a href="#">Payment</a></p>

<p><a href="#">Gift card</a></p>

<p><a href="#">Return</a></p>

<p><a href="#">Help</a></p>

</div>

<div class="w3-col s4 w3-justify">

<h4>Store</h4>

<p><i class="fa fa-fw fa-map-marker"></i> Company Name</p>

<p><i class="fa fa-fw fa-phone"></i> 0044123123</p>

<p><i class="fa fa-fw fa-envelope"></i> ex@mail.com</p>

<h4>We accept</h4>

<p><i class="fa fa-fw fa-cc-amex"></i> Amex</p>

<p><i class="fa fa-fw fa-credit-card"></i> Credit Card</p>

<br>

<i class="fa fa-facebook-official w3-hover-opacity w3-large"></i>

<i class="fa fa-instagram w3-hover-opacity w3-large"></i>

<i class="fa fa-snapchat w3-hover-opacity w3-large"></i>

<i class="fa fa-pinterest-p w3-hover-opacity w3-large"></i>

<i class="fa fa-twitter w3-hover-opacity w3-large"></i>

<i class="fa fa-linkedin w3-hover-opacity w3-large"></i>

</div>

</div>

</footer>

<div class="w3-black w3-center w3-padding-24">Powered by <a href="https://www.w3schools.com/w3css/default.asp" title="W3.CSS" target="\_blank" class="w3-hover-opacity">w3.css</a></div>

<!-- End page content -->

</div>

<!-- Newsletter Modal -->

<div id="newsletter" class="w3-modal">

<div class="w3-modal-content w3-animate-zoom" style="padding:32px">

<div class="w3-container w3-white w3-center">

<i onclick="document.getElementById('newsletter').style.display='none'" class="fa fa-remove w3-right w3-button w3-transparent w3-xxlarge"></i>

<h2 class="w3-wide">NEWSLETTER</h2>

<p>Join our mailing list to receive updates on new arrivals and special offers.</p>

<p><input class="w3-input w3-border" type="text" placeholder="Enter e-mail"></p>

<button type="button" class="w3-button w3-padding-large w3-red w3-margin-bottom" onclick="document.getElementById('newsletter').style.display='none'">Subscribe</button>

</div>

</div>

</div>

<script>

// Accordion

function myAccFunc() {

var x = document.getElementById("demoAcc");

if (x.className.indexOf("w3-show") == -1) {

x.className += " w3-show";

} else {

x.className = x.className.replace(" w3-show", "");

}

}

// Click on the "Jeans" link on page load to open the accordion for demo purposes

document.getElementById("myBtn").click();

// Open and close sidebar

function w3\_open() {

document.getElementById("mySidebar").style.display = "block";

document.getElementById("myOverlay").style.display = "block";

}

function w3\_close() {

document.getElementById("mySidebar").style.display = "none";

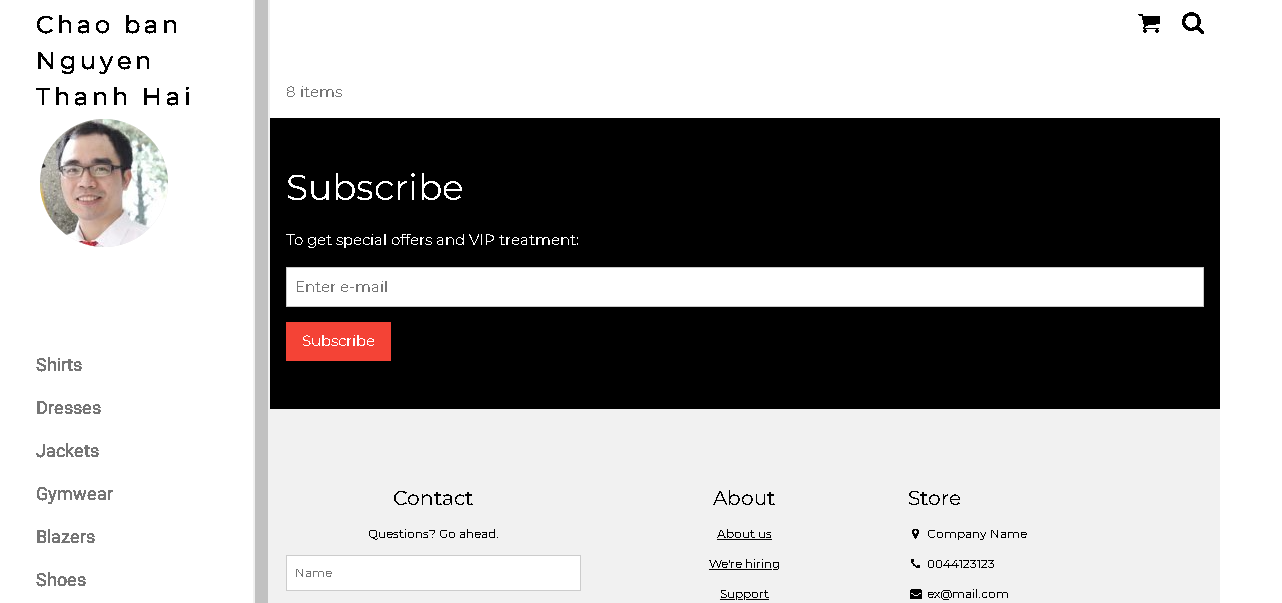
document.getElementById("myOverlay").style.display = "none";

}

</script>

</body>

</html>



Ở đây do biểu diễn từng bước nên đoạn này chúng ta lấy dữ liệu link ảnh profile từ id của người dùng. Trong thực tế, các bạn có thể lưu link ảnh profile vào cookie/session ngay từ khi đăng nhập.

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

Thao tác đọc dữ liệu từ các tập tin là quan trọng, giúp chúng ta backup dữ liệu và phục hồi hay import dữ liệu từ các hệ thống khác. Ví dụ dưới đây giúp minh họa cho các bạn thao tác đọc dữ liệu từ tập tin csv và từ đó đưa vào mảng để phục vụ cho việc xử lý.

### read-csv.php

<?php

$csv = array();

$name\_file = 'cus.csv';

$lines = file($name\_file, FILE\_IGNORE\_NEW\_LINES);

//dua du lieu tu file csv vao mang:

foreach ($lines as $key => $value)

{

$csv[$key] = str\_getcsv($value);

}

//in mang

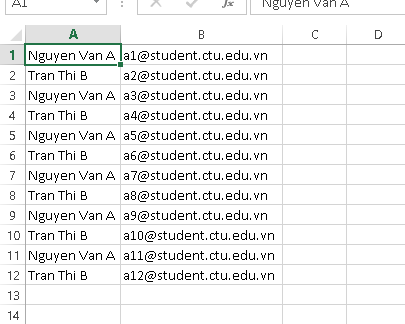
echo '<pre>';

print\_r($csv);

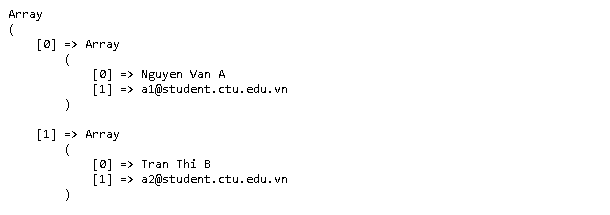
echo '</pre>';

?>

Tạo tập tin cus.csv với dữ liệu như sau



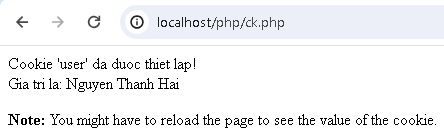
Khi chạy code đọc trên ta sẽ có dữ liệu đã được đưa vào mảng và hiển thị



# Yêu cầu bài thực hành:

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

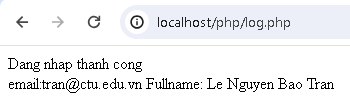
* Kết quả tập tin ck.php :



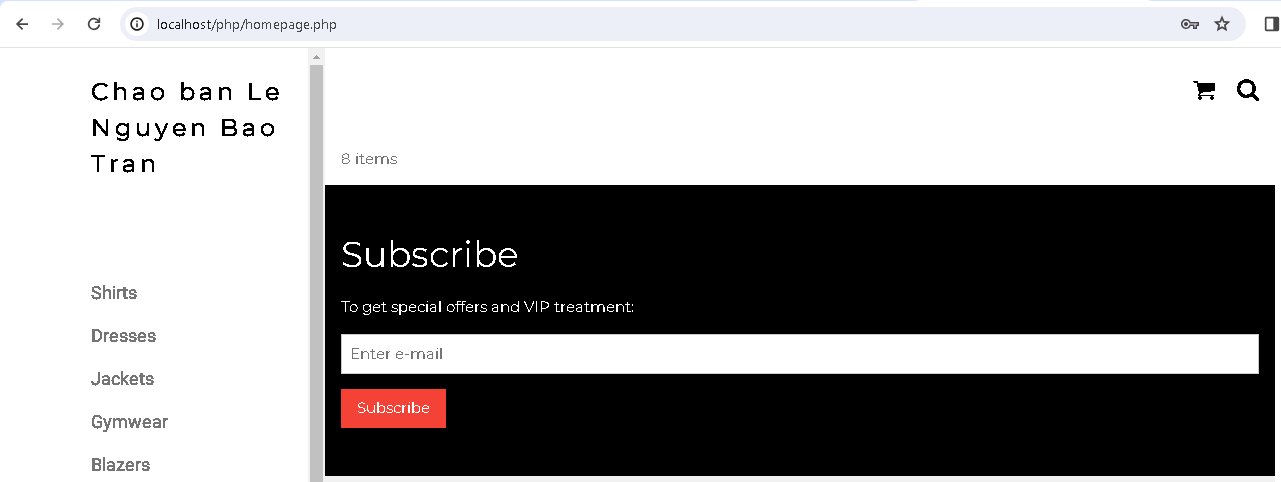
* Kết quả tạo một trang đăng ký người dùng với mật khẩu được mã hóa :



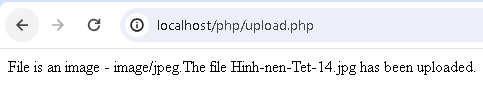
* Kết quả tạo form nhập :



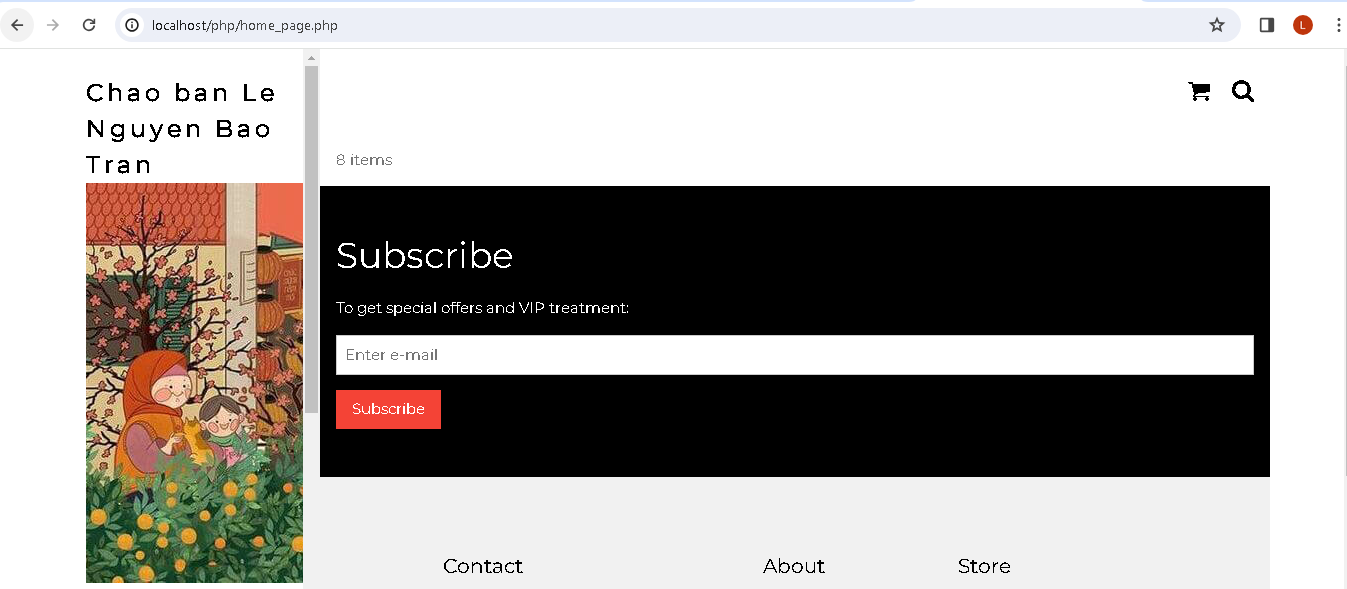
* Kết quả dùng cookies lưu lại tên đăng nhập , email và điều hướng :



* Kết quả upload tập tin :



* Kết quả upload ảnh và lưu dữ liệu về ảnh trong CSDL:



* Kết quả upload file csv và đọc dữ liệu vào mảng :



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.

* SQL là một kỹ thuật chèn mã có thể phá hủy cơ sở dữ liệu của bạn.
* SQL là một trong những kỹ thuật hack web phổ biến nhất.
* SQL là việc đặt mã độc vào 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.

* Cookie thường được sử dụng để nhận dạng người dùng. Cookie là một tệp nhỏ mà máy chủ nhúng vào máy tính của người dùng. Mỗi lần máy tính đó yêu cầu một trang bằng trình duyệt, nó cũng sẽ gửi cookie. Với PHP, bạn có thể vừa tạo vừa truy xuất các giá trị cookie.
* Cú pháp : setcookie(*name, value, expire, path, domain, secure, httponly*);
* Trong đó :
* name : tên của cookie , bắt buộc có
* value: Giá trị của cookie
* expire : Thời gian hết hạn của cookie
* path : Đường dẫn đến cookie . Nếu không có tham số này cookie sẽ chỉ có hiệu lực đối với trang web hiện tại
* domain : Tên miền mà cookie sẽ có hiệu lực
* secure: Nếu tham số này được đặt là true , cookie sẽ được gửi qua HTTPS
* httponly : Nếu tham số này được đặt là true , cookie chỉ có thể truy cập từ máy chủ và không thể truy cập từ javascript
* Cách lấy giá trị trong cookie sử dụng cú pháp :

$\_COOKIE[$name];

* Cách xóa giá trị trong cookie :

Để xóa cookie, sử dụng setcookie() hàm có ngày hết hạn trong quá khứ

* Để lưu trữ Cookie ta dùng cú pháp sau và phải đặt trước thẻ html: setcookie($name, $value, $expire, $path, $domain).

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

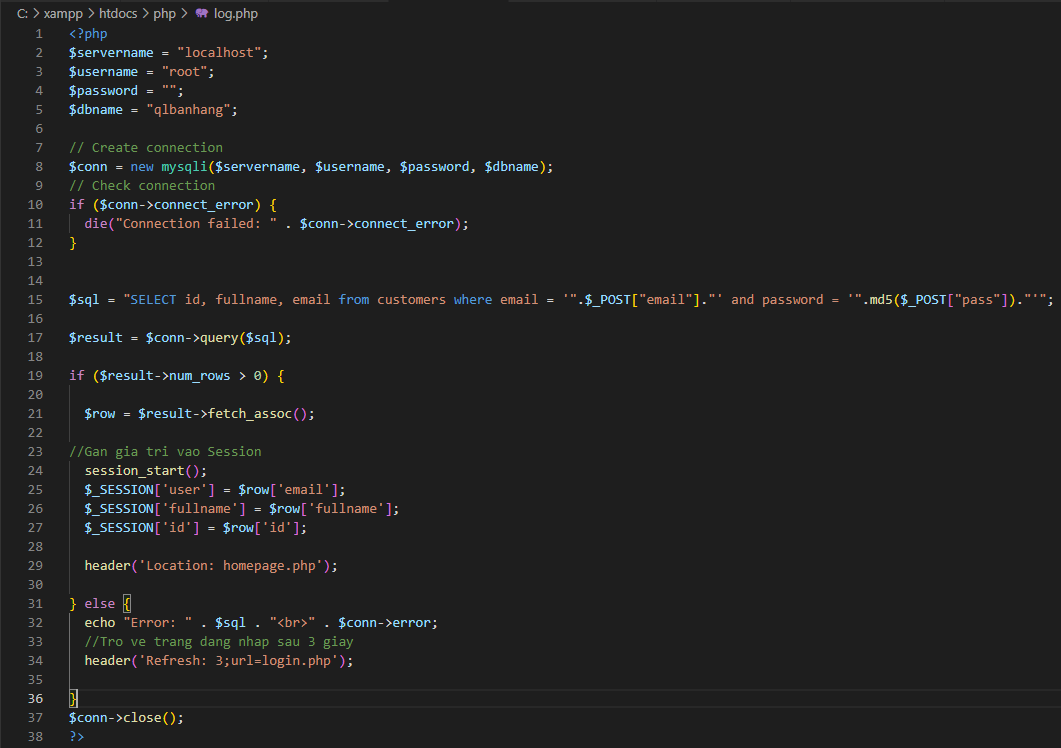
* Biến Session trong PHP được dùng để lưu trữ thông tin của người dùng hoặc là lưu trữ tùy chọn cấu hình hệ thống cho người dùng
* Để lưu một giá trị mới vào Session ta dùng cú pháp như sau:$\_SESSION['session\_name'] = $session\_value
* Để xóa dùng hàm : unset($\_SESSION['name']);

1. Bạn hãy so sánh Cookie và Session.

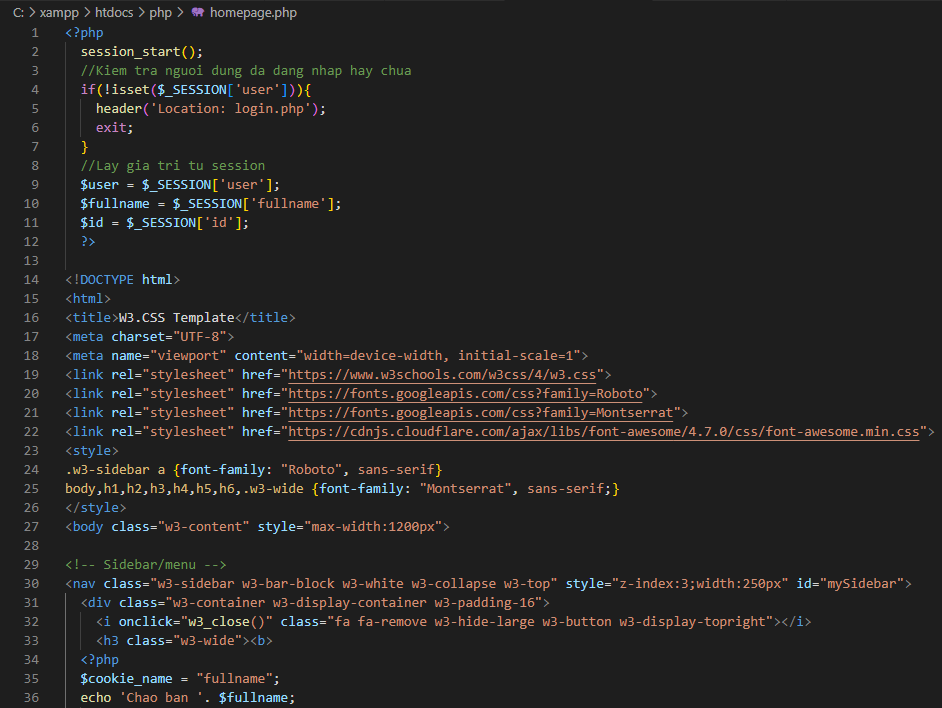
| Cookie | Session |
| --- | --- |
| Lưu trữ trên trình duyệt của người dùng | Không được lưu trữ trong trình duyệt của người dùng |
| Dữ liệu cookie được lưu trữ ở phía máy khách | Dữ liệu session được lưu trữ ở phía máy chủ |
| Dữ liệu cookie dễ dàng sửa đổi khi chúng được lưu trữ ở phía khách hàng | 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 |

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.

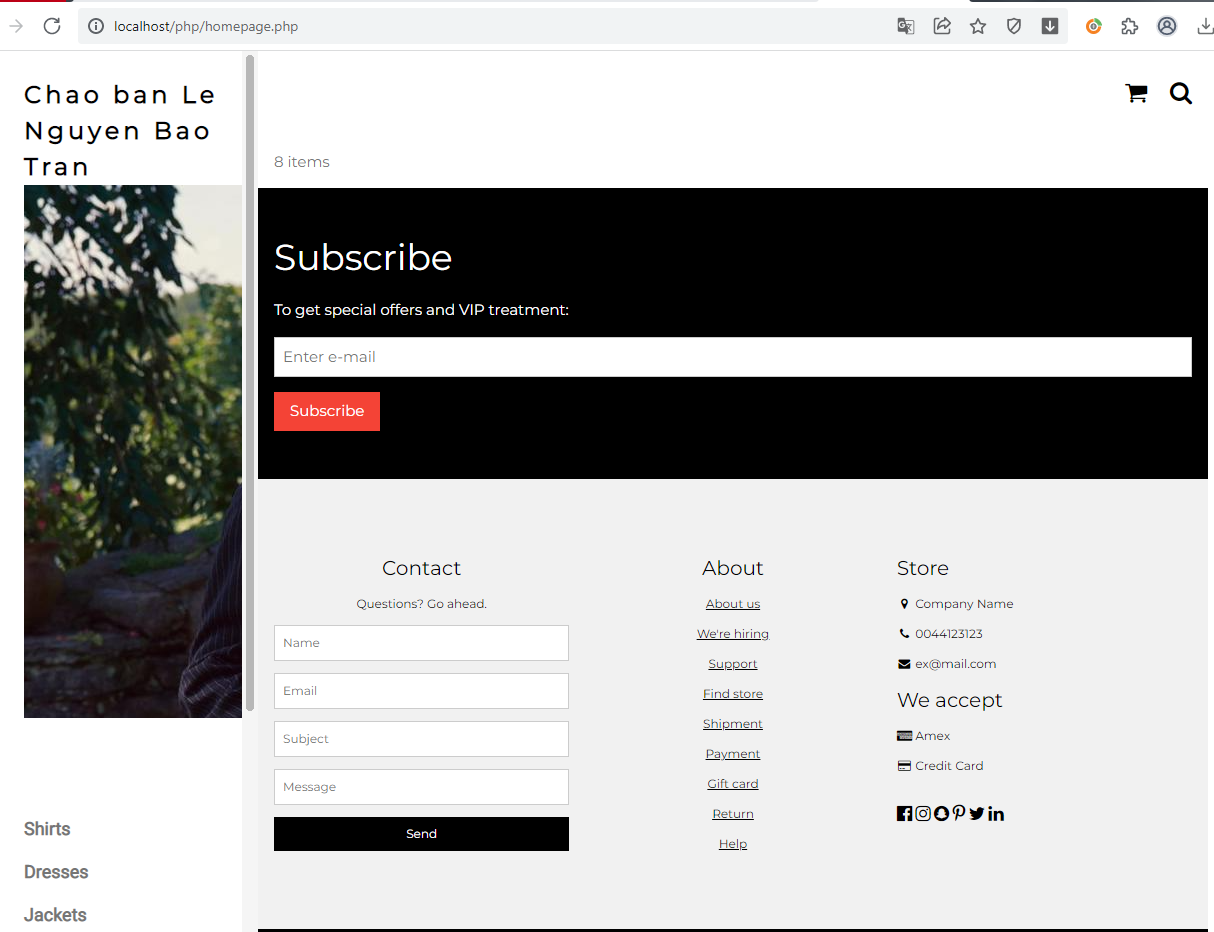
* Sửa log.php:



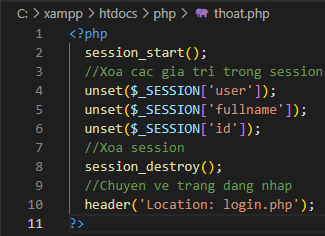
* Sửa tập tin homepage.php:



* Kết quả :

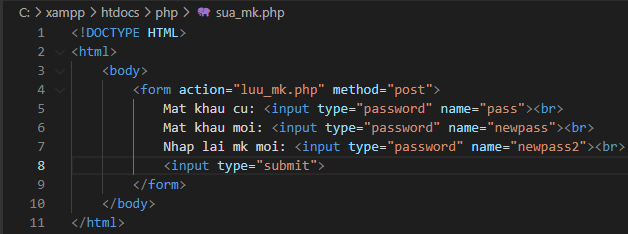


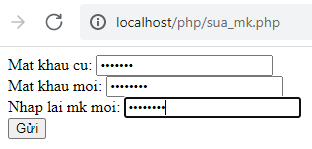
* Tập tin thoat.php:



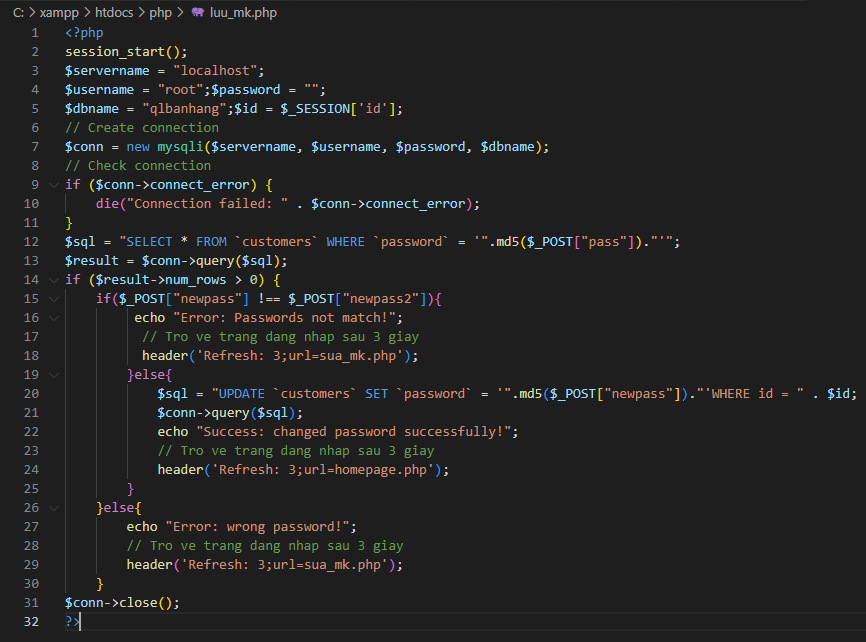
1. Bạn hãy tạo form sua\_mk.php cho phép người dùng chỉnh sửa mật khẩu sau khi đăng nhập. Yêu cầu gồm 3 input: ô để nhập mật khẩu cũ, 1 ô để nhập mật khẩu mới, 1 ô cho phép nhập mật lại mật khẩu mới. Khi nhập xong cần đảm bảo: mật khẩu cũ là khớp với CSDL đang lưu, 2 ô nhập mật khẩu mới phải khớp với 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.

* Tập tin sua\_mk.php:





* Tập tin luu\_mk.php:



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

Upload file Xử lý upload file là công việc mà chúng ta thường xuyên gặp nhất khi làm việc với file và form upload file cũng là nơi để hacker dễ dàng khai thác lỗ hỏng nhằm upload shellscript lên trên webserver. Vì vậy chúng ta cần kiểm tra kỹ định dạng file trước khi di chuyển nó sang thư mục được chỉ định trên website.

Một số hàm thường sử dụng để xử lý file và thư mục trong PHP

1. is\_file($path): trả về TRUE nếu $path tồn tại và là một file
2. is\_dir($path): trả về TRUE nếu $path tồn tại và là một thư mục
3. file\_exists($path): trả về TRUE nếu $path tồn tại và là một file hoặc thư mục
4. getcwd(): trả về chuỗi biểu diễn thư mục hiện tại đang làm việc
5. scandir($path): trả về một mảng chứa danh sách file và thư mục trong đường dẫn $path nếu $path là tên 1 thư mục tồn tại, nếu không trả về FALSE Chúng ta xem qua một ví dụ đơn giản liệt kê các file và thư mục hiện hành

Để đọc file chúng ta sử dụng hàm fread($file, $length) và để ghi file chúng ta sử dụng hàm fwrite($file, $data).

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).

* Đọc file trong PHP:
* Đọc một tập tin vào một mảng:

<?php

print\_r(file("test.txt"));

?>

* Cú pháp : file(*filename*, *flag*, *context*)
* Trong đó :

filename: Yêu cầu. Chỉ định đường dẫn tới file cần đọc

flag : Không bắt buộc. Có thể là một hoặc nhiều hằng số sau:

FILE\_USE\_INCLUDE\_PATH - Tìm kiếm tệp trong include\_path (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 việc xử lý tập tin. Ngữ cảnh là một tập hợp các tùy chọn có thể sửa đổi hành vi của luồng. Có thể 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.

# Chú ý:

* Các bạn nộp file word: Đặt tên file: <mssv><hoten><bai4>.docx nộp lên classroom, kèm với các file code đã tạo (**ngoại trừ file word trả lời câu hỏi, các file còn lại các bạn nén vào file .zip**).
* Mỗi câu các bạn trả lời bằng hình/trả lời dạng text tùy vào yêu cầu của câu hỏi, và ghi rõ số thứ tự câu hỏi mà bạn trả lời.
* Các bài phát hiện copy từ các bài của bạn khác sẽ không được tính điểm.
* *Chú ý: Các câu trả lời có tham khảo trên Internet phải trích dẫn link*

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)