《数据库系统原理》实验报告（3）

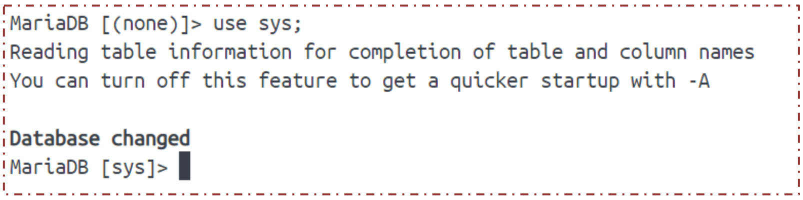
题目：数据库安全性

学号	2154312	姓名	郑博远	日期	2023.10.31

实验环境：**Docker MariaDB**

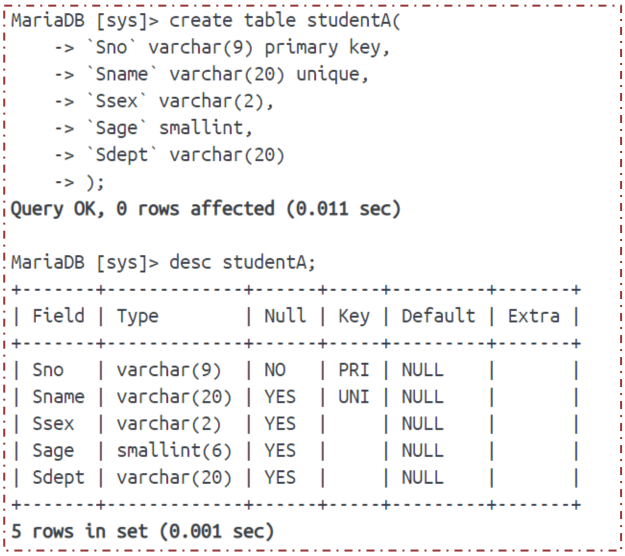
实验步骤及结果截图：

1.进入名为 sys 的数据库：



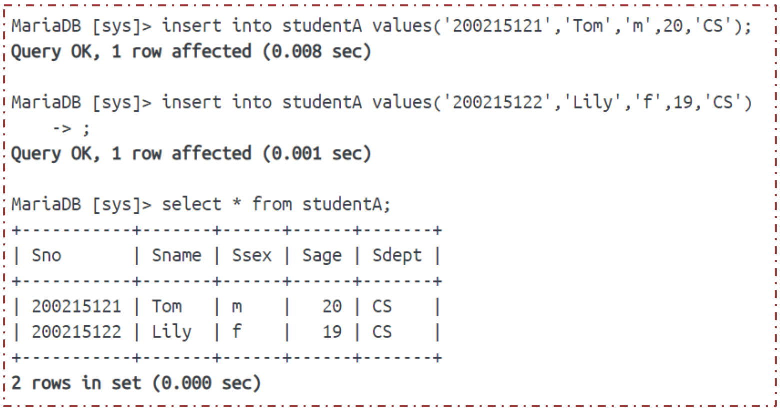
```
MariaDB [(none)]> use sys;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [sys]> 
```

2.在 sys 数据库中，创建表 studentA：



```
MariaDB [sys]> create table studentA(
    -> `Sno` varchar(9) primary key,
    -> `Sname` varchar(20) unique,
    -> `Ssex` varchar(2),
    -> `Sage` smallint,
    -> `Sdept` varchar(20)
    -> );
Query OK, 0 rows affected (0.011 sec)

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 (0.001 sec)
```

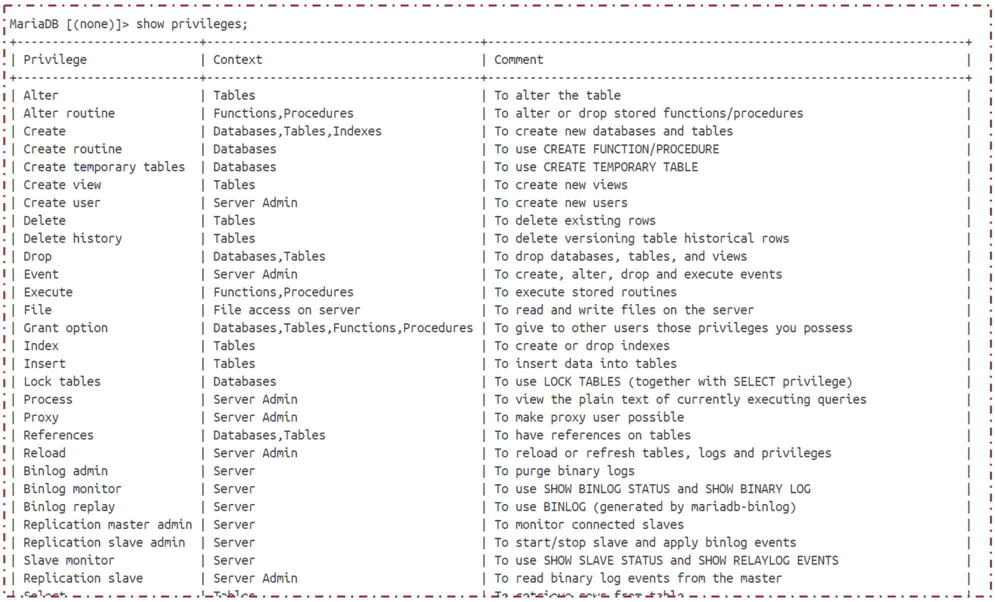
3. 向 table studentA 插入两个元组('200215121','Tom','m',20,'CS')、('200215122','Lily','f',19,'CS')。并查询：



```
MariaDB [sys]> insert into studentA values('200215121','Tom','m',20,'CS');
Query OK, 1 row affected (0.008 sec)

MariaDB [sys]> insert into studentA values('200215122','Lily','f',19,'CS')
    -> ;
Query OK, 1 row affected (0.001 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 (0.000 sec)
```

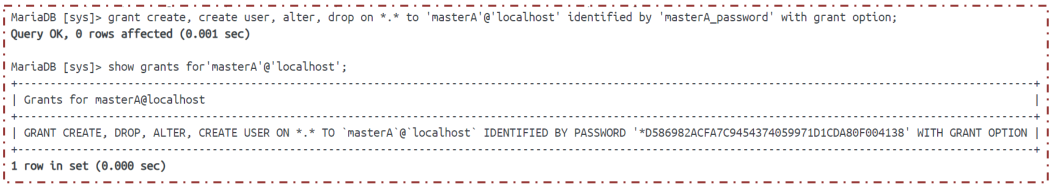
4. 建立用户 masterA，授予用户 masterA 以系统特权，包括 create session、create table、create user、alter user 和 drop user 等，并赋予其再授权的能力。

MariaDB 中，所对应的系统特权与任务要求略有不同。可以通过“show privileges”命令查看：



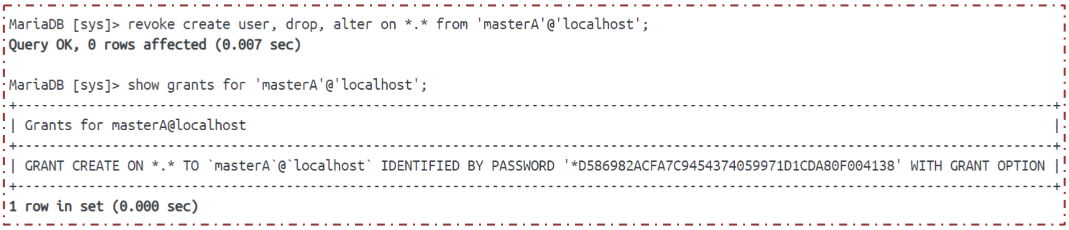
```
MariaDB [(none)]> show privileges;
+--------------------------+---------------------------------------+-------------------------------------------------------+
| Privilege                | Context                               | Comment                                               |
+--------------------------+---------------------------------------+-------------------------------------------------------+
| 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                           |
```

可以观察到不存在“create session”、“create table”指令，此处用“create”指令替代。“create user”指令即涵盖了 alter、drop 的权限，此处为方便后一个实验任务中进行删除，对“masterA”用户赋予“alter”、“drop”权限（权限内容不同，只是为了后一个任务中左删除）：



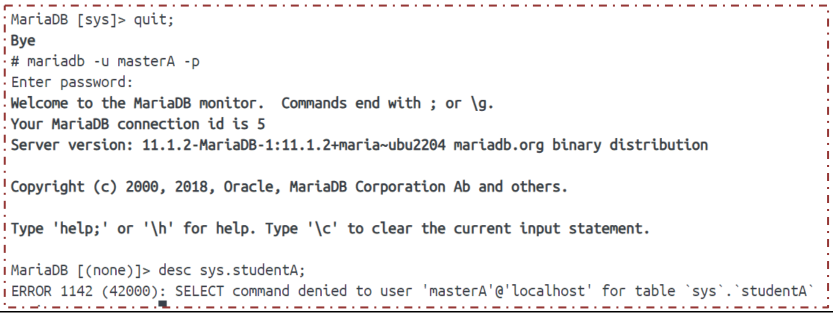
```
MariaDB [sys]> grant create, create user, alter, drop on *.* to 'masterA'@'localhost' identified by 'masterA_password' with grant option;
Query OK, 0 rows affected (0.001 sec)

MariaDB [sys]> show grants for'masterA'@'localhost';
+---------------------------------------------------------------------------------------------------------------------------------+
| Grants for masterA@localhost                                                                                                    |
+---------------------------------------------------------------------------------------------------------------------------------+
| GRANT CREATE, DROP, ALTER, CREATE USER ON *.* TO `masterA`@`localhost` IDENTIFIED BY PASSWORD '*D586982ACFA7C9454374059971D1CDA80F004138' WITH GRANT OPTION |
+---------------------------------------------------------------------------------------------------------------------------------+
1 row in set (0.000 sec)
```

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



```
MariaDB [sys]> revoke create user, drop, alter on *.* from 'masterA'@'localhost';
Query OK, 0 rows affected (0.007 sec)

MariaDB [sys]> show grants for 'masterA'@'localhost';
+----------------------------------------------------------------------------------------------------------------------------+
| Grants for masterA@localhost                                                                                               |
+----------------------------------------------------------------------------------------------------------------------------+
| GRANT CREATE ON *.* TO `masterA`@`localhost` IDENTIFIED BY PASSWORD '*D586982ACFA7C9454374059971D1CDA80F004138' WITH GRANT OPTION |
+----------------------------------------------------------------------------------------------------------------------------+
1 row in set (0.000 sec)
```

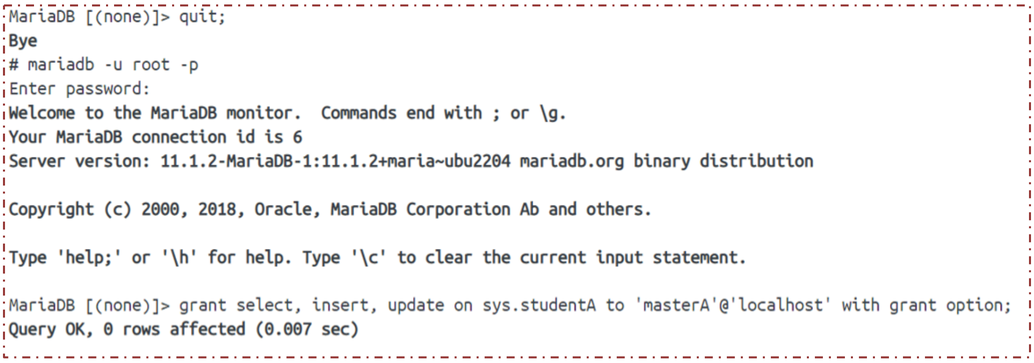
6. 在 masterA 用户下尝试查询 table studentA(注意使用 sys.studentA):



```
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 5
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)]> desc sys.studentA;
ERROR 1142 (42000): SELECT command denied to user 'masterA'@'localhost' for table `sys`.`studentA`
```

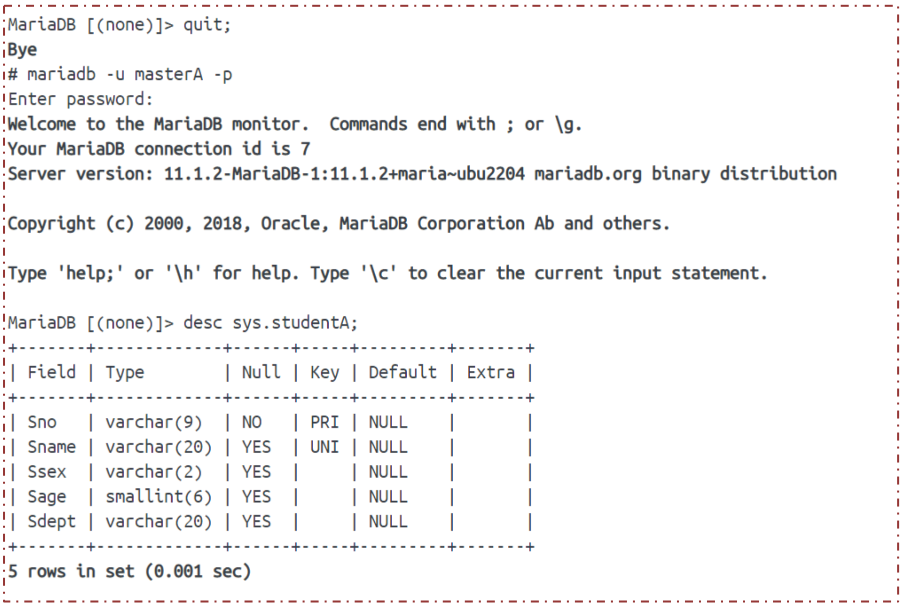
观察到由于“masterA”用户没有 select 权限，无法查询 table studentA。

7. 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：



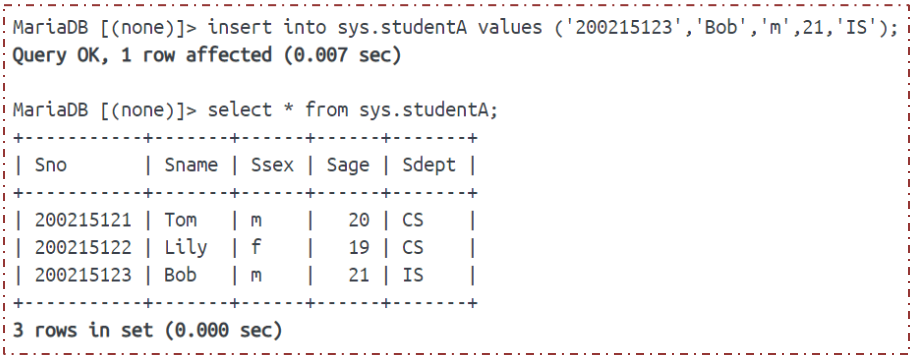
```
MariaDB [(none)]> quit;
Bye
# mariadb -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 6
Server version: 11.1.2-MariaDB-1:11.1.2+maria~ubu2204 mariadb.org binary distribution

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)]> grant select, insert, update on sys.studentA to 'masterA'@'localhost' with grant option;
Query OK, 0 rows affected (0.007 sec)
```

8. 在 masterA 用户下查询 sys.studentA(注意使用 sys.studentA)：



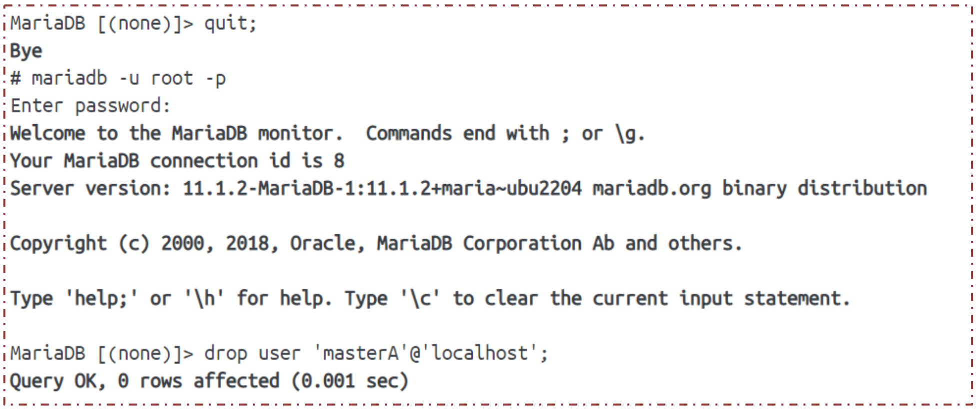
```
MariaDB [(none)]> quit;
Bye
# mariadb -u masterA -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 7
Server version: 11.1.2-MariaDB-1:11.1.2+maria~ubu2204 mariadb.org binary distribution

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)]> desc sys.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 (0.001 sec)
```

9. 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 (0.007 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)
```

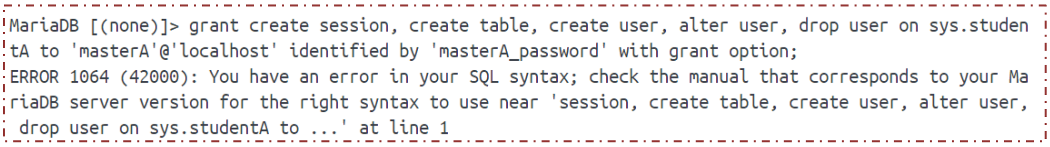
10.删除今天创建的 masterA 用户：



```
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 8
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'@'localhost';
Query OK, 0 rows affected (0.001 sec)
```

出现的问题：

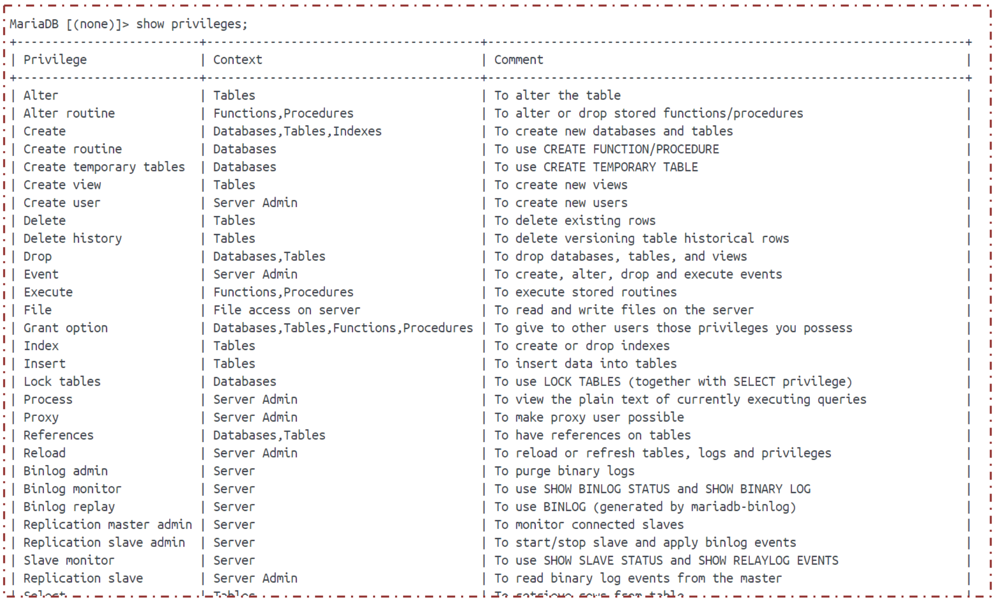
1.　对“masterA”用户赋予实验中要求的权限会报错：



```
MariaDB [(none)]> grant create session, create table, create user, alter user, drop user on sys.studen
tA to 'masterA'@'localhost' identified by 'masterA_password' with grant option;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your Ma
riaDB server version for the right syntax to use near 'session, create table, create user, alter user,
 drop user on sys.studentA to ...' at line 1
```

解决方案：

1. MariaDB 中，所对应的系统特权与任务要求略有不同。可以通过“show privileges”命令查看：



```
MariaDB [(none)]> show privileges;
+--------------------------+---------------------------------------+-------------------------------------------------------+
| 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
```

可以观察到不存在“**create session**”、“**create table**”指令，“**create**”指令即可涵盖对 **databases**、**indexes** 以及 **tables** 的创建权限。此外，也不存在“**alter user**”、“**drop user**”的系统特权，“**create user**”指令即涵盖了“**alter user**”、“**drop user**”的权限。在实验时，选用其他的特权进行替代。