Lab 05 – Database Security

E/15/202

In Class Exercise

1. CREATE DATABASE company_security;
2. Loaded the given company_security.sql file to the company_security database.
3. `CREATE USER 'user1'@'localhost' IDENTIFIED BY '1234';` (Given at the mysql root)
4. When I logged in as user1 I do not have any authority to access the database.

```
C:\wamp64\bin\mysql\mysql5.7.14\bin>mysql.exe -u user1 -p
Enter password: ****
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 49
Server version: 5.7.14 MySQL Community Server (GPL)

Copyright (c) 2000, 2016, 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> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
+--------------------+
1 row in set (0.00 sec)

mysql> exit;
Bye
```

```
C:\wamp64\bin\mysql\mysql5.7.14\bin>mysql.exe -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 50
Server version: 5.7.14 MySQL Community Server (GPL)

Copyright (c) 2000, 2016, 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> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| buy_t_shirts_online |
| company            |
| company_security   |
| database_project   |
| e15                |
| e15202             |
```

5. GRANT SELECT ON company_security.employee TO 'user1'@'localhost';
   (This command was given at the user shell and below figure shows all the grants to the new user user1)

```
mysql> show grants;
+-----------------------------------------------------------------------------+
| Grants for user1@localhost                                                  |
+-----------------------------------------------------------------------------+
| GRANT USAGE ON *.* TO 'user1'@'localhost'                                   |
| GRANT SELECT ON `company_security`.`employee` TO 'user1'@'localhost'        |
+-----------------------------------------------------------------------------+
2 rows in set (0.00 sec)
```

6. select * from employee;
   (Since the user1 has permission to read the company_security.employee table the above statement will run without any error)

```
mysql> use company_security;
Database changed
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)
```

INSERT INTO EMPLOYEE VALUES('Alex','X','Ramsey',999888888,'1995-08-14','202 Boston, London, TX','M', 40000,'333445555',1);

```
mysql> INSERT INTO EMPLOYEE VALUES('Alex','X','Ramsey',999888888,'1995-08-14','202 Boston, London, TX','M', 40000,'333445555',1);
ERROR 1142 (42000): INSERT command denied to user 'user1'@'localhost' for table 'employee'
mysql>
```

Since user1 has given only the read permission for the employee table in database company_security, user1 is not allowed to insert data to the employee table. To fix that problem we have to give insert permission to the user1 from the mysql root.

From the root,
GRANT INSERT ON company_security.employee TO 'user1'@'localhost';

From the user1,

```
mysql> show grants;
+-----------------------------------------------------------------------------------------+
| Grants for user1@localhost                                                              |
+-----------------------------------------------------------------------------------------+
| GRANT USAGE ON *.* TO 'user1'@'localhost'                                               |
| GRANT SELECT, INSERT ON `company_security`.`employee` TO 'user1'@'localhost'            |
+-----------------------------------------------------------------------------------------+
2 rows in set (0.00 sec)
```

Now run,
INSERT INTO EMPLOYEE VALUES('Alex','X','Ramsey',999888888,'1995-08-14','202 Boston, London, TX','M', 40000,'333445555',1);

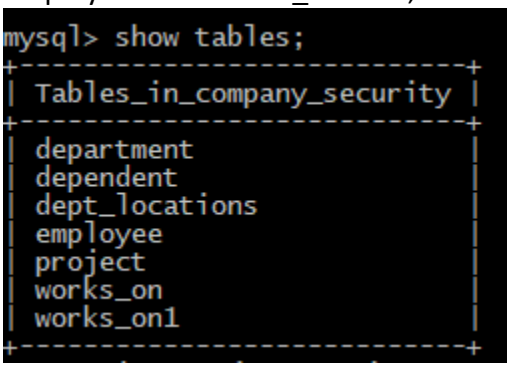
```
mysql> use company_security;
Database changed
mysql> INSERT INTO EMPLOYEE VALUES('Alex','X','Ramsey',999888888,'1995-08-14','202 Boston, London, TX','M', 40000,'333445555',1);
Query OK, 1 row affected (0.07 sec)

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 |
| Alex     | X     | Ramsey   | 999888888 | 1995-08-14 | 202 Boston, London, TX  | M   | 40000.00 | 333445555 |   1 |
+----------+-------+----------+-----------+------------+-------------------------+-----+----------+-----------+-----+
9 rows in set (0.00 sec)
```

7. At the root,
   GRANT SELECT ON company_security.works_on TO 'user1'@'localhost';
   GRANT CREATE VIEW ON company_security.* TO 'user1'@'localhost';
   GRANT SHOW VIEW ON company_security.* TO 'user1'@'localhost';
   flush privileges;

   At the user1,

```
mysql> show grants;
+-----------------------------------------------------------------------------------------+
| Grants for user1@localhost                                                              |
+-----------------------------------------------------------------------------------------+
| GRANT USAGE ON *.* TO 'user1'@'localhost'                                               |
| GRANT CREATE VIEW, SHOW VIEW ON `company_security`.* TO 'user1'@'localhost'             |
| GRANT SELECT ON `company_security`.`works_on` TO 'user1'@'localhost'                    |
| GRANT SELECT, INSERT ON `company_security`.`employee` TO 'user1'@'localhost'            |
+-----------------------------------------------------------------------------------------+
```

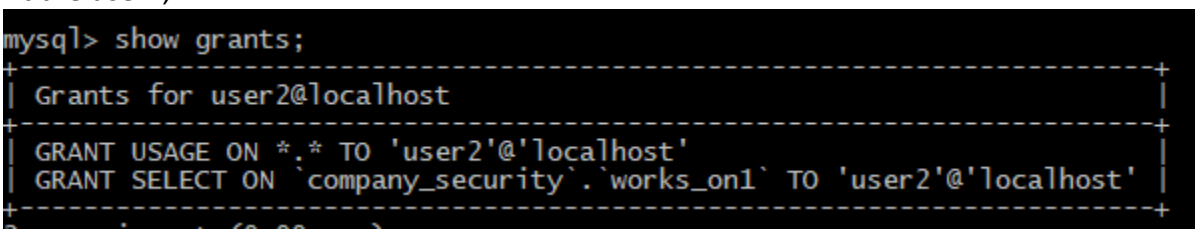
create view works_on1 as select Fname,Lname,Pno from employee,works_on where employee.Ssn = works_on.Essn;



At the root,
The created view works_on1 at the user1 is also visible at the root. Not only that but also works_on1 view has all the privileges at the root. But at the user1 it has no privileges to select or drop the view.

CREATE USER 'user2'@'localhost' IDENTIFIED BY '1234';
GRANT SELECT ON company_security.works_on1 TO 'user2'@'localhost';
flush privileges;
exit;

mysql.exe -u user2 –p
At the user2,



8. user2 will show the selected tuples from the works_on1 view without an error.

```
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 |
+----------+---------+-----+
```

9. REVOKE SELECT ON company_security.works_on from 'user1'@'localhost';
   REVOKE CREATE VIEW ON company_security.* FROM 'user1'@'localhost';
   REVOKE SHOW VIEW ON company_security.* FROM 'user1'@'localhost';
   REVOKE INSERT ON company_security.employee FROM 'user1'@'localhost';
   flush privileges;

   At the user1,

```
mysql> use company_security;
ERROR 1044 (42000): Access denied for user 'user1'@'localhost' to database 'company_security'
mysql> show grants;
+----------------------------------------+
| Grants for user1@localhost             |
+----------------------------------------+
| GRANT USAGE ON *.* TO 'user1'@'localhost' |
+----------------------------------------+
1 row in set (0.00 sec)
```

   But we never deleted the view works_on1. So when I run `SHOW TABLES` query at the root I could see the created view was still there. But since all the permissions have been revoked from the user1, it has no permission to access the database.

   At the user2,

```
c:\wamp64\bin\mysql\mysql5.7.14\bin>mysql.exe -u user2 -p
Enter password: ****
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 229
Server version: 5.7.14 MySQL Community Server (GPL)

Copyright (c) 2000, 2016, 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> use company_security;
Database changed
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/invoker of view lack rights to use them
mysql>
```

Although we have not changed any permission to the user2, still it will not allow accessing the view works_on1.

Reason for this is that the view works_on1 was created at the user1. And for that user1 was given all the permissions needed to create that view. But now those permissions have been revoked.

Although created view was there it has no permission to access the needed tables at the user1.

SQL Injection Attacks

```
mysql> use company_security;
Database changed
mysql>
mysql>
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 (0.03 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 |
| Alex     | X     | Ramsey  | 999888888 | 1995-08-14 | 202 Boston, London, TX   | M    | 40000.00 | 333445555 |   1 |
+----------+-------+---------+-----------+------------+--------------------------+------+----------+-----------+-----+
9 rows in set (0.00 sec)
```