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.

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?