E/15/366

S.THINESH

4. In Class Exercise

1.Create database company security.

use company_security;

Database changed

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

```
C:\wamp\bin\mysql\mysql5.6.12\bin>mysql -u root -p company_security <company_security.sql
Enter password:

C:\wamp\bin\mysql\mysql5.6.12\bin>
```

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

```
mysql> create user  'user1'@'localhost' IDENTIFIED BY'password1';
Query OK, 0 rows affected (0.00 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.

```
C:\wamp\bin\mysql\mysql5.6.12\bin>mysql -u user1 -p
Enter password: *********
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 2
Server version: 5.6.12-log MySQL Community Server (GPL)

Copyright (c) 2000, 2013, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

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

mysql> select * from employee;
ERROR 1046 (3D000): No database selected
mysql> use company_security;
Database changed
```

We can see, user1 does not have permission to enter the database.

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

```
mysql> grant select on employee to 'user1'@'localhost';
Query OK, 0 rows affected (0.04 sec)
```

```
mysql> 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 (0.00 sec)

mysql> use company_security;
Database changed
mysql> insert into employee (Fname,Minit,Lname,Ssn,Bdate,Address,Sex,Salary,Super_ssn,Dno) values
    -> (Thinesh,C,Satha,999998877,1996-04-01,jaffna,M,30000,98755525,6);
ERROR 1142 (42000): INSERT command denied to user 'user1'@'localhost' for table 'employee'
```

We can see, user1 only have read permission , user1 can not insert values.

Insert command denied to user1 for table employee.

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

Before grant insert permission to user1 on employee table , user1 can not insert.

Fix the problem : grant insert permission to user1 on employee table.

```
mysql> use company_security;
Database changed
mysql> grant insert on employee to 'user1'@'localhost';
Query OK, 0 rows affected (0.01 sec)

mysql>
```

```
mysql> insert into employee (Fname,Lname,Ssn,Bdate,Address,Salary,Dno) values
    -> ('Thinesh','Satha','999998877',1996-04-01,'jaffna',30000,5);
Query OK, 1 row affected, 1 warning (0.00 sec)
```

```
mysql> 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 |
| Thinesh  | NULL  | Satha   | 999998877 | 0000-00-00 | jaffna                  | NULL | 30000.00 | NULL      |   5 |
+----------+-------+---------+-----------+------------+-------------------------+------+----------+-----------+-----+
9 rows in set (0.00 sec)

mysql>
```

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).

```
mysql> grant create view on company_security.* to 'user1'@'localhost';
Query OK, 0 rows affected (0.00 sec)

mysql> grant select on works_on to 'user1'@'localhost';
Query OK, 0 rows affected (0.00 sec)

mysql> create view works_on1 as select Fname,Lname,Pno from employee,works_on;
Query OK, 0 rows affected (0.02 sec)
```

```
mysql> grant select on works_on1 to 'user2'@'localhost';
Query OK, 0 rows affected (0.00 sec)
```

8. Select tuples from user2 account. What happens?

Open user2 account and select the tuple. It shows the touple.

```
C:\wamp\bin\mysql\mysql5.6.12\bin>mysql -u user2 -p
Enter password: *********
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 7
Server version: 5.6.12-log MySQL Community Server (GPL)

Copyright (c) 2000, 2013, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

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

mysql> select * from works_on1;
ERROR 1046 (3D000): No database selected
mysql> use company_security;
Database changed
mysql> 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 |
```

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

```
mysql> REVOKE SELECT
    -> ON company_security.*
    -> from 'user1'@'localhost';
Query OK, 0 rows affected (0.00 sec)
```

User1 can not access the WORK ON1

```
mysql> select * from works_on1;
ERROR 1142 (42000): SELECT command denied to user 'user1'@'localhost' for table 'works_on1'
mysql>
```

But works_on1 works fine.

```
mysql> REVOKE SELECT
    -> ON company_security.*
    -> from 'user1'@'localhost';
Query OK, 0 rows affected (0.00 sec)

mysql> 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 |
| Thinesh  | Satha   |   1 |
| John     | Smith   |   1 |
| Franklin | Wong    |   1 |
| Joyce    | English |   1 |
| Ramesh   | Narayan |   1 |
```

This command will REVOKE a SELECT privilege user1.

- When you REVOKE SELECT privilege on a table from a user, the user will not be able to SELECT data from that table anymore.

- However, if the user has received SELECT privileges on that table from more than one users, he/she can SELECT from that table until everyone who granted the permission revoked it.

SQL Injection Attacks

```
mysql> 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 (0.01 sec)

mysql> 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 |
| Thinesh  | NULL  | Satha   | 999998877 | 0000-00-00 | jaffna                  | NULL | 30000.00 | NULL      |   5 |
+----------+-------+---------+-----------+------------+-------------------------+------+----------+-----------+-----+
9 rows in set (0.00 sec)
```

5. Assignment

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

GRANT SELECT, UPDATE

ON EMPLOYEE, DEPARTMENT, DEPT_LOCATIONS, PROJECT, WORKS_ON

TO A WITH GRANT OPTION;

```
mysql> GRANT SELECT, UPDATE
    -> ON DEPARTMENT
    -> TO A
    -> WITH GRANT OPTION;
Query OK, 0 rows affected (0.00 sec)

mysql> GRANT SELECT, UPDATE
    -> ON PROJECT
    -> TO A
    -> WITH GRANT OPTION;
Query OK, 0 rows affected (0.00 sec)

mysql> GRANT SELECT, UPDATE
    -> ON DEPT_LOCATIONS
    -> TO A
    -> WITH GRANT OPTION;
Query OK, 0 rows affected (0.00 sec)

mysql> GRANT SELECT, UPDATE
    -> ON WORKS_ON
    -> TO A
    -> WITH GRANT OPTION;
Query OK, 0 rows affected (0.00 sec)

mysql> GRANT SELECT, UPDATE
    -> ON EMPLOYEE
    -> TO A
    -> WITH GRANT OPTION;
Query OK, 0 rows affected (0.00 sec)
```

```
mysql> SHOW GRANTS FOR A;
+-----------------------------------------------------------------------------------------------+
| Grants for A@%                                                                                |
+-----------------------------------------------------------------------------------------------+
| GRANT USAGE ON *.* TO 'A'@'%'                                                                 |
| GRANT SELECT, UPDATE ON `company_security`.`department` TO 'A'@'%' WITH GRANT OPTION          |
| GRANT SELECT, UPDATE ON `company_security`.`project` TO 'A'@'%' WITH GRANT OPTION             |
| GRANT SELECT, UPDATE ON `company_security`.`employee` TO 'A'@'%' WITH GRANT OPTION            |
| GRANT SELECT, UPDATE ON `company_security`.`dept_locations` TO 'A'@'%' WITH GRANT OPTION      |
| GRANT SELECT, UPDATE ON `company_security`.`works_on` TO 'A'@'%' WITH GRANT OPTION            |
+-----------------------------------------------------------------------------------------------+
6 rows in set (0.00 sec)
```

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

CREATE VIEW EMP_VIEW AS SELECT FNAME, MINIT, LNAME, SSN, BDATE, ADDRESS, SEX SUPERSSN, DNO FROM EMPLOYEE;

GRANT SELECT ON EMP_VIEW TO B;

CREATE VIEW DEPT_VIEW AS SELECT DNAME, DNUMBER FROM DEPARTMENT;

GRANT SELECT ON DEPT_VIEW TO B;

```
mysql> CREATE VIEW EMP_VIEW AS
    -> SELECT FNAME, MINIT, LNAME, SSN, BDATE, ADDRESS, SEX
    -> SUPERSSN, DNO
    -> FROM EMPLOYEE;
Query OK, 0 rows affected (0.01 sec)

mysql> GRANT SELECT ON EMP_VIEW TO B;
Query OK, 0 rows affected (0.00 sec)

mysql> CREATE VIEW DEPT_VIEW AS SELECT DNAME, DNUMBER FROM DEPARTMENT;
Query OK, 0 rows affected (0.03 sec)

mysql> GRANT SELECT ON DEPT_VIEW TO B;
Query OK, 0 rows affected (0.00 sec)
```

```
mysql> SHOW GRANTS FOR B;
+-----------------------------------------------------------+
| Grants for B@%                                            |
+-----------------------------------------------------------+
| GRANT USAGE ON *.* TO 'B'@'%'                             |
| GRANT SELECT ON `company_security`.`emp_view` TO 'B'@'%'  |
| GRANT SELECT ON `company_security`.`dept_view` TO 'B'@'%' |
+-----------------------------------------------------------+
3 rows in set (0.00 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.

GRANT SELECT, UPDATE ON WORKS_ON TO C;

CREATE VIEW EMP_VIEW1 AS SELECT FNAME, MINIT, LNAME, SSN FROM EMPLOYEE;

GRANT SELECT ON EMP_VIEW1 TO C;

CREATE VIEW PROJ_VIEW AS SELECT PNAME, PNUMBER FROM PROJECT;

GRANT SELECT ON PROJ_VIEW TO C;

```
0 rows in set (0.00 sec)

mysql> GRANT SELECT, UPDATE ON WORKS_ON TO C;
Query OK, 0 rows affected (0.00 sec)

mysql> CREATE VIEW EMP_VIEW1 AS SELECT FNAME, MINIT, LNAME, SSN FROM EMPLOYEE;
Query OK, 0 rows affected (0.01 sec)

mysql> GRANT SELECT ON EMP_VIEW1 TO C;
Query OK, 0 rows affected (0.00 sec)

mysql> CREATE VIEW PROJ_VIEW AS SELECT PNAME, PNUMBER FROM PROJECT;
Query OK, 0 rows affected (0.01 sec)

mysql> GRANT SELECT ON PROJ_VIEW TO C;
Query OK, 0 rows affected (0.00 sec)

mysql> SHOW GRANTS FOR C;
+-----------------------------------------------------------------------+
| Grants for C@%                                                        |
+-----------------------------------------------------------------------+
| GRANT USAGE ON *.* TO 'C'@'%'                                         |
| GRANT SELECT ON `company_security`.`emp_view1` TO 'C'@'%'             |
| GRANT SELECT, UPDATE ON `company_security`.`works_on` TO 'C'@'%'      |
| GRANT SELECT ON `company_security`.`proj_view` TO 'C'@'%'             |
+-----------------------------------------------------------------------+
4 rows in set (0.00 sec)
```

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

GRANT SELECT ON EMPLOYEE, DEPENDENT TO D;

GRANT UPDATE ON DEPENDENT TO D;

```
for the right syntax to use near ' DEPENDENT TO D' at line 1
mysql> GRANT SELECT ON EMPLOYEE TO D;
Query OK, 0 rows affected (0.00 sec)

mysql> GRANT SELECT ON DEPENDENT TO D;
Query OK, 0 rows affected (0.00 sec)

mysql> SHOW GRANTS FOR D;
+-----------------------------------------------------------+
| Grants for D@%                                            |
+-----------------------------------------------------------+
| GRANT USAGE ON *.* TO 'D'@'%'                             |
| GRANT SELECT ON `company_security`.`dependent` TO 'D'@'%' |
| GRANT SELECT ON `company_security`.`employee` TO 'D'@'%'  |
+-----------------------------------------------------------+
3 rows in set (0.00 sec)
```

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

CREATE VIEW DNO_VIEW AS SELECT * FROM EMPLOYEE WHERE DNO = 3;

GRANT SELECT ON DNO_VIEW TO E;