实验四 数据库安全

姓名：应承峻 **学号：**3170103456 **实验日期：**2019年4月4日

实验目的

1. 熟悉通过SQL进行数据完整性控制的方法。
2. 熟悉数据库中登录，用户，角色的概念和作用

实验内容

- 建立表，考察表的生成者拥有该表的哪些权限。
- 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。
- 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。
- 建立新的角色，并为其赋予权限（create table，view，procedure等），给用户添加角色
- 完成实验报告。

实验步骤

1. 基于上一次实验的library数据库和book表,以root用户身份登录，创建普通用户B

```
create user ycj identified by 'zjuycj'
/*此时需要重启mysql服务: net stop mysql 和 net start mysql*/
```

```
mysql> create user 'ycj' identified by 'zjuycj';
Query OK, 0 rows affected (0.11 sec)

mysql> select host,user,password from user;
+-----------+------+-------------------------------------------+
| host      | user | password                                  |
+-----------+------+-------------------------------------------+
| localhost | root |                                           |
| 127.0.0.1 | root |                                           |
| ::1       | root |                                           |
| localhost |      |                                           |
| localhost | pma  |                                           |
| %         | ycj  | *B59F6018BD48142BBE33555E228ABA72FCC76326 |
+-----------+------+-------------------------------------------+
6 rows in set (0.00 sec)
```

2. 退出root，登录用户B ,看B是否能对library进行查询和插入操作

```
mysql -hlocalhost -uycj -pzjuycj
```

不仅数据库不显示，而且不能进行任何查询或是插入操作。

```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
+--------------------+
1 row in set (0.00 sec)

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

3. 用root登录，利用grant语句赋于B表查询和插入的权限

```
grant select,insert on library.* to 'ycj'@'localhost' identified by 'zjuycj';
flush privileges;  /*冲刷权限*/
```

```
mysql> grant select,insert on library.* to 'ycj'@'localhost' identified by 'zjuycj';
Query OK, 0 rows affected (0.00 sec)

mysql> flush privileges;
Query OK, 0 rows affected (0.00 sec)
```

4. 用B登录测试是否具有相应的权限

能够进入library数据库

```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| library            |
+--------------------+
2 rows in set (0.00 sec)

mysql> use library;
Database changed
```

能够对数据表进行查询

```
mysql> select * from book;
+------+----------+--------------------------------+--------------------+------+-----------+-------+-------+-------+
| bno  | category | title                          | press              | year | author    | price | total | stock |
+------+----------+--------------------------------+--------------------+------+-----------+-------+-------+-------+
| 10   | 心理学   | 新的世界                       | 浙江大学           | 2002 | 高云鹏    | 48.00 |    20 |     4 |
| bno1 | 计算机   | SQL Server 2008完全学习手册    | 清华出版社         | 2001 | 郭郑州    | 85.80 |     5 |     3 |
| bno2 | 计算机   | 程序员的自我修养               | 电子工业出版社     | 2013 | 俞甲子    | 65.00 |     5 |     5 |
| bno3 | 教育     | 做新教育的行者                 | 福建教育出版社     | 2002 | 高云鹏    | 25.00 |     3 |     2 |
| bno4 | 教育     | 做孩子眼中有本领的父母         | 电子工业出版社     | 2013 | 高云鹏    | 23.00 |     5 |     5 |
| bno5 | 英语     | 实用英文写作                   | 高等教育出版社     | 2010 | 庞继贤    | 33.00 |     3 |     2 |
+------+----------+--------------------------------+--------------------+------+-----------+-------+-------+-------+
6 rows in set (0.10 sec)
```

能够对数据表进行插入

```
mysql> insert into book values('bno6','计算机','SQL入门','浙江大学出版社',2019,'应承峻',22.50,10,8);
Query OK, 1 row affected (0.12 sec)
```

```
mysql> select * from book;
+------+----------+--------------------------------+--------------------+------+-----------+-------+-------+-------+
| bno  | category | title                          | press              | year | author    | price | total | stock |
+------+----------+--------------------------------+--------------------+------+-----------+-------+-------+-------+
| 10   | 心理学   | 新的世界                       | 浙江大学           | 2002 | 高云鹏    | 48.00 |    20 |     4 |
| bno1 | 计算机   | SQL Server 2008完全学习手册    | 清华出版社         | 2001 | 郭郑州    | 85.80 |     5 |     3 |
| bno2 | 计算机   | 程序员的自我修养               | 电子工业出版社     | 2013 | 俞甲子    | 65.00 |     5 |     5 |
| bno3 | 教育     | 做新教育的行者                 | 福建教育出版社     | 2002 | 高云鹏    | 25.00 |     3 |     2 |
| bno4 | 教育     | 做孩子眼中有本领的父母         | 电子工业出版社     | 2013 | 高云鹏    | 23.00 |     5 |     5 |
| bno5 | 英语     | 实用英文写作                   | 高等教育出版社     | 2010 | 庞继贤    | 33.00 |     3 |     2 |
| bno6 | 计算机   | SQL入门                        | 浙江大学出版社     | 2019 | 应承峻    | 22.50 |    10 |     8 |
+------+----------+--------------------------------+--------------------+------+-----------+-------+-------+-------+
7 rows in set (0.00 sec)
```

不能对数据表进行删除

```
mysql> drop table book;
ERROR 1142 (42000): DROP command denied to user 'ycj'@'localhost' for table 'book'
mysql> delete from book;
ERROR 1142 (42000): DELETE command denied to user 'ycj'@'localhost' for table 'book'
mysql>
```

不能对数据表进行更新

```
mysql> update book set price=100.00 where bno='bno6';
ERROR 1142 (42000): UPDATE command denied to user 'ycj'@'localhost' for table 'book'
```

5. 用root登录，利用revoke语句收回用户B的操作权限，再进行测试

```
1 revoke select,insert on library.* from 'ycj'@'localhost';
2 flush privileges;
```

```
mysql> revoke select,insert on library.* from 'ycj'@'localhost';
Query OK, 0 rows affected (0.00 sec)
```

```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
+--------------------+
1 row in set (0.00 sec)

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

发现收回用户的操作权限后不能够再进入数据库进行操作。

6. 实验总结及思考

本次实验主要模拟了用户的权限管理操作，具体实现了权限的赋予和权限的回收操作。这为我的SRTP提供了一定的指导：我参与的"基于Mysql的在线评测系统"SRTP项目需要将用户SQL语句放入沙盒进行测试，为防止用户进行恶意操作，需要将用户的SQL语句放在低权限账号中运行。此时可以创建一个低权限的账号，只提供查询操作，这样可以防止用户的恶意输入。