**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**](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)



