

## Database Design, CSCI 340, Spring 2016

### Lab 8, SQL Injection, April 8

Say that you are in a class of 6 students (student ids are 1-6) and the instructor has chosen to let the students see their grades via a web site. Here is the link of the web site:

[https://katie.mtech.edu/~schahczenski/SQL\\_InjectionExperiment/](https://katie.mtech.edu/~schahczenski/SQL_InjectionExperiment/)

Where it says "Enter your student ID" enter a number between 1 and 6 to see the grade of that person.

Try using SQL Injection to see the grades of the other students in that class.

What did you enter?

Files:

#### index.php

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
  "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">

<head>
  <title>Experiment With SQL Injection</title>
  <link rel="stylesheet" type="text/css" href="main.css" />
  <meta http-equiv="Content-Type"
    content="text/html; charset=utf-8" />
</head>

<body>

  <h1>Find Grade</h1>

  <form action="displayGrade.php" method="post">

    <label>
      Enter your student ID:
    </label>
    <input type="text" name="txtStudID" />

    <br />
    <br />
    <input type="submit" value="Display Grade">

    <br />
  </form>

</body>
</html>
```

## displayGrade.php

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
  "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">

<head>
  <title>Experiment With SQL Injection</title>
  <link rel="stylesheet" type="text/css" href="main.css" />
  <meta http-equiv="Content-Type"
    content="text/html; charset=utf-8" />
</head>

<body>

  <h1>Display Grade</h1>

<?php
  $dbname='StudentInformation';
  $username = 'csci340User';
  $password = 'csci340Pass';

  mysql_connect('localhost',$username, $password);
  @mysql_select_db($dbname) or die("Unable to seelct database");

  // Get student ID from input form.
  $studentID = $_POST['txtStudID'];

  // Retrieve grade for the student
  $query = "SELECT CONCAT(fName,' ', lName) AS 'name', score, grade
    FROM Student
    WHERE studentId=".$studentID.";";

  $result = mysql_query($query);
  $row_count = mysql_numrows($result);

  // Handle an empty table.
  if($row_count==0) {
    echo ("<h3>Student ID not found in the database.</h3>");
  } else {

?>

<table>
  <tr>
    <th>Name</th>
    <th>Score</th>
    <th>Grade</th>
  </tr>

<?php
  $i=0;
  while($i < $row_count) {
    $name = mysql_result($result, $i, "name");
    $score = mysql_result($result, $i, "score");
    $grade = mysql_result($result, $i, "grade");

?>
```

```
<tr>
  <td><?php echo ($name); ?></td>
  <td><?php echo ($score); ?></td>
  <td><?php echo ($grade); ?></td>
</tr>
<?php
    $i++;
  } // while
?>

</table>

<?php
  } // else

  echo ("<br /><br />Here is the query: ".$query."<br /><br />");
?>

<br /><br /><br />
<a href="index.php">Back</a>

</body>
</html>
```