1. Ad Hoc Distributed Queries开启/关闭

EXECUTE sp\_configure 'show advanced options', 1;

RECONFIGURE;

EXECUTE sp\_configure 'Ad Hoc Distributed Queries', 0; #开启即把这个参数改为1

RECONFIGURE;

GO

EXECUTE sp\_configure 'show advanced options', 0;

RECONFIGURE;

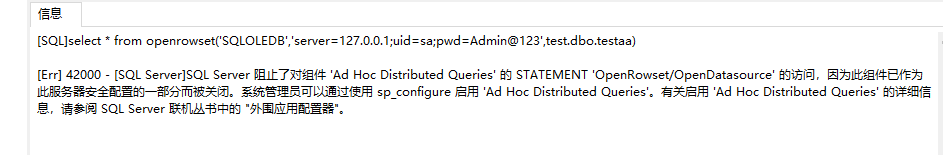
关闭Ad Hoc Distributed Queries会禁用OpenRowset/OpenDatasource远程访问

1. Openrowset/OpenDatasource连接开启Ad Hoc Distributed Queries的数据库

1）select \* from openrowset('SQLOLEDB','server=127.0.0.1;uid=sa;pwd=Admin@123',test.dbo.testaa)

2）select \* from opendatasource('SQLOLEDB','Data Source=127.0.0.1;User ID=sa;Password=Admin@123').test.dbo.testaa

如果开启了Ad Hoc Distributed Queries，则能够访问到指定服务器上的内容，否则会提示目标服务器Ad Hoc Distributed Queries没有开启



我们可以使用Openrowset/OpenDatasource将远程目标库的数据写到本地，也可以将本地的数据写到远程服务器（应用到sql注入）

将本地表写入远程表

1)insert openrowset( 'SQLOLEDB','server=sql服务器名;uid=用户名;pwd=密码 ',数据库名.dbo.表名) select \*from 本地表

2)insert opendatasource( 'SQLOLEDB','Data Source=ip/ServerName;User ID=登陆名;Password=密码').数据库.dbo.表名 select \* from