Лабораторна робота 7

План роботи

1. Слід створиту копію своєї БД.

2. Для кожного з варіантів Вашу БД можливо подати як сукупність трьох таблиць А –АВ—В. Слід створити кілька типів користувачів БД:

*«гість»* може тільки читати дані;

*«операторА»* може читати, писати, модифікувати та знищувати дані у таблиці А;

*«операторВ»* може читати, писати, модифікувати та знищувати дані у таблиці В;

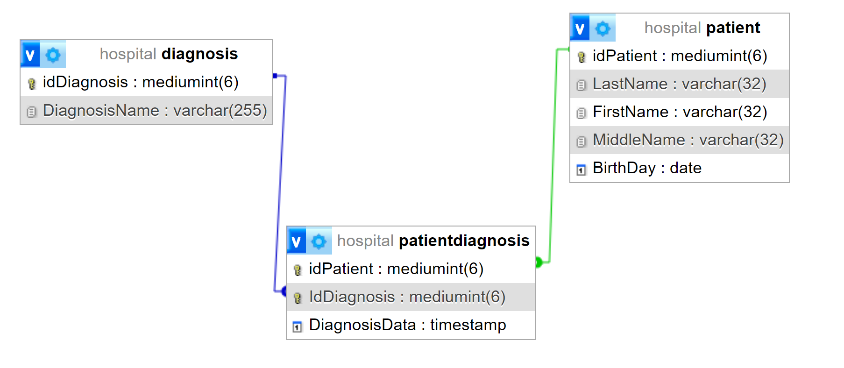
*«операторАВ»* може читати, писати, модифікувати та знищувати дані у таблиці АВ, а також тільки читати дані з таблиць А та В;

*Коже з користувачів повинен мати своє ім’я та пароль, що Користувач має змінити відразу після входження у систему.*

Це створить перший рівень захисту від несанкціонованого доступу до БД.

1. На другому рівні захисту даних слід додати Шифрування-Дешифрування. Дані слід зберігати у таблицях зашифрованими. Кожна з таблиць повінна мати свій пароль. Для доступу до даних слід створити відповідні збережені процедури/функції, якій й мають забезпечувати інтерфейс користувача.
2. Визначити склад системних процедур та функцій для шифрування даних.
3. Створити збережені процедури, що будуть шифрувати дані перед занесенням їх у таблиці нової БД.
4. Створити збережені функції, що будуть відображати дешифровані дані.
5. Перевірити коректність шифрування-дешифрування
6. Оформити звіт.

Фізична модель БД



1. Слід створиту копію своєї БД.

Створення структури таблиці:

|  |  |
| --- | --- |
| CREATE TABLE назва\_нової таблиці [AS] SELECT \* FROM назва\_таблиці\_існуючої\_БД; | CREATE TABLE copy\_table LIKE source\_table; |
| CREATE TABLE Patient2 AS SELECT \* FROM Patient; | CREATE TABLE Patient3 LIKE Patient; |
| Маємо нову таблицю Patient2 |  |
|  |  |

Для копіювання даних з однієї таблиці до іншої слід використати:

INSERT INTO copy\_table (`column1`, `column2`) SELECT `column1`, `column2` FROM source\_table;

Для копіювання усіх даних слід виконати такий оператор:

INSERT INTO copy\_table SELECT \* FROM source\_table;

INSERT INTO Patient2 SELECT \* FROM Patient;

Якщо таблиця дуже велика і ви не можете її заблокувати для доступу інших користувачів, то слід:

CREATE TABLE table2 LIKE table1; // робимо копію структури таблиці

SELECT \* INTO OUTFILE '/tmp/table1.txt' FROM table1; // робимо копію даних таблиці в окремий файл

LOAD DATA INFILE '/tmp/table1.txt' INTO TABLE table2; // заносимо дані у нову таблицю з файлу

Як створити нову таблицю у новій БД і занести туди дані?

Спочатку слід створити нову БД: create database НАЗВА\_НОВОЇ\_БАЗИ\_ДАНИХ;

Наприклад, CREATE DATABASE HOSPITAL2;

Якщо треба, то слід обрати нову БД так: USE HOSPITAL2;

Переміщення таблиці з однієї БД до іншої БД виконуємо так: RENAME TABLE hospital2.patient TO hospital.patient;

Для створення нової таблиці у новій БД і занесення даних зі «старої» таблиці слід зробити так:

CREATE TABLE hospital2.patient LIKE hospital.patient; // створюємо структурну копію таблиці

INSERT INTO hospital2.patient SELECT \* from hospital.patient; // а тепер дані з однієї таблиці копіюються у нову таблицю нової БД

2. Для кожного з варіантів Вашу БД можливо подати як сукупність трьох таблиць А –АВ—В. Слід створити кілька типів користувачів БД:

*«гість»* може тільки читати дані;

*«операторА»* може читати, писати, модифікувати та знищувати дані у таблиці А;

*«операторВ»* може читати, писати, модифікувати та знищувати дані у таблиці В;

*«операторАВ»* може читати, писати, модифікувати та знищувати дані у таблиці АВ, а також тільки читати дані з таблиць А та В;

*Кожен з користувачів повинен мати своє ім’я та пароль, що Користувач має змінити відразу після входження у систему.*

Це створить перший рівень захисту від несанкціонованого доступу до БД.

*Глянемо уважно на завдання: треба створити кілька типів користувачів БД, тобто кілька ролей ( у термінах реляційних БД):*

*Тобто у нас кілька користувачів відповідають одній ролі*

*Користувачі мають своє ім’я та пароль*

*Як базу даних будемо використовувати Госпіталь*

*Матимемо ролі:*

*Guest - може читати усі три таблиці БД: patient, diagnosis, patientdiagnosis*

*OperatorP - читає, пише, модифікує, знищує дані з таблиці: patient.*

*OperatorD - читає, пише, модифікує, знищує дані з таблиці: diagnosis.*

*OperatorDP - читає, пише, модифікує, знищує дані з таблиці: patientdiagnosis*

*Читає дані з таблиць: patient, diagnosis.*

*MySQL пропонує кілька десятків привілей, але нам знадобляться лише:*

*SELECT, INSERT, UPDATE, DELETE*

*Створимо чотири ролі так:*

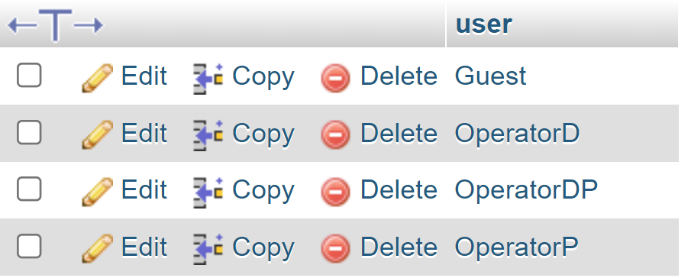
*CREATE ROLE Guest, OperatorP, OperatorD, OperatorDP;*

*CREATE ROLE 'Guest'@'localhost';*

( щоб вилучити ролі слід набрати DROP ROLE *Guest, OperatorP, OperatorD, OperatorDP;)*

*'localhost' – означає, що ця роль виконується на локальній машині*

*Для перевірки наберемо:* SELECT user FROM mysql.user

**

*А тепер надамо цим ролям привілеї ( права )*

GRANT SELECT ON hospital.\* TO ‘*Guest'*; // гість може читати з усіх таблиць БД

*Надамо права ролі OperatorP*,*що читає, пише, модифікує, знищує дані з таблиці: patient.*

GRANT SELECT,INSERT, UPDATE, DELETE ON hospital.patient TO *'OperatorP';*

*Надамо права ролі 'OperatorD'*,*що читає, пише, модифікує, знищує дані з таблиці: diagnosis.*

GRANT SELECT,INSERT, UPDATE, DELETE ON hospital. *diagnosis* TO *'OperatorD';*

*Надамо права ролі 'OperatorDP'*,

*Що читає, пише, модифікує, знищує дані з таблиці: patientdiagnosis*

*Читає дані з таблиць: patient, diagnosis.*

*Для цього слід використати два таких оператори:*

GRANT INSERT, UPDATE, DELETE ON hospital. *patientdiagnosis* TO *'OperatorDP'*;

GRANT SELECT ON hospital.\* TO *'OperatorDP'*;

*Тепер слід зробити кілька користувачів, що належать різним ролям:*

*SimpleUser - Guest*

*UserP - OperatorP*

*UserD - OperatorD*

*UserDP - OperatorDP*

*Спочатку створимо користувачів з паролем, який треба змінити*

CREATE USER 'QWERTY'@'localhost' PASSWORD EXPIRE DEFAULT;

Користувач під’єднується до системи без паролю

*Розберемо детально створення користувача*

CREATE USER ' **QWERTY** '@'localhost' PASSWORD EXPIRE DEFAULT;

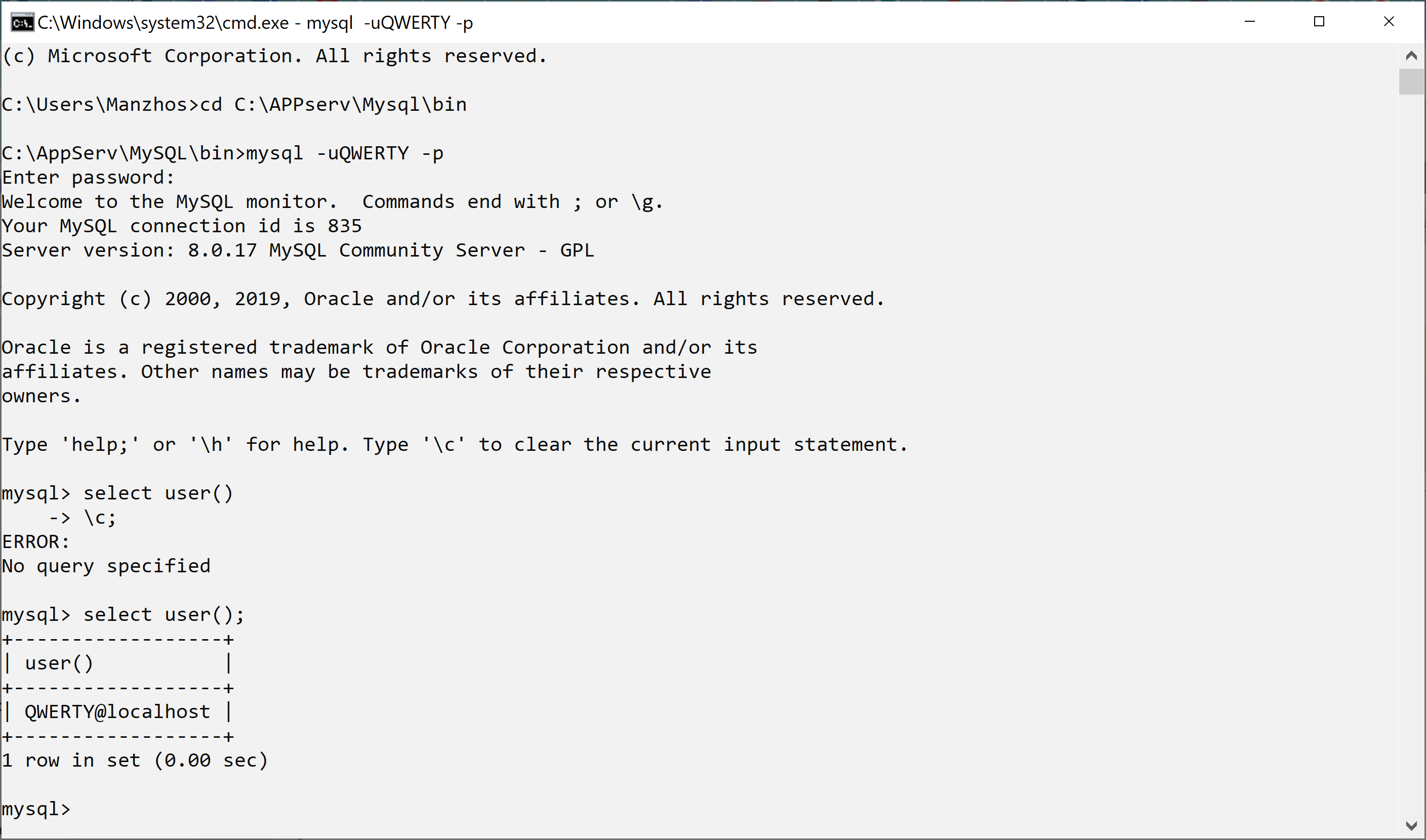
*Створюємо користувача , логін якого* **QWERTY** *.Користувач може під’єднуватися тільки з локальної машини. Пароль користувача пустий, тобто треба просто натиснути кнопку. Пароль користувача слід змінити негайно після входу*

*Якщо треба дозволити користувачу працювати з певної ІР адреси, то слід*

CREATE USER ' **QWERTY** '@'192.168.0.1' PASSWORD EXPIRE DEFAULT;

*Якщо треба дозволити користувачу працювати з будь-якого місця, то слід*

CREATE USER ' **QWERTY** '@'%' PASSWORD EXPIRE DEFAULT;

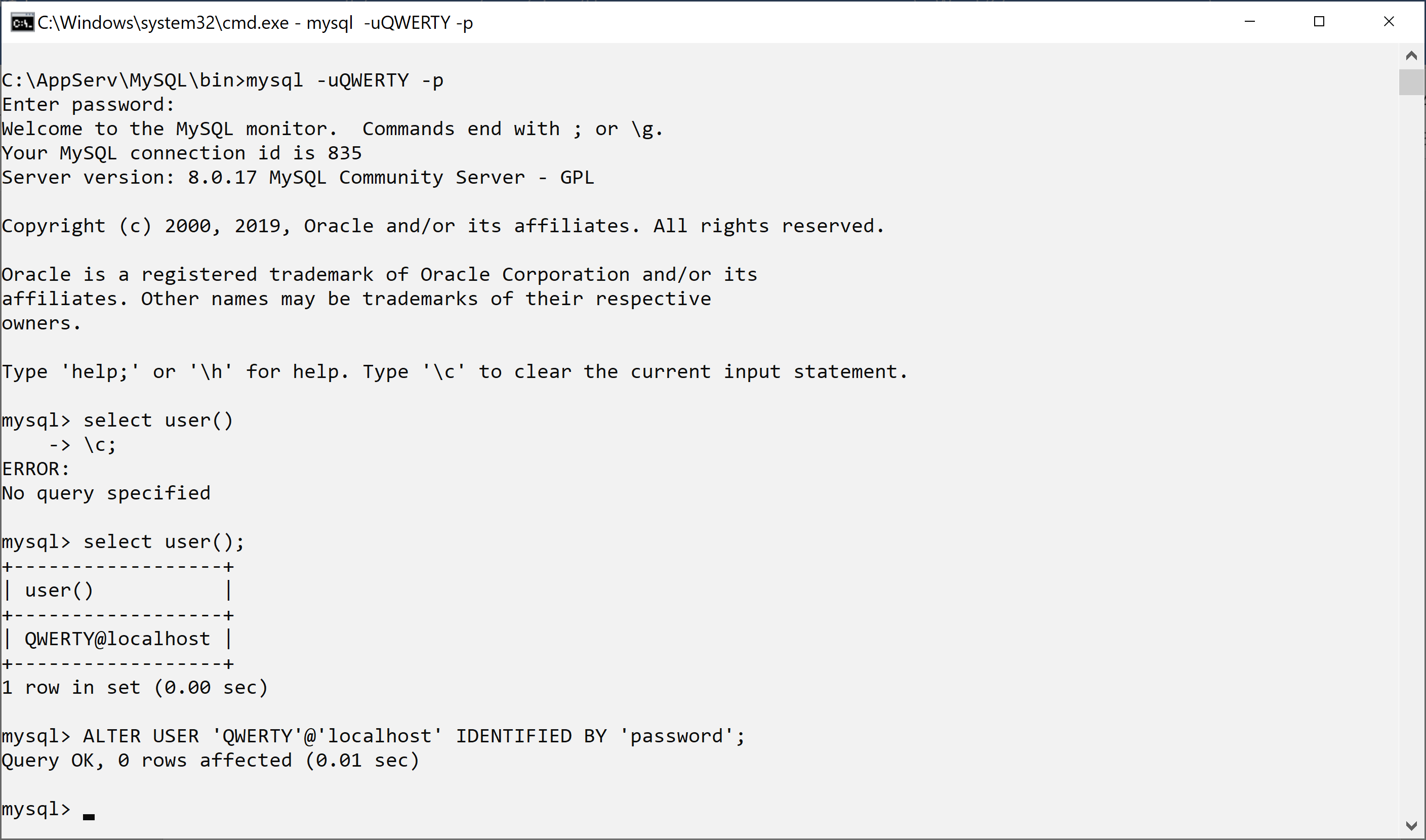


*Користувач має негайно визначити свій пароль так:*

*ALTER USER 'username'@'localhost' IDENTIFIED BY 'new\_password';*

*Наприклад,*

*ALTER USER 'QWERTY'@'localhost' IDENTIFIED BY 'password';*



*Створимо кілька користувачів:*

CREATE USER '*SimpleUser*'@'localhost' PASSWORD EXPIRE DEFAULT;

CREATE USER 'UserP'@'localhost' PASSWORD EXPIRE DEFAULT;

CREATE USER 'UserD'@'localhost' PASSWORD EXPIRE DEFAULT;

CREATE USER 'UserDP'@'localhost' PASSWORD EXPIRE DEFAULT;

*(видаляють користувача так:*  **DROP** USER 'account\_name'; *)*

|  |  |
| --- | --- |
| *Для перевірки наберемо:* SELECT user FROM mysql.user |  |

*Бачимо, що нових користувачів було створено*

*Тепер нам слід надати певні ролі користувачам:*

*Спочатку виконаємо такий оператор (необов'язково, але бажано):*

FLUSH **PRIVILEGES**; - він змушує систему прийняти усі зміни прав, користувачів тощо

*Тепер визначаємо ролі користувачів, наприклад:*

GRANT '<role>'@'<host>' TO '<user>'@'<host>';

*Grant 'Guest'@'localhost' TO 'SimpleUser'@'localhost';*

*Тепер активізуємо роль так:*

*Set default role 'Guest'*@*'localhost' to* '*SimpleUser*'@*'localhost';*

*Перевіримо права:* SHOW GRANTS **for** **Guest@localhost**

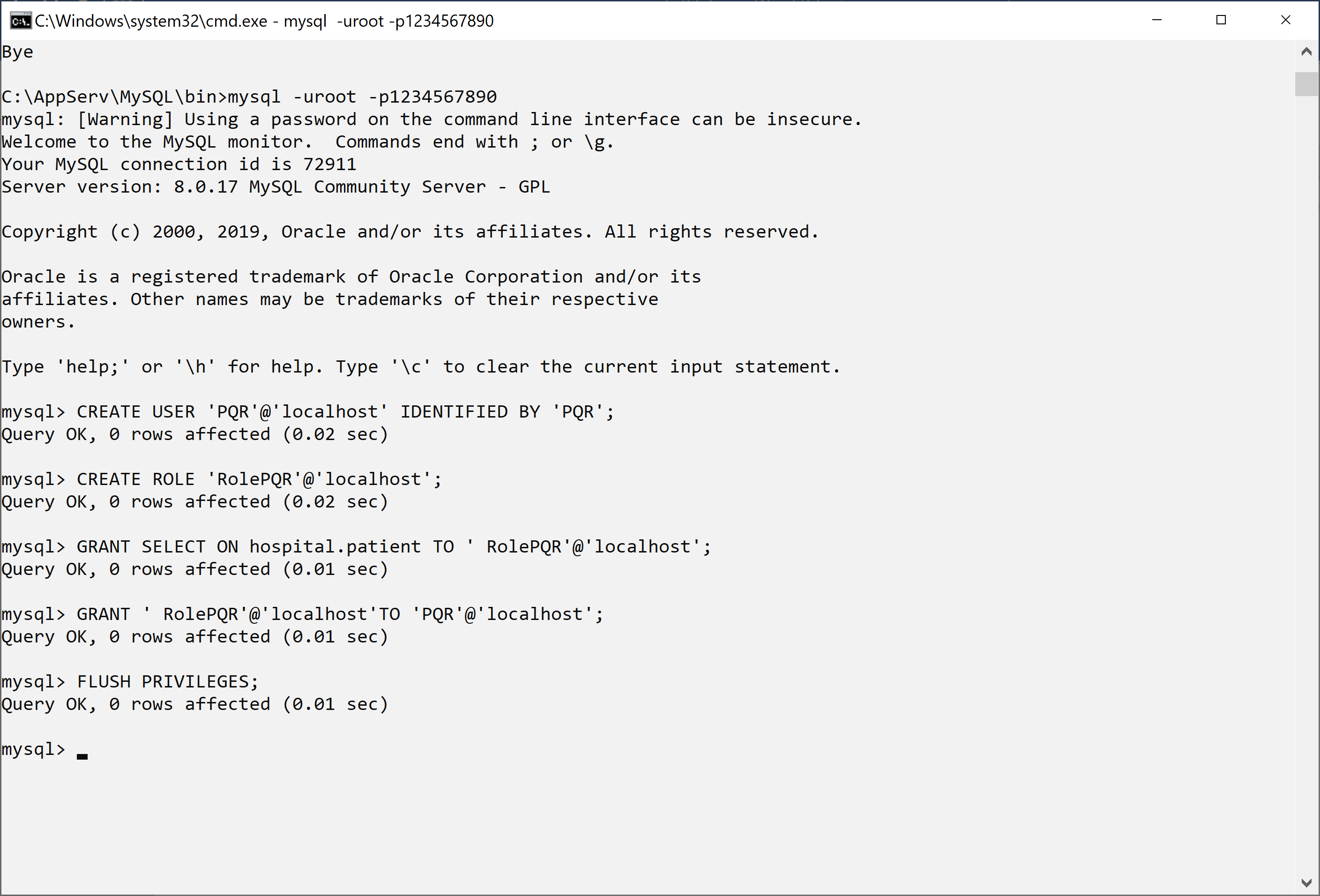
| **Grants for Guest@localhost** |  |
| --- | --- |
| GRANT USAGE ON \*.\* TO `Guest`@`localhos |  |

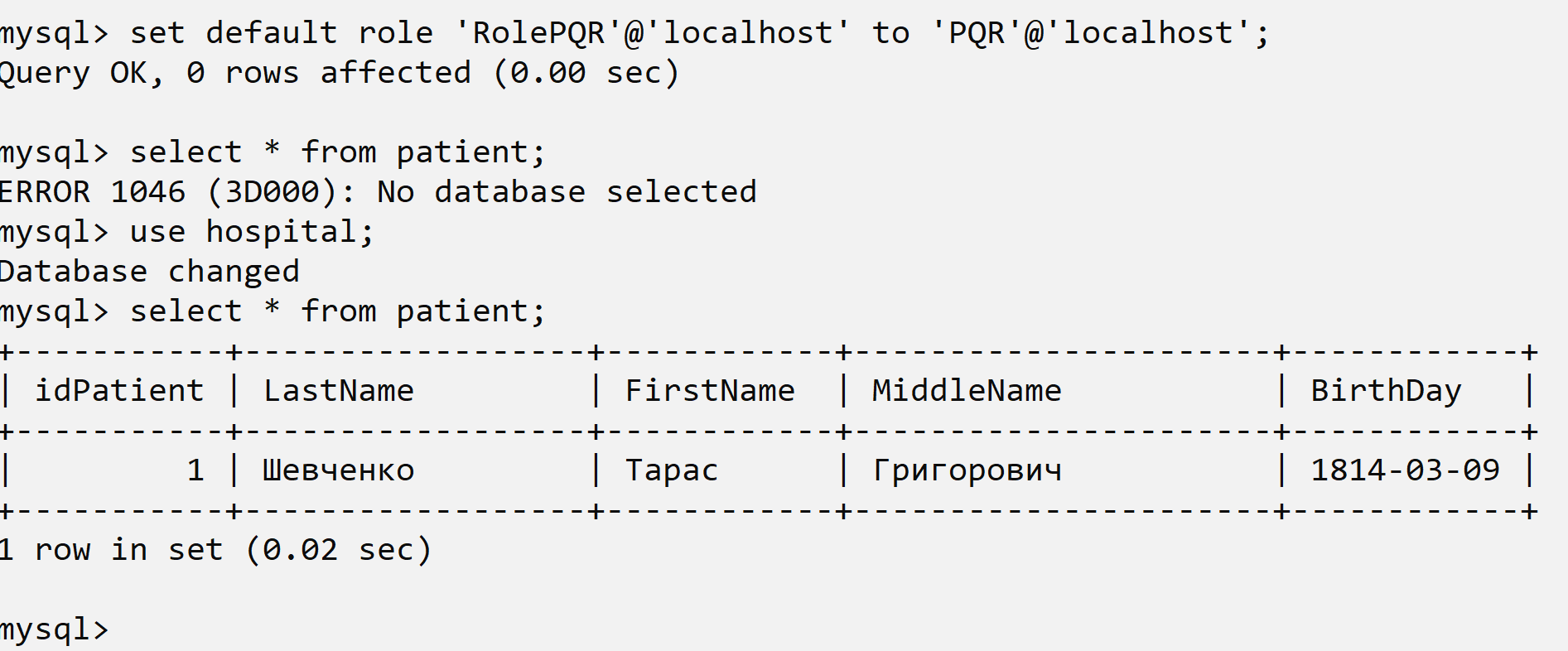
*Додамо привілеї до ролі* **Guest@localhost**

GRANT SELECT ON hospital.\* TO 'Guest' @'localhost';

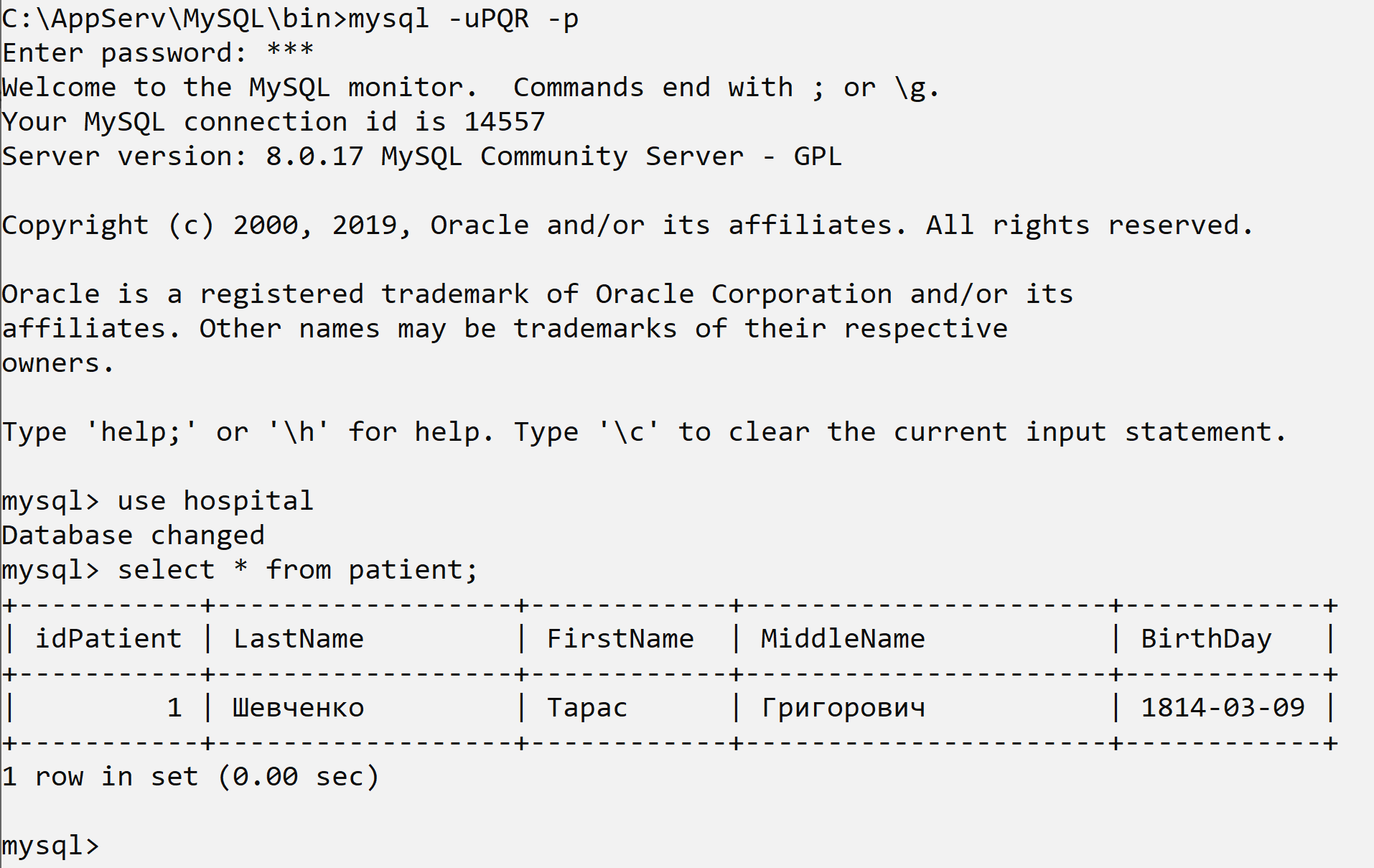
*Перевіримо права:* *SHOW GRANTS for 'Guest'@'localhost'*

| **Grants for Guest@localhost** |  |
| --- | --- |
| GRANT USAGE ON \*.\* TO `Guest`@`localhost` |  |
| GRANT SELECT ON `hospital`.\* TO `Guest`@`localhost... |  |





*Для виходу потрібна команда exit*



CREATE USER 'joe'@'10.0.0.1' DEFAULT ROLE administrator, developer;