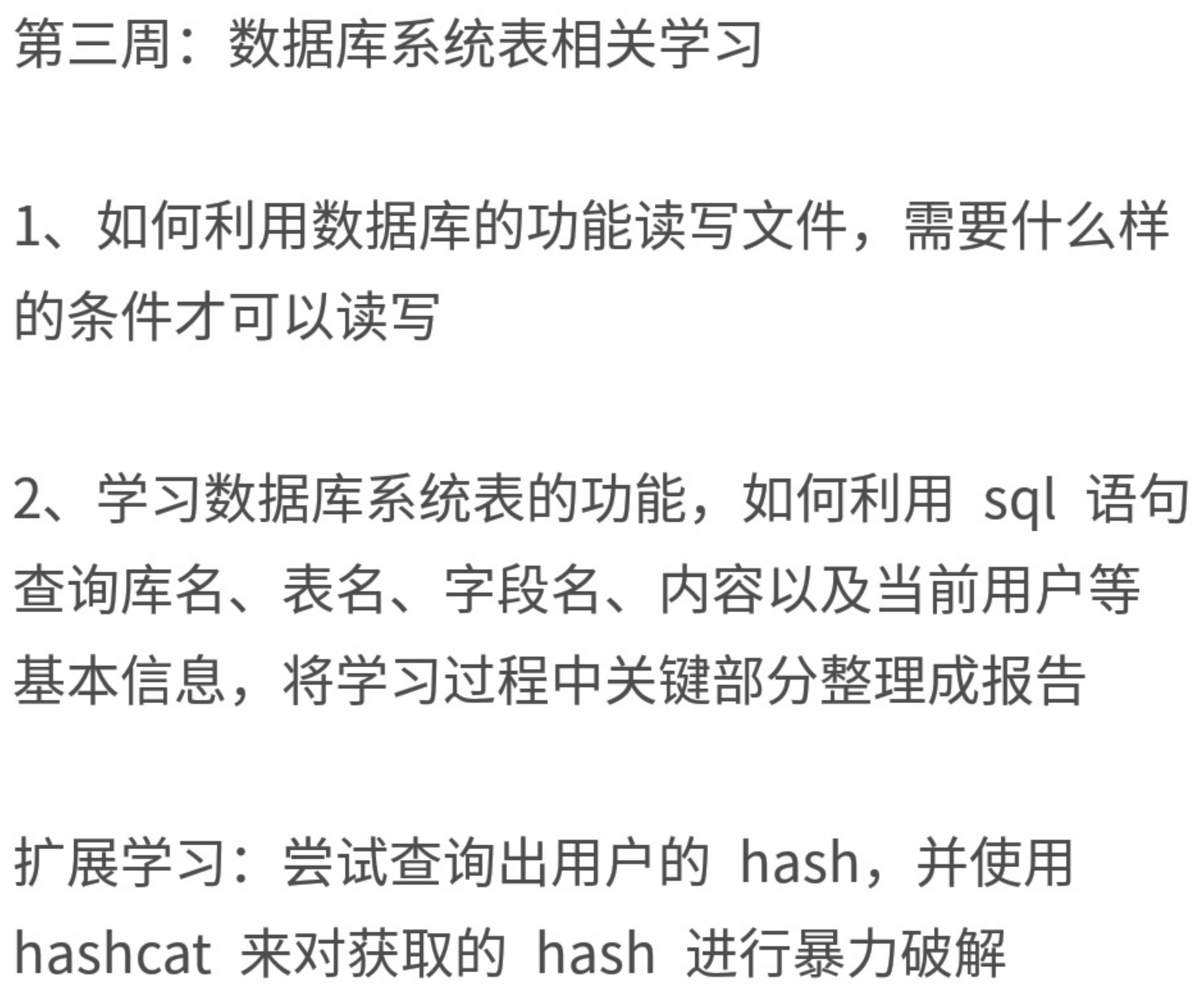
信安之路

第03周

前言

这周自主研究的任务如下：



第三周：数据库系统表相关学习

1、如何利用数据库的功能读写文件，需要什么样的条件才可以读写

2、学习数据库系统表的功能，如何利用 sql 语句查询库名、表名、字段名、内容以及当前用户等基本信息，将学习过程中关键部分整理成报告

扩展学习：尝试查询出用户的 hash，并使用 hashcat 来对获取的 hash 进行暴力破解

任务附录的解释：

1. 文件读写在通过数据库注入漏洞获取webshell的时候很有用
2. 系统库和表存放了很多关键信息，在利用注入漏洞获取更多信息和权限的过程很有帮助
    - eg：库信息、表信息、用户信息、权限信息、安装配置信息
3. 用户信息表一般密码都是hash加密过的，可以利用hashcat暴力破解（GPU）

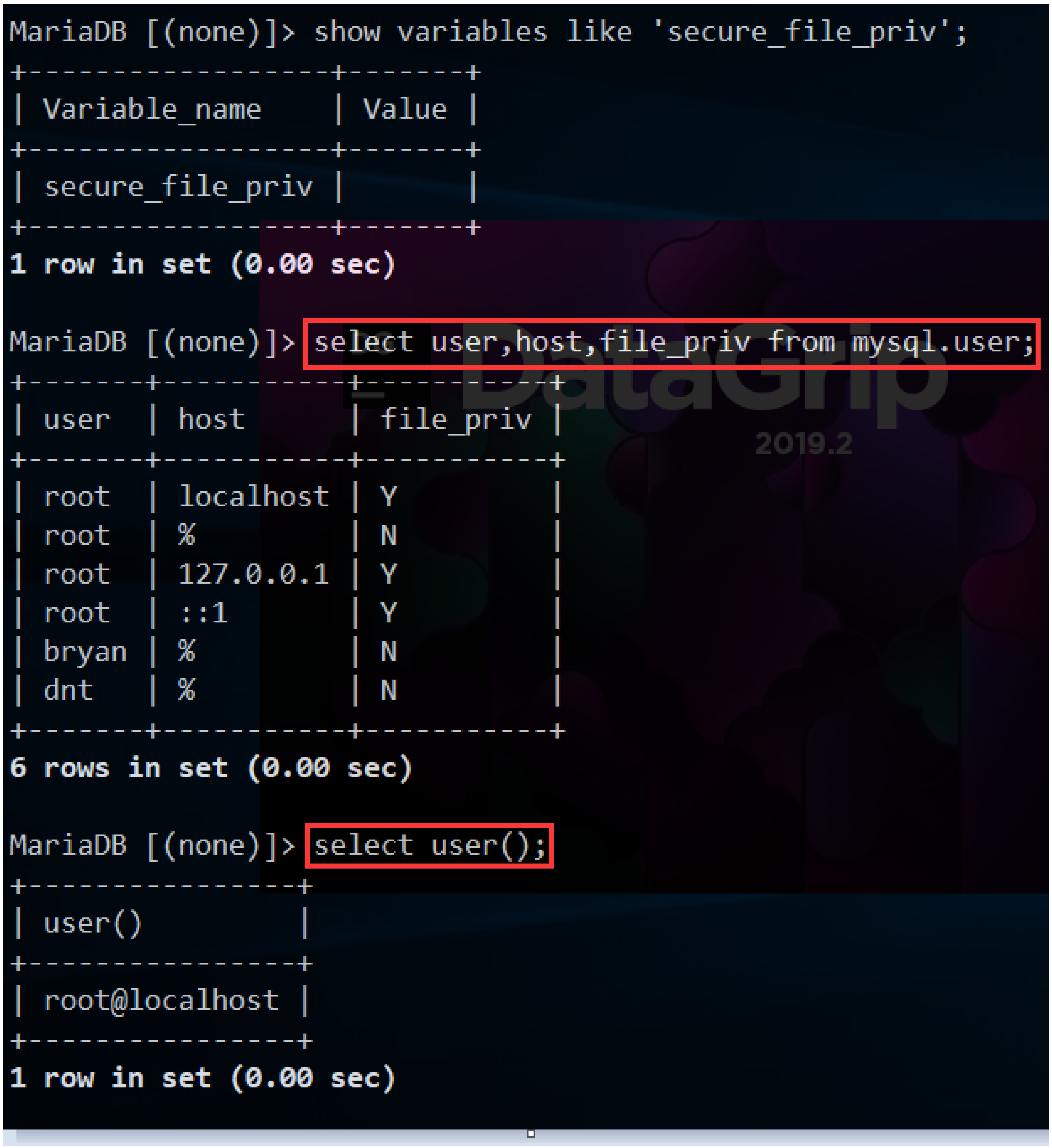
1.文件操作相关

1.1.探索与发现

需要什么权限才可以进行**文件读写操作**，看个简单测试：

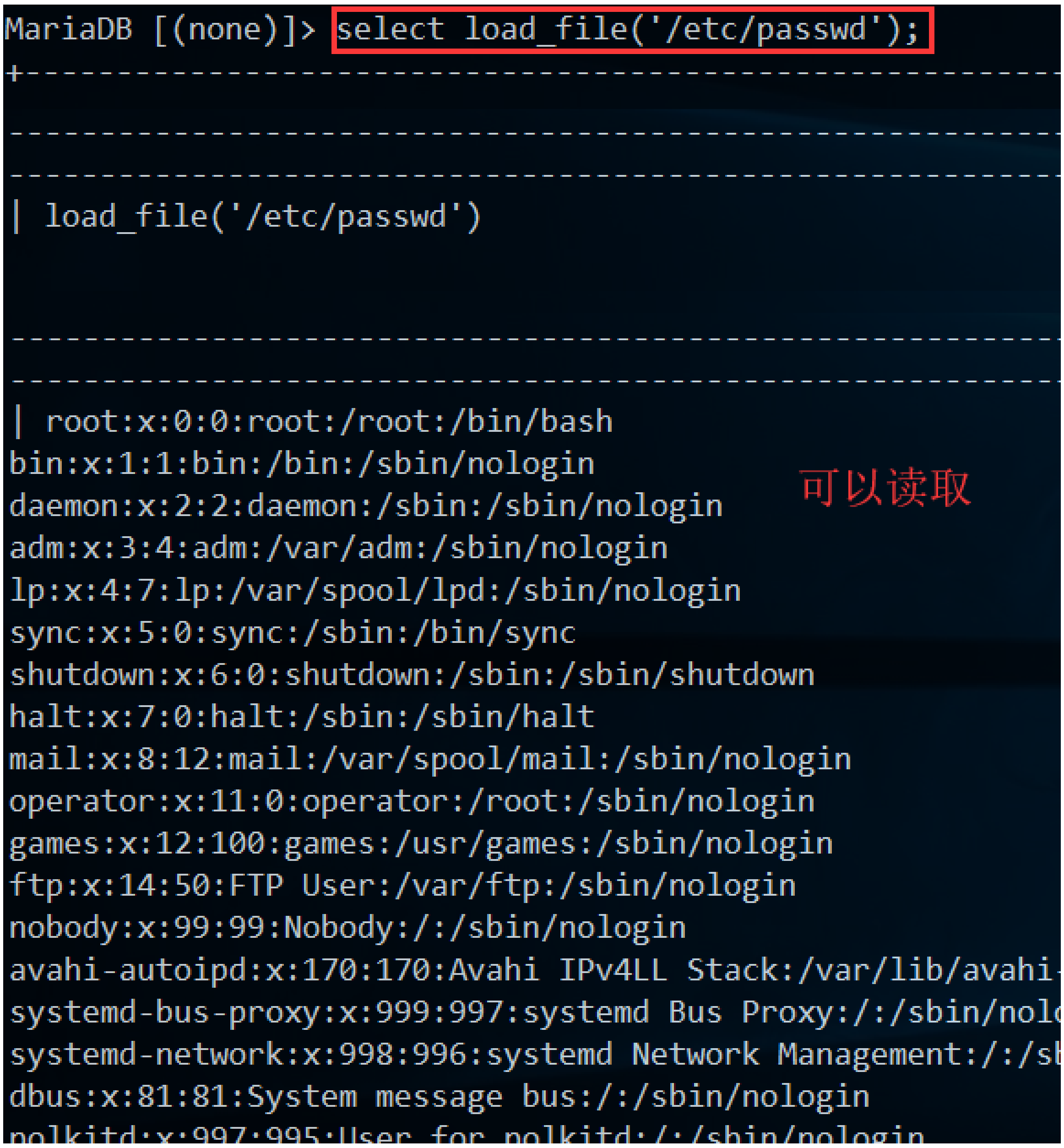
> 读写前提： `secure_file_priv` 不为 `NULL` 、用户具有 `File` 权限（ `mysql.user` 中用户的 `file_priv=Y` ）

先看权限：



```
MariaDB [(none)]> show variables like 'secure_file_priv';
+------------------+-------+
| Variable_name    | Value |
+------------------+-------+
| secure_file_priv |       |
+------------------+-------+
1 row in set (0.00 sec)

MariaDB [(none)]> select user,host,file_priv from mysql.user;
+-------+-----------+-----------+
| user  | host      | file_priv |
+-------+-----------+-----------+
| root  | localhost | Y         |
| root  | %         | N         |
| root  | 127.0.0.1 | Y         |
| root  | ::1       | Y         |
| bryan | %         | N         |
| dnt   | %         | N         |
+-------+-----------+-----------+
6 rows in set (0.00 sec)

MariaDB [(none)]> select user();
+----------------+
| user()         |
+----------------+
| root@localhost |
+----------------+
1 row in set (0.00 sec)
```

`root@localhost` 账号直接可以读取文件



```
MariaDB [(none)]> select load_file('/etc/passwd');
+-------------------------------------------------------------
-------------------------------------------------------------
-------------------------------------------------------------
| load_file('/etc/passwd')

-------------------------------------------------------------
-------------------------------------------------------------
| root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
avahi-autoipd:x:170:170:Avahi IPv4LL Stack:/var/lib/avahi
systemd-bus-proxy:x:999:997:systemd Bus Proxy:/:/sbin/nol
systemd-network:x:998:996:systemd Network Management:/:/s
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:997:995:User for polkitd:/:/sbin/nologin
```

命令附录：

```
show variables like 'secure_file_priv';
select user,host,file_priv from mysql.user;
select load_file("etc/passwd");
```

1.2.参数说明

secure_file_priv的简单说明：

> PS： `MariaDB5.x` 默认为空，

1. secure_file_priv= `NULL`
   - 表示**不允许**文件读写
2. secure_file_priv= `/xxx` （ `/` 则代表任意目录读写）
   - 表示只能在**指定目录** `/xxx` 中文件读写，其他目录不行
3. secure_file_priv**为空**时

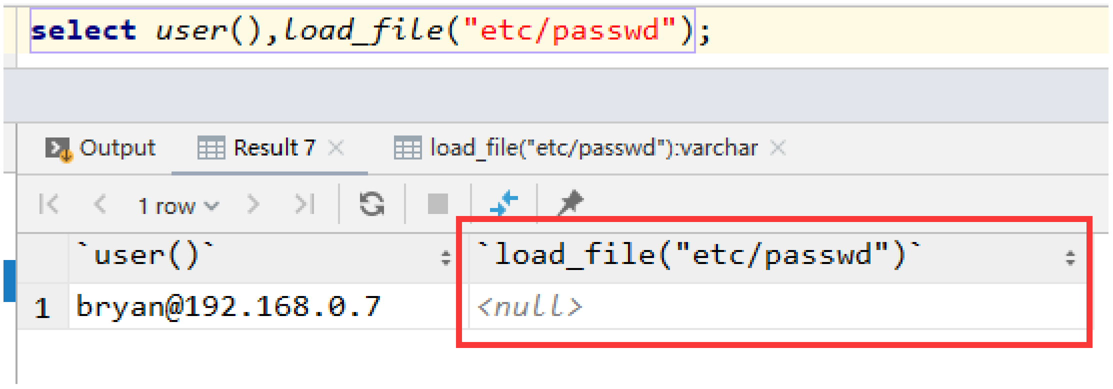
- 表示可在**任意目录**文件读写

PS：**目标文件大小**必须小于 `select @@max_allowed_packet;` 的值

```
# MariaDB默认值
MariaDB [(none)]> select @@max_allowed_packet;
+----------------------+
| @@max_allowed_packet |
+----------------------+
|              1048576 |
+----------------------+
1 row in set (0.00 sec)
```

1.3.用户授权

bryan账号本来是没 `file` 权限的（`file_priv=N`）

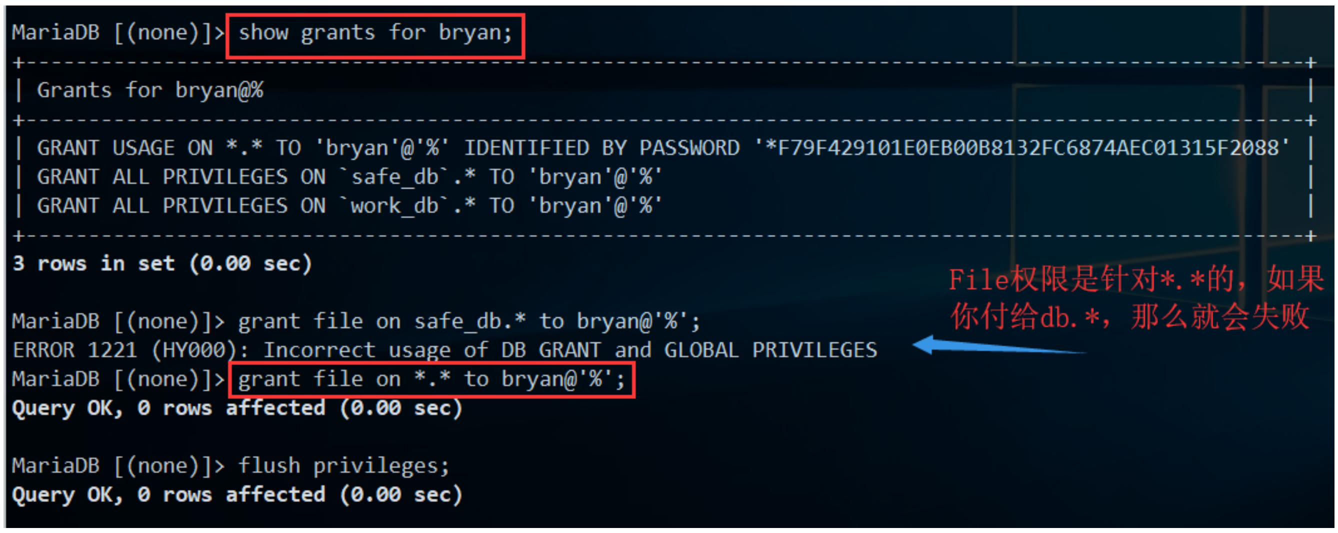


```
select user(),load_file("etc/passwd");
```

```
  `user()`               `load_file("etc/passwd")`
1 bryan@192.168.0.7      <null>
```

我们授权一下：`grant file on *.* to bryan@'%';`

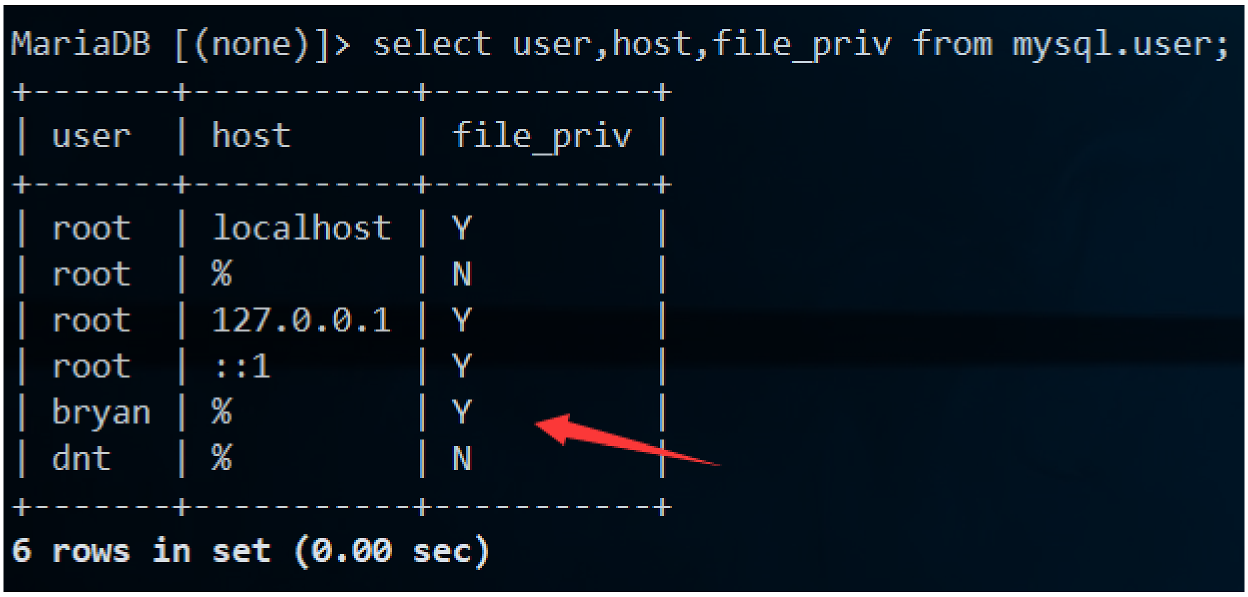
> PS：查看数据库支持哪些权限：`show privileges;`、刷新权限：`flush privileges;`



```
MariaDB [(none)]> show grants for bryan;
+-----------------------------------------------------------------------------------------------------------+
| Grants for bryan@%                                                                                        |
+-----------------------------------------------------------------------------------------------------------+
| GRANT USAGE ON *.* TO 'bryan'@'%' IDENTIFIED BY PASSWORD '*F79F429101E0EB00B8132FC6874AEC01315F2088' |
| GRANT ALL PRIVILEGES ON `safe_db`.* TO 'bryan'@'%'                                                     |
| GRANT ALL PRIVILEGES ON `work_db`.* TO 'bryan'@'%'                                                     |
+-----------------------------------------------------------------------------------------------------------+
3 rows in set (0.00 sec)

MariaDB [(none)]> grant file on safe_db.* to bryan@'%';
ERROR 1221 (HY000): Incorrect usage of DB GRANT and GLOBAL PRIVILEGES
MariaDB [(none)]> grant file on *.* to bryan@'%';
Query OK, 0 rows affected (0.00 sec)

MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0.00 sec)
```

这时候用root权限查看下 `bryan` 的 `file_priv` 就会发现有权限了

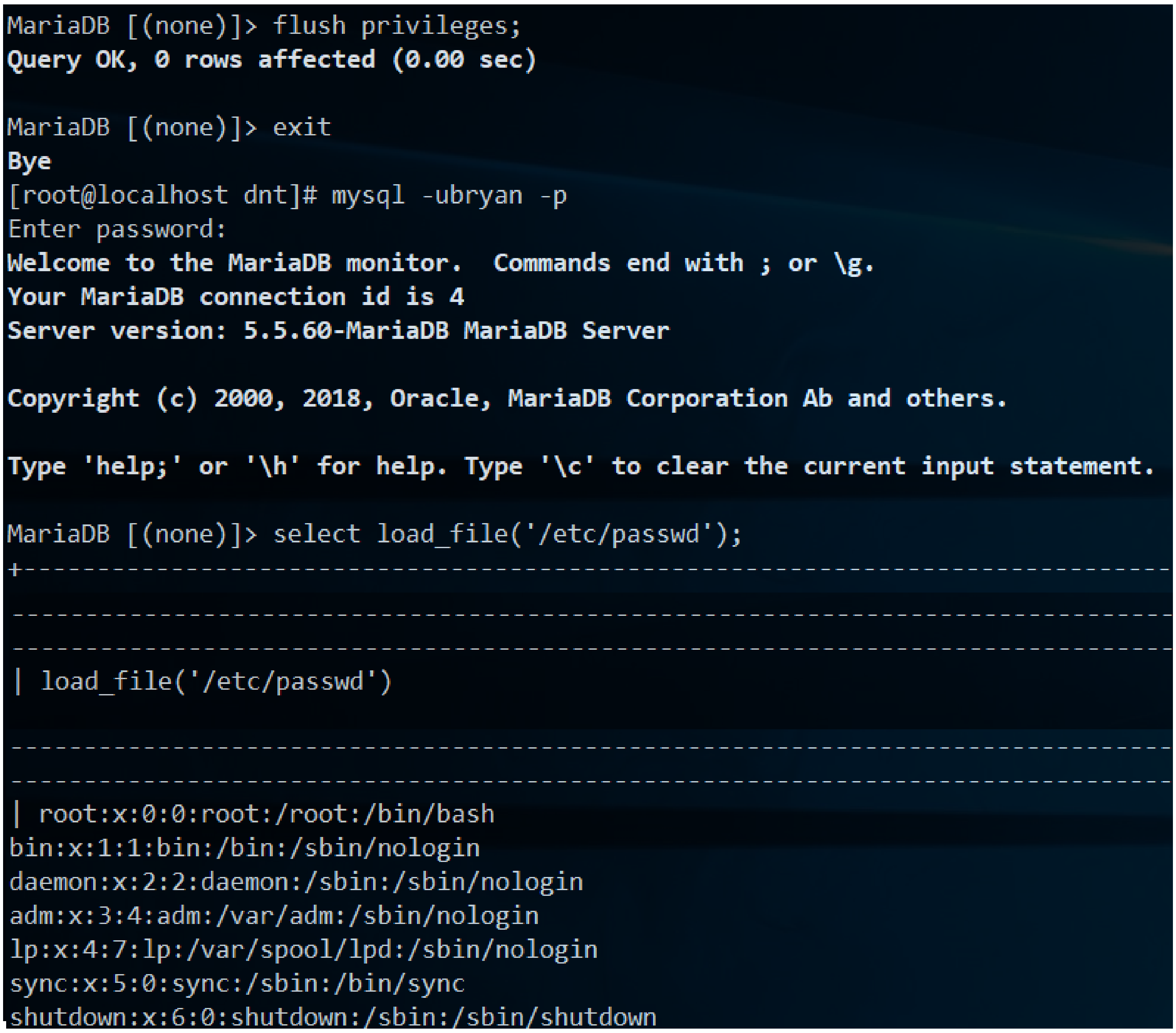
> PS：**回收权限**：`revoke file from *.* from bryan@'%'`



```
MariaDB [(none)]> select user,host,file_priv from mysql.user;
+-------+-----------+-----------+
| user  | host      | file_priv |
+-------+-----------+-----------+
| root  | localhost | Y         |
| root  | %         | N         |
| root  | 127.0.0.1 | Y         |
| root  | ::1       | Y         |
| bryan | %         | Y         |
| dnt   | %         | N         |
+-------+-----------+-----------+
6 rows in set (0.00 sec)
```

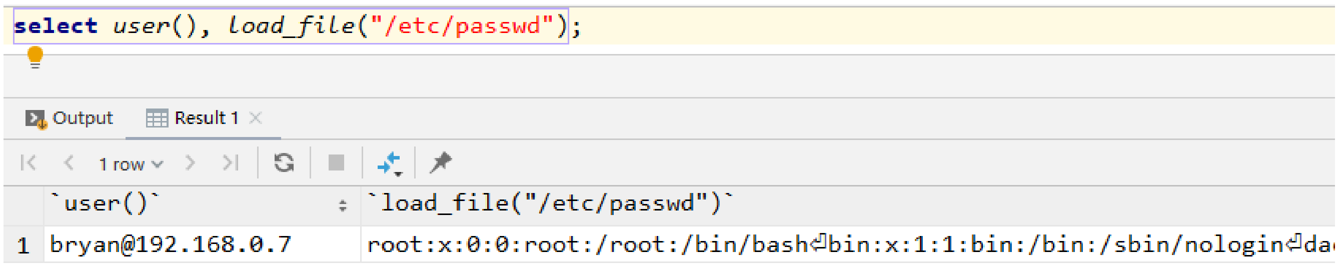
1.4. `load_file` 测试

本地测试： `bryan@localhost`



```
MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0.00 sec)

MariaDB [(none)]> exit
Bye
[root@localhost dnt]# mysql -ubryan -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 4
Server version: 5.5.60-MariaDB MariaDB Server

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 load_file('/etc/passwd');
+---------------------------------------------------------------------------------
---------------------------------------------------------------------------------
---------------------------------------------------------------------------------
| load_file('/etc/passwd')

---------------------------------------------------------------------------------
---------------------------------------------------------------------------------
| root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
```

远程测试：`bryan@'%'`（重开一个查询窗口/会话）



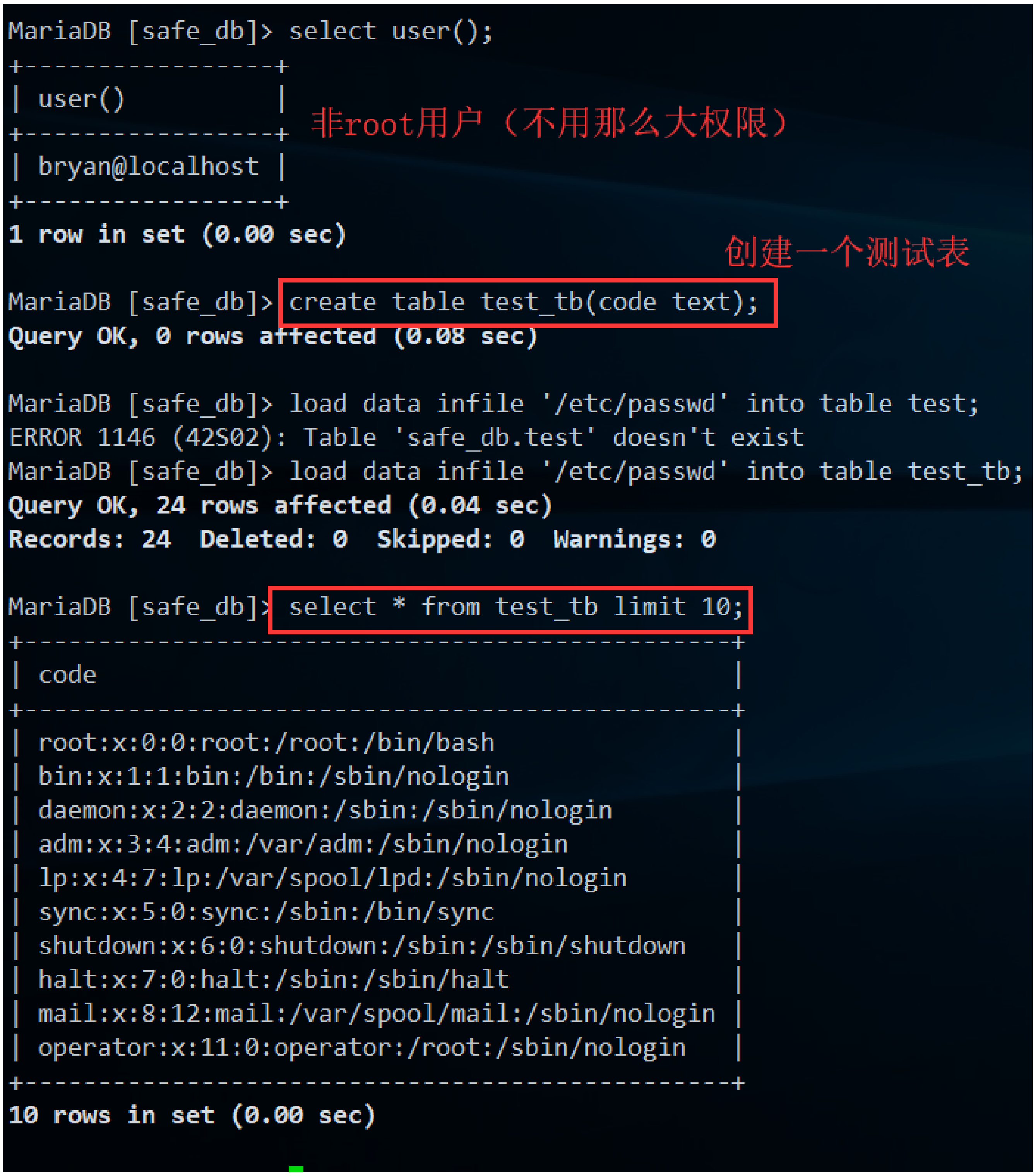
```
select user(), load_file("/etc/passwd");
```

```
   `user()`            `load_file("/etc/passwd")`
1  bryan@192.168.0.7   root:x:0:0:root:/root:/bin/bash⏎bin:x:1:1:bin:/bin:/sbin/nologin⏎da
```

1.5. `load data infile` 测试

`load data infile` 的主要作用就是**从一个文本文件中读取行，并写入一个表中**

> 语法：`load data infile '文件路径' into table 表名;`

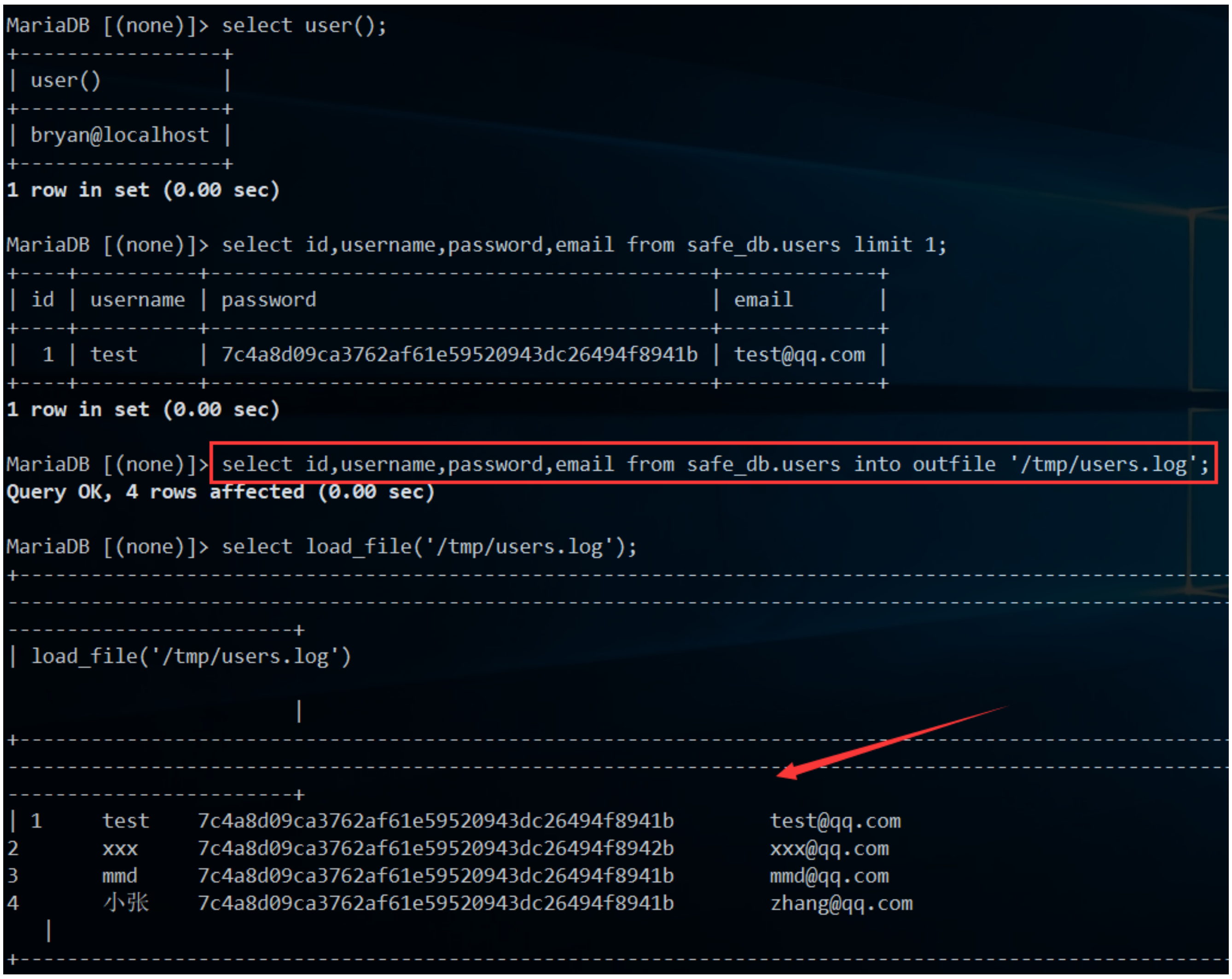


```
MariaDB [safe_db]> select user();
+-----------------+
| user()          |
+-----------------+
| bryan@localhost |
+-----------------+
1 row in set (0.00 sec)

MariaDB [safe_db]> create table test_tb(code text);
Query OK, 0 rows affected (0.08 sec)

MariaDB [safe_db]> load data infile '/etc/passwd' into table test;
ERROR 1146 (42S02): Table 'safe_db.test' doesn't exist
MariaDB [safe_db]> load data infile '/etc/passwd' into table test_tb;
Query OK, 24 rows affected (0.04 sec)
Records: 24  Deleted: 0  Skipped: 0  Warnings: 0

MariaDB [safe_db]> select * from test_tb limit 10;
+------------------------------------------------+
| code                                           |
+------------------------------------------------+
| root:x:0:0:root:/root:/bin/bash                |
| bin:x:1:1:bin:/bin:/sbin/nologin               |
| daemon:x:2:2:daemon:/sbin:/sbin/nologin        |
| adm:x:3:4:adm:/var/adm:/sbin/nologin           |
| lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin       |
| sync:x:5:0:sync:/sbin:/bin/sync                |
| shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown   |
| halt:x:7:0:halt:/sbin:/sbin/halt               |
| mail:x:8:12:mail:/var/spool/mail:/sbin/nologin |
| operator:x:11:0:operator:/root:/sbin/nologin   |
+------------------------------------------------+
10 rows in set (0.00 sec)
```

1.6. `select into outfile` 测试

`select into outfile` 主要作用就是：**把查询写入文件中**

> 语法： `select * from 表名 into outfile '权限范围内文件路径';`

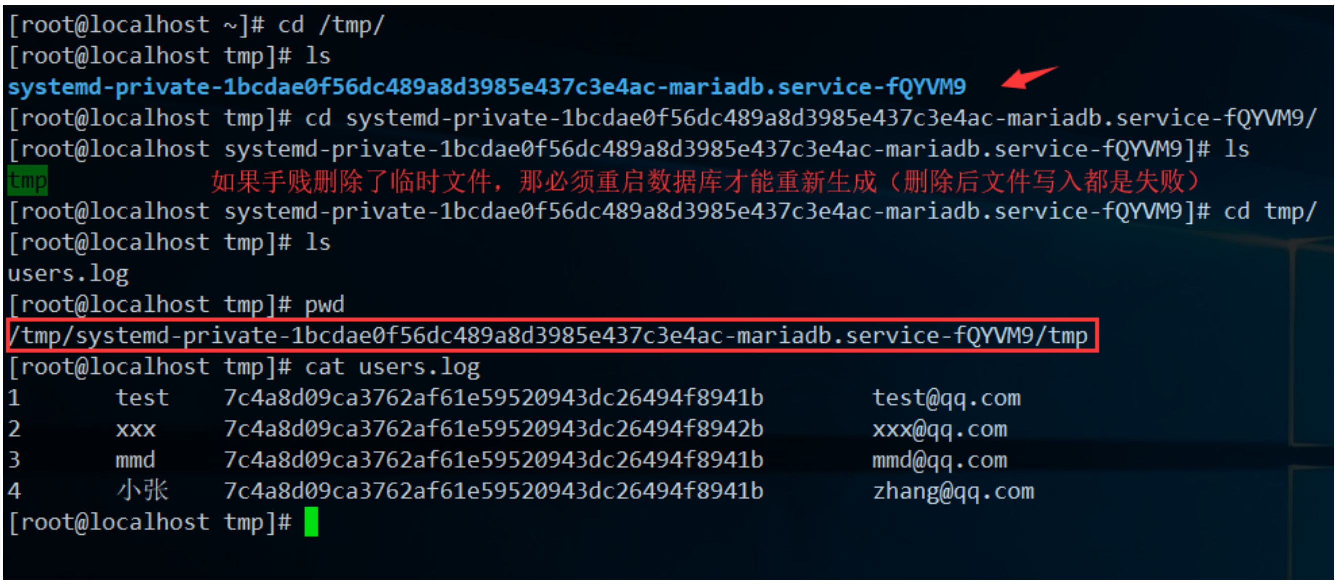


```
MariaDB [(none)]> select user();
+----------------+
| user()         |
+----------------+
| bryan@localhost |
+----------------+
1 row in set (0.00 sec)

MariaDB [(none)]> select id,username,password,email from safe_db.users limit 1;
+----+----------+------------------------------------------+-------------+
| id | username | password                                 | email       |
+----+----------+------------------------------------------+-------------+
|  1 | test     | 7c4a8d09ca3762af61e59520943dc26494f8941b | test@qq.com |
+----+----------+------------------------------------------+-------------+
1 row in set (0.00 sec)

MariaDB [(none)]> select id,username,password,email from safe_db.users into outfile '/tmp/users.log';
Query OK, 4 rows affected (0.00 sec)

MariaDB [(none)]> select load_file('/tmp/users.log');
+------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------
-----------------------+
| load_file('/tmp/users.log')
                       |
+------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------
-----------------------+
| 1     test    7c4a8d09ca3762af61e59520943dc26494f8941b        test@qq.com
2       xxx     7c4a8d09ca3762af61e59520943dc26494f8942b        xxx@qq.com
3       mmd     7c4a8d09ca3762af61e59520943dc26494f8941b        mmd@qq.com
4       小张    7c4a8d09ca3762af61e59520943dc26494f8941b        zhang@qq.com
   |
+------------------------------------------------------------------------------------------
```

PS：**如果文件已经存在则写入失败**

> 删除了临时文件夹创建也会失败，必须重启数据库，或者创建文件夹后改成mysql所有

系统中真正路径：



```
[root@localhost ~]# cd /tmp/
[root@localhost tmp]# ls
systemd-private-1bcdae0f56dc489a8d3985e437c3e4ac-mariadb.service-fQYVM9
[root@localhost tmp]# cd systemd-private-1bcdae0f56dc489a8d3985e437c3e4ac-mariadb.service-fQYVM9/
[root@localhost systemd-private-1bcdae0f56dc489a8d3985e437c3e4ac-mariadb.service-fQYVM9]# ls
tmp          如果手贱删除了临时文件，那必须重启数据库才能重新生成（删除后文件写入都是失败）
[root@localhost systemd-private-1bcdae0f56dc489a8d3985e437c3e4ac-mariadb.service-fQYVM9]# cd tmp/
[root@localhost tmp]# ls
users.log
[root@localhost tmp]# pwd
/tmp/systemd-private-1bcdae0f56dc489a8d3985e437c3e4ac-mariadb.service-fQYVM9/tmp
[root@localhost tmp]# cat users.log
1       test    7c4a8d09ca3762af61e59520943dc26494f8941b        test@qq.com
2       xxx     7c4a8d09ca3762af61e59520943dc26494f8942b        xxx@qq.com
3       mmd     7c4a8d09ca3762af61e59520943dc26494f8941b        mmd@qq.com
4       小张    7c4a8d09ca3762af61e59520943dc26494f8941b        zhang@qq.com
[root@localhost tmp]#
```

扩展：system命令

mysql命令行下的 `system` 摸索过程：

> PS：任意读 + 权限范围内写（`本地执行` or `SSH连接Linux` 进入 `MySQL` 命令行执行）

渗透思路：

1. 读取某些敏感的配置文件（eg：数据库连接的配置文件）
2. 当有目录越权访问漏洞的时候可以越权执行脚本（权限范围内的目录中写入脚本）

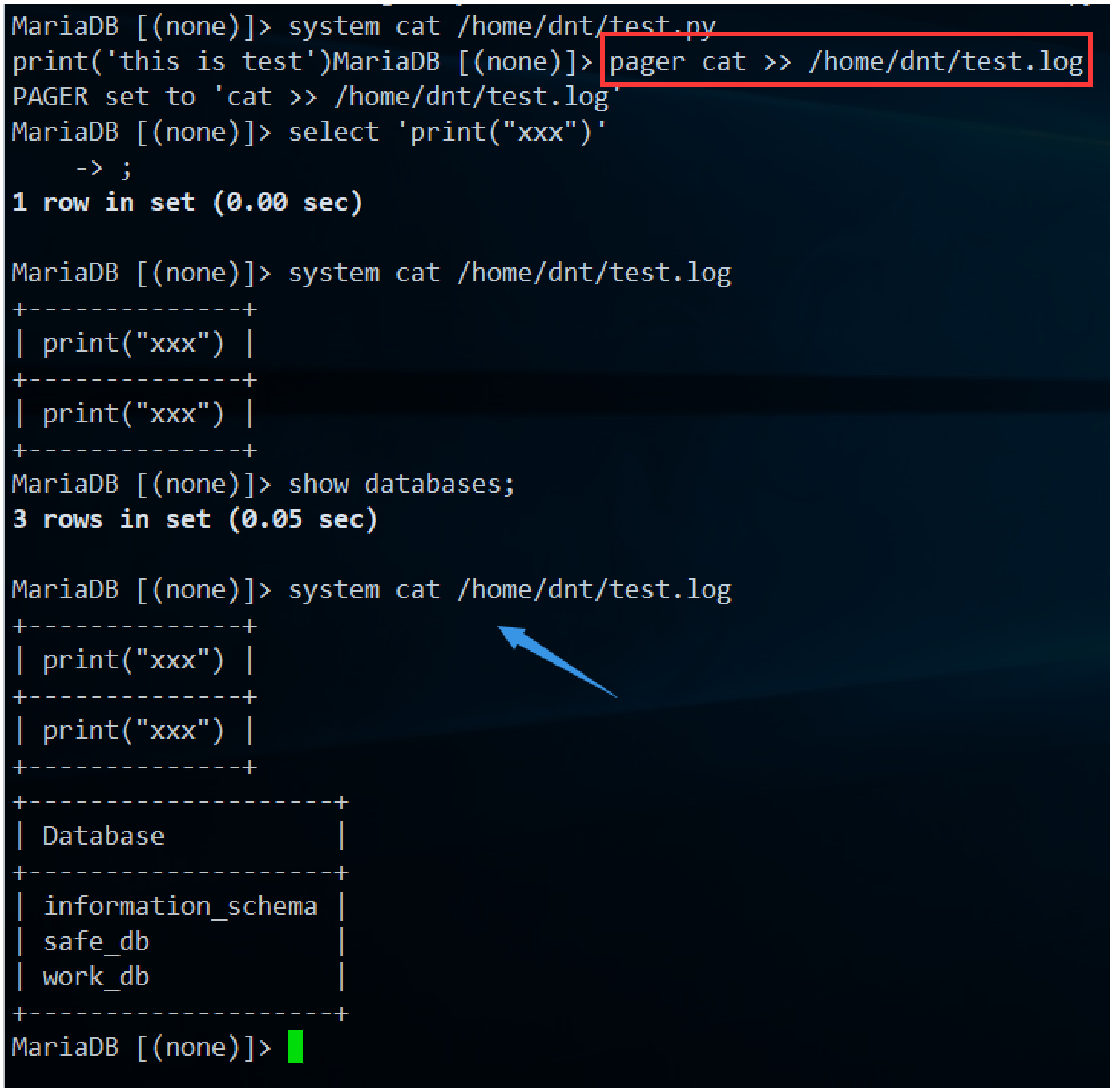
```
PS C:\Users\Mao> ssh -l bryan 192.168.0.9
bryan@192.168.0.9 password:
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 5.0.0-23-generic x86_64)

bryan@bryan-pc:~$ mysql -ubryan -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 10
Server version: 5.7.27-0ubuntu0.18.04.1-log (Ubuntu)

Copyright (c) 2000, 2019, Oracle and/or its affiliates. All rights reserved.

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 user();
+------------------+
| user()           |
+------------------+
| bryan@localhost |
+------------------+
1 row in set (0.06 sec)

# mysql> system ls /home
dnt
# mysql> system ls /var/www/html
index.nginx-debian.html  index.php
# mysql> system cat /var/www/html/index.php
<?php
  phpinfo();
?>
# mysql> system vi /home/bryan/test.py
# mysql> system cat /home/bryan/test.py
print("test")
# mysql> system cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
```

```
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
avahi-autoipd:x:170:170:Avahi IPv4LL Stack:/var/lib/avahi-autoipd:/sbin/nologin
systemd-bus-proxy:x:999:997:systemd Bus Proxy:/:/sbin/nologin
systemd-network:x:998:996:systemd Network Management:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:997:995:User for polkitd:/:/sbin/nologin
tss:x:59:59:Account used by the trousers package to sandbox the tcsd
daemon:/dev/null:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
bryan:x:1000:1000:xxx:/home/bryan:/bin/bash
mysql:x:27:27:MariaDB Server:/var/lib/mysql:/sbin/nologin
nginx:x:1001:1001::/home/nginx:/sbin/nologin
```

扩展命令：pager

重定向查询结果：`pager cat >> /home/dnt/test.log`

> 把查询的结果，全部**追加**写入到指定文件中（只针对当前会话）

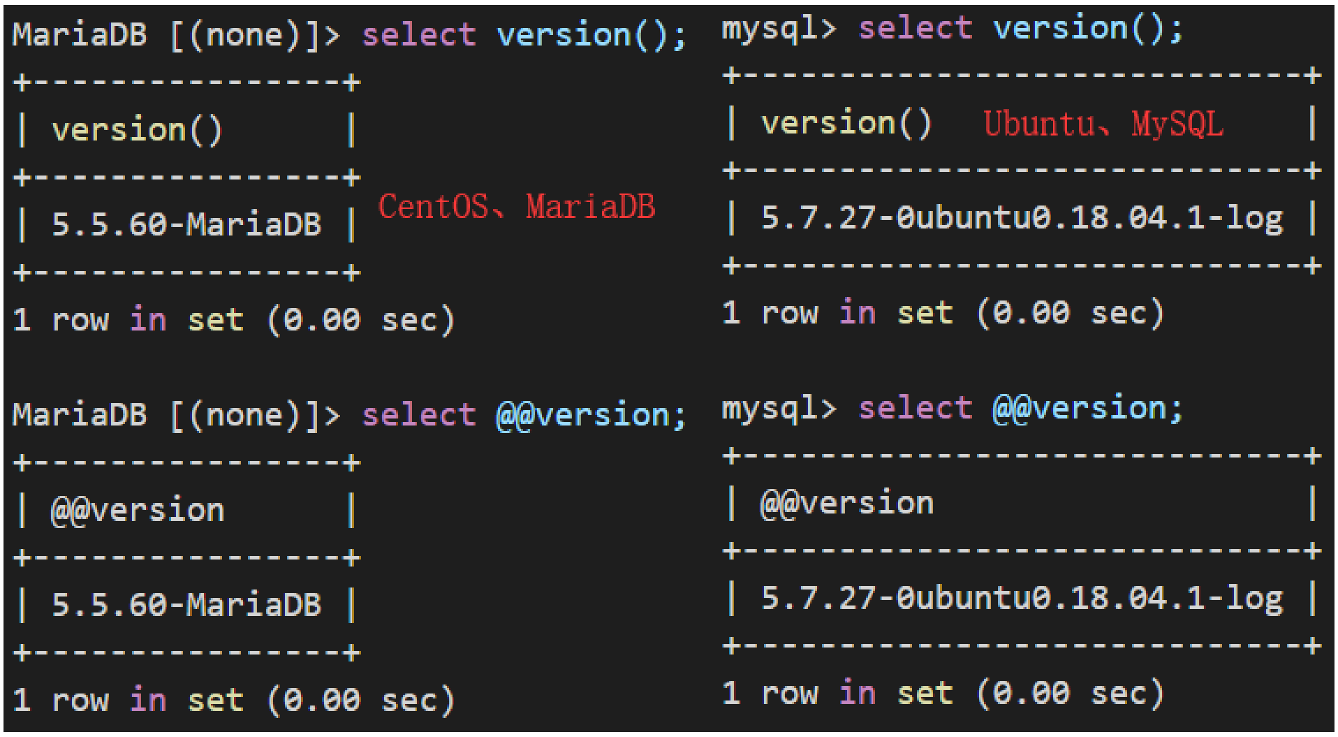


```
MariaDB [(none)]> system cat /home/dnt/test.py
print('this is test')MariaDB [(none)]> pager cat >> /home/dnt/test.log
PAGER set to 'cat >> /home/dnt/test.log'
MariaDB [(none)]> select 'print("xxx")'
    -> ;
1 row in set (0.00 sec)

MariaDB [(none)]> system cat /home/dnt/test.log
+--------------+
| print("xxx") |
+--------------+
| print("xxx") |
+--------------+
MariaDB [(none)]> show databases;
3 rows in set (0.05 sec)

MariaDB [(none)]> system cat /home/dnt/test.log
+--------------+
| print("xxx") |
+--------------+
| print("xxx") |
+--------------+
+--------------------+
| Database           |
+--------------------+
| information_schema |
| safe_db            |
| work_db            |
+--------------------+
MariaDB [(none)]>
```

2.获取系统信息

2.1.获取数据库版本

`select version();` or `select @@version;`



```
MariaDB [(none)]> select version();
+-----------------+
| version()       |
+-----------------+
| 5.5.60-MariaDB  |
+-----------------+
1 row in set (0.00 sec)

MariaDB [(none)]> select @@version;
+-----------------+
| @@version       |
+-----------------+
| 5.5.60-MariaDB  |
+-----------------+
1 row in set (0.00 sec)
```

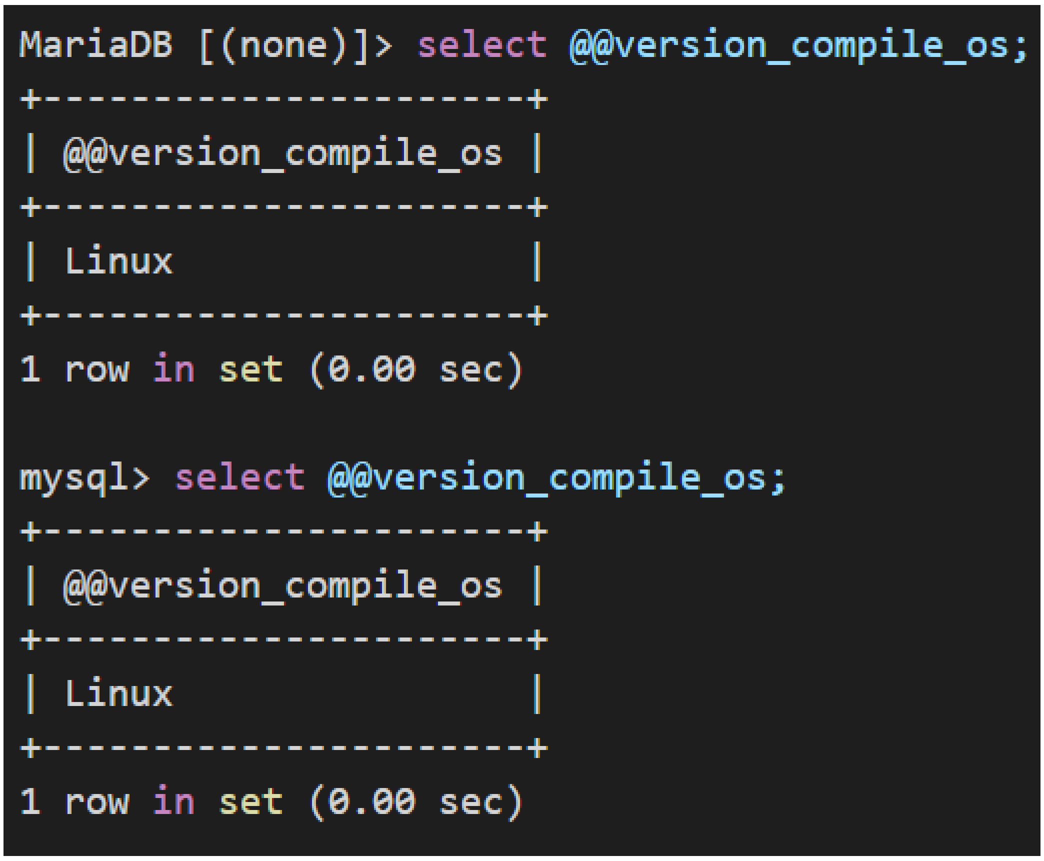
CentOS、MariaDB

```
mysql> select version();
+-------------------------------+
| version()                     |
+-------------------------------+
| 5.7.27-0ubuntu0.18.04.1-log   |
+-------------------------------+
1 row in set (0.00 sec)

mysql> select @@version;
+-------------------------------+
| @@version                     |
+-------------------------------+
| 5.7.27-0ubuntu0.18.04.1-log   |
+-------------------------------+
1 row in set (0.00 sec)
```

Ubuntu、MySQL

2.2.获取操作系统类型

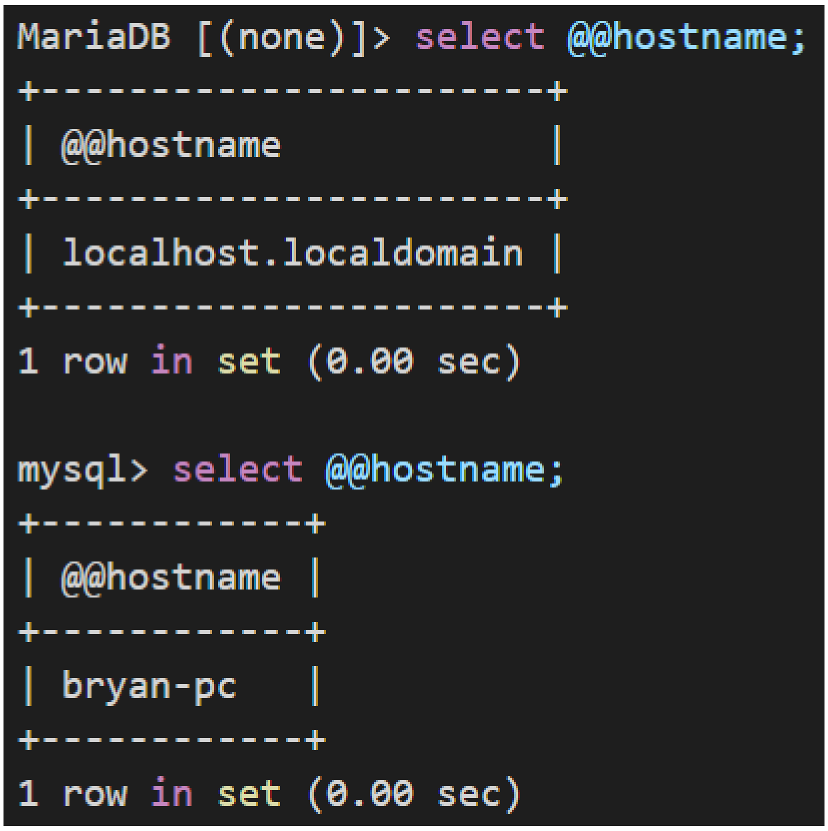
`select @@version_compile_os;`



```
MariaDB [(none)]> select @@version_compile_os;
+----------------------+
| @@version_compile_os |
+----------------------+
| Linux                |
+----------------------+
1 row in set (0.00 sec)

mysql> select @@version_compile_os;
+----------------------+
| @@version_compile_os |
+----------------------+
| Linux                |
+----------------------+
1 row in set (0.00 sec)
```

2.3.获取服务器主机名

`select @@hostname;`



```
MariaDB [(none)]> select @@hostname;
+-----------------------+
| @@hostname            |
+-----------------------+
| localhost.localdomain |
+-----------------------+
1 row in set (0.00 sec)

mysql> select @@hostname;
+------------+
| @@hostname |
+------------+
| bryan-pc   |
+------------+
1 row in set (0.00 sec)
```

3.获取DB信息

3.1.获取数据库列表

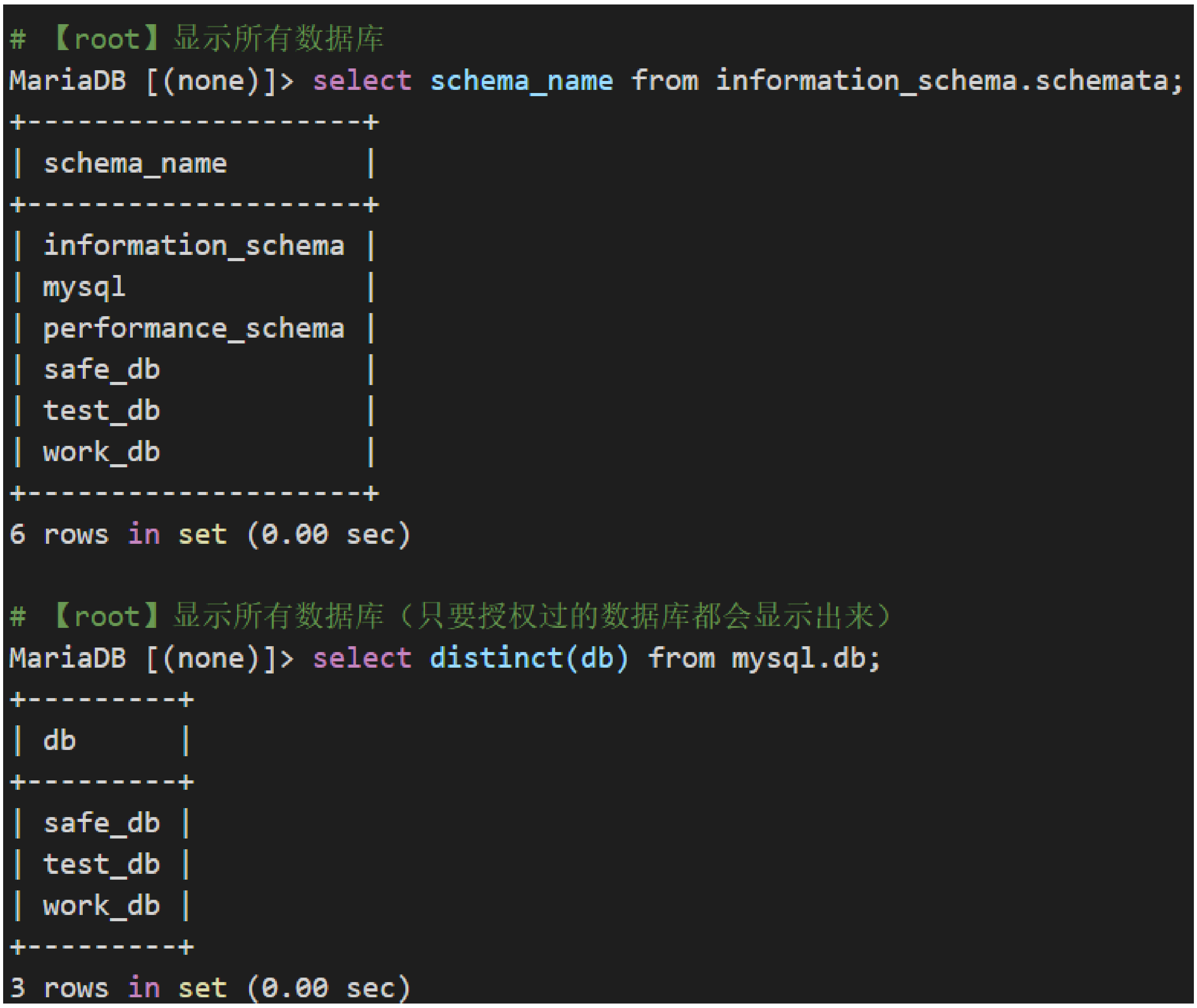
`select schema_name from information_schema.schemata;`

> PS：MySQL5.x可以通过schemata表来查询 `权限范围内` 的数据库

```
# 1.MySQL5.x可以通过schemata表来查询`权限范围内`的数据库
MariaDB [safe_db]> select schema_name from information_schema.schemata;
+--------------------+
| schema_name        |
+--------------------+
| information_schema |
| safe_db            |
| work_db            |
+--------------------+
3 rows in set (0.00 sec)

# 验证如下: show databases;
MariaDB [safe_db]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| safe_db            |
| work_db            |
+--------------------+
3 rows in set (0.00 sec)
```

root权限下获取所有DB列表

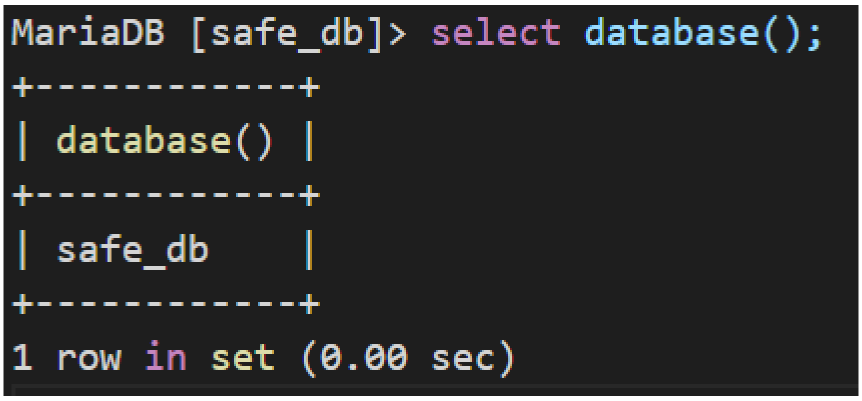
PS：**root权限**可以使用 `select schema_name from information_schema.schemata;` or `select distinct(db) from mysql.db;` 来**显示所有数据库**



```
# 【root】显示所有数据库
MariaDB [(none)]> select schema_name from information_schema.schemata;
+--------------------+
| schema_name        |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| safe_db            |
| test_db            |
| work_db            |
+--------------------+
6 rows in set (0.00 sec)

# 【root】显示所有数据库（只要授权过的数据库都会显示出来）
MariaDB [(none)]> select distinct(db) from mysql.db;
+---------+
| db      |
+---------+
| safe_db |
| test_db |
| work_db |
+---------+
3 rows in set (0.00 sec)
```

3.2.获取当前数据库

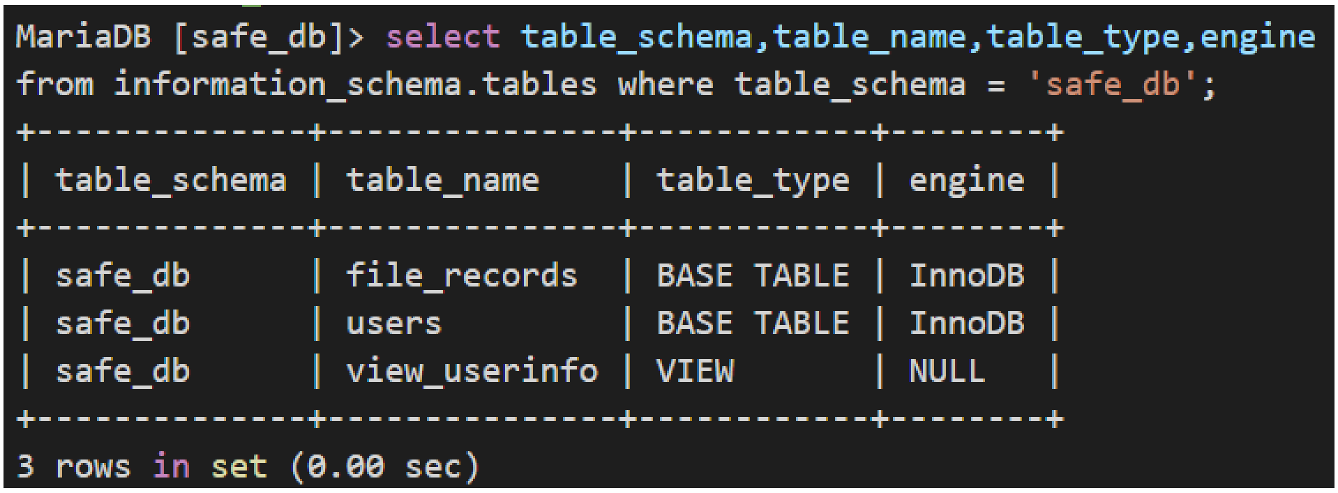
获取正在 `use` 的数据库： `select database();`



```
MariaDB [safe_db]> select database();
+------------+
| database() |
+------------+
| safe_db    |
+------------+
1 row in set (0.00 sec)
```

3.3.获取指定DB有哪些表

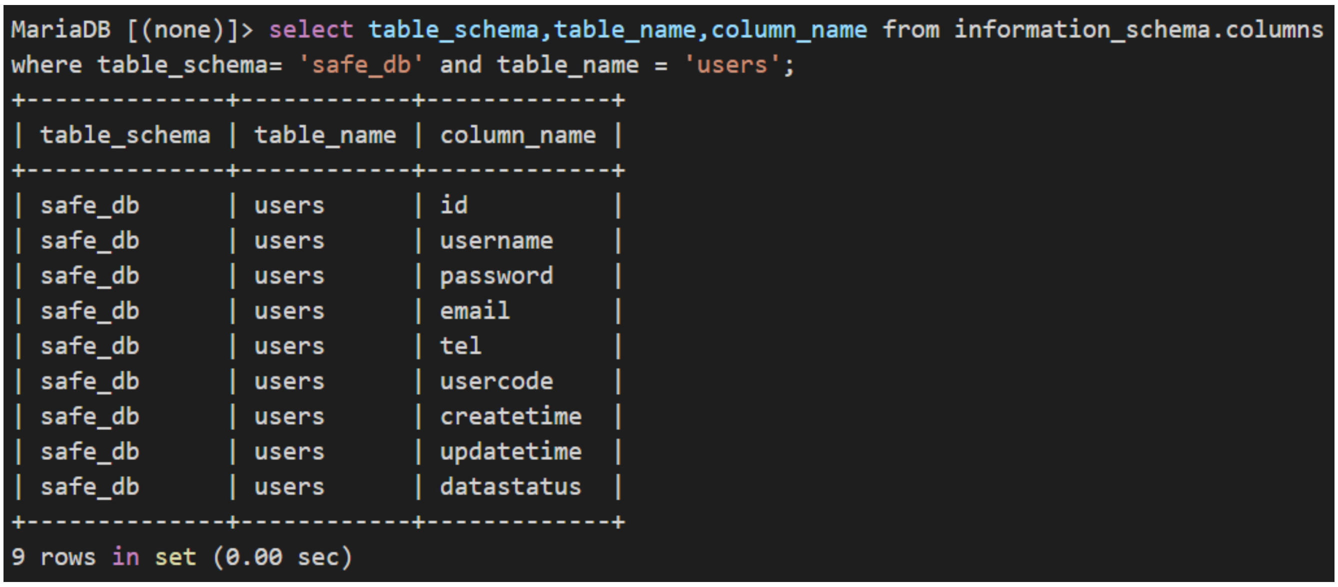
`select table_schema,table_name,table_type,engine from information_schema.tables where table_schema = '数据库名';`



```
MariaDB [safe_db]> select table_schema,table_name,table_type,engine
from information_schema.tables where table_schema = 'safe_db';
+--------------+--------------+------------+--------+
| table_schema | table_name   | table_type | engine |
+--------------+--------------+------------+--------+
| safe_db      | file_records | BASE TABLE | InnoDB |
| safe_db      | users        | BASE TABLE | InnoDB |
| safe_db      | view_userinfo | VIEW       | NULL   |
+--------------+--------------+------------+--------+
3 rows in set (0.00 sec)
```

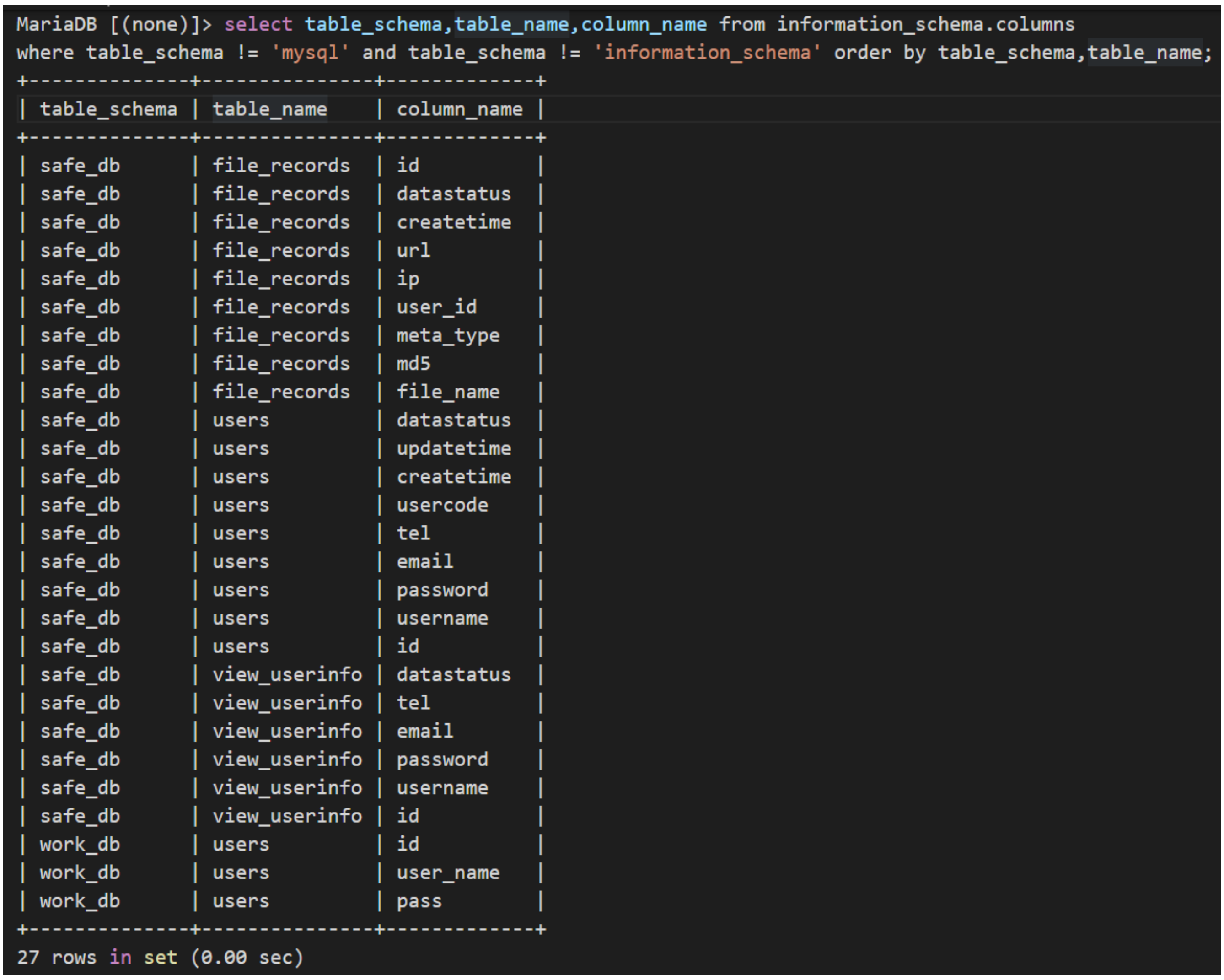
3.4.查询指定表含哪些列

`select table_schema,table_name,column_name from information_schema.columns where table_schema= '数据库名' and table_name = '表名';`



```
MariaDB [(none)]> select table_schema,table_name,column_name from information_schema.columns
where table_schema= 'safe_db' and table_name = 'users';
+--------------+------------+-------------+
| table_schema | table_name | column_name |
+--------------+------------+-------------+
| safe_db      | users      | id          |
| safe_db      | users      | username    |
| safe_db      | users      | password    |
| safe_db      | users      | email       |
| safe_db      | users      | tel         |
| safe_db      | users      | usercode    |
| safe_db      | users      | createtime  |
| safe_db      | users      | updatetime  |
| safe_db      | users      | datastatus  |
+--------------+------------+-------------+
9 rows in set (0.00 sec)
```

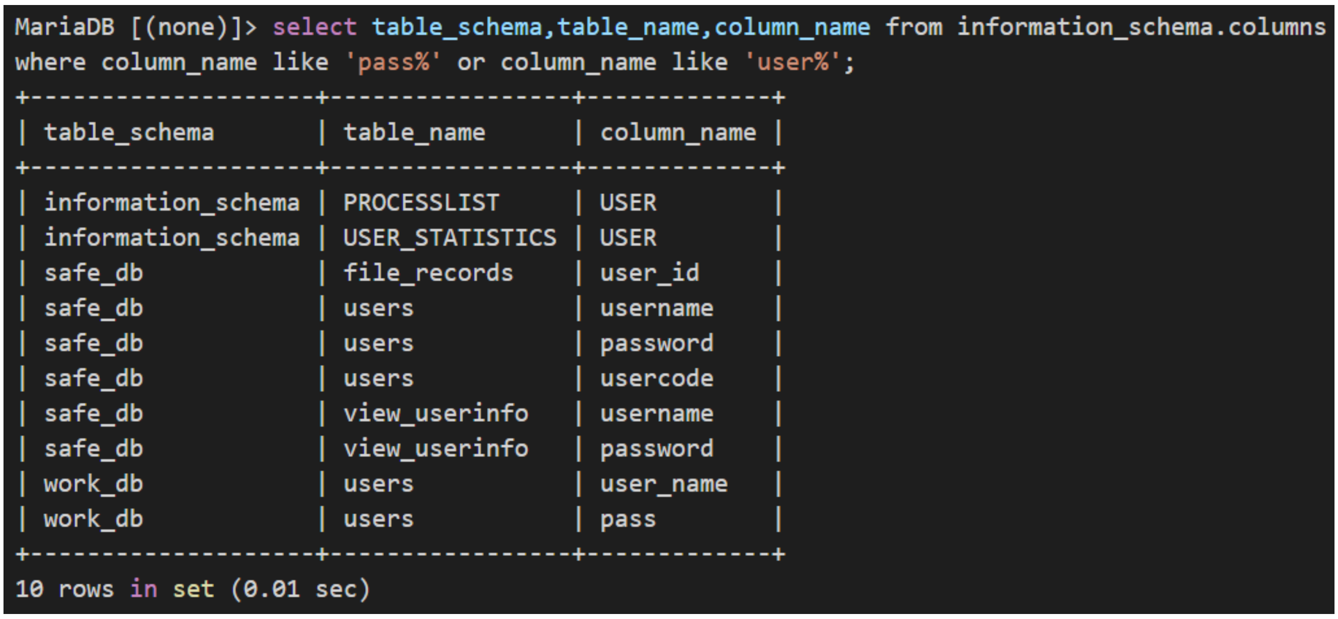
PS：**查询除内置数据库外其他数据库和表**： `select table_schema,table_name,column_name from information_schema.columns where table_schema != 'mysql' and table_schema != 'information_schema' order by table_schema,table_name;`



```
MariaDB [(none)]> select table_schema,table_name,column_name from information_schema.columns
where table_schema != 'mysql' and table_schema != 'information_schema' order by table_schema,table_name;
+--------------+--------------+-------------+
| table_schema | table_name   | column_name |
+--------------+--------------+-------------+
| safe_db      | file_records | id          |
| safe_db      | file_records | datastatus  |
| safe_db      | file_records | createtime  |
| safe_db      | file_records | url         |
| safe_db      | file_records | ip          |
| safe_db      | file_records | user_id     |
| safe_db      | file_records | meta_type   |
| safe_db      | file_records | md5         |
| safe_db      | file_records | file_name   |
| safe_db      | users        | datastatus  |
| safe_db      | users        | updatetime  |
| safe_db      | users        | createtime  |
| safe_db      | users        | usercode    |
| safe_db      | users        | tel         |
| safe_db      | users        | email       |
| safe_db      | users        | password    |
| safe_db      | users        | username    |
| safe_db      | users        | id          |
| safe_db      | view_userinfo | datastatus |
| safe_db      | view_userinfo | tel        |
| safe_db      | view_userinfo | email      |
| safe_db      | view_userinfo | password   |
| safe_db      | view_userinfo | username   |
| safe_db      | view_userinfo | id         |
| work_db      | users        | id          |
| work_db      | users        | user_name   |
| work_db      | users        | pass        |
+--------------+--------------+-------------+
27 rows in set (0.00 sec)
```

寻找自己感兴趣的列

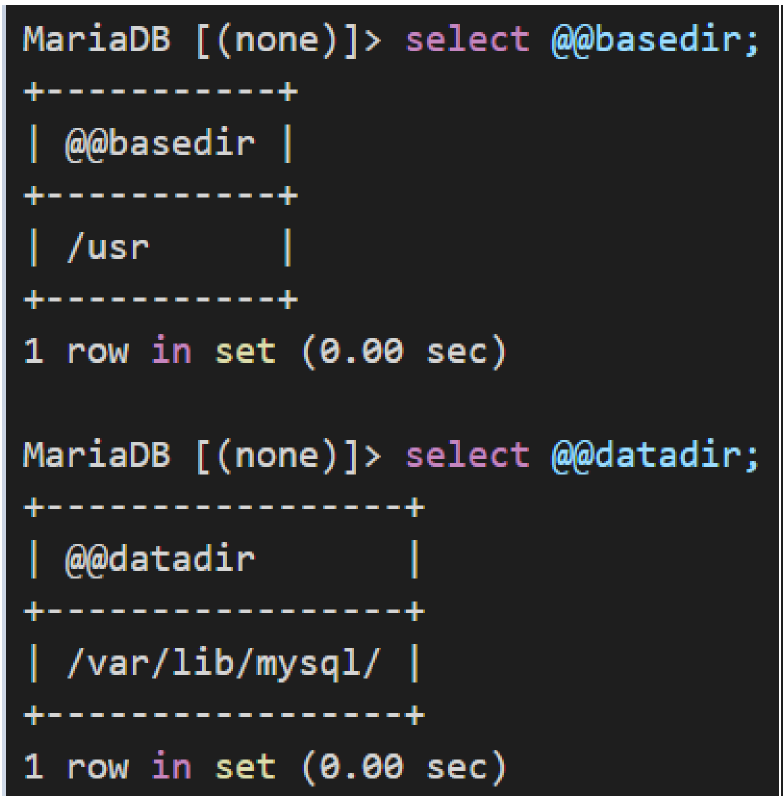
根据特定关键词就可以省去暴力解猜： `select table_schema,table_name,column_name from information_schema.columns where column_name like 'pass%' or column_name like 'user%';`



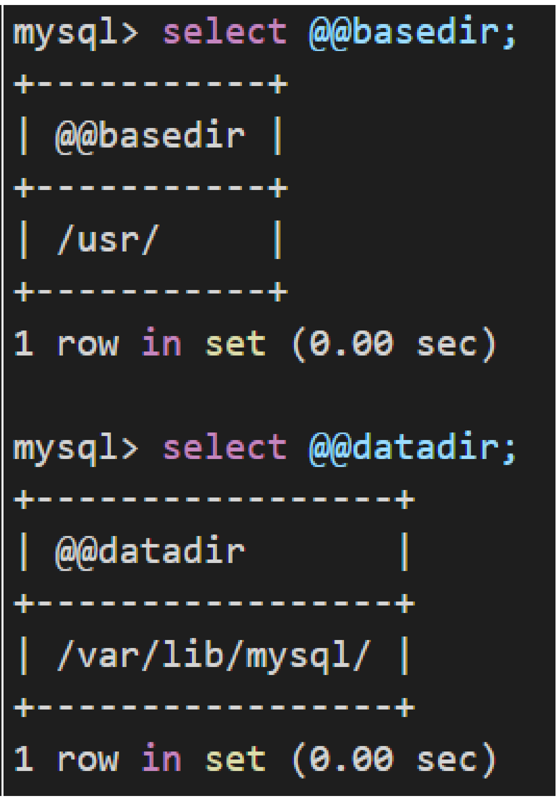
```
MariaDB [(none)]> select table_schema,table_name,column_name from information_schema.columns
where column_name like 'pass%' or column_name like 'user%';
+--------------------+-----------------+-------------+
| table_schema       | table_name      | column_name |
+--------------------+-----------------+-------------+
| information_schema | PROCESSLIST     | USER        |
| information_schema | USER_STATISTICS | USER        |
| safe_db            | file_records    | user_id     |
| safe_db            | users           | username    |
| safe_db            | users           | password    |
| safe_db            | users           | usercode    |
| safe_db            | view_userinfo   | username    |
| safe_db            | view_userinfo   | password    |
| work_db            | users           | user_name   |
| work_db            | users           | pass        |
+--------------------+-----------------+-------------+
10 rows in set (0.01 sec)
```

3.5.获取目录信息

1. 获取数据库**安装目录**： `select @@basedir;`
2. 获取**数据目录**： `select @@datadir;`



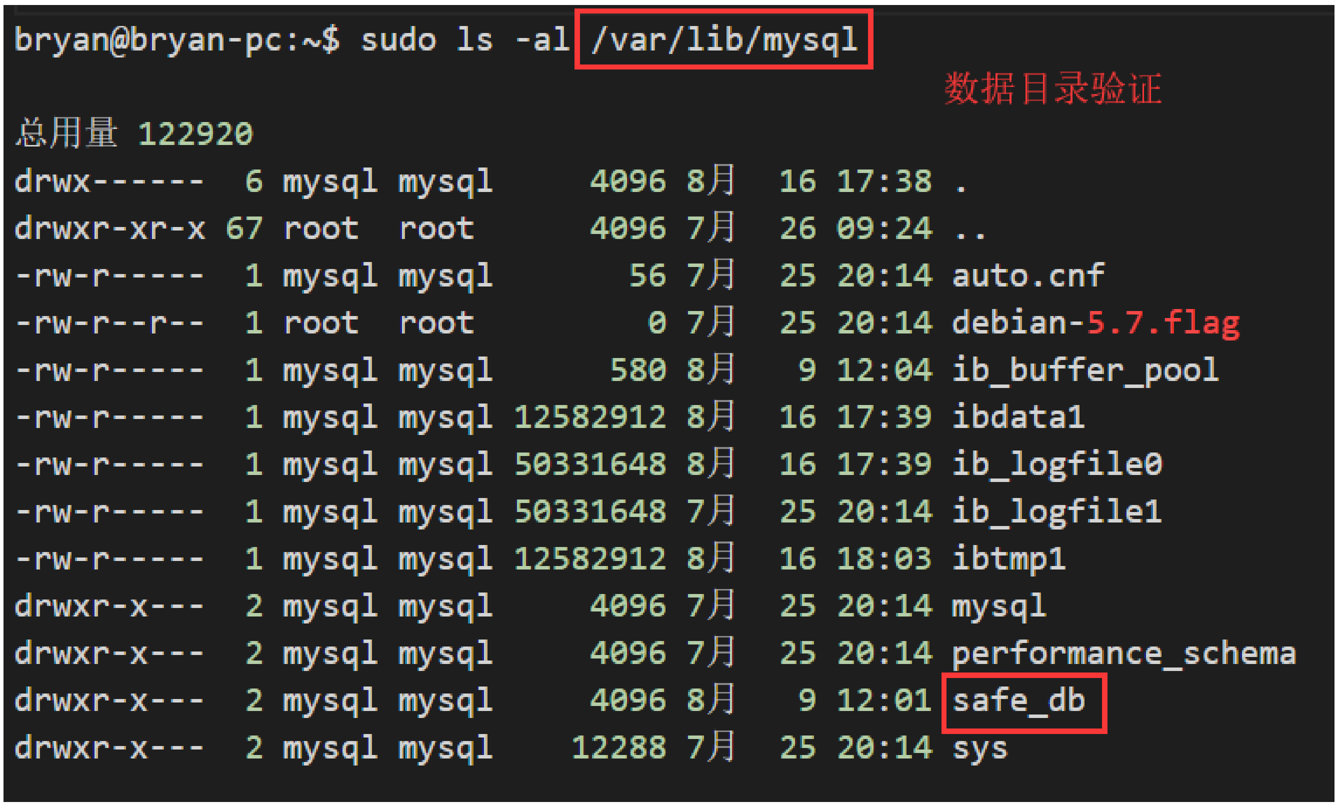
```
MariaDB [(none)]> select @@basedir;
+-----------+
| @@basedir |
+-----------+
| /usr      |
+-----------+
1 row in set (0.00 sec)

MariaDB [(none)]> select @@datadir;
+-----------------+
| @@datadir       |
+-----------------+
| /var/lib/mysql/ |
+-----------------+
1 row in set (0.00 sec)
```



```
mysql> select @@basedir;
+-----------+
| @@basedir |
+-----------+
| /usr/     |
+-----------+
1 row in set (0.00 sec)

mysql> select @@datadir;
+-----------------+
| @@datadir       |
+-----------------+
| /var/lib/mysql/ |
+-----------------+
1 row in set (0.00 sec)
```

目录验证：

```
mysql> show variables like '%basedir%';
+---------------+-------+
| Variable_name | Value |
+---------------+-------+
| basedir       | /usr/ |
+---------------+-------+
1 row in set (0.00 sec)

mysql> show variables like '%datadir%';
+---------------+-----------------+
| Variable_name | Value           |
+---------------+-----------------+
| datadir       | /var/lib/mysql/ |
+---------------+-----------------+
1 row in set (0.00 sec)
```

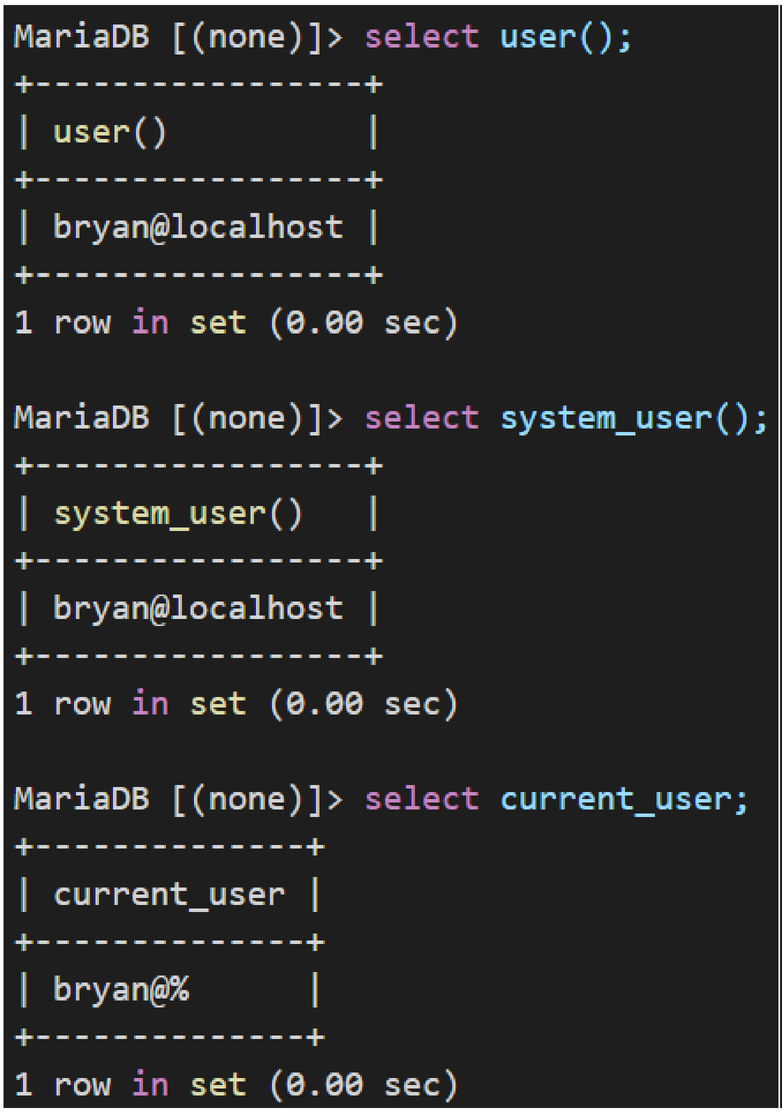


```
bryan@bryan-pc:~$ sudo ls -al /var/lib/mysql
总用量 122920
drwx------  6 mysql mysql     4096 8月  16 17:38 .
drwxr-xr-x 67 root  root      4096 7月  26 09:24 ..
-rw-r-----  1 mysql mysql       56 7月  25 20:14 auto.cnf
-rw-r--r--  1 root  root         0 7月  25 20:14 debian-5.7.flag
-rw-r-----  1 mysql mysql      580 8月   9 12:04 ib_buffer_pool
-rw-r-----  1 mysql mysql 12582912 8月  16 17:39 ibdata1
-rw-r-----  1 mysql mysql 50331648 8月  16 17:39 ib_logfile0
-rw-r-----  1 mysql mysql 50331648 7月  25 20:14 ib_logfile1
-rw-r-----  1 mysql mysql 12582912 8月  16 18:03 ibtmp1
drwxr-x---  2 mysql mysql     4096 7月  25 20:14 mysql
drwxr-x---  2 mysql mysql     4096 7月  25 20:14 performance_schema
drwxr-x---  2 mysql mysql     4096 8月   9 12:01 safe_db
drwxr-x---  2 mysql mysql    12288 7月  25 20:14 sys
```

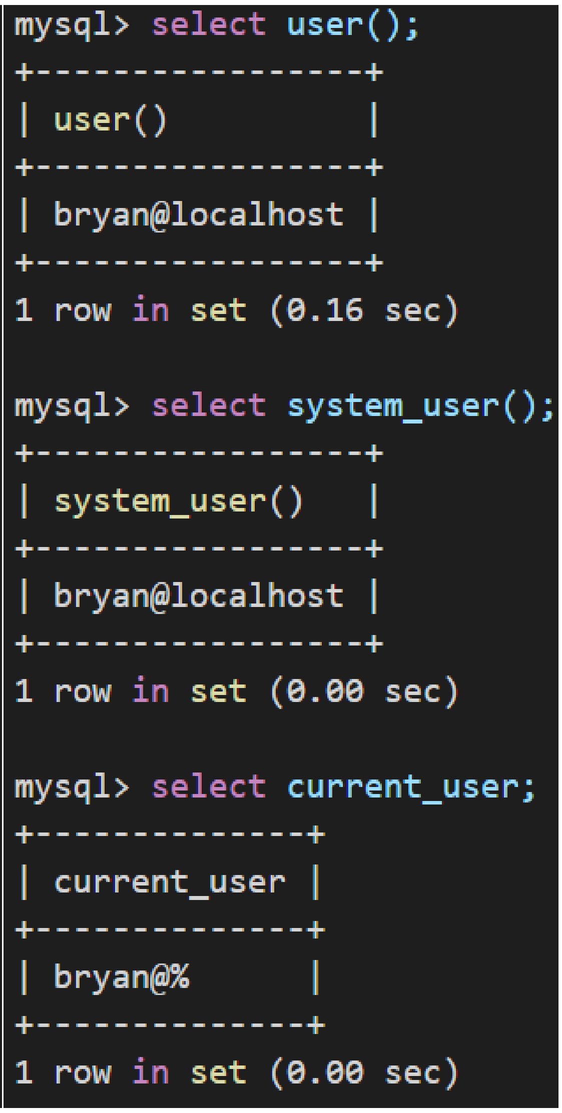
4.获取用户信息

4.1.获取当前用户名

`select user();` or `select system_user();` or `select current_user;`



```
MariaDB [(none)]> select user();
+----------------+
| user()         |
+----------------+
| bryan@localhost |
+----------------+
1 row in set (0.00 sec)

MariaDB [(none)]> select system_user();
+----------------+
| system_user()   |
+----------------+
| bryan@localhost |
+----------------+
1 row in set (0.00 sec)

MariaDB [(none)]> select current_user;
+--------------+
| current_user |
+--------------+
| bryan@%      |
+--------------+
1 row in set (0.00 sec)
```

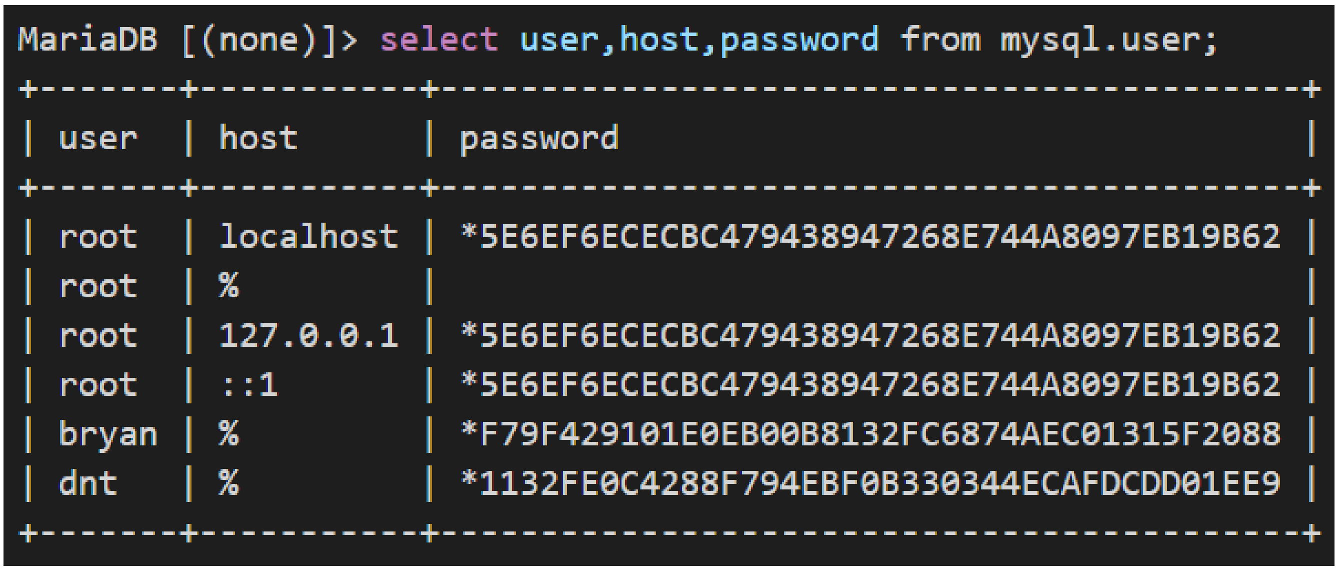


```
mysql> select user();
+----------------+
| user()         |
+----------------+
| bryan@localhost |
+----------------+
1 row in set (0.16 sec)

mysql> select system_user();
+----------------+
| system_user()   |
+----------------+
| bryan@localhost |
+----------------+
1 row in set (0.00 sec)

mysql> select current_user;
+--------------+
| current_user |
+--------------+
| bryan@%      |
+--------------+
1 row in set (0.00 sec)
```

获取用户信息（含密码）

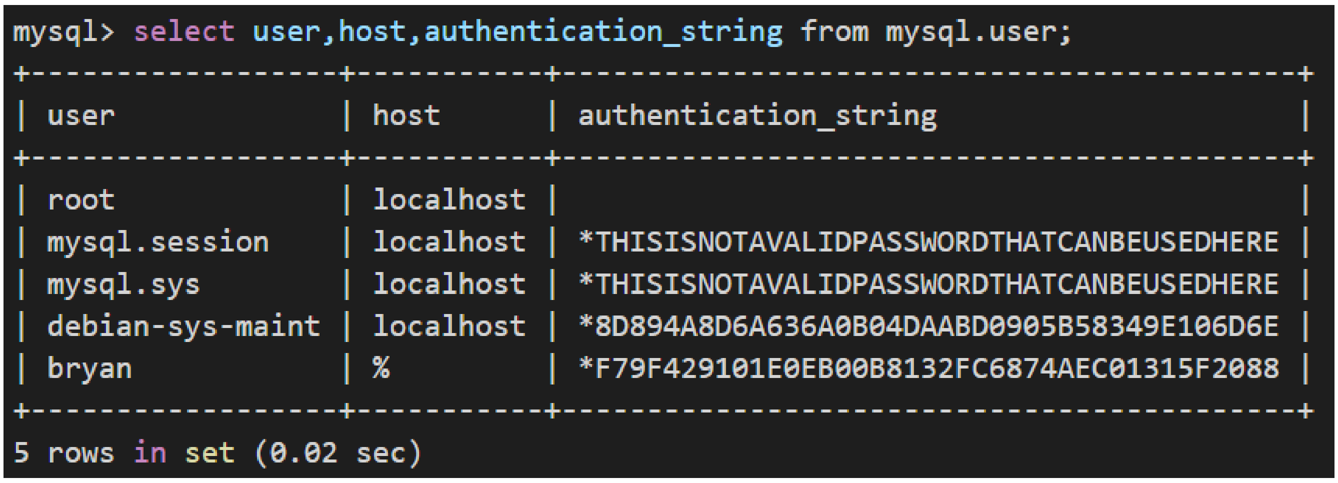
【root权限】**显示所有用户（含密码）**

MariaDB5.x： `select user,host,password from mysql.user;`



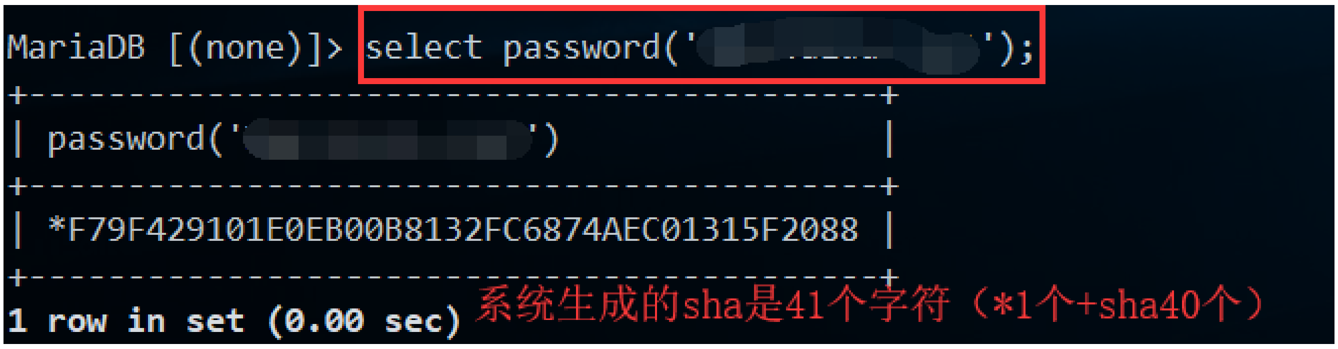
```
MariaDB [(none)]> select user,host,password from mysql.user;
+-------+-----------+-------------------------------------------+
| user  | host      | password                                  |
+-------+-----------+-------------------------------------------+
| root  | localhost | *5E6EF6ECECBC479438947268E744A8097EB19B62 |
| root  | %         |                                           |
| root  | 127.0.0.1 | *5E6EF6ECECBC479438947268E744A8097EB19B62 |
| root  | ::1       | *5E6EF6ECECBC479438947268E744A8097EB19B62 |
| bryan | %         | *F79F429101E0EB00B8132FC6874AEC01315F2088 |
| dnt   | %         | *1132FE0C4288F794EBF0B330344ECAFDCDD01EE9 |
+-------+-----------+-------------------------------------------+
```

MySQL5.x： `select user,host,authentication_string from mysql.user;`


```
mysql> select user,host,authentication_string from mysql.user;
+------------------+-----------+-------------------------------------------+
| user             | host      | authentication_string                     |
+------------------+-----------+-------------------------------------------+
| root             | localhost |                                           |
| mysql.session    | localhost | *THISISNOTAVALIDPASSWORDTHATCANBEUSEDHERE |
| mysql.sys        | localhost | *THISISNOTAVALIDPASSWORDTHATCANBEUSEDHERE |
| debian-sys-maint | localhost | *8D894A8D6A636A0B04DAABD0905B58349E106D6E |
| bryan            | %         | *F79F429101E0EB00B8132FC6874AEC01315F2088 |
+------------------+-----------+-------------------------------------------+
5 rows in set (0.02 sec)
```

PS：系统生成的加密sha字符串是41位（ `*` 1位+sha40位）

> sha1是40位，但mysql的加密是变种sha1


```
MariaDB [(none)]> select password('[redacted]');
+-------------------------------------------+
| password('[redacted]')                    |
+-------------------------------------------+
| *F79F429101E0EB00B8132FC6874AEC01315F2088 |
+-------------------------------------------+
1 row in set (0.00 sec)
```

4.2.查看指定DB的用户权限

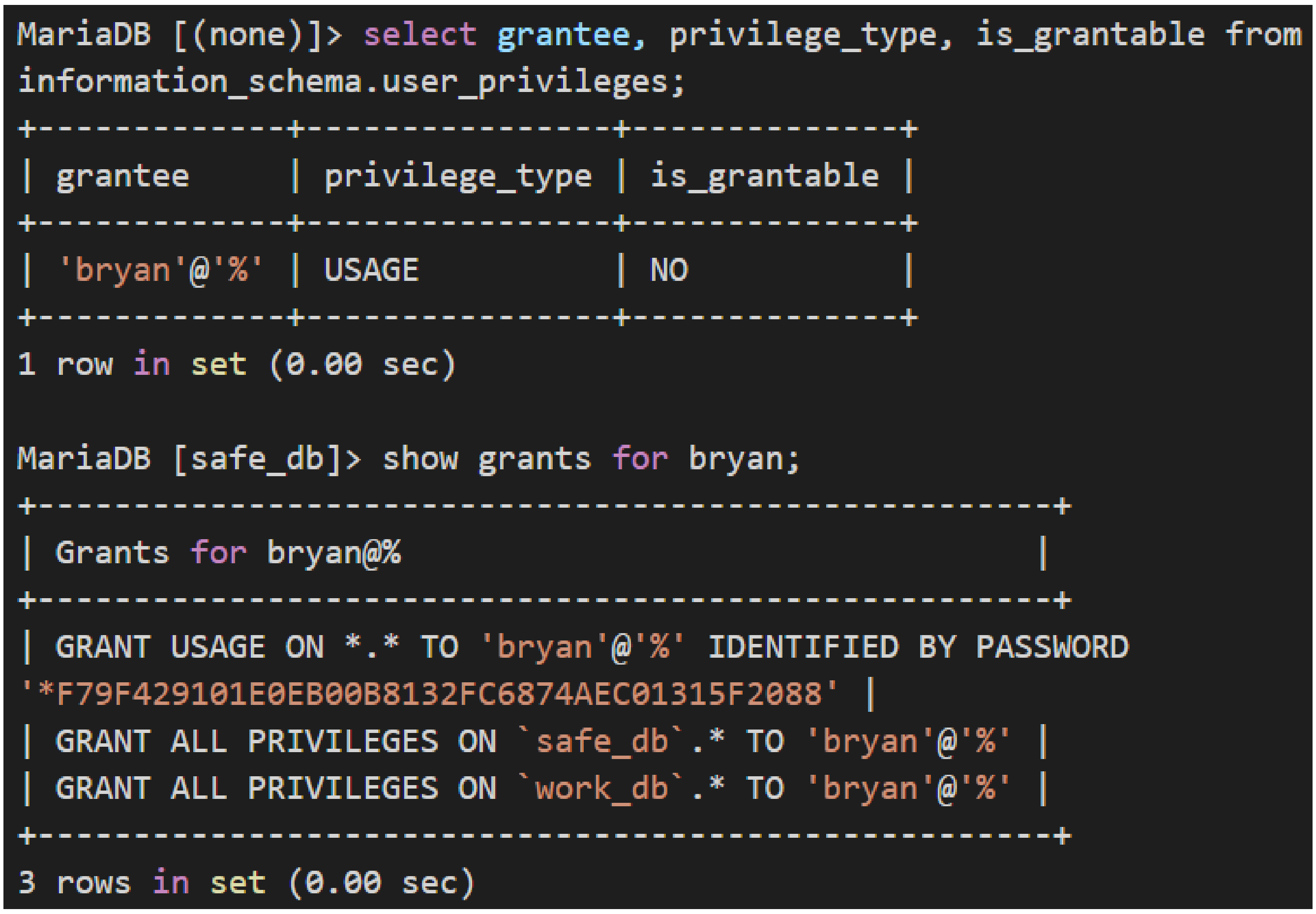
`select grantee, table_schema, privilege_type from information_schema.schema_privileges where table_schema = 'safe_db';`

```
MariaDB [(none)]>  select grantee, table_schema, privilege_type from
information_schema.schema_privileges where table_schema = 'safe_db';
+-------------+--------------+-------------------------+
| grantee     | table_schema | privilege_type          |
+-------------+--------------+-------------------------+
| 'bryan'@'%' | safe_db      | SELECT                  |
| 'bryan'@'%' | safe_db      | INSERT                  |
| 'bryan'@'%' | safe_db      | UPDATE                  |
| 'bryan'@'%' | safe_db      | DELETE                  |
| 'bryan'@'%' | safe_db      | CREATE                  |
| 'bryan'@'%' | safe_db      | DROP                    |
| 'bryan'@'%' | safe_db      | REFERENCES              |
| 'bryan'@'%' | safe_db      | INDEX                   |
| 'bryan'@'%' | safe_db      | ALTER                   |
| 'bryan'@'%' | safe_db      | CREATE TEMPORARY TABLES |
| 'bryan'@'%' | safe_db      | LOCK TABLES             |
| 'bryan'@'%' | safe_db      | EXECUTE                 |
| 'bryan'@'%' | safe_db      | CREATE VIEW             |
| 'bryan'@'%' | safe_db      | SHOW VIEW               |
| 'bryan'@'%' | safe_db      | CREATE ROUTINE          |
| 'bryan'@'%' | safe_db      | ALTER ROUTINE           |
| 'bryan'@'%' | safe_db      | EVENT                   |
| 'bryan'@'%' | safe_db      | TRIGGER                 |
+-------------+--------------+-------------------------+
18 rows in set (0.00 sec)
```

4.3.查询用户权限列表

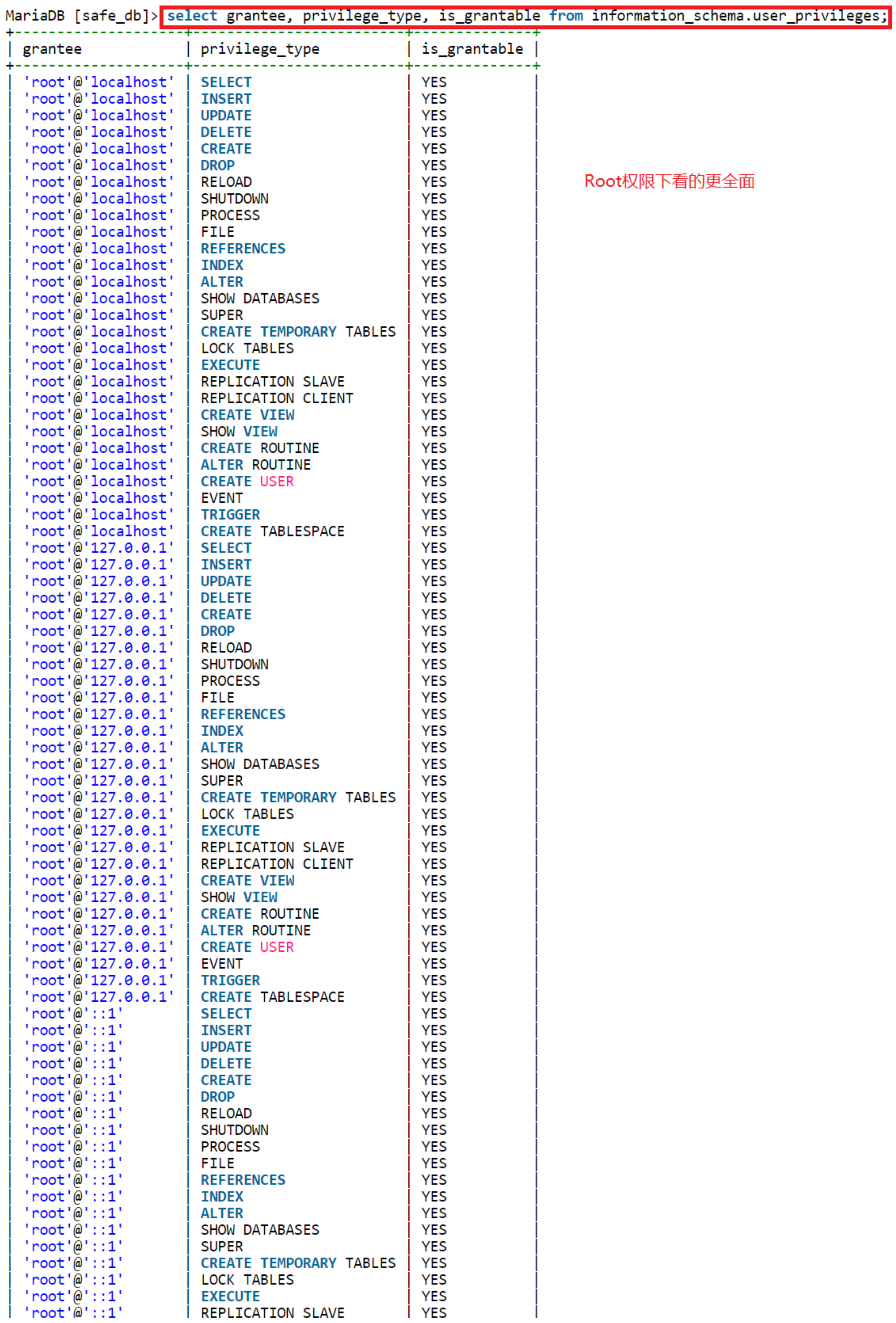
`select grantee, privilege_type, is_grantable from information_schema.user_privileges;`

> PS：也可使用 `show grants for bryan;`



```
MariaDB [(none)]> select grantee, privilege_type, is_grantable from
information_schema.user_privileges;
+-------------+----------------+--------------+
| grantee     | privilege_type | is_grantable |
+-------------+----------------+--------------+
| 'bryan'@'%' | USAGE          | NO           |
+-------------+----------------+--------------+
1 row in set (0.00 sec)

MariaDB [safe_db]> show grants for bryan;
+-----------------------------------------------------+
| Grants for bryan@%                                  |
+-----------------------------------------------------+
| GRANT USAGE ON *.* TO 'bryan'@'%' IDENTIFIED BY PASSWORD
'*F79F429101E0EB00B8132FC6874AEC01315F2088' |
| GRANT ALL PRIVILEGES ON `safe_db`.* TO 'bryan'@'%' |
| GRANT ALL PRIVILEGES ON `work_db`.* TO 'bryan'@'%' |
+-----------------------------------------------------+
3 rows in set (0.00 sec)
```

PS：root权限查询的更全面



```
MariaDB [safe_db]> select grantee, privilege_type, is_grantable from information_schema.user_privileges;
+--------------------+-------------------------+--------------+
| grantee            | privilege_type          | is_grantable |
+--------------------+-------------------------+--------------+
| 'root'@'localhost' | SELECT                  | YES          |
| 'root'@'localhost' | INSERT                  | YES          |
| 'root'@'localhost' | UPDATE                  | YES          |
| 'root'@'localhost' | DELETE                  | YES          |
| 'root'@'localhost' | CREATE                  | YES          |
| 'root'@'localhost' | DROP                    | YES          |
| 'root'@'localhost' | RELOAD                  | YES          |
| 'root'@'localhost' | SHUTDOWN                | YES          |
| 'root'@'localhost' | PROCESS                 | YES          |
| 'root'@'localhost' | FILE                    | YES          |
| 'root'@'localhost' | REFERENCES              | YES          |
| 'root'@'localhost' | INDEX                   | YES          |
| 'root'@'localhost' | ALTER                   | YES          |
| 'root'@'localhost' | SHOW DATABASES          | YES          |
| 'root'@'localhost' | SUPER                   | YES          |
| 'root'@'localhost' | CREATE TEMPORARY TABLES | YES          |
| 'root'@'localhost' | LOCK TABLES             | YES          |
| 'root'@'localhost' | EXECUTE                 | YES          |
| 'root'@'localhost' | REPLICATION SLAVE       | YES          |
| 'root'@'localhost' | REPLICATION CLIENT      | YES          |
| 'root'@'localhost' | CREATE VIEW             | YES          |
| 'root'@'localhost' | SHOW VIEW               | YES          |
| 'root'@'localhost' | CREATE ROUTINE          | YES          |
| 'root'@'localhost' | ALTER ROUTINE           | YES          |
| 'root'@'localhost' | CREATE USER             | YES          |
| 'root'@'localhost' | EVENT                   | YES          |
| 'root'@'localhost' | TRIGGER                 | YES          |
| 'root'@'localhost' | CREATE TABLESPACE       | YES          |
| 'root'@'127.0.0.1' | SELECT                  | YES          |
| 'root'@'127.0.0.1' | INSERT                  | YES          |
| 'root'@'127.0.0.1' | UPDATE                  | YES          |
| 'root'@'127.0.0.1' | DELETE                  | YES          |
| 'root'@'127.0.0.1' | CREATE                  | YES          |
| 'root'@'127.0.0.1' | DROP                    | YES          |
| 'root'@'127.0.0.1' | RELOAD                  | YES          |
| 'root'@'127.0.0.1' | SHUTDOWN                | YES          |
| 'root'@'127.0.0.1' | PROCESS                 | YES          |
| 'root'@'127.0.0.1' | FILE                    | YES          |
| 'root'@'127.0.0.1' | REFERENCES              | YES          |
| 'root'@'127.0.0.1' | INDEX                   | YES          |
| 'root'@'127.0.0.1' | ALTER                   | YES          |
| 'root'@'127.0.0.1' | SHOW DATABASES          | YES          |
| 'root'@'127.0.0.1' | SUPER                   | YES          |
| 'root'@'127.0.0.1' | CREATE TEMPORARY TABLES | YES          |
| 'root'@'127.0.0.1' | LOCK TABLES             | YES          |
| 'root'@'127.0.0.1' | EXECUTE                 | YES          |
| 'root'@'127.0.0.1' | REPLICATION SLAVE       | YES          |
| 'root'@'127.0.0.1' | REPLICATION CLIENT      | YES          |
| 'root'@'127.0.0.1' | CREATE VIEW             | YES          |
| 'root'@'127.0.0.1' | SHOW VIEW               | YES          |
| 'root'@'127.0.0.1' | CREATE ROUTINE          | YES          |
| 'root'@'127.0.0.1' | ALTER ROUTINE           | YES          |
| 'root'@'127.0.0.1' | CREATE USER             | YES          |
| 'root'@'127.0.0.1' | EVENT                   | YES          |
| 'root'@'127.0.0.1' | TRIGGER                 | YES          |
| 'root'@'127.0.0.1' | CREATE TABLESPACE       | YES          |
| 'root'@'::1'       | SELECT                  | YES          |
| 'root'@'::1'       | INSERT                  | YES          |
| 'root'@'::1'       | UPDATE                  | YES          |
| 'root'@'::1'       | DELETE                  | YES          |
| 'root'@'::1'       | CREATE                  | YES          |
| 'root'@'::1'       | DROP                    | YES          |
| 'root'@'::1'       | RELOAD                  | YES          |
| 'root'@'::1'       | SHUTDOWN                | YES          |
| 'root'@'::1'       | PROCESS                 | YES          |
| 'root'@'::1'       | FILE                    | YES          |
| 'root'@'::1'       | REFERENCES              | YES          |
| 'root'@'::1'       | INDEX                   | YES          |
| 'root'@'::1'       | ALTER                   | YES          |
| 'root'@'::1'       | SHOW DATABASES          | YES          |
| 'root'@'::1'       | SUPER                   | YES          |
| 'root'@'::1'       | CREATE TEMPORARY TABLES | YES          |
| 'root'@'::1'       | LOCK TABLES             | YES          |
| 'root'@'::1'       | EXECUTE                 | YES          |
| 'root'@'::1'       | REPLICATION SLAVE       | YES          |
```

Root权限下看的更全面

```
| 'root'@'::1'        | REPLICATION CLIENT      | YES          |
| 'root'@'::1'        | CREATE VIEW             | YES          |
| 'root'@'::1'        | SHOW VIEW               | YES          |
| 'root'@'::1'        | CREATE ROUTINE          | YES          |
| 'root'@'::1'        | ALTER ROUTINE           | YES          |
| 'root'@'::1'        | CREATE USER             | YES          |
| 'root'@'::1'        | EVENT                   | YES          |
| 'root'@'::1'        | TRIGGER                 | YES          |
| 'root'@'::1'        | CREATE TABLESPACE       | YES          |
| 'root'@'%'          | USAGE                   | NO           |
| 'bryan'@'%'         | USAGE                   | NO           |
| 'dnt'@'%'           | USAGE                   | NO           |
+---------------------+-------------------------+--------------+
87 rows in set (0.00 sec)
```

root权限通过mysql.user查询更详细权限信息

【root权限】通过 `mysql.user` 查询更详细权限信息： `select host, user, Select_priv, Insert_priv, Update_priv, Delete_priv, Create_priv, Drop_priv, Reload_priv, Shutdown_priv, Process_priv, File_priv, Grant_priv, References_priv, Index_priv, Alter_priv, Show_db_priv, Super_priv, Create_tmp_table_priv, Lock_tables_priv, Execute_priv, Repl_slave_priv, Repl_client_priv,Create_view_priv,Show_view_priv,Create_routine_priv,Alter_routine_priv,Create_user_priv,Event_priv,Trigger_priv,Create_tablespace_priv from mysql.user;`

1. **Select_priv**：用户是否可以通过SELECT命令选择数据
2. **Insert_priv**：用户是否可以通过INSERT命令插入数据
3. **Update_priv**：用户是否可以通过UPDATE命令修改现有数据
4. Delete_priv：用户是否可以通过DELETE命令删除现有数据
5. **Create_priv**：用户是否可以**创建新的数据库和表**
6. Drop_priv：用户是否可以删除现有数据库和表
7. Reload_priv：用户是否可以执行刷新和重新加载MySQL所用各种内部缓存的特定命令（包括日志、权限、主机、查询和表重新加载权限表）
8. Shutdown_priv：用户是否可以关闭MySQL服务器（不推荐付给root外用户）
9. Process_priv：用户是否可以通过 `show processlist;` 命令查看其他用户的进程服务器管理
10. **File_priv**：用户是否可以执行 `select into outfile` 和 `load data infile` 命令加载服务器上的文件
11. Grant_priv：用户是否可以将已经授予给该用户自己的权限再授予其他用户(可赋予全部已有权限)
12. References_priv：目前只是某些未来功能的占位符；现在没有作用
13. **Index_priv**：用户是否可以创建和删除表索引用索引查询表
14. **Alter_priv**：用户是否可以重命名和修改表结构
15. Show_db_priv：用户是否可以查看服务器上所有数据库的名字（不推荐开启）
16. **Super_priv**：用户是否可以执行某些强大的管理功能
    1. 例如通过 `kill` 命令删除用户进程
    2. 使用 `set global` 修改全局MySQL变量
    3. 执行关于复制和日志的各种命令超级权限
17. **Create_tmp_table_priv**：用户是否可以创建临时表
18. Lock_tables_priv：用户是否可以使用 `lock tables` 命令阻止对表的访问/修改
19. Execute_priv：用户是否可以执行存储过程此（MySQL 5新增）
20. Repl_slave_priv：用户是否可以读取用于维护复制数据库环境的二进制日志文件

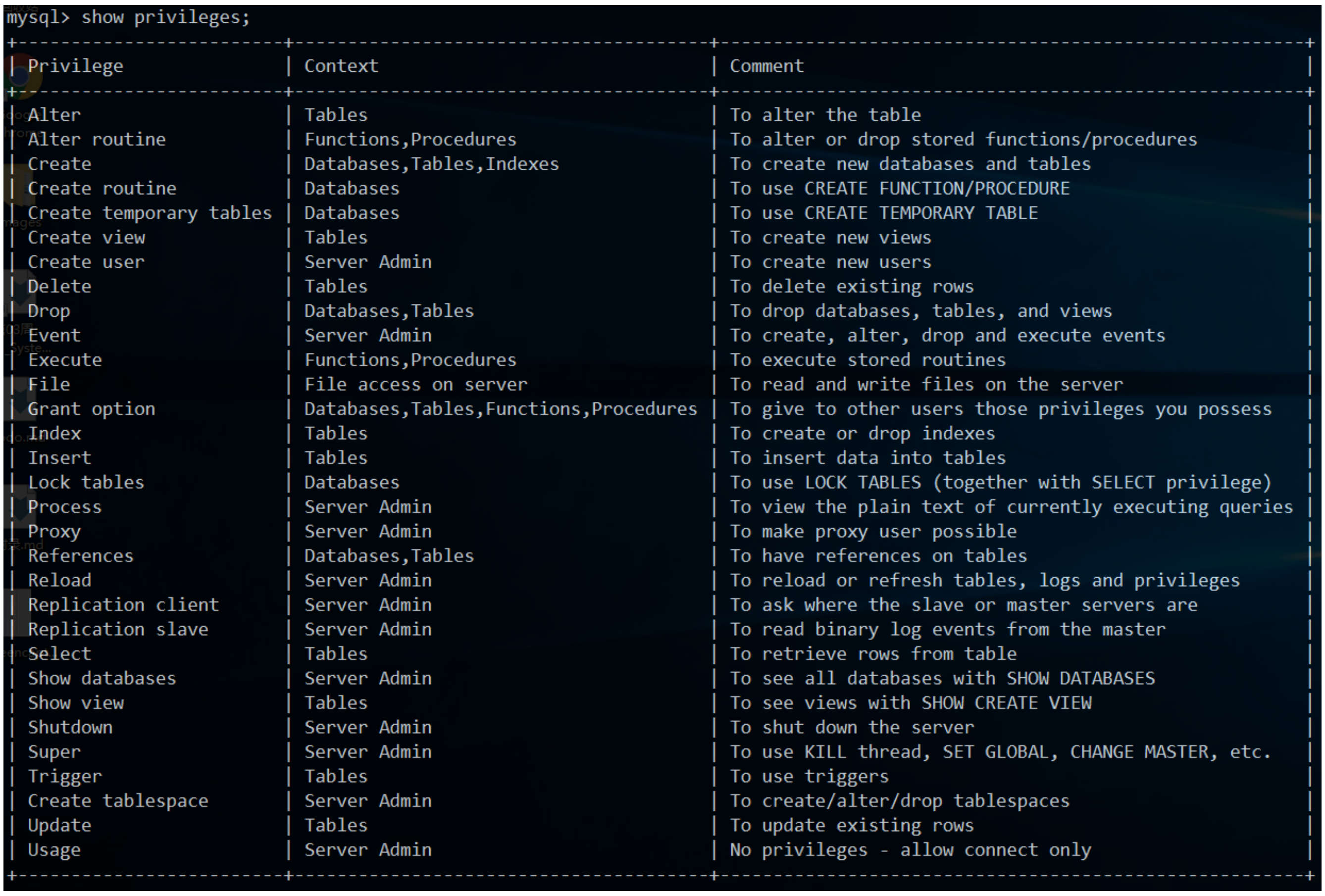
21. Repl_client_priv：用户是否可以确定复制从服务器和主服务器的位置从服务器管理
22. Create_view_priv：用户是否可以创建视图（MySQL 5新增）
23. Show_view_priv：用户是否可以查看视图或了解视图如何执行（MySQL 5新增）
24. Create_routine_priv：用户是否可以更改或放弃存储过程和函数（MySQL 5新增）
25. Alter_routine_priv：用户是否可以修改或删除存储函数及函数（MySQL 5新增）
26. Create_user_priv：用户是否可以执行 `CREATE USER` 用于创建新的MySQL账户
27. Event_priv：用户是否创建、修改和删除事件（MySQL 5.1.6新增）
28. Trigger_priv：用户是否创建和删除触发器（MySQL 5.1.6新增）
29. Create_tablespace_priv：用户是否可以创建表空间

```
MariaDB [safe_db]> select host, user, Select_priv, Insert_priv, Update_priv, Delete_priv,
Create_priv, Drop_priv, Reload_priv, Shutdown_priv, Process_priv, File_priv, Grant_priv,
References_priv, Index_priv, Alter_priv, Show_db_priv, Super_priv, Create_tmp_table_priv,
Lock_tables_priv, Execute_priv, Repl_slave_priv,
Repl_client_priv,Create_view_priv,Show_view_priv,Create_routine_priv,Alter_routine_priv,Create_us
er_priv,Event_priv,Trigger_priv,Create_tablespace_priv from mysql.user\G;

*************************** 1. row ***************************
                  host: localhost
                  user: root
           Select_priv: Y
           Insert_priv: Y
           Update_priv: Y
           Delete_priv: Y
           Create_priv: Y
             Drop_priv: Y
           Reload_priv: Y
         Shutdown_priv: Y
          Process_priv: Y
             File_priv: Y
            Grant_priv: Y
       References_priv: Y
            Index_priv: Y
            Alter_priv: Y
          Show_db_priv: Y
            Super_priv: Y
 Create_tmp_table_priv: Y
      Lock_tables_priv: Y
          Execute_priv: Y
       Repl_slave_priv: Y
      Repl_client_priv: Y
      Create_view_priv: Y
        Show_view_priv: Y
   Create_routine_priv: Y
    Alter_routine_priv: Y
      Create_user_priv: Y
            Event_priv: Y
          Trigger_priv: Y
Create_tablespace_priv: Y
*************************** 2. row ***************************
```

```
                 host: %
                 user: root
          Select_priv: N
          Insert_priv: N
          Update_priv: N
          Delete_priv: N
          Create_priv: N
            Drop_priv: N
          Reload_priv: N
        Shutdown_priv: N
         Process_priv: N
            File_priv: N
           Grant_priv: N
      References_priv: N
           Index_priv: N
           Alter_priv: N
         Show_db_priv: N
           Super_priv: N
 Create_tmp_table_priv: N
     Lock_tables_priv: N
         Execute_priv: N
      Repl_slave_priv: N
     Repl_client_priv: N
     Create_view_priv: N
       Show_view_priv: N
  Create_routine_priv: N
   Alter_routine_priv: N
     Create_user_priv: N
           Event_priv: N
         Trigger_priv: N
Create_tablespace_priv: N

。。。。。。

*************************** 5. row ***************************
                 host: %
                 user: bryan
          Select_priv: N
          Insert_priv: N
          Update_priv: N
          Delete_priv: N
          Create_priv: N
            Drop_priv: N
          Reload_priv: N
        Shutdown_priv: N
         Process_priv: N
            File_priv: N
           Grant_priv: N
      References_priv: N
           Index_priv: N
           Alter_priv: N
         Show_db_priv: N
           Super_priv: N
  Create_tmp_table_priv: N
       Lock_tables_priv: N
           Execute_priv: N
        Repl_slave_priv: N
       Repl_client_priv: N
       Create_view_priv: N
         Show_view_priv: N
    Create_routine_priv: N
     Alter_routine_priv: N
       Create_user_priv: N
             Event_priv: N
           Trigger_priv: N
 Create_tablespace_priv: N

 6 rows in set (0.00 sec)
```

扩展

查看当前数据库支持哪些权限： `show privileges;`



```
mysql> 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                               |
| 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      |
| Replication client      | Server Admin                          | To ask where the slave or master servers are          |
| 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 use KILL thread, SET GLOBAL, CHANGE MASTER, etc.   |
| Trigger                 | Tables                                | To use triggers                                       |
| Create tablespace       | Server Admin                          | To create/alter/drop tablespaces                      |
| Update                  | Tables                                | To update existing rows                               |
| Usage                   | Server Admin                          | No privileges - allow connect only                    |
+-------------------------+---------------------------------------+-------------------------------------------------------+
```

获取列的权限列表（用的不多）

> `select table_schema, table_name, column_name, privilege_type from information_schema.column_privileges;`

5.hashcat初探

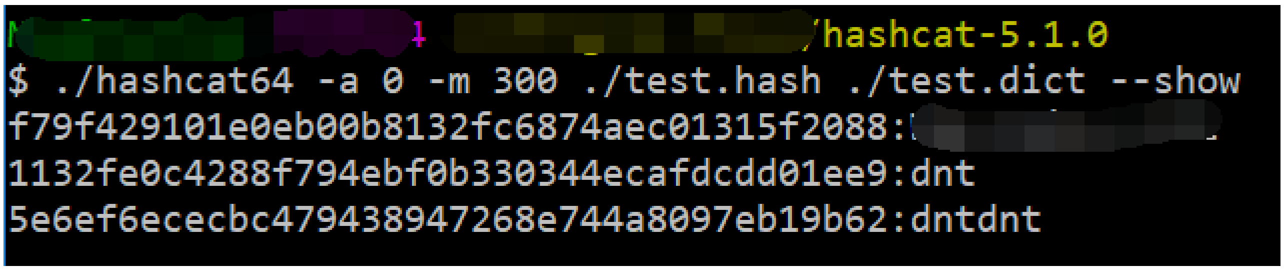
官方**下载**地址：https://hashcat.net/hashcat/

> PS：GitHub：https://github.com/hashcat/hashcat

简单使用：`hashcat64 --force -a 破解模式编号 -m hash类型 需要破解的hash文件路径 字典路径`

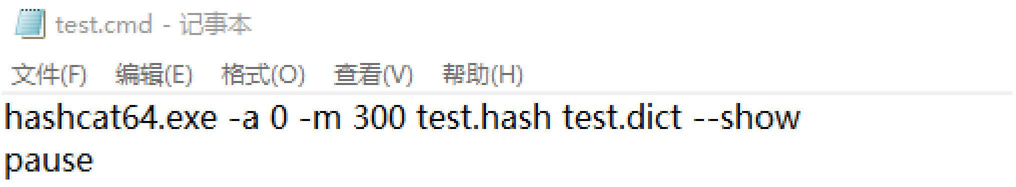
Linux：`./hashcat64 -a 0 -m 300 ./test.hash ./test.dict --show`

> PS：如果出问题把 `--show` 去除即可

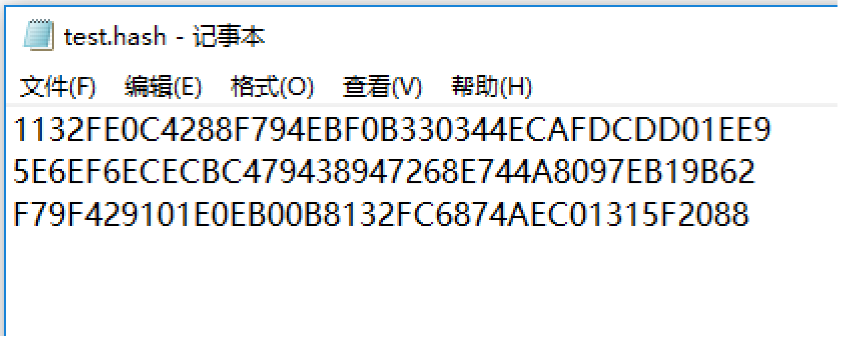


```
[redacted] [redacted] [redacted]/hashcat-5.1.0
$ ./hashcat64 -a 0 -m 300 ./test.hash ./test.dict --show
f79f429101e0eb00b8132fc6874aec01315f2088:[redacted]
1132fe0c4288f794ebf0b330344ecafdcdd01ee9:dnt
5e6ef6ececbc479438947268e744a8097eb19b62:dntdnt
```

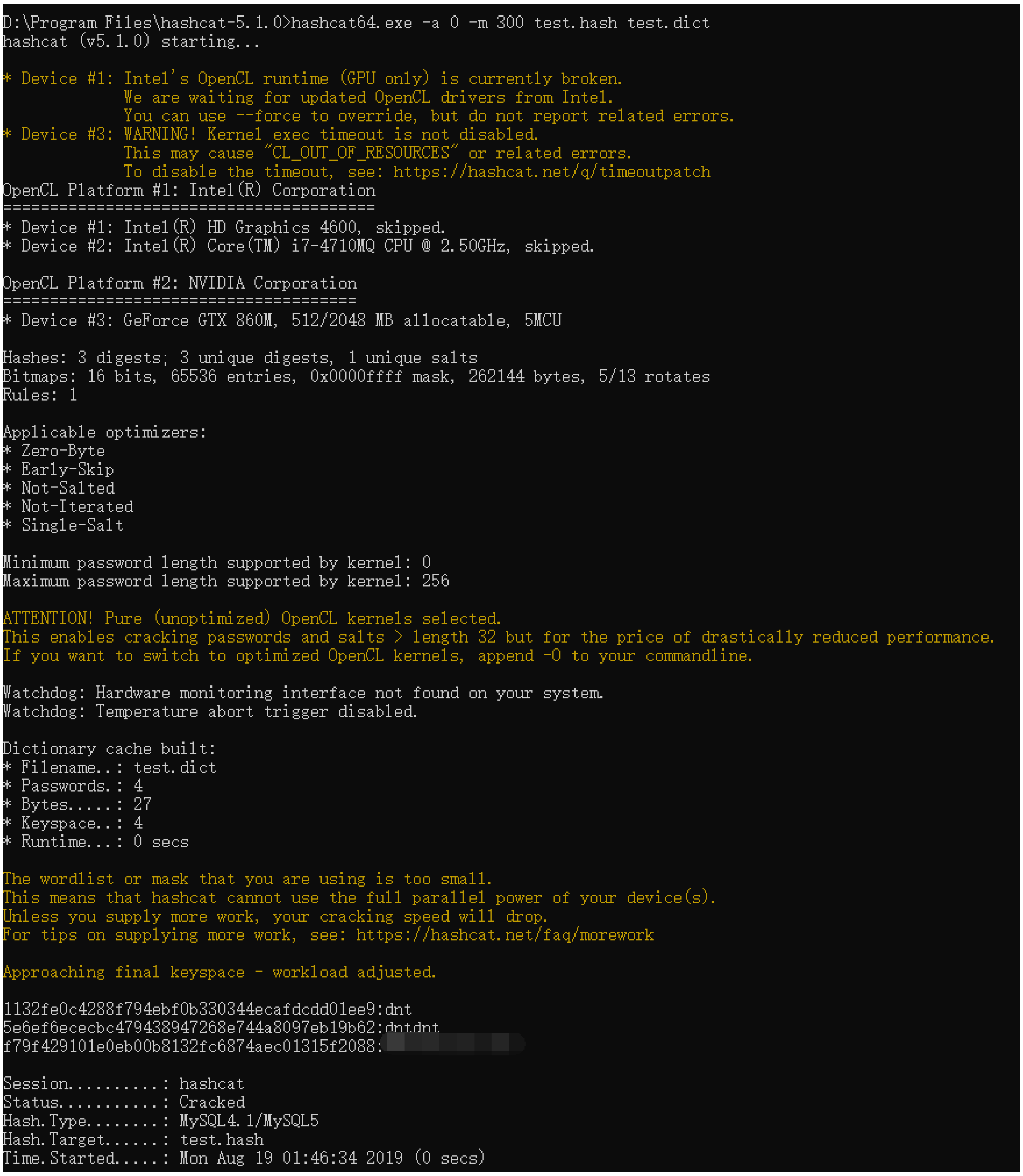
PS：Win下：`hashcat64.exe -a 0 -m 300 test.hash test.dict --show`



```
hashcat64.exe -a 0 -m 300 test.hash test.dict --show
pause
```



```
1132FE0C4288F794EBF0B330344ECAFDCDD01EE9
5E6EF6ECECBC479438947268E744A8097EB19B62
F79F429101E0EB00B8132FC6874AEC01315F2088
```



```
D:\Program Files\hashcat-5.1.0>hashcat64.exe -a 0 -m 300 test.hash test.dict
hashcat (v5.1.0) starting...

* Device #1: Intel's OpenCL runtime (GPU only) is currently broken.
             We are waiting for updated OpenCL drivers from Intel.
             You can use --force to override, but do not report related errors.
* Device #3: WARNING! Kernel exec timeout is not disabled.
             This may cause "CL_OUT_OF_RESOURCES" or related errors.
             To disable the timeout, see: https://hashcat.net/q/timeoutpatch
OpenCL Platform #1: Intel(R) Corporation
========================================
* Device #1: Intel(R) HD Graphics 4600, skipped.
* Device #2: Intel(R) Core(TM) i7-4710MQ CPU @ 2.50GHz, skipped.

OpenCL Platform #2: NVIDIA Corporation
======================================
* Device #3: GeForce GTX 860M, 512/2048 MB allocatable, 5MCU

Hashes: 3 digests; 3 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Applicable optimizers:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Salt

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

ATTENTION! Pure (unoptimized) OpenCL kernels selected.
This enables cracking passwords and salts > length 32 but for the price of drastically reduced performance.
If you want to switch to optimized OpenCL kernels, append -O to your commandline.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Dictionary cache built:
* Filename..: test.dict
* Passwords.: 4
* Bytes.....: 27
* Keyspace..: 4
* Runtime...: 0 secs

The wordlist or mask that you are using is too small.
This means that hashcat cannot use the full parallel power of your device(s).
Unless you supply more work, your cracking speed will drop.
For tips on supplying more work, see: https://hashcat.net/faq/morework

Approaching final keyspace - workload adjusted.

1132fe0c4288f794ebf0b330344ecafdcdd01ee9:dnt
5e6ef6ececbc479438947268e744a8097eb19b62:dntdnt
f79f429101e0eb00b8132fc6874aec01315f2088:[redacted]

Session..........: hashcat
Status...........: Cracked
Hash.Type........: MySQL4.1/MySQL5
Hash.Target......: test.hash
Time.Started.....: Mon Aug 19 01:46:34 2019 (0 secs)
```

5.1.参数说明

```
-a 指定要使用的破解模式，其值参考后面对参数。“-a 0”字典攻击，“-a 1” 组合攻击；“-a 3”掩码攻
击。
-m 指定要破解的hash类型，如果不指定类型，则默认是MD5
-o 指定破解成功后的hash及所对应的明文密码的存放位置,可以用它把破解成功的hash写到指定的文件中
--force 忽略破解过程中的警告信息,跑单条hash可能需要加上此选项
--show 显示已经破解的hash及该hash所对应的明文
--increment 启用增量破解模式,你可以利用此模式让hashcat在指定的密码长度范围内执行破解过程
--increment-min 密码最小长度,后面直接等于一个整数即可,配置increment模式一起使用
--increment-max 密码最大长度,同上
--outfile-format 指定破解结果的输出格式id,默认是3
--username   忽略hash文件中的指定的用户名,在破解linux系统用户密码hash可能会用到
--remove    删除已被破解成功的hash
-r     使用自定义破解规则
```

5.2.攻击模式

```
0 = Straight  (字典破解)

1 = Combination  (组合破解)

2 = Toggle-Case  (大小写转换)

3 = Brute-force (掩码暴力破解)

4 = Permutation (序列破解)

5 = Table-Lookup (查表破解)

6 = Hybrid dict + mask 字典加掩码破解

7 = Hybrid mask + dict 掩码+字典破解

8 = Prince (王子破解)
```

5.3.Hash类型

```
0 = MD5

10 = md5($pass.$salt)

20 = md5($salt.$pass)

30 = md5(unicode($pass).$salt)

40 = md5($salt.unicode($pass))

50 = HMAC-MD5 (key = $pass)

60 = HMAC-MD5 (key = $salt)

100 = SHA1

110 = sha1($pass.$salt)
```

```
120 = sha1($salt.$pass)

130 = sha1(unicode($pass).$salt)

140 = sha1($salt.unicode($pass))

150 = HMAC-SHA1 (key = $pass)

160 = HMAC-SHA1 (key = $salt)

200 = MySQL323

300 = MySQL4.1/MySQL5

400 = phpass, MD5(WordPress), MD5(phpBB3),MD5(Joomla)

500 = md5crypt, MD5(Unix), FreeBSD MD5,Cisco-IOS MD5

900 = MD4

1000 = NTLM

1100 = Domain Cached Credentials (DCC), MSCache

1400 = SHA256

1410 = sha256($pass.$salt)

1420 = sha256($salt.$pass)

1430 = sha256(unicode($pass).$salt)

1431 = base64(sha256(unicode($pass)))

1440 = sha256($salt.unicode($pass))

1450 = HMAC-SHA256 (key = $pass)

1460 = HMAC-SHA256 (key = $salt)

1600 = md5apr1, MD5(APR), Apache MD5

1700 = SHA512

1710 = sha512($pass.$salt)

1720 = sha512($salt.$pass)

1730 = sha512(unicode($pass).$salt)

1740 = sha512($salt.unicode($pass))
```

```
1750 = HMAC-SHA512 (key = $pass)

1760 = HMAC-SHA512 (key = $salt)

1800 = SHA-512(Unix)

2400 = Cisco-PIX MD5

2410 = Cisco-ASA MD5

2500 = WPA/WPA2

2600 = Double MD5

3200 = bcrypt, Blowfish(OpenBSD)

3300 = MD5(Sun)

3500 = md5(md5(md5($pass)))

3610 = md5(md5($salt).$pass)

3710 = md5($salt.md5($pass))

3720 = md5($pass.md5($salt))

3800 = md5($salt.$pass.$salt)

3910 = md5(md5($pass).md5($salt))

4010 = md5($salt.md5($salt.$pass))

4110 = md5($salt.md5($pass.$salt))

4210 = md5($username.0.$pass)

4300 = md5(strtoupper(md5($pass)))

4400 = md5(sha1($pass))

4500 = Double SHA1

4600 = sha1(sha1(sha1($pass)))

4700 = sha1(md5($pass))

4800 = MD5(Chap), iSCSI CHAP authentication

4900 = sha1($salt.$pass.$salt)

5000 = SHA-3(Keccak)

5100 = Half MD5
```

```
5200 = Password Safe SHA-256

5300 = IKE-PSK MD5

5400 = IKE-PSK SHA1

5500 = NetNTLMv1-VANILLA / NetNTLMv1-ESS

5600 = NetNTLMv2

5700 = Cisco-IOS SHA256

5800 = Android PIN

6300 = AIX {smd5}

6400 = AIX {ssha256}

6500 = AIX {ssha512}

6700 = AIX {ssha1}

6900 = GOST, GOST R 34.11-94

7000 = Fortigate (FortiOS)

7100 = OS X v10.8+

7200 = GRUB 2

7300 = IPMI2 RAKP HMAC-SHA1

7400 = sha256crypt, SHA256(Unix)

7900 = Drupal7

8400 = WBB3, Woltlab Burning Board 3

8900 = scrypt

9200 = Cisco $8$

9300 = Cisco $9$

9800 = Radmin2

10000 = Django (PBKDF2-SHA256)

10200 = Cram MD5

10300 = SAP CODVN H (PWDSALTEDHASH) iSSHA-1
```

```
11000 = PrestaShop

11100 = PostgreSQL Challenge-ResponseAuthentication (MD5)

11200 = MySQL Challenge-Response Authentication(SHA1)

11400 = SIP digest authentication (MD5)

99999 = Plaintext

特殊哈希类型

11 = Joomla < 2.5.18

12 = PostgreSQL

21 = osCommerce, xt:Commerce

23 = Skype

101 = nsldap, SHA-1(Base64), Netscape LDAPSHA

111 = nsldaps, SSHA-1(Base64), Netscape LDAPSSHA

112 = Oracle S: Type (Oracle 11+)

121 = SMF > v1.1

122 = OS X v10.4, v10.5, v10.6

123 = EPi

124 = Django (SHA-1)

131 = MSSQL(2000)

132 = MSSQL(2005)

133 = PeopleSoft

141 = EPiServer 6.x < v4

1421 = hMailServer

1441 = EPiServer 6.x > v4

1711 = SSHA-512(Base64), LDAP {SSHA512}

1722 = OS X v10.7

1731 = MSSQL(2012 & 2014)

2611 = vBulletin < v3.8.5
```

```
2612 = PHPS

2711 = vBulletin > v3.8.5

2811 = IPB2+, MyBB1.2+

3711 = Mediawiki B type

3721 = WebEdition CMS

7600 = Redmine Project Management Web App
```

附录

1.获取系统信息

```
# 获取数据库版本
MariaDB [(none)]> select version();
+----------------+
| version()      |
+----------------+
| 5.5.60-MariaDB |
+----------------+
1 row in set (0.00 sec)

MariaDB [(none)]> select @@version;
+----------------+
| @@version      |
+----------------+
| 5.5.60-MariaDB |
+----------------+
1 row in set (0.00 sec)

# 获取操作系统
MariaDB [(none)]> select @@version_compile_os;
+----------------------+
| @@version_compile_os |
+----------------------+
| Linux                |
+----------------------+
1 row in set (0.00 sec)

# 获取主机名
MariaDB [(none)]> select @@hostname;
+-----------------------+
| @@hostname            |
+-----------------------+
| localhost.localdomain |
+-----------------------+
1 row in set (0.00 sec)

mysql> select @@hostname;
```

```
+------------+
| @@hostname |
+------------+
| bryan-pc   |
+------------+
1 row in set (0.00 sec)
```

2.获取DB信息

```
# 1.MySQL5.x可以通过schemata表来查询`权限范围内`的数据库
MariaDB [safe_db]> select schema_name from information_schema.schemata;
+--------------------+
| schema_name        |
+--------------------+
| information_schema |
| safe_db            |
| work_db            |
+--------------------+
3 rows in set (0.00 sec)

# 验证如下: show databases;
MariaDB [safe_db]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| safe_db            |
| work_db            |
+--------------------+
3 rows in set (0.00 sec)

# 【root】显示所有数据库
MariaDB [(none)]> select schema_name from information_schema.schemata;
+--------------------+
| schema_name        |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| safe_db            |
| test_db            |
| work_db            |
+--------------------+
6 rows in set (0.00 sec)

# 【root】显示所有数据库（只要授权过的数据库都会显示出来）
MariaDB [(none)]> select distinct(db) from mysql.db;
+---------+
| db      |
+---------+
| safe_db |
| test_db |
| work_db |
+---------+
3 rows in set (0.00 sec)

# 获取当前数据库
MariaDB [safe_db]> select database();
+------------+
| database() |
+------------+
| safe_db    |
+------------+
1 row in set (0.00 sec)

# 2.查询safe_db里的表名和视图
MariaDB [safe_db]> select table_schema,table_name,table_type,engine
from information_schema.tables where table_schema = 'safe_db';
+--------------+---------------+------------+--------+
| table_schema | table_name    | table_type | engine |
+--------------+---------------+------------+--------+
| safe_db      | file_records  | BASE TABLE | InnoDB |
| safe_db      | users         | BASE TABLE | InnoDB |
| safe_db      | view_userinfo | VIEW       | NULL   |
+--------------+---------------+------------+--------+
3 rows in set (0.00 sec)

# 3.查询指定表含哪些列
MariaDB [(none)]> select table_schema,table_name,column_name from information_schema.columns
where table_schema= 'safe_db' and table_name = 'users';
+--------------+------------+-------------+
| table_schema | table_name | column_name |
+--------------+------------+-------------+
| safe_db      | users      | id          |
| safe_db      | users      | username    |
| safe_db      | users      | password    |
| safe_db      | users      | email       |
| safe_db      | users      | tel         |
| safe_db      | users      | usercode    |
| safe_db      | users      | createtime  |
| safe_db      | users      | updatetime  |
| safe_db      | users      | datastatus  |
+--------------+------------+-------------+
9 rows in set (0.00 sec)

# 查询除内置数据库外其他数据库和表
MariaDB [(none)]> select table_schema,table_name,column_name from information_schema.columns
where table_schema != 'mysql' and table_schema != 'information_schema' order by
table_schema,table_name;
+--------------+---------------+-------------+
| table_schema | table_name    | column_name |
+--------------+---------------+-------------+
| safe_db      | file_records  | id          |
| safe_db      | file_records  | datastatus  |
| safe_db      | file_records  | createtime  |
| safe_db      | file_records  | url         |
| safe_db       | file_records  | ip           |
| safe_db       | file_records  | user_id      |
| safe_db       | file_records  | meta_type    |
| safe_db       | file_records  | md5          |
| safe_db       | file_records  | file_name    |
| safe_db       | users         | datastatus   |
| safe_db       | users         | updatetime   |
| safe_db       | users         | createtime   |
| safe_db       | users         | usercode     |
| safe_db       | users         | tel          |
| safe_db       | users         | email        |
| safe_db       | users         | password     |
| safe_db       | users         | username     |
| safe_db       | users         | id           |
| safe_db       | view_userinfo | datastatus   |
| safe_db       | view_userinfo | tel          |
| safe_db       | view_userinfo | email        |
| safe_db       | view_userinfo | password     |
| safe_db       | view_userinfo | username     |
| safe_db       | view_userinfo | id           |
| work_db       | users         | id           |
| work_db       | users         | user_name    |
| work_db       | users         | pass         |
+---------------+---------------+--------------+
27 rows in set (0.00 sec)

# 寻找自己感兴趣的列
MariaDB [(none)]> select table_schema,table_name,column_name from information_schema.columns
where column_name like 'pass%' or column_name like 'user%';
+--------------------+-----------------+-------------+
| table_schema       | table_name      | column_name |
+--------------------+-----------------+-------------+
| information_schema | PROCESSLIST     | USER        |
| information_schema | USER_STATISTICS | USER        |
| safe_db            | file_records    | user_id     |
| safe_db            | users           | username    |
| safe_db            | users           | password    |
| safe_db            | users           | usercode    |
| safe_db            | view_userinfo   | username    |
| safe_db            | view_userinfo   | password    |
| work_db            | users           | user_name   |
| work_db            | users           | pass        |
+--------------------+-----------------+-------------+
10 rows in set (0.01 sec)

# 获取数据库安装目录
MariaDB [(none)]> select @@basedir;
+-----------+
| @@basedir |
+-----------+
| /usr      |
+-----------+
1 row in set (0.00 sec)
```

```
# 获取数据目录
MariaDB [(none)]> select @@datadir;
+------------------+
| @@datadir        |
+------------------+
| /var/lib/mysql/ |
+------------------+
1 row in set (0.00 sec)
```

3.获取用户信息

```
# 查看当前用户
MariaDB [(none)]> select user();
+------------------+
| user()           |
+------------------+
| bryan@localhost |
+------------------+
1 row in set (0.00 sec)

MariaDB [(none)]> select system_user();
+------------------+
| system_user()    |
+------------------+
| bryan@localhost |
+------------------+
1 row in set (0.00 sec)

MariaDB [(none)]> select current_user;
+---------------+
| current_user |
+---------------+
| bryan@%       |
+---------------+
1 row in set (0.00 sec)

# MariaDB5.x ~ 【root】显示所有用户（含密码）
MariaDB [(none)]> select user,host,password from mysql.user;
+-------+-----------+-------------------------------------------+
| user  | host      | password                                  |
+-------+-----------+-------------------------------------------+
| root  | localhost | *5E6EF6ECECBC479438947268E744A8097EB19B62 |
| root  | %         |                                           |
| root  | 127.0.0.1 | *5E6EF6ECECBC479438947268E744A8097EB19B62 |
| root  | ::1       | *5E6EF6ECECBC479438947268E744A8097EB19B62 |
| bryan | %         | *F79F429101E0EB00B8132FC6874AEC01315F2088 |
| dnt   | %         | *1132FE0C4288F794EBF0B330344ECAFDCDD01EE9 |
+-------+-----------+-------------------------------------------+

# MySQL5.x ~ 【root】显示所有用户（含密码）
mysql> select user,host,authentication_string from mysql.user;
```

```
+------------------+-----------+-------------------------------------------+
| user             | host      | authentication_string                     |
+------------------+-----------+-------------------------------------------+
| root             | localhost |                                           |
| mysql.session    | localhost | *THISISNOTAVALIDPASSWORDTHATCANBEUSEDHERE |
| mysql.sys        | localhost | *THISISNOTAVALIDPASSWORDTHATCANBEUSEDHERE |
| debian-sys-maint | localhost | *8D894A8D6A636A0B04DAABD0905B58349E106D6E |
| bryan            | %         | *F79F429101E0EB00B8132FC6874AEC01315F2088 |
+------------------+-----------+-------------------------------------------+
5 rows in set (0.02 sec)

# PS: MySQL的sha1是变种加密
MariaDB [safe_db]> select password('xxxx');
+-------------------------------------------+
| password('xxxx')                          |
+-------------------------------------------+
| *F79F429101E0EB00B8132FC6874AEC01315F2088 |
+-------------------------------------------+
1 row in set (0.00 sec)

# 查看指定数据库授予用户的权限
MariaDB [(none)]>  select grantee, table_schema, privilege_type from
information_schema.schema_privileges where table_schema = 'safe_db';
+-------------+--------------+-------------------------+
| grantee     | table_schema | privilege_type          |
+-------------+--------------+-------------------------+
| 'bryan'@'%' | safe_db      | SELECT                  |
| 'bryan'@'%' | safe_db      | INSERT                  |
| 'bryan'@'%' | safe_db      | UPDATE                  |
| 'bryan'@'%' | safe_db      | DELETE                  |
| 'bryan'@'%' | safe_db      | CREATE                  |
| 'bryan'@'%' | safe_db      | DROP                    |
| 'bryan'@'%' | safe_db      | REFERENCES              |
| 'bryan'@'%' | safe_db      | INDEX                   |
| 'bryan'@'%' | safe_db      | ALTER                   |
| 'bryan'@'%' | safe_db      | CREATE TEMPORARY TABLES |
| 'bryan'@'%' | safe_db      | LOCK TABLES             |
| 'bryan'@'%' | safe_db      | EXECUTE                 |
| 'bryan'@'%' | safe_db      | CREATE VIEW             |
| 'bryan'@'%' | safe_db      | SHOW VIEW               |
| 'bryan'@'%' | safe_db      | CREATE ROUTINE          |
| 'bryan'@'%' | safe_db      | ALTER ROUTINE           |
| 'bryan'@'%' | safe_db      | EVENT                   |
| 'bryan'@'%' | safe_db      | TRIGGER                 |
+-------------+--------------+-------------------------+
18 rows in set (0.00 sec)

# 查询用户权限列表
MariaDB [(none)]> select grantee, privilege_type, is_grantable from
information_schema.user_privileges;
+-------------+----------------+--------------+
| grantee     | privilege_type | is_grantable |
+-------------+----------------+--------------+
| 'bryan'@'%' | USAGE          | NO           |
+-------------+----------------+--------------+
1 row in set (0.00 sec)

MariaDB [safe_db]> show grants for bryan;
+-------------------------------------------------------+
| Grants for bryan@%                                    |
+-------------------------------------------------------+
| GRANT USAGE ON *.* TO 'bryan'@'%' IDENTIFIED BY PASSWORD
'*F79F429101E0EB00B8132FC6874AEC01315F2088' |
| GRANT ALL PRIVILEGES ON `safe_db`.* TO 'bryan'@'%' |
| GRANT ALL PRIVILEGES ON `work_db`.* TO 'bryan'@'%' |
+-------------------------------------------------------+
3 rows in set (0.00 sec)

# 【root】用户查看全部用户权限列表
MariaDB [safe_db]> select grantee, privilege_type, is_grantable from
information_schema.user_privileges;
+---------------------+-------------------------+--------------+
| grantee             | privilege_type          | is_grantable |
+---------------------+-------------------------+--------------+
| 'root'@'localhost' | SELECT                  | YES          |
| 'root'@'localhost' | INSERT                  | YES          |
| 'root'@'localhost' | UPDATE                  | YES          |
| 'root'@'localhost' | DELETE                  | YES          |
| 'root'@'localhost' | CREATE                  | YES          |
| 'root'@'localhost' | DROP                    | YES          |
| 'root'@'localhost' | RELOAD                  | YES          |
| 'root'@'localhost' | SHUTDOWN                | YES          |
| 'root'@'localhost' | PROCESS                 | YES          |
| 'root'@'localhost' | FILE                    | YES          |
| 'root'@'localhost' | REFERENCES              | YES          |
| 'root'@'localhost' | INDEX                   | YES          |
| 'root'@'localhost' | ALTER                   | YES          |
| 'root'@'localhost' | SHOW DATABASES          | YES          |
| 'root'@'localhost' | SUPER                   | YES          |
| 'root'@'localhost' | CREATE TEMPORARY TABLES | YES          |
| 'root'@'localhost' | LOCK TABLES             | YES          |
| 'root'@'localhost' | EXECUTE                 | YES          |
| 'root'@'localhost' | REPLICATION SLAVE       | YES          |
| 'root'@'localhost' | REPLICATION CLIENT      | YES          |
| 'root'@'localhost' | CREATE VIEW             | YES          |
| 'root'@'localhost' | SHOW VIEW               | YES          |
| 'root'@'localhost' | CREATE ROUTINE          | YES          |
| 'root'@'localhost' | ALTER ROUTINE           | YES          |
| 'root'@'localhost' | CREATE USER             | YES          |
| 'root'@'localhost' | EVENT                   | YES          |
| 'root'@'localhost' | TRIGGER                 | YES          |
| 'root'@'localhost' | CREATE TABLESPACE       | YES          |
| 'root'@'127.0.0.1' | SELECT                  | YES          |
| 'root'@'127.0.0.1' | INSERT                  | YES          |
| 'root'@'127.0.0.1' | UPDATE                  | YES          |
| 'root'@'127.0.0.1' | DELETE                  | YES          |
| 'root'@'127.0.0.1' | CREATE                  | YES          |
| 'root'@'127.0.0.1' | DROP                    | YES          |
| 'root'@'127.0.0.1' | RELOAD                  | YES          |
| 'root'@'127.0.0.1' | SHUTDOWN                | YES          |
| 'root'@'127.0.0.1' | PROCESS                 | YES          |
| 'root'@'127.0.0.1' | FILE                    | YES          |
| 'root'@'127.0.0.1' | REFERENCES              | YES          |
| 'root'@'127.0.0.1' | INDEX                   | YES          |
| 'root'@'127.0.0.1' | ALTER                   | YES          |
| 'root'@'127.0.0.1' | SHOW DATABASES          | YES          |
| 'root'@'127.0.0.1' | SUPER                   | YES          |
| 'root'@'127.0.0.1' | CREATE TEMPORARY TABLES | YES          |
| 'root'@'127.0.0.1' | LOCK TABLES             | YES          |
| 'root'@'127.0.0.1' | EXECUTE                 | YES          |
| 'root'@'127.0.0.1' | REPLICATION SLAVE       | YES          |
| 'root'@'127.0.0.1' | REPLICATION CLIENT      | YES          |
| 'root'@'127.0.0.1' | CREATE VIEW             | YES          |
| 'root'@'127.0.0.1' | SHOW VIEW               | YES          |
| 'root'@'127.0.0.1' | CREATE ROUTINE          | YES          |
| 'root'@'127.0.0.1' | ALTER ROUTINE           | YES          |
| 'root'@'127.0.0.1' | CREATE USER             | YES          |
| 'root'@'127.0.0.1' | EVENT                   | YES          |
| 'root'@'127.0.0.1' | TRIGGER                 | YES          |
| 'root'@'127.0.0.1' | CREATE TABLESPACE       | YES          |
| 'root'@'::1'       | SELECT                  | YES          |
| 'root'@'::1'       | INSERT                  | YES          |
| 'root'@'::1'       | UPDATE                  | YES          |
| 'root'@'::1'       | DELETE                  | YES          |
| 'root'@'::1'       | CREATE                  | YES          |
| 'root'@'::1'       | DROP                    | YES          |
| 'root'@'::1'       | RELOAD                  | YES          |
| 'root'@'::1'       | SHUTDOWN                | YES          |
| 'root'@'::1'       | PROCESS                 | YES          |
| 'root'@'::1'       | FILE                    | YES          |
| 'root'@'::1'       | REFERENCES              | YES          |
| 'root'@'::1'       | INDEX                   | YES          |
| 'root'@'::1'       | ALTER                   | YES          |
| 'root'@'::1'       | SHOW DATABASES          | YES          |
| 'root'@'::1'       | SUPER                   | YES          |
| 'root'@'::1'       | CREATE TEMPORARY TABLES | YES          |
| 'root'@'::1'       | LOCK TABLES             | YES          |
| 'root'@'::1'       | EXECUTE                 | YES          |
| 'root'@'::1'       | REPLICATION SLAVE       | YES          |
| 'root'@'::1'       | REPLICATION CLIENT      | YES          |
| 'root'@'::1'       | CREATE VIEW             | YES          |
| 'root'@'::1'       | SHOW VIEW               | YES          |
| 'root'@'::1'       | CREATE ROUTINE          | YES          |
| 'root'@'::1'       | ALTER ROUTINE           | YES          |
| 'root'@'::1'       | CREATE USER             | YES          |
| 'root'@'::1'       | EVENT                   | YES          |
| 'root'@'::1'       | TRIGGER                 | YES          |
| 'root'@'::1'       | CREATE TABLESPACE       | YES          |
| 'root'@'%'         | USAGE                   | NO           |
| 'bryan'@'%'          | USAGE                    | NO            |
| 'dnt'@'%'            | USAGE                    | NO            |
+--------------------+-------------------------+--------------+
87 rows in set (0.00 sec)

# 【root】查询更详细的用户权限
MariaDB [safe_db]> select host, user, Select_priv, Insert_priv, Update_priv, Delete_priv,
Create_priv, Drop_priv, Reload_priv, Shutdown_priv, Process_priv, File_priv, Grant_priv,
References_priv, Index_priv, Alter_priv, Show_db_priv, Super_priv, Create_tmp_table_priv,
Lock_tables_priv, Execute_priv, Repl_slave_priv, Repl_client_priv from mysql.user\G;

*************************** 1. row ***************************
                 host: %
                 user: root
          Select_priv: N
          Insert_priv: N
          Update_priv: N
          Delete_priv: N
          Create_priv: N
            Drop_priv: N
          Reload_priv: N
        Shutdown_priv: N
         Process_priv: N
            File_priv: N
           Grant_priv: N
      References_priv: N
           Index_priv: N
           Alter_priv: N
         Show_db_priv: N
           Super_priv: N
Create_tmp_table_priv: N
     Lock_tables_priv: N
         Execute_priv: N
      Repl_slave_priv: N
     Repl_client_priv: N

。。。。。。

*************************** 5. row ***************************
                 host: %
                 user: bryan
          Select_priv: N
          Insert_priv: N
          Update_priv: N
          Delete_priv: N
          Create_priv: N
            Drop_priv: N
          Reload_priv: N
        Shutdown_priv: N
         Process_priv: N
            File_priv: N
           Grant_priv: N
      References_priv: N
```

```
           Index_priv: N
           Alter_priv: N
         Show_db_priv: N
           Super_priv: N
Create_tmp_table_priv: N
     Lock_tables_priv: N
         Execute_priv: N
      Repl_slave_priv: N
     Repl_client_priv: N
*************************** 6. row ***************************
                 host: %
                 user: dnt
          Select_priv: N
          Insert_priv: N
          Update_priv: N
          Delete_priv: N
          Create_priv: N
            Drop_priv: N
          Reload_priv: N
        Shutdown_priv: N
         Process_priv: N
            File_priv: N
           Grant_priv: N
      References_priv: N
           Index_priv: N
           Alter_priv: N
         Show_db_priv: N
           Super_priv: N
Create_tmp_table_priv: N
     Lock_tables_priv: N
         Execute_priv: N
      Repl_slave_priv: N
     Repl_client_priv: N
6 rows in set (0.00 sec)

# PS：获取列的权限列表（用的不多）
select table_schema, table_name, column_name, privilege_type from
information_schema.column_privileges;

# PS：查询数据库支持哪些权限
mysql> 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
                        |
| 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      |
| Replication client      | Server Admin                           | To ask where the slave or
master servers are          |
| 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 use KILL thread, SET
GLOBAL, CHANGE MASTER, etc.   |
| Trigger                 | Tables                                 | To use triggers
                        |
| Create tablespace       | Server Admin                           | To create/alter/drop
tablespaces                      |
| Update                    | Tables                                  | To update existing rows
                         |
| Usage                     | Server Admin                            | No privileges - allow connect
only                     |
+---------------------------+---------------------------------------+------------------------------
-------------------------+
31 rows in set (0.00 sec)
```

other

```
# 获取会话id
MariaDB [(none)]> select connection_id();
+-----------------+
| connection_id() |
+-----------------+
|               6 |
+-----------------+
1 row in set (0.00 sec)

# 获取最后一个插入的id
MariaDB [(none)]> select last_insert_id();
+------------------+
| last_insert_id() |
+------------------+
|                0 |
+------------------+
1 row in set (0.00 sec)

# 返回前一个SQL进行`update、delete、insert`操作所影响的行数
MariaDB [(none)]> select row_count();
+-------------+
| row_count() |
+-------------+
|          -1 |
+-------------+
1 row in set (0.00 sec)
```

参考链接

国外常用的SQLi备忘录：

- MySQL： http://pentestmonkey.net/category/cheat-sheet
- MSSQL： http://pentestmonkey.net/cheat-sheet/sql-injection/mssql-sql-injection-cheat-sheet

MySQL系统表相关知识：

- https://blog.csdn.net/xlxxcc/article/details/51754524
- https://jingyan.baidu.com/article/636f38bb8e6b3ad6b84610df.html

HashCat使用： https://www.freebuf.com/sectool/164507.html