Lab 6

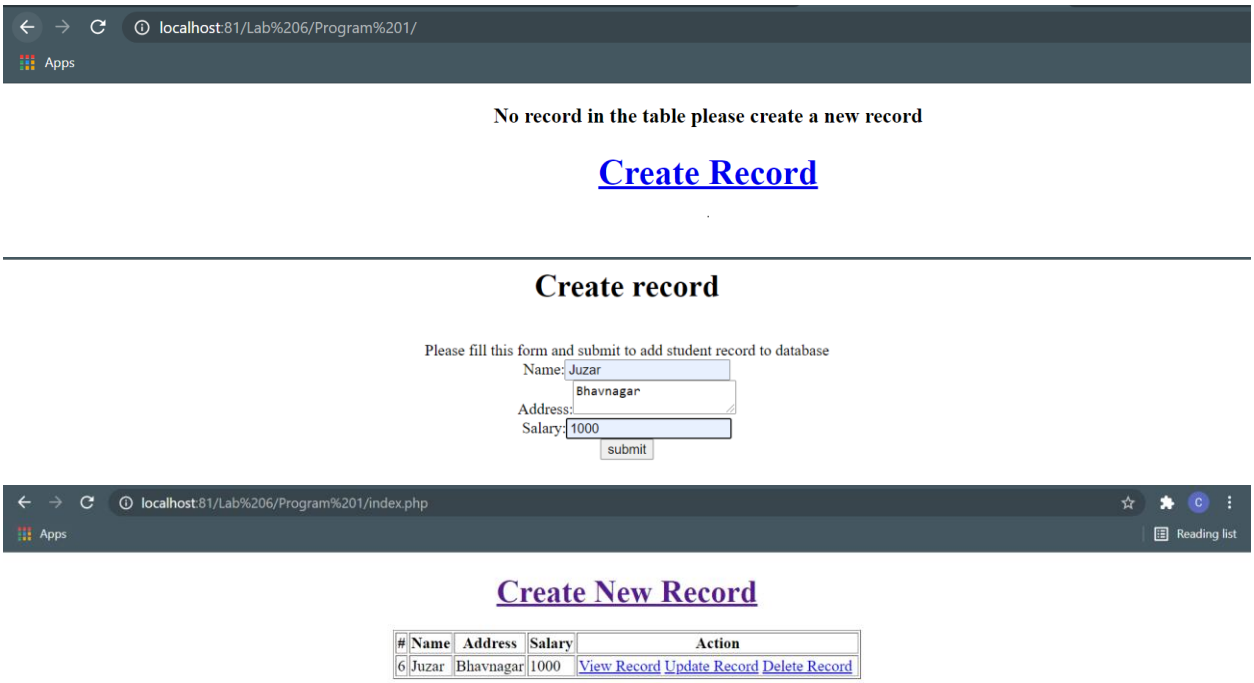
1. Create page index.php as shown below.

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> <a
href='update.php?id=".$row['id']."'>Update Record</a> <a href='delete.php?id=".$row['id']."'>Delete
Record</a> </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:

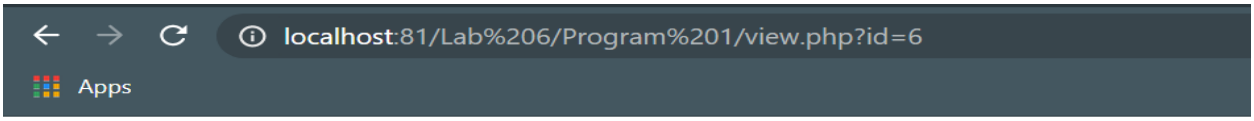


2. Output for view.php click on back takes user to index.php

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:



View record

Name

Juzar

Address

Bhavnagar

Salary

1000

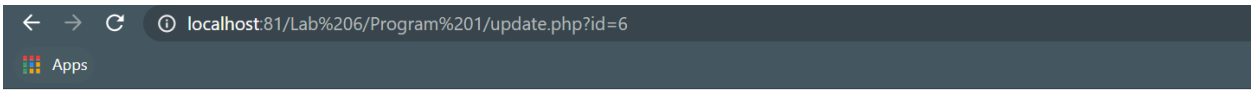
Back

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:



Create record

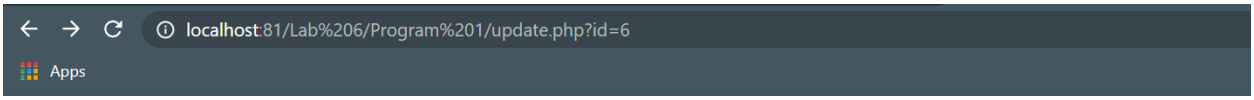
Please edit the input values and submit to update the record

Name:

Address:

Salary:

submit



Create record

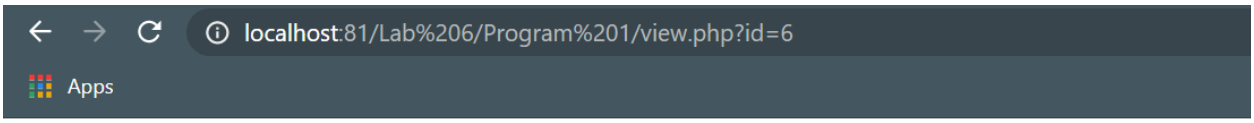
Please edit the input values and submit to update the record

Name: Juzar Antri

Address: Sihor

Salary: 10000

submit



View record

Name

Juzar Antri

Address

Sihor

Salary

10000

Back

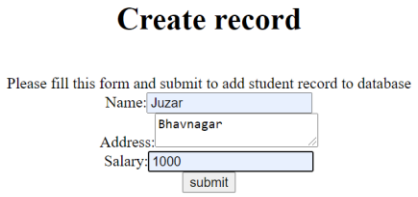
4. Output for create.php user is redirected to index.php with or without created record.

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:

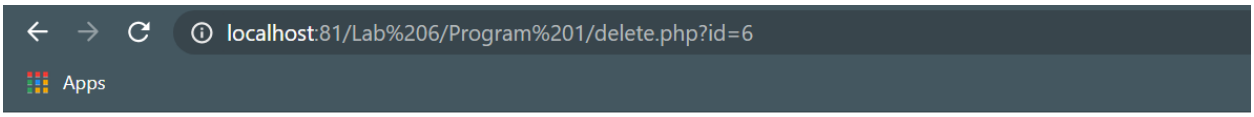
```
<?php
        define('DB_SERVER','localhost');
        define('DB_PASSWORD','');
        define('DB_USERNAME','root');
        define('DB_NAME','DM_LAB_6');

        $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">   <a href="index.php">no</a>
</form>
```

Output:



Delete Record

Are you sure youn want to delete this record

Yes no

No record in the table please create a new record

Create Record

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

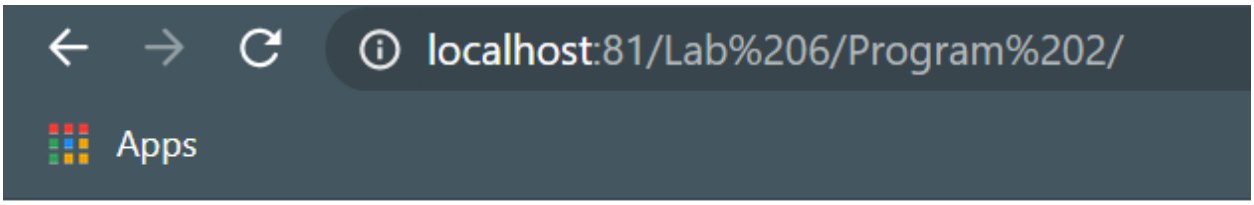
config.php:

```
<?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:      <input type='text' name='uname'/><br>
	password:<input type='password' name='upass'/><br>
	<input type="submit" name="submit"><br>
</form>
```

Output:

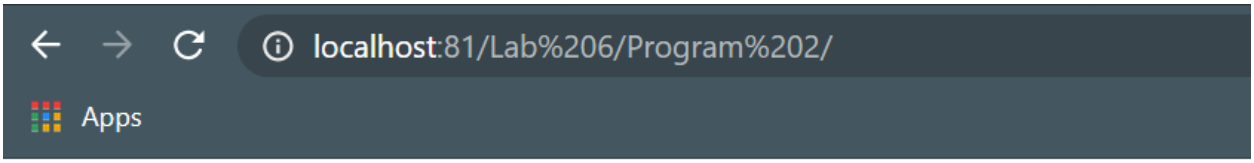


Enter email and password to get data

email: juzar@antri.com' OR 1= 1 -

password: •••••••

Submit



UserName	Password
juzar@antri.com	12345
dev@permar.com	12345
yash@joshi.com	12345