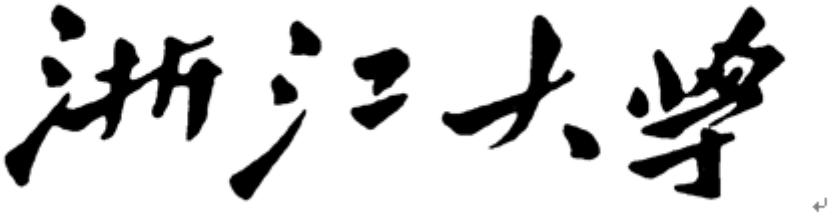

实验四 SQL安全性

学号：3220104519

姓名：蔡佳伟

一、实验目的

熟悉通过SQL进行安全性控制的办法

二、实验环境

Windows11；

DBMS: MySQL

三、实验原理

在MySQL中，需要先创建用户，使用如下命令

```
create user [username]@[hostname] identified by [password]
```

然后再使用授权命令

```
grant [privilege] on [database].[table_name] to [username]@[hostname]
```

其中privilege表示所授予的权限（select, insert等或all表示所有权限），hostname指定了用户可以从哪些主机上登录，设置为localhost表明只能本地登录，设置为%表示可以从任意主机上远程登录。

此外注意，在 MySQL 中，默认所有的用户都能对 test 数据库和名称以 test_ 开头的数据库进行访问和操作（即使没有明确授予他们权限），因此本实验中，新建的数据库名称不能是 test 或是以 test_ 开头。

四、实验过程

1. 创建用户

```
mysql>  create user A@localhost identified by '040517cc';
Query OK, 0 rows affected (0.04 sec)

mysql> select user,host from mysql.user;
+------------------+-----------+
| user             | host      |
+------------------+-----------+
| A                | localhost |
| Muzibing         | localhost |
| cjw              | localhost |
| mysql.infoschema | localhost |
| mysql.session    | localhost |
| mysql.sys        | localhost |
| root             | localhost |
+------------------+-----------+
7 rows in set (0.02 sec)
```

创建完成后，查看所有用户，发现创建成功

2. 赋予权限

```
mysql> create database db1;
Query OK, 1 row affected (0.02 sec)

mysql> grant all privileges on db1.* to 'A'@'localhost' with grant option;
Query OK, 0 rows affected (0.02 sec)
```

对用户A赋予该数据库db1的所有权限。在赋予权限的命令最后加上with grant option，可以使用户A能把数据库权限再赋予其他用户。

3. 非root用户登录与操作

1. A用户登录数据库db1

```
C:\Users\Administrator>mysql -u A -p
Enter password: ********
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 9
Server version: 8.0.36 MySQL Community Server - GPL

Copyright (c) 2000, 2024, 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> show databases;
+--------------------+
| Database           |
+--------------------+
| db1                |
| information_schema |
| performance_schema |
+--------------------+
3 rows in set (0.01 sec)
```

如图，只能看到db1的数据库

2. 创建表并插入数据

```
mysql> use db1;
Database changed
mysql> create table book (bno char(4),stock int);
Query OK, 0 rows affected (0.05 sec)

mysql> insert into book values('0001',4);
Query OK, 1 row affected (0.02 sec)

mysql> select * from book;
+------+-------+
| bno  | stock |
+------+-------+
| 0001 |     4 |
+------+-------+
1 row in set (0.00 sec)
```

3. 创建B用户，B用户登录，查看能否访问数据库db1

```
mysql> create user B@localhost identified by '040517cc';
Query OK, 0 rows affected (0.02 sec)
```

```
C:\Users\Administrator>mysql -p -u B db1
Enter password: ********
ERROR 1044 (42000): Access denied for user 'B'@'localhost' to database 'db1'
```

发现不能访问，没有权限

4. 使用A用户登录，用grant语句赋予B用户对book的查询和插入权限

```
C:\Users\Administrator>mysql -p -u A db1
Enter password: ********
```

```
mysql> grant select,insert on book to 'B'@'localhost';
Query OK, 0 rows affected (0.02 sec)
```

5. 使用B用户登录，测试查询操作

```
C:\Users\Administrator>mysql -p -u B db1
Enter password: ********
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 18
Server version: 8.0.36 MySQL Community Server - GPL

Copyright (c) 2000, 2024, 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 book;
+------+-------+
| bno  | stock |
+------+-------+
| 0001 |     4 |
+------+-------+
1 row in set (0.00 sec)
```

查询成功，说明已经赋予了权限

6. 回收权限，使用A用户登录，用revoke回收B用户对book的查询、插入权限

```
C:\Users\Administrator>mysql -u A -p db1
Enter password: ********
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 19
Server version: 8.0.36 MySQL Community Server - GPL

Copyright (c) 2000, 2024, 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 statemer

mysql> revoke insert,select on book from 'B'@'localhost';
Query OK, 0 rows affected (0.02 sec)
```

7. 再次用B用户测试权限

```
C:\Users\Administrator>mysql -u B -p db1
Enter password: ********
ERROR 1044 (42000): Access denied for user 'B'@'localhost' to database 'db1'
```

没有权限，说明删除权限成功

4. 视图权限

1. 建立视图

   使用root登录，在数据库db1中建立book表的一个视图

```
C:\Users\Administrator>mysql -u root -p
Enter password: *********
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 21
Server version: 8.0.36 MySQL Community Server - GPL

Copyright (c) 2000, 2024, 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 db1;
Database changed
mysql> create view book_view as select * from book;
Query OK, 0 rows affected (0.02 sec)

mysql> select * from book_view;
+------+-------+
| bno  | stock |
+------+-------+
| 0001 |     4 |
+------+-------+
1 row in set (0.00 sec)
```

2. 分别测试A用户，B用户对视图的访问权限

```
C:\Users\Administrator>mysql -u A -p db1
Enter password: ********
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 22
Server version: 8.0.36 MySQL Community Server - GPL

Copyright (c) 2000, 2024, 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 book_view;
+------+-------+
| bno  | stock |
+------+-------+
| 0001 |     4 |
+------+-------+
1 row in set (0.00 sec)

mysql> insert into book_view values('0002',3);
Query OK, 1 row affected (0.02 sec)
```

A用户有权限

先赋予B用户对book的查询权限

```
C:\Users\Administrator>mysql -u B -p db1
Enter password: ********
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 24
Server version: 8.0.36 MySQL Community Server - GPL

Copyright (c) 2000, 2024, 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 book_view;
ERROR 1142 (42000): SELECT command denied to user 'B'@'localhost' for table 'book_view'
mysql>
```

B用户对视图没有查询权限

登录用户A，赋予B用户对视图的查询权限

```
C:\Users\Administrator>mysql -u A -p db1
Enter password: ********
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 31
Server version: 8.0.36 MySQL Community Server - GPL

Copyright (c) 2000, 2024, 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 st
.

mysql> grant select on book_view to B@localhost;
Query OK, 0 rows affected (0.01 sec)
```

再次登录用户B，查询视图，成功

```
C:\Users\Administrator>mysql -u B -p db1
Enter password: ********
Welcome to the MySQL monitor.  Commands end with ; or \g
Your MySQL connection id is 32
Server version: 8.0.36 MySQL Community Server - GPL

Copyright (c) 2000, 2024, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation a
affiliates. Other names may be trademarks of their respe
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the cu
.

mysql> select * from book_view;
+------+-------+
| bno  | stock |
+------+-------+
| 0001 |     4 |
| 0002 |     3 |
+------+-------+
2 rows in set (0.00 sec)
```

五、总结

本次实验是SQL安全性相关的测试，包括创建用户，授权，撤销权限和视图权限相关操作等。

本次实验我不明白的是有时候'A'和localhost要打引号，有时候不用打，什么时候打引号不是很了解。不过通过这次实验，我对数据库的安全性有了更加全新的认识，了解了用户可以远程连接数据库的操作和安全性的保证等。