Anna Poluektova

ID: 100786356

**add.php**

<?php

session\_start(); //DONT FORGET SESSION START

if (!(isset($\_SESSION['logged\_in']) && $\_SESSION['logged\_in']==1)) {

echo "error - not logged in";

die();

}

require 'site\_functions.php';

?>

<script language="JavaScript" type="text/JavaScript">

function validateData(){

alert("hello");

window.event.returnValue = false;

}

</script>

<!DOCTYPE html>

<html lang ="en">

<head>

<meta charset="utf-8">

<title> </title>

</head>

<body>

<?php

echo getcwd ();

if (isset($\_FILES['userfile']))

{

$uploaddir = '/home/s2786356/public\_html/comp1230/assignments/assignment1/uploads/';

$bb = basename($\_FILES['userfile']['name']);

$uploadfile = $uploaddir . $bb ;

echo "<p>";

if (move\_uploaded\_file($\_FILES['userfile']['tmp\_name'], $uploadfile)) {

echo "File is valid, and was successfully uploaded.\n";

} else {

echo "Upload failed";

}

}

else {

echo "File not set";

}

?> <br />

<form enctype="multipart/form-data" action="" method="POST">

Send this file: <input name="userfile" type="file" />

<input type="submit" name="send\_file" value="Upload" /><br />

</form>

<form action="" method="">

\* Title

<input type="text" name="title" value="" /><br />

\* First Name

<input type="text" name="first\_name" value="" /><br />

\* Last Name

<input type="text" name="last\_name" value="" /><br />

E-mail

<input type="email" name="e-mail" value="" /><br />

Site

<input type="text" name="site" value="" /><br />

Cell Number

<input type="text" name="cell\_number" value="" /><br />

Home Number

<input type="text" name="home\_number" value="" /><br />

Office Number

<input type="text" name="office\_number" value="" /><br />

Twitter URL

<input type="text" name="twitter\_url" value="" /><br />

Facebook URL

<input type="text" name="facebook\_url" value="" /><br />

Comment

<textarea rows="2" cols="7" name="comment" value="" > </textarea><br />

<input type='submit' name='add' value="add" /><br />

<input type="hidden" name="11" value="<?php echo $bb; ?>" />

</form>

<?php

if(\_get('add'))

{

add\_user();

}

?>

</body>

</html>

**admin\_page.php**

<?php

session\_start(); //DONT FORGET SESSION START

if (!(isset($\_SESSION['logged\_in']) && $\_SESSION['logged\_in']==1)) {

echo "error - not logged in";

die();

}

require 'site\_functions.php';

?>

<!DOCTYPE html>

<html lang ="en">

<head>

<meta charset="utf-8">

<title> </title>

</head>

<body>

<a href="index.php?logout=true" style="float:right;">LOGOUT</a></br>

<form action="search.php?sea=<?php \_get("search"); ?>" method="">

<input type="text" name="search" value="" style="float:right;" />

<input type="submit" name="search\_b" value="search" style="float:right;" />

</form>

<div style="float:center"><h1>Welcome to Admin's Page</h1><br /></div>

<div style='float:left;'>

<a href="add.php">Create new contact</a><br />

<a href="change.php">Change</a>

</div>

<div style="float:right;">

<table border="1">

<tr>

<th>Title</th>

<th>First Name</th>

<th>Last Name</th>

<th>Picture</th>

<th>View</th>

<th>Modify</th>

<th>Delete</th>

</tr>

<tbody>

<?php if (filesize("students.txt") != 0) {

get\_students();

}else { ?>

<tr><td colspan='7'>No students records found</td></tr>

<?php }?>

</tbody>

</table>

</div>

</body>

</html>

**change.php**

<?php

session\_start(); //DONT FORGET SESSION START

if (!(isset($\_SESSION['logged\_in']) && $\_SESSION['logged\_in']==1)) {

echo "error - not logged in";

die();

}

require 'site\_functions.php';

?>

<!DOCTYPE html>

<html lang ="en">

<head>

<meta charset="utf-8">

<title> </title>

</head>

<body>

<?php

//change user to users array

if ((isset($\_POST['newpassword'])) && (isset($\_POST['repeatnewpassword']))) {

if (($\_POST['newpassword']) == ($\_POST['repeatnewpassword'])) {

$h2 = fopen('users.txt', 'w');

fwrite($h2, "admin," . sha1($\_POST['newpassword']));

fclose($h2);

header('Location: index.php');

} else {

echo "Passwords don't match";

}

}

?>

<h1>Change</h1>

<form action='' method='post'>

New password: <input type='password' name='newpassword'>

Repeat new password: <input type='password' name='repeatnewpassword'>

<input type='submit' name='submit' value='change\_password'>

</form>

</body>

</html>

**delete.php**

<?php

session\_start(); //DONT FORGET SESSION START

if (!(isset($\_SESSION['logged\_in']) && $\_SESSION['logged\_in']==1)) {

echo "error - not logged in";

die();

}

require 'site\_functions.php';

?>

<!DOCTYPE html>

<html lang ="en">

<head>

<meta charset="utf-8">

<title> </title>

</head>

<body>

<?php

$id=\_get('id');

$handle=fopen('students.txt','r');

$var1=explode(PHP\_EOL, fread($handle, filesize('students.txt')));

for ($i=0;$i<count($var1);$i++) {

$var2 = explode(",", $var1[$i]);

if ($var2[0] == $id) {

unset($var1[$i]);

$handle1 = fopen('students.txt', 'w');

fwrite($handle1, implode(PHP\_EOL , $var1));

fclose($handle1);

echo '<meta http-equiv="refresh" content="0;URL=admin\_page.php">';

}

}

?>

</body>

</html>

**edit.php**

<?php

require 'site\_functions.php';

{

$err\_t="";

$err\_f="";

$err\_l="";

$is\_allowed=0;

$id=\_get('record\_id');

$title=\_get('title');

$first\_name=\_get('first\_name');

$last\_name=\_get('last\_name');

$email=\_get('email');

$site=\_get('site');

$cell\_number=\_get('cell\_number');

$home\_number=\_get('home\_number');

$office\_number=\_get('office\_number');

$twitter\_url=\_get('twitter\_url');

$facebook\_url=\_get('facebook\_url');

$comment=\_get('comment');

$picture=\_get('picture');

if(!$title){

$err\_t = "Title cannot be empty \\n";

$is\_allowed=1;

}

if(!$first\_name){

$err\_f = "First Name cannot be empty \\n";

$is\_allowed=1;

}

if(!$last\_name){

$err\_l = "Last Name cannot be empty \\n";

$is\_allowed=1;

}

if ($is\_allowed==0)

{

$handle=fopen('students.txt','r');

$var1=explode(PHP\_EOL, fread($handle, filesize('students.txt')));

for ($i=0;$i<count($var1);$i++) {

$var2 = explode(",", $var1[$i]);

if ($var2[0] == $id) {

$var1[$i] = "$id,$title,$first\_name,$last\_name,$email,$site,$cell\_number,$home\_number,$office\_number,$twitter\_url,$facebook\_url,$comment,$picture";

$handle1 = fopen('students.txt', 'w');

fwrite($handle1, implode(PHP\_EOL , $var1));

fclose($handle1);

}} }

else if($err\_t || $err\_f || $err\_l){

echo "<script>alert('".$err\_t.$err\_f.$err\_l."')</script>";

}

echo '<meta http-equiv="refresh" content="0;URL=admin\_page.php">';

}

**index.php**

<?php

session\_start(); //DONT FORGET SESSION START

require 'site\_functions.php';

//check if user has filled out the form

if(isset($\_POST['usrnme'])){

//check if credentials are correct

if(authenticate($\_POST['usrnme'], $\_POST['pass'])){

$\_SESSION['logged\_in'] = 1;

$\_SESSION['user\_n'] = $\_POST['usrnme'];

}else{ //inform user of an error

$err = "Invalid username or password";

}

//check if user has clicked log out

}else if(isset($\_GET['logout'])){

unset($\_SESSION['logged\_in']);

unset($\_SESSION['user\_n']);

}

?>

<!DOCTYPE html>

<html>

<head>

<style type="text/css">

#wrap {

width:800px;

margin:0 auto;

}

#left\_col {

float:center;

}

#right\_col {

float:right;

width:200px;

}

</style>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

<title></title>

</head>

<body>

<div id="wrap">

<div id="left\_col">

<h1>Welcome to Anna's Address Book</h1>

<?php if(isset($err)){

echo '<span style="color:red;">' . $err .'</span>';

}?>

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

Username: <input type="text" name="usrnme" value="admin" ><br>

Password: <input type="password" name="pass"value="123"><br>

<input type="submit" value="login">

</form>

</div>

<div id="right\_col">

<?php if(is\_logged\_in()):

echo '<meta http-equiv="refresh" content="0;URL=admin\_page.php">';

?>

<?php else : ?>

<?php

if(isset($\_SESSION['msg'])){

echo $\_SESSION['msg'];

unset($\_SESSION['msg']);

}

?>

<?php endif;?>

</div>

</div>

</body>

</html>

**modify.php**

<?php

session\_start(); //DONT FORGET SESSION START

if (!(isset($\_SESSION['logged\_in']) && $\_SESSION['logged\_in']==1)) {

echo "error - not logged in";

die();

}

require 'site\_functions.php';

?>

<!DOCTYPE html>

<html lang ="en">

<head>

<meta charset="utf-8">

<title> </title>

</head>

<body>

<?php

$id=\_get('id');

$title=\_get('title');

$first\_name=\_get('first\_name');

$last\_name=\_get('last\_name');

$email=\_get('email');

$site=\_get('site');

$cell\_number=\_get('cell\_number');

$home\_number=\_get('home\_number');

$office\_number=\_get('office\_number');

$twitter\_url=\_get('twitter\_url');

$facebook\_url=\_get('facebook\_url');

$comment=\_get('comment');

$picture=\_get('picture');

?>

<form action="edit.php" method="">

\* Title

<input type="text" name="title" value="<?php echo $title; ?>" /><br />

\* First Name

<input type="text" name="first\_name" value="<?php echo $first\_name; ?>" /><br />

\* Last Name

<input type="text" name="last\_name" value="<?php echo $last\_name; ?>" /><br />

E-mail

<input type="email" name="email" value="<?php echo $email; ?>" /><br />

Site

<input type="text" name="site" value="<?php echo $site; ?>" /><br />

Cell Number

<input type="text" name="cell\_number" value="<?php echo $cell\_number; ?>" /><br />

Home Number

<input type="text" name="home\_number" value="<?php echo $home\_number; ?>" /><br />

Office Number

<input type="text" name="office\_number" value="<?php echo $office\_number; ?>" /><br />

Twitter URL

<input type="text" name="twitter\_url" value="<?php echo $twitter\_url; ?>" /><br />

Facebook URL

<input type="text" name="facebook\_url" value="<?php echo $facebook\_url; ?>" /><br />

Comment

<textarea rows="2" cols="7" name="comment" value="<?php echo $comment; ?>" > </textarea><br />

<input type="text" name="picture" value="<?php echo $picture; ?>" />

<input type="hidden" name="record\_id" value="<?php echo $id; ?>"/>

<input type="submit" name="edit\_name" value="edit\_name" />

<img src='uploads/<?php echo $picture; ?>' height="100" />

</form>

</body>

</html>

**search.php**

<?php

session\_start(); //DONT FORGET SESSION START

if (!(isset($\_SESSION['logged\_in']) && $\_SESSION['logged\_in']==1)) {

echo "error - not logged in";

die();

}

require 'site\_functions.php';

?>

<!DOCTYPE html>

<html lang ="en">

<head>

<meta charset="utf-8">

<title> </title>

</head>

<body>

<?php

$filename = "students.txt";

$fp = fopen($filename, "r") or die("Couldn't open $filename");

while(!feof($fp))

{

$line = fgets($fp);

if (preg\_match('/'.\_get("search").'/',$line))

print "$line<br>";

}

fclose($fp);

?>

</body>

</html>

**site\_functions.php**

<?php

//check if user is logged in

function is\_logged\_in(){

if(isset($\_SESSION['logged\_in']) && $\_SESSION['logged\_in'] == true){

return true;

}

return false;

}

//redirect user if not logged in

function bouncer($url){

if(!is\_logged\_in()){

header("Location: $url");

exit();

}

}

//gets all users and saves them into $users array

function get\_users(){

$users = array();

$cred\_file = fopen('users.txt', 'r');

if(!$cred\_file)

return array();

while($creds = fgetcsv($cred\_file)){

$users[$creds[0]] = $creds[1];

}

fclose($cred\_file);

return $users;

}

//check user credentials

function authenticate($user, $pass){

$h2 = fopen('users.txt', 'r');

if ($h2) {

$contacts = explode(",", fread($h2, filesize("users.txt")));

fclose($h2);

}

if($contacts[0] == $user && $contacts[1] == sha1($pass)){

return true;

}

return false;

}

//check to see if a user exists

function user\_exists($user){

$users = get\_users();

return isset($users[$user]);

}

//add user to users array

function register\_user($user, $pass){

$users = get\_users();

$users[$user] = sha1($pass);

write\_users($users);

}

//write users to file

function write\_users($users){

$cred\_file = fopen('users.txt', 'w');

foreach($users as $user=>$pass){

fputcsv($cred\_file, array($user, $pass));

}

fclose($cred\_file);

}

function get\_val($index){

echo $\_POST[$index];

if(isset($\_POST[$index]))

return $\_POST[$index];

}

function \_get($name)

{

return (isset($\_GET[$name]) && !empty($\_GET[$name]) ? $\_GET[$name] : '');

}

function add\_user()

{

$err\_t="";

$err\_f="";

$err\_l="";

$is\_allowed=0;

$title = \_get('title');

$first\_name = \_get('first\_name');

$last\_name = \_get('last\_name');

$email = \_get('e-mail');

$site = \_get('site');

$cell\_number = \_get('cell\_number');

$home\_number = \_get('home\_number');

$office\_number = \_get('office\_number');

$twitter\_url = \_get('twitter\_url');

$facebook\_url = \_get('facebook\_url');

$comment = \_get('comment');

$picture = \_get('11');

$fin = fopen('students.txt','a');

if(!$title){

$err\_t = "Title cannot be empty \\n";

$is\_allowed=1;

}

if(!$first\_name){

$err\_f = "First Name cannot be empty \\n";

$is\_allowed=1;

}

if(!$last\_name){

$err\_l = "Last Name cannot be empty \\n";

$is\_allowed=1;

}

if ($is\_allowed==0)

{

if($fin)

{

$id = getID(); // we need id only when there is no error

$record = $id . ',' . $title . ',' . $first\_name . ',' . $last\_name . ',' . $email . ','

. $site . ',' . $cell\_number . ',' . $home\_number . ',' . $office\_number . ','

. $twitter\_url . ',' . $facebook\_url . ',' . $comment . ',' . $picture ;

fwrite($fin, $record . PHP\_EOL);

fclose($fin);

}

}

else if($err\_t || $err\_f || $err\_l){

echo "<script>alert('".$err\_t.$err\_f.$err\_l."')</script>";

}

echo '<meta http-equiv="refresh" content="0;URL=admin\_page.php">';

}

function view\_contact()

{

$id=\_get('id');

$found = false;

$records = file('students.txt');

foreach($records as $record):

$contact = explode (",", $record);

if(is\_array($contact) && !empty($contact[0]) && $id == $contact[0])

{

print "we found the contact<br />";

echo "<table border='1'><tr><td>Title</td><td>First Name</td><td>Last Name</td><td>E-mail</td><td>

Site</td><td>Cell number</td><td>Home number</td><td>Office number</td><td>Twitter url</td><td>

Facebook url</td><td>Comment</td><td>Picture</td></tr>" . "<tr><td>" . $contact[1]

. "</td><td>" . $contact[2] . "</td><td>" .

$contact[3] . "</td><td>" . $contact[4] . "</td><td>" . $contact[5] . "</td><td>" .

$contact[6] . "</td><td>" . $contact[7] . "</td><td>" . $contact[8] .

"</td><td>" . $contact[9] . "</td><td>" . $contact[10] . "</td><td>" . $contact[11] .

"</td><td>" . $contact[12] . "</td></tr></table>";

$found = true;

}

endforeach;

if(!$found)

{

print "cannot find the user";

}

die;

}

function get\_students()

{

$i=0;

$handle = fopen('students.txt','r+');

while (!feof($handle))

{

$student = fgets($handle);

$student\_data = explode (",", $student);

if(!is\_array($student\_data) || empty($student\_data[0])) continue;

print "<tr><td>" . $student\_data[1] . "</td>";

print "<td>" . $student\_data[2] . "</td>";

print "<td>" . $student\_data[3] . "</td>";

echo "<td><img src='uploads/" . $student\_data[12] . "' alt='' weight='40px' height='40px' /></td>";

echo "<td><a href='view.php?id=$student\_data[0]'>View</a></td>";

echo "<td><a href='modify.php?id=$student\_data[0]&title=$student\_data[1]&first\_name=$student\_data[2]&last\_name=$student\_data[3]&email=$student\_data[4]&site=$student\_data[5]&cell\_number=$student\_data[6]&home\_number=$student\_data[7]&office\_number=$student\_data[8]&twitter\_url=$student\_data[9]&facebook\_url=$student\_data[10]&comment=$student\_data[11]&picture=$student\_data[12]' >Modify</a></td>";

echo "<td><a href='delete.php?id=$student\_data[0]' onclick=\"return confirm('Are you sure you want to delete?')\">Delete</a></td></tr>";

$i++;

}

}

function getID()

{

$file\_name = 'ids';

if (!file\_exists($file\_name))

{

touch($file\_name);

$handle = fopen($file\_name,'r+');

$id = 0;

}

else

{

$handle = fopen($file\_name, 'r+');

$id = fread($handle, filesize($file\_name));

settype ($id, "integer");

}

rewind ($handle);

fwrite($handle, ++$id);

fclose($handle);

return $id;

}

**upload.php**

<?php

if (isset($\_FILES['userfile']))

{

$uploaddir = '/home/s2786356/public\_html/comp1230/assignments/assignment1/uploads/';

$bb = basename($\_FILES['userfile']['name']);

$uploadfile = $uploaddir . $bb ;

if (move\_uploaded\_file($\_FILES['userfile']['tmp\_name'], $uploadfile)) {

} else {

echo "Upload failed";

}

echo '<meta http-equiv="refresh" content="0;URL=add.php">';

}

**view.php**

<?php

session\_start(); //DONT FORGET SESSION START

if (!(isset($\_SESSION['logged\_in']) && $\_SESSION['logged\_in']==1)) {

echo "error - not logged in";

die();

}

require 'site\_functions.php';

?>

<!DOCTYPE html>

<html lang ="en">

<head>

<meta charset="utf-8">

<title> </title>

</head>

<body>

<?php

view\_contact();

?>

</body>

</html>



