Secure Viewing SQL from HTML

Start by creating a new table in your database called users:

Enter the command that follows to create a table in your database. In this table the user ID number of a user serves as the primary key. Each model ID number is correlated with its first and last name.

mysql> CREATE TABLE users (

-> user\_id INT UNSIGNED NOT NULL AUTO\_INCREMENT,

-> username VARCHAR(128),

-> password VARCHAR(128),

-> PRIMARY KEY (user\_id));

Next you will need to add users into this database so they have admin rights.  Here is an example of adding a user:

mysql> insert into users(username, password) values ('admin', 'pass');

Then, we will make two new pages for pulling data.

pullDataAdmin.html

|  |  |
| --- | --- |
|  | <html>  <head>  <h2>A webpage that adds information to my database.</h2>  </head>   <body>  <h3>Username:</h3>  <form action="pullDataAdmin.php" method="post">  <input type="text" name="username">   <h3>Password:</h3>  <input type="password" name="password">  <br><br>    <input type="submit" value="Retrieve Data">  </form>  </body> </html> |

pullDataAdmin.php

|  |  |
| --- | --- |
|  | <head> <title>The data</title> <body> <h1> Database information </h1> <?php $servername = getenv('IP'); $username = getenv('C9\_USER'); $password = ""; $database = "c9"; $dbport = 3306;  // Create connection $db = new mysqli($servername, $username, $password, $database, $dbport); // Check connection if ($db->connect\_error) { die("Connection failed: " . $db->connect\_error); }  echo "Connected successfully (".$db->host\_info.")"; echo "<br><hr>";  //Get the username and password that they typed  $name = $\_POST['username']; $pass = $\_POST['password']; //Check our database to see if there are any records where this matches. $sqlStr = "SELECT \* FROM users WHERE username = '$name' and password = '$pass';";  $result = $db->query($sqlStr); $num\_rows = $result->num\_rows;  //If there are one or more people in our user list with this user/password combo, display info. if ($num\_rows > 0) { $sqlStr = "Select \* from names;";  $selRes = $db->query($sqlStr); echo $sqlRes; if ($selRes) { while($selRow = mysqli\_fetch\_assoc($selRes)) { echo $selRow['lastName'] . ', ' . $selRow['firstName'] . '<br/>'; } } }  //There was nobody with this name & password. else { echo 'Invalid username & password.'; } ?> <br><br> </body> </html> |

Try to log in with the username and password that you setup earlier.

Now try a name that is not in the database.  Do you still see the information?

Finally, try the following combo

Username: fakeuser  
Password: fakepassword' OR 1='1

What happens?  Why?