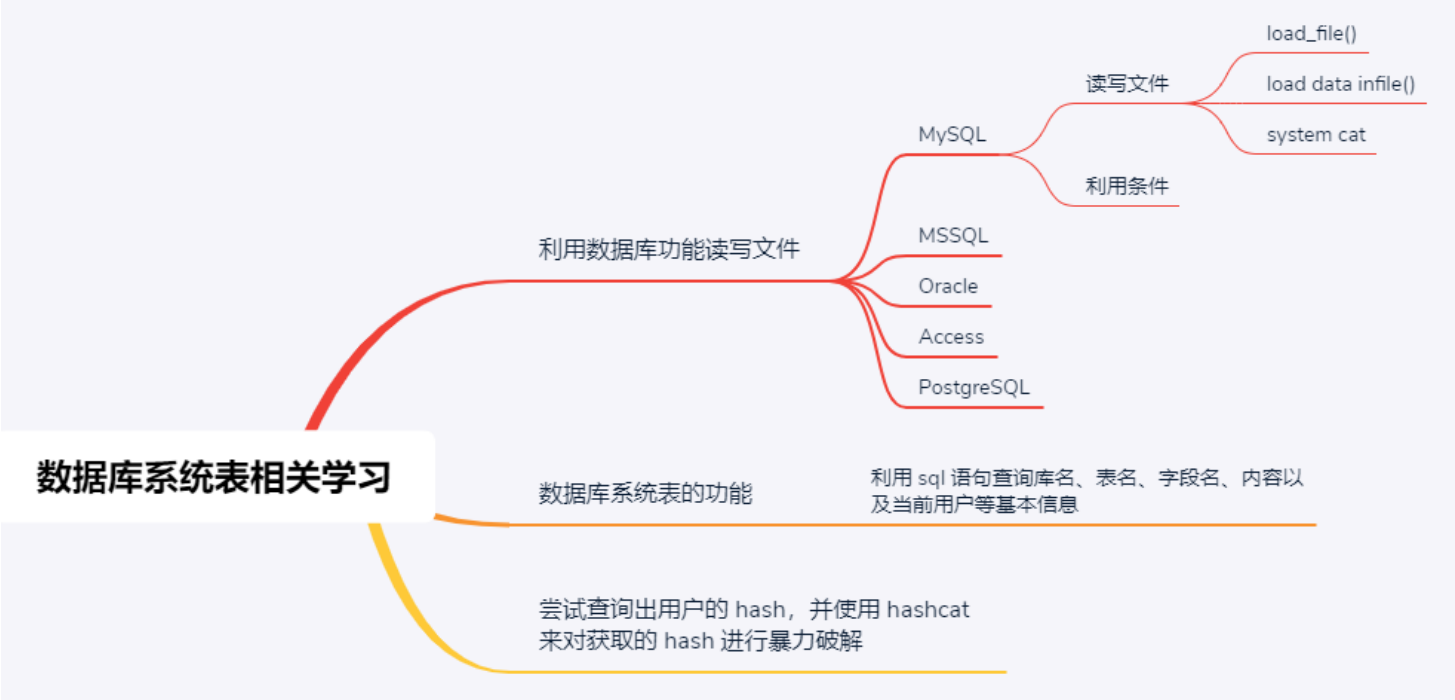
0x01 概况



0x02 利用数据库读写文件

MySQL数据库

- mysql在不同版本读取文件方法大致有这3个:
  1. load_file()
  2. load data infile()
  3. system cat

利用条件

load_file()和**load data infile**读取文件需要下面两个权限

- file 权限
- secure_file_priv
  1. secure_file_priv 为 null 表示不允许导入导出
  2. secure_file_priv 指定文件夹时，表示 mysql 的导入导出只能发生在指定的文件夹
  3. secure_file_priv 没有设置时，则表示没有任何限制

查看 secure_file_priv 的值

```
MariaDB [(none)]> show global variables like "secure_file_priv";
+------------------+-------+
| Variable_name    | Value |
+------------------+-------+
| secure_file_priv |       |
+------------------+-------+
1 row in set (0.001 sec)
```

修改 secure_file_priv 的值

- Windows 如下图，在 my.ini 中修改，添加 secure_file_priv =

```
[mysqld]
port=3306
explicit_defaults_for_timestamp = TRUE
secure_file_priv =
```

读取文件

```
+-----------------------------------------------+
| load_file("C:\\Users\\wenrou\\Desktop\\1.txt") |
+-----------------------------------------------+
| wenrou                                        |
+-----------------------------------------------+
1 row in set (0.00 sec)
```

- Linux
  在 /etc/my.cnf 的 [mysqld] 下面添加 local-infile=0 选项
  我们先来看一下本地 centos 系统的配置文件

```
[mysqld]
port            = 3306
socket          = /tmp/mysql.sock
skip-external-locking
key_buffer_size = 256M
max_allowed_packet = 1M
table_open_cache = 256
sort_buffer_size = 1M
read_buffer_size = 1M
read_rnd_buffer_size = 4M
myisam_sort_buffer_size = 64M
thread_cache_size = 8
query_cache_size= 16M
```

如图，并没有添加 `local-infile=0` 选项

此时我们来读取一下文件

```
MariaDB [(none)]> select load_file("/root/1.txt");
+--------------------------+
| load_file("/root/1.txt") |
+--------------------------+
| NULL                     |
+--------------------------+
1 row in set (0.01 sec)
```

现在我们加入 `local-infile=0` 选项，重启服务，再来读取一下

```
MariaDB [wenrou]> select load_file("/tmp/1.txt");
+-------------------------+
| load_file("/tmp/1.txt") |
+-------------------------+
| wenrou
                |
+-------------------------+
1 row in set (0.00 sec)
```

system cat

在mysql版本为5.x时,除了可以使用上两种方法外，还可以使用系统命令直接读取文件

```
MariaDB [wenrou]> system cat /tmp/1.txt;
wenrou


--------------------------------
```

写入文件

`select * from user into outfile '/tmp.1.txt';`
将表中的数据导出到文件

0x03 数据库系统表的功能

MySQL 内置数据库 information_schema

该数据库保存着关于 MySQL 服务器所维护的所有其他数据库的信息。如数据库名，数据库的表，表栏的数据类型与访问权限等。

MySQL 数据库部分重要数据表说明

- SCHEMATA 表，提供了当前mysql实例中所有数据库的信息，其表中实际存储的就是 show databases结果中各数据库的详细信息

```
use information_schema;

select * from SCHEMATA;
```

	CATALOG_NAME String	SCHEMA_NAME String	DEFAULT_CHARACTER_SET_NAME String	DEFAULT_COLLATION_NAME String	SQL_PATH String
1	def	information_schema	utf8	utf8_general_ci	NULL
2	def	mysql	latin1	latin1_swedish_ci	NULL
3	def	performance_schema	utf8	utf8_general_ci	NULL
4	def	pikachu	latin1	latin1_swedish_ci	NULL
5	def	pkxss	latin1	latin1_swedish_ci	NULL
6	def	test	latin1	latin1_swedish_ci	NULL
7	def	yiqicms	utf8	utf8_general_ci	NULL

- TABLES 表，详细表述了某个表属于哪个schema，表类型，表引擎，创建时间等信息

```
use information_schema;

select * from TABLES;
```

	TABLE_CATALOG String	TABLE_SCHEMA String	TABLE_NAME String	TABLE_TYPE String	ENGINE String	VERSION UInt64	ROW_FORMAT String	TABLI
1	def	information_schema	CHARACTER_SETS	SYSTEM VIEW	MEMORY	10	Fixed	NULL
2	def	information_schema	COLLATIONS	SYSTEM VIEW	MEMORY	10	Fixed	NULL
3	def	information_schema	COLLATION_CHARACTER_SET_APPLICAB...	SYSTEM VIEW	MEMORY	10	Fixed	NULL
4	def	information_schema	COLUMNS	SYSTEM VIEW	MyISAM	10	Dynamic	NULL
5	def	information_schema	COLUMN_PRIVILEGES	SYSTEM VIEW	MEMORY	10	Fixed	NULL
6	def	information_schema	ENGINES	SYSTEM VIEW	MEMORY	10	Fixed	NULL
7	def	information_schema	EVENTS	SYSTEM VIEW	MyISAM	10	Dynamic	NULL
8	def	information_schema	FILES	SYSTEM VIEW	MEMORY	10	Fixed	NULL
9	def	information_schema	GLOBAL_STATUS	SYSTEM VIEW	MEMORY	10	Fixed	NULL

- COLUMNS 表，提供了表中的列信息。详细表述了某张表的所有列以及每个列的信息

```
use information_schema;

select * from COLUMNS;
```

	TABLE_CATALOG String	TABLE_SCHEMA String	TABLE_NAME String	COLUMN_NAME String	ORDINAL_POSITION UInt64	COLUMN_DEFAULT String	IS_NULLABLE St
1	def	information_schema	CHARACTER_SETS	CHARACTER_SET_NAME	1		NO
2	def	information_schema	CHARACTER_SETS	DEFAULT_COLLATE_NAME	2		NO
3	def	information_schema	CHARACTER_SETS	DESCRIPTION	3		NO
4	def	information_schema	CHARACTER_SETS	MAXLEN	4	0	NO
5	def	information_schema	COLLATIONS	COLLATION_NAME	1		NO
6	def	information_schema	COLLATIONS	CHARACTER_SET_NAME	2		NO
7	def	information_schema	COLLATIONS	ID	3	0	NO
8	def	information_schema	COLLATIONS	IS_DEFAULT	4		NO
9	def	information_schema	COLLATIONS	IS_COMPILED	5		NO
10	def	information_schema	COLLATIONS	SORTLEN	6	0	NO
11	def	information_schema	COLLATION_CHAR...	COLLATION_NAME	1		NO
12	def	information_schema	COLLATION_CHAR...	CHARACTER_SET_NAME	2		NO
13	def	information_schema	COLUMNS	TABLE_CATALOG	1		NO
14	def	information_schema	COLUMNS	TABLE_SCHEMA	2		NO
15	def	information_schema	COLUMNS	TABLE_NAME	3		NO

- USER_PRIVILEGES 用户权限表，显示用户的各项权限

```
use information_schema;
select * from USER_PRIVILEGES;
```

	GRANTEE String	TABLE_CATALOG String	PRIVILEGE_TYPE String	IS_GRANTABLE String
1	'root'@'localhost'	def	SELECT	YES
2	'root'@'localhost'	def	INSERT	YES
3	'root'@'localhost'	def	UPDATE	YES
4	'root'@'localhost'	def	DELETE	YES
5	'root'@'localhost'	def	CREATE	YES
6	'root'@'localhost'	def	DROP	YES
7	'root'@'localhost'	def	RELOAD	YES
8	'root'@'localhost'	def	SHUTDOWN	YES
9	'root'@'localhost'	def	PROCESS	YES
10	'root'@'localhost'	def	FILE	YES
11	'root'@'localhost'	def	REFERENCES	YES

MySQL 内置数据库 mysql

- user 表，详细记录用户相关操作权限及登录相关，详细见下文参考文献

```
use mysql;
select * from user;
```

	Host	User	Password	Select_priv	Insert_priv	Update_priv	Delete_priv	Create_priv	Drop_priv
1	localhost	root	*81F5E21E35407D884A6CD4A731AEBF...	Y	Y	Y	Y	Y	Y
2	127.0.0.1	root	*81F5E21E35407D884A6CD4A731AEBF...	Y	Y	Y	Y	Y	Y
3	::1	root		Y	Y	Y	Y	Y	Y
4	localhost			N	N	N	N	N	N

- db 表，记录所创建的数据库相关信息

```
select * from db;
```

	Host	Db	User	Select_priv	Insert_priv	Update_priv	Delete_priv	Create_priv	Drop_priv	Grant_priv	Referenc
1	%	test		Y	Y	Y	Y	Y	Y	N	Y
2	%	test_%		Y	Y	Y	Y	Y	Y	N	Y

参考文献

> MySQL 常用系统表大全
> https://blog.csdn.net/xlxxcc/article/details/51754524
> mysql.user 表字段详解
> https://blog.csdn.net/lthirdonel/article/details/79011033

利用系统表查数据

参考：https://wenku.baidu.com/view/45ef64663b3567ec102d8ae5.html

0x04 暴力破解 hash

hash 识别工具

```
HASH 识别工具
    hash-identifier
    Hashid
    可能识别错误或无法识别
```

hashcat 工具

HASHCAT

开源多线程密码破解工具

支持80多种加密算法破解

基于CPU的计算能力破解

六种模式

-a 指定模式

0 Straight:字典破解

1 Combination:将字典中密码进行组合 （1 2 > 11 22 12 21）

2 Toggle case：尝试字典中所有密码的大小写字母组合

3 Brute force：指定字符集(或全部字符集)所有集合

4 Permutation：字典中密码的全部字符置换组合(12 21)

5 Table-lookup:程序为字典中所有密码自动生成掩码

命令：

hashcat -b

测试当前机器的CPU计算能力

hashcat -m 100 hash.dump pass.lst

hashcat -m 0 hash.txt -a 3 ?l?l?l?l?l?l?l?l?d?d

结果：hashcat.pot

hashcat -m 100 -a 3 hash -i --increment-min 6 --increment-max 8 ?l?l?l?l?l?l?l?l

?l = abcdefghijklmnopqrstuvwxyz

?u = ABCDEFGHIJKLMNOPQRSTUVWXYZ

?d = 0123456789

?s = !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~

?a = ?l?u?d?s

?b = 0x00 - 0xff

获取数据库用户密码 hash 值

```
mysql> select password from user where user='root';
+-------------------------------------------+
| password                                  |
+-------------------------------------------+
| *81F5E21E35407D884A6CD4A731AEBFB6AF209E1B |
| *81F5E21E35407D884A6CD4A731AEBFB6AF209E1B |
|                                           |
+-------------------------------------------+
3 rows in set (0.00 sec)
```

判断 hash 类型

```
root@kali:~# hash-identifier
   ##########################################################################
   #     __  __                     __           ______    _____           #
   #    /\ \/\ \                   /\ \         /\__  _\  /\  _ `\         #
   #    \ \ \_\ \      __      ____ \ \ \___     \/_/\ \/  \ \ \/\ \        #
   #     \ \  _  \   /'__`\   / ,__\ \ \  _ `\      \ \ \   \ \ \ \ \       #
   #      \ \ \ \ \ /\ \_\ \_/\__, `\ \ \ \ \ \      \_\ \__ \ \ \_\ \      #
   #       \ \_\ \_\ \___ \_\/\____/  \ \_\ \_\     /\_____\ \ \____/      #
   #        \/_/\/_/\/__/\/_/\/___/    \/_/\/_/     \/_____/  \/___/  v1.1 #
   #                                                             By Zion3R #
   #                                                    www.Blackploit.com #
   #                                                   Root@Blackploit.com #
   ##########################################################################

   --------------------------------------------------------------------------
 HASH: 81F5E21E35407D884A6CD4A731AEBFB6AF209E1B

Possible Hashs:
[+]  SHA-1
[+]  MySQL5 - SHA-1(SHA-1($pass))
```

hashcat 破解

- 查看 hash 所对应的 hashcat 参数

```
rain-password=bZfhCvGUSjRq
     --brain-session           | Hex  | Overrides automatically calculated brain session     | --b
rain-session=0x2ae611db
     --brain-session-whitelist | Hex  | Allow given sessions only, separated with commas     | --b
rain-session-whitelist=0x2ae611db

- [ Hash modes ] -

      # | Name                                               | Category
  ======+==================================================+======================================
    900 | MD4                                                | Raw Hash
      0 | MD5                                                | Raw Hash
   5100 | Half MD5                                           | Raw Hash
    100 | SHA1                                               | Raw Hash
   1300 | SHA2-224                                           | Raw Hash
   1400 | SHA2-256                                           | Raw Hash
  10800 | SHA2-384                                           | Raw Hash
   1700 | SHA2-512                                           | Raw Hash
  17300 | SHA3-224                                           | Raw Hash
  17400 | SHA3-256                                           | Raw Hash
  17500 | SHA3-384                                           | Raw Hash
  17600 | SHA3-512                                           | Raw Hash
  17700 | Keccak-224                                         | Raw Hash
  17800 | Keccak-256                                         | Raw Hash
  17900 | Keccak-384                                         | Raw Hash
  18000 | Keccak-512                                         | Raw Hash
    600 | BLAKE2b-512                                        | Raw Hash
  10100 | SipHash                                            | Raw Hash
   6000 | RIPEMD-160                                         | Raw Hash
```

- 破解

```
hashcat -m 100 -a 3 hash -i --increment-min 4 --increment-max 4 ?l?l?l?l --force
```

参考文献

密码破解全能工具：Hashcat密码破解攻略

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