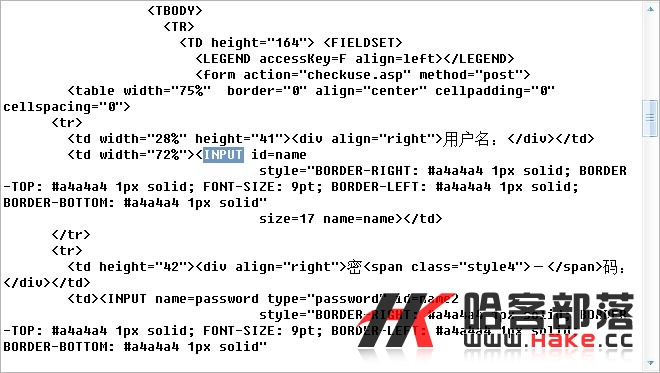
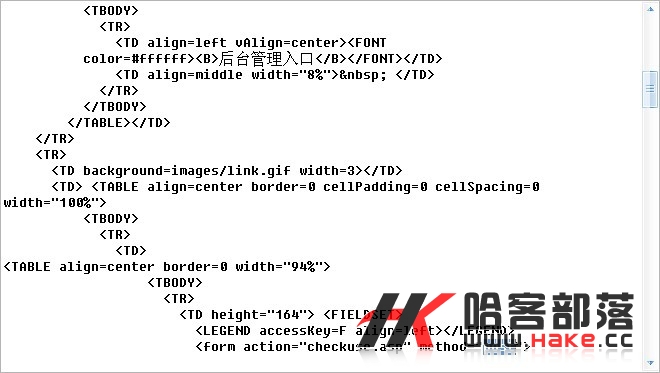
关于此站的信息，就和谐掉了，不影响学习  
前提是要sql server数据库  
首先说下，构造注入点可以任何登录或者搜索栏，并不是只有后台  
测试方式' and user>0;--  
'or'='or'  
' and db\_name()>0;--  
   
接下来，就是看是否存在漏洞了，  
' and user>0;--  
   
这已经可以看出存在注入了  
下面我们构造  
   
如何构造呢  
<http://www.xxx.cn/manage/>   
这是后台  
下面我们要post的数据，所以第一个要找的就是post的地址checkuse.asp  
接下来找登录字段  
name和password如何找，多看文章，这个最简单的基础了，就是input后面跟的name=""就是字段  
<http://www.xxx.cn/manage/checkuse.asp?name=xx&password=xx>  
  
构造完毕后，直接拿nbsi来操作  
如果构造的语句在nbsi里无法检测到类型，可以对语句进行修改  
   
下面就没什么可操作的了，就是db权限备份，拿shell提权，就不多做介绍了，就这么多吧