**CO527 – Advanced Database Systems**

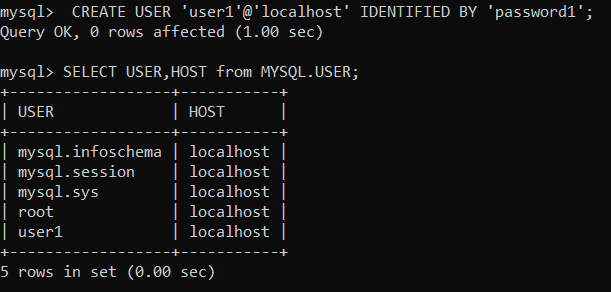
**Lab 05**

**E/17/407**

**Wijesooriya H.D**

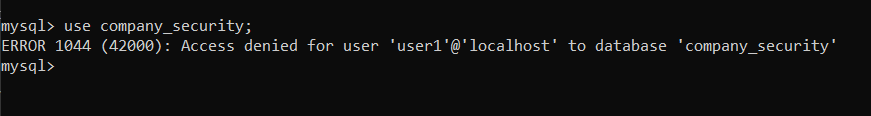
**Exercise**

**(03) Create a new user ‘user1’ within the MySQL shell.**

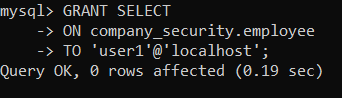
****

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

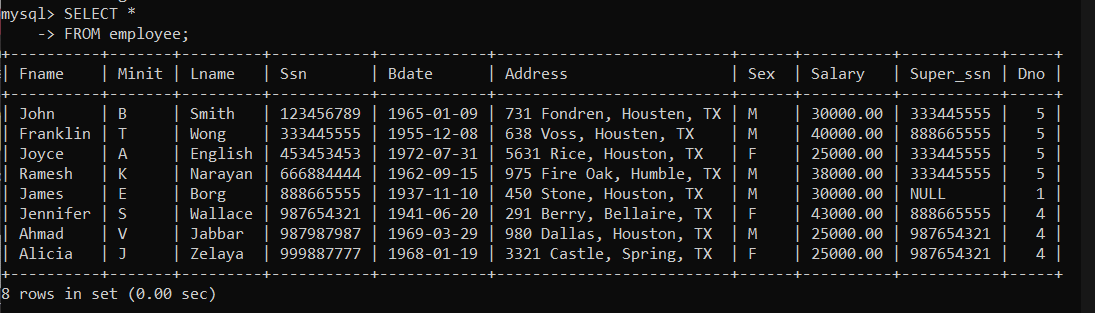
User1 was not allowed to access to the database ‘company\_security’.

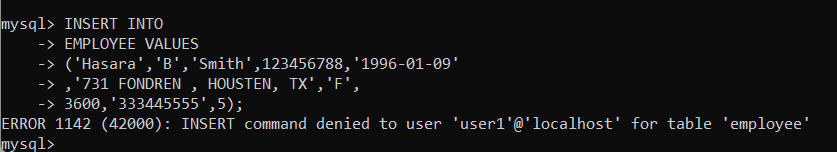


**(05) Make sure the new user has only read only permission to ‘Employee’ table.**

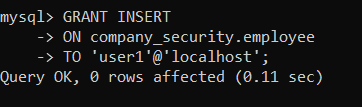
****

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

****

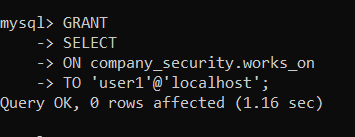
****

User 1 was not allowed to insert new records. To fix that issue we need to give write (insert) permission to user1 to employees table as shown bellow.

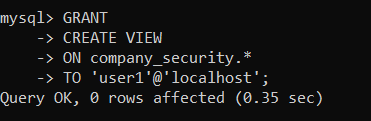
****

**(07) 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).**

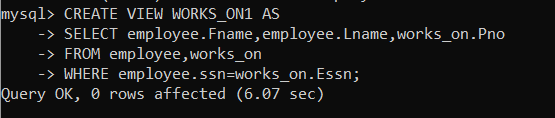
* Giving read only permission to user1 on works\_on table.

****

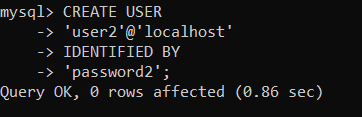
* Giving permission to user1 on CREATE VIEW.

****

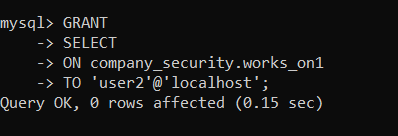
* Creating the view works\_on1.

****

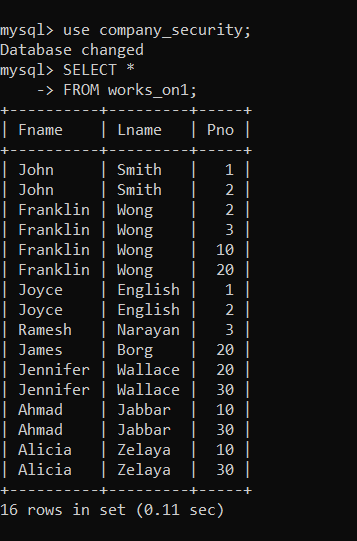
* Creating a new user ‘user2’

****

* Giving permission to user2 to select tuples from the view ‘works\_on1’

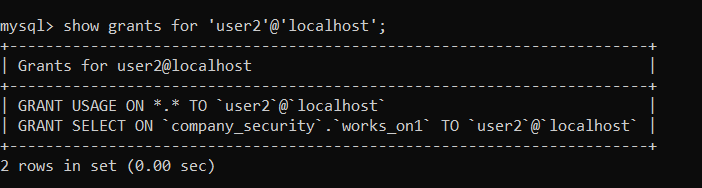
****

**(08) Select tuples from user2 account. What happens?**

****

User2 was able to see all the records in the view ‘works\_on1’. because user2 was given read only permission on that view.

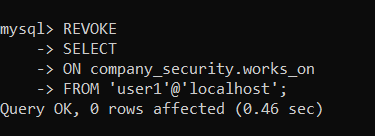
* Grants related to user2

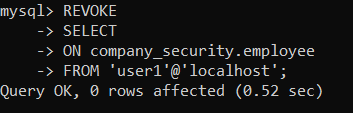
****

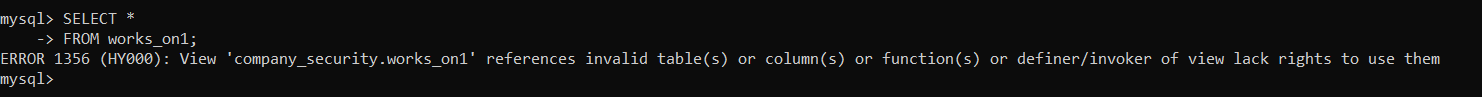
**(09)**

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

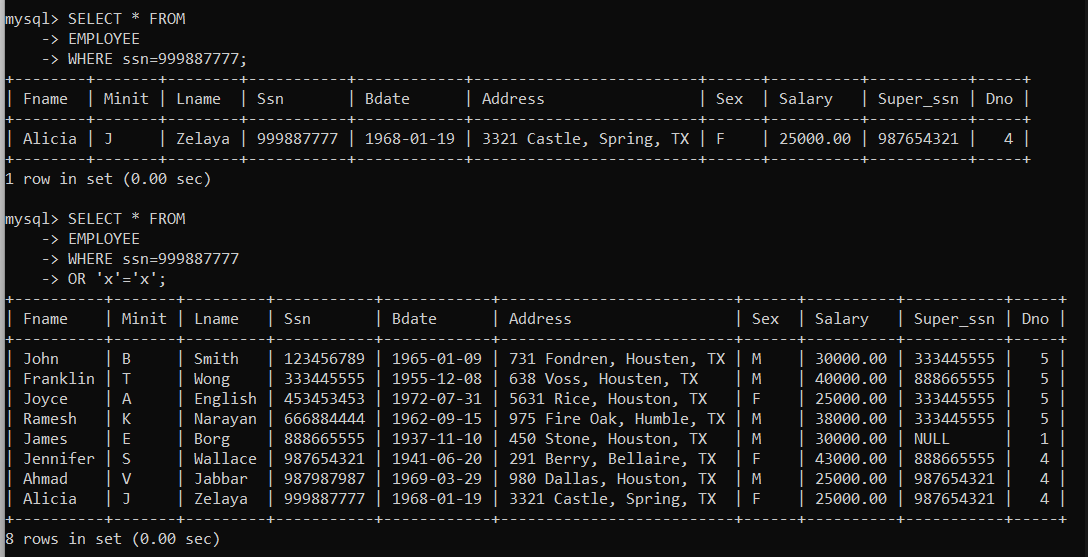
User1 was not able to access to the view ‘WORKS\_ON1’ . Because the user1 did not have read permissions on the tables which are related to the view.

****



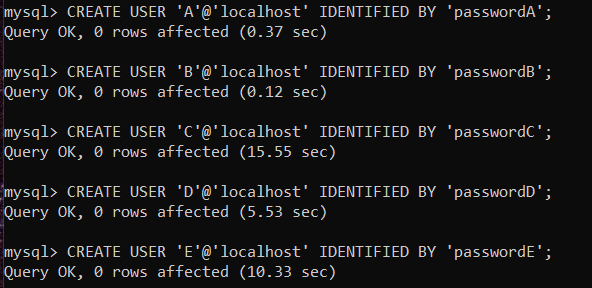


**SQL INJECTION ATTCK**



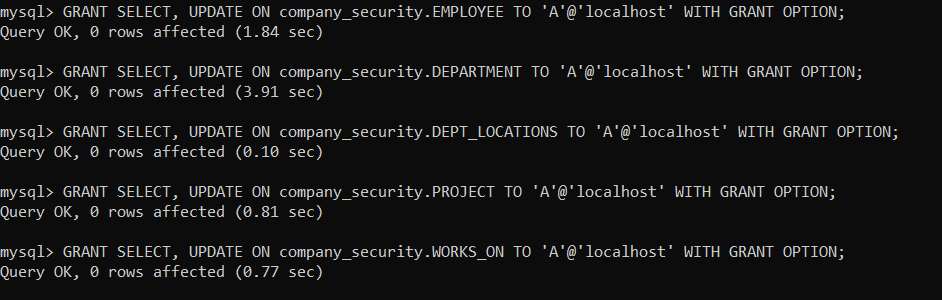
The attacker was able to see all the records of the table ‘EMPLOYEE’. This SQL injection attack occurs when data from the user is used to modify a SQL statement.

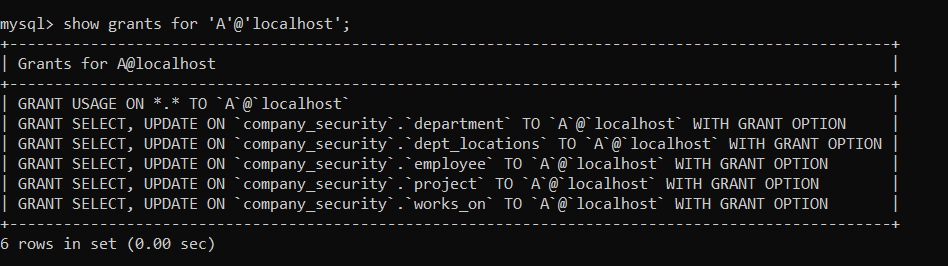
**Assignment**

****

**(i)**

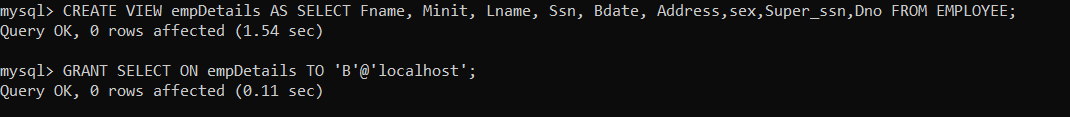
**Account A can retrieve or modify any relation except DEPENDENT and can grant any of these privileges to other users.**

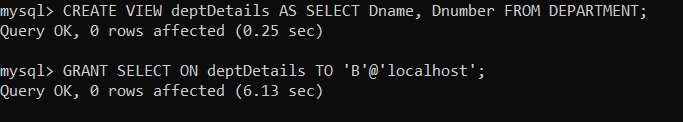
****

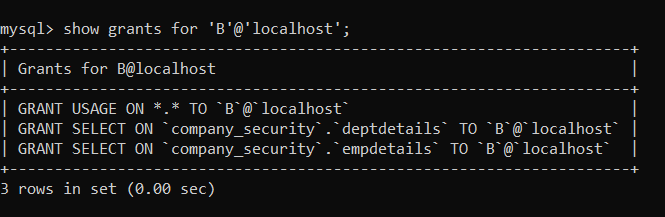
****

**(ii)**

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

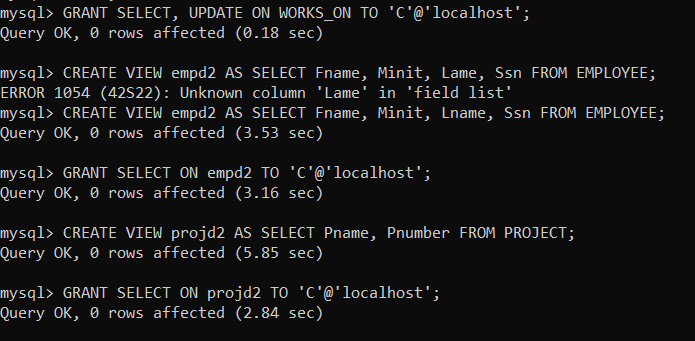
****

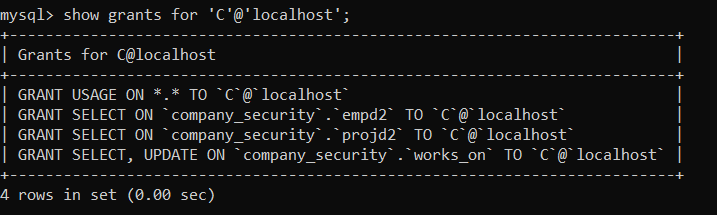
****

****

**(iii)**

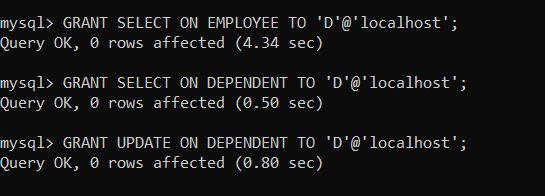
**Account C can retrieve or modify WORKS ON but can only retrieve the Fname, Minit, Lname, and Ssn attributes of EMPLOYEE and the Pname and Pnumber attributes of PROJECT.**

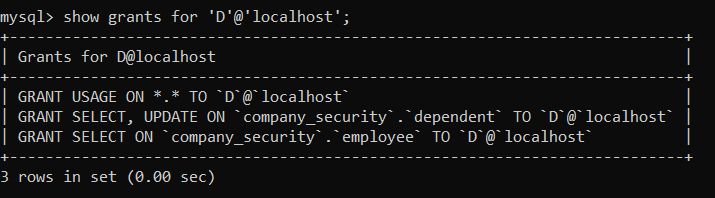
****

****

**(iv)**

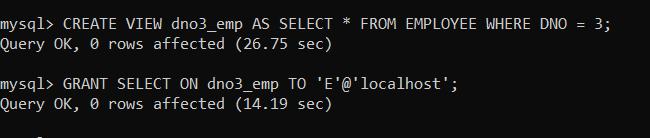
**Account D can retrieve any attribute of EMPLOYEE or DEPENDENT and can modify DEPENDENT.**

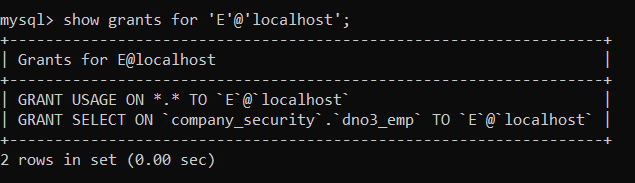
****

****

**(v)**

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

****

****