

CO527 – Advanced Database Systems

Lab 05

E/17/407

Wijesooriya H.D

Exercise

(03) Create a new user 'user1' within the MySQL shell.

```
mysql> CREATE USER 'user1'@'localhost' IDENTIFIED BY 'password1';
Query OK, 0 rows affected (1.00 sec)

mysql> SELECT USER,HOST from MYSQL.USER;
+-----+-----+
| USER          | HOST      |
+-----+-----+
| mysql.infoschema | localhost |
| mysql.session   | localhost |
| mysql.sys       | localhost |
| root           | localhost |
| user1          | localhost |
+-----+-----+
5 rows in set (0.00 sec)
```

(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'.

```
mysql> use company_security;
ERROR 1044 (42000): Access denied for user 'user1'@'localhost' to database 'company_security'
mysql>
```

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

```
mysql> GRANT SELECT
-> ON company_security.employee
-> TO 'user1'@'localhost';
Query OK, 0 rows affected (0.19 sec)
```

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

```
mysql> SELECT *
-> FROM employee;
```

Fname	Minit	Lname	Ssn	Bdate	Address	Sex	Salary	Super_ssn	Dno
John	B	Smith	123456789	1965-01-09	731 Fondren, Houston, TX	M	30000.00	333445555	5
Franklin	T	Wong	333445555	1955-12-08	638 Voss, Houston, 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> INSERT INTO
-> EMPLOYEE VALUES
-> ('Hasara','B','Smith',123456788,'1996-01-09'
-> , '731 FONDREN , HOUSTEN, TX','F',
-> 3600,'333445555',5);
ERROR 1142 (42000): INSERT command denied to user 'user1'@'localhost' for table 'employee'
mysql>
```

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.

```
mysql> GRANT INSERT
-> ON company_security.employee
-> TO 'user1'@'localhost';
Query OK, 0 rows affected (0.11 sec)
```

(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.

```
mysql> GRANT
-> SELECT
-> ON company_security.works_on
-> TO 'user1'@'localhost';
Query OK, 0 rows affected (1.16 sec)
```

- Giving permission to user1 on CREATE VIEW.

```
mysql> GRANT
-> CREATE VIEW
-> ON company_security.*
-> TO 'user1'@'localhost';
Query OK, 0 rows affected (0.35 sec)
```

- Creating the view works_on1.

```
mysql> CREATE VIEW WORKS_ON1 AS
-> SELECT employee.Fname,employee.Lname,works_on.Pno
-> FROM employee,works_on
-> WHERE employee.ssn=works_on.Essn;
Query OK, 0 rows affected (6.07 sec)
```

- Creating a new user 'user2'

```
mysql> CREATE USER
-> 'user2'@'localhost'
-> IDENTIFIED BY
-> 'password2';
Query OK, 0 rows affected (0.86 sec)
```

- Giving permission to user2 to select tuples from the view 'works_on1'

```
mysql> GRANT
-> SELECT
-> ON company_security.works_on1
-> TO 'user2'@'localhost';
Query OK, 0 rows affected (0.15 sec)
```

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

```
mysql> use company_security;
Database changed
mysql> SELECT *
-> FROM works_on1;
+-----+-----+-----+
| Fname | Lname | Pno |
+-----+-----+-----+
| John  | Smith | 1   |
| John  | Smith | 2   |
| Franklin | Wong  | 2   |
| Franklin | Wong  | 3   |
| Franklin | Wong  | 10  |
| Franklin | Wong  | 20  |
| Joyce  | English | 1   |
| Joyce  | English | 2   |
| Ramesh | Narayan | 3   |
| James  | Borg   | 20  |
| Jennifer | Wallace | 20  |
| Jennifer | Wallace | 30  |
| Ahmad  | Jabbar | 10  |
| Ahmad  | Jabbar | 30  |
| Alicia | Zelaya | 10  |
| Alicia | Zelaya | 30  |
+-----+-----+-----+
16 rows in set (0.11 sec)
```

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

```
mysql> show grants for 'user2'@'localhost';
+-----+
| Grants for user2@localhost |
+-----+
| GRANT USAGE ON *.* TO `user2`@`localhost` |
| GRANT SELECT ON `company_security`.`works_on1` TO `user2`@`localhost` |
+-----+
2 rows in set (0.00 sec)
```

(09)

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.works_on
-> FROM 'user1'@'localhost';
Query OK, 0 rows affected (0.46 sec)
```

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.

```
mysql> REVOKE
-> SELECT
-> ON company_security.employee
-> FROM 'user1'@'localhost';
Query OK, 0 rows affected (0.52 sec)
```

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

SQL INJECTION ATTCK

```
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 (0.00 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, Houston, TX | M   | 30000.00 | 333445555 | 5   |
| Franklin | T   | Wong  | 333445555 | 1955-12-08 | 638 Voss, Houston, 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)
```

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

```
mysql> CREATE USER 'A'@'localhost' IDENTIFIED BY 'passwordA';
Query OK, 0 rows affected (0.37 sec)

mysql> CREATE USER 'B'@'localhost' IDENTIFIED BY 'passwordB';
Query OK, 0 rows affected (0.12 sec)

mysql> CREATE USER 'C'@'localhost' IDENTIFIED BY 'passwordC';
Query OK, 0 rows affected (15.55 sec)

mysql> CREATE USER 'D'@'localhost' IDENTIFIED BY 'passwordD';
Query OK, 0 rows affected (5.53 sec)

mysql> CREATE USER 'E'@'localhost' IDENTIFIED BY 'passwordE';
Query OK, 0 rows affected (10.33 sec)
```

(i)

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

```
mysql> GRANT SELECT, UPDATE ON company_security.EMPLOYEE TO 'A'@'localhost' WITH GRANT OPTION;
Query OK, 0 rows affected (1.84 sec)

mysql> GRANT SELECT, UPDATE ON company_security.DEPARTMENT TO 'A'@'localhost' WITH GRANT OPTION;
Query OK, 0 rows affected (3.91 sec)

mysql> GRANT SELECT, UPDATE ON company_security.DEPT_LOCATIONS TO 'A'@'localhost' WITH GRANT OPTION;
Query OK, 0 rows affected (0.10 sec)

mysql> GRANT SELECT, UPDATE ON company_security.PROJECT TO 'A'@'localhost' WITH GRANT OPTION;
Query OK, 0 rows affected (0.81 sec)

mysql> GRANT SELECT, UPDATE ON company_security.WORKS_ON TO 'A'@'localhost' WITH GRANT OPTION;
Query OK, 0 rows affected (0.77 sec)
```

```
mysql> show grants for 'A'@'localhost';
+-----+
| Grants for A@localhost |
+-----+
| GRANT USAGE ON *.* TO `A`@`localhost` |
| GRANT SELECT, UPDATE ON `company_security`.`department` TO `A`@`localhost` WITH GRANT OPTION |
| 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`.`works_on` TO `A`@`localhost` 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.

```
mysql> CREATE VIEW empDetails AS SELECT Fname, Minit, Lname, Ssn, Bdate, Address,sex,Super_ssn,Dno FROM EMPLOYEE;
Query OK, 0 rows affected (1.54 sec)

mysql> GRANT SELECT ON empDetails TO 'B'@'localhost';
Query OK, 0 rows affected (0.11 sec)
```



```
mysql> CREATE VIEW deptDetails AS SELECT Dname, Dnumber FROM DEPARTMENT;
Query OK, 0 rows affected (0.25 sec)
```

```
mysql> GRANT SELECT ON deptDetails TO 'B'@'localhost';
Query OK, 0 rows affected (6.13 sec)
```

```
mysql> show grants for 'B'@'localhost';
```

```
+-----+
| Grants for B@localhost |
+-----+
| GRANT USAGE ON *.* TO `B`@`localhost` |
| GRANT SELECT ON `company_security`.`deptdetails` TO `B`@`localhost` |
| GRANT SELECT ON `company_security`.`empdetails` TO `B`@`localhost` |
+-----+
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.

```
mysql> GRANT SELECT, UPDATE ON WORKS_ON TO 'C'@'localhost';
Query OK, 0 rows affected (0.18 sec)
```

```
mysql> CREATE VIEW empd2 AS SELECT Fname, Minit, Lame, Ssn FROM EMPLOYEE;
ERROR 1054 (42S22): Unknown column 'Lame' in 'field list'
```

```
mysql> CREATE VIEW empd2 AS SELECT Fname, Minit, Lname, Ssn FROM EMPLOYEE;
Query OK, 0 rows affected (3.53 sec)
```

```
mysql> GRANT SELECT ON empd2 TO 'C'@'localhost';
Query OK, 0 rows affected (3.16 sec)
```

```
mysql> CREATE VIEW projd2 AS SELECT Pname, Pnumber FROM PROJECT;
Query OK, 0 rows affected (5.85 sec)
```

```
mysql> GRANT SELECT ON projd2 TO 'C'@'localhost';
Query OK, 0 rows affected (2.84 sec)
```

```
mysql> show grants for 'C'@'localhost';
+-----+
| Grants for C@localhost |
+-----+
| GRANT USAGE ON *.* TO `C`@`localhost` |
| GRANT SELECT ON `company_security`.`empd2` TO `C`@`localhost` |
| GRANT SELECT ON `company_security`.`projd2` TO `C`@`localhost` |
| GRANT SELECT, UPDATE ON `company_security`.`works_on` TO `C`@`localhost` |
+-----+
4 rows in set (0.00 sec)
```

(iv)

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

```
mysql> GRANT SELECT ON EMPLOYEE TO 'D'@'localhost';
Query OK, 0 rows affected (4.34 sec)

mysql> GRANT SELECT ON DEPENDENT TO 'D'@'localhost';
Query OK, 0 rows affected (0.50 sec)

mysql> GRANT UPDATE ON DEPENDENT TO 'D'@'localhost';
Query OK, 0 rows affected (0.80 sec)
```

```
mysql> show grants for 'D'@'localhost';
+-----+
| Grants for D@localhost |
+-----+
| GRANT USAGE ON *.* TO `D`@`localhost` |
| GRANT SELECT, UPDATE ON `company_security`.`dependent` TO `D`@`localhost` |
| GRANT SELECT ON `company_security`.`employee` TO `D`@`localhost` |
+-----+
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.

```
mysql> CREATE VIEW dno3_emp AS SELECT * FROM EMPLOYEE WHERE DNO = 3;
Query OK, 0 rows affected (26.75 sec)

mysql> GRANT SELECT ON dno3_emp TO 'E'@'localhost';
Query OK, 0 rows affected (14.19 sec)
```

```
mysql> show grants for 'E'@'localhost';
+-----+
| Grants for E@localhost |
+-----+
| GRANT USAGE ON *.* TO `E`@`localhost` |
| GRANT SELECT ON `company_security`.`dno3_emp` TO `E`@`localhost` |
+-----+
2 rows in set (0.00 sec)
```