

课程名称:	数据库系统
实验名称:	SQL安全性
姓名:	杨吉祥
学院:	计算机科学与技术学院
系:	竺可桢学院图灵班
专业:	计算机科学与技术
学号:	3230106222
指导教师:	陈刚

# 一、实验目的:

熟悉通过SQL进行安全性控制的方法。

## 二、实验内容和要求:

1. 建立表,考察表的生成者拥有该表的哪些权限。

表的生成者默认拥有该表的所有权限,可以执行任何操作。

mysql> CREATE TABLE my_table ( -> id INT PRIMARY KEY, -> name VARCHAR(50),	
-> salary DECIMAL(10, 2) -> );	
Query OK, 0 rows affected (0.05 sec)	
mysql> SHOW GRANTS FOR CURRENT_USER();	
<u>-</u>	
Grants for root@localhost	·-+
+	·

GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, DROP, RELOAD, SHUTDOWN, PROCESS, FILE, REFERENCES, INDEX, ALTER, SHOW DA TABASES, SUPER, CREATE TEMPORARY TABLES, LOCK TABLES, EXECUTE, REPLICATION SLAVE, REPLICATION CLIENT, CREATE VIEW, SHOW VIEW, CREATE ROUTINE, ALTER ROUTINE, CREATE USER, EVENT, TRIGGER, CREATE TABLESPACE, CREATE ROLE, DROP ROLE ON *.* TO 'r oot'@'localhost' WITH GRANT OPTION
GRANT APPLICATION_PASSWORD_ADMIN, AUDIT_ABORT_EXEMPT, AUDIT_ADMIN, AUTHENTICATION_POLICY_ADMIN, BACKUP_ADMIN, BINLOG_ADMIN, BINLOG_ENCRYPTION_ADMIN, CLONE_ADMIN, CONNECTION_ADMIN, ENCRYPTION_KEY_ADMIN, FIREWALL_EXEMPT, FLUSH_OPTIMIZER_COSTS, FLUSH_ST ATUS, FLUSH_TABLES, FLUSH_USER_RESOURCES, GROUP_REPLICATION_ADMIN, GROUP_REPLICATION_STREAM, INNODB_REDO_LOG_ARCHIVE, INNODB_REDO_LOG_ENABLE, PASSWORDLESS_USER_ADMIN, PERSIST_RO_VARIABLES_ADMIN, REPLICATION_APPLIER, REPLICATION_SLAVE_ADMIN, RESOURCE_GROUP_ADMIN, RESOURCE_GROUP_USER, ROLE_ADMIN, SENSITIVE_VARIABLES_OBSERVER, SERVICE_CONNECTION_ADMIN, SESSION_VARIABLES_ADMIN, SET_USER_ID, SHOW_ROUTHE, SYSTEM_USER, SYSTEM_VARIABLES_ADMIN, TABLE_ENCRYPTION_ADMIN, TELEMETRY_LOG_ADMIN, XA_RECOVER_ADMIN ON *.* TO `root`@`localhost` WITH GRANT OPTION      GRANT PROXY ON ``@`` TO `root`@`localhost` WITH GRANT OPTION
3 rows in set (0.01 sec)

- 2. 使用SQL的grant 和revoke命令对其他用户进行授权和权力回收,考察相应的作用。
- 插入测试数据

• 创建测试用户

```
mysql> CREATE USER user1 IDENTIFIED BY 'password1';
Query OK, 0 rows affected (0.03 sec)
mysql> CREATE USER user2 IDENTIFIED BY 'password2';
Query OK, 0 rows affected (0.02 sec)
```

- 授权并验证权限
  - 授予user1 SELECT权限并进行验证

```
mysql> GRANT SELECT ON my_table TO user1; Query OK, 0 rows affected (0.01 sec)
```

```
C:\Users\杨吉祥>mysql -u user1 -p
Enter password: *******
Welcome to the MySQL monitor. Commands end with ; or \gray{g}.
Your MySQL connection id is 9
Server version: 8.0.41 MySQL Community Server - GPL
Copyright (c) 2000, 2025, Oracle and/or its affiliates.
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 my_table;
ERROR 1046 (3D000): No database selected
mysql> use test;
Database changed
mysql> SELECT * FROM my_table;
| id | name
                    | salary
   1 | Alice | 50000.00
2 | Bob | 60000.00
3 | Charlie | 70000.00
3 rows in set (0.01 sec)
mysql>
```

### ○ 授予user2 INSERT权限并进行验证:

## mysql> GRANT INSERT ON my\_table TO user2; Query OK, 0 rows affected (0.01 sec)

## • 尝试未授权的操作:

○ user1 尝试插入数据:

## ○ user2 尝试查询数据:

```
C:\Users\杨吉祥>mysql -u user2 -p
Enter password: *******
Welcome to the MySQL monitor.
                               Commands end with ; or \g.
Your MySQL connection id is 10
Server version: 8.0.41 MySQL Community Server - GPL
Copyright (c) 2000, 2025, Oracle and/or its affiliates.
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 test;
Database changed
mysql> INSERT INTO my_table (id, name, salary)
-> VALUES (4, 'David', 80000);
Query OK, 1 row affected (0.01 sec)
mysql> SELECT * FROM my_table;
ERROR 1142 (42000): SELECT command denied to user 'user2'@'localhost' for table 'my_table'
```

## • 收回权限并验证

○ 收回 user1 的 SELECT 权限并进行验证:

```
mysql> REVOKE SELECT ON my_table FROM user1; Query OK, 0 rows affected (0.01 sec)
```

```
C:\Users\杨吉祥>mysql -u user1 -p
Enter password: ********
Welcome to the MySQL monitor. Commands end with; or \g.
Your MySQL connection id is 13
Server version: 8.0.41 MySQL Community Server - GPL

Copyright (c) 2000, 2025, Oracle and/or its affiliates.

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 test;
ERROR 1044 (42000): Access denied for user 'user1'@'%' to database 'test' mysql>
```

○ 收回 user2 的 INSERT 权限并进行验证:

## mysql> REVOKE INSERT ON my\_table FROM user2; Query OK, 0 rows affected (0.01 sec)

```
C:\Users\杨吉祥>mysql -u user2 -p
Enter password: ********
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 14
Server version: 8.0.41 MySQL Community Server - GPL

Copyright (c) 2000, 2025, Oracle and/or its affiliates.

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 test;
ERROR 1044 (42000): Access denied for user 'user2'@'%' to database 'test' mysql>
```

• 通过以上操作, 我们可以清楚地看到:

#### 授权:

• 使用 GRANT 命令授予用户特定权限后,用户可以执行相应的操作(如 SELECT 、 INSERT 等)。

#### 权限验证:

• 用户只能执行被授权的操作,未授权的操作会失败。

#### 收回权限:

- 使用 REVOKE 命令收回权限后,用户无法再执行相应的操作。
- 3. 建立视图, 并把该视图的查询权限授予其他用户, 考察通过视图进行权限控制的作用。
- 创建一个视图,仅显示 my\_table 表中的 id 和 name 列:

```
C:\Users\杨吉祥>mysql -u root -p
Enter password: ******
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 15
Server version: 8.0.41 MySQL Community Server - GPL
Copyright (c) 2000, 2025, Oracle and/or its affiliates.
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 test;
Database changed
mysql> CREATE VIEW my_view AS
   -> SELECT id, name
    -> FROM my_table;
Query OK, 0 rows affected (0.02 sec)
mysql>
```

• 授予用户 user1 对视图 my\_view 的 SELECT 权限:

# mysql> GRANT SELECT ON my\_view TO user1; Query OK, 0 rows affected (0.01 sec)

## mysql>

• 用户 user1 可以查询视图:

```
C:\Users\杨吉祥>mysql -u user1 -p
Enter password: *****
Welcome to the MySQL monitor. Commands end with ; or \g. Your MySQL connection id is 16
Server version: 8.0.41 MySQL Community Server - GPL
Copyright (c) 2000, 2025, Oracle and/or its affiliates.
Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
mysql> use test;
Database changed
mysql> SELECT * FROM my_view;
  id
       name
   1
       Alice
   2
       Bob
   3
       Charlie
   4
       David
4 rows in set (0.00 sec)
```

• 用户 user1 无法直接访问 my\_table 表:

```
mysql> SELECT * FROM my_table;
ERROR 1142 (42000): SELECT command denied to user 'user1'@'localhost' for table 'my_table'
mysql> |
```