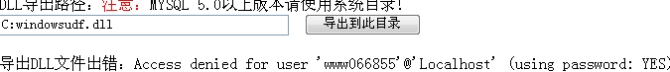
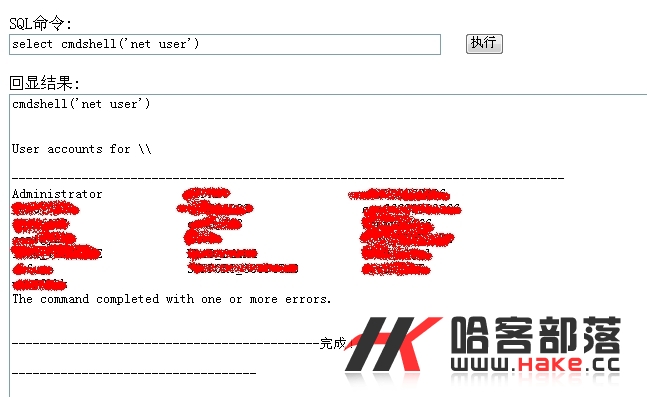
声明：原创文章，转载请注明来自哈客部落([www.hake.cc](http://www.hake.cc/)），违者必究！  
作者：Falling  
前段时间拿下shell  
感觉还不错。。  
后来一直忙于某些事就没去搞了。。  
服务器安装N点虚拟主机。  
破root的方法就是自己在本地搭建IIS进行破解  
代码如图：  
   
找了资料。是某个大牛发布的。呵呵。  
但是家里的电脑卡成一团糟。很麻烦。。就没进行本地破解了。  
在某个论坛让我看见了  
   
不是root帐号。  
还是udf提权吧。  
在UDF过程中。导入不了udf.dll  
   
/或\\都测试了。。  
都没用。。  
思路停止了几分钟。  
后来用select cmsshell('net user');  
终于出来帐号  
   
  
兴奋得连上3889。  
哪知道出现没有缺个远程用户组  
又终止了十几分钟。。  
还是用udf改掉管理员的密码算了。逼着没办法。  
   
写的不好请大牛别见笑