**CO527: Advanced Database Systems**

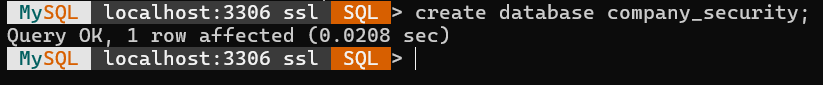
**Lab 05 - Database Security**

Ranage R.D.P.R.

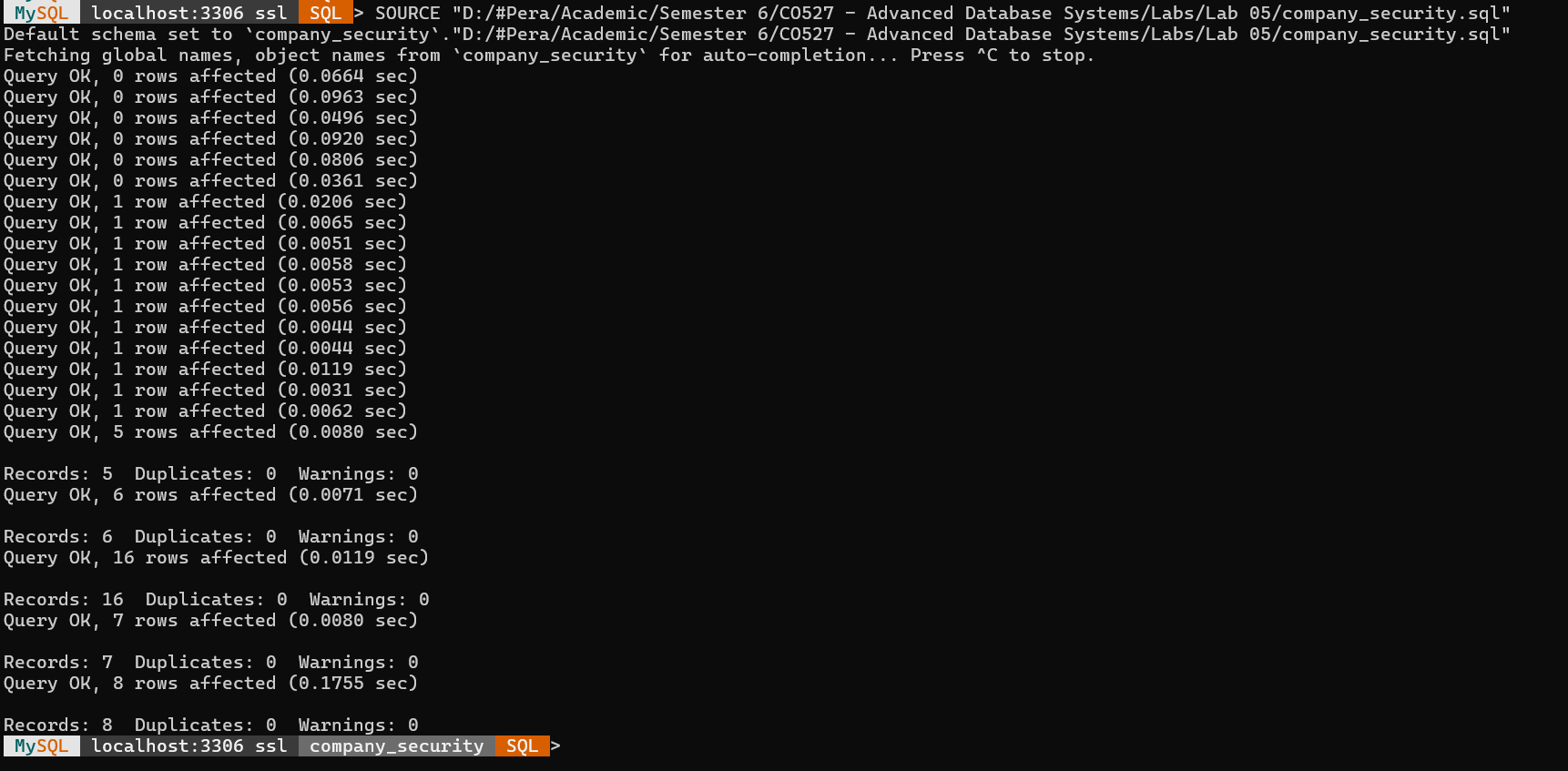
E/19/310

**Exercise**

**1. Create database company security.**

****

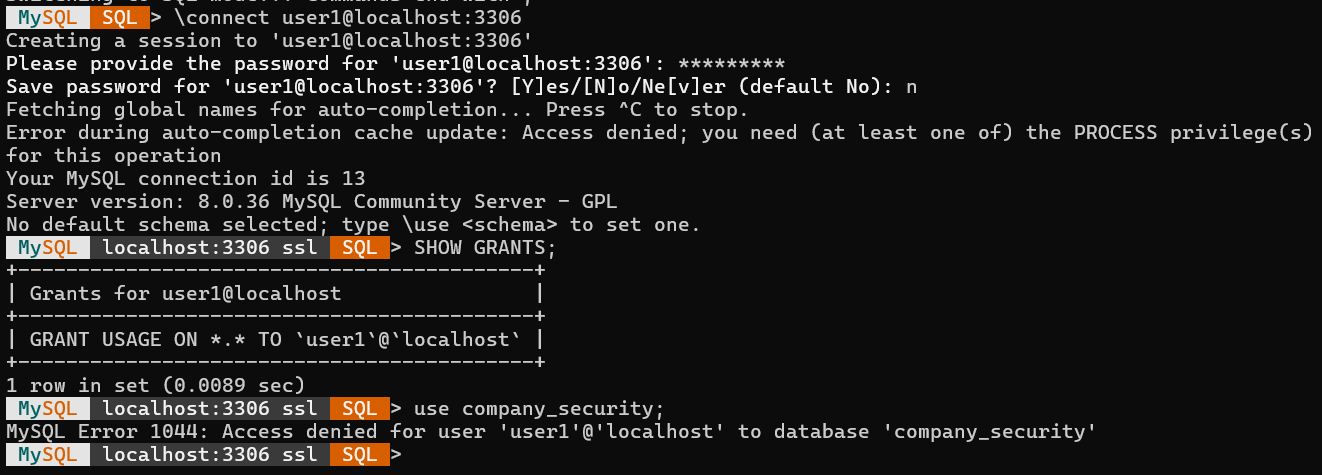
**2. Load the given company security.sql file to the company security database.**

****

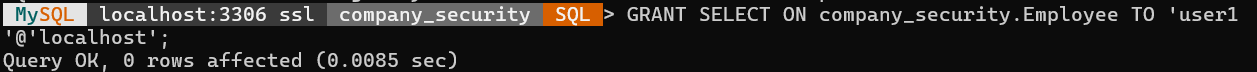
**3. Create a new user ‘user1’ within the MySQL shell.**

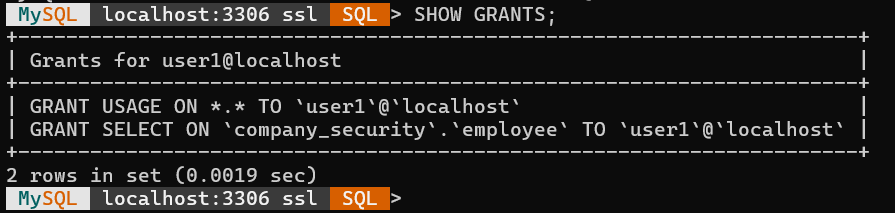
****

**4. Login to MySQL with a new user account and password and see if the new user has any authorities or privileges to the database.**

****

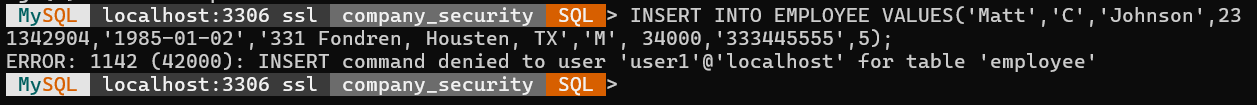
**5. Make sure the new user has only read only permission to ‘Employee’ table.**

****

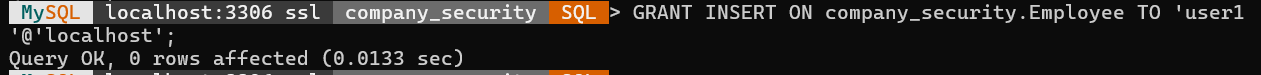
****

**6. Now allow ‘user1’ to query the followings: SELECT \* FROM Employee; INSER into Employee(...)VALUES(...). What happens? Fix the problem.**

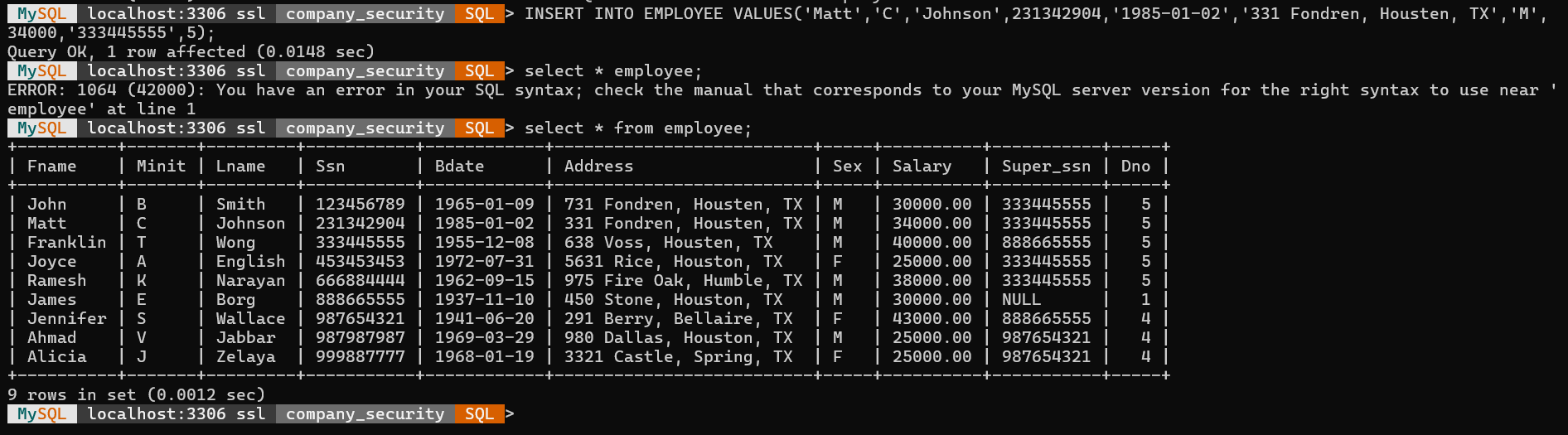
At first, insert command is denied to user1 on the database

****

Then, insert privilege is granted to user1

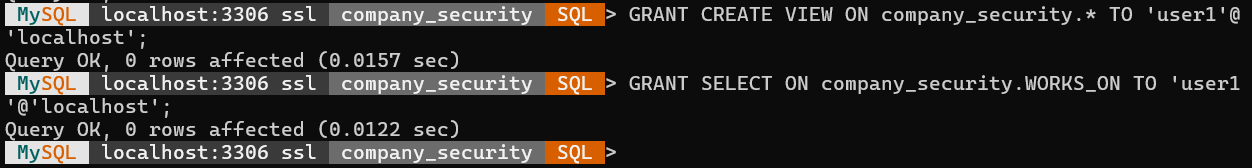
****

After that, user1 can insert into the table employee.

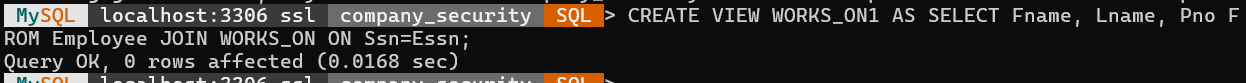


**7. From user1 create a view WORKS ON1(Fname,Lname,Pno) on EMPLOYEE and WORKS ON. (Note: You will have to give permission to user1 on CREATE VIEW). Give another user ‘user2’ permission to select tuples from WORKS ON1(Note: user2 will not be able to see WORKS ON or EMPLOYEE).**

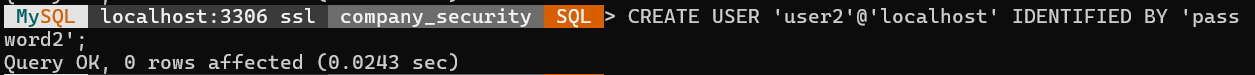
Giving permission to user1 to create views on the database and to select on WORKS\_ON table.

****

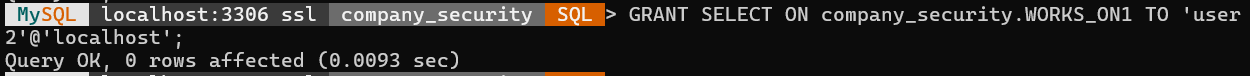
Creating the view WORKS\_ON1

****

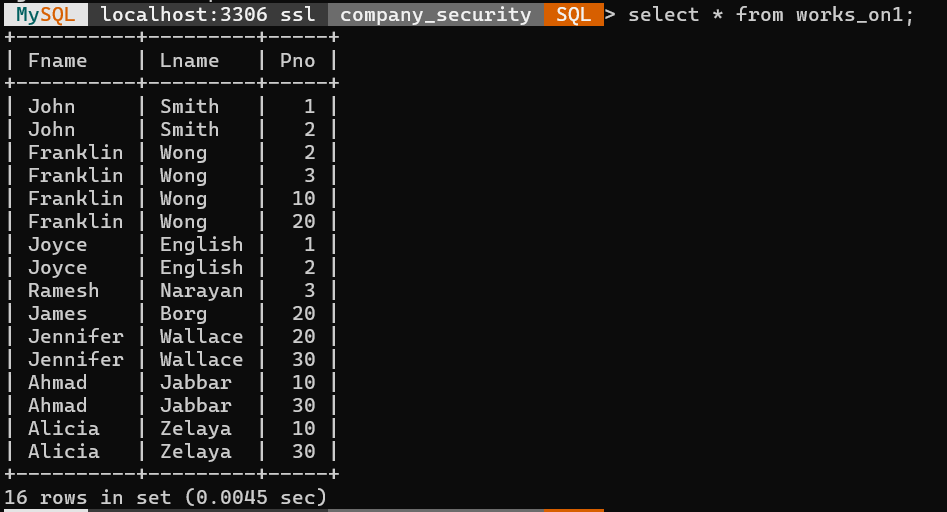
Creating a new user called “user2”

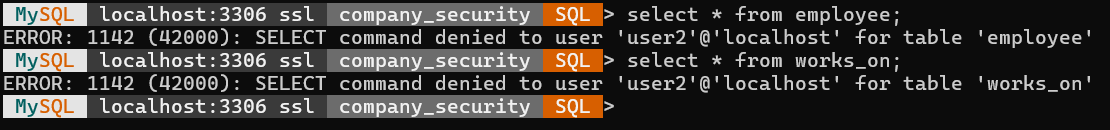
****

Granting permission to user2 on works\_on1 to SELECT.

****

**8. Select tuples from user2 account. What happens?**

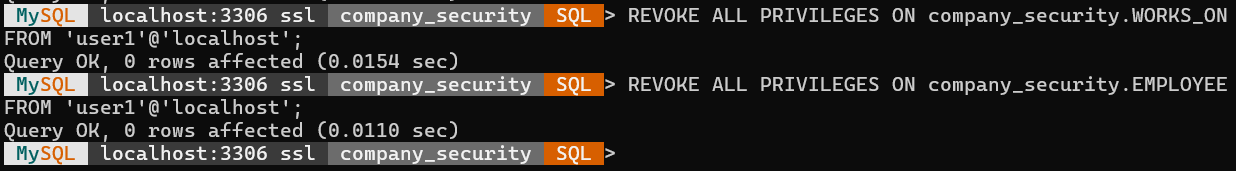
****

****

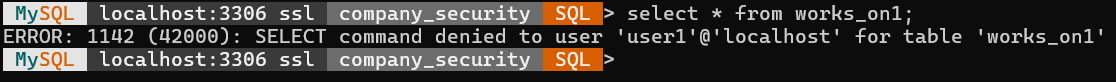
user2 can see the rows form the created view WORKS\_ON1 but he cannot see any data from the separate tables EMPLOYEE and WORKS\_ON. This is because the user2 hasn’t permission on those separate table but the created view only.

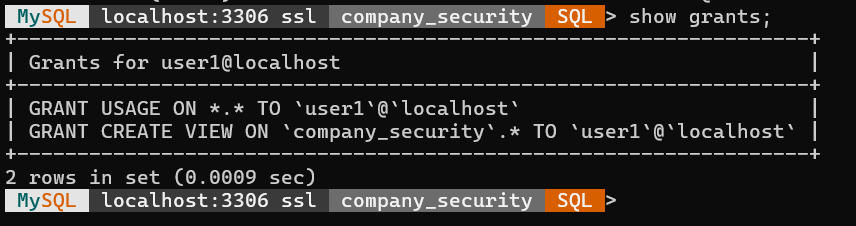
**9. Remove privileges of user1 on WORKS ON and EMPLOYEE. Can user1 still access WORKS ON1? What happened to WORKS ON1? Why?**

Removing all the permissions from user1

****

Trying to access WORKS\_ON1 view

****

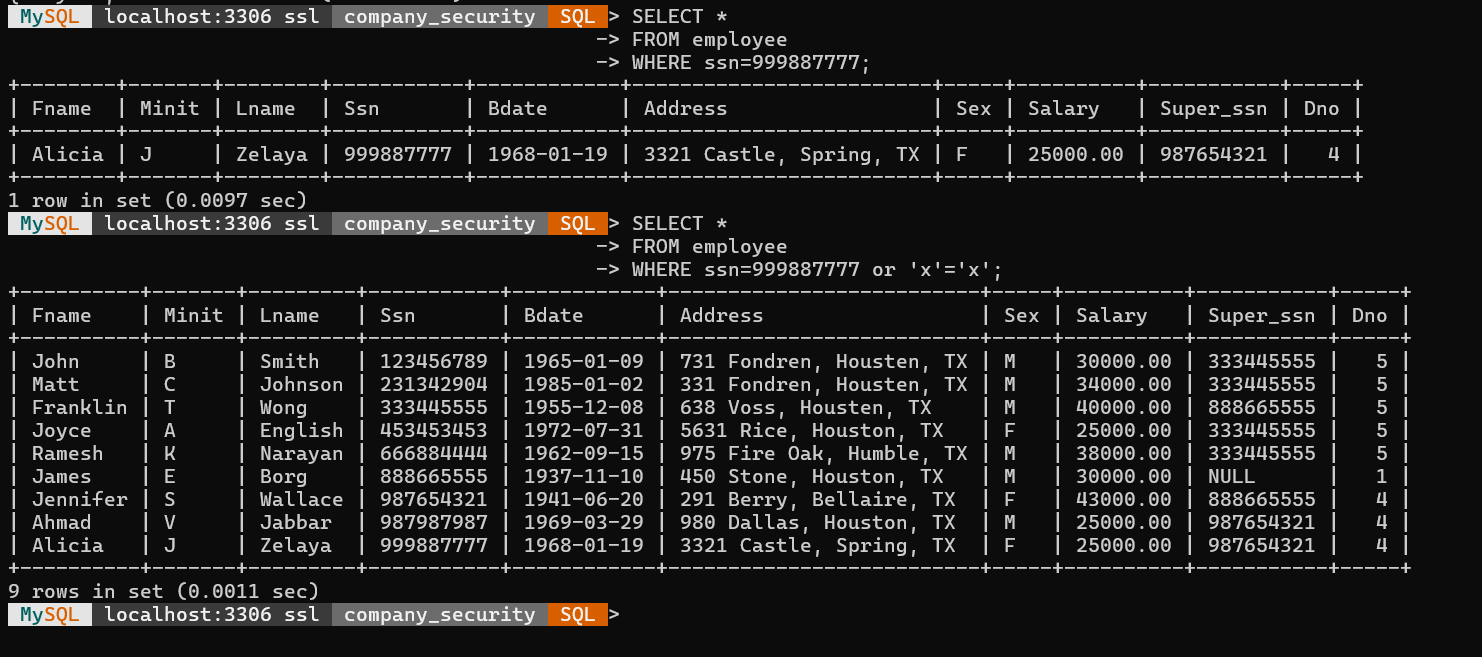
****

Since all the privileges of user1 are provoked, he doesn’t have permission to access the view WORKS\_ON1.

**SQL Injection Attacks**

**Since you do not have any authentication related tables in your database, you can try the following two queries to see what happens in an SQL injection.**

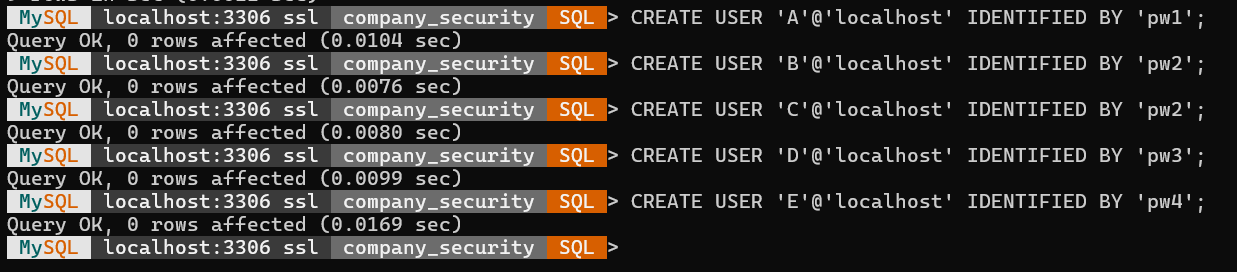
**Observe the result. What happens?**

****

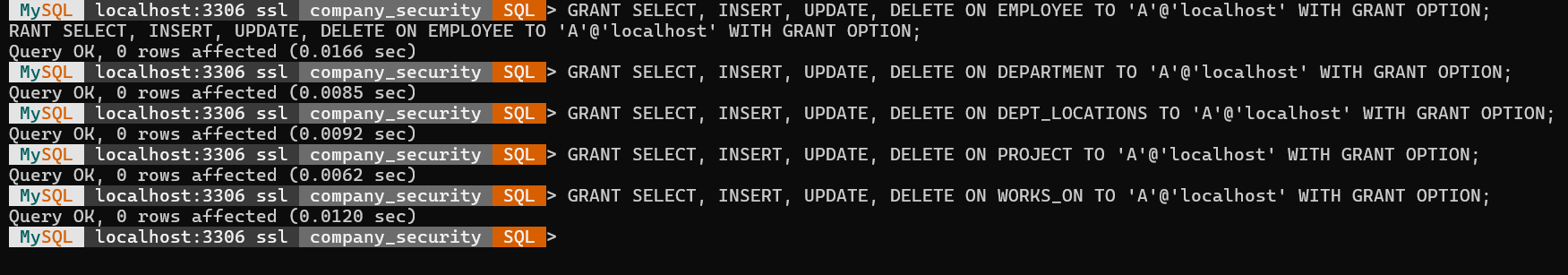
The second query exposes an SQL injection flaw by including the always-true condition 'x'='x', which retrieves all records from the employee table regardless of the SSN value.

**Assignment**

**Consider the relational database schema provided. Suppose that all the relations were created by (and hence are owned by) user X, who wants to grant the following privileges to user accounts A, B, C, D, and E:**

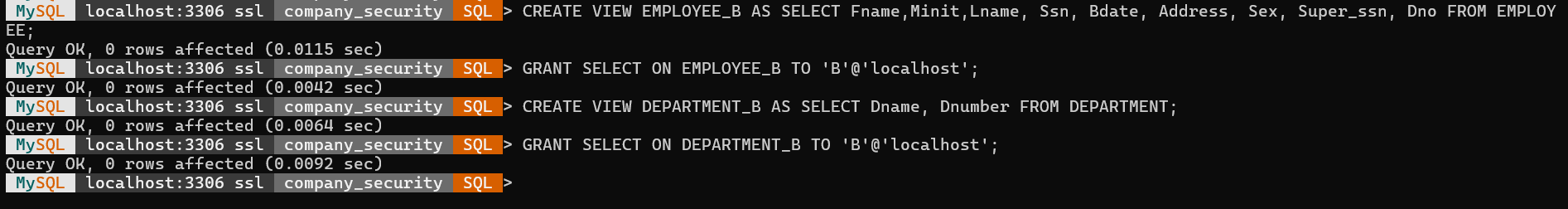
****

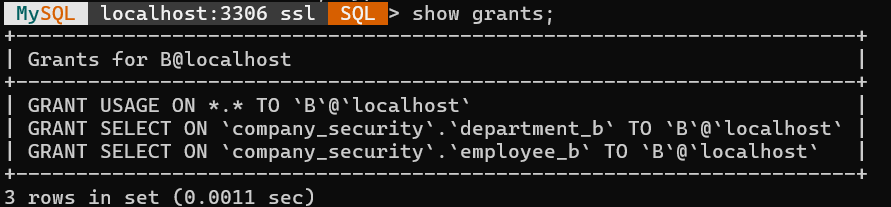
**I. Account A can retrieve or modify any relation except DEPENDENT and can grant any of these privileges to other users.**

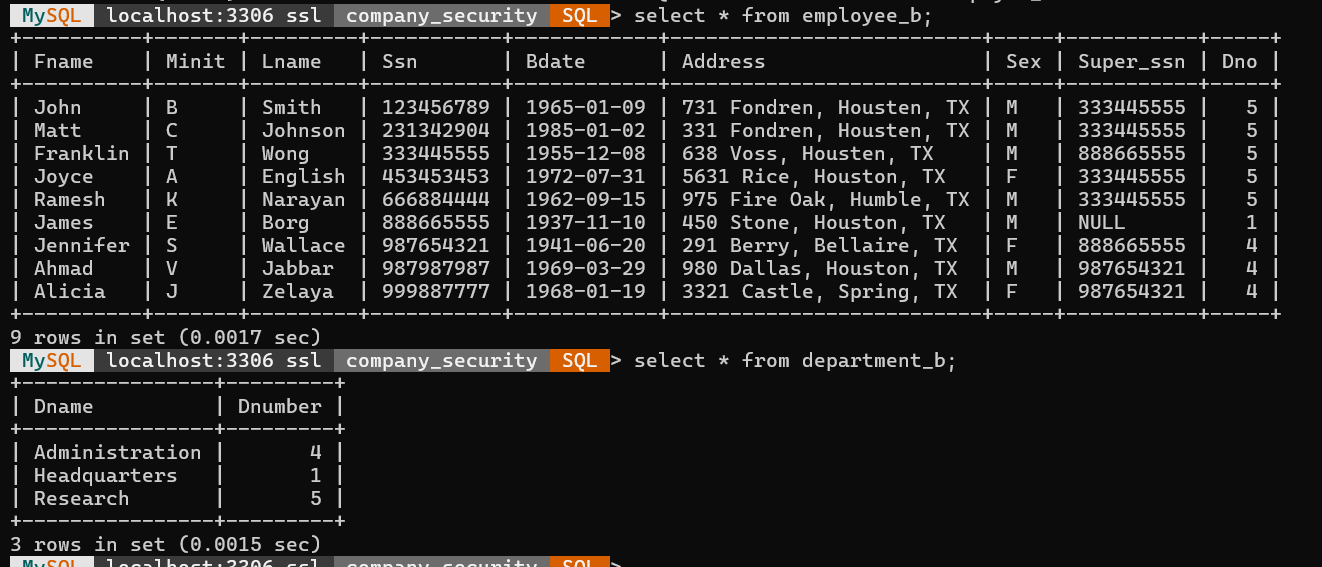
****

****

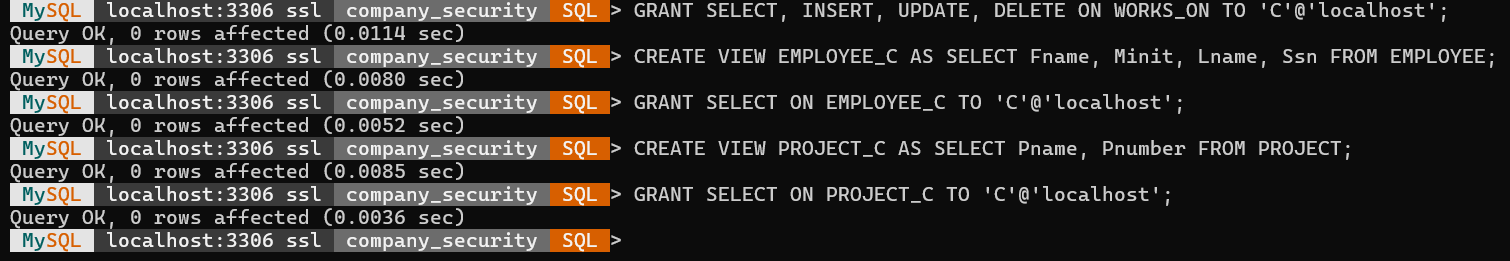
**II. Account B can retrieve all the attributes of EMPLOYEE and DEPARTMENT except for Salary, Mgr ssn, and Mgr start date.**

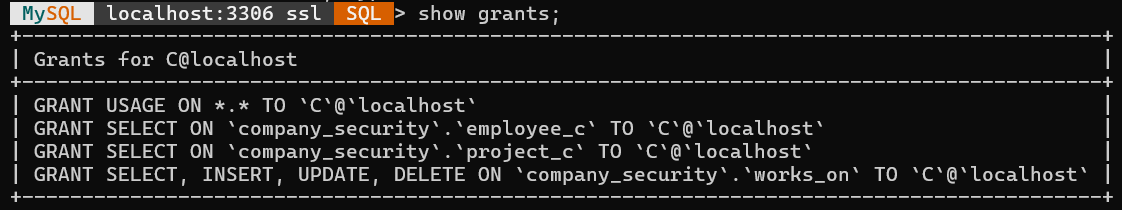
****

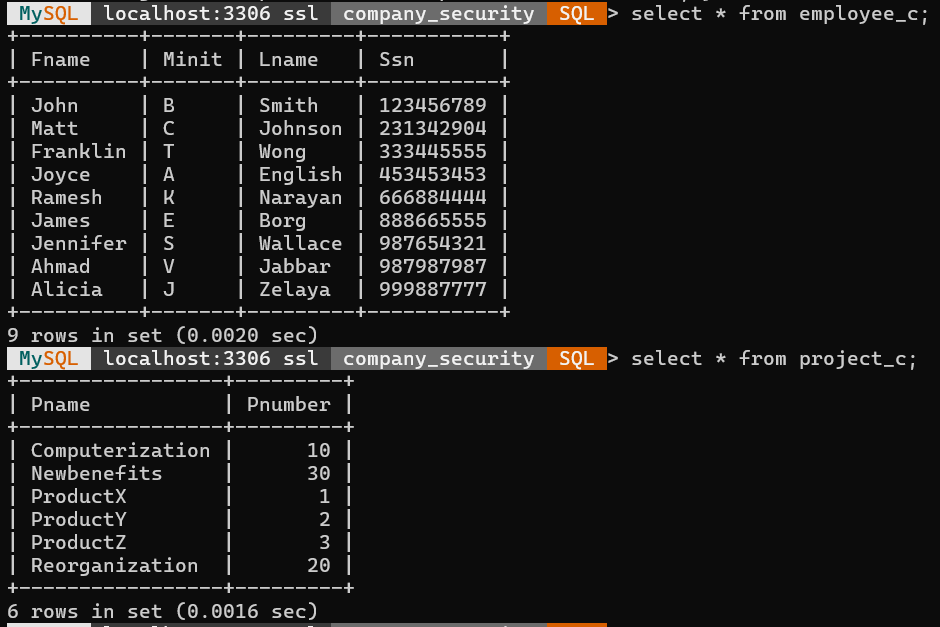
****

****

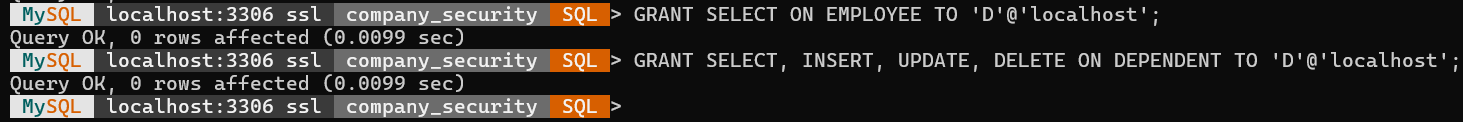
**III. Account C can retrieve or modify WORKS ON but can only retrieve the Fname, Minit, Lname, and Ssn attributes of EMPLOYEE and the Pname and Pnumber attributes of PROJECT.**

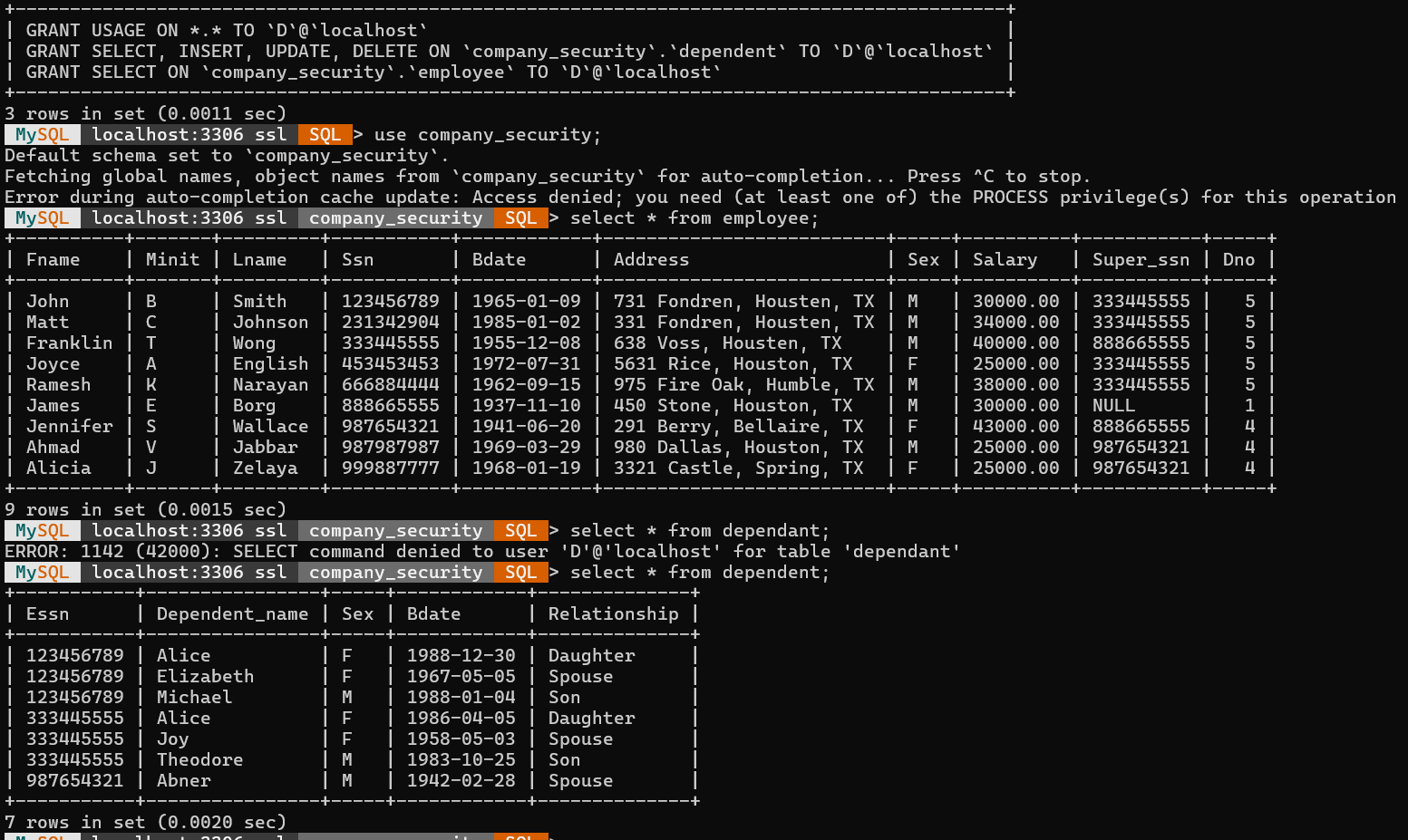
****

****

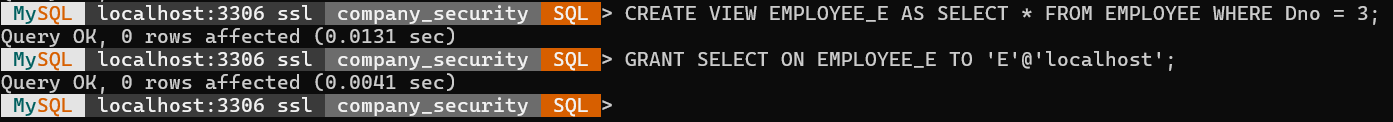
****

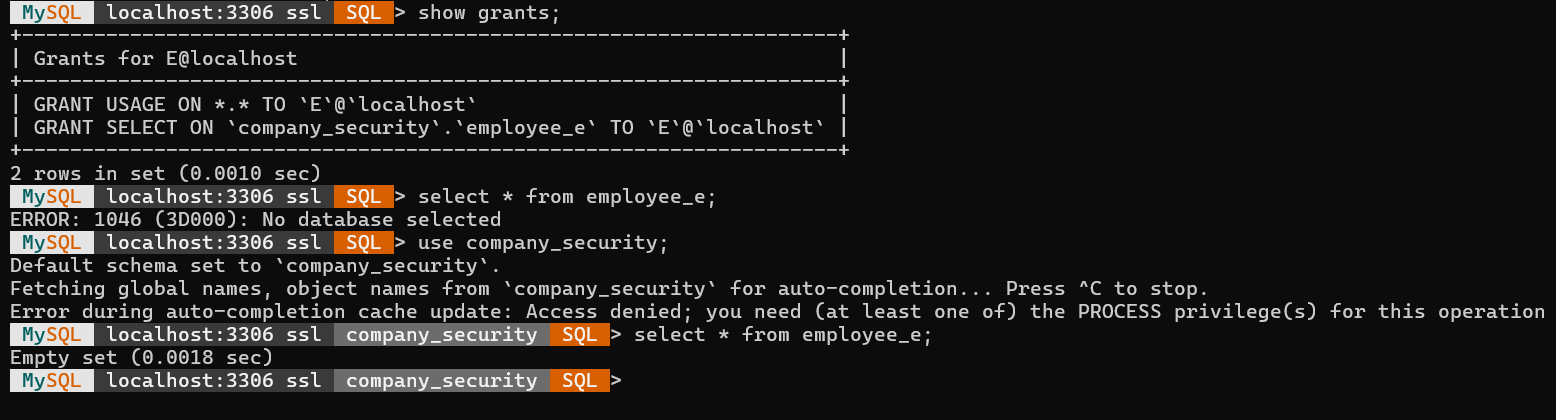
**IV. Account D can retrieve any attribute of EMPLOYEE or DEPENDENT and can modify DEPENDENT.**

****

****

**V. Account E can retrieve any attribute of EMPLOYEE but only for EMPLOYEE tuples that have Dno = 3.**

****

****