**USER AND AUTHORIZATION**

**EXPT NO: 8 DATE: 2/12/22**

**AIM:**  To implement multiple users and authorization operations in SQL

**THEORY**

1. Users

The MySQL user is a record in the **USER** table of the MySQL server that contains the login information, account privileges, and the host information for MySQL account. It is essential to create a user in MySQL for accessing and managing the databases.

The MySQL Create User statement allows us to create a new user account in the database server. It provides authentication, SSL/TLS, resource-limit, role, and password management properties for the new accounts. It also enables us to control the accounts that should be initially locked or unlocked.

Syntax:

* To create a new user and set a password for the user at the same time:

CREATE USER ‘*username*’@’localhost’ identified by ‘*password*’;

* To login as a user:

mysql -u *username* -p

When you are prompted, enter the password for the user.

* To show all users:

Select user from mysql.user;

* To show current user:

Select user();

* To drop user:

drop user ‘*username*’

2. Privileges

In MySQL, a **privilege** is a right to perform an action on a database that must be **granted**to users. This effectively defines a user's access level on a database and what they can do within it. We can organize these privileges by scope into levels:

* Global privileges

Apply to all databases on the server. Administrative privileges fall into the global group because they enable a user to manage operations of the MySQL server and aren't specific to a particular database.

* Database privileges

Apply to specific databases in your MySQL instance and all of the objects within those databases (e.g., tables, columns, and views). You can also grant database privileges globally.

* Proxy privileges

Allow a user to act as if they have the privileges granted to another user.

* Privileges for database objects (tables, columns, stored routines, views, etc.)

Can apply to all objects of one type within a particular database or to specific objects, such as a certain table or view. You can also grant database object privileges globally.

We can choose access right from the below list on which privileges can be applied.

1. SELECT: It enables us to view the result set from a specified table.
2. INSERT: It enables us to add records in a given table.
3. DELETE: It enables us to remove rows from a table.
4. CREATE: It enables us to create tables/schemas.
5. ALTER: It enables us to modify tables/schemas.
6. UPDATE: It enables us to modify a table.
7. DROP: It enables us to drop a table.
8. INDEX: It enables us to create indexes on a table.
9. ALL: It enables us to give ALL permissions except GRANT privilege.
10. GRANT: It enables us to change or add access rights.

Syntax:

To grant privilege:

**GRANT** privilege\_name(s)  **ON** database\_name.table\_name **TO** user\_account\_name;

To grant privileges to all databases or tables we use a \*.

To show grants for user:

**SHOW** GRANTS **FOR** user\_account\_name;

To revoke privilege:

**REVOKE**  privilege [privilege] ON database\_name.table\_name privilege\_level **FROM** user1 [, user2] ..;

3. Indexes

**Indexes** are used to retrieve data from the database more quickly than otherwise. The users cannot see the indexes, they are just used to speed up searches/queries.

Syntax:

* To create index

CREATE INDEX *index\_name* ON *table\_name* (*column1*, *column2*, ...);

* To drop index

ALTER TABLE *table\_name* DROP INDEX *index\_name*;

**QUERIES**

1) Create 2 users lib1, lib2 and lib3.

2) Give all privileges on the view created in question 1(expt7)to lib1.

3) Give select, update privilege on title and publishername attribute of book table to lib2 with grant

option.

4) Let lib2 grant these privileges to lib1.

5) Grant all privileges on all the databases on the mysql server to lib3.

6) Login and check the privileges.

7) Revoke the view privileges from lib1.

8) Provide a list of various privileges available to the user.

9) Create an index on bookid attribute of book table.

**CONCLUSION**

The concept of User and authorization was studied in this experiment.