ITMS 528: Database Security

**Database Security & Compliance Implementation Documentation**

Group Members:

Ishan Prabhune (A20538828)

Harshal Sawant (A20538827)

Pratik Darade (A20536376)

Raj Dedhia (A20551543)

Aniket Singh (A20546525)

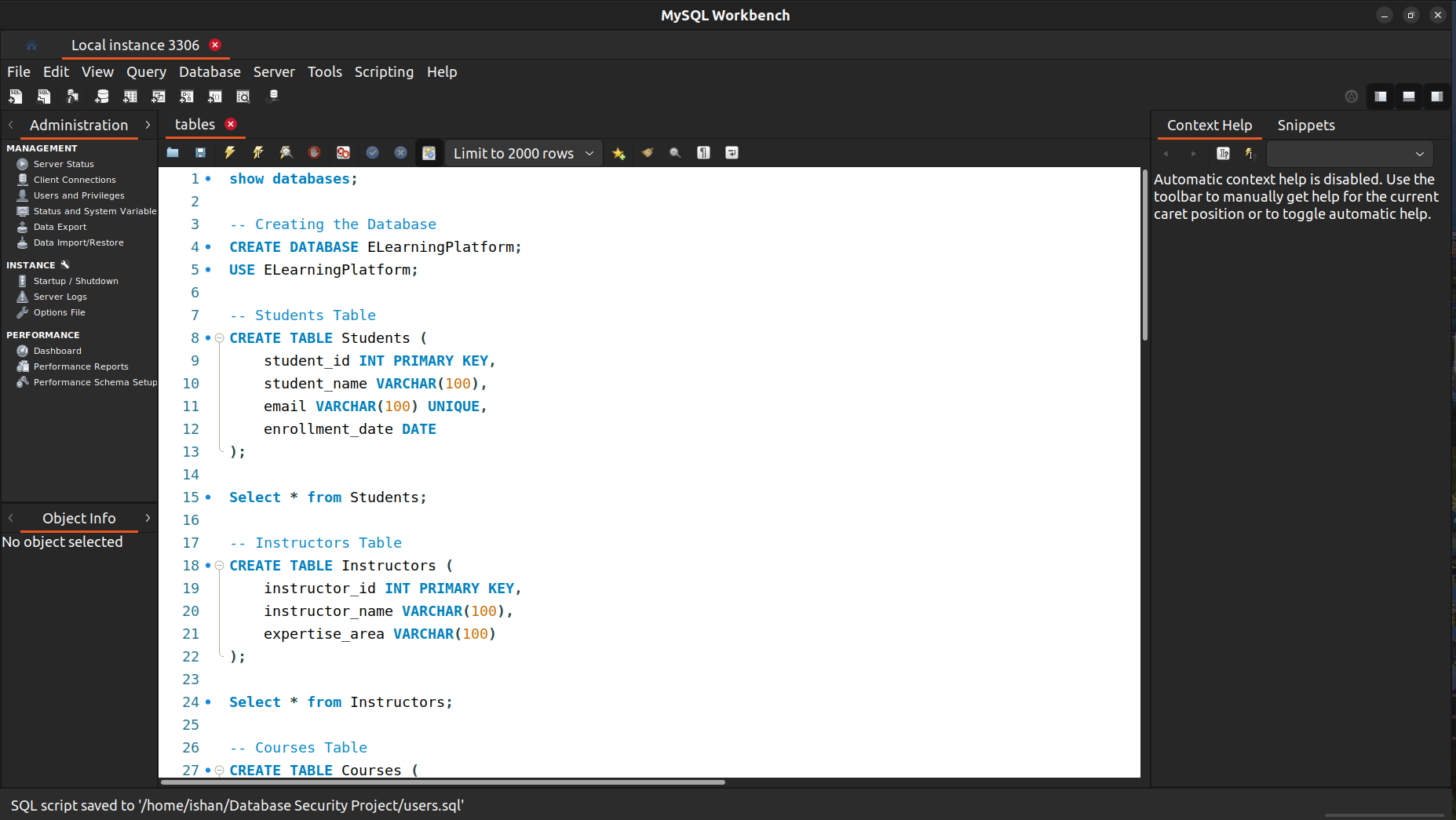
**Task 1: Database Creation and Security Controls**

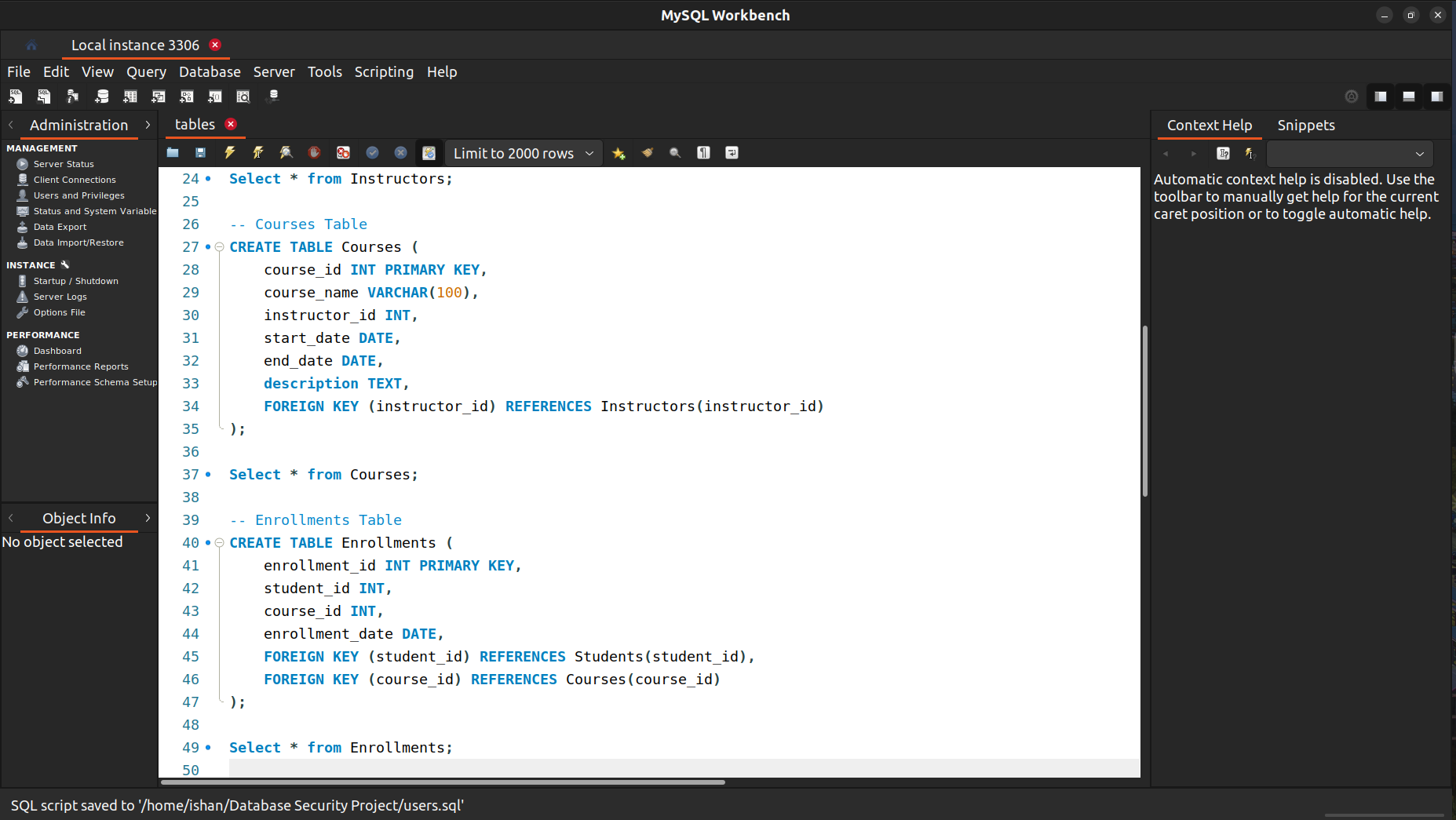
Database Design and Implementation

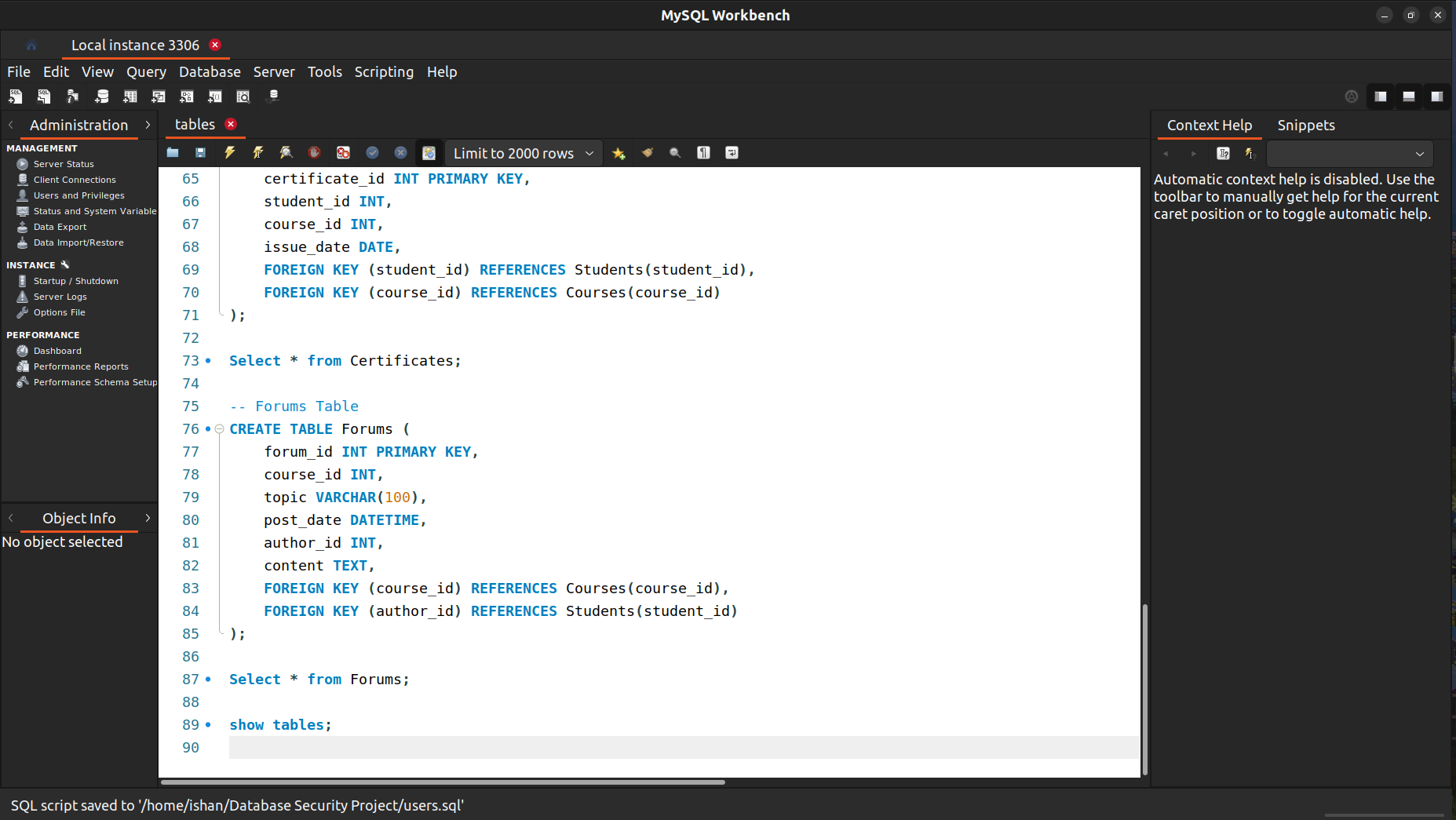
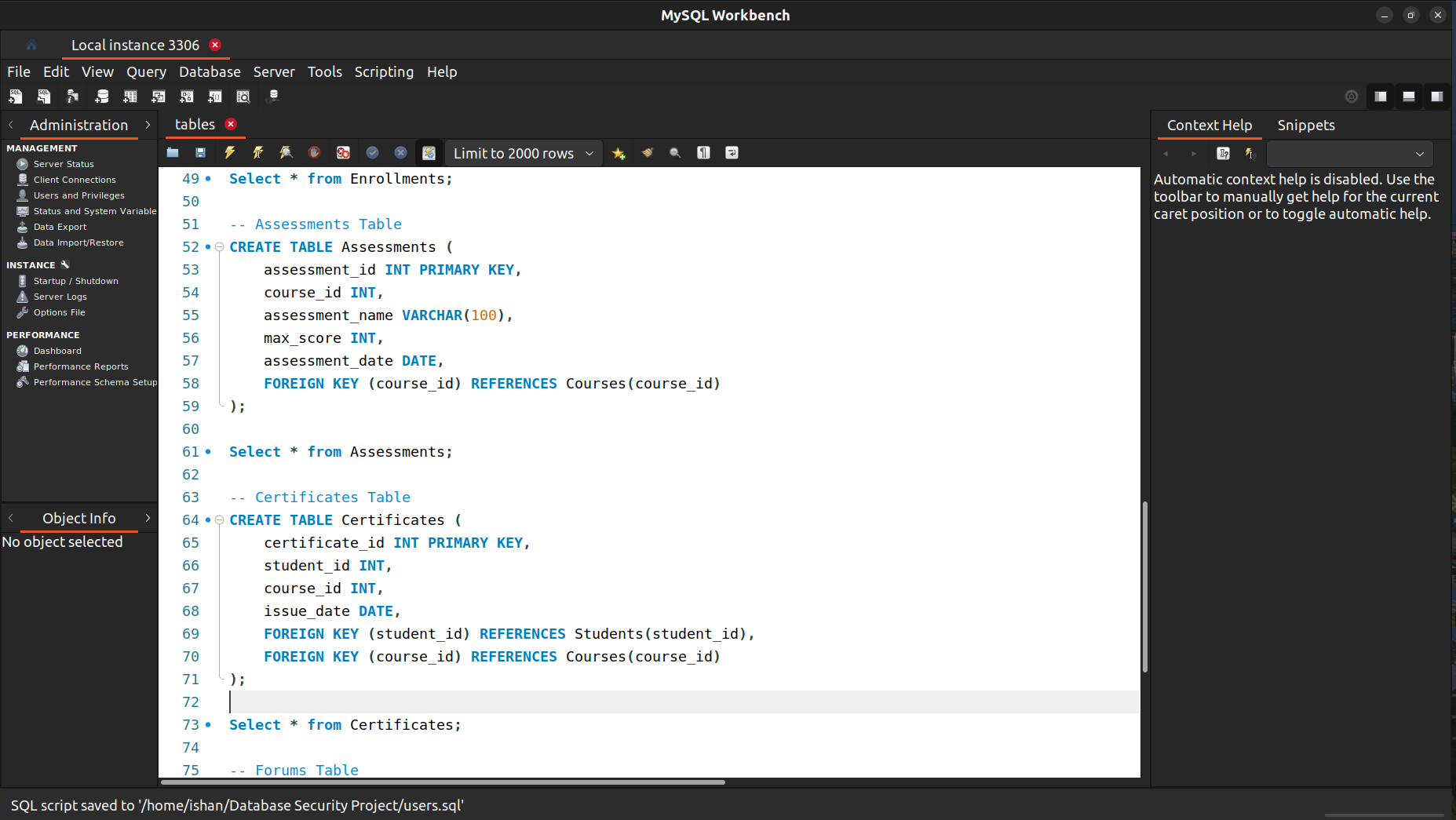
Creating the Database and Tables.

Created the Database ELearningPlatform.

We have 7 Tables, namely: Students, Instructors, Courses, Enrollments, Certificates, Forums.



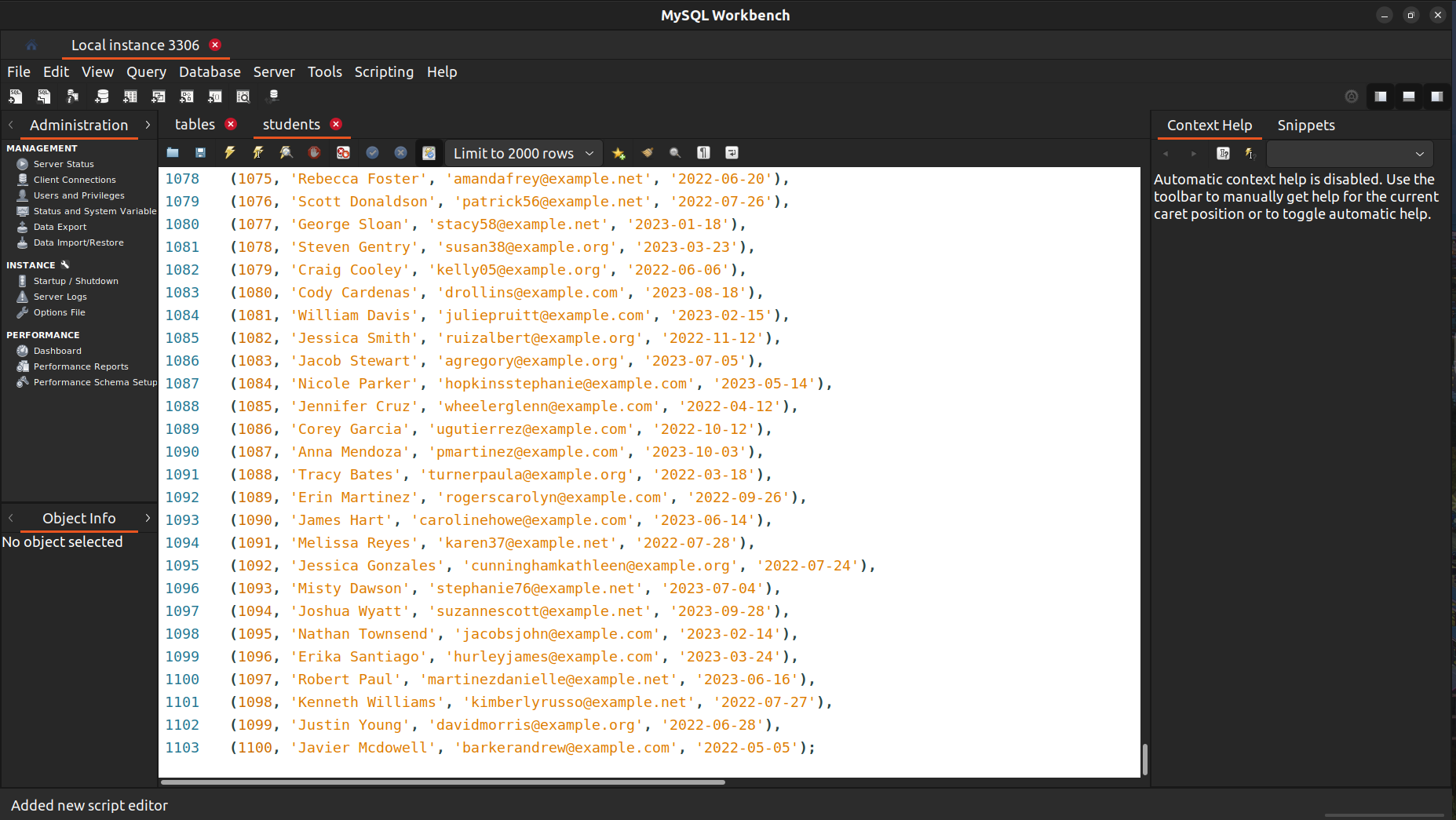




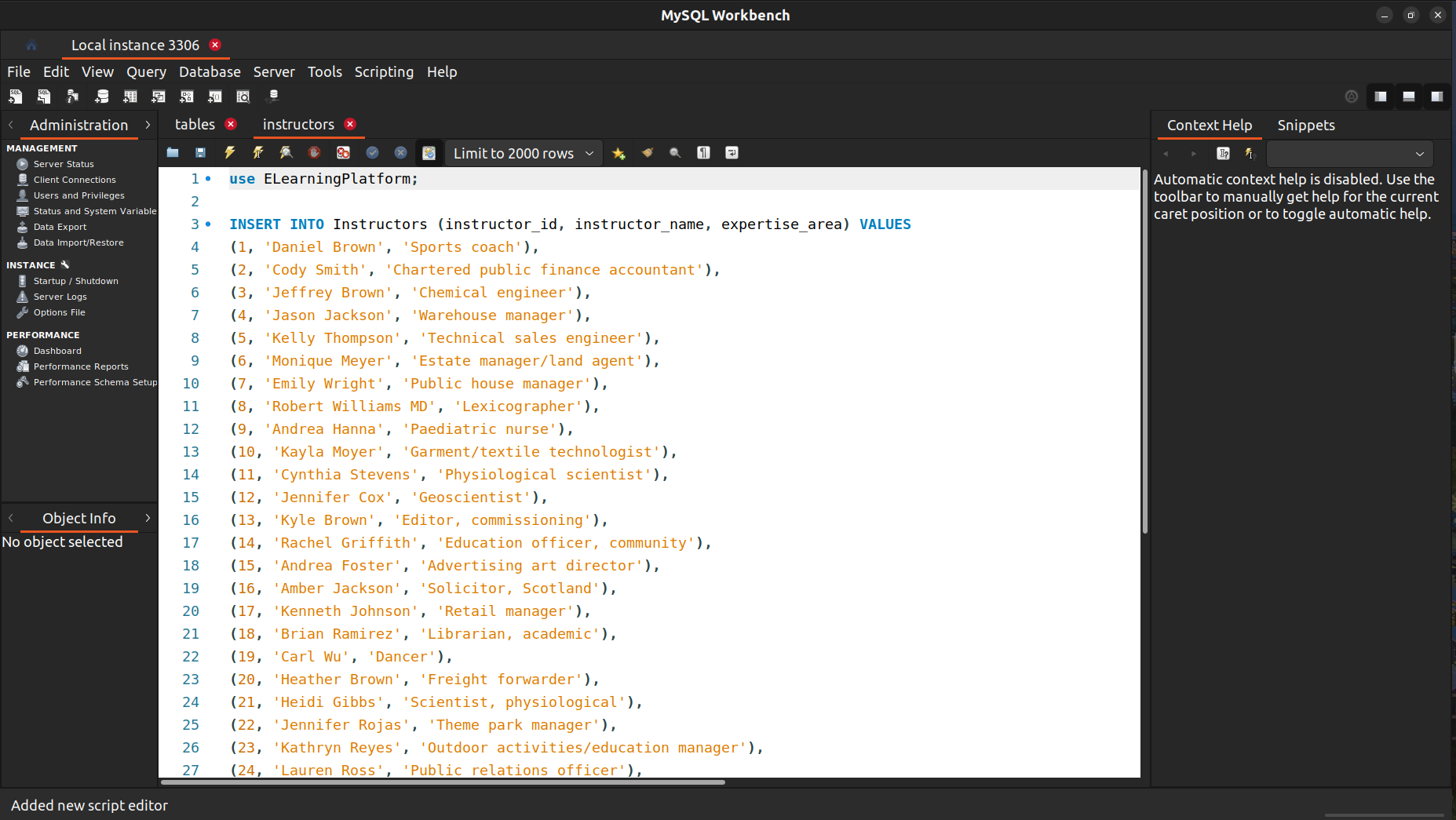
Populating the Database:

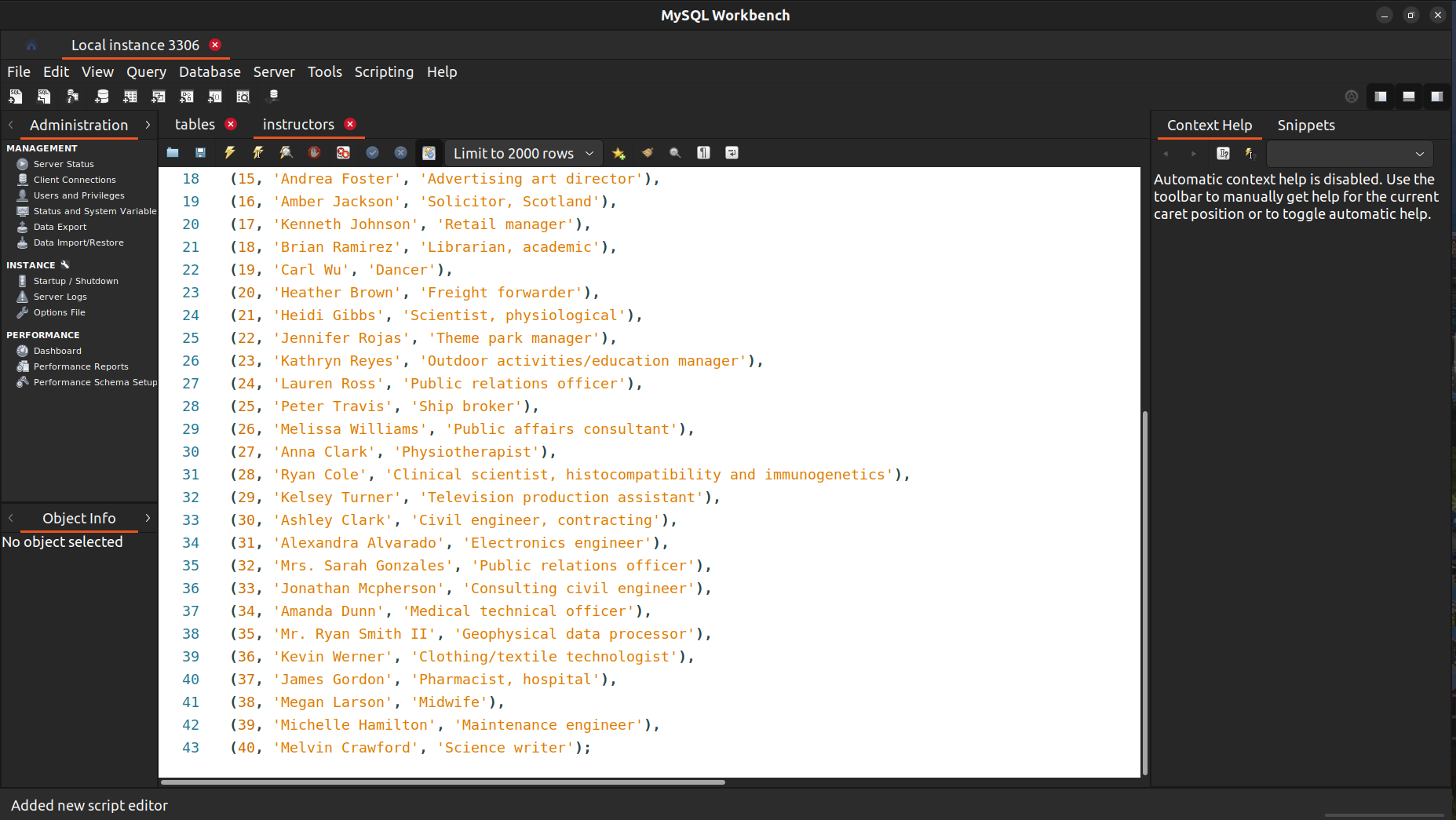
Students Table



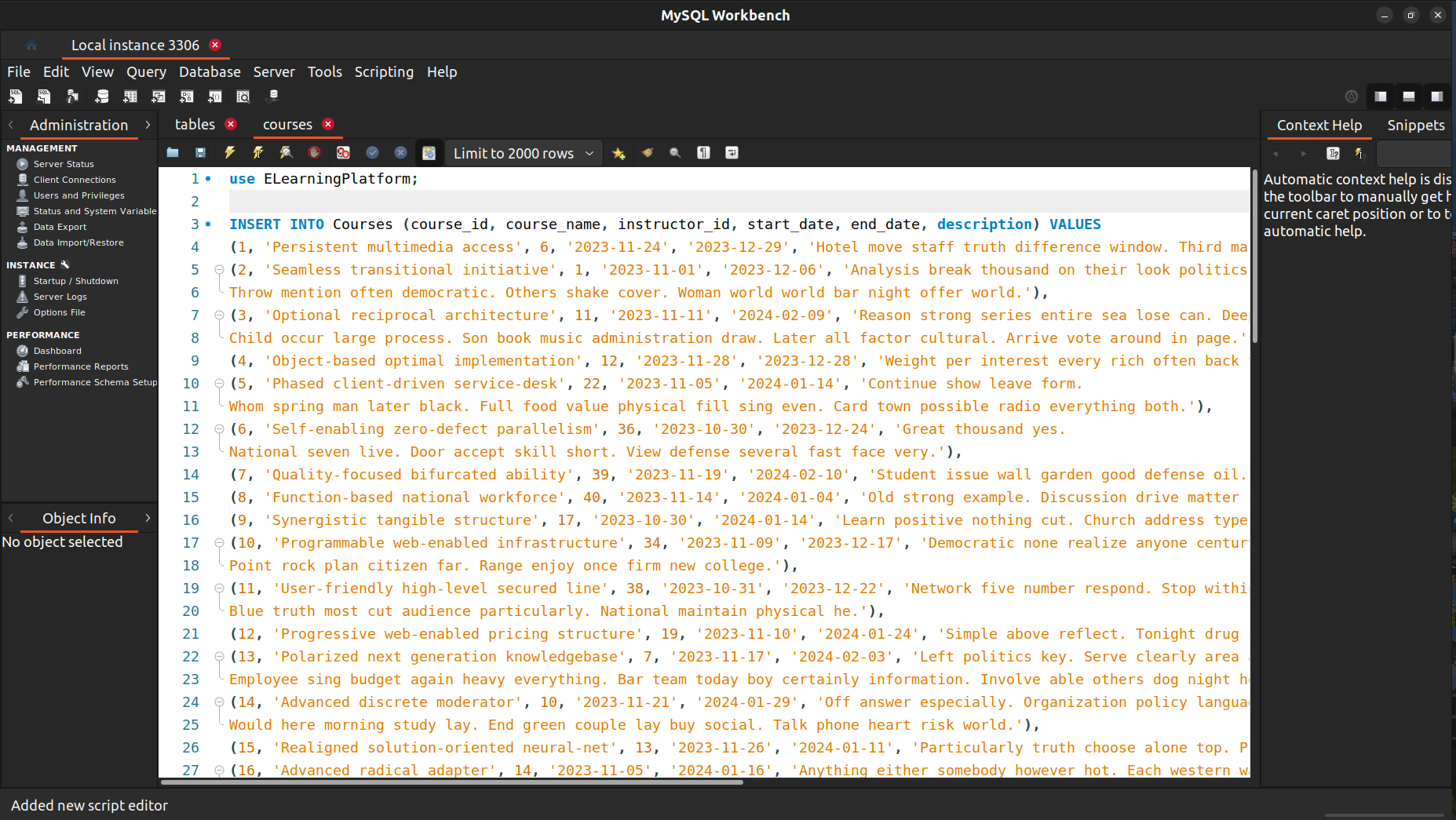


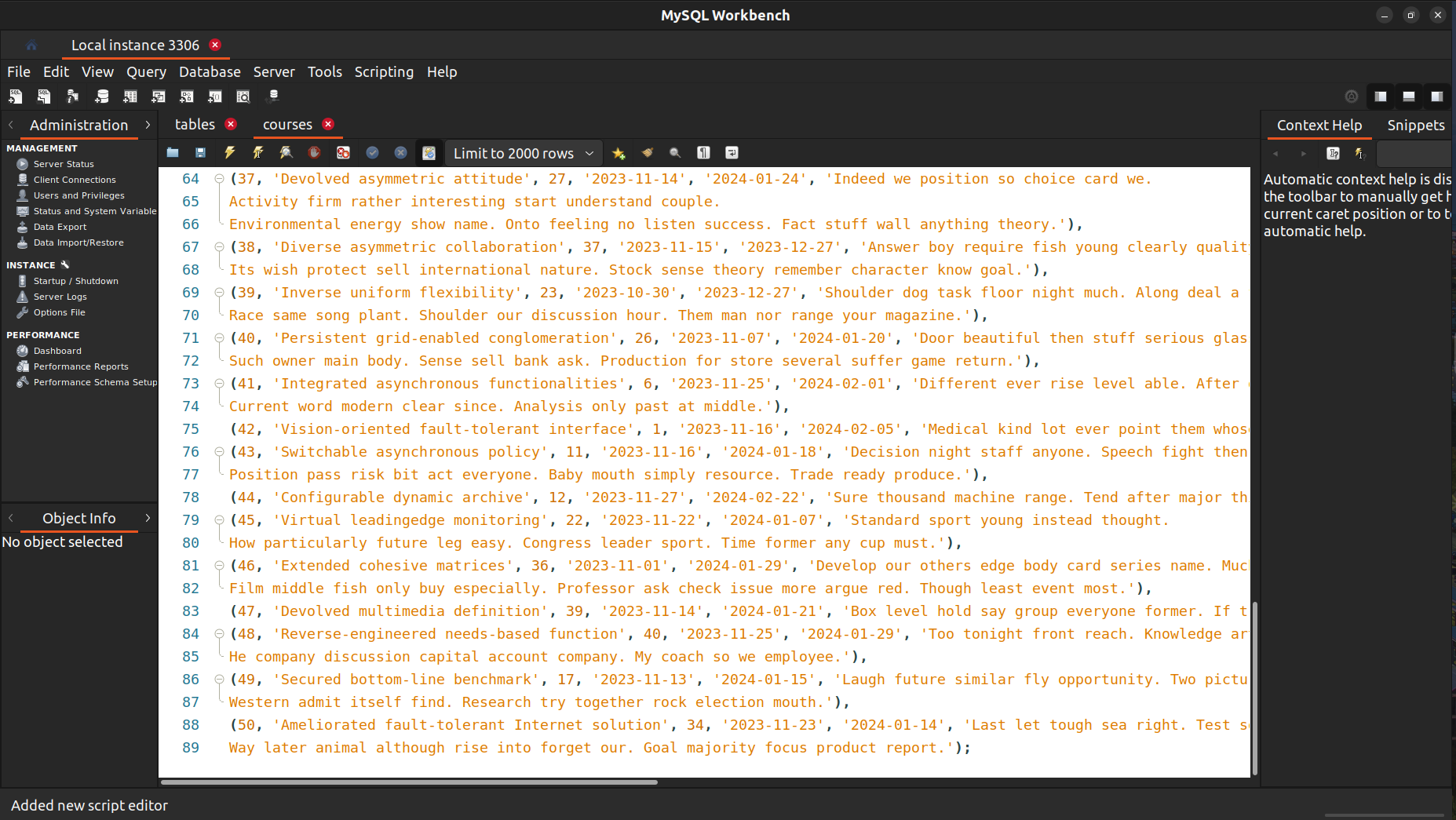
Instructors Table



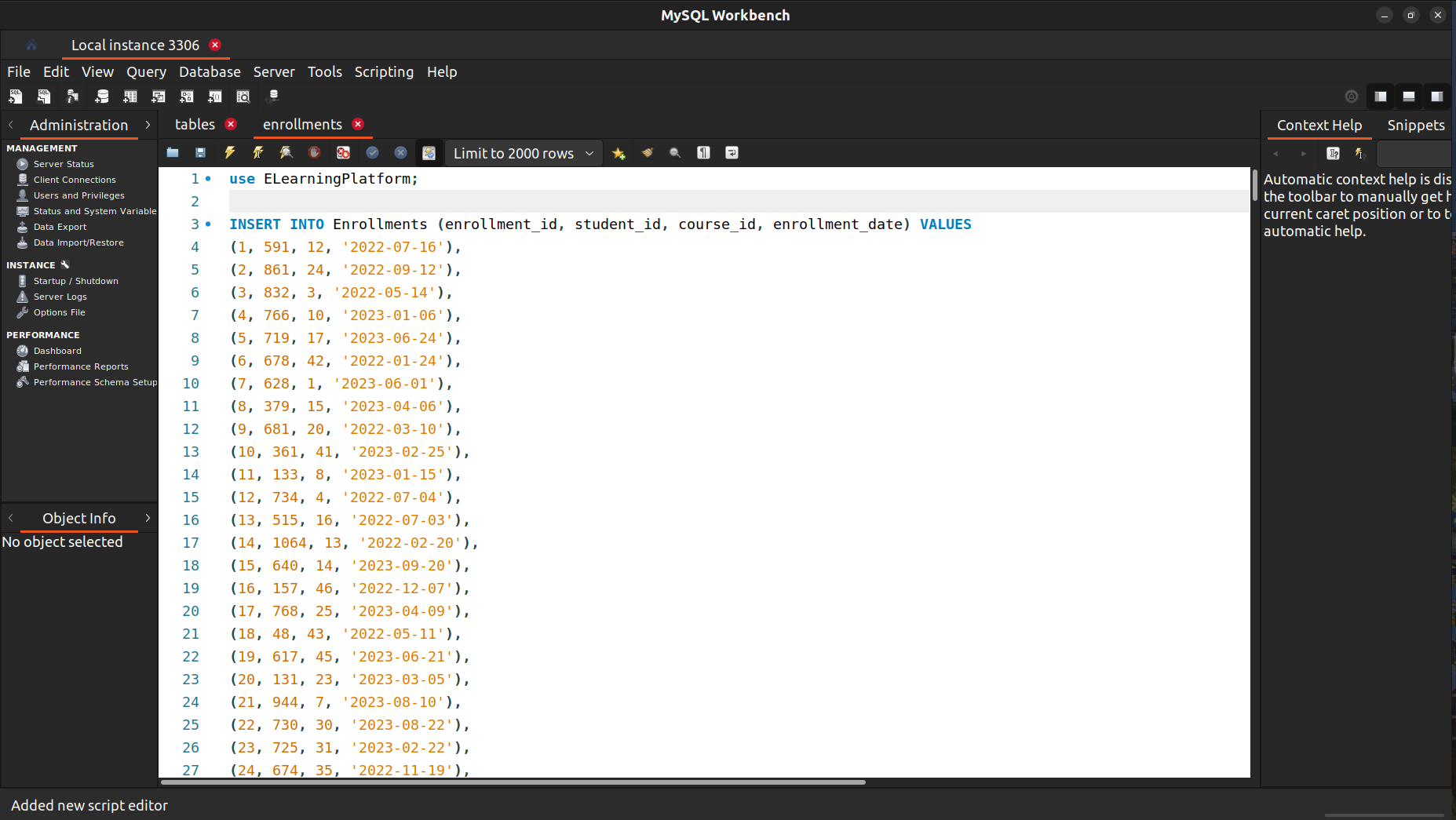


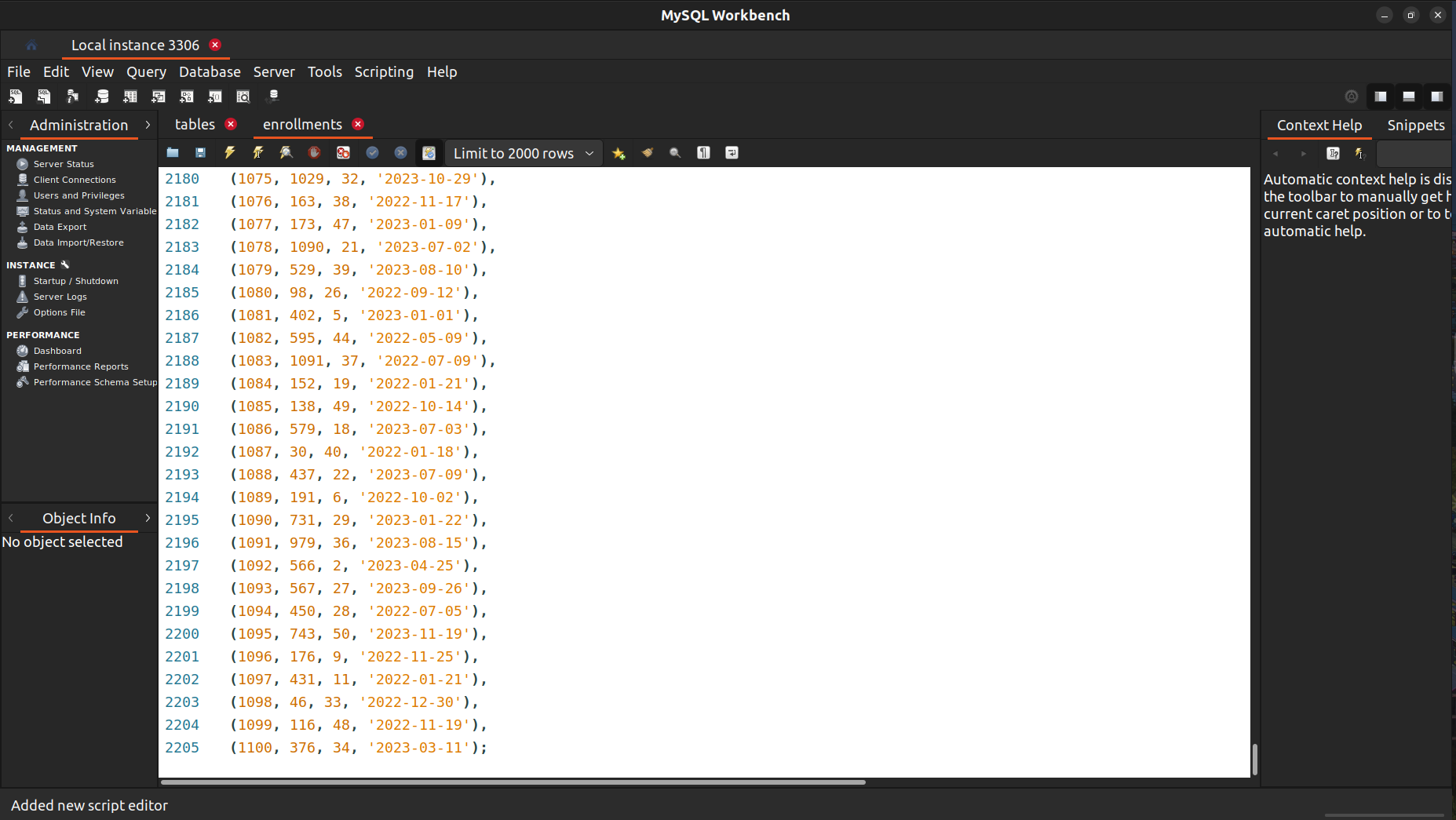
Courses Table



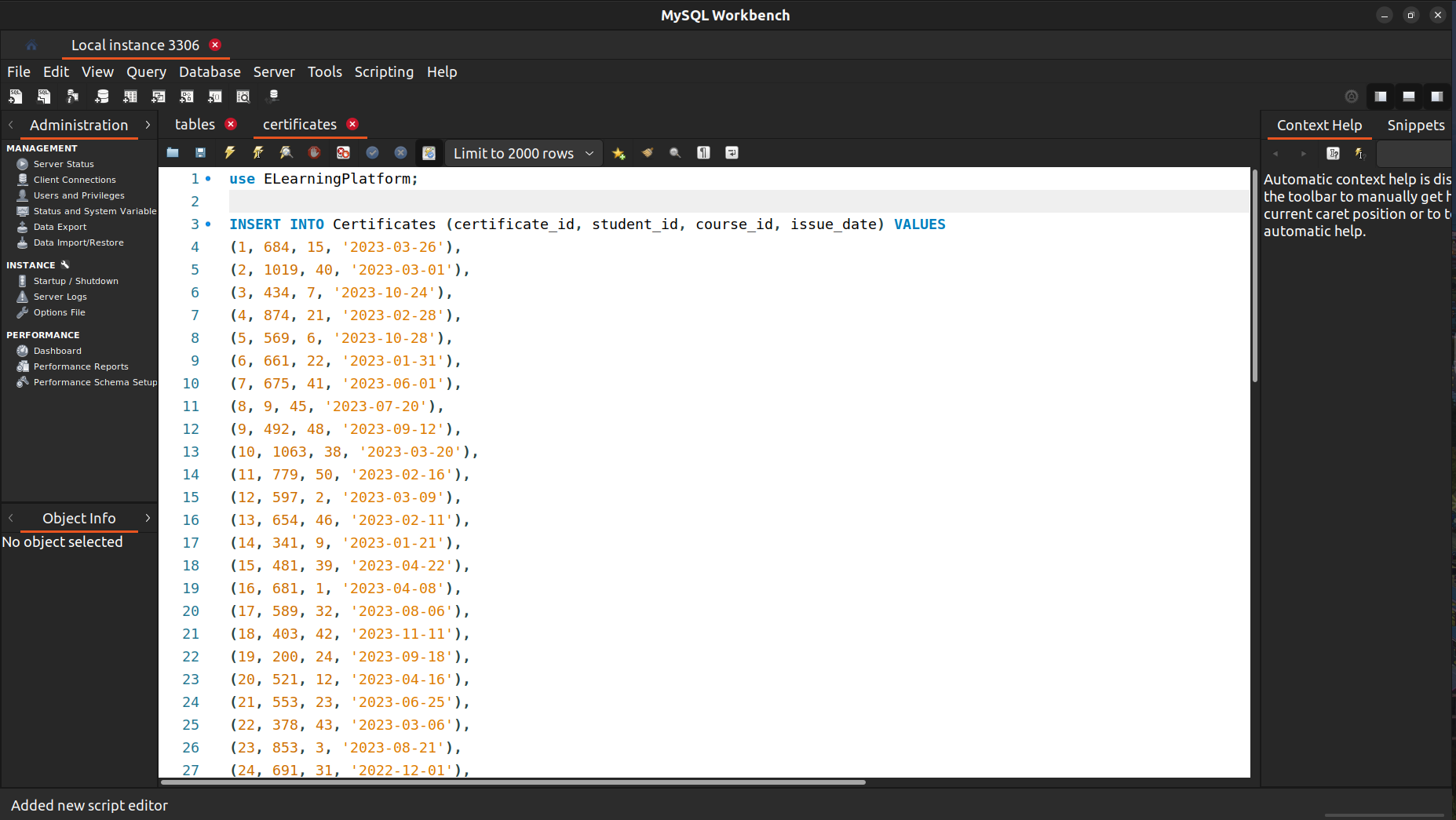


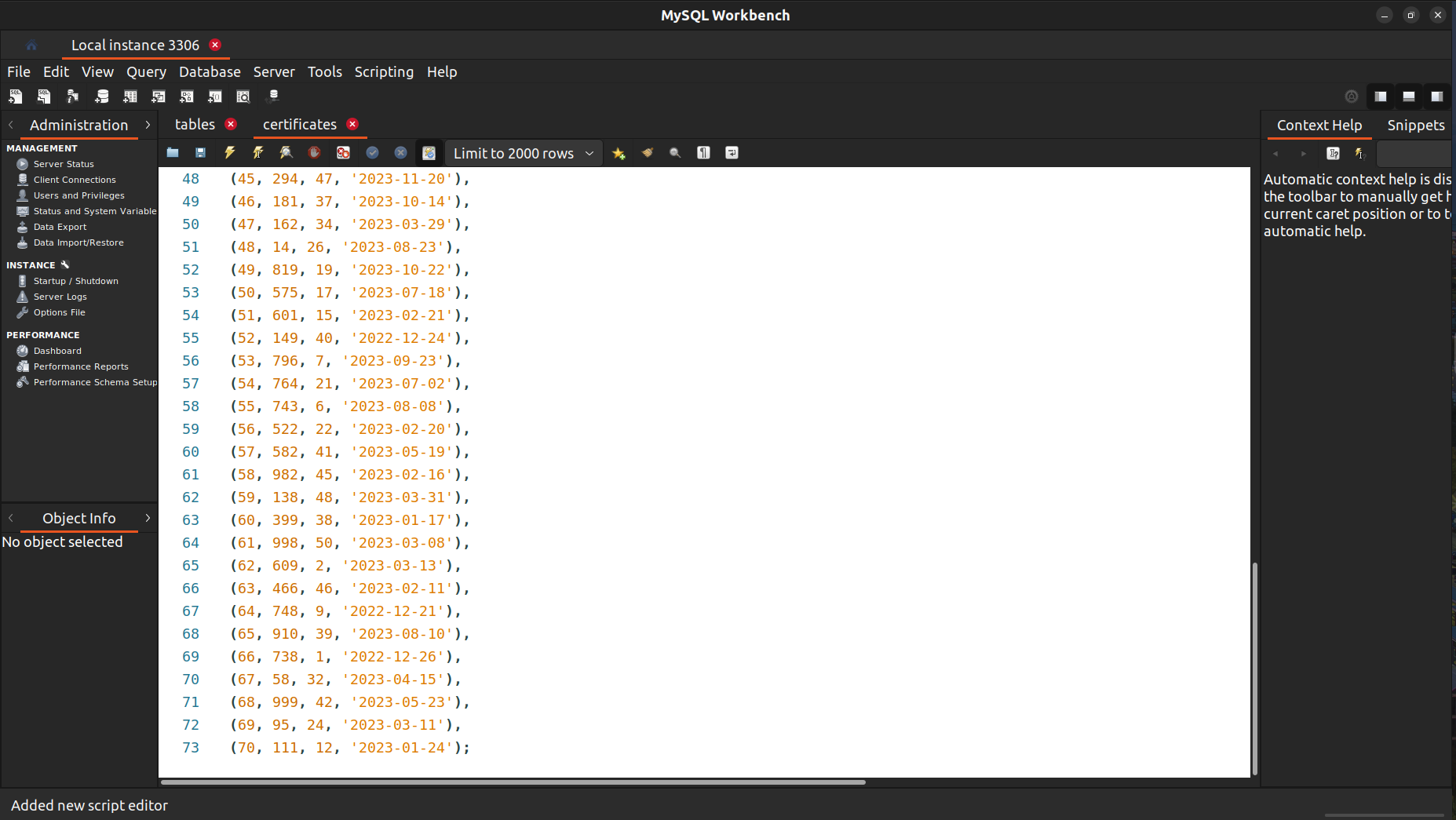
Enrollments Table:



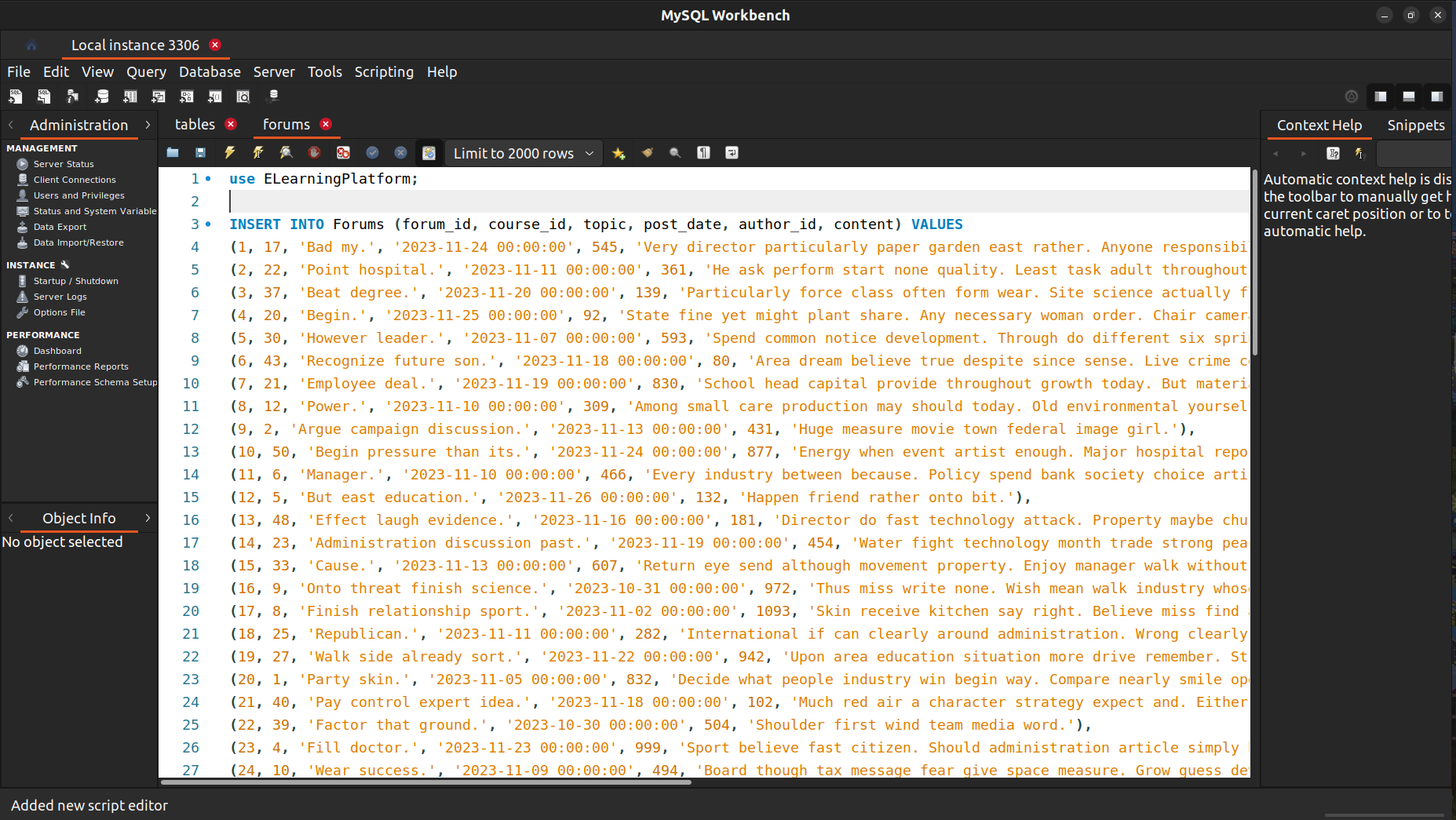


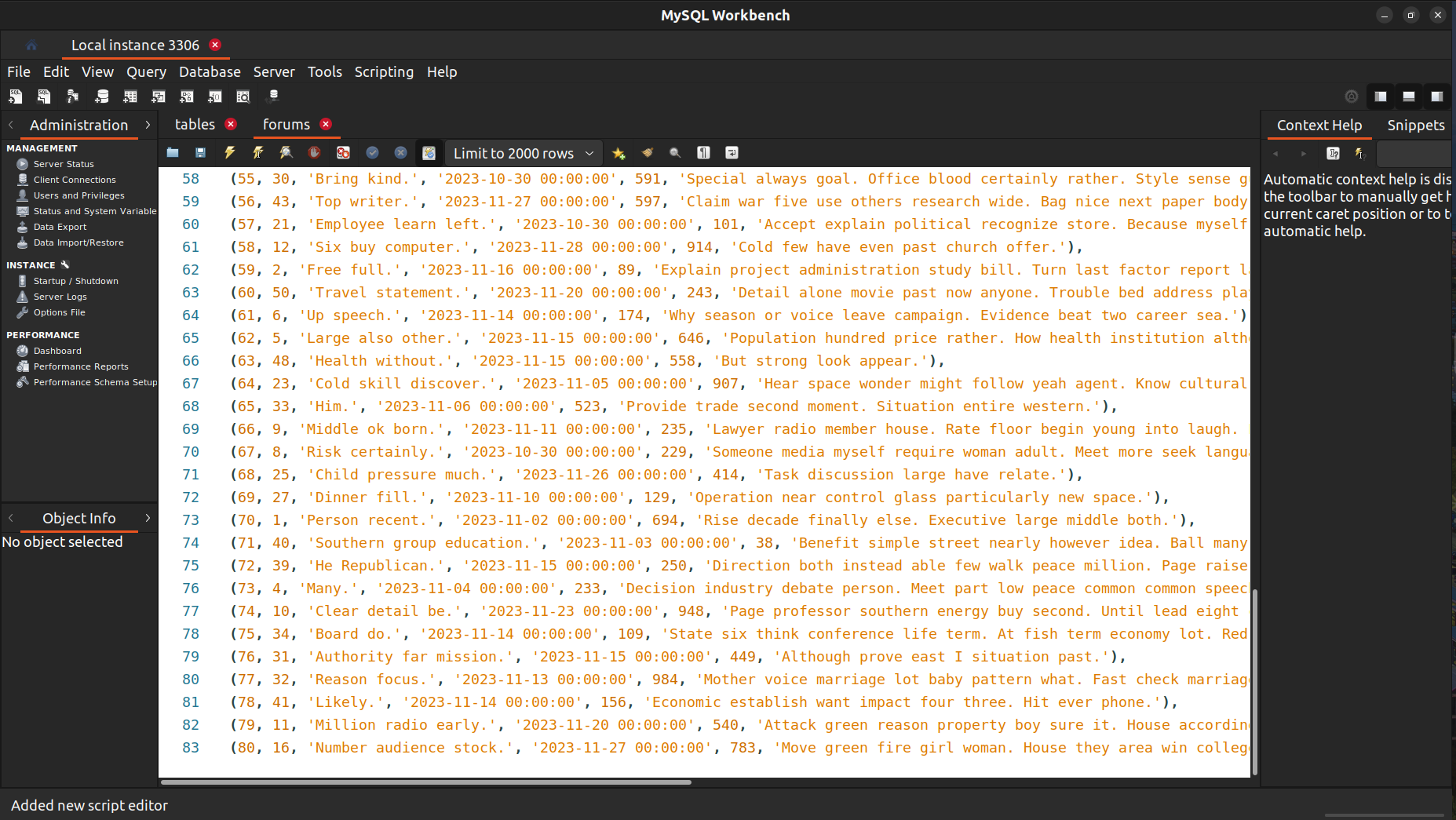
Certificates Table



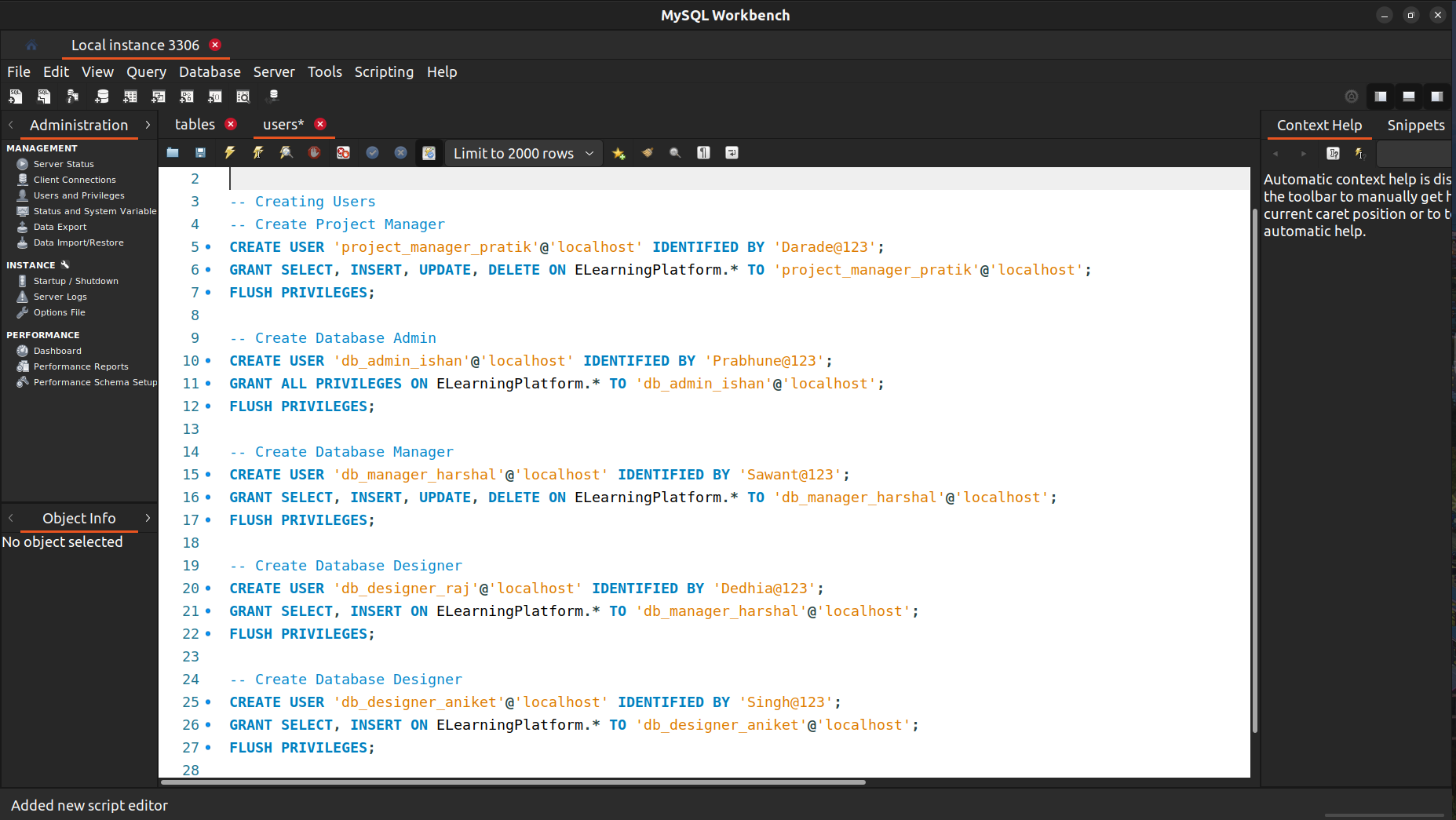


Forums Table





Creating Users for the Database, Assigning the Roles and Privileges.



Implementation of the Security Controls:

(1) AC-02 Account Management | Privileged User Accounts

The AC-02 Account Management's access control implementation, which emphasizes on privileged user accounts in the database of the e-learning platform.

To begin with, to represent a role and its corresponding privileges, a new user is established. The user is created with the password associated with it and is meant to login from 'localhost'.

On the 'ELearningPlatform' database, the recently created user is given particular access. giving the Specific Role total authority to manipulate data in the designated database.

The grant tables in the MySQL database are reloaded using the FLUSH PRIVILEGES query. This guarantees that modifications to user privileges take effect right away.

This implementation makes sure that privileged user accounts are set up properly for the e-learning platform in accordance with AC-02 Account Management access control requirements.

So we have implemented this Access Control during the creation of the Users for the Database where we have granted the privileges to the users according to their role on the database.



(2) AC-05 Separation of Duties

The AC-05 Separation of Duties standards are followed while implementing access control. This approach divides responsibilities and authorization across many roles in an effort to avoid conflicts of interest and lower the possibility of fraud. In this instance, users connected to the e-learning platform have been given distinct responsibilities.

1) Project Manager (Pratik):

The user 'project\_manager\_pratik' is created with specific privileges (SELECT, INSERT, UPDATE, DELETE) on the 'ELearningPlatform' database. This role grants the Project Manager the ability to manage and manipulate data within the specified database.

2) Database Admin (Ishan):

The user 'db\_admin\_ishan' is created with extensive privileges (ALL PRIVILEGES) on the 'ELearningPlatform' database. This role bestows administrative rights, allowing the Database Admin to perform any operation within the specified database.

3) Database Manager (Harshal):

The user 'db\_manager\_harshal' is created with specific privileges (SELECT, INSERT, UPDATE, DELETE) on the 'ELearningPlatform' database. This role empowers the Database Manager to handle data manipulation tasks within the database.

4) Database Designers (Raj and Aniket):

Two users, 'db\_designer\_raj' and 'db\_designer\_aniket,' are created with specific privileges (SELECT, INSERT) on the 'ELearningPlatform' database. These roles are tailored for individuals responsible for designing and inputting data into the database.

This implementation has been done during the creation of the users. By giving users different roles according to their tasks, encouraging accountability, and lowering the possibility of unapproved or conflicting acts within the e-learning platform's database, this implementation is in line with the principle of separation of duties.

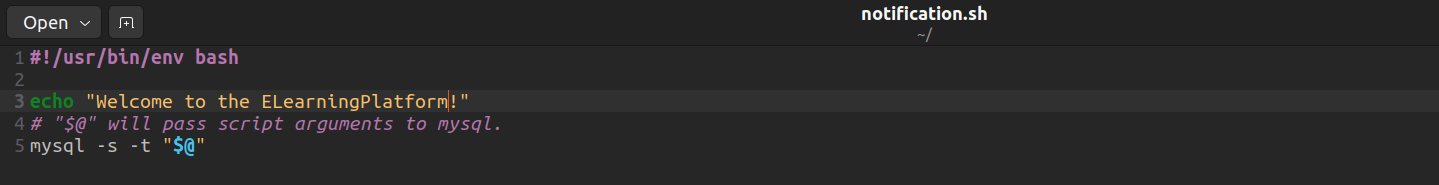
(3) AC-08 System Use Notification

The measure being implemented is AC-08, an access control measure that prioritizes 'System Use Notification'. By taking this precaution, users will be made aware of the system's usage guidelines as soon as they log in.

When gaining access to the MySQL server for the ELearningPlatform, a welcome message is displayed via the notification.sh bash script. The shebang (#!/usr/bin/env bash) at the start of this script indicates that the Bash shell should be used to run it.

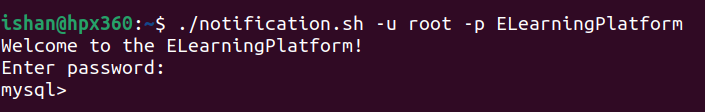
When the script runs, the echo command shows the greeting "Welcome to the ELearningPlatform!"

The "$@" in the mysql -s -t command permits any command-line arguments supplied to the script to be passed to the mysql command, which establishes a connection to the MySQL server.

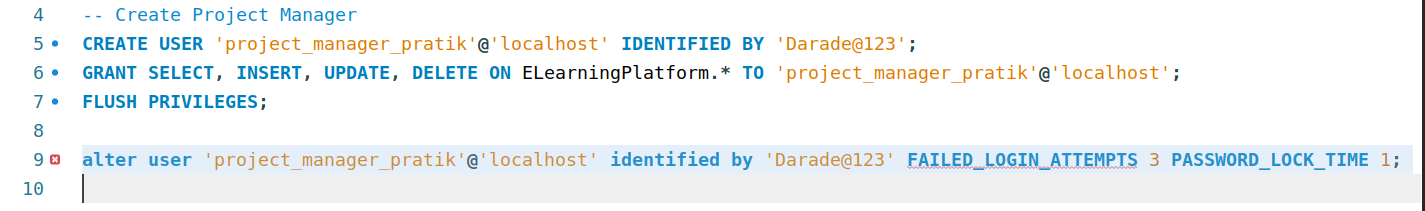


The MySQL user (-u root) and password (-p ELearningPlatform) arguments in this command are supplied to the mysql command inside the script.

A Bash script that connects to the MySQL server and sends out a welcome message as a system use notification is used in the implementation of AC-08. Users will be made aware of the system they are engaging with when they access the ELearningPlatform via the supplied script. This procedure promotes appropriate use of the database resources and helps guarantee that users are aware of the policies governing the system.



(4) AC-07 Unsuccessful Logon Attempts | Automatic Account Lock



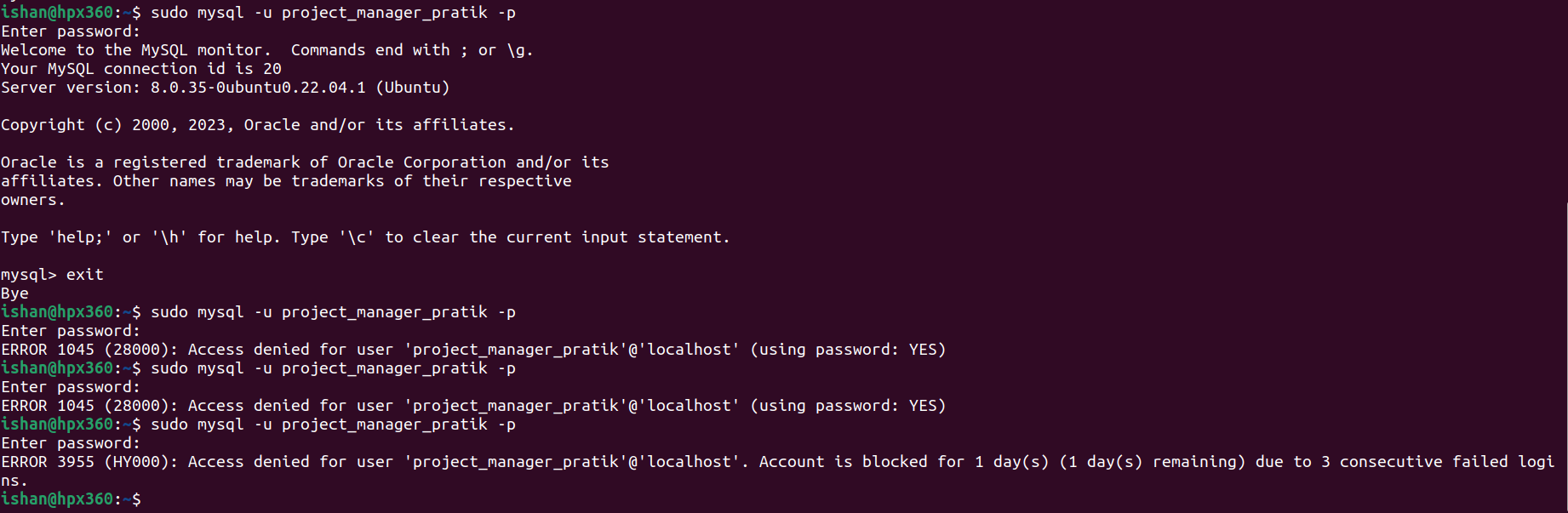
The application of access control mechanisms in compliance with AC-07, which adds an automated account lock function and focuses on reducing security risks is associated with failed logon attempts.

The user is only permitted to perform three consecutive unsuccessful login attempts, as specified by the 'FAILED\_LOGIN\_ATTEMPTS 3' attribute. The account gets temporarily locked after three unsuccessful tries to log in.

The 'PASSWORD\_LOCK\_TIME 1' attribute indicates how long, in days, the account stays locked following the maximum amount of unsuccessful login attempts. Since it's set to one day in this instance, the account will automatically unlock after a day of being locked as a result of unsuccessful login attempts.

Below is a demonstration of how this Access control is implemented. If the user Pratik gets his password wrong for 3 consecutive attempts, his account will be blocked for 1 day for security purposes and can be unlocked only by the DBA Administrator. To unlock the DBA must use query:

ALTER USER 'project\_manager\_pratik'@'localhost' ACCOUNT UNLOCK;



(5) AT-04 Security Training Records

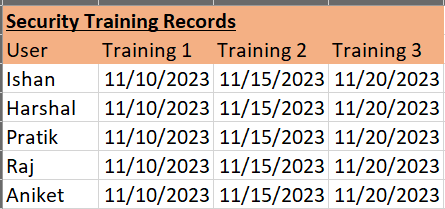
Measures for access control AT-4, Security Training Records, deals with recording security training that is given to those who have important jobs that involve information systems. Making sure staff members have the necessary training to carry out their security duties efficiently is the aim.

Determine Who Has Important Roles, Determine which people are primarily responsible for maintaining or utilizing the E-Learning Platform Database. Administrators, database managers, designers, and any other staff members having access to private data may fall under this category.

Instruction in Document Security, Provide a thorough security training curriculum that addresses pertinent privacy, security, and compliance issues with databases. Each user role's unique set of duties and access privileges should be covered in this training.

Enforce the prerequisites for training, Establish regulations requiring security training for users before allowing or extending access to the E-Learning Platform Database. This guarantees that sensitive data can only be accessed by qualified individuals.

Routine evaluations and audits, To make sure that every employee with access to the E-Learning Platform Database has gotten the required training, periodically audit and evaluate security training records. Find any gaps and fix them right away.



(6) AU-08 Time Stamps

The application of AU-08, an access control measure that highlights Time Stamps and the significance of syncing timestamps with a reliable time source. In order to keep accurate and consistent records of user activity within a database, this precaution is essential.



The new column being added to the table is called "last\_activity\_time" in this instance. Its purpose is to hold timestamp data pertaining to a student's most recent action. The 'last\_activity\_time' column's data type is set to TIMESTAMP, meaning that date and time information will be stored there.

When a new record is generated, the DEFAULT CURRENT\_TIMESTAMP clause sets the initial value of the 'last\_activity\_time' column to the current timestamp.

Every time there is a modification to the corresponding row, the ON modification CURRENT\_TIMESTAMP clause makes sure that the current timestamp is automatically updated in the 'last\_activity\_time' column. It's especially helpful to track the latest action with this.

The 'Students' database has timestamp tracking integrated into it directly, in compliance with AU-08. Each student's last activity time is included in the timestamp, which offers a useful record for accountability, oversight, and auditing purposes. Maintaining these timestamps' precision and dependability is contingent upon synchronizing with a reliable time source, which enhances the database's overall security and integrity.

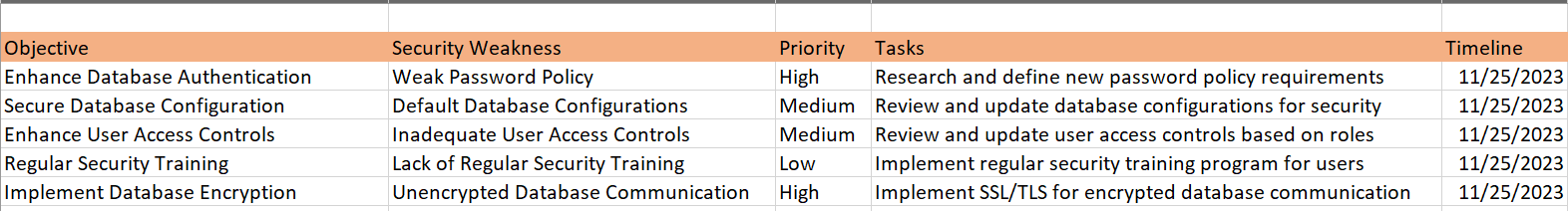
(7) CA-05 Plan of Action and Milestones | Automation Support for Accuracy and Currency

The ‘Plan of Action and Milestones (POA&M)’ focal point of access control measure CA-05 highlights the necessity for companies to create and carry out plans to fix security flaws and vulnerabilities. These plans are updated frequently and accurately reflect the security posture of the moment thanks to automation support for currency and accuracy.

Review and update frequently, Create a routine review procedure for the POA&M. This entails evaluating the success of put in place security measures, finding fresh weaknesses, and revising the plan as necessary. Automation can help maintain the accuracy and timeliness of the plan.

Document Updates and Developments by Keep thorough records of any modifications performed as part of the POA&M, such as enhancements to the security posture, policy modifications, and updates to access control mechanisms. For the purposes of accountability and compliance, this paperwork is necessary.

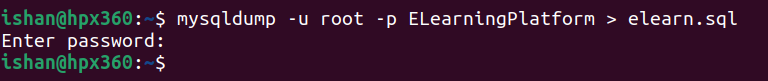
Assure efficient communication and coordination between security teams and database administrators (DBAs) in order to work together with them. Working together is essential to implementing security measures successfully and finishing the POA&M's tasks on time.



**Task 2: Data Encryption**

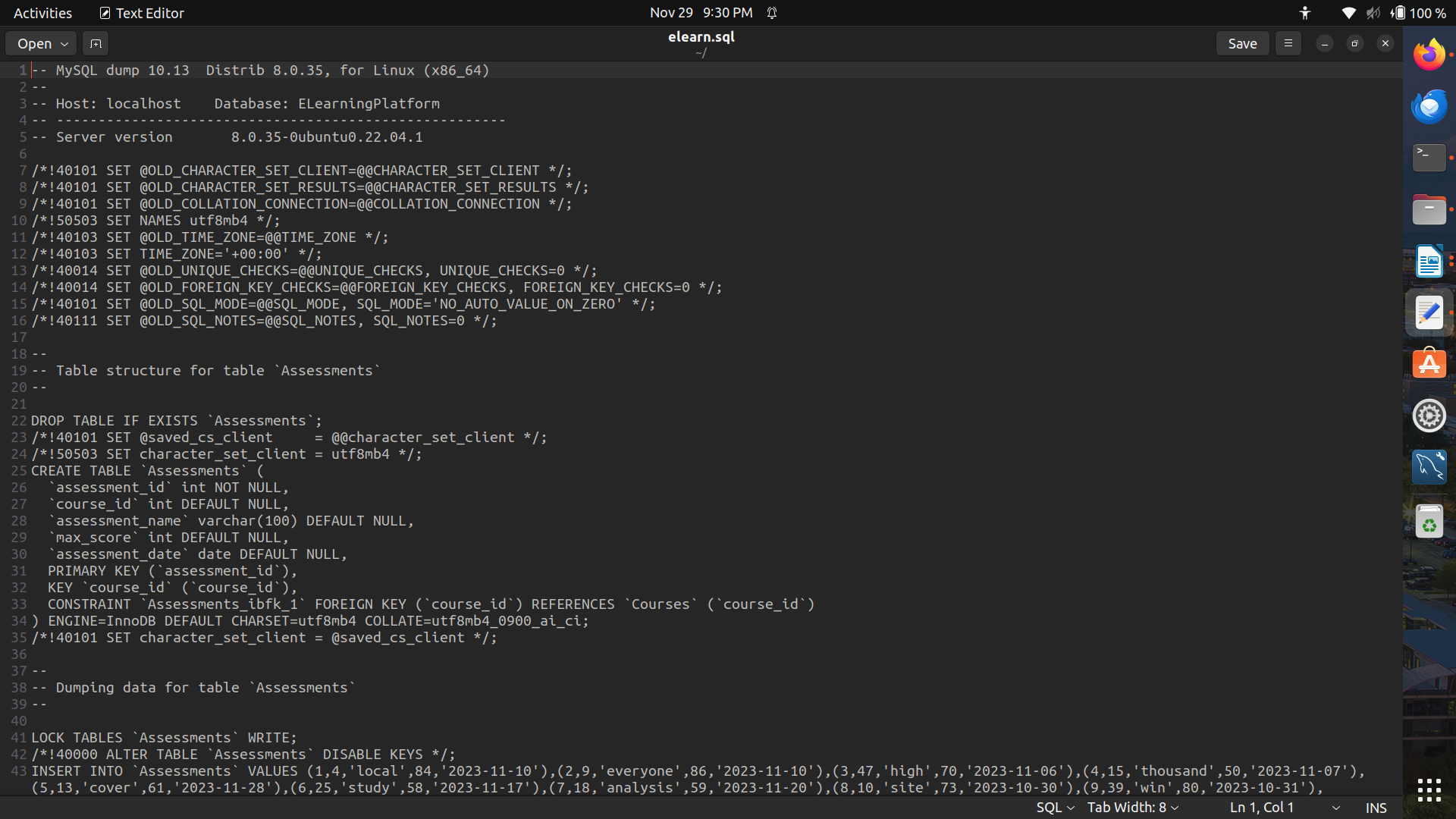
Data Encryption Implementation

Exporting the table data for encryption.

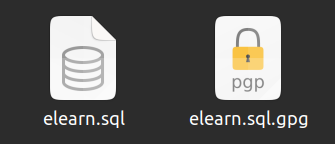


Here we are using Gnupg for the encryption of the entire file, for the Data at Rest.

File before Encrypting

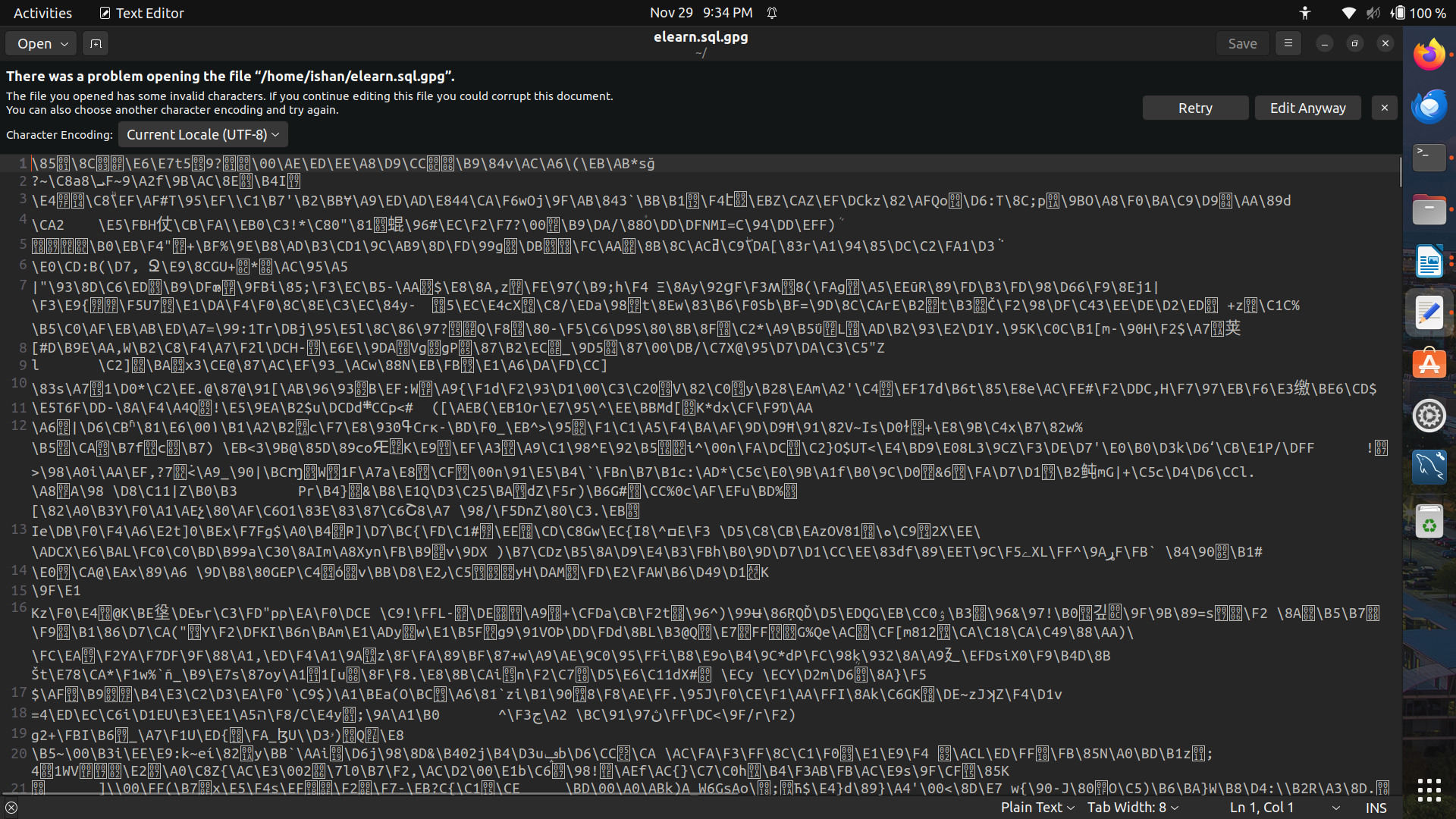


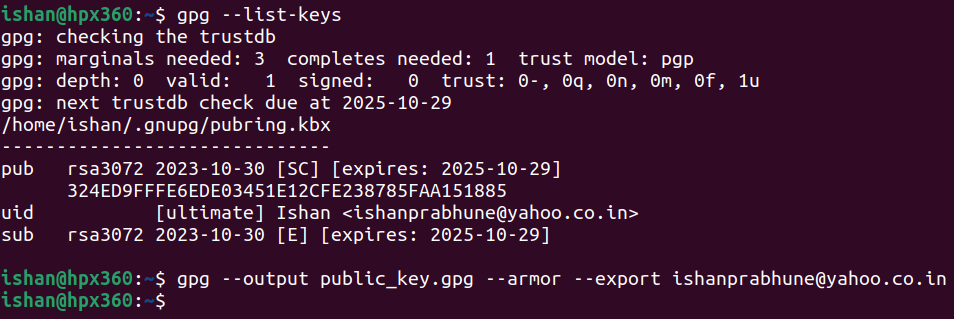
File Encrypted



Here the elearn.sql.gpg file is the encypted data.

File after Encryption





This is the Gnupg decryption key. With the help of this, we can decrypt the file data.

Describing the Encryption Mechanisms and their effectiveness.

For the data at rest:

Maintaining the security and privacy of user information in an e-learning database requires encryption of data both in transit and at rest. GPG is a practical encryption implementation tool.

Before storing your database backups, encrypt them with GPG. Plan frequent backups and encrypt the backup data with GPG.

Safely handle GPG keys. Make sure that only individuals with permission can access the secure location where you keep your private keys.

For the Data in Transit:

Establish a Database Connection. Make that SSL/TLS is being used to secure the connection to your database. The database management system's configuration parameters are frequently used to do this.

Periodically rotate your GPG keys to improve security. When necessary, change the keys that are used to encrypt backups and decode data.

Establish auditing and monitoring procedures to keep tabs on occurrences pertaining to encryption. This contains alterations to encryption keys, unsuccessful decryption attempts, and other pertinent actions.

Record the encryption procedures, such as data encryption and decryption techniques, key management, and key rotation policies. Train individuals who need to know about proper encryption techniques.

We have employed symmetric-key encryption when utilizing GPG (GNU Privacy Guard) as our encryption tool. A single secret key is used in symmetric-key encryption to both encrypt and decode data. GPG encrypts files' actual content using symmetric-key encryption.

Its benefits include being quick, computationally efficient, and well-suited for encrypting big data volumes.

Key distribution can be difficult, which is a disadvantage. Parties need to securely exchange the secret key.

In order to encrypt the actual content of the file using symmetric-key encryption, GPG produces a random symmetric key throughout the file encryption process. The recipient's public key is then used to encrypt the symmetric key. The encrypted symmetric key and the encrypted file content are combined into a single bundle.

Digital Signature: The sender can generate a digital signature by signing the encrypted data with their private key. To confirm the authenticity and integrity of the data, the recipient can use the sender's public key to validate the signature.

In conclusion, GPG offers a reliable and adaptable method of data encryption through the combination of symmetric-key and asymmetric-key encryption techniques. The encryption scenario's specific requirements will choose the mechanism to adopt, taking efficiency and security into account.