Unit 9

Implementing Databases with SQL

(Reflection)

This unit dealt with SQL language to query and manipulate databases and addressed the need to understand access security aspects of a SQL-based database. The majority of the SQL exercises used MySQL. However, the concepts apply to other SQL implementations, such as Oracle's SQL implementation or even Microsoft's SQL Server. *For examples of DML and DDL SQL exercises, please refer to* ***Unit 10: Working with SQL - Codio Exercises.***

SQL Queries

Two categories of SQL queries exist:

- ***Data Manipulation (DML).*** These queries deal with modifications to row data within tables, such as SELECT, INSERT, UPDATE or DELETE data. These statements are often known as CRUD statements because they support Create; Read; Update, and Delete operations.
- ***Data Definition (DDL).*** These SQL statements deal with database schemas such as tables, views, stored procedures, indexes and triggers. These groups of queries include ALTER, DROP, TRUNCATE, CREATE on various database objects.
- ***Data Control (DCL).*** These statements focus on access control and permissions and include keywords like GRANT and REVOKE.
- ***Transaction Control (TCL).*** These SQL statements are concerned about the transaction support within the database environment. They include keywords such as COMMIT, ROLLBACK, SAVEPOINT and SET TRANSACTION.

SQL Issues

Regardless of the category of SQL statements to execute, various issues can arise from incorrectly configured database systems. Therefore I learned from this unit the need to consider the following main points:

- ***Privileged access.*** Users may execute queries against the database for which they usually do not have access. They may have more privileges than required, allowing them to access sensitive information.

  > **CONSIDERATION:** *This concept is applicable across the whole spectrum of Information Systems, not just databases.*

- ***SQL injection.*** This issue involves a lack of validation on user-provided data that is used directly within SQL queries. For example, "Forename" requires input, and the user provides "`jo'; `**`drop table authors;`**". The server then executes the DML "`select * from authors where name= <user_input>`"

- ***Coss Site Scripting (XSS).*** The application inserts part of the user's input in the following HTML page/database query. The inserted code is not sanitised and may execute destructive script or database query code. Usually, such attacks make use of social engineering to trick the user into navigating to a malicious URL.