Troubleshooting activity
Web Systems
Alexis Consuelo
BSIS-2

Scenario 1:

```
<?php
$conn = mysqli_connect("localhost", "root", "", "class_db");
$id = $_POST['id'];
$sql = "SELECT * FROM students WHERE id = $id";
$res = mysqli_query($conn, $sql);
$r = mysqli_fetch_assoc($res);
echo $r['first_name'];
?>
```

Fixed code:

```
<?php
$conn = mysqli_connect("localhost", "root", "", "class_db");
$id = $_GET['id'];
if (!is_numeric($id)) {
   echo "Invalid ID";
   exit;
}
$sql = "SELECT * FROM students WHERE student_id = $id";
$res = mysqli_query($conn, $sql);
$r = mysqli_fetch_assoc($res);
echo $r['first_name'];
?>
```

Explanation:

Replace $_POST to $_GET to be able to acces the url

Scenario 2:

```
<?php
$conn = mysqli_connect("localhost","root","","class_db");
$fname = $_POST['fname'];
$sql = "SELECT * FROM students WHERE first_name = $fname";
```

```
$res = mysqli_query($conn, $sql);
?>
```

Fixed Code:

```
<?php
$conn = mysqli_connect("localhost","root","","class_db");
$fname = $_POST ['fname'];
$sql = "SELECT * FROM students WHERE first_name = '$fname'";
$res = mysqli_query($conn, $sql);
?>
```

Explanation:

Add single quotes to $fname

Scenario 3:

```
<?php
$conn = mysqli_connect("localhost","root","","class_db");
$age = $_GET['age'];
$sql = "SELECT * FROM students WHERE age = $age";
$res = mysqli_query($conn, $sql);
?>
```

Fixed Code:

```
<?php
$conn = mysqli_connect("localhost","root","","class_db");
$age = intval($_GET['age']);
$sql = "SELECT * FROM students WHERE age = $age";
$res = mysqli_query($conn, $sql);
?>
```

Explanation:

Replace $_GET with intval to avoid non numbers to be inputed

Scenario 4:

```
<?php
```

```
$conn = mysqli_connect("localhost","root","","class_db");
$first = $_POST['fname'];
$last = $_POST['lname'];
$sql = "INSERT INTO students (first_name,last_name) VALUES ('$first', '$last')";
mysqli_query($conn, $sql);
echo "Inserted!";
?>
```

Fixed Code:

```
<?php
$conn = mysqli_connect("localhost","root","","class_db");
$first =  $_POST['fname'];
$last = $_POST['lname'];
if (empty($first) || empty($last)) {
   echo "First name and last name are required.";
   exit;
}
$sql = "INSERT INTO students (first_name, last_name) VALUES ('$first', '$last')";
mysqli_query($conn, $sql);
echo "Inserted!";
?>
```

Explanation:

Adding the if statements checks to see if there are any empty spaces

Scenario 5:

```
<?php
$conn = mysqli_connect("localhost","root","","class_db");
$email = $_POST['emial']; // misspelled
$sql = "SELECT * FROM students WHERE email='$email'";
$res = mysqli_query($conn, $sql);
?>
```

Fixed Code:

```
<?php
$conn = mysqli_connect("localhost","root","","class_db");
$email = $_POST['email'];
```

```
$sql = "SELECT * FROM students WHERE email='$email'";
$res = mysqli_query($conn, $sql);
?>
```

Explanation:

Correct the spelling of 'email'

Scenario 6:

```
<?php
$conn = mysqli_connect("localhost","root","","class_db");
$sql = "DELETE FROM students WHERE id = " . $_GET['id'];
mysqli_query($conn, $sql);
?>
```

Fixed Code:

```
<?php
$conn = mysqli_connect("localhost","root","","class_db");
$id = intval($_GET['id']);
$sql = "DELETE FROM students WHERE student_id = $id";
mysqli_query($conn, $sql);
?>
```

Explanation:

Adding the intval allows to receive a number input

Scenario 7:

```
<?php
$conn = mysqli_connect("localhost","root","","class_db");
$id = $_POST['id'];
$email = $_POST['email'];
$sql = "UPDATE students SET email=$email WHERE id=$id";
$res = mysqli_query($conn, $sql);
echo "Updated!";
?>
```

Fixed Code:

```
<?php
$conn = mysqli_connect("localhost","root","","class_db");
$id = $_POST['id'];
$email = $_POST['email'];
$sql = "UPDATE students SET email='$email' WHERE student_id=$id";
$res = mysqli_query($conn, $sql);
if ($res && mysqli_query($conn) > 0) {
  echo "Updated!";
} else {
  echo "Error: " . mysqli_error($conn);
}
?>
```

Explanation:

Add single quotes around $email and checks if anything has changed to be able to say updated

Scenario 8:

```
<?php
$conn = mysqli_connect("localhost","root","","class_db");
$res = mysqli_query($conn,"SELECT * FROM students");
$row = mysqli_fetch_assoc($res);
echo $row['email']; // prints first only
?>
```

Fixed Code:

```
<?php
$conn = mysqli_connect("localhost","root","","class_db");
$res = mysqli_query($conn,"SELECT * FROM students");
while ($row = mysqli_fetch_assoc($res)) {
  echo $row['email'] . "<br>";
}
?>
```

Explanation:

Uses loop to display the rows

Scenario 9:

```
<?php
$id = $_POST['id'];
?>
<a href="view.php?id=3">View Student</a>
```

Fixed Code:

```
<?php
$id = $_GET['id'];
?>
<a href="view.php?id=3">View Student</a>
```

Explanation:

Replace $_POST with $_GET to access the url

Scenario 10:

```
<?php
$age = $_POST['age'];
$sql = "SELECT * FROM students WHERE age = $aeg"; // wrong variable
name
?>
```

Fixed Code:

```
<?php
$age = $_POST['age'];
$sql = "SELECT * FROM students WHERE age = $age";
?>
```

Explanation:

Correct spelling "aeg" to "age"

Scenario 11:

```
<form method="GET" action="save.php">
<input name="email">
</form>
```

Fixed Code:

```
<form method="POST" action="save.php">
<input name="email">
</form>
```

Explanation:

Replace method GET to POST

Scenario 12:

```
<?php
$id = $_GET['id'];
$sql = "SELECT * FROM students WHERE id = '$id'"; // id is int
?>
```

Fixed Code:

```
<?php
$id = (int)$_GET['id'];
$sql = "SELECT * FROM students WHERE student_id = $id";
?>
```

Explanation:

Adding an int to the code allows numbers to be inputed/accepted

Scenario 13:

```
<?php
$newEmail = $_POST['email'];
$sql = "UPDATE students SET email='$newEmail'";
mysqli_query($conn,$sql);
?>
```

Fixed Code:

```
<?php
$newEmail = $_POST['email'];
$id = $_POST['id'];
$sql = "UPDATE students SET email='$newEmail' WHERE student_id=$id";
mysqli_query($conn,$sql);
```

```
?>
```

Explanation:

Adding WHERE allows to update the record

Scenario 14:

```
<?php
$data = $_POST;
$sql = "INSERT INTO students (first_name, last_name, email)
VALUES ($data[first_name], $data[last_name], $data[email])";
?>
```

Fixed Code:

```
<?php
$first =  $_POST['fname'];
$last = $_POST['lname'];
$email = $_POST['email'];
$sql = "INSERT INTO students (first_name, last_name, email) VALUES ('$first', '$last',
'$email')";
mysqli_query($conn, $sql);
?>
```

Explanation:

Use proper syntax and single quotes

Scenario 15:

```
<?php
$page = $_GET['page'];
$limit = 5;
$offset = $page * $limit;
$sql = "SELECT * FROM students LIMIT $offset, $limit";
?>
```

Fixed Code:

```
<?php
$page = intval($_GET['page']);
```

```
if ($page < 0) $page = 0;
$limit = 5;
$offset = $page * $limit;
$sql = "SELECT * FROM students LIMIT $offset, $limit";
?>
```

Explanation:

Limiting the pages available by using the $page <0