**add.php**

<?php

session\_start();

require\_once "C:/MAMP/htdocs/Ass/pdo.php";

if ( ! isset($\_SESSION['name']))

{

die('Not logged in');

}

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

header('Location: index.php');

return;

}

if(isset($\_POST['subject'])&&isset($\_POST['name'])&&isset($\_POST['topic'])

&&isset($\_POST['htno'])&&isset($\_POST['link'])&&isset($\_POST['class'])&&isset($\_POST['teacher']))

{

if(strlen($\_POST['subject'])<1||strlen($\_POST['name'])<1||strlen($\_POST['topic'])<1||

strlen($\_POST['htno'])<1||strlen($\_POST['link'])<1||strlen($\_POST['class'])<1||strlen($\_POST['teacher'])<1)

{

$\_SESSION['error']="All fields are required";

header("Location: add.php");

return;

}

/\*else if(!filter\_var($\_POST['email'],FILTER\_VALIDATE\_EMAIL))

{

$\_SESSION['error'] = "Email must have an at-sign (@)";

header("Location: add.php");

return;

}\*/

else

{

try {

$stmt = $pdo->prepare('INSERT INTO ass

(user\_id, subject, name, topic, htno, link, class, teacher)

VALUES ( :uid, :su, :na, :to, :ht, :li, :cl, :te)');

$stmt->execute(array(

':uid' => (int)$\_SESSION['user\_id'],

':su' => $\_POST['subject'],

':na' => $\_POST['name'],

':to' => $\_POST['topic'],

':ht' => $\_POST['htno'],

':li' => $\_POST['link'],

':cl' => $\_POST['class'],

':te' => $\_POST['teacher']

));

$\_SESSION['success'] = "Record added";

header("Location: index.php");

return;

}

catch(Exception $ex)

{

echo("Internal error, please contact support");

error\_log("add.php, SQL error=".$ex->getMessage());

}

}

}

?>

<!DOCTYPE html>

<html>

<head>

<title>Student Assignments</title>

</head>

<body>

<div class="container">

<?php

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

echo "<h1>Adding entries for ";

echo htmlentities($\_SESSION['name']);

echo "</h1>\n";

}

echo ('<br>'."Note : All fields are Required".'<br>');

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

echo('<p style="color: red;">'.htmlentities($\_SESSION['error'])."</p>\n");

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

}

?>

<form method="post">

<p>Name of the Student:

<input type="text" name="name" size="60"/></p>

<p>Subject:

<input type="text" name="subject" size="60"/></p>

<p>Topic:

<input type="text" name="topic" size="60"/></p>

<p>Hall ticket num :<br>

<input type="text" name="htno" size="60"/></p>

<p>Class :<br>

<input type="text" name="class" size="60"/></p>

<p>Teacher :<br>

<input type="text" name="teacher" size="60"/></p>

<p>Link : (Enter the Shareable link from Google Drive)<br>

<textarea name="link" rows="8" cols="80"></textarea> </p>

<p>

<input type="submit" name="add" value="Add">

<input type="submit" name="cancel" value="Cancel">

</p>

</form>

</div>

</body>

</html>

**delete.php**

<?php

require\_once "C:/MAMP/htdocs/Ass1/pdo.php";

session\_start();

if ( ! isset($\_SESSION['name']))

{

die('Not logged in');

}

if ( isset($\_POST['delete']) && isset($\_POST['ass\_id']) ) {

$sql = "DELETE FROM ass WHERE ass\_id = :aid";

$stmt = $pdo->prepare($sql);

$stmt->execute(array(':aid' => $\_POST['ass\_id']));

$\_SESSION['success'] = 'Record deleted';

header( 'Location: index.php' ) ;

return;

}

if(isset($\_POST['cancel']))

{

header('Location: index.php');

return;

}

// Guardian: Make sure that user\_id is present

if ( ! isset($\_GET['ass\_id']) ) {

$\_SESSION['error'] = "Missing ass\_id";

header('Location: index.php');

return;

}

$stmt = $pdo->prepare("SELECT name, htno, subject, topic FROM ass where ass\_id = :abc");

$stmt->execute(array(':abc' => htmlEntities($\_GET['ass\_id'])));

$row = $stmt->fetch(PDO::FETCH\_ASSOC);

if ( $row === false ) {

$\_SESSION['error'] = 'Bad value for ass\_id';

header( 'Location: index.php' ) ;

return;

}

?>

<html>

<head>

<title> Deleting Entry</title>

</head>

<body>

<div class="container">

<h1><p>Deleting Assignment</p></h1>

<p> Name of the Student : <?= htmlEntities($row['name']) ?></p>

<p> Hall Ticket No. : <?= htmlEntities($row['htno']) ?></p>

<p> Subject : <?= htmlEntities($row['subject']) ?></p>

<p> Topic : <?= htmlEntities($row['topic']) ?></p>

<form method="post">

<input type="hidden" name="ass\_id" value="<?= $row['ass\_id'] ?>">

<input type="submit" value="Delete" name="delete">

<input type="submit" value="Cancel" name="cancel">

</form>

</div>

</body>

</html>

**edit.php**

<?php

session\_start();

require\_once "C:/MAMP/htdocs/Ass/pdo.php";

if ( ! isset($\_SESSION['name']))

{

die('Not logged in');

}

if(isset($\_POST['cancel']))

{

header('Location: index.php');

return;

}

if(isset($\_POST['ass\_id']) && isset($\_POST['name'])&&isset($\_POST['subject'])&&isset($\_POST['topic'])

&&isset($\_POST['htno'])&&isset($\_POST['class'])&&isset($\_POST['teacher'])&&isset($\_POST['link']))

{

if(strlen($\_POST['name'])<1||strlen($\_POST['subject'])<1||strlen($\_POST['topic'])<1||

strlen($\_POST['htno'])<1||strlen($\_POST['class'])<1||strlen($\_POST['teacher'])<1||strlen($\_POST['link'])<1)

{

$\_SESSION['error']="All fields are required";

header("Location: edit.php?ass\_id=".$\_GET['ass\_id']);

return;

}

/\*else if(!filter\_var($\_POST['email'],FILTER\_VALIDATE\_EMAIL))

{

$\_SESSION['error'] = "Email must have an at-sign (@)";

header("Location: edit.php?profile\_id=".$\_POST['profile\_id']);

return;

}\*/

else

{

try {

$sql = "UPDATE ass SET name = :na,

subject = :su, topic = :to, htno= :ht,

class= :cl, teacher= :te, link= :li

WHERE ass\_id = :aid AND user\_id=:uid";

$stmt = $pdo->prepare($sql);

$stmt->execute(array(

':na' => $\_POST['name'],

':su' => $\_POST['subject'],

':to' => $\_POST['topic'],

':ht' => $\_POST['htno'],

':cl' => $\_POST['class'],

':te' => $\_POST['teacher'],

':li' => $\_POST['link'],

':aid' => $\_POST['ass\_id'],

':uid' => $\_SESSION['user\_id']

));

$\_SESSION['success'] = 'Record updated';

header( 'Location: index.php' ) ;

return;

}

catch(Exception $ex)

{

echo("Internal error, please contact support");

error\_log("edit.php, SQL error=".$ex->getMessage());

}

}

}

// Guardian: Make sure that user\_id is present

if ( ! isset($\_GET['ass\_id']) ) {

$\_SESSION['error'] = "Missing ass\_id";

header('Location: index.php');

return;

}

$stmt = $pdo->prepare("SELECT \* FROM ass where ass\_id = :aid");

$stmt->execute(array(':aid' => htmlEntities($\_GET['ass\_id'])));

$row = $stmt->fetch(PDO::FETCH\_ASSOC);

if ( $row === false ) {

$\_SESSION['error'] = 'Bad value for ass\_id';

header( 'Location: index.php' ) ;

return;

}

$na = htmlentities($row['name']);

$su = htmlentities($row['subject']);

$to = htmlentities($row['topic']);

$ht = htmlentities($row['htno']);

$cl = htmlentities($row['class']);

$te = htmlentities($row['teacher']);

$li = htmlentities($row['link']);

$ass\_id = $row['ass\_id'];

?>

<html><head>

<title> Student Assignments </title>

</head><body>

<div class="container">

<h1><p>Editing information for <?= $\_SESSION['name']?></p></h1>

<?php

// Flash pattern

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

echo '<p style="color:red">'.$\_SESSION['error']."</p>\n";

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

}

?>

<form method="post">

<input type="hidden" name="ass\_id" value="<?= $ass\_id ?>"/>

<p>Name of the Student:

<input type="text" name="name" size="60" value="<?= $na ?>"/></p>

<p>Subject:

<input type="text" name="subject" size="60" value="<?= $su ?>"/></p>

<p>Topic:

<input type="text" name="topic" size="60" value="<?= $to ?>"/></p>

<p>Hall Ticket Number :

<input type="text" name="htno" size="60" value="<?= $ht ?>"/></p>

<p>Class:

<input type="text" name="class" size="60" value="<?= $cl ?>"/></p>

<p>Teacher:

<input type="text" name="teacher" size="60" value="<?= $te ?>"/></p>

<p>Link : (Enter the Shareable link from Google Drive)<br>

<textarea name="link" rows="8" cols="80"><?= $li ?></textarea> </p>

<p>

<input type="submit" name="save" value="Save">

<input type="submit" name="cancel" value="Cancel">

</p>

</form>

</div>

</body>

</html>

**index.php**

<!DOCTYPE html>

<html>

<head>

<title>Online Admission System</title>

<style>

table,th,td{

border:2px solid green;

}

td{

height : 30px;

text-align:center;

padding:6px;

}

tbody th{

height : 30px;

background : PowderBlue;

text-align : center;

}

tbody tr:nth-child(even){

background :MistyRose;

}

</style>

<?php

session\_start();

require\_once "C:/MAMP/htdocs/Adm/pdo.php";

?>

</head>

<body>

<div class="container">

<h1>Online Admission</h1>

<?php

$stmt = $pdo->query("SELECT adm\_name, aadhar no, phone no, certificates, percentage link FROM adm ORDER BY teachers");

$rows = $stmt->fetchAll(PDO::FETCH\_ASSOC);

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

echo '<p style="color:red">'.$\_SESSION['error']."</p>\n";

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

}

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

echo '<p style="color:green">'.$\_SESSION['success']."</p>\n";

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

}

if(isset($\_SESSION['name']))

{

echo('<p><a href="logout.php">Log Out</a></p>');

}

else

{

echo ('<p> <a href ="login.php">Please log in</a> </p>');

}

if(isset($\_SESSION['name']))

{

echo('<a href="add.php">Submit Assignment</a>');

}

if($stmt->rowCount())

{

echo('<table border="1">');

echo "<tr><th><b>Name</b></th>";

echo "<th><b>aadhar no.</b></th>";

echo "<th><b>phone no</b></th>";

echo "<th><b>certificates</b></th>";

echo "<th><b>percentage</b></th>";

echo "<th><b>Teacher</b></th>";

echo "<th><b>Admission link</b></th>";

if(isset($\_SESSION['name']))

{

echo "<th><b>Action</b></th></tr>";

}

}

foreach ( $rows as $row )

{

echo "<tr><td>";

echo(htmlEntities($row['name']));

echo("</td><td>");

echo(htmlEntities($row['htno']));

echo("</td><td>");

echo(htmlEntities($row['subject']));

echo("</td><td>");

echo(htmlEntities($row['topic']));

echo("</td><td>");

echo(htmlEntities($row['class']));

echo("</td><td>");

echo(htmlEntities($row['teacher']));

echo("</td><td>");

echo('<a href="'.htmlEntities($row['link']).'" target="\_blank">'."Click Here"."</a>");

if(isset($\_SESSION['name']))

{

echo("</td><td>");

echo('<a href="edit.php?adm\_id='.htmlEntities($row['adm\_name']).'">Edit</a> / ');

echo('<a href="delete.php?adm\_id='.$row['ass\_name'].'">Delete</a>');

}

echo("</td></tr>\n");

}

echo('</table><br>');

if(isset($\_SESSION['name']))

{

echo('<a href="add.php">online admission system</a>');

}

?>

<br><br><a href="C:/MAMP/htdocs/Adm/index.php"> Exit </a>

</div>

</body>

</html>

**login.php**

<?php

session\_start();

require\_once "C:/MAMP/htdocs/Ass/pdo.php";

$salt = 'XyZzy12\*\_';

if ( isset($\_POST['cancel']) )

{

header('Location: index.php');

return;

}

if ( isset($\_POST['email']) && isset($\_POST['pass']) )

{

$check = hash('md5', $salt.$\_POST['pass']);

$stmt=$pdo->prepare('SELECT user\_id,name FROM users WHERE email=:em AND password= :pw');

$stmt->execute(array(':em'=>$\_POST['email'], ':pw'=>$check));

$row=$stmt->fetch(PDO::FETCH\_ASSOC);

if ( $row!==false )

{

error\_log("Login success " .$\_POST['email']);

$\_SESSION['name']=htmlEntities($row['name']);

$\_SESSION['user\_id'] = htmlEntities($row['user\_id']);

header("Location: index.php");

return;

}

else

{

error\_log("Login fail ".$\_POST['email']." $check");

$\_SESSION['error'] = "Incorrect email/password";

header("Location: login.php");

return;

}

}

?>

<html>

<head>

<title>LMS by our Faculty</title>

<script type="text/javascript">

function doValidate()

{

console.log('Validating...');

try {

pw = document.getElementById('id\_1723').value;

em = document.getElementById('email\_id').value;

console.log("Validating em="+em);

var mailformat = /^\w+([\.-]?\w+)\*@\w+([\.-]?\w+)\*(\.\w{2,3})+$/;

if(em==""|| !(em.match(mailformat)) )

{

alert("Invalid email address");

return false;

}

console.log("Validating pw="+pw);

if (pw == null || pw == "" )

{

alert("Both fields must be filled out");

return false;

}

return true;

}

catch(e){

return false;

}

return false;

}

</script>

</head>

<body>

<div class="container">

<h1>Please Log In</h1>

<?php

if ( isset($\_SESSION['error']) )

{

echo('<p style="color: red;">'. htmlEntities($\_SESSION['error'])."</p>\n");

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

}

?>

<form method="post">

<p>Email:

<input type="text" size="40" name="email" id="email\_id"></p>

<p>Password:

<input type="password" size="40" name="pass" id="id\_1723"></p>

<p><input type="submit" name="login" value="Log In" onclick="return doValidate();">

<input type="submit" name="cancel" value="Cancel">

</p>

</form>

</div>

</body>

**Notes**

To get started run the following SQL commands:

CREATE DATABASE CS;

GRANT ALL ON CS.\* TO 'student'@'localhost' IDENTIFIED BY 'stu@2021';

GRANT ALL ON CS.\* TO 'student'@'127.0.0.1' IDENTIFIED BY 'stu@2021';

USE CS; (Or select misc in phpMyAdmin)

CREATE TABLE users (

user\_id INTEGER NOT NULL

AUTO\_INCREMENT PRIMARY KEY,

name VARCHAR(128),

email VARCHAR(128),

password VARCHAR(128),

INDEX(email)

) ENGINE=InnoDB CHARSET=utf8;

INSERT INTO users(name,email,password) values("Student","students@gcwa.in","54321");

CREATE TABLE ass (

ass\_id INTEGER NOT NULL

AUTO\_INCREMENT PRIMARY KEY,

user\_id INTEGER,

name VARCHAR(128),

htno VARCHAR(128),

subject VARCHAR(128),

topic VARCHAR(128),

class VARCHAR(128),

teacher VARCHAR(128),

link VARCHAR(128),

INDEX(teacher),

foreign key(user\_id) references users(user\_id)

) ENGINE=InnoDB CHARSET=utf8;