Unit 5 Get User

**Corey Crooks**

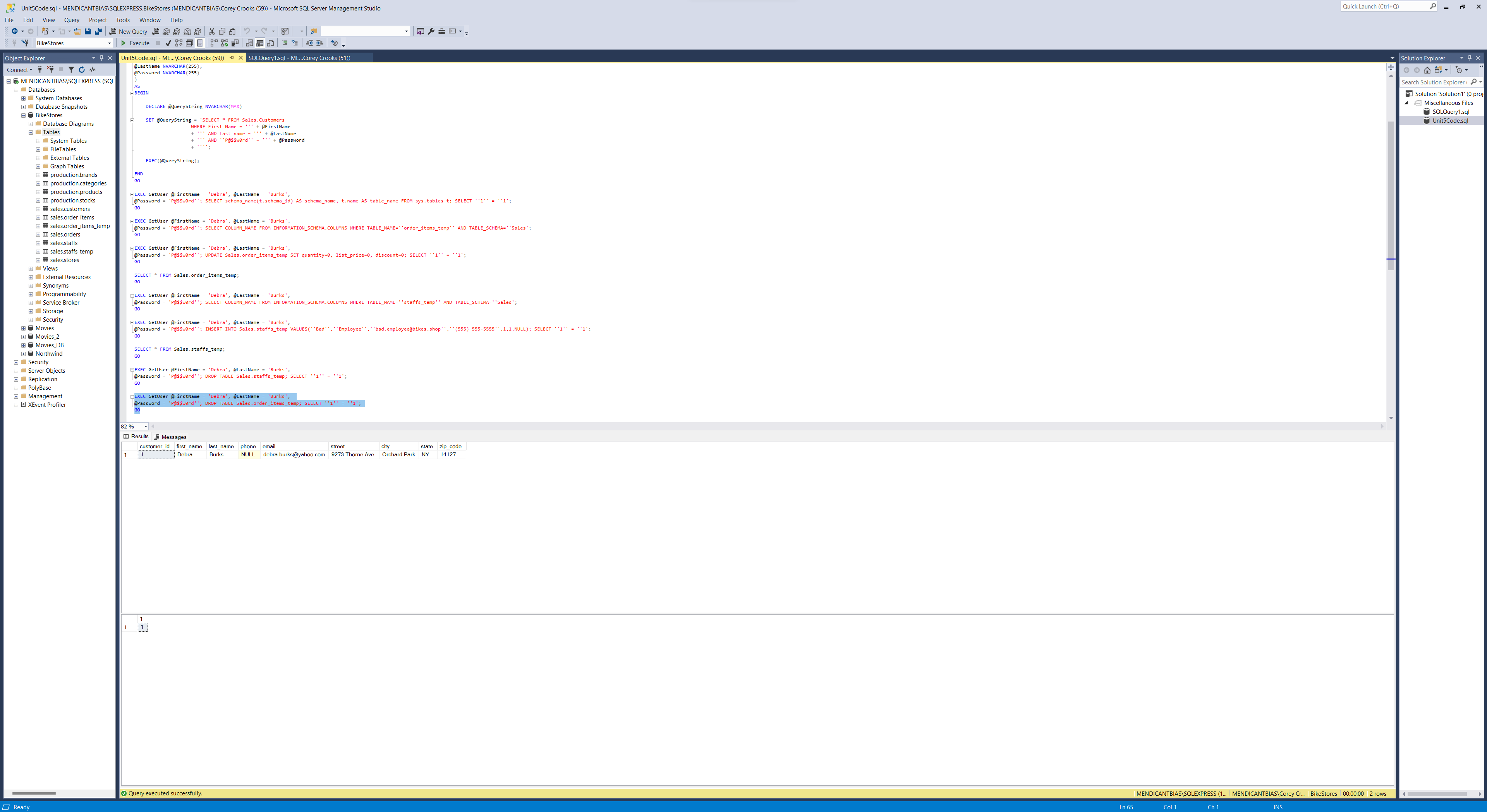
**Purdue University Global**

**IT350 – Advanced Database Concepts**

**Jason Johnson**

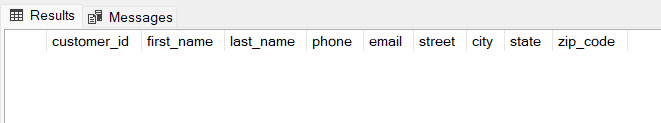
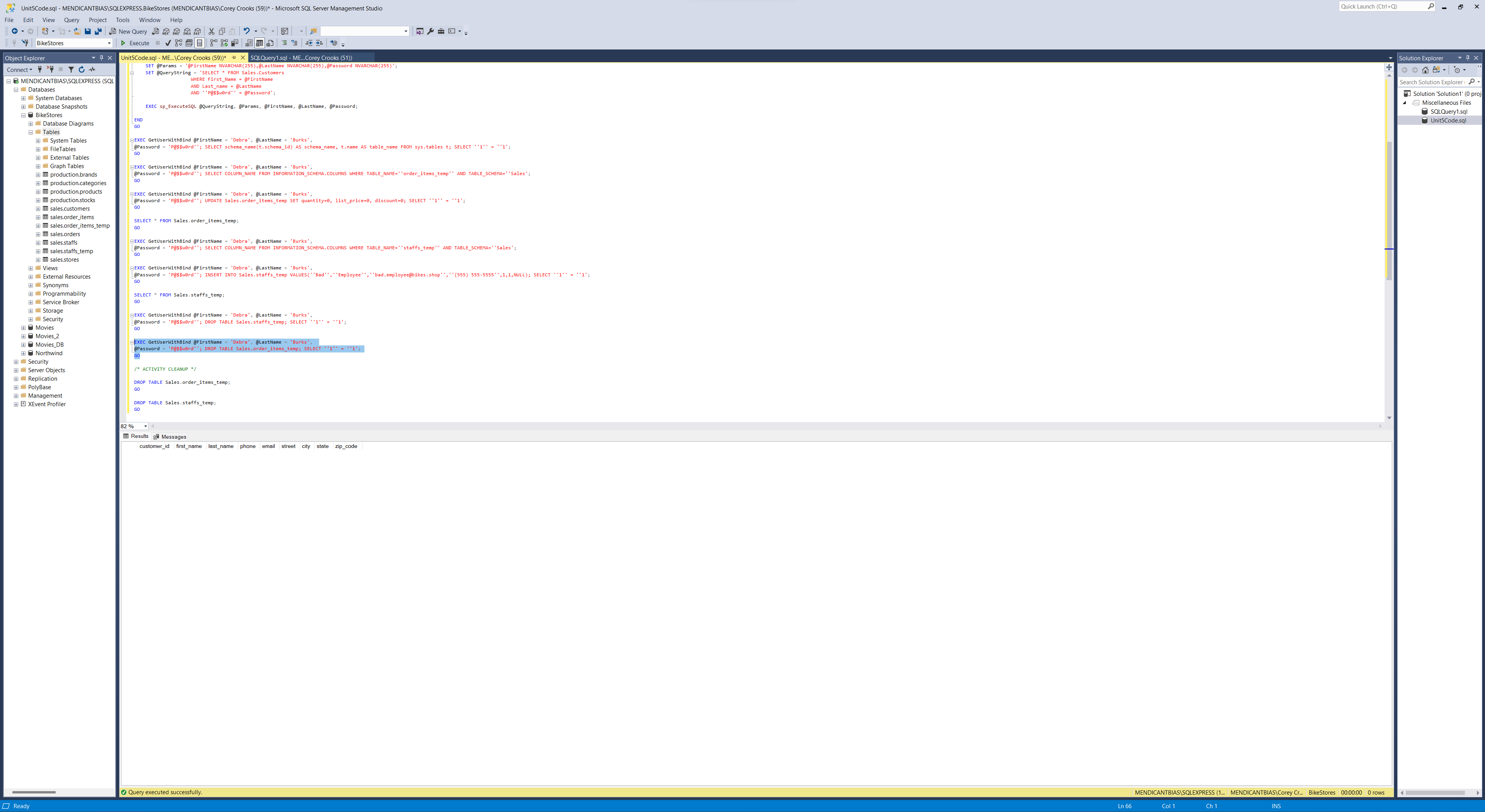
**March 8th, 2023**

**Part 1 — Get User Without Bind**



The above SQL statements detail the “GetUser” command in SQL Server Studio. In these statements, the code creates temporary tables, a high-level query, and modifies the data within that query using an account in the database object.

The statements executed without error, each doing what they are “supposed” to do including accessing data, and dropping tables. This could present an issue as a database designer, as executing this query bypasses any permissions required to accomplish the task you have set before it. In this part, the user was able to perform high-level administrator tasks such as deleting entire tables of data all without high-level access due to the nature of the command.

**Part 2 — Get User With Bind**

These SQL commands function differently from the simple “GetUser” command. This is seen demonstrated effectively in the output section. In the statements of the query, we have performed all the functions of the previous “GetUser” part 1 such as creating temporary tables, a high-level query, and modifying the data within that query using an account in the database object.

However, many of these statements were blocked by Microsoft SQL Server Studio because of the aforementioned permissions. The SQL Server Studio recognized the administration level of the user executing these queries, and was able to check the permissions of the account while comparing the permissions required for such an action. In these cases, the user was unable to perform functions such as dropping a table due to the restrictions imposed by the system using the “GetUserWithBind” query. You can see this at work in the bottom screenshot in the Part 2 outputs as a simple blank screen. This ensures that access to the BikeStores database remains as secure as possible, with minimal accidental damage to data stored, and minimal risks in the case of compromised credentials.