系统表相关学习

1.利用数据库读写文件及所需条件

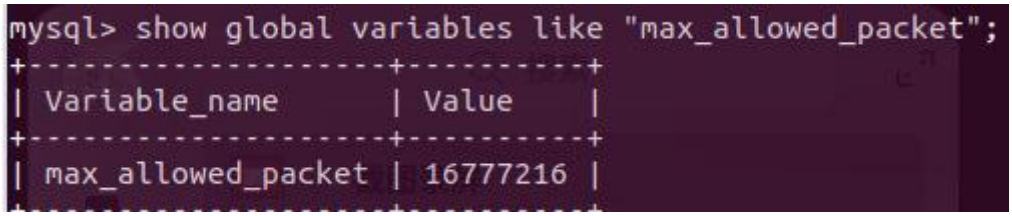
1.1 load_file

1.1.1 条件

1.1.1.1文件权限和大小

（1）对该文件可读

（2）大小小于max_allowed_packet



1.1.1.2 用户权限

有FILE

1.1.1.3 可操作路径

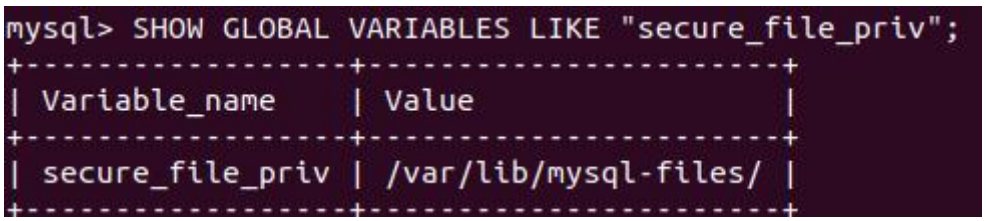
查看secure_file_priv，它被用来限制

load_file, load data, select sql outfile操作哪个目录

为NULL，表示不可导入导出

为具体目录，表示只可对该目录下文件操作

无具体值，表示无限制



1.1.2 读取数据

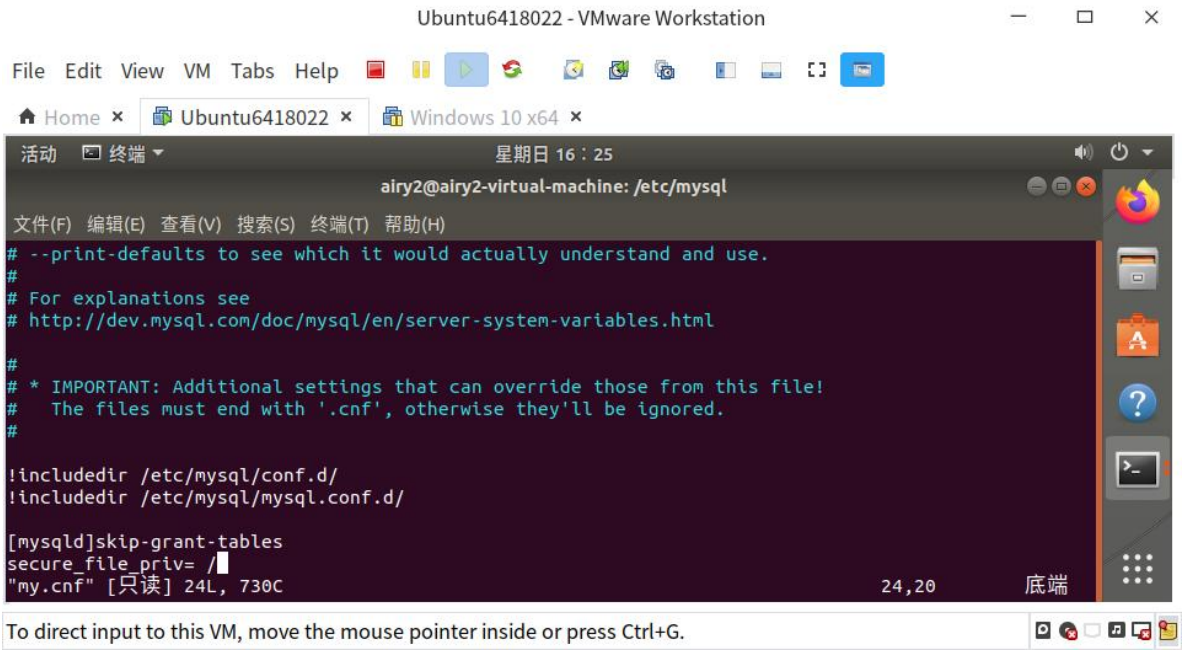
这里我已进入新建的库

```
CREATE TABLE user(data text);
INSERT INTI user(data) VALUES(load_file('/var/lib/mysql-files'));
```

读取失败

```
mysql> select * from user;
+------+
| data |
+------+
| NULL |
+------+
```

更改my.cnf配置



重启mysql

```
sudo service mysql restart
```

以 /etc/passwd为目标文件读取

```
mysql> INSERT INTO user(data) VALUES(load_file('/etc/passwd'));
```

```
mysql> INSERT INTO user(data) VALUES(load_file('/etc/passwd'));
Query OK, 1 row affected (0.00 sec)

mysql> SELECT * FROM user;
+--------------------------------------------------------------------
--------------------------------------------------------------------
--------------------------------------------------------------------
--------------------------------------------------------------------
```

1.2 load data infile

1.2.1 条件

1.2.1.1文件权限

可读 / 可写

1.2.1.2 用户权限

FILE

1.2.1.3 可操作路径

secure_file_priv

```
mysql> load data infile '/etc/passwd' INTO TABLE user;
Query OK, 42 rows affected (0.01 sec)
Records: 42  Deleted: 0  Skipped: 0  Warnings: 0

mysql> SELECT * FROM user;
+-----------------------------------------------------
-----------------------------------------------------
-----------------------------------------------------
-----------------------------------------------------
```

```
| root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
```

load_file() 和 load data infile 基本没有区别，不过在注入过程中，load_file()往往会被过滤掉，而 load data infile 可以使用

1.3 system cat

```
mysql> system cat '/etc/passwd';
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
```

注意：

1.此方法只能在本地读取，远程连接mysql时无法使用system

2.无法越权读取

1.4 select sql outfile

1.4.1 条件

1.4.1.1 文件权限

可写

1.4.1.2 用户权限

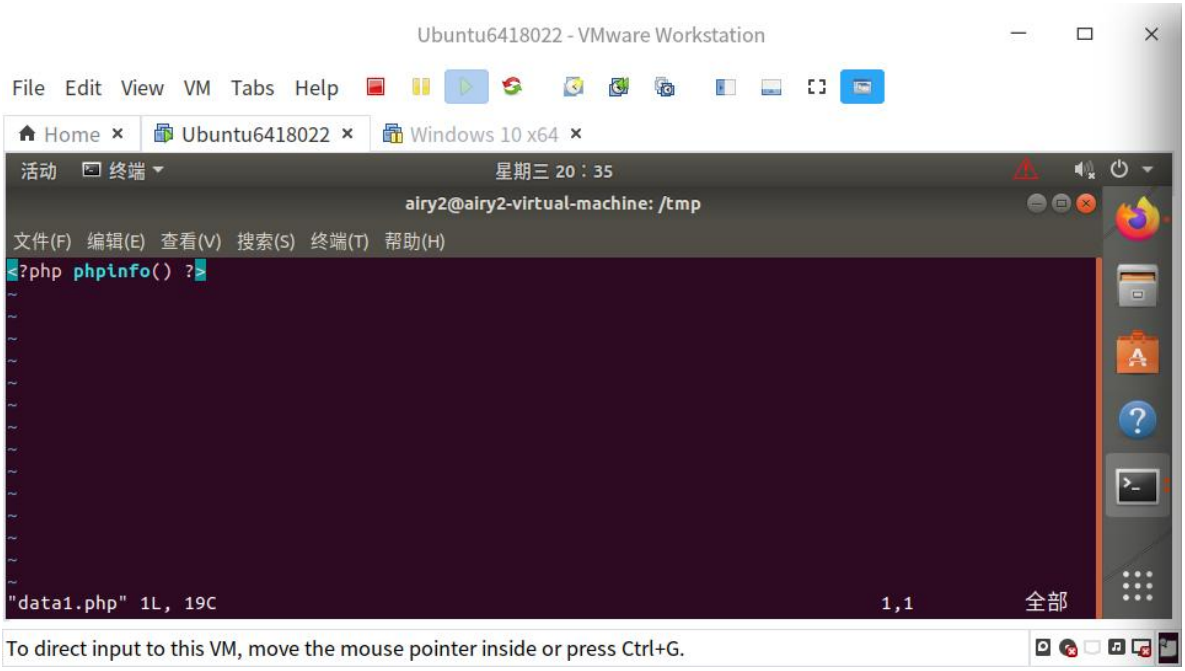
FILE

1.4.1.3 可操作路径

secure_file_priv

```
mysql> select '<?php phpinfo() ?>' into outfile "/tmp/data1.php";
Query OK, 1 row affected (0.00 sec)
```

```
airy2@airy2-virtual-machine:/etc/nginx/sites-enabled$ cd /tmp/
airy2@airy2-virtual-machine:/tmp$ ls
config-err-Z86dUi
data1.php
data.php
hsperfdata_airy2
mozilla_airy20
```



1.4.2 问题

这里虽然能够写入/tmp文件夹，但是对于没有权限的/var/www/test文件夹无法写入，然而虽然知道原因，仍不知如何给予mysql权限（尝试过更改权限，最后导致mysql无法运行）