查看数据库版本

Select @@version

查看sessionID

Select @@spid

查看用户和其session

Select @@spid as ‘ID’,SYSTEM\_USER as ‘Login Name’,USER as ‘User Name’;

xp\_cmdshell存储过程

Xp\_cmdshell可以让系统管理员以操作系统命令行的方式执行给定的命令字符串，并且以文本的行的方式返回任何的输出，是一个功能非常强大的拓展存储过程。通常情况下，xp\_cmdshell对管理员来说不是必要的。

SQL开启xp\_cmdshell

sp\_configure 'show advanced options',**1**

Reconfigure

go

sp\_configure 'xp\_cmdshell',**1**

Reconfigure

Go

sp\_configure 'show advanced options',0

Reconfigure

命令参数：xp\_cmdshell cmdstring (no\_output)

示例：exec xp\_cmdshell ‘whami’ 返回：服务器用户名