**MYSQL Database Setup and Configuration**

Ishan Prabhune (A20538828)

iprabhune@hawk.iit.edu

College of Computing,

Illinois Institute of Technology

ITMS 528: Database Security

Prof. Maurice Dawson

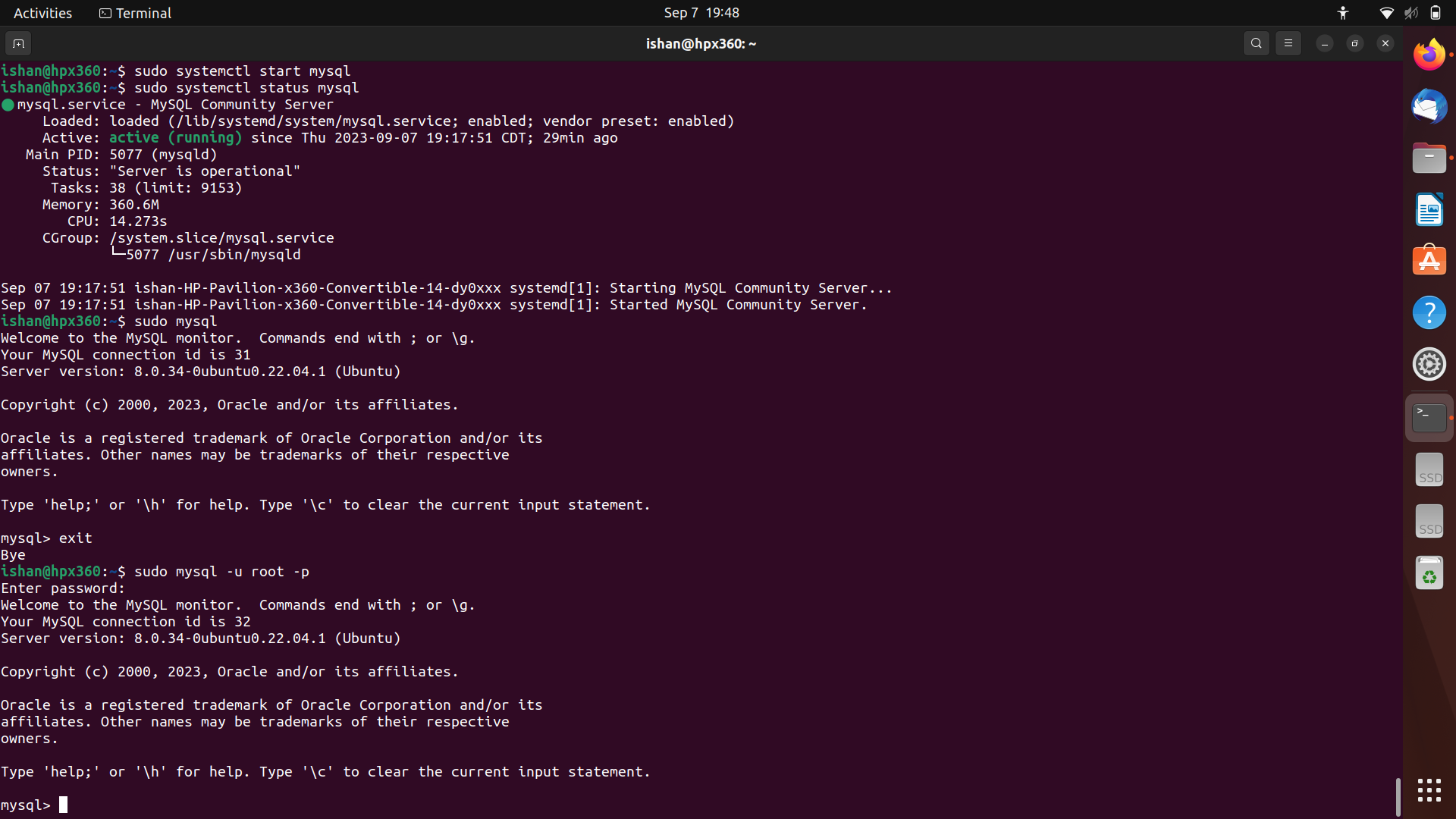
September 7, 2023

**Task 1: Installation and Setup:**

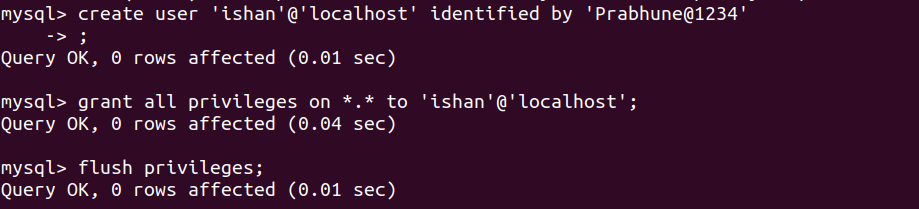
1. First Install MySql-Server from Terminal.
2. After Installation check status.
3. There are 3 types of security levels: Low, Medium & High.



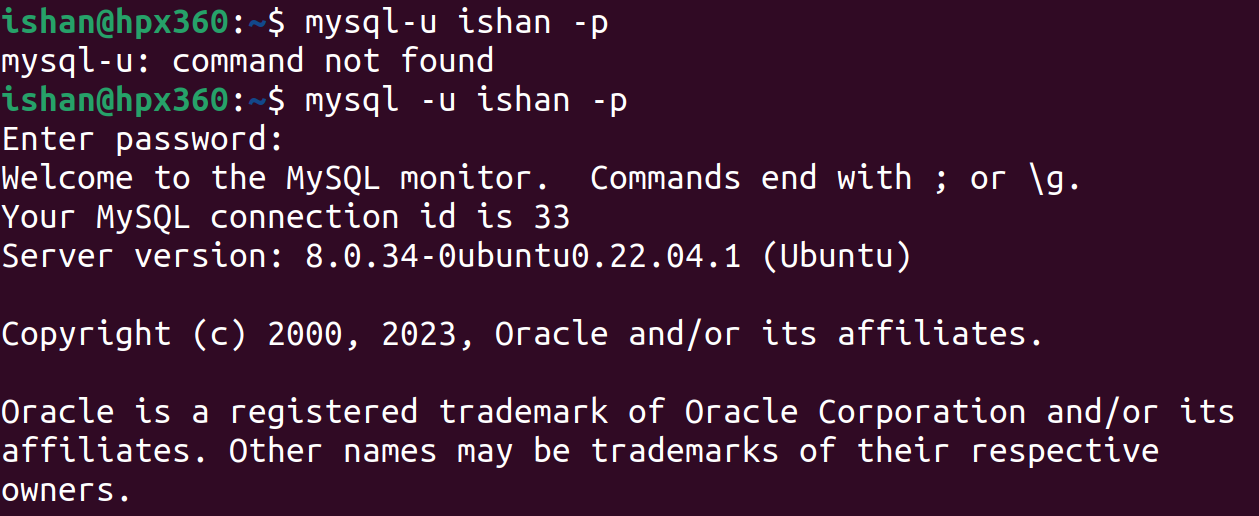
1. Start MySQL.



1. Create new SQL user.



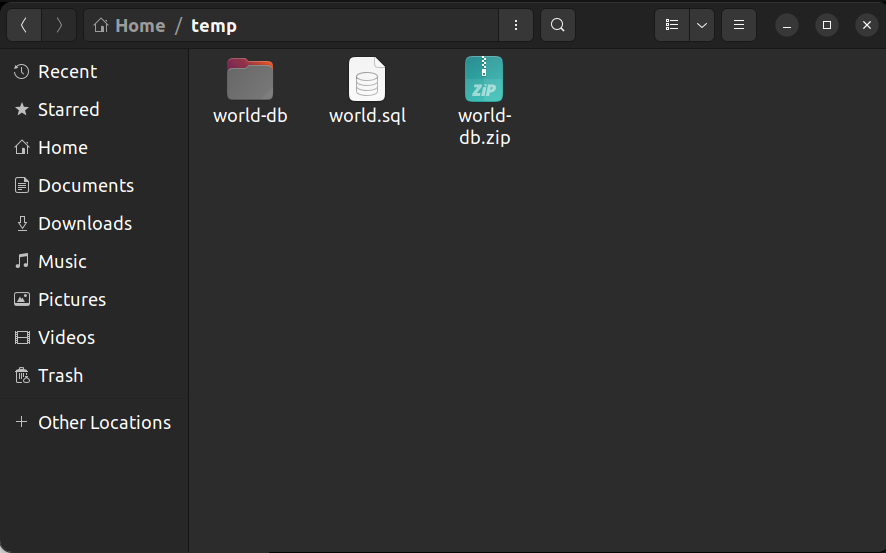
1. Login with new user.



1. Here we have created new user and logged in with new user credentials.

**Task 2: Database Creation and Population:**

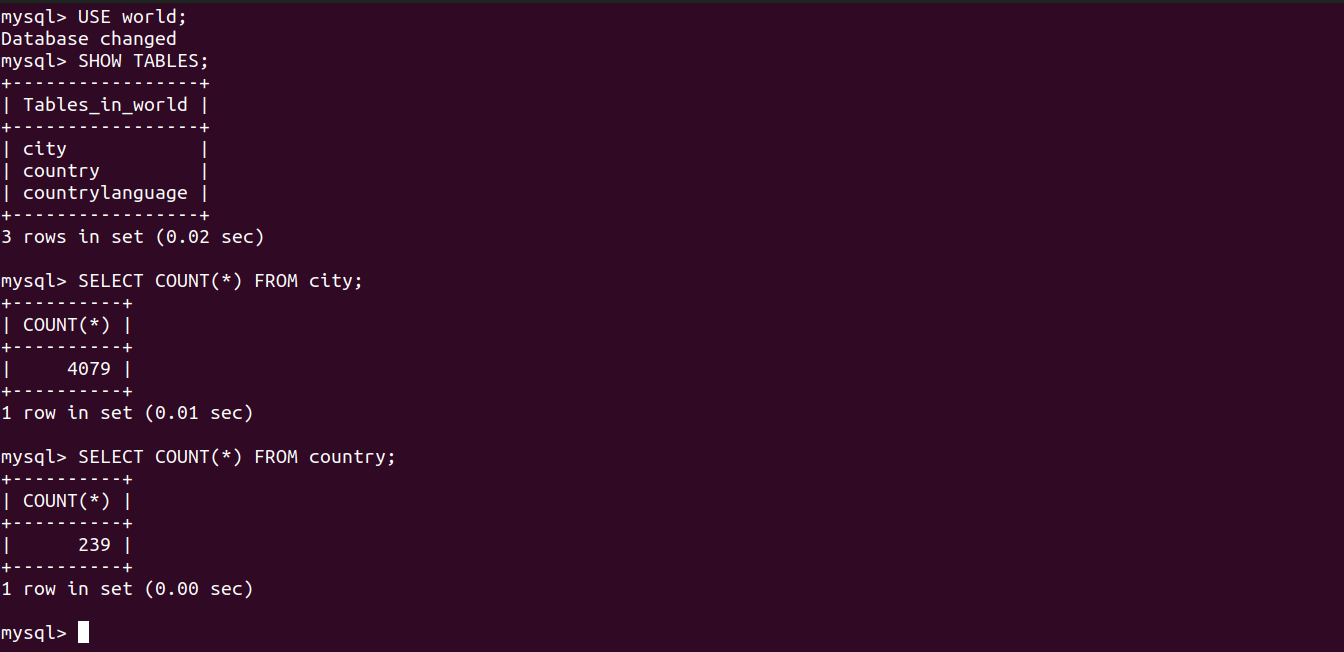
1. Download the world database and extract it.



1. Give the ‘world’ database path to MySQL.



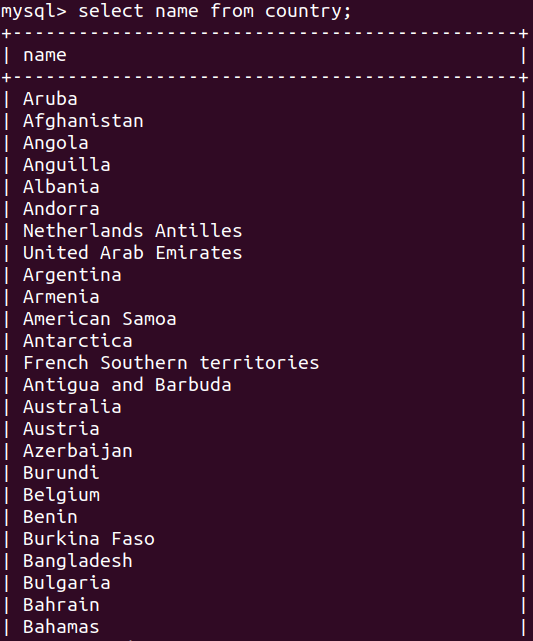
1. Verify the database is created and populated.

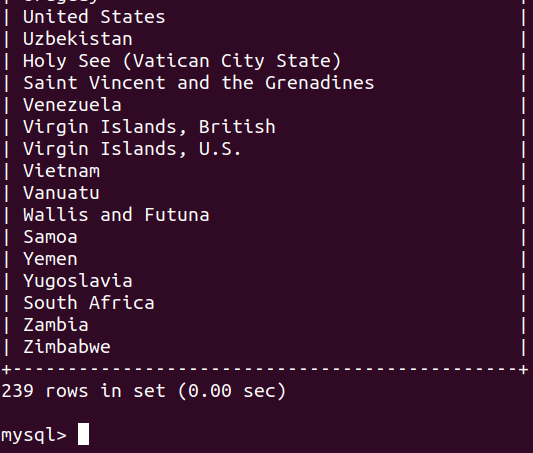


**Task 3: Querying the Database:**

Write SQL queries to retrieve following information from ‘world’ database:

* List of All Countries

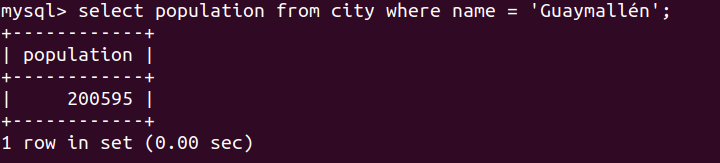




* List of cities in a specific country

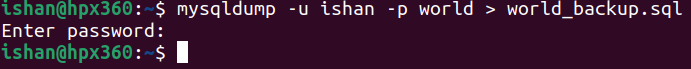


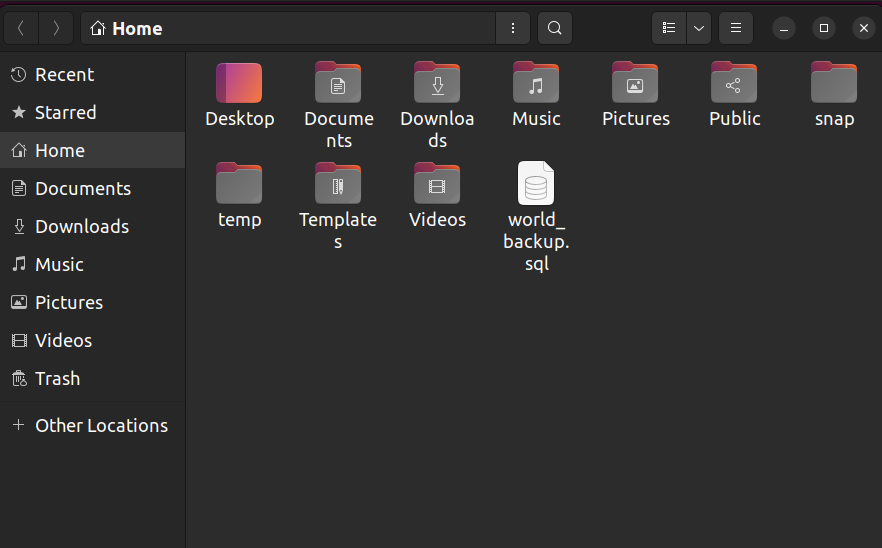
* Population of a specific country



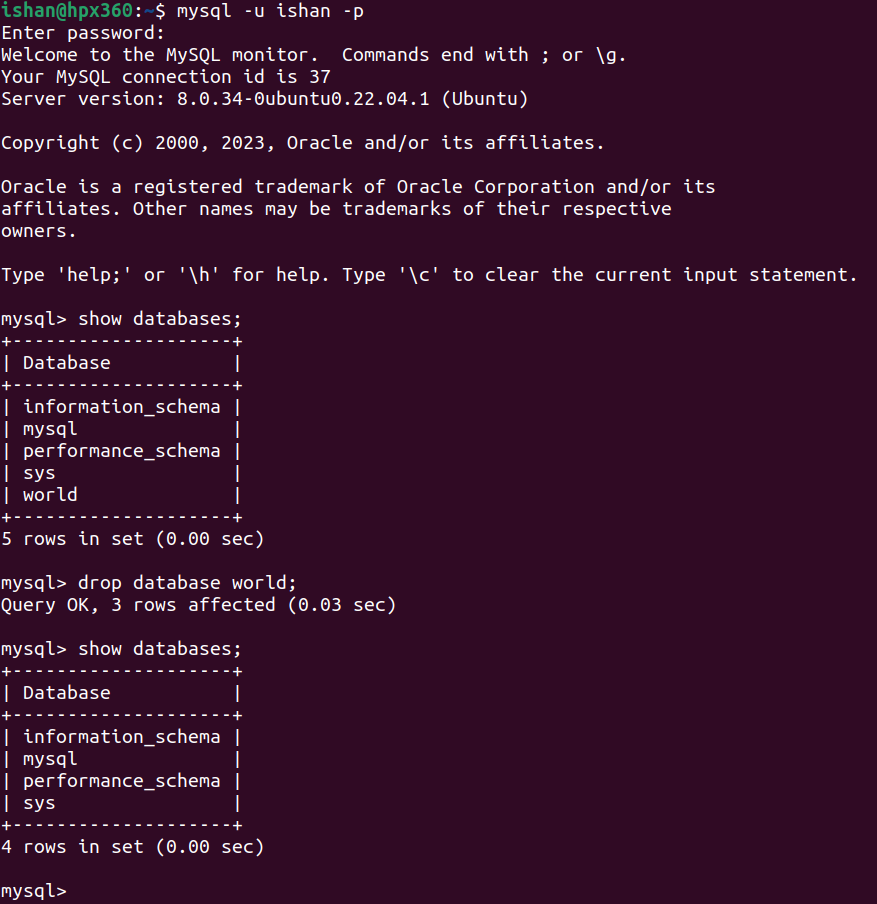
**Task 4: Backup and Restore:**

1. Create Backup for the world database for safety purpose in case of loss of data.





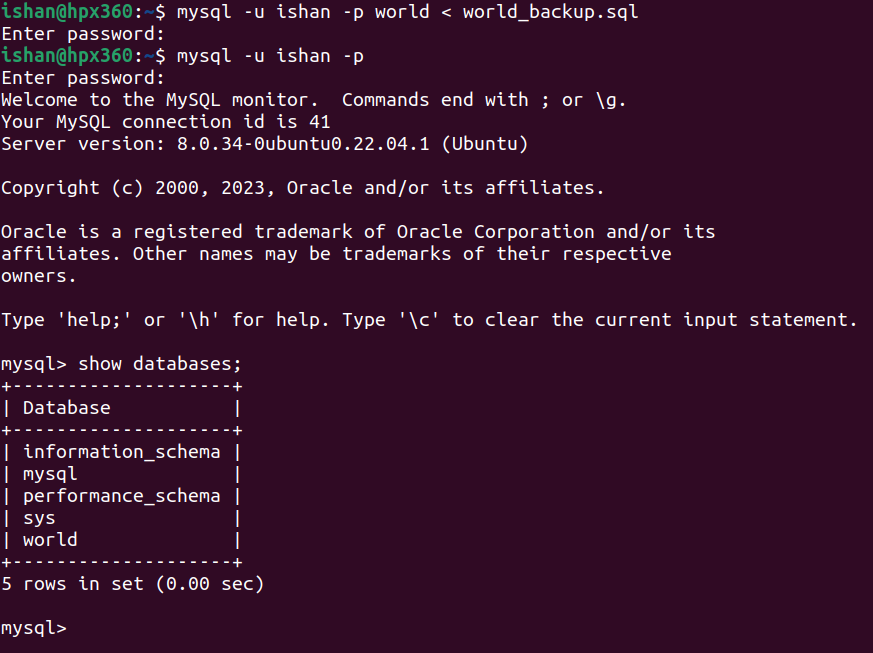
1. Check databases and to simulate the loss of data we will delete the world database.



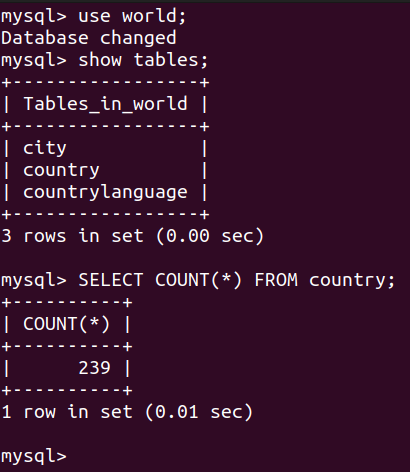
1. Now the ‘world’ database is removed from list of databases. To bring back data of the ‘world’ we will use the backup file ‘world\_backup’ created before.
2. Create new database of the name ‘world’ so that we can get backup into this file.



1. Now, in ‘world’ input our previous backup file ‘world\_backup.sql’ to regain all data through backup.
2. Now check databases, ‘world’ has all the data restored similar to before through backup.



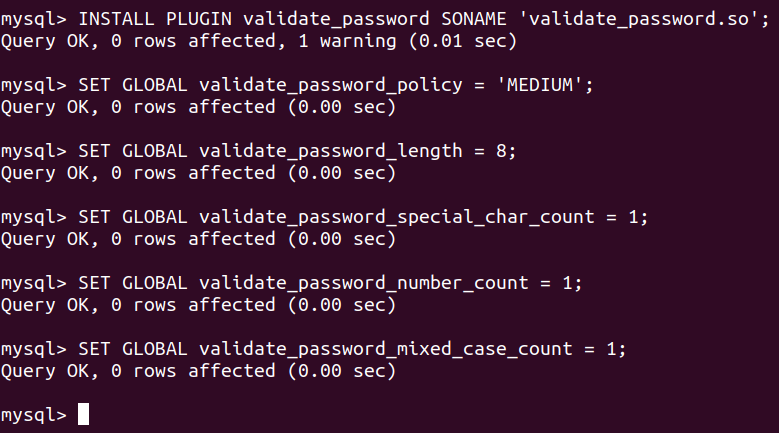
1. Now to verify the data in the ‘world’ database, select ‘world’ database and verify if it contains required data.



1. The ‘world’ database has restored all previous data with the help of backup.
2. Also run some queries to ensure data is not corrupt.

**Task 5: Security and Access Control:**

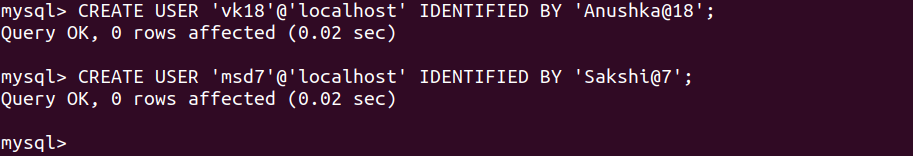
1. Implementing password policies on users.
2. For this, we installed Plugin ‘validate\_password’ to set some rules for Password policy.



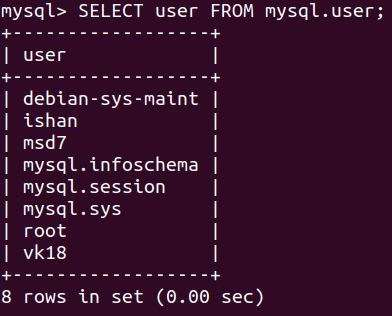
1. validate\_password\_length: is for the minimum length of the password.
2. validate\_password\_special\_char\_count is minimum special character count.
3. validate\_password\_number\_count is minimum number in the password.
4. validate\_password\_mixed\_case\_count is minimum count of lowercase & highercase characters.
5. Now if we create user without satisfying the current policy requirements, then user will not be created unless password policy is satisfied.



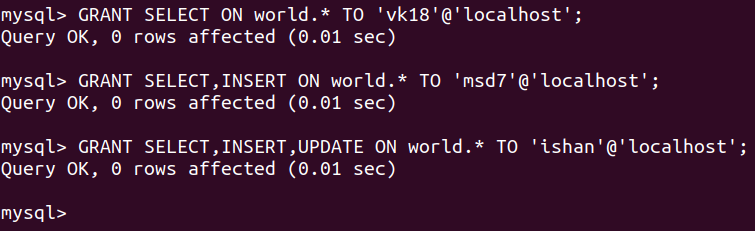
1. When we follow Password policy requirements and create user then User is created and added to the database.



1. Here, we can see created users in the database.



1. Now, grant permissions to the users.



1. Flush Privileges is the command which applies all grants given to users.



By implementing these security measures, database administrators and organizations can significantly reduce the risk of data breaches and ensure the confidentiality, integrity, and availability of their data. It's essential to adopt a layered security approach and regularly review and update security measures to stay ahead of evolving threats