I approached this activity by using the video in the module resources as a guide. I started by creating a function that escapes all user supplied input to prevent them from being injected. In the same function I inserted a quote after the first equals sign and then at the end of the input, this will pass both NAME and the user input as a single parameter to the database which return no results.

Inside of the run\_query function I created an if statement that finds an “OR” clause in the query, if one is found it then moves forward with escaping all injected SQL. Once the escaped input is returned, I then output the information regarding the query. I display the original query, a statement possible SQL Injection detected and finally the escaped input. Finally, I return false which prevents the code from being run.

