**Lab 6**

**1. Create page index.php as shown below.**

**index.php:**

<!DOCTYPE html>

<html>

<head>

<title>

Lab 6

</title>

</head>

<body>

<center>

<table border="1">

<?php

require\_once "config.php";

$sql = 'SELECT \* FROM students';

if($result = mysqli\_query($link,$sql)){

if(mysqli\_num\_rows($result) > 0){

echo "<tr>";

echo "<th>#</th>";

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

echo "<th>Address</th>";

echo "<th>Salary</th>";

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

echo "</tr>";

while ($row = mysqli\_fetch\_array($result)) {

echo "<tr>";

echo "<td>".$row['id']."</td>";

echo "<td>".$row['name']."</td>";

echo "<td>".$row['address']."</td>";

echo "<td>".$row['salary']."</td>";

echo "<td><a href='view.php?id=".$row['id']."'>View Record</a>&nbsp<a href='update.php?id=".$row['id']."'>Update Record</a>&nbsp<a href='delete.php?id=".$row['id']."'>Delete Record</a>&nbsp</td>";;

echo "</tr>";

}

echo "<h1><a href='create.php'>Create New Record</a></h1>";

}else{

echo "<h3>No record in the table please create a new record</h3>";

echo "<h1><a href='create.php'>Create Record</a></h1>";

}

}else{

die ("Error occured: ".mysql\_error());

}

?>

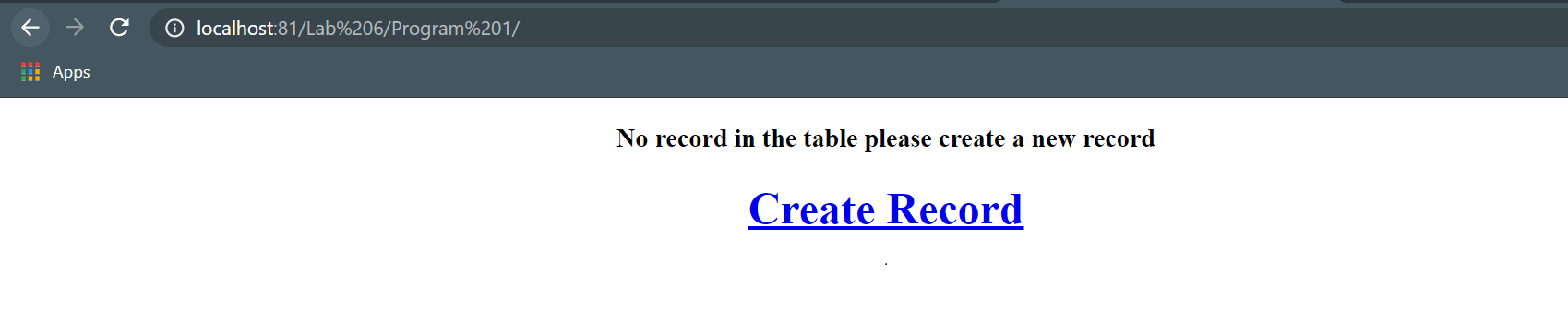
</table>

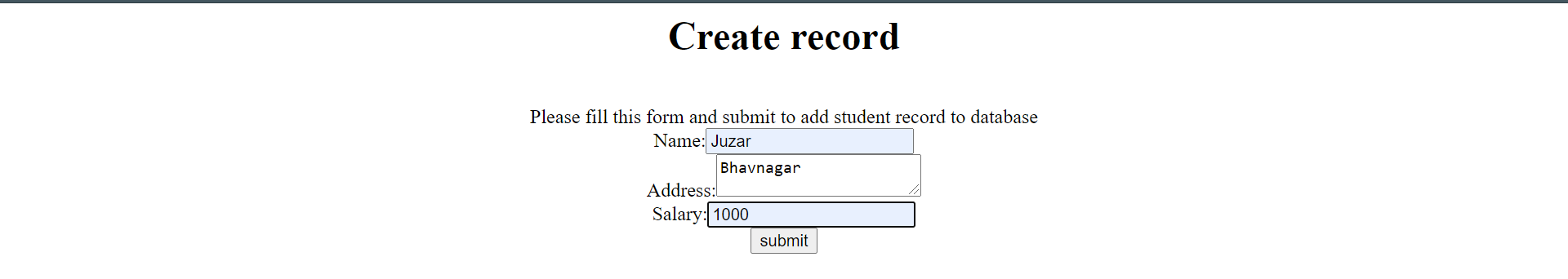
</center>

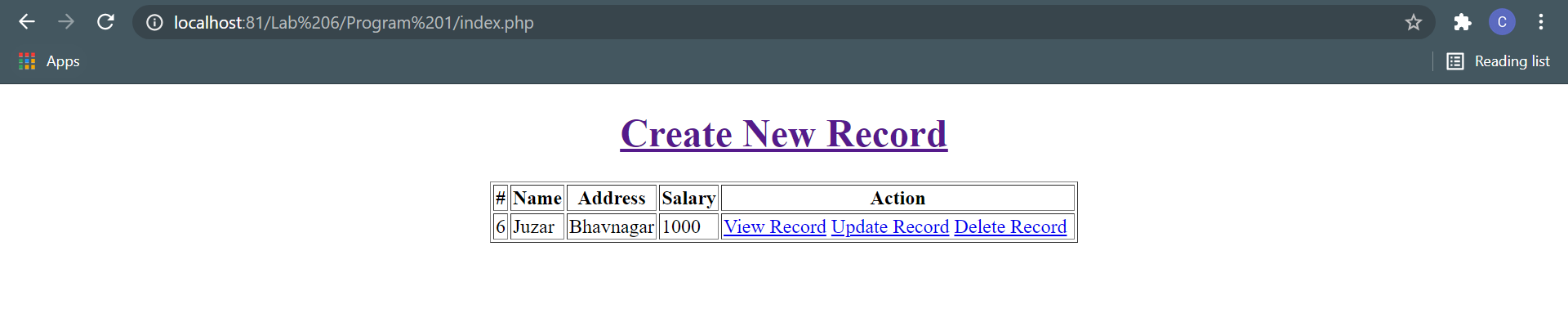
</body>

</html>

**Output:**

****

****

****

**2. Output for view.php click on back takes user to index.php**

**view.php:**

<?php

require\_once "config.php";

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

$sql = "SELECT \* FROM students WHERE id = '".$id."'";

if($result = mysqli\_query($link,$sql)){

if(mysqli\_num\_rows($result) > 0){

$row = mysqli\_fetch\_array($result);

echo "<h1>View record</h1>";

echo "<h3><b>Name</b></h3>";

echo $row['name']."<br>";

echo "<h3><b>Address</b></h3>";

echo $row['address']."<br>";

echo "<h3><b>Salary</b></h3>";

echo $row['salary']."<br>";

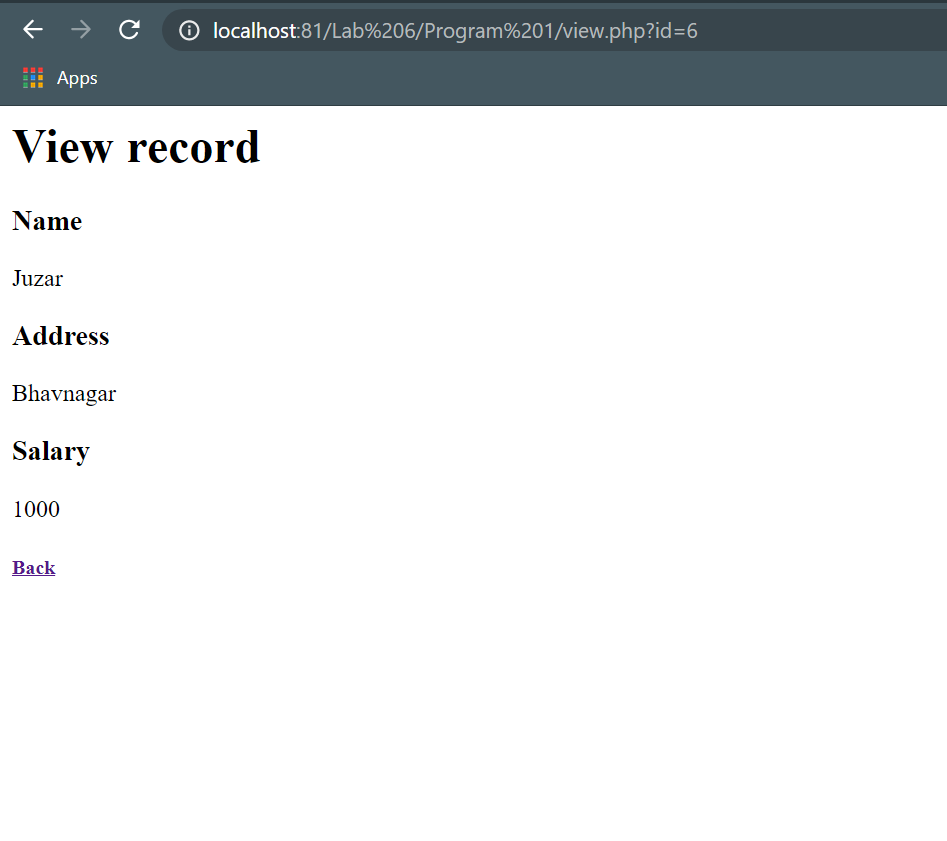
echo "<h5><a href='index.php'>Back</a><br>";

}

}

?>

**Output:**

****

**3. Output for update.php user is redirected to index.php with or without updated record.**

**update.php:**

<?php

require\_once "config.php";

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

if(empty($\_POST["name"])){

die("Please enter a name.");

} elseif(!filter\_var($\_POST["name"], FILTER\_VALIDATE\_REGEXP, array("options"=>array("regexp"=>"/^[a-zA-Z\s]+$/")))){

die("Please enter a valid name.");

}

// Validate address

if(empty($\_POST["add"])){

die("Please enter an address.");

}

// Validate salary

if(empty($\_POST["salary"])){

die("Please enter the salary amount.");

} elseif(!ctype\_digit($\_POST["salary"])){

die("Please enter a positive integer value.");

}

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

$sql = "UPDATE students SET name ='". $\_POST['name']."', salary ='". $\_POST['salary']."',address ='".

$\_POST['add']."' WHERE id = '".$id."'";

if(mysqli\_query($link,$sql)){

header("Location: index.php");

exit();

}

}

?>

<form action="" method="post">

<center>

<h1>Create record</h1><br>

Please edit the input values and submit to update the record <br>

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

Address:<textarea type="textarea" name="add" rows=2 cols=20></textarea><br>

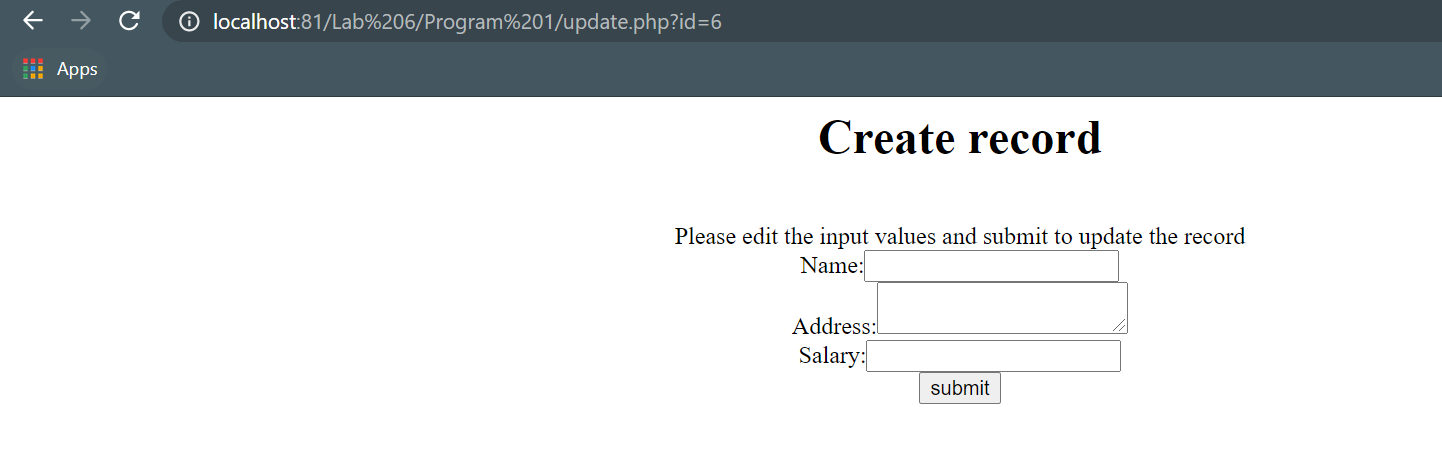
Salary:<input type="text" name="salary"><br>

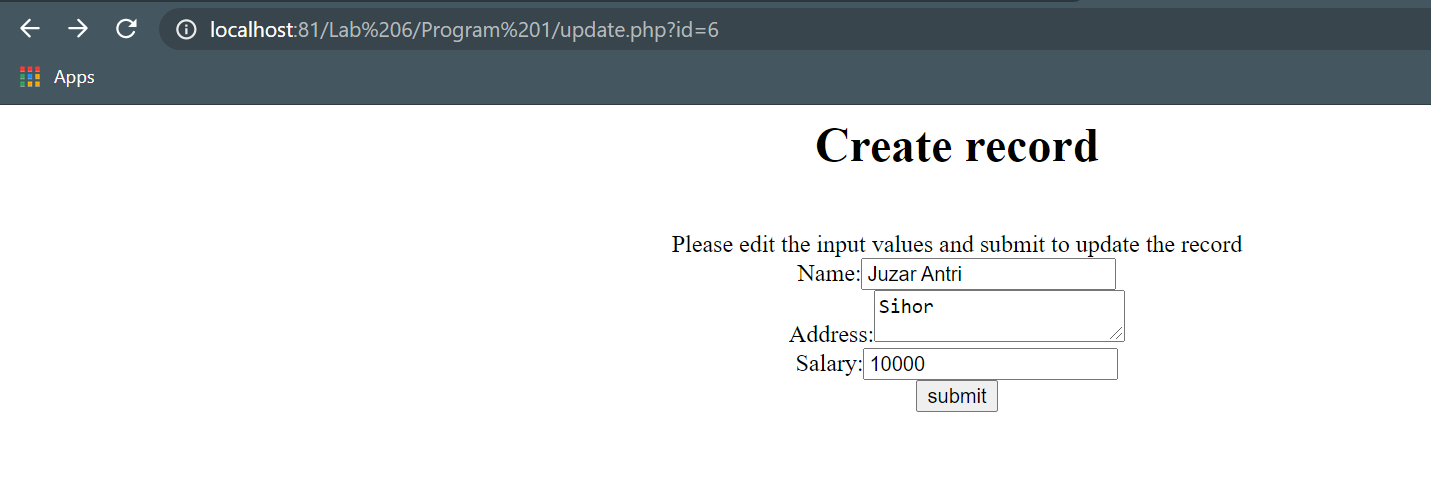
<input type="submit" name="submit" value="submit">

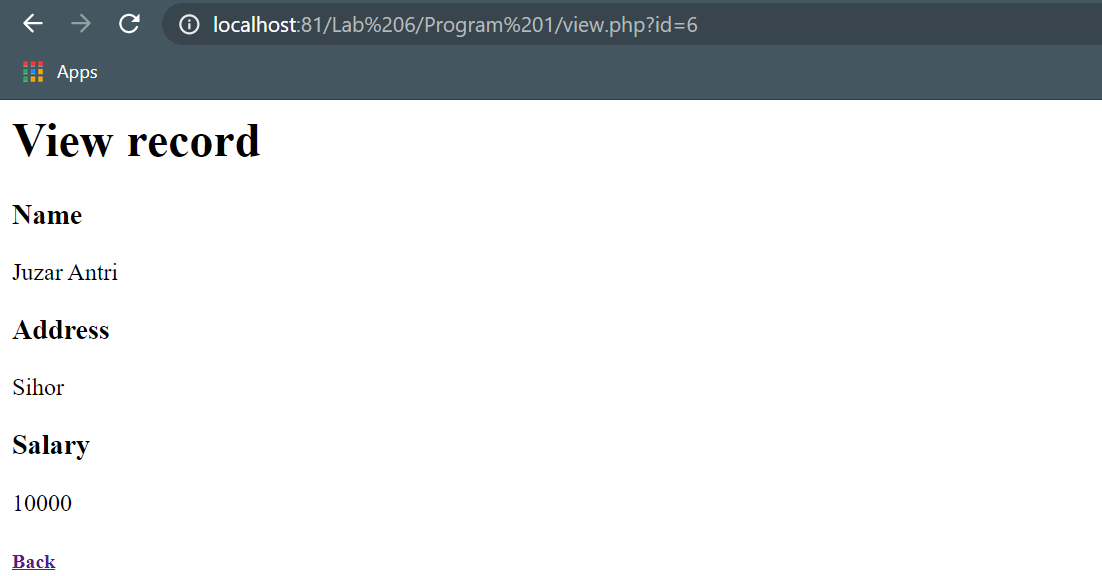
</center>

</form>

**Output:**

****

****

****

**4. Output for create.php user is redirected to index.php with or without created record.**

**create.php:**

<?php

require\_once "config.php";

if(isset($\_POST["submit"])){

// validate name

if(empty($\_POST["name"])){

die("Please enter a name.");

} elseif(!filter\_var($\_POST["name"], FILTER\_VALIDATE\_REGEXP, array("options"=>array("regexp"=>"/^[a-zA-Z\s]+$/")))){

die("Please enter a valid name.");

}

// Validate address

if(empty($\_POST["add"])){

die("Please enter an address.");

}

// Validate salary

if(empty($\_POST["salary"])){

die("Please enter the salary amount.");

} elseif(!ctype\_digit($\_POST["salary"])){

die("Please enter a positive integer value.");

}

$sql = 'INSERT INTO students(name,salary,address) VALUES(?,?,?)';

if($stmt = mysqli\_prepare($link,$sql)){

mysqli\_stmt\_bind\_param($stmt,"sis",$name,$salary,$address);

$name = $\_POST["name"];

$salary = $\_POST["salary"];

$address = $\_POST["add"];

if(mysqli\_stmt\_execute($stmt)){

header("location: index.php");

exit();

} else{

echo "Something went wrong. Please try again later.";

}

}

}

?>

<form action="" method="post">

<center>

<h1>Create record</h1><br>

Please fill this form and submit to add student record to database<br>

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

Address:<textarea type="textarea" name="add" rows=2 cols=20></textarea><br>

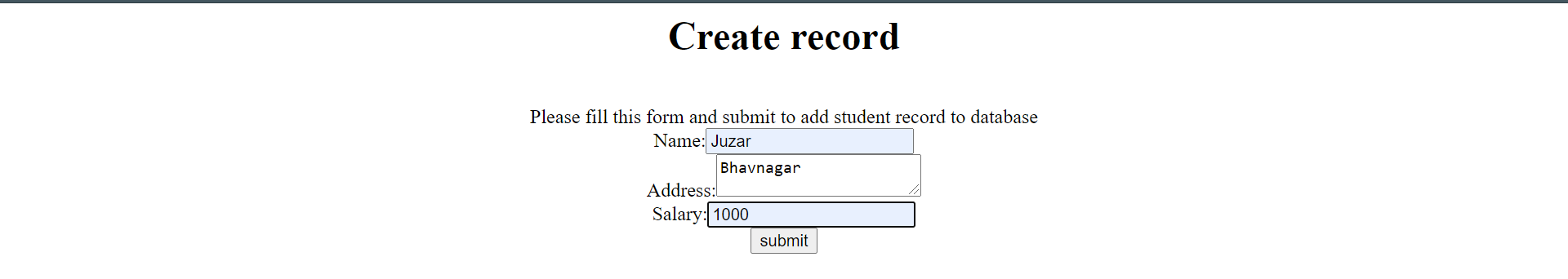
Salary:<input type="text" name="salary"><br>

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

</center>

</form>

**Output:**

****

**config.php:**

<?php

define('DB\_SERVER','localhost');

define('DB\_PASSWORD','');

define('DB\_USERNAME','root');

define('DB\_NAME','DM\_LAB\_6');

$link = mysqli\_connect(DB\_SERVER,DB\_USERNAME,DB\_PASSWORD,DB\_NAME);

if($link === false){

die("Error: Could not connect.".mysqli\_connect\_error());

}

?>

**5. Output for delete.php user is redirected to index.php with or without deleted record.**

**delete.php:**

<?php

require\_once "config.php";

session\_start();

$\_SESSION['id'] = $\_GET['id'];

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

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

$sql = "DELETE FROM students WHERE id = '".$id."'";

if(mysqli\_query($link,$sql)){

header("Location: index.php");

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

exit();

}

}

?>

<form action="" method="post">

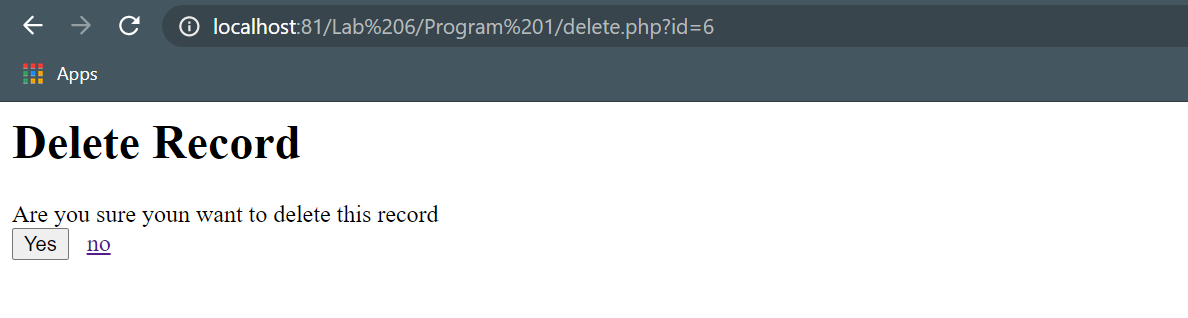
<h1>Delete Record</h1>

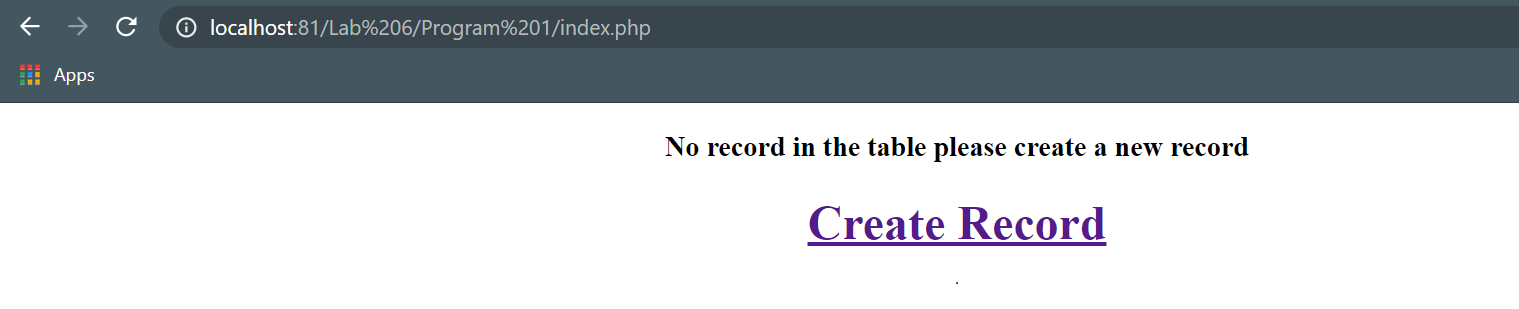
Are you sure youn want to delete this record<br>

<input type="submit" name="yes" value="Yes"> &nbsp&nbsp<a href="index.php">no</a>

</form>

**Output:**

****

****

**6. Write a code to demonstrate attack of sql injection.**

**config.php:**

<?php

define('DB\_SERVER','localhost');

define('DB\_PASSWORD','');

define('DB\_USERNAME','root');

define('DB\_NAME','DM\_LAB\_6');

$link = mysqli\_connect(DB\_SERVER,DB\_USERNAME,DB\_PASSWORD,DB\_NAME);

if($link === false){

die("Error: Could not connect.".mysqli\_connect\_error());

}

?>

**index.php:**

<?php

require\_once("config.php");

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

// juzar@antri.com' OR 1= 1 -- for sql injection

$sql = "SELECT \* FROM sqlinject WHERE uname = '".$\_POST['uname']."' AND password = '".$\_POST['upass']."'";

if($result = mysqli\_query($link,$sql)){

if(mysqli\_num\_rows($result) > 0){

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

echo "<tr>";

echo "<th>UserName</th>";

echo "<th>Password</th>";

echo "</tr>";

while ($row = mysqli\_fetch\_array($result)) {

echo "<tr>";

echo "<td>".$row['uname']."</td>";

echo "<td>".$row['password']."</td>";

echo "</tr>";

}

exit();

echo "</table>";

}

}

}

?>

<form action="" method="post">

Enter email and password to get data<br>

email: &nbsp&nbsp&nbsp&nbsp&nbsp<input type='text' name='uname'/><br>

password:<input type='password' name='upass'/><br>

<input type="submit" name="submit"><br>

</form>

**Output:**

