Bài tập thực hành 04

Lập trình PHP nâng cao

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>

A screenshot of a computer

Description automatically generated

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

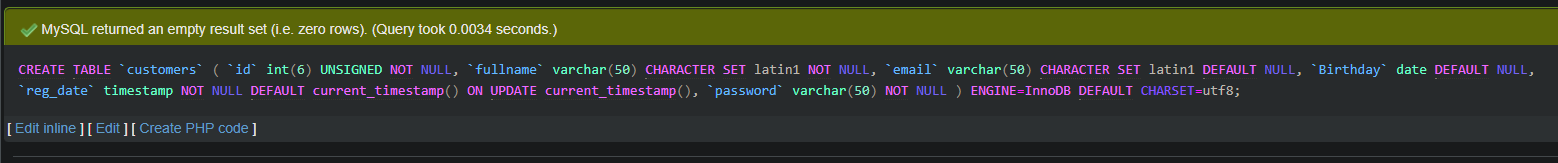
current\_timestamp(),

`password` varchar(50) NOT NULL

) ENGINE=InnoDB DEFAULT CHARSET=utf8;

A screenshot of a computer

Description automatically generated



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>

A screenshot of a computer

Description automatically generated A screenshot of a computer

Description automatically generated

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"] ."', '".$date ->format('Y-md') ."','".md5($\_POST["pass"])."' )";

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

echo "Them sinh vien thanh cong";

} else {

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

}

$conn->close();

?>

A screenshot of a phone

Description automatically generated  
A screenshot of a computer

Description automatically generated

Sau khi chúng ta nhập xong mật khẩu với 123456 nhưng khi quan sát trong CSDL ta sẽ thấy mật

khẩu đã được mã hóa ra chuỗi e10adc3949ba59abbe56e057f20f883e:

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 TABLE `customers` ADD UNIQUE( `email`);

A screenshot of a computer

Description automatically generated

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();

?>

A screenshot of a computer

Description automatically generated

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;

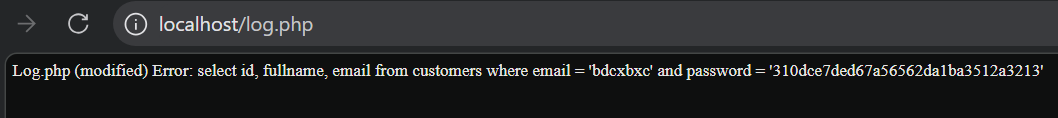
//Tro ve trang dang nhap sau 3 giay

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

}

$conn->close();

?>



A screenshot of a computer

Description automatically generated

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/fontawesome.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="zindex: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-displaytopright"></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>

A screenshot of a computer

Description automatically generated

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/formdata">

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>

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

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:

A screenshot of a computer program

Description automatically generated

ALTER TABLE `customers` ADD `img\_profile` VARCHAR(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.";

}

}

?>

A screen shot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

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/fontawesome.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="zindex: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-displaytopright"></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>

A screenshot of a video game

Description automatically generated

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

A screenshot of a computer

Description automatically generated

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

A screenshot of a computer

Description automatically generated

Yêu cầu bài thực hành:

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

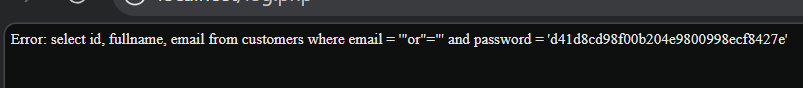
2. Trong vài trường hợp, hacker có thể sử dụng các kỹ thuật SQL Injection để hack hệ thống của bạn. Bạn hãy trình bày SQL Injection là gì và thử các ví dụ trình bày trong 1. Ứng dụng kỹ thuật đó vào trang đăng nhập mà bạn đã tạo, chụp lại các kết quả.

* SQL Injection là:
  + Một kỹ thuật chèn mã có thể phá hủy cơ sở dữ liệu của bạn
  + Một trong những kỹ thuất hack web phổ biến nhất
  + Việc đặt mã độc vào lệnh SQL thông qua đầu vào trang web
* Ứng dụng vào trang đăng nhập



A screenshot of a computer

Description automatically generated



* Nguồn tham khảo:

<https://www.w3schools.com/sql/sql_injection.asp>

3. 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 thường được sử dụng để nhận dạng người dùng; 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
* Tạo cookie với PHP bằng hàm:



* Hàm setcookie(): xác định một cookie sẽ được gửi cùng với phần còn lại của tiên đề HTTP và phải xuất hiện trước thẻ <html>
* Giá trị của cookie được tự động mã hóa URL khi gửi cookie và tự động giải mã khi nhận được (để ngăn chặn mã háo URL, thay vào đó hãy sử dụng setrawcookie() )

|  |  |
| --- | --- |
| Tham số | Mô tả |
| Name(tên) | Yêu cầu, chỉ định tên của cookie |
| value (giá trị) | Không bắt buộc, chỉ định giá trị của cookie |
| Expire (hết hạn) | Không bắt buộc, chỉ định thời điểm cookie hết hạn. Gái trị: time()+86400\*30, sẽ đặt cookie hết hạn sau 30 ngày. Nếu tham số này bị bỉ qua hoặc được đặt thành 0, cookie sẽ hết hạn vào cuối phiên (khi đóng trình duyệt). Mặc định là 0. |
| path (đường dẫn) | Tùy chọn. chỉ định đường dẫn máy chủ của cookie. Nếu được đặt thành ”/”, cookie sẽ khả dụng trong toàn bộ miền. Nếu được đặt thành “/php/”, cookie sẽ chỉ khả dụng trong thưu mục php và tất cả các thư mục con của php. Giá trị mặc định là thư mục hiện tại mà cookie đang được đặt |
| domain (tên miền) | Tùy chọn. Chỉ định tên miền của cookie. Để cung cấp cookie trên tất cả các tên miền phụ của example.com, hãy đặt tên miền thành “example.com”. Đặt nó thành [www.example.com](http://www.example.com) sẽ làm cho cookie chỉ khả dụng trong tên miền phụ www |
| secure (an toàn) | Tùy chọn. Chỉ định xem cookie chỉ được truyền qua kết nối HTTPS an toàn hay không. TRUE chỉ ra rằng cookie sẽ chỉ được đặt nếu tồn tại kết nối an toàn. Mặc định là FALSE |
| httponly | Tùy chọn. Nếu được đặt thành TRUE, cookie sẽ chỉ có thể truy cập được thông báo qua giao thức HTTP (cookie sẽ không thể truy cập được bằng ngôn ngữ tập lệnh). Cài đặt này có thể giúp giảm hành vi trộm cắp danh tính thông qua các cuộc tấn XSS. Mặc định là FALSE |

<https://www.w3schools.com/sql/sql_injection.asp>

<https://www.w3schools.com/php/php_cookies.asp>

* Cách lưu, lấy, xóa giá trị trong cookie.
* Lưu, lấy giá trị cookie: Ví dụ sau tạo cookie có tên "người dùng" với giá trị "John Doe". Cookie sẽ hết hạn sau 30 ngày (86400 \* 30). "/" có nghĩa là cookie có sẵn trên toàn bộ trang web (nếu không, hãy chọn thư mục bạn thích).

A black screen with green text

Description automatically generated

* Xóa cookie: sử dụng setcookie() hàm có ngày hết hạn trong quá khứ

A black screen with a black background

Description automatically generated with medium confidence

https://www.w3schools.com/php/php\_cookies.asp

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

* Phiên là một cách lưu trữ thông tin (theo biến) để sử dụng trên nhiều trang
* Không giống như cookie, thông tin không được lưu trữ trên máy tính của người dùng.
* Khi bạn làm việc với một ứng dụng, bạn mở nó, thực hiện một số thay đổi rồi đóng nó lại. Điều này giống như một Phiên. Máy tính biết bạn là ai. Nó biết khi nào bạn khởi động ứng dụng và khi nào bạn kết thúc. Nhưng trên internet có một vấn đề: máy chủ web không biết bạn là ai hoặc bạn làm gì, vì địa chỉ HTTP không duy trì trạng thái.
* Biến phiên giải quyết vấn đề này bằng cách lưu trữ thông tin người dùng sẽ được sử dụng trên nhiều trang (ví dụ: tên người dùng, màu yêu thích, v.v.). Theo mặc định, các biến phiên kéo dài cho đến khi người dùng đóng trình duyệt.
* Vì thế; Các biến phiên chứa thông tin về một người dùng và có sẵn cho tất cả các trang trong một ứng dụng.
* Cách lưu, lấy, xóa giá trị trong Session.
* Một phiên được bắt đầu với session\_start()chức năng.
* Các biến phiên được đặt bằng biến toàn cục PHP: $\_SESSION.
* Bây giờ, hãy tạo một trang mới có tên "demo\_session1.php". Trong trang này, chúng tôi bắt đầu một phiên PHP mới và đặt một số biến phiên:

<https://www.w3schools.com/php/php_sessions.asp>

A screenshot of a computer

Description automatically generated

* Tiếp theo, chúng tôi tạo một trang khác có tên "demo\_session2.php". Từ trang này, chúng tôi sẽ truy cập thông tin phiên mà chúng tôi đã đặt trên trang đầu tiên ("demo\_session1.php").
* Lưu ý rằng các biến phiên không được chuyển riêng lẻ đến từng trang mới, thay vào đó chúng được truy xuất từ ​​phiên chúng ta mở ở đầu mỗi trang ( session\_start()).
* Cũng lưu ý rằng tất cả các giá trị biến phiên được lưu trữ trong biến $\_SESSION toàn cục:

A black rectangular object with a black border

Description automatically generated

* Để xóa tất cả các biến phiên toàn cục và hủy phiên, hãy sử dụng session\_unset() and session\_destroy():

A screenshot of a computer program

Description automatically generated

https://www.w3schools.com/php/php\_sessions.asp

5. Bạn hãy so sánh Cookie và Session.

|  |  |
| --- | --- |
| COOKIE | SESSION |
| Được lưu trữ trên trình duyệt của người dùng | Không được lưu trữ trên trình duyệt |
| Dữ liệu: được lưu ở phía client (máy khách), dễ dàng sửa đổi hoặc đánh cắp khi chúng được lưu trữ ở phía client, có sẵn trong trình duyệt đến khi expired | Dữ liệu: được lưu ở server (máy chủ), không dễ dàng sửa đổi vì chúng được lưu trữ ở phía máy chủ nên sẽ bảo mật tốt hơn cookie |
| Kết thúc tùy vào thời gian Developer cài đặt | Một session sẽ kết thúc khi bị đóng trình duyệt |
| Không bị phụ thuộc vào session | Session phụ thuộc vào Cookie (SessionID được lưu ở cookie) |
| Dễ bị tấn công do lưu ở phía client | Dữ liệu session không dễ bị sửa đổi, tấn công |
|  | Sau khi đóng trình duyệt sẽ hết phiên làm việc (session |

<https://hocjavascript.net/tong-quan/so-sanh-session-va-cookie/#So_sanh_Session_va_Cookie>

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.

A screenshot of a computer program

Description automatically generated

A screenshot of a computer program

Description automatically generated

A screen shot of a computer

Description automatically generated

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.

A screenshot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

A computer screen shot of a code

Description automatically generated

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

## Định cấu hình tệp "php.ini"

* Trước tiên, hãy đảm bảo rằng PHP được cấu hình để cho phép tải tệp lên.
* Trong tệp "php.ini" của bạn, tìm kiếm lệnh file\_uploadsvà đặt thành Bật:



## Tạo biểu mẫu HTML

* Tiếp theo, tạo một biểu mẫu HTML cho phép người dùng chọn tệp hình ảnh họ muốn tải lên:

A computer screen shot of a program

Description automatically generated

* Một số quy tắc cần tuân theo đối với biểu mẫu HTML ở trên:
* Đảm bảo rằng biểu mẫu sử dụng phương thức = "post"
* Biểu mẫu cũng cần thuộc tính sau: enctype="multipart/form-data". Nó chỉ định loại nội dung nào sẽ sử dụng khi gửi biểu mẫu
* Nếu không có các yêu cầu trên thì việc tải file lên sẽ không thành công.

Những điều khác cần chú ý:

* + Thuộc tính type="file" của thẻ <input> hiển thị trường đầu vào dưới dạng điều khiển chọn tệp, với nút "Duyệt" bên cạnh điều khiển đầu vào

Biểu mẫu ở trên gửi dữ liệu đến một tệp có tên "upload.php", tệp này chúng ta sẽ tạo tiếp theo.

## Tạo tập lệnh PHP tệp tải lên

Tệp "upload.php" chứa mã để tải tệp lên:

A screen shot of a computer program

Description automatically generated

* Tập lệnh PHP đã 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 chứa phần mở rộng tệp của tệp (viết thường)
* Tiếp theo kiểm tra 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 tập tin được 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 đúng như vậy, một thông báo lỗi sẽ hiển thị và $uploadOk được đặt thành 0:

A computer code with text

Description automatically generated with medium confidence

Giới hạn kích thước tệp

Trường nhập tệp trong biểu mẫu HTML của chúng tôi ở trên có tên là "fileToUpload".

Bây giờ, chúng tôi muốn kiểm tra kích thước của tập tin. Nếu tệp lớn hơn 500KB, thông báo lỗi sẽ hiển thị và $uploadOk được đặt thành 0:

A close up of text

Description automatically generated

## Giới hạn loại tệp

Mã bên dưới 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:

A screenshot of a computer program

Description automatically generated

## Hoàn tất tải lên tập lệnh PHP

Tệp "upload.php" hoàn chỉnh bây giờ trông như thế này:

A screenshot of a computer program

Description automatically generated A screenshot of a computer program

Description automatically generated

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

Định nghĩa và cách sử dụng

file() đọc một tập tin vào một mảng.

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

Cú pháp

A black background with white text

Description automatically generated

Giá trị tham số.

|  |  |
| --- | --- |
| Tham số | Mô tả |
| Filename (tên tập tin) | Bắt buộc, chỉ định đường dẫn tới file cần đọc |
| Flag (cờ) | Tùy chọn, 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 dòn mới ở cuối mỗi phần từ mảng * FILE\_SKIP\_EMPTY\_LINES – Bỏ qua các dòng trống trong tệp |
| Context (ngữ cảnh) | Tùy chọn, 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 |

https://www.w3schools.com/php/func\_filesystem\_file.asp

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 .

* 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: [[1]](#footnote-1),[[2]](#footnote-2). 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.

A screenshot of a computer

Description automatically generated

A screen shot of a computer program

Description automatically generated

A screen shot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated

1 https://www.w3schools.com/sql/sql\_injection.asp

2 https://www.w3schools.com/php/php\_cookies.asp

3 https://www.w3schools.com/php/php\_sessions.asp

4 https://www.w3schools.com/php/php\_file\_upload.asp

5 https://www.w3schools.com/php/func\_filesystem\_file.asp

6 https://www.php.net/manual/en/features.file-upload.post-method.php,

7 https://stackoverflow.com/questions/6654351/check-file-uploaded-is-in-csv-format

1. <https://www.php.net/manual/en/features.file-upload.post-method.php>, [↑](#footnote-ref-1)
2. https://stackoverflow.com/questions/6654351/check-file-uploaded-is-in-csv-format [↑](#footnote-ref-2)