**NEPAL COLLEGE OF INFORMATION TECHNOLOGY**

Balkumari, Lalitpur

*Affiliated to Pokhara University*

**LAB REPORT FOR DATABASE MANAGEMENT SYSTEM**



**LAB REPORT 5: FAMILIARIZATION WITH DCL COMMANDS (GRANT, REVOKE)**

Submitted by: Submitted to:

Name: Arpan Adhikari Er. Simanta Kasaju

Roll No.: 231309

BE-CE (3rd SEM)

|  |  |  |  |
| --- | --- | --- | --- |
| **S. N** | **LAB TOPIC** | **DATE** | **REMARKS** |
| **1.** | **INTRODUCTION TO SQL** | 10th Nov |  |
| **2.** | **FAMILIARIZATION WITH DDL COMMAND** | 17th Nov |  |
| **3.** | **FAMILIARIZATION WITH VARIOUS CONSTRAINTS IN SQL** | 24th Nov |  |
| **4.** | **FAMILIARIZATION WITH DML C­­OMMANDS (INSERT, UPDATE, DELETE)** | 1st Dec |  |
| **5.** | **FAMILIARIZATION WITH DCL C­­OMMANDS (GRANT, REVOKE)** | 8th Dec |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**LAB 4: FAMLIARIZATION WITH DCL COMMANDS (GRANT, REVOKE)**

**OBJECTIVE:**

The objective of this lab is to understand and demonstrate the use of **Data Control Language (DCL)** commands, specifically **GRANT** and **REVOKE**, to manage database access permissions. Through this lab, students will learn how to:

1. Assign user privileges to perform specific actions on a database or its objects using the GRANT command.
2. Remove user privileges using the REVOKE command.
3. Implement controlled access to ensure database security and proper user management.
4. Explore practical scenarios for managing roles and permissions in a multi-user database environment.

This lab aims to provide hands-on experience with DCL commands, highlighting their role in database security and administration.

**THEORY:**

**1. Introduction to DCL (Data Control Language):** Data Control Language (DCL) is a subset of SQL used to define and manage the access control rights and permissions of users in a database system. The two main DCL commands are:

* **GRANT**: This command is used to assign specific privileges (permissions) to a user or a role.
* **REVOKE**: This command is used to remove or revoke the privileges granted to a user or a role.

DCL commands play a vital role in database security by restricting unauthorized access to sensitive data, ensuring that only authorized users can perform certain actions.

**2. GRANT Command:**

The GRANT command is used to assign specific privileges to a user or role on database objects like tables, views, procedures, etc. The syntax for the GRANT command is:

Syntax: GRANT privilege\_type ON object TO user;

* **privilege\_type**: Specifies the type of privilege (e.g., SELECT, INSERT, UPDATE, DELETE, ALL PRIVILEGES).
* **object**: The database object (e.g., table, column, database).
* **user**: The user or role to whom the privileges are being granted.

**Example:**

GRANT SELECT, INSERT ON college TO 'User1';

This command grants the SELECT and INSERT privileges on the employees table to User1 when connecting from localhost.

The GRANT command can be used to grant privileges at different levels:

* **Database level**: Grants access to all objects within the database.
* **Table level**: Grants access to specific tables.
* **Column level**: Grants access to specific columns within a table.
* **Global level**: Grants access to all databases on the server.

**3. REVOKE Command:**

The REVOKE command is used to remove privileges that were previously granted to a user or role. The syntax for the REVOKE command is:

Syntax: REVOKE privilege\_type ON object FROM user;

* **privilege\_type**: The type of privilege that is to be revoked (e.g., SELECT, UPDATE, ALL PRIVILEGES).
* **object**: The database object from which the privilege is being revoked.
* **user**: The user or role from whom the privilege is being revoked.

**Example:**

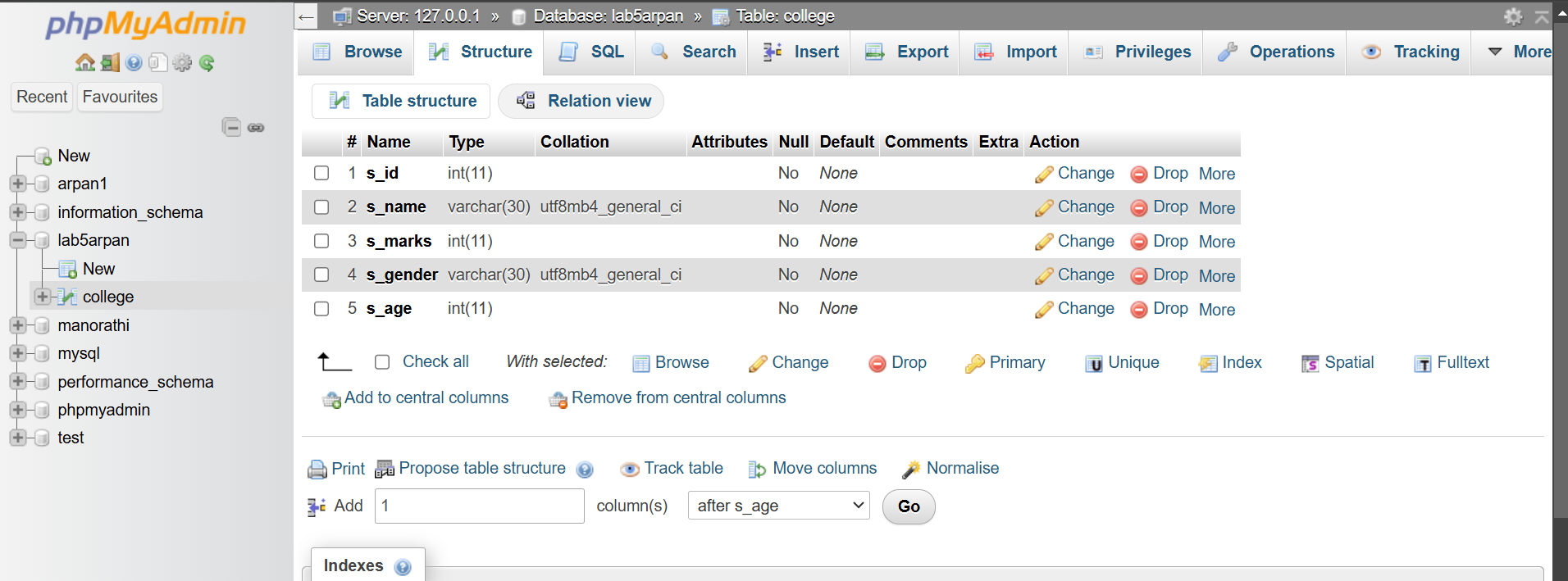
REVOKE SELECT ON college FROM 'User1';

This command removes the SELECT privilege on the employees table from User1.

If the user or role has been granted multiple privileges, each privilege must be revoked individually, unless ALL PRIVILEGES is used.

**Question 1:**

1. Create a table college with attributes s\_id, s\_name, s\_marks, s\_gender, and s\_age with constraints.

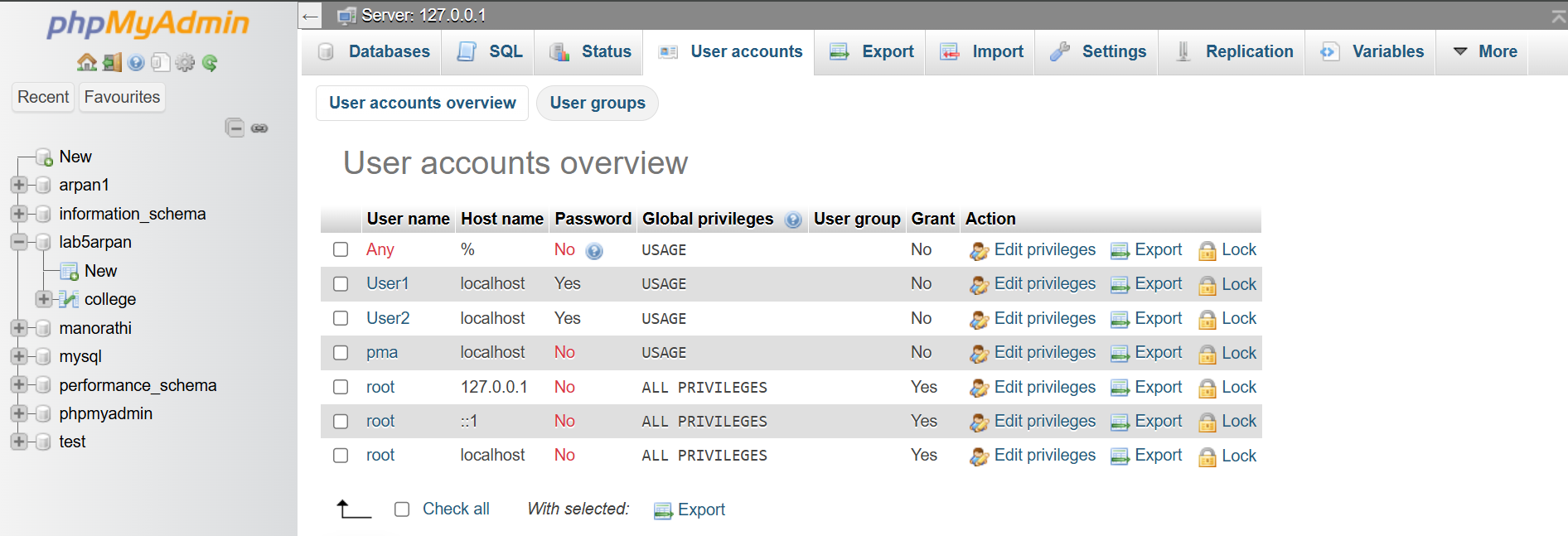


2. Create 2 new users with usernames User1 and User2 and give passwords to them. Grant select, insert, update to the 1st user and grant select, insert, delete to the 2nd user.

Creating users:

create user 'User1' @localhost identified by 'abcd';

create user 'User2' @localhost identified by 'abcd';



Granting Users:

GRANT select,insert,update on lab5arpan.college TO 'User1';

GRANT select,insert,delete on lab5arpan.college TO 'User2';



3.From user1, insert 2 new records on that table.

In User1:

use lab5arpan;

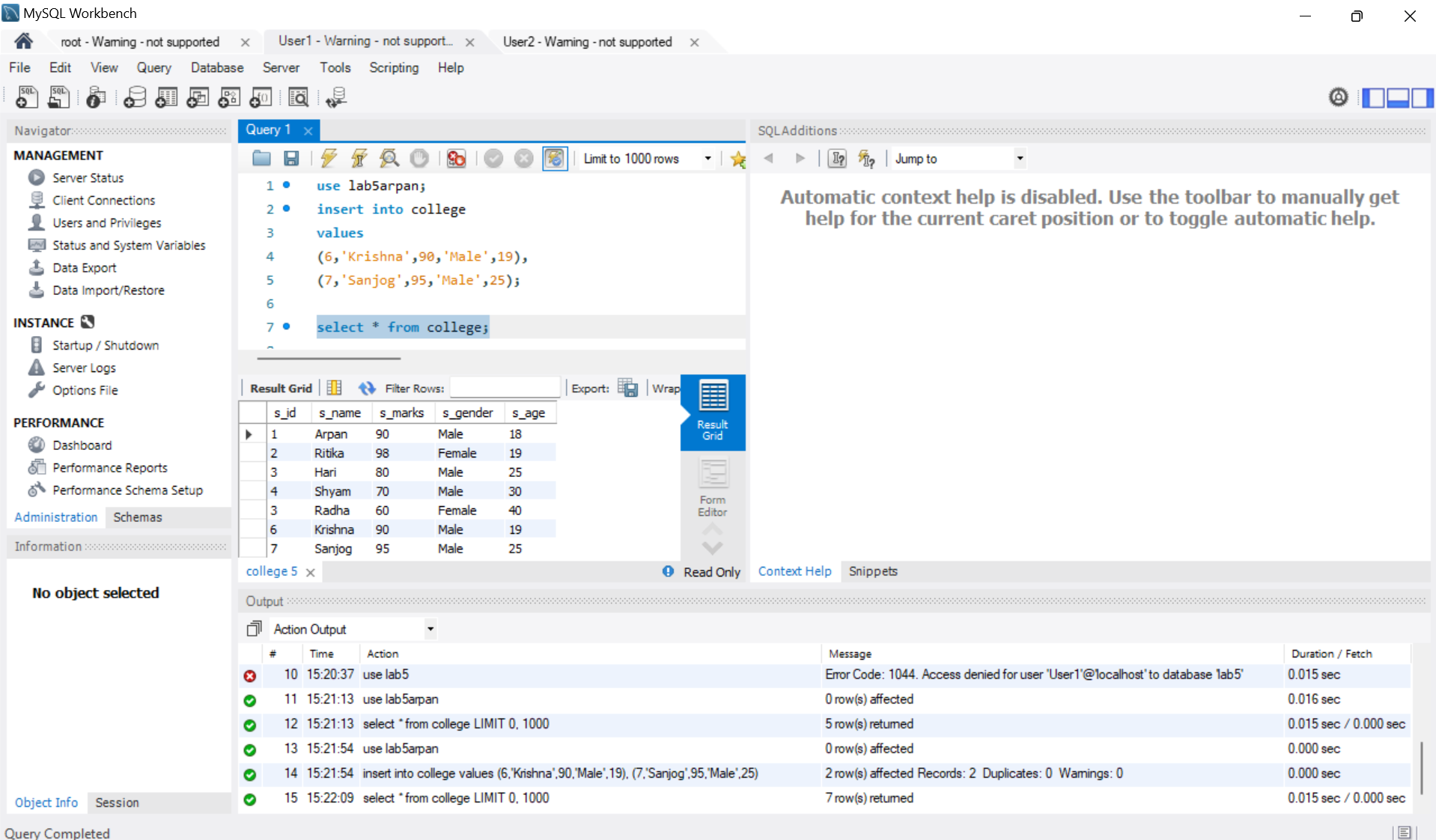
insert into college

values

(6,'Krishna',90,'Male',19),

(7,'Sanjog',95,'Male',25);

select \* from college;



4.From user2, insert 2 new records on that table.

In User2:

use lab5arpan;

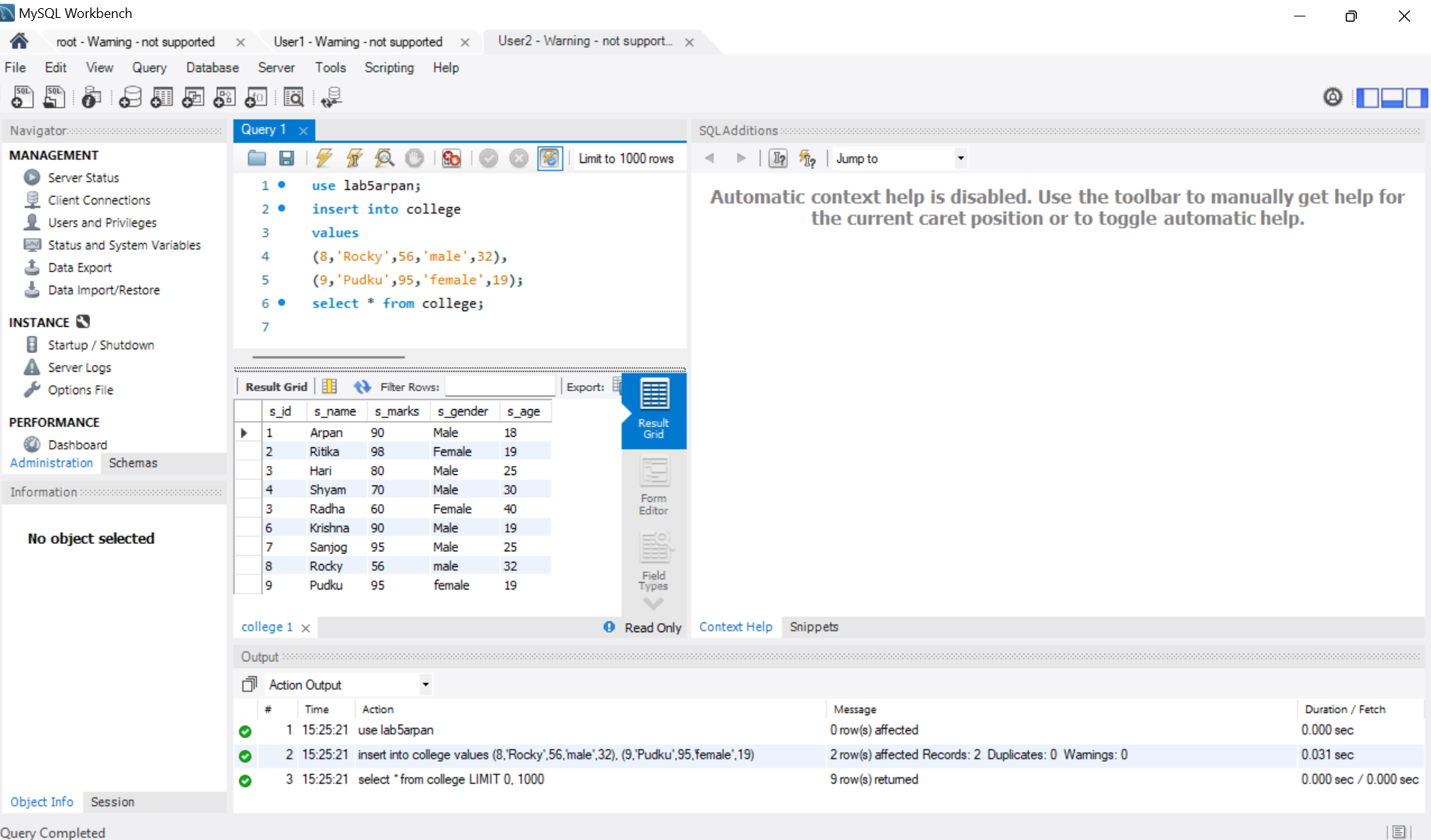
insert into college

values

(8,'Rocky',56,'male',32),

(9,'Pudku',95,'female',19);

select \* from college;



5. Display tables from both user accounts.

In 3,4.

6. Update the s\_name to 'ram' who scored 90 from user1 and display the result.

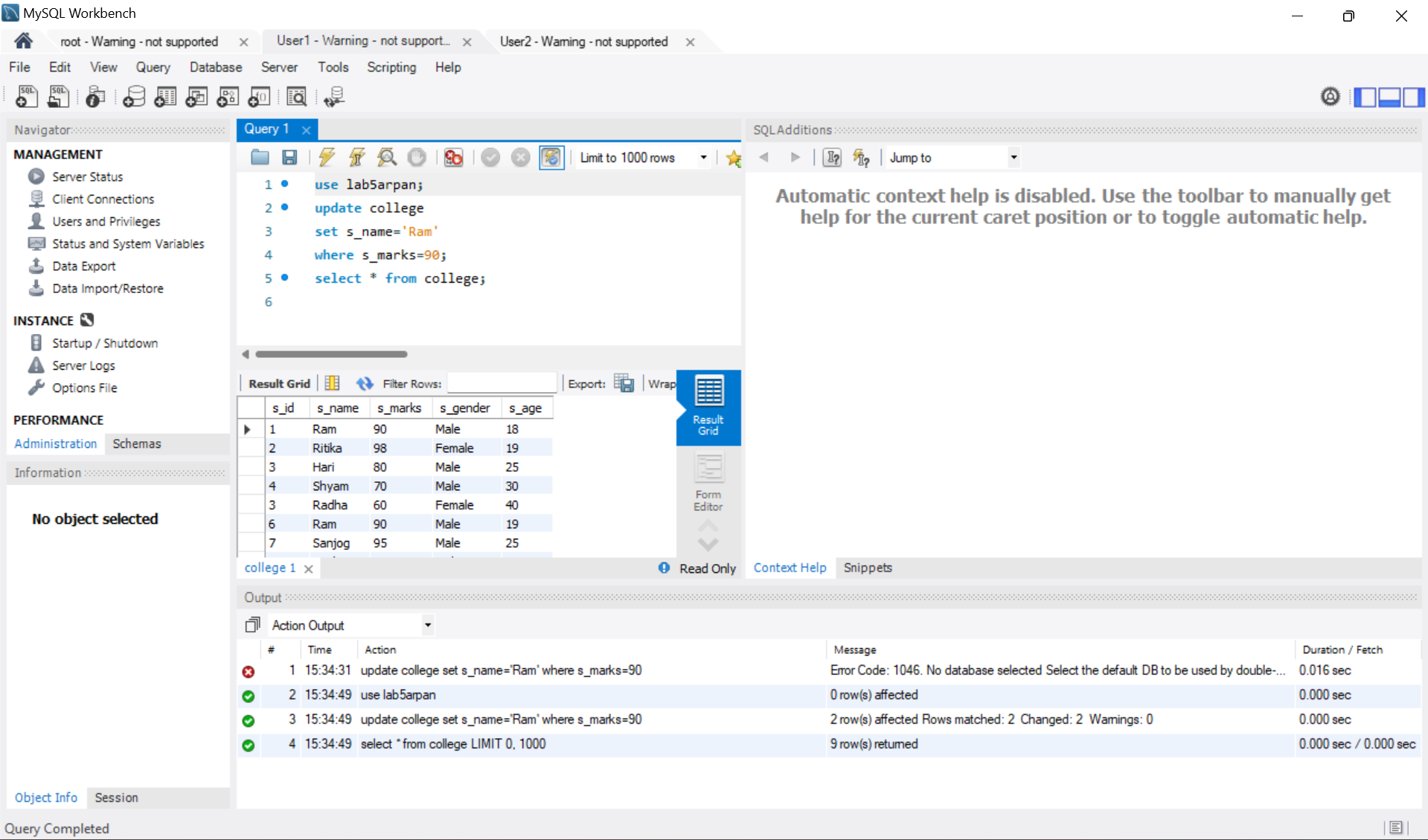
use lab5arpan;

update college

set s\_name='Ram'

where s\_marks=90;

select \* from college;



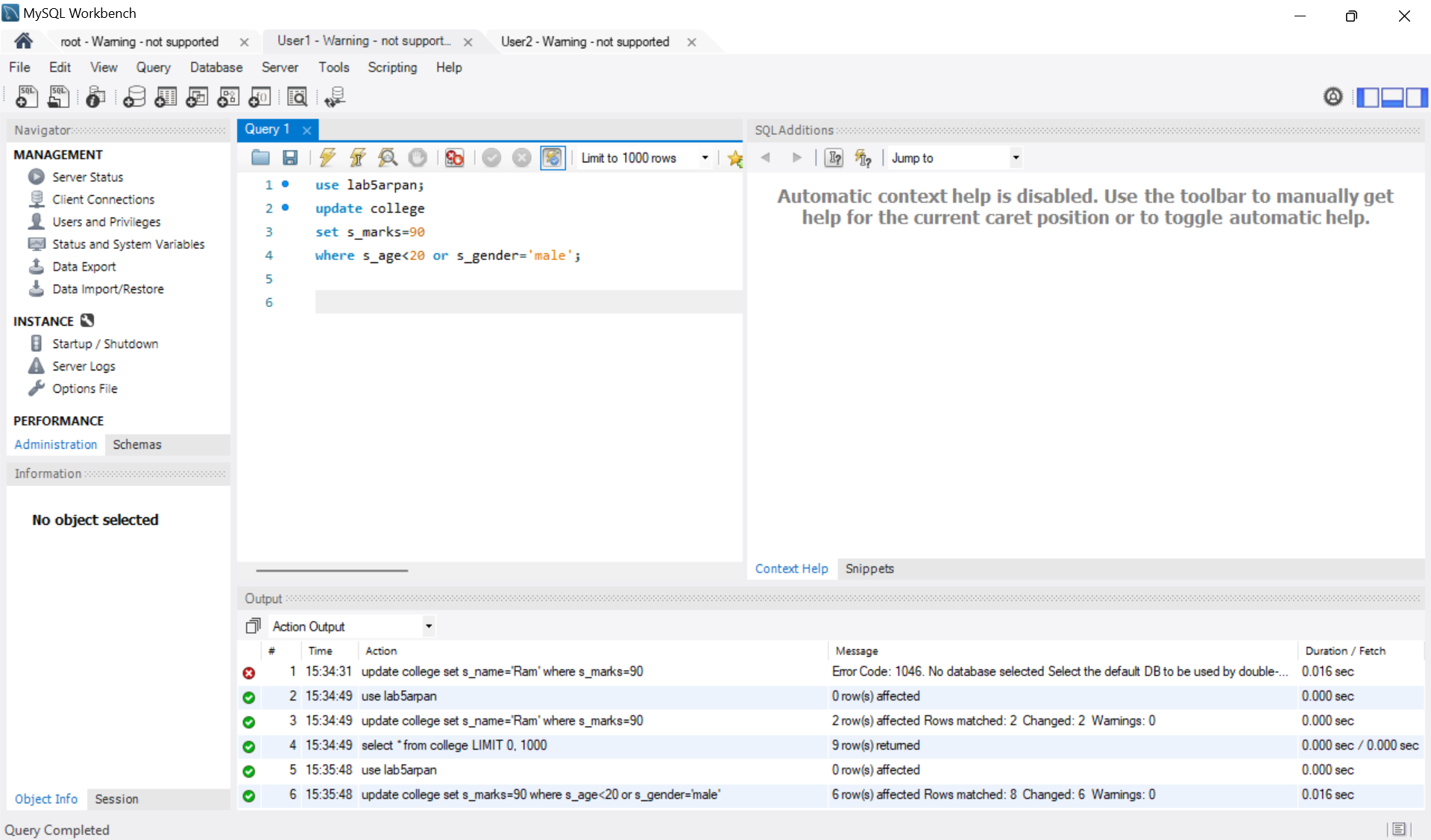
7. Update s\_marks to 90 who is below 20 years old or male from user1.

use lab5arpan;

update college

set s\_marks=90

where s\_age<20 or s\_gender='male';

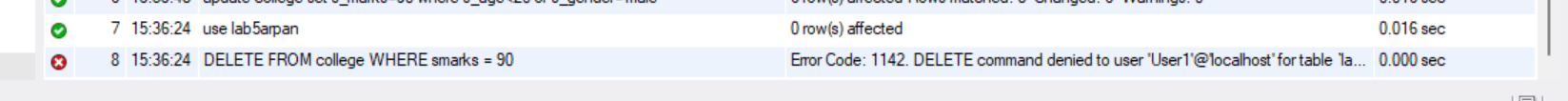


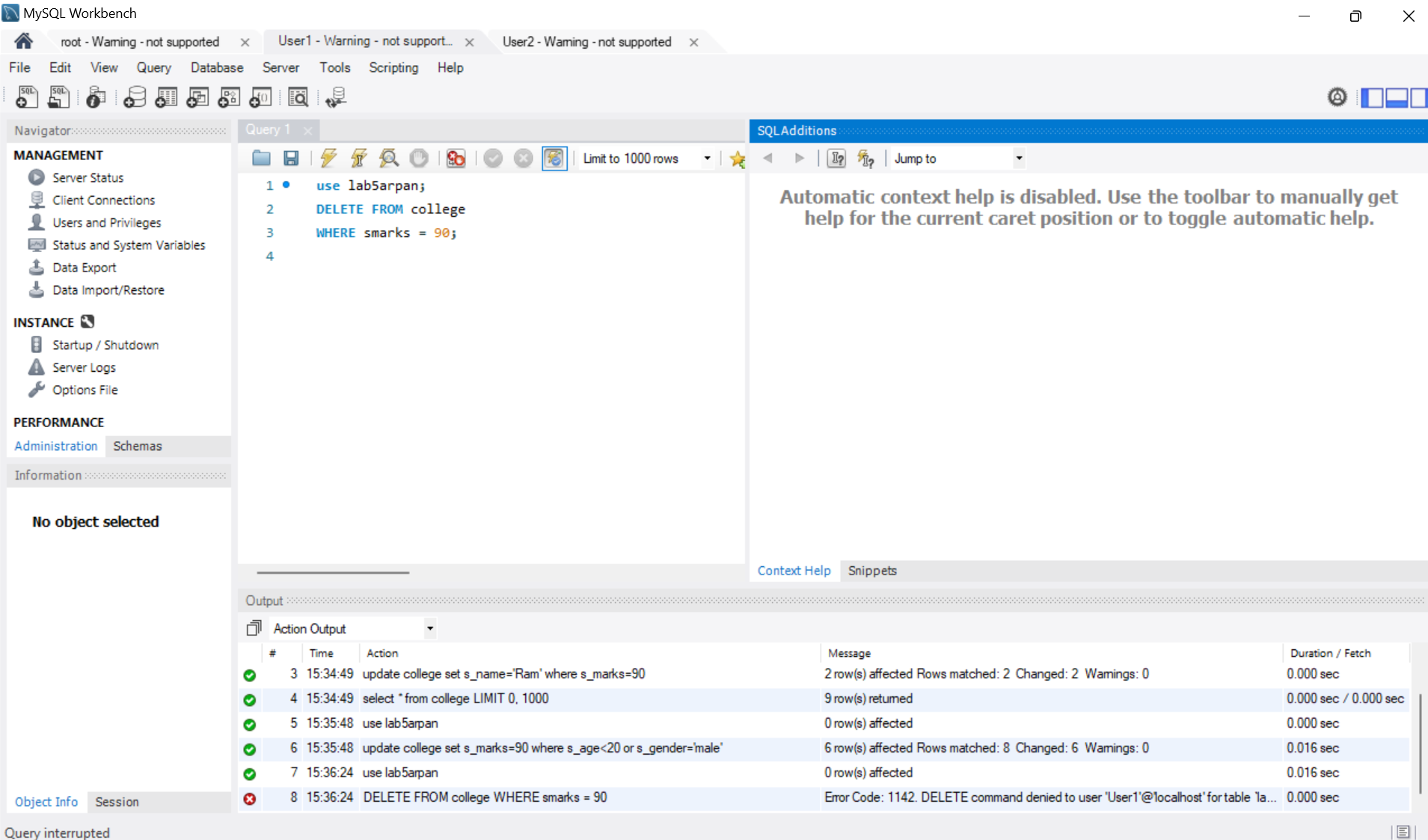
8. Show delete operation from user account 1, which is denied.

use lab5arpan;

DELETE FROM college

WHERE smarks = 90;





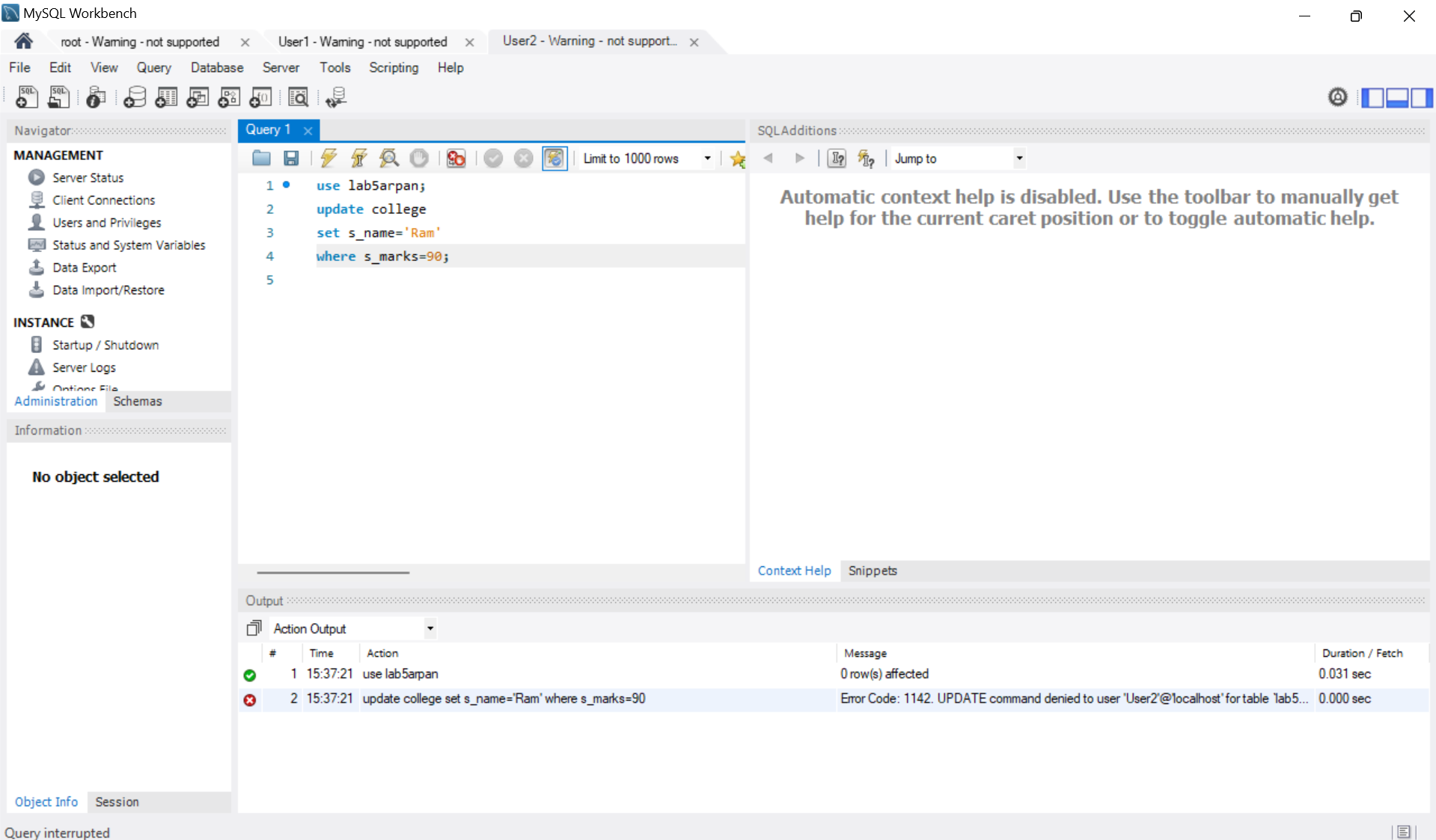
9. Show update operation from user account 2, which is denied

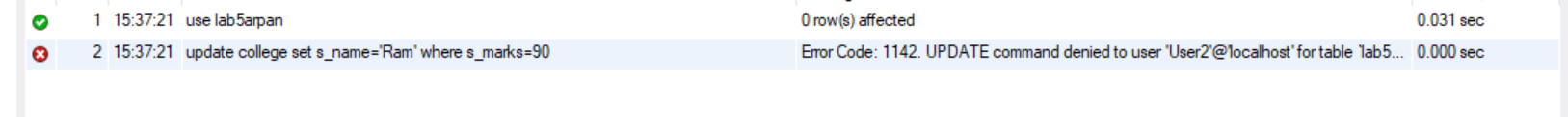
use lab5arpan;

update college

set s\_name='Ram'

where s\_marks=90;





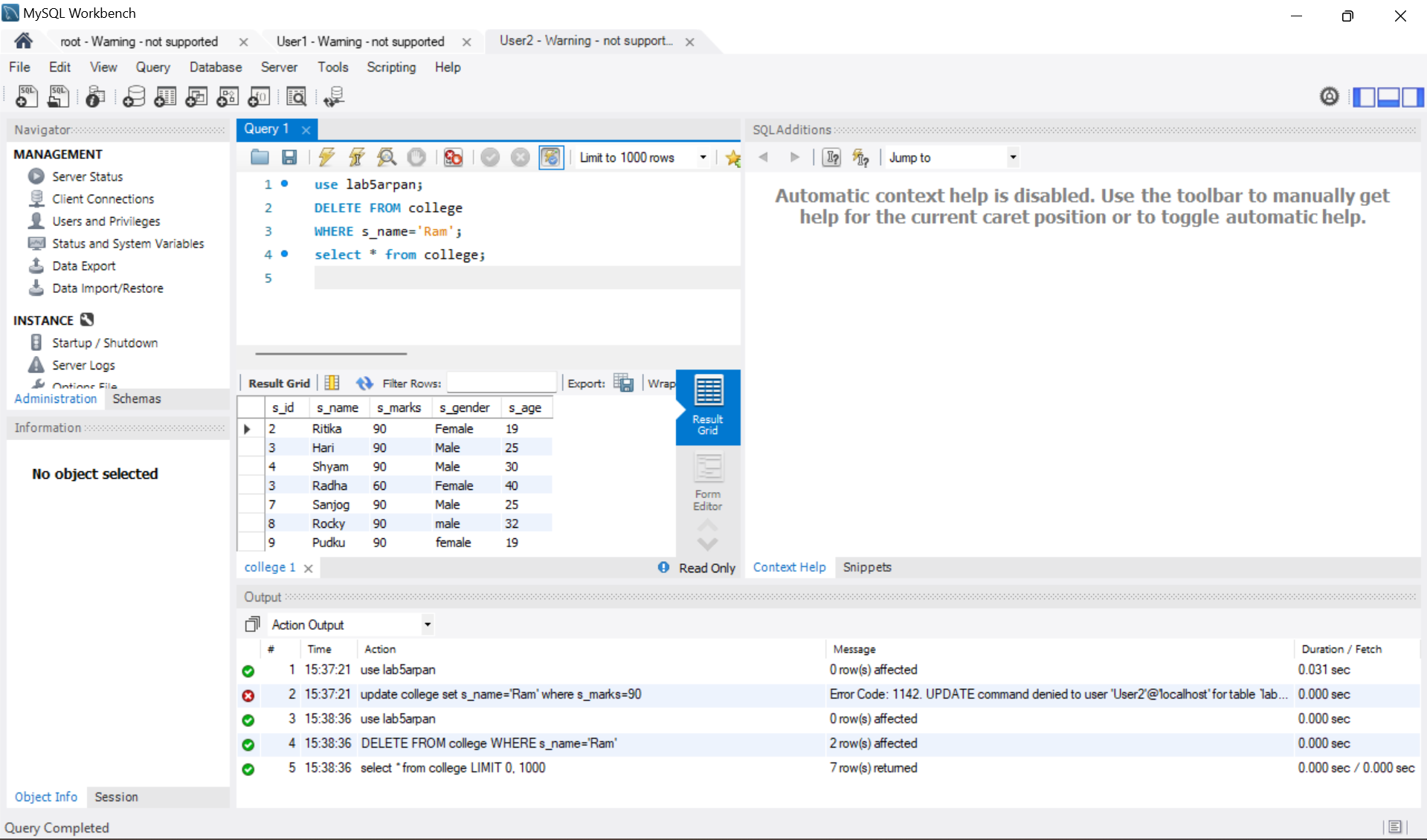
10.Delete from user2 where sname = 'Ram'.

use lab5arpan;

DELETE FROM college

WHERE s\_name='Ram';

select \* from college;



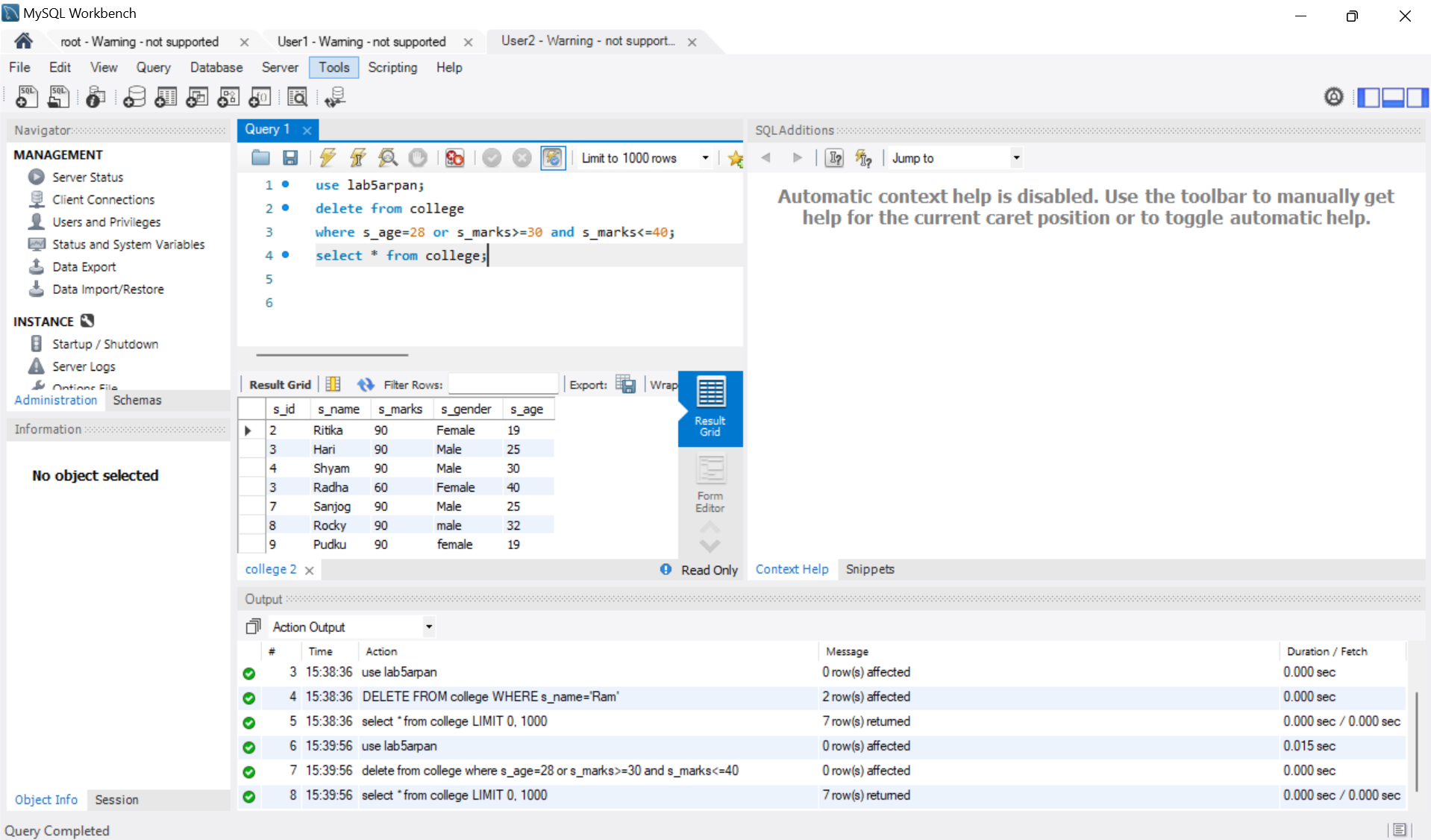
11. Delete from user2 where s\_age = 14 or s\_marks between 30 and 40.

use lab5arpan;

delete from college

where s\_age=28 or s\_marks>=30 and s\_marks<=40;

select \* from college;



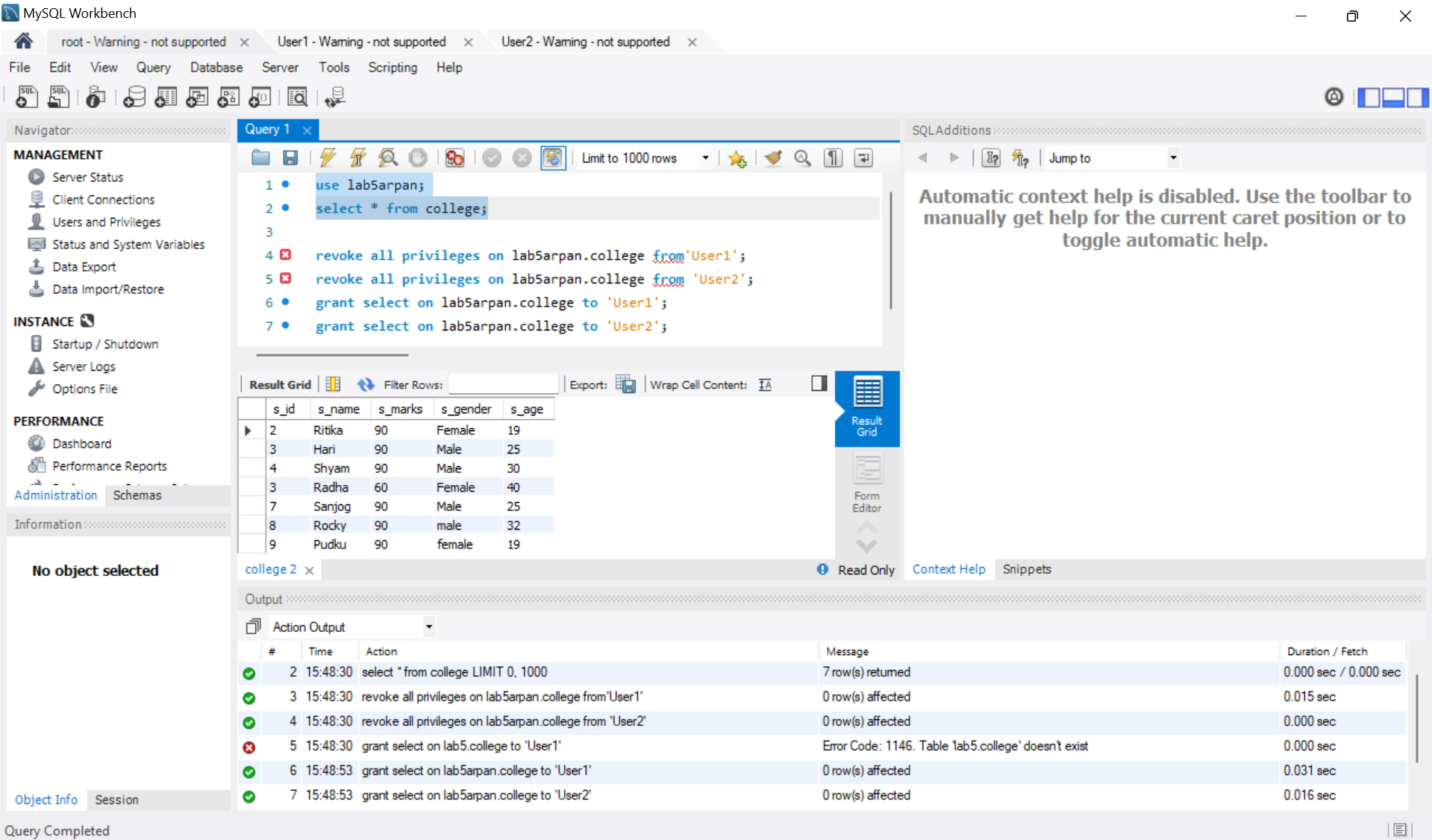
12. Revoke all privileges except select from both users.

revoke all privileges on lab5.college from'User1';

revoke all privileges on lab5.college from 'User2';

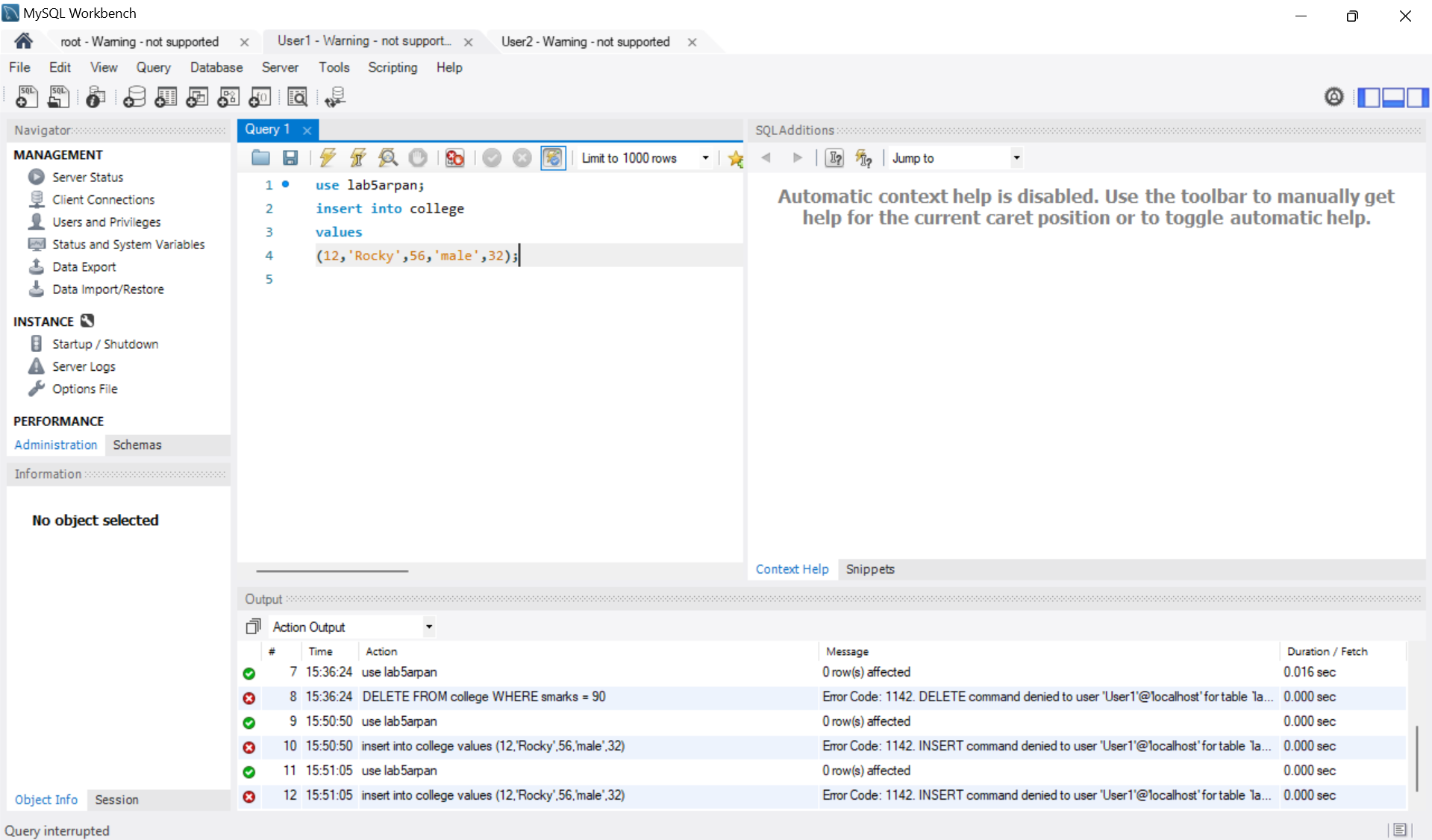
grant select on lab5.college to 'User1';

grant select on lab5.college to 'User2'



13. Now try to perform insert, update, and delete from both users; it will deny.

From User1:

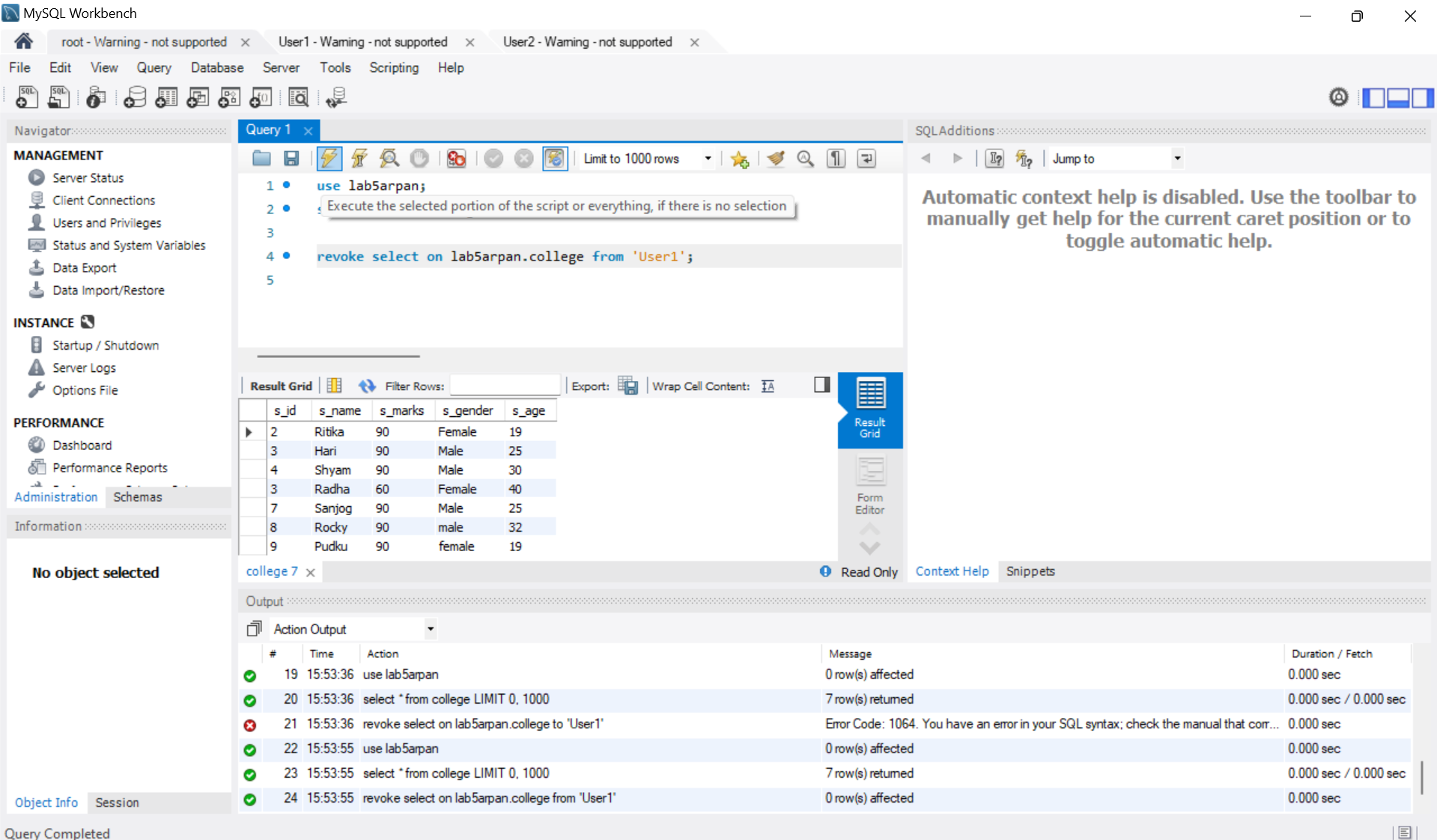


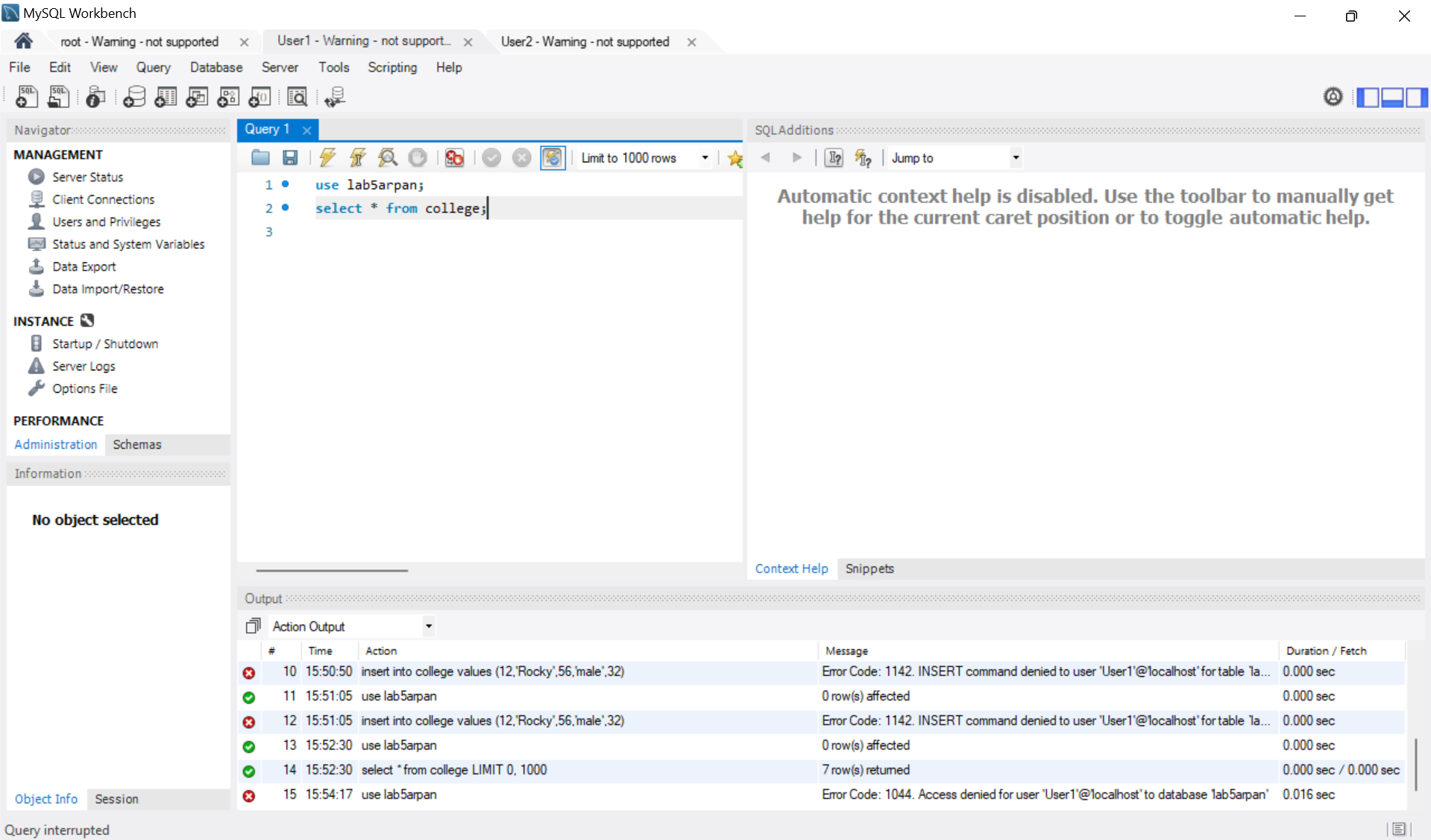
From User2:



14. Now also revoke the select privilege from user1 and show the denied message.

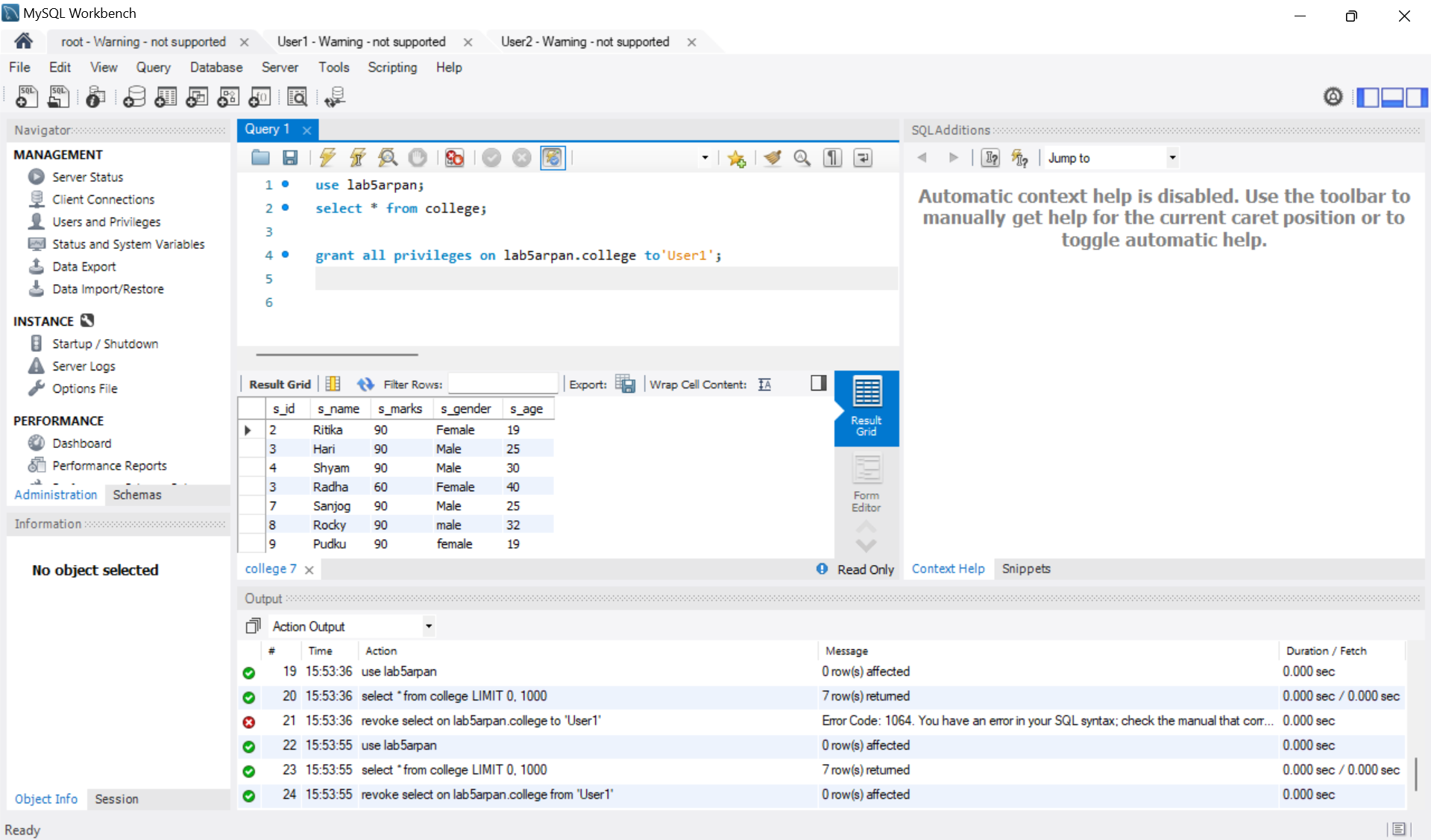
Revoke select on lab5arpan.college from ‘User1’;





16. Give all privileges to user1 and from user1 give select and insert privilege to user2.

grant all privileges on lab5arpan.college to 'User1';



From User1: granting select and insert privilege to User2.

grant select,insert on lab5arpan.college to 'User2';

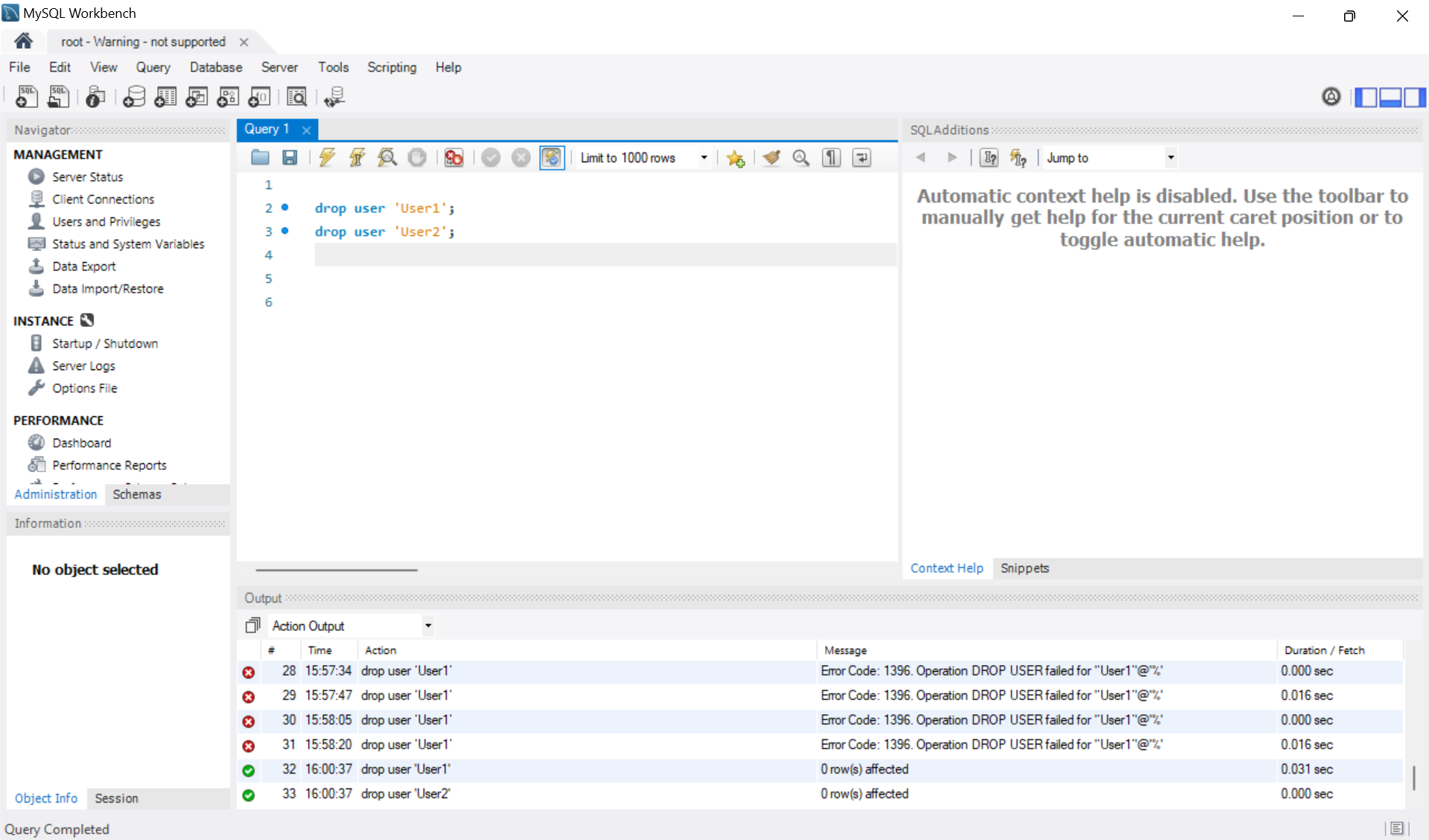


(Note:GRANT command is denied to users)

17. Finally, drop users 1 and 2.

drop user 'User1';

drop user 'User2';



**CONCLUSION:**

In this Lab, we learned about DCL COMMANDS such as GRANT and REVOKE commands which are fundamental in managing user access to a database. By using these commands, administrators can ensure that users have the right level of access while maintaining the security and integrity of the database system. Mastery of these commands is crucial for managing database security and implementing effective access control mechanisms in an organization.