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

```
https://www.xp.cn/jishu-php-3132.html   phpstudy for linux版环境安装
```

之前搭建的是apache+php+postgresql，为了能够偷懒，默默打开了phpstudy。。。。。。。。。。

首先是MYSQL

1.配置中的secure_file_priv变量

```
###################以root登录
###########################读文件
mysql> show global variables like "%secure_file_priv%";
+------------------+-----------------------+
| Variable_name    | Value                 |
+------------------+-----------------------+
| secure_file_priv | /var/lib/mysql-files/ |
+------------------+-----------------------+
1 row in set (0.00 sec)

mysql> select load_file('/etc/passwd');
+--------------------------+
| load_file('/etc/passwd') |
+--------------------------+
| NULL                     |
+--------------------------+
1 row in set (0.00 sec)

mysql> select load_file('/var/lib/mysql-files/1');
+-------------------------------------+
| load_file('/var/lib/mysql-files/1') |
+-------------------------------------+
| jambolt
                            |
+-------------------------------------+
1 row in set (0.00 sec)
##########################写文件
mysql> select load_file('/var/lib/mysql-files/1');
+-------------------------------------+
| load_file('/var/lib/mysql-files/1') |
+-------------------------------------+
| jambolt
                            |
+-------------------------------------+
1 row in set (0.00 sec)

mysql> select 'jambolt' into outfile'/var/lib/mysql-files/3';
Query OK, 1 row affected (0.00 sec)

mysql> select load_file('/var/lib/mysql-files/3');
```

```
+-------------------------------------+
| load_file('/var/lib/mysql-files/3') |
+-------------------------------------+
| jambolt
                            |
+-------------------------------------+
1 row in set (0.00 sec)

mysql> select load_file('/etc/123');
+-----------------------+
| load_file('/etc/123') |
+-----------------------+
| NULL                  |
+-----------------------+
1 row in set (0.00 sec)
```

2.mysql账户拥有文件的读写权限

查看用户权限

```
mysql> select * from mysql.user where user='root';
+-----------+------+-------------+-------------+-------------+-------------+----
---------+-----------+-------------+---------------+--------------+-----------+-
-----------+-----------------+------------+------------+--------------+---------
---+-----------------------+------------------+--------------+-----------------
+------------------+------------------+----------------+---------------------+--
------------------+------------------+------------+--------------+--------------
----------+----------+------------+-------------+--------------+---------------
+-------------+-----------------+----------------------+-----------------------
+-------------------------------------------+------------------+----------------
-------+-------------------+----------------+
| 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 | ssl_type | ssl_cipher | x509_issuer |
x509_subject | max_questions | max_updates | max_connections |
max_user_connections | plugin                | authentication_string
        | password_expired | password_last_changed | password_lifetime |
account_locked |
+-----------+------+-------------+-------------+-------------+-------------+----
---------+-----------+-------------+---------------+--------------+-----------+-
-----------+-----------------+------------+------------+--------------+---------
---+-----------------------+------------------+--------------+-----------------
+------------------+------------------+----------------+---------------------+--
------------------+------------------+------------+--------------+--------------
----------+----------+------------+-------------+--------------+---------------
+-------------+-----------------+----------------------+-----------------------
+-------------------------------------------+------------------+----------------
-------+-------------------+----------------+
| localhost | root | Y           | Y           | Y           | Y           | Y
        | Y         | Y           | Y             | Y            | Y         | Y
         | Y               | Y          | Y          | Y            | Y
| Y                     | Y                | Y            | Y               | Y
               | Y                | Y              | Y                   | Y
             | Y                | Y          | Y            | Y
     |          |            |             |              |             0 |
      0 |               0 |                    0 | mysql_native_password |
*36E11893339B331EC468212189CFB3ABF80CB458 | N                | 2019-08-12
18:56:37   |              NULL | N              |
+-----------+------+-------------+-------------+-------------+-------------+----
---------+-----------+-------------+---------------+--------------+-----------+-
-----------+-----------------+------------+------------+--------------+---------
---+-----------------------+------------------+--------------+-----------------
+------------------+------------------+----------------+---------------------+--
------------------+------------------+------------+--------------+--------------
----------+----------+------------+-------------+--------------+---------------
+-------------+-----------------+----------------------+-----------------------
+-------------------------------------------+------------------+----------------
-------+-------------------+----------------+
1 row in set (0.00 sec)
```

```
#创建新用户
mysql> create user 'jambolt'@'localhost' identified by 'Jam@123456';
Query OK, 0 rows affected (0.00 sec)
#更新权限
mysql> flush privileges;
Query OK, 0 rows affected (0.00 sec)
#查看新用户权限
mysql> select * from mysql.user where user='jambolt';
+-----------+---------+-------------+-------------+-------------+-------------+-
------------+-----------+-------------+---------------+--------------+----------
-+------------+-----------------+------------+------------+--------------+------
------+-----------------------+------------------+--------------+---------------
--+------------------+------------------+----------------+---------------------
+--------------------+------------------+------------+--------------+-----------
-------------+----------+------------+-------------+--------------+-------------
--+-------------+-----------------+----------------------+----------------------
-+-------------------------------------------+------------------+---------------
--------+-------------------+----------------+
| 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 | ssl_type | ssl_cipher | x509_issuer |
x509_subject | max_questions | max_updates | max_connections |
max_user_connections | plugin                | authentication_string
        | password_expired | password_last_changed | password_lifetime |
account_locked |
+-----------+---------+-------------+-------------+-------------+-------------+-
------------+-----------+-------------+---------------+--------------+----------
-+------------+-----------------+------------+------------+--------------+------
------+-----------------------+------------------+--------------+---------------
--+------------------+------------------+----------------+---------------------
+--------------------+------------------+------------+--------------+-----------
-------------+----------+------------+-------------+--------------+-------------
--+-------------+-----------------+----------------------+----------------------
-+-------------------------------------------+------------------+---------------
--------+-------------------+----------------+
| localhost | jambolt | N           | N           | N           | N           |
N           | N         | N           | N             | N            | N
| N          | N               | N          | N          | N            | N
     | N                     | N                | N            | N
| N               | N                | N                | N                    | N
                | N                | N          | N            | N
         |          |            |             |              |            0 |
          0 |                0 |                      0 | mysql_native_password |
*084F91FFF15AB4E7A21BA39E44F82BC32DD5757D | N                | 2019-08-12
19:23:40   |              NULL | N              |
+-----------+---------+-------------+-------------+-------------+-------------+-
------------+-----------+-------------+---------------+--------------+----------
-+------------+-----------------+------------+------------+--------------+------
------+-----------------------+------------------+--------------+---------------
--+------------------+------------------+----------------+---------------------
+--------------------+------------------+------------+--------------+-----------
-------------+----------+------------+-------------+--------------+-------------
--+-------------+-----------------+----------------------+----------------------
-+-------------------------------------------+------------------+---------------
--------+-------------------+----------------+
1 row in set (0.00 sec)

mysql> exit
以jambolt登录
mysql> show global variables like "%secure_file_priv%";
+------------------+-----------------------+
| Variable_name    | Value                 |
+------------------+-----------------------+
| secure_file_priv | /var/lib/mysql-files/ |
+------------------+-----------------------+
1 row in set (0.01 sec)

mysql> select load_file('/var/lib/mysql-files/1');
+-------------------------------------+
| load_file('/var/lib/mysql-files/1') |
+-------------------------------------+
| NULL                                |
+-------------------------------------+
1 row in set (0.00 sec)

切换root添加权限
mysql> grant file on *.* to jambolt@localhost identified by 'Jam@123456';
Query OK, 0 rows affected, 1 warning (0.00 sec)
切换jambolt
mysql> select load_file('/var/lib/mysql-files/1');
+-------------------------------------+
| load_file('/var/lib/mysql-files/1') |
+-------------------------------------+
| jambolt
                            |
+-------------------------------------+
1 row in set (0.00 sec)
```

2.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

```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
+--------------------+
1 row in set (0.00 sec)
#查询数据库名
```

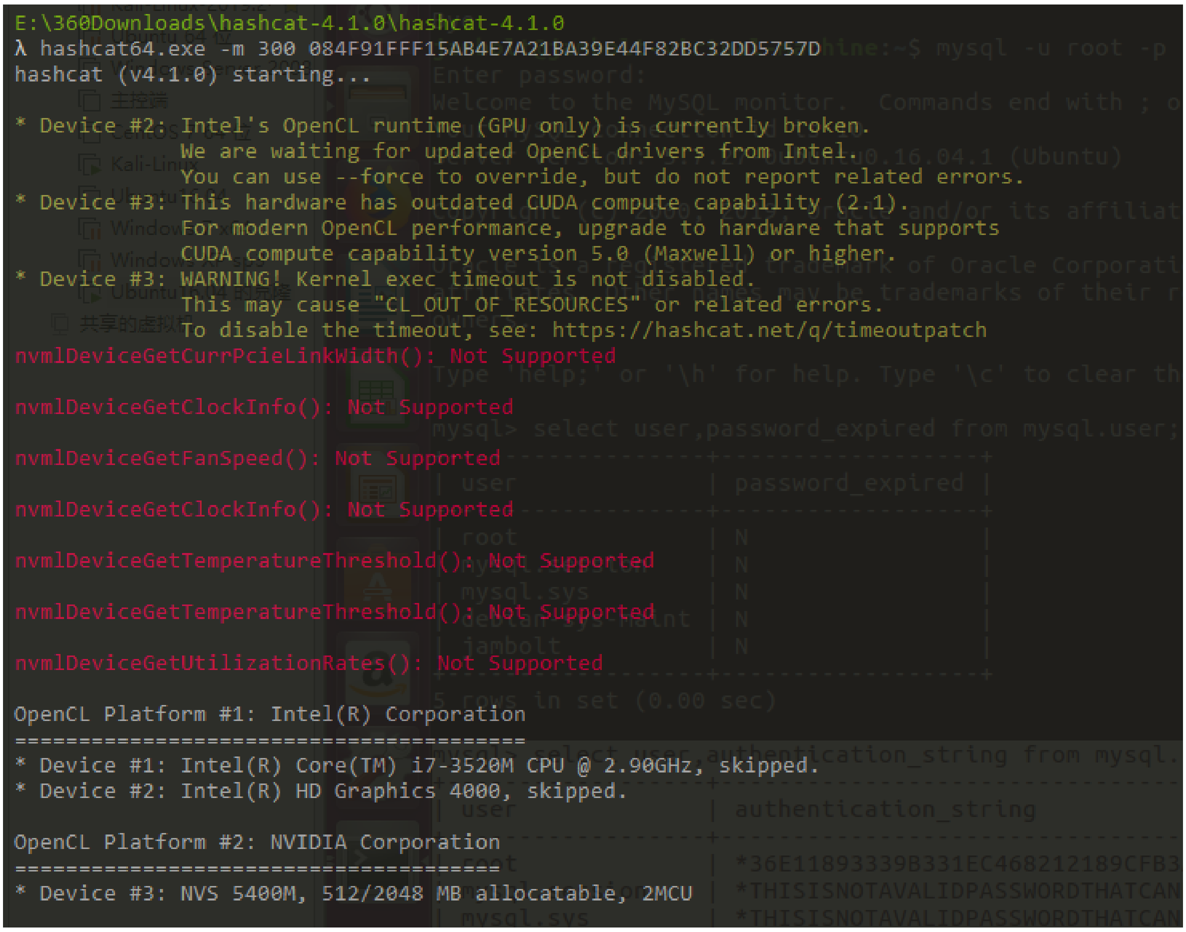
```
mysql> select schema_name from information_schema.SCHEMATA;
#查询表名
mysql> select table_name from information_schema.tables where
table_schema='information_schema';
#查询字段名
mysql> select column_name from information_schema.columns where
table_name='FILES';
+----------------------+
| column_name          |
+----------------------+
| FILE_ID              |
| FILE_NAME            |
| FILE_TYPE            |
| TABLESPACE_NAME      |
| TABLE_CATALOG        |
| TABLE_SCHEMA         |
| TABLE_NAME           |
| LOGFILE_GROUP_NAME   |
| LOGFILE_GROUP_NUMBER |
| ENGINE               |
| FULLTEXT_KEYS        |
| DELETED_ROWS         |
| UPDATE_COUNT         |
| FREE_EXTENTS         |
| TOTAL_EXTENTS        |
| EXTENT_SIZE          |
| INITIAL_SIZE         |
| MAXIMUM_SIZE         |
| AUTOEXTEND_SIZE      |
| CREATION_TIME        |
| LAST_UPDATE_TIME     |
| LAST_ACCESS_TIME     |
| RECOVER_TIME         |
| TRANSACTION_COUNTER  |
| VERSION              |
| ROW_FORMAT           |
| TABLE_ROWS           |
| AVG_ROW_LENGTH       |
| DATA_LENGTH          |
| MAX_DATA_LENGTH      |
| INDEX_LENGTH         |
| DATA_FREE            |
| CREATE_TIME          |
| UPDATE_TIME          |
| CHECK_TIME           |
| CHECKSUM             |
| STATUS               |
| EXTRA                |
+----------------------+
38 rows in set (0.00 sec)

#查询内容
mysql> select FILE_ID,FILE_NAME,FILE_TYPE from information_schema.FILES;
+---------+--------------------------------------+------------+
| FILE_ID | FILE_NAME                            | FILE_TYPE  |
+---------+--------------------------------------+------------+
|       0 | ./ibdata1                            | TABLESPACE |
|      20 | ./mysql/engine_cost.ibd              | TABLESPACE |
|       18 | ./mysql/gtid_executed.ibd             | TABLESPACE |
|        5 | ./mysql/help_category.ibd             | TABLESPACE |
|        7 | ./mysql/help_keyword.ibd              | TABLESPACE |
|        6 | ./mysql/help_relation.ibd             | TABLESPACE |
|        4 | ./mysql/help_topic.ibd                | TABLESPACE |
|       14 | ./mysql/innodb_index_stats.ibd        | TABLESPACE |
|       13 | ./mysql/innodb_table_stats.ibd        | TABLESPACE |
|        2 | ./mysql/plugin.ibd                    | TABLESPACE |
|       19 | ./mysql/server_cost.ibd               | TABLESPACE |
|        3 | ./mysql/servers.ibd                   | TABLESPACE |
|       16 | ./mysql/slave_master_info.ibd         | TABLESPACE |
|       15 | ./mysql/slave_relay_log_info.ibd      | TABLESPACE |
|       17 | ./mysql/slave_worker_info.ibd         | TABLESPACE |
|        9 | ./mysql/time_zone.ibd                 | TABLESPACE |
|       12 | ./mysql/time_zone_leap_second.ibd     | TABLESPACE |
|        8 | ./mysql/time_zone_name.ibd            | TABLESPACE |
|       10 | ./mysql/time_zone_transition.ibd      | TABLESPACE |
|       11 | ./mysql/time_zone_transition_type.ibd | TABLESPACE |
|       21 | ./sys/sys_config.ibd                  | TABLESPACE |
|       22 | ./ibtmp1                              | TEMPORARY  |
+---------+---------------------------------------+------------+
22 rows in set (0.00 sec)
#查看mysql版本
mysql> select @@version;
+-------------------------+
| @@version               |
+-------------------------+
| 5.7.27-0ubuntu0.16.04.1 |
+-------------------------+
1 row in set (0.00 sec)
#查看用户
mysql> select user();
+-------------------+
| user()            |
+-------------------+
| jambolt@localhost |
+-------------------+
1 row in set (0.00 sec)

mysql> select system_user();
+-------------------+
| system_user()     |
+-------------------+
| jambolt@localhost |
+-------------------+
1 row in set (0.00 sec)
#查看数据库路径
mysql> select @@datadir;
+-----------------+
| @@datadir       |
+-----------------+
| /var/lib/mysql/ |
+-----------------+
1 row in set (0.00 sec)
```

扩展 hashcat 对获取的hash进行暴力破解

```
#查询用户名与hash
mysql> select user,authentication_string from mysql.user;
+------------------+-------------------------------------------+
| user             | authentication_string                     |
+------------------+-------------------------------------------+
| root             | *36E11893339B331EC468212189CFB3ABF80CB458 |
| mysql.session    | *THISISNOTAVALIDPASSWORDTHATCANBEUSEDHERE |
| mysql.sys        | *THISISNOTAVALIDPASSWORDTHATCANBEUSEDHERE |
| debian-sys-maint | *FE191D6E8BF4FB12BCAF4065E182089EA5AF4C0B |
| jambolt          | *084F91FFF15AB4E7A21BA39E44F82BC32DD5757D |
+------------------+-------------------------------------------+
5 rows in set (0.00 sec)
```

切换window10 对jambolt的hash进行爆破

```
λ hashcat64.exe -h | grep MySQL
  11200 | MySQL CRAM (SHA1)                                   | Network Protocols
    200 | MySQL323                                            | Database Server
    300 | MySQL4.1/MySQL5                                     | Database Server
```



```
E:\360Downloads\hashcat-4.1.0\hashcat-4.1.0
λ hashcat64.exe -m 300 084F91FFF15AB4E7A21BA39E44F82BC32DD5757D
hashcat (v4.1.0) starting...

* Device #2: 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: This hardware has outdated CUDA compute capability (2.1).
             For modern OpenCL performance, upgrade to hardware that supports
             CUDA compute capability version 5.0 (Maxwell) or higher.
* 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
nvmlDeviceGetCurrPcieLinkWidth(): Not Supported

nvmlDeviceGetClockInfo(): Not Supported

nvmlDeviceGetFanSpeed(): Not Supported

nvmlDeviceGetClockInfo(): Not Supported

nvmlDeviceGetTemperatureThreshold(): Not Supported

nvmlDeviceGetTemperatureThreshold(): Not Supported

nvmlDeviceGetUtilizationRates(): Not Supported

OpenCL Platform #1: Intel(R) Corporation
========================================
* Device #1: Intel(R) Core(TM) i7-3520M CPU @ 2.90GHz, skipped.
* Device #2: Intel(R) HD Graphics 4000, skipped.

OpenCL Platform #2: NVIDIA Corporation
======================================
* Device #3: NVS 5400M, 512/2048 MB allocatable, 2MCU
```

```
hashcat64.exe -m 300 36E11893339B331EC468212189CFB3ABF80CB458 -a 3 ?l?l?l?l?l?l?l?d?d?d --force
```