《数据库系统原理》实验报告（3）					
题目：数据库安全性					
学号		姓名		日期	10/31/2023

实验环境：

Docker MariaDB

处理器：11th Gen Intel(R) Core(TM) i5-11300H @ 3.10GHz　　3.11 GHz

实验步骤及结果截图：

1. 创建表 studentA

```
MariaDB [sys]> create table studentA (
    ->   Sno varchar(9) primary key,
    ->   Sname varchar(20),
    ->   Ssex varchar(2),
    ->   Sage smallint,
    ->   Sdept varchar(20),
    ->   constraint studentA_ul unique (Sname)
    -> );
Query OK, 0 rows affected (0.023 sec)

MariaDB [sys]>
MariaDB [sys]> desc studentA;
+-------+-------------+------+-----+---------+-------+
| Field | Type        | Null | Key | Default | Extra |
+-------+-------------+------+-----+---------+-------+
| Sno   | varchar(9)  | NO   | PRI | NULL    |       |
| Sname | varchar(20) | YES  | UNI | NULL    |       |
| Ssex  | varchar(2)  | YES  |     | NULL    |       |
| Sage  | smallint(6) | YES  |     | NULL    |       |
| Sdept | varchar(20) | YES  |     | NULL    |       |
+-------+-------------+------+-----+---------+-------+
5 rows in set (0.012 sec)
```

2. 向 studentA table 插入数据

```
MariaDB [sys]> insert into studentA values ('200215121', 'Tom', 'm', 20, 'CS');
Query OK, 1 row affected (0.005 sec)

MariaDB [sys]> insert into studentA values ('200215122', 'Lily', 'f', 19, 'CS');
Query OK, 1 row affected (0.005 sec)

MariaDB [sys]> select * from studentA;
+-----------+-------+------+------+-------+
| Sno       | Sname | Ssex | Sage | Sdept |
+-----------+-------+------+------+-------+
| 200215121 | Tom   | m    |   20 | CS    |
| 200215122 | Lily  | f    |   19 | CS    |
+-----------+-------+------+------+-------+
2 rows in set (0.001 sec)
```

3. 建立用户 masterA，授予用户 masterA 以系统特权，包括 create session、create table、create user、alter user 和 drop user 等，并赋予其再授权的能力

```
MariaDB [sys]> drop user masterA
    -> ;
Query OK, 0 rows affected (0.002 sec)

MariaDB [sys]> create user masterA identified by "key";
Query OK, 0 rows affected (0.002 sec)

MariaDB [sys]> grant create,
    ->       create user,
    ->       alter,
    ->       drop on *.*
    ->       to masterA
    ->       with grant option;
Query OK, 0 rows affected (0.002 sec)
```

4. 删除 masterA 的 create user、alter user 和 drop user 的系统特权

```
MariaDB [sys]> revoke create user, alter, drop on *.* from masterA;
Query OK, 0 rows affected (0.008 sec)
```

5. 在 masterA 用户下尝试查询 table studentA(注意使用 sys.studentA)，结果为拒绝查询

```
MariaDB [sys]> quit
Bye
# mariadb -u masterA -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 7
Server version: 11.1.2-MariaDB-1:11.1.2+maria~ubu2204 mariadb.org binary distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> select * from sys.studentA
    -> ;
ERROR 1142 (42000): SELECT command denied to user 'masterA'@'localhost' for table `sys`.`studentA`
```

6. 授予用户 masterA 对表 studentA 的查询、插入、修改等对象特权，并赋予其再授权的能力

```
# mariadb -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 9
Server version: 11.1.2-MariaDB-1:11.1.2+maria~ubu2204 mariadb.org binary distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> use sys
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [sys]> grant select, insert, update, delete on studentA to masterA with grant option;
Query OK, 0 rows affected (0.006 sec)
```

7. 在 masterA 用户下查询 sys.studentA(注意使用 sys.studentA)，结果为查询成功

```
MariaDB [sys]> quit
Bye
# mariadb -u masterA -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 10
Server version: 11.1.2-MariaDB-1:11.1.2+maria~ubu2204 mariadb.org binary distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> select * from sys.studentA
    -> ;
+-----------+-------+------+------+-------+
| Sno       | Sname | Ssex | Sage | Sdept |
+-----------+-------+------+------+-------+
| 200215121 | Tom   | m    |   20 | CS    |
| 200215122 | Lily  | f    |   19 | CS    |
+-----------+-------+------+------+-------+
2 rows in set (0.000 sec)
```

8. 在 masterA 用户下再插入一个元组的数据('200215123','Bob','m',21,'IS')，并在 masterA 用户下查询(注意使用 sys.studentA)

```
MariaDB [(none)]> insert into sys.studentA values ('200215123','Bob','m',21,'IS');
Query OK, 1 row affected (0.003 sec)

MariaDB [(none)]> select * from sys.studentA;
+-----------+-------+------+------+-------+
| Sno       | Sname | Ssex | Sage | Sdept |
+-----------+-------+------+------+-------+
| 200215121 | Tom   | m    |   20 | CS    |
| 200215122 | Lily  | f    |   19 | CS    |
| 200215123 | Bob   | m    |   21 | IS    |
+-----------+-------+------+------+-------+
3 rows in set (0.000 sec)
```

9. 删除今天创建的 masterA 用户

```
MariaDB [(none)]> quit
Bye
# mariadb -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 11
Server version: 11.1.2-MariaDB-1:11.1.2+maria~ubu2204 mariadb.org binary distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> drop user masterA
    -> ;
Query OK, 0 rows affected (0.002 sec)
```

出现的问题：

在实际 grant 权限过程中没有查看现有的 privilege 表，同时没有显式表明 on ，导致报错

```
MariaDB [sys]> grant create session,
    ->       create table,
    ->       create user,
    ->       alter user,
    ->       drop user
    ->       to masterA
    ->       with grant option;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your
MariaDB server version for the right syntax to use near 'session,
```

解决方案：

首先查看 privilege 表

Privilege	Context	Comment
Alter	Tables	To alter the table
Alter routine	Functions,Procedures	To alter or drop stored functions/procedures
Create	Databases,Tables,Indexes	To create new databases and tables
Create routine	Databases	To use CREATE FUNCTION/PROCEDURE
Create temporary tables	Databases	To use CREATE TEMPORARY TABLE
Create view	Tables	To create new views
Create user	Server Admin	To create new users
Delete	Tables	To delete existing rows
Delete history	Tables	To delete versioning table historical rows
Drop	Databases,Tables	To drop databases, tables, and views
Event	Server Admin	To create, alter, drop and execute events
Execute	Functions,Procedures	To execute stored routines
File	File access on server	To read and write files on the server
Grant option	Databases,Tables,Functions,Procedures	To give to other users those privileges you possess
Index	Tables	To create or drop indexes
Insert	Tables	To insert data into tables
Lock tables	Databases	To use LOCK TABLES (together with SELECT privilege)
Process	Server Admin	To view the plain text of currently executing queries
Proxy	Server Admin	To make proxy user possible
References	Databases,Tables	To have references on tables
Reload	Server Admin	To reload or refresh tables, logs and privileges
Binlog admin	Server	To purge binary logs
Binlog monitor	Server	To use SHOW BINLOG STATUS and SHOW BINARY LOG
Binlog replay	Server	To use BINLOG (generated by mariadb-binlog)
Replication master admin	Server	To monitor connected slaves
Replication slave admin	Server	To start/stop slave and apply binlog events
Slave monitor	Server	To use SHOW SLAVE STATUS and SHOW RELAYLOG EVENTS
Replication slave	Server Admin	To read binary log events from the master
Select	Tables	To retrieve rows from table
Show databases	Server Admin	To see all databases with SHOW DATABASES
Show view	Tables	To see views with SHOW CREATE VIEW
Shutdown	Server Admin	To shut down the server
Super	Server Admin	To set few server variables
Trigger	Tables	To use triggers
Create tablespace	Server Admin	To create/alter/drop tablespaces
Update	Tables	To update existing rows
Set user	Server	To create views and stored routines with a different definer
Federated admin	Server	To execute the CREATE SERVER, ALTER SERVER, DROP SERVER statements
Connection admin	Server	To bypass connection limits and kill other users' connections
Read_only admin	Server	To perform write operations even if @@read_only=ON
Usage	Server Admin	No privileges - allow connect only

可以发现 create session 是没有的，而与 user 相关的操作仅有 create user 这一项，所以在操作时 create session 可以用 create 代替，user 相关的操作用 create user 操作代替，同时显式表明 on 即可

```
MariaDB [sys]> drop user masterA
    -> ;
Query OK, 0 rows affected (0.002 sec)

MariaDB [sys]> create user masterA identified by "key";
Query OK, 0 rows affected (0.002 sec)

MariaDB [sys]> grant create,
    ->       create user,
    ->       alter,
    ->       drop on *.*
    ->       to masterA
    ->       with grant option;
Query OK, 0 rows affected (0.002 sec)
```