Exercise 11.11 – Sanitize Inputs

- **PHP Functions & Procedures**
  - **$connection = mysqli_connect(DBHOST, DBUSER, DBPASS, DBNAME);**
  - **$result = mysqli_query($connection, $sql);**
  - **$row = mysqli_fetch_assoc($result);**
  - **mysqli_free_result($result);**
  - **if ($_SERVER["REQUEST_METHOD"] == "GET") {**
  - **if (isset($_GET['gallery']) && $_GET['gallery'] > 0) {**
  - **$gallery = $mysqli->real_escape_string ($_GET['gallery']);**
  - **$mysqli->real_escape_string(), http://php.net/manual/en/mysqli.real-escape-string.php**

```
<?php
//config.php - lab11-exercise08-mysqli.php
define('DBHOST', 'localhost');
define('DBNAME', 'art');
define('DBUSER', 'testuser');
define('DBPASS', 'secret');
define('DBCONNSTRING','mysql:host=localhost;dbname=art');
?>
//lab11-exercise11.php
<?php require_once('config.php'); ?>
<!DOCTYPE html>
<html>
 <head>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Chapter 11</title>
  <!-- Bootstrap core CSS  -->
  <link href="bootstrap3_defaultTheme/dist/css/bootstrap.css" rel="stylesheet">
 </head>
<body>
<form method="get" action="lab11-exercise09.php">
 <div class="well">
   <h1>User Input (mysqli)</h1>
   Gallery:
   <select name="gallery">
     <option value="0">Select a gallery</option>
     <?php
     $connection = mysqli_connect(DBHOST, DBUSER, DBPASS, DBNAME);
     if ( mysqli_connect_errno() ) {
       die( mysqli_connect_error() );
     }
     $sql = 'select * from Galleries order by GalleryName';
     if ($result = mysqli_query($connection, $sql)) {
       // loop through the data
       while($row = mysqli_fetch_assoc($result))
        {
```

```
            echo '<option value="' . $row['GalleryID'] . '"';
            if (isset($_GET['gallery']) && $row['GalleryID'] == $_GET['gallery']) echo ' selected ';
            echo '>';
            echo htmlentities($row['GalleryName'], ENT_IGNORE | ENT_HTML5, "ISO-8859-1");
            echo ' (' . $row['GalleryCity'] . ')';
            echo '</option>';
          }
          // release the memory used by the result set
          mysqli_free_result($result);
        }

        ?>
      </select>
      <input class="btn btn-default" type="submit" value="Submit">
</div>
<div class="container">
  <div class="row">

  <?php
  if ($_SERVER["REQUEST_METHOD"] == "GET") {
    if (isset($_GET['gallery']) && $_GET['gallery'] > 0) {
      $gallery = $mysqli->real_escape_string($_GET['gallery']);
      $sql = 'select * from ArtWorks where GalleryId=' . $gallery;
      if ($result = mysqli_query($connection, $sql)) {
        // loop through the data
        while($row = mysqli_fetch_assoc($result))
        {
  ?>
            <div class="col-md-3">
              <div class="thumbnail">
                <img src="images/art/works/square-medium/<?php echo $row['ImageFileName']; ?>.jpg"
                  title="<?php echo $row['Title']; ?>" alt="<?php echo $row['Title']; ?>"
                  class="img-thumbnail img-responsive">
                <div class="caption">
                  <?php echo $row['Title']; ?>
                </div>
              </div>
            </div>
<?php
        } // end while

        // release the memory used by the result set
        mysqli_free_result($result);

      } // end if ($result

    } // end if (isset
```

```
  } // end if ($_SERVER
  // close the database connection
  mysqli_close($connection);
?>
   </div>
</div>
</form>
</body>
</html>
```

Nothing is selected: (No selection, click submit, no action is taken)