**Artifact Three Enhancement DAD 220 Project One**

Original work performed in Dec of 2022

Enhancements performed in September of 2023

To enhance the original work, I first downloaded and installed the environment MySQL.

Putting security first, my initial steps were to configure my user profile to include an authentication plugin. MySQL was able to accommodate this requirement:

A screenshot of a computer

Description automatically generated

The authentication type is the newer item, caching\_sha2\_password. In summary, mysql\_native\_password is the default authentication plugin, which is less secure and suitable for legacy applications. caching\_sha2\_password is a more secure plugin that supports strong password encryption and is suitable for modern applications.

A screenshot of a computer

Description automatically generated

Data at Rest EncryptionData is encrypted automatically, in real time, prior to writing to storage and decrypted when read from storage. As a result, hackers and malicious users are unable to read sensitive data directly from database files. MySQL Enterprise TDE uses industry standard AES algorithms. In a real-world application this feature would be utilized to ensure secure data. The screenshot below shows the permissions I have as the Administrator.

A screenshot of a computer

Description automatically generated

To expound on the subject of security, at the very beginning of a project it is necessary to plan out exactly how every phase and component will be protected. Whether your system is on premises or with a cloud provider, shared or dedicated servers be aware of who has access to the equipment. When possible and each work environment is different, however, if possible, a separate server is always a safer option in the event of an issue with for example a Linux OS or PHP issue. Most compromises occur from password selections, ensure that password complexity is in place and utilized. Sensitive data will need to be encrypted and decrypted. In some cases, a third party will be involved in handling this function. Default Ports and Firewalls using an allowed IP address are other areas which also need to be considered when working on a project with databases. Backups are another consideration in the process. It is advisable to have a regular schedule for handling back ups which also need to be encrypted. Finally, it is vital to keep applications software up to date. Out of date applications are much more vulnerable to cyberattacks. Also ensuring that your code is up to date completes a smooth and secure project.

Below I have screenshots of the recreated schema “QuantigrationUpdates” showing its three tables: Customers, Orders, and RMA.

A screenshot of a computer

Description automatically generated

I have populated the tables with fictious data for demonstration purposes.

A screenshot of a computer

Description automatically generated

I chose to use different values than were used in the original assignment to demonstrate adaptability.

A screenshot of a computer

Description automatically generated

Another way to load data is to use a SQL script. I will include separate SQL files for the “QuantigrationUpdates” and for the “store” schemas. When MySQL opens a file such as this it will load the commands in the document eliminating and streamlining the process of creating and populating the tables from the command prompt manually. Below are screenshots of the process initiated:

A screenshot of a computer

Description automatically generated

This shows the process to choose a file to load.

A screenshot of a computer

Description automatically generated

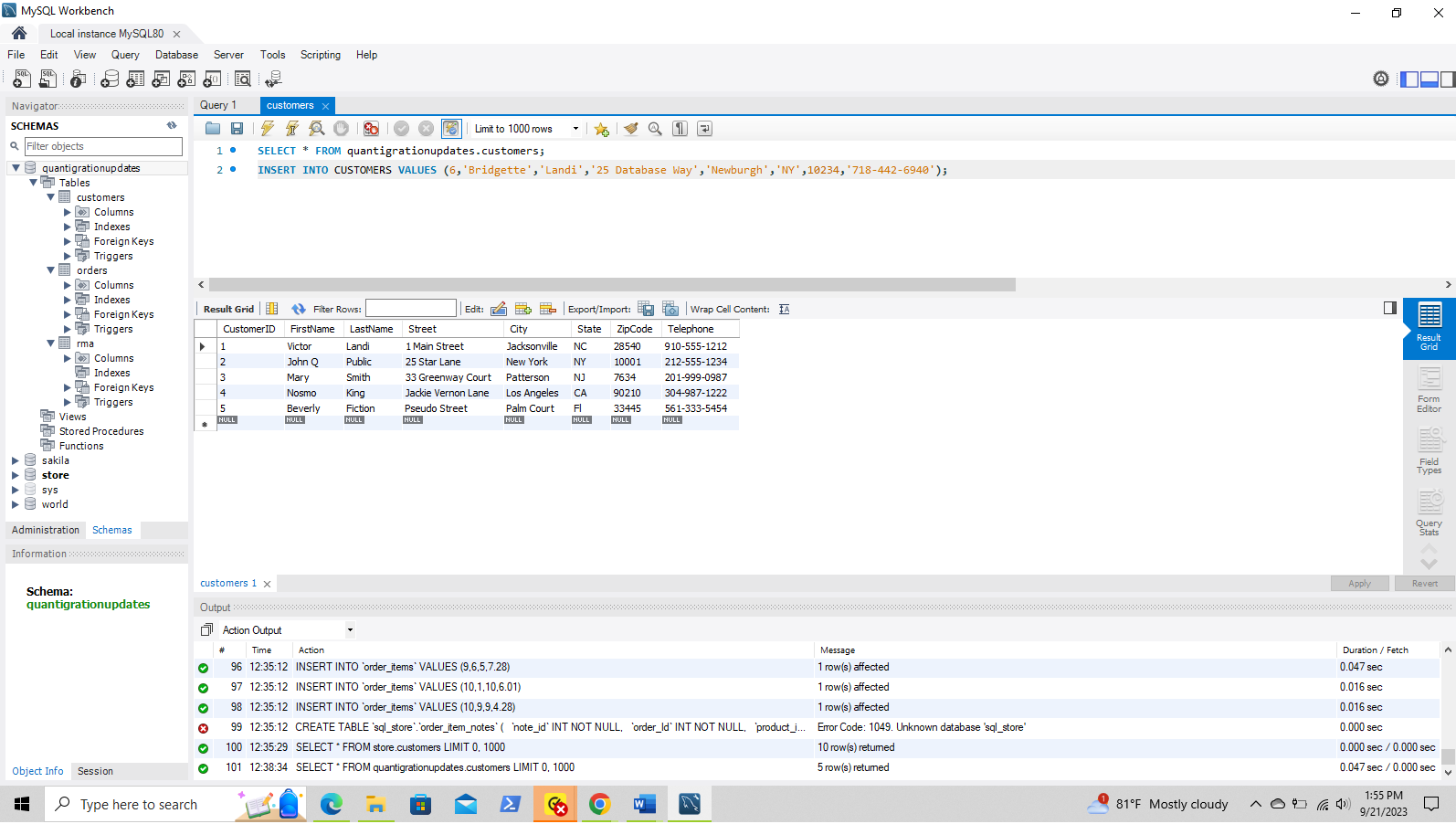
The file is loaded and ready to run, clicking on the lightning bolt shown in the pix above the cursor above line 1 will initiate the functions.

A screenshot of a computer

Description automatically generated

The above shot shows the new data added, I selected “customers” from the newly added schema “store.”

I will now demonstrate the CRUD functions to CREATE, READ, UPDATE, and DELETE: The screenshot below shows the command used. The screen shot following this shows the data changed, in this case a new row was added.



The process to insert the data is the CREATE function and the READ function is demonstrated below to show that the data was successfully added to the table.

A screenshot of a computer

Description automatically generated

Next, we will see the UPDATE function

A screenshot of a computer

Description automatically generated

This screenshot below shows the data updated, I changed the City from Newburgh to Staten Island

A screenshot of a computer

Description automatically generated

Finally, the DELETE function is shown in the following two screenshots.

A screenshot of a computer

Description automatically generated

From the RMA table I chose to delete all the records which met the following criteria: The Reason field reads “Wrong Part.”

A screenshot of a computer

Description automatically generated

The above screenshot shows the RMA refreshed after the change to reflect that all records previously showing the reason as “wrong part” have been successfully deleted. To accomplish the delete function it was necessary to make a change in the Preferences section to allow for deletion capabilities. The screenshot below will show the above-mentioned area in the MySQL Workbench.

A screenshot of a computer

Description automatically generated

The box reading “Safe Updates (rejects UPDATEs and DELETEs with no restrictions) needed to be unchecked to allow me to perform some of the functions demonstrated above.