CO527 – Advanced Database Systems

Lab 05 – Database Security

Karunachandra R.H.I.O.

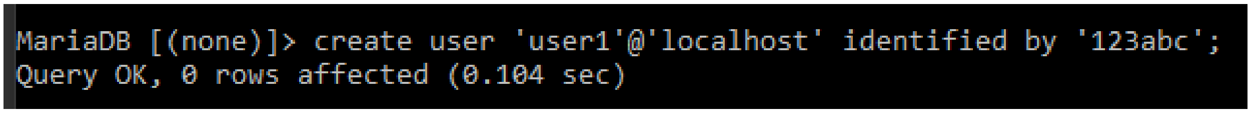
E/17/153

4.Exercise

1.Create database company security

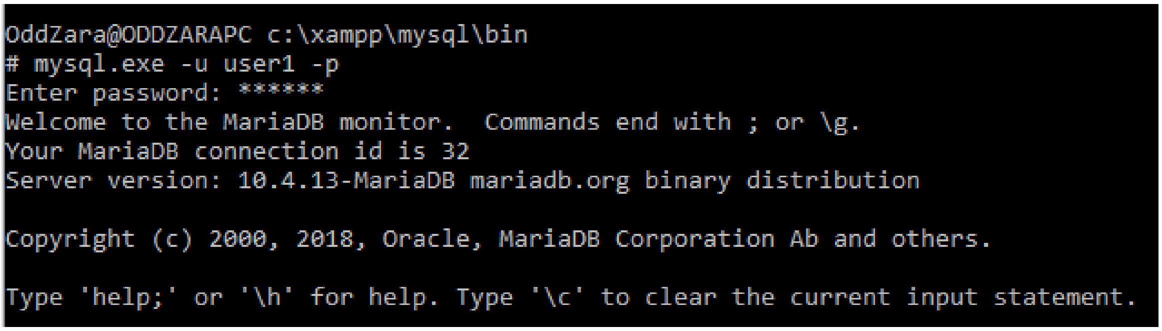
2.Load the given company security.sql file to the company security database.

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

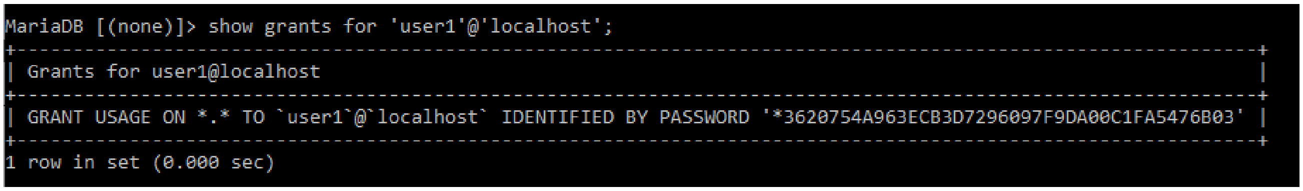


```
MariaDB [(none)]> create user 'user1'@'localhost' identified by '123abc';
Query OK, 0 rows affected (0.104 sec)
```

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

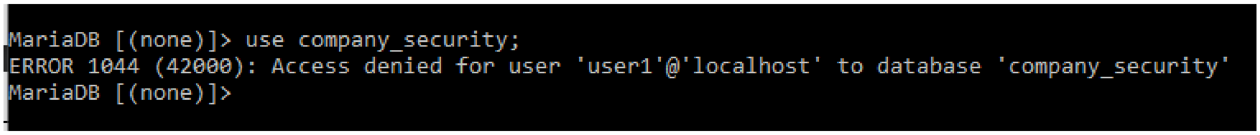


```
OddZara@ODDZARAPC c:\xampp\mysql\bin
# mysql.exe -u user1 -p
Enter password: ******
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 32
Server version: 10.4.13-MariaDB mariadb.org binary distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```



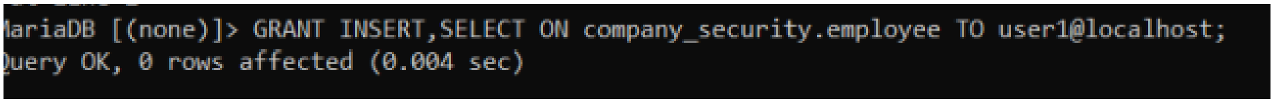
```
MariaDB [(none)]> show grants for 'user1'@'localhost';
+--------------------------------------------------------------------------------------------------------------+
| Grants for user1@localhost                                                                                   |
+--------------------------------------------------------------------------------------------------------------+
| GRANT USAGE ON *.* TO `user1`@`localhost` IDENTIFIED BY PASSWORD '*3620754A963ECB3D7296097F9DA00C1FA5476B03' |
+--------------------------------------------------------------------------------------------------------------+
1 row in set (0.000 sec)
```

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



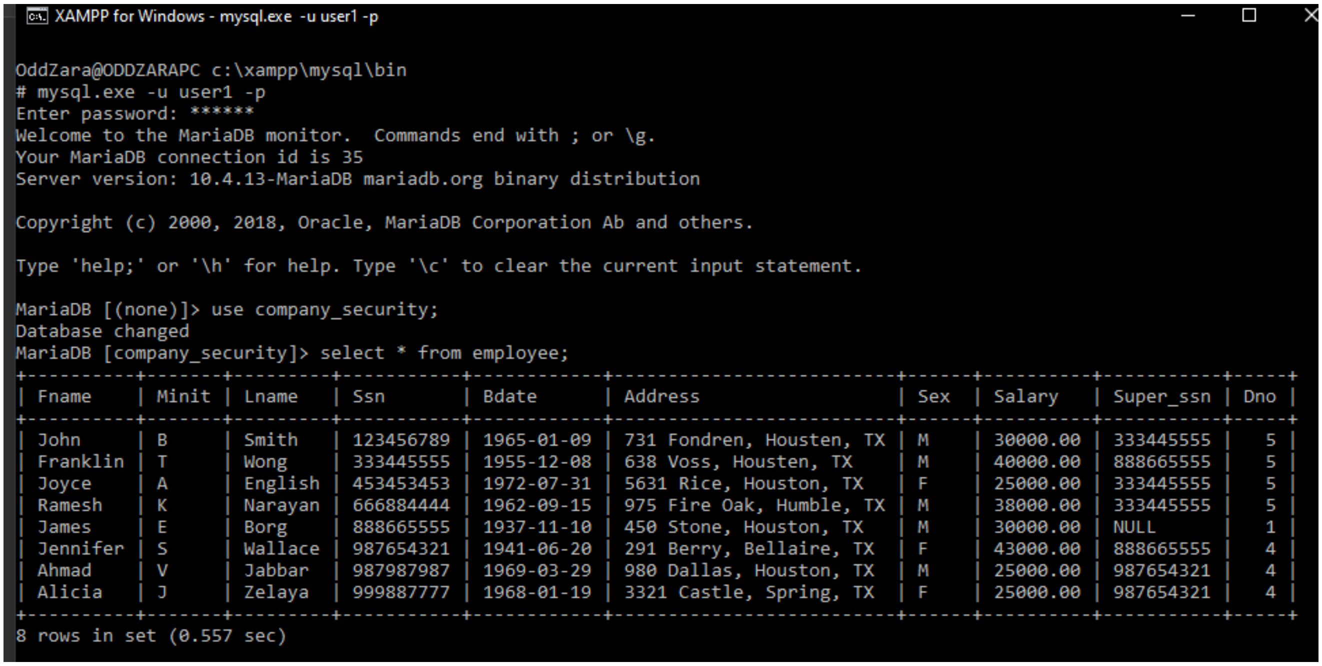
```
MariaDB [(none)]> use company_security;
ERROR 1044 (42000): Access denied for user 'user1'@'localhost' to database 'company_security'
MariaDB [(none)]>
```

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



```
lariaDB [(none)]> GRANT INSERT,SELECT ON company_security.employee TO user1@localhost;
uery OK, 0 rows affected (0.004 sec)
```

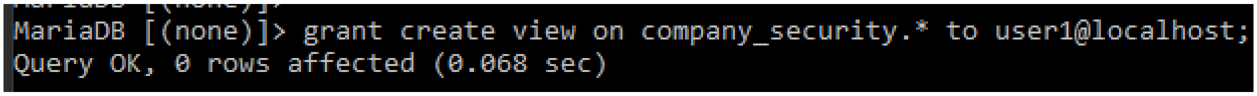
Now user1 can use the database.



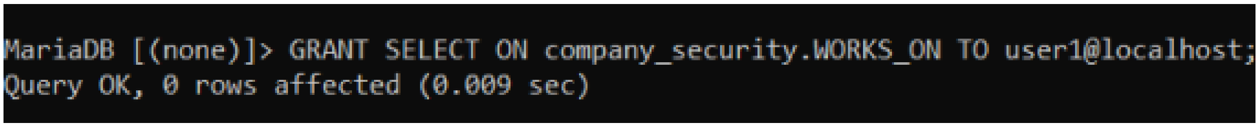
```
OddZara@ODDZARAPC c:\xampp\mysql\bin
# mysql.exe -u user1 -p
Enter password: ******
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 35
Server version: 10.4.13-MariaDB mariadb.org binary distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> use company_security;
Database changed
MariaDB [company_security]> select * from employee;
+----------+-------+---------+-----------+------------+--------------------------+------+----------+-----------+-----+
| Fname    | Minit | Lname   | Ssn       | Bdate      | Address                  | Sex  | Salary   | Super_ssn | Dno |
+----------+-------+---------+-----------+------------+--------------------------+------+----------+-----------+-----+
| John     | B     | Smith   | 123456789 | 1965-01-09 | 731 Fondren, Housten, TX | M    | 30000.00 | 333445555 |   5 |
| Franklin | T     | Wong    | 333445555 | 1955-12-08 | 638 Voss, Housten, TX    | M    | 40000.00 | 888665555 |   5 |
| Joyce    | A     | English | 453453453 | 1972-07-31 | 5631 Rice, Houston, TX   | F    | 25000.00 | 333445555 |   5 |
| Ramesh   | K     | Narayan | 666884444 | 1962-09-15 | 975 Fire Oak, Humble, TX | M    | 38000.00 | 333445555 |   5 |
| James    | E     | Borg    | 888665555 | 1937-11-10 | 450 Stone, Houston, TX   | M    | 30000.00 | NULL      |   1 |
| Jennifer | S     | Wallace | 987654321 | 1941-06-20 | 291 Berry, Bellaire, TX  | F    | 43000.00 | 888665555 |   4 |
| Ahmad    | V     | Jabbar  | 987987987 | 1969-03-29 | 980 Dallas, Houston, TX  | M    | 25000.00 | 987654321 |   4 |
| Alicia   | J     | Zelaya  | 999887777 | 1968-01-19 | 3321 Castle, Spring, TX  | F    | 25000.00 | 987654321 |   4 |
+----------+-------+---------+-----------+------------+--------------------------+------+----------+-----------+-----+
8 rows in set (0.557 sec)
```

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

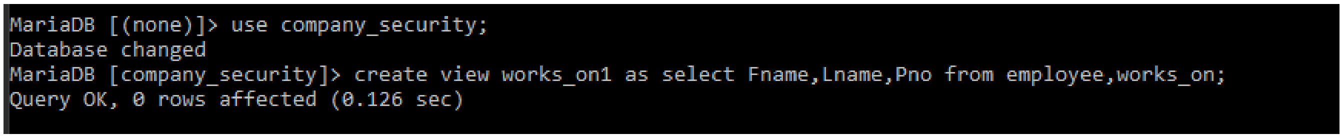


```
MariaDB [(none)]> grant create view on company_security.* to user1@localhost;
Query OK, 0 rows affected (0.068 sec)
```



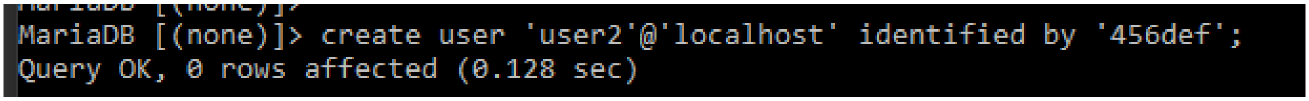
```
MariaDB [(none)]> GRANT SELECT ON company_security.WORKS_ON TO user1@localhost;
Query OK, 0 rows affected (0.009 sec)
```

Creating a view from user1

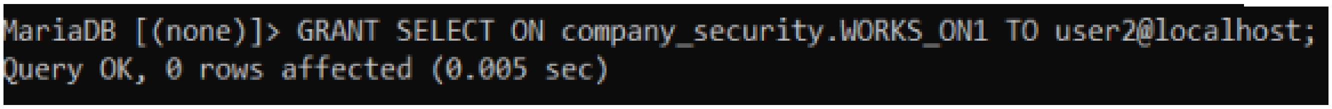


```
MariaDB [(none)]> use company_security;
Database changed
MariaDB [company_security]> create view works_on1 as select Fname,Lname,Pno from employee,works_on;
Query OK, 0 rows affected (0.126 sec)
```

Creating user2 and giving permissions

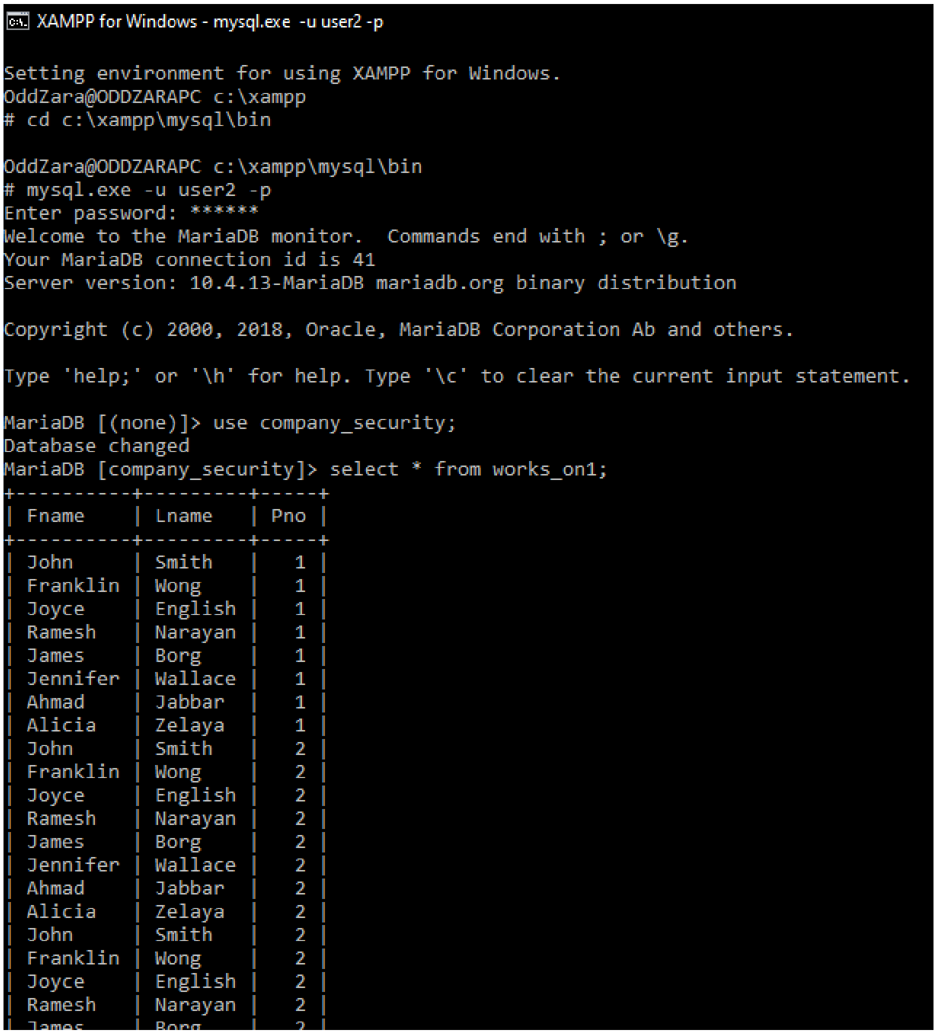


```
MariaDB [(none)]> create user 'user2'@'localhost' identified by '456def';
Query OK, 0 rows affected (0.128 sec)
```



```
MariaDB [(none)]> GRANT SELECT ON company_security.WORKS_ON1 TO user2@localhost;
Query OK, 0 rows affected (0.005 sec)
```

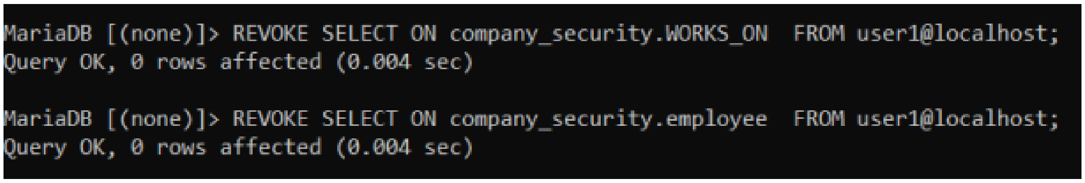
8. Select tuples from user2 account. What happens?



XAMPP for Windows - mysql.exe -u user2 -p

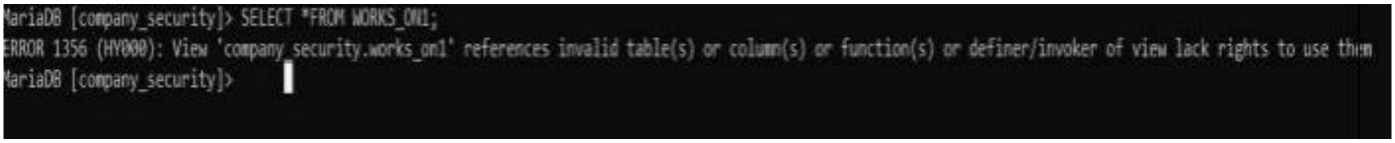
```
Setting environment for using XAMPP for Windows.
OddZara@ODDZARAPC c:\xampp
# cd c:\xampp\mysql\bin

OddZara@ODDZARAPC c:\xampp\mysql\bin
# mysql.exe -u user2 -p
Enter password: ******
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 41
Server version: 10.4.13-MariaDB mariadb.org binary distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> use company_security;
Database changed
MariaDB [company_security]> select * from works_on1;
+----------+---------+-----+
| Fname    | Lname   | Pno |
+----------+---------+-----+
| John     | Smith   |   1 |
| Franklin | Wong    |   1 |
| Joyce    | English |   1 |
| Ramesh   | Narayan |   1 |
| James    | Borg    |   1 |
| Jennifer | Wallace |   1 |
| Ahmad    | Jabbar  |   1 |
| Alicia   | Zelaya  |   1 |
| John     | Smith   |   2 |
| Franklin | Wong    |   2 |
| Joyce    | English |   2 |
| Ramesh   | Narayan |   2 |
| James    | Borg    |   2 |
| Jennifer | Wallace |   2 |
| Ahmad    | Jabbar  |   2 |
| Alicia   | Zelaya  |   2 |
| John     | Smith   |   2 |
| Franklin | Wong    |   2 |
| Joyce    | English |   2 |
| Ramesh   | Narayan |   2 |
| James    | Borg    |   2 |
```

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



```
MariaDB [(none)]> REVOKE SELECT ON company_security.WORKS_ON  FROM user1@localhost;
Query OK, 0 rows affected (0.004 sec)

MariaDB [(none)]> REVOKE SELECT ON company_security.employee  FROM user1@localhost;
Query OK, 0 rows affected (0.004 sec)
```

After revoking the permissions on works_on and employee table user1 cannot view the WORKS_ON1 view as it references to the tables that user1 doesn't have access

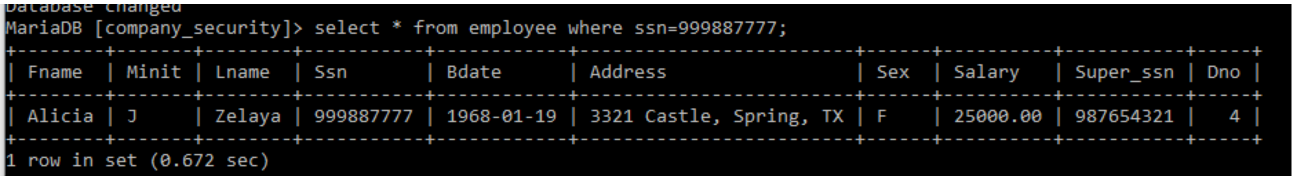


```
MariaDB [company_security]> SELECT *FROM WORKS_ON1;
ERROR 1356 (HY000): View 'company_security.works_on1' references invalid table(s) or column(s) or function(s) or definer/invoker of view lack rights to use them
MariaDB [company_security]>
```

10.Try the following two queries to see what happens in an SQL injection

Query 1:

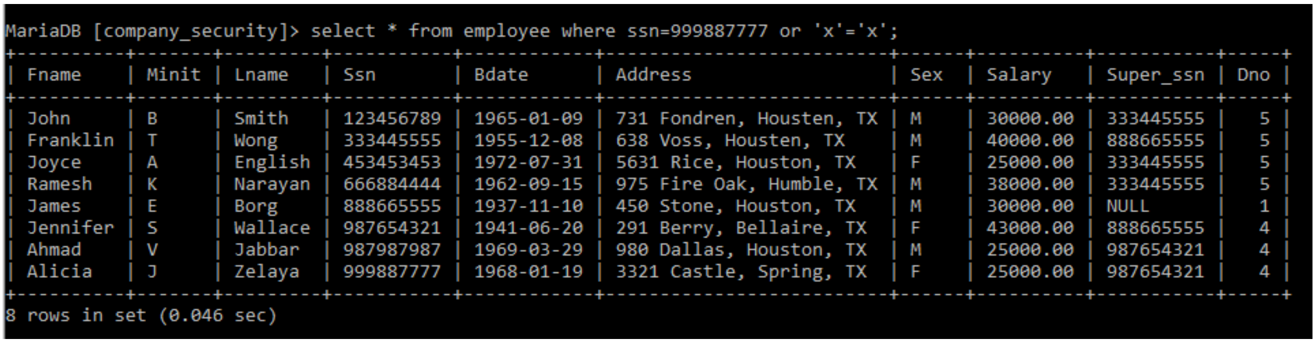
SELECT * FROM employee WHERE ssn=999887777;



```
Database changed
MariaDB [company_security]> select * from employee where ssn=999887777;
+--------+-------+--------+-----------+------------+-------------------------+------+----------+-----------+-----+
| Fname  | Minit | Lname  | Ssn       | Bdate      | Address                 | Sex  | Salary   | Super_ssn | Dno |
+--------+-------+--------+-----------+------------+-------------------------+------+----------+-----------+-----+
| Alicia | J     | Zelaya | 999887777 | 1968-01-19 | 3321 Castle, Spring, TX | F    | 25000.00 | 987654321 |   4 |
+--------+-------+--------+-----------+------------+-------------------------+------+----------+-----------+-----+
1 row in set (0.672 sec)
```

Query 2:

SELECT * FROM employee WHERE ssn=999887777 or ’x’=’x’;



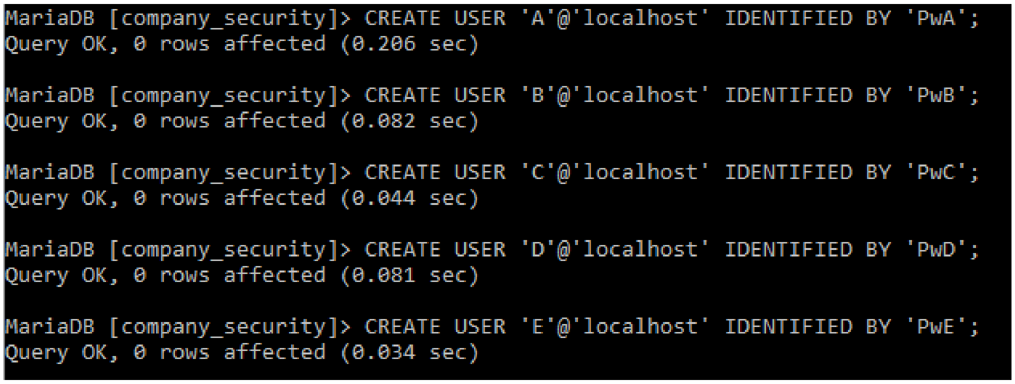
```
MariaDB [company_security]> select * from employee where ssn=999887777 or 'x'='x';
+----------+-------+---------+-----------+------------+--------------------------+------+----------+-----------+-----+
| Fname    | Minit | Lname   | Ssn       | Bdate      | Address                  | Sex  | Salary   | Super_ssn | Dno |
+----------+-------+---------+-----------+------------+--------------------------+------+----------+-----------+-----+
| John     | B     | Smith   | 123456789 | 1965-01-09 | 731 Fondren, Housten, TX | M    | 30000.00 | 333445555 |   5 |
| Franklin | T     | Wong    | 333445555 | 1955-12-08 | 638 Voss, Housten, TX    | M    | 40000.00 | 888665555 |   5 |
| Joyce    | A     | English | 453453453 | 1972-07-31 | 5631 Rice, Houston, TX   | F    | 25000.00 | 333445555 |   5 |
| Ramesh   | K     | Narayan | 666884444 | 1962-09-15 | 975 Fire Oak, Humble, TX | M    | 38000.00 | 333445555 |   5 |
| James    | E     | Borg    | 888665555 | 1937-11-10 | 450 Stone, Houston, TX   | M    | 30000.00 | NULL      |   1 |
| Jennifer | S     | Wallace | 987654321 | 1941-06-20 | 291 Berry, Bellaire, TX  | F    | 43000.00 | 888665555 |   4 |
| Ahmad    | V     | Jabbar  | 987987987 | 1969-03-29 | 980 Dallas, Houston, TX  | M    | 25000.00 | 987654321 |   4 |
| Alicia   | J     | Zelaya  | 999887777 | 1968-01-19 | 3321 Castle, Spring, TX  | F    | 25000.00 | 987654321 |   4 |
+----------+-------+---------+-----------+------------+--------------------------+------+----------+-----------+-----+
8 rows in set (0.046 sec)
```

Query 1 outputs only the details of employee who has ssn=999887777.

Query 2 outputs details of all employees. This conveys that the attacker who knows there is a valid login for ssn=999887777 can login to the database system as an authorized user without knowing his password and is able to do everything that who has ssn=999887777 may be authorized to do to the database system.

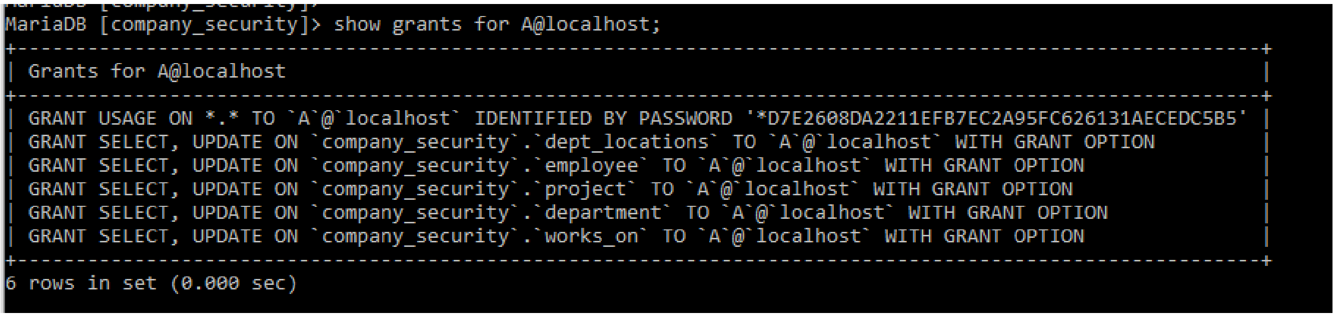
5.Assignment

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:



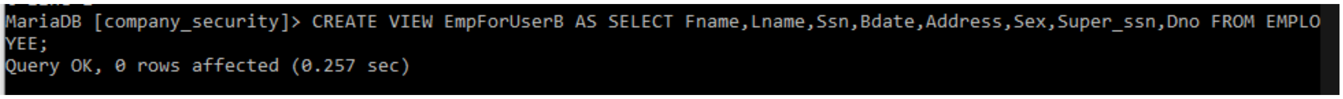
```
MariaDB [company_security]> CREATE USER 'A'@'localhost' IDENTIFIED BY 'PwA';
Query OK, 0 rows affected (0.206 sec)

MariaDB [company_security]> CREATE USER 'B'@'localhost' IDENTIFIED BY 'PwB';
Query OK, 0 rows affected (0.082 sec)

MariaDB [company_security]> CREATE USER 'C'@'localhost' IDENTIFIED BY 'PwC';
Query OK, 0 rows affected (0.044 sec)

MariaDB [company_security]> CREATE USER 'D'@'localhost' IDENTIFIED BY 'PwD';
Query OK, 0 rows affected (0.081 sec)

MariaDB [company_security]> CREATE USER 'E'@'localhost' IDENTIFIED BY 'PwE';
Query OK, 0 rows affected (0.034 sec)
```

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

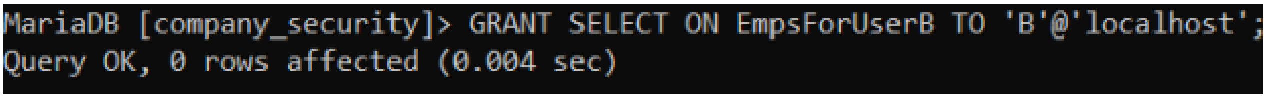


```
MariaDB [company_security]> show grants for A@localhost;
+-------------------------------------------------------------------------------------------------------+
| Grants for A@localhost                                                                                |
+-------------------------------------------------------------------------------------------------------+
| GRANT USAGE ON *.* TO `A`@`localhost` IDENTIFIED BY PASSWORD '*D7E2608DA2211EFB7EC2A95FC626131AECEDC5B5' |
| GRANT SELECT, UPDATE ON `company_security`.`dept_locations` TO `A`@`localhost` WITH GRANT OPTION      |
| GRANT SELECT, UPDATE ON `company_security`.`employee` TO `A`@`localhost` WITH GRANT OPTION            |
| GRANT SELECT, UPDATE ON `company_security`.`project` TO `A`@`localhost` WITH GRANT OPTION             |
| GRANT SELECT, UPDATE ON `company_security`.`department` TO `A`@`localhost` WITH GRANT OPTION          |
| GRANT SELECT, UPDATE ON `company_security`.`works_on` TO `A`@`localhost` WITH GRANT OPTION            |
+-------------------------------------------------------------------------------------------------------+
6 rows in set (0.000 sec)
```

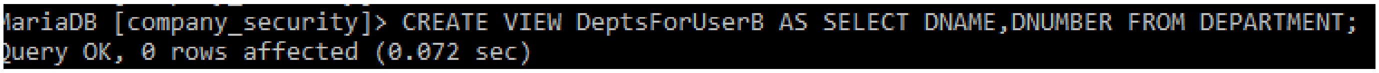
II. Account B can retrieve all the attributes of EMPLOYEE and DEPARTMENT except for Salary, Mgr ssn, and Mgr start date.



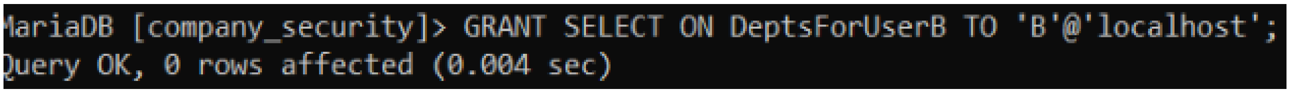
```
MariaDB [company_security]> CREATE VIEW EmpForUserB AS SELECT Fname,Lname,Ssn,Bdate,Address,Sex,Super_ssn,Dno FROM EMPLO
YEE;
Query OK, 0 rows affected (0.257 sec)
```



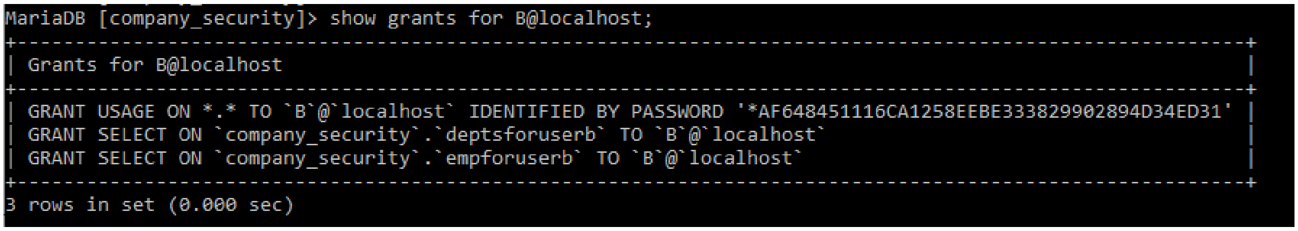
```
MariaDB [company_security]> GRANT SELECT ON EmpsForUserB TO 'B'@'localhost';
Query OK, 0 rows affected (0.004 sec)
```



```
MariaDB [company_security]> CREATE VIEW DeptsForUserB AS SELECT DNAME,DNUMBER FROM DEPARTMENT;
Query OK, 0 rows affected (0.072 sec)
```

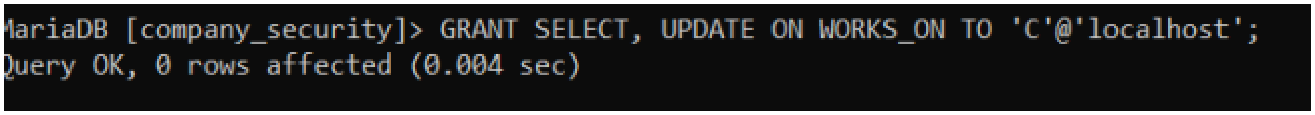


```
MariaDB [company_security]> GRANT SELECT ON DeptsForUserB TO 'B'@'localhost';
Query OK, 0 rows affected (0.004 sec)
```

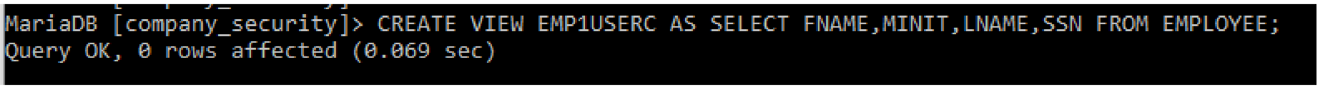


```
MariaDB [company_security]> show grants for B@localhost;
+-------------------------------------------------------------------------------------------------------+
| Grants for B@localhost                                                                                |
+-------------------------------------------------------------------------------------------------------+
| GRANT USAGE ON *.* TO `B`@`localhost` IDENTIFIED BY PASSWORD '*AF648451116CA1258EEBE333829902894D34ED31' |
| GRANT SELECT ON `company_security`.`deptsforuserb` TO `B`@`localhost`                                 |
| GRANT SELECT ON `company_security`.`empforuserb` TO `B`@`localhost`                                   |
+-------------------------------------------------------------------------------------------------------+
3 rows in set (0.000 sec)
```

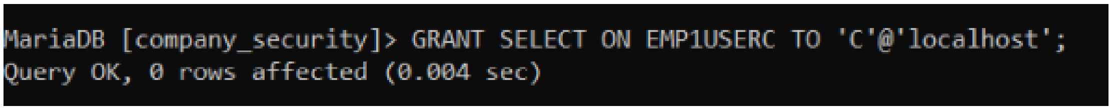
III. Account C can retrieve or modify WORKS ON but can only retrieve the Fname, Minit, Lname, and Ssn attributes of EMPLOYEE and the Pname and Pnumber attributes of PROJECT.



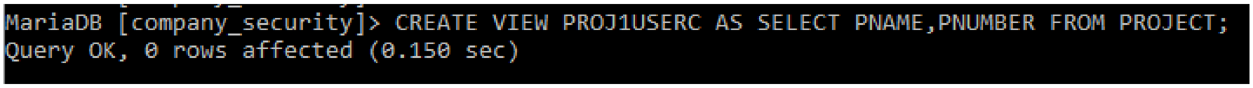
```
MariaDB [company_security]> GRANT SELECT, UPDATE ON WORKS_ON TO 'C'@'localhost';
Query OK, 0 rows affected (0.004 sec)
```



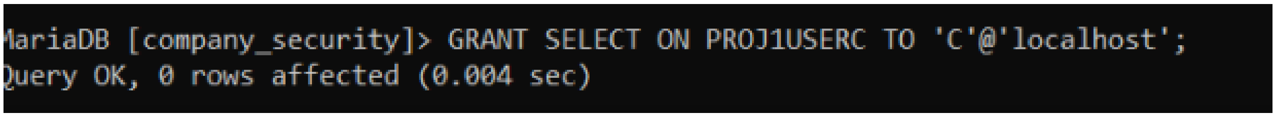
```
MariaDB [company_security]> CREATE VIEW EMP1USERC AS SELECT FNAME,MINIT,LNAME,SSN FROM EMPLOYEE;
Query OK, 0 rows affected (0.069 sec)
```



```
MariaDB [company_security]> GRANT SELECT ON EMP1USERC TO 'C'@'localhost';
Query OK, 0 rows affected (0.004 sec)
```

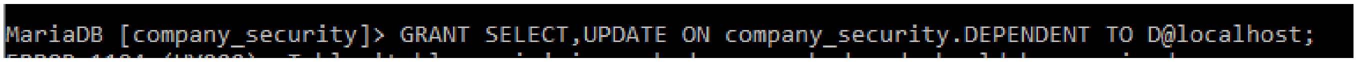


```
MariaDB [company_security]> CREATE VIEW PROJ1USERC AS SELECT PNAME,PNUMBER FROM PROJECT;
Query OK, 0 rows affected (0.150 sec)
```

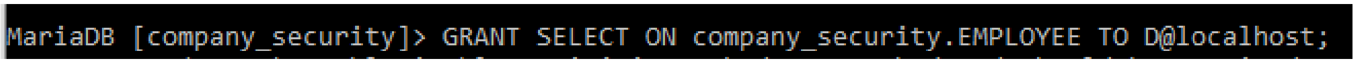


```
MariaDB [company_security]> GRANT SELECT ON PROJ1USERC TO 'C'@'localhost';
Query OK, 0 rows affected (0.004 sec)
```

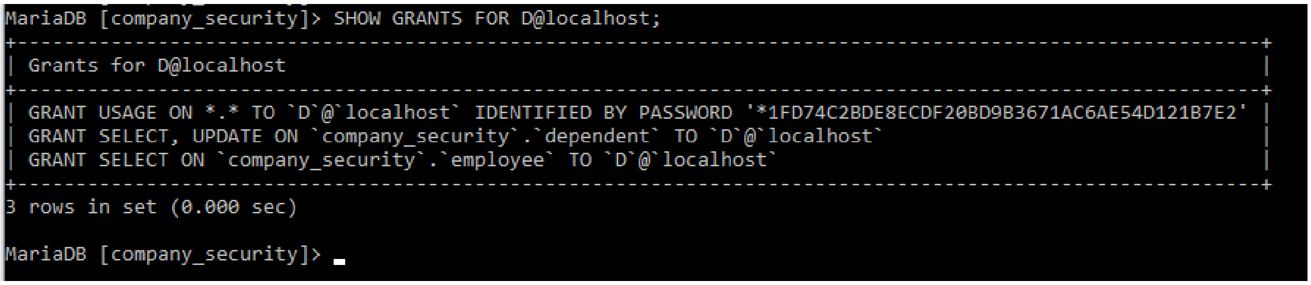
IV. Account D can retrieve any attribute of EMPLOYEE or DEPENDENT and can modify DEPENDENT.



```
MariaDB [company_security]> GRANT SELECT,UPDATE ON company_security.DEPENDENT TO D@localhost;
```

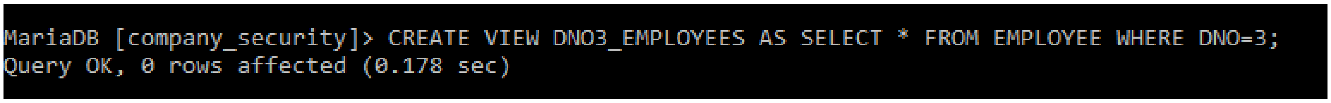


```
MariaDB [company_security]> GRANT SELECT ON company_security.EMPLOYEE TO D@localhost;
```

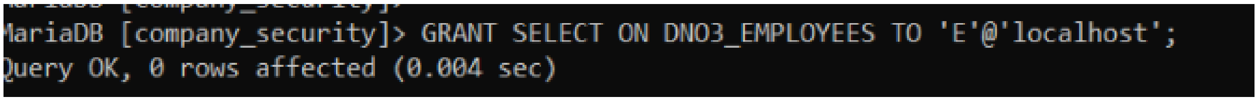


```
MariaDB [company_security]> SHOW GRANTS FOR D@localhost;
+-----------------------------------------------------------------------------------------------------+
| Grants for D@localhost                                                                              |
+-----------------------------------------------------------------------------------------------------+
| GRANT USAGE ON *.* TO `D`@`localhost` IDENTIFIED BY PASSWORD '*1FD74C2BDE8ECDF20BD9B3671AC6AE54D121B7E2' |
| GRANT SELECT, UPDATE ON `company_security`.`dependent` TO `D`@`localhost`                           |
| GRANT SELECT ON `company_security`.`employee` TO `D`@`localhost`                                    |
+-----------------------------------------------------------------------------------------------------+
3 rows in set (0.000 sec)

MariaDB [company_security]>
```

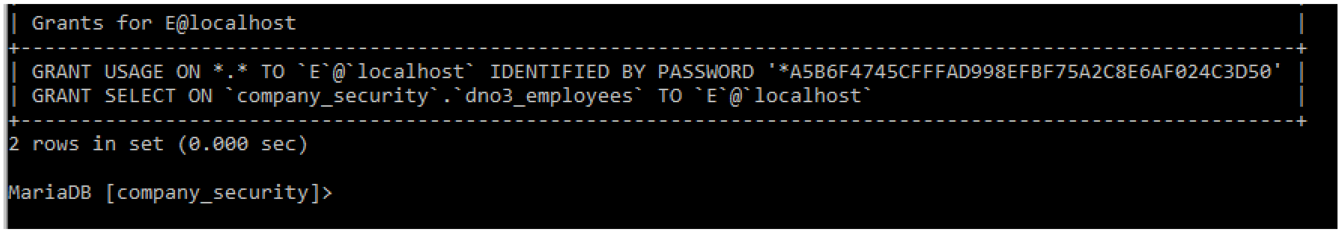
V. Account E can retrieve any attribute of EMPLOYEE but only for EMPLOYEE tuples that have Dno = 3.



```
MariaDB [company_security]> CREATE VIEW DNO3_EMPLOYEES AS SELECT * FROM EMPLOYEE WHERE DNO=3;
Query OK, 0 rows affected (0.178 sec)
```



```
MariaDB [company_security]> GRANT SELECT ON DNO3_EMPLOYEES TO 'E'@'localhost';
Query OK, 0 rows affected (0.004 sec)
```



```
| Grants for E@localhost                                                                              |
+-----------------------------------------------------------------------------------------------------+
| GRANT USAGE ON *.* TO `E`@`localhost` IDENTIFIED BY PASSWORD '*A5B6F4745CFFFAD998EFBF75A2C8E6AF024C3D50' |
| GRANT SELECT ON `company_security`.`dno3_employees` TO `E`@`localhost`                              |
+-----------------------------------------------------------------------------------------------------+
2 rows in set (0.000 sec)

MariaDB [company_security]>
```