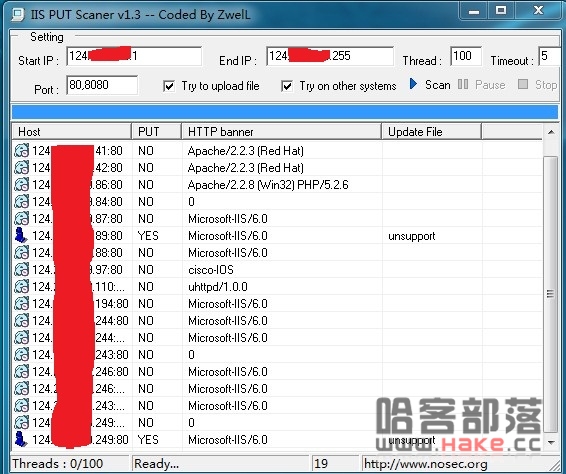
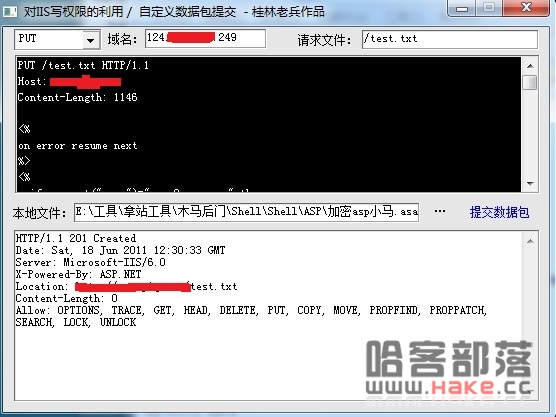
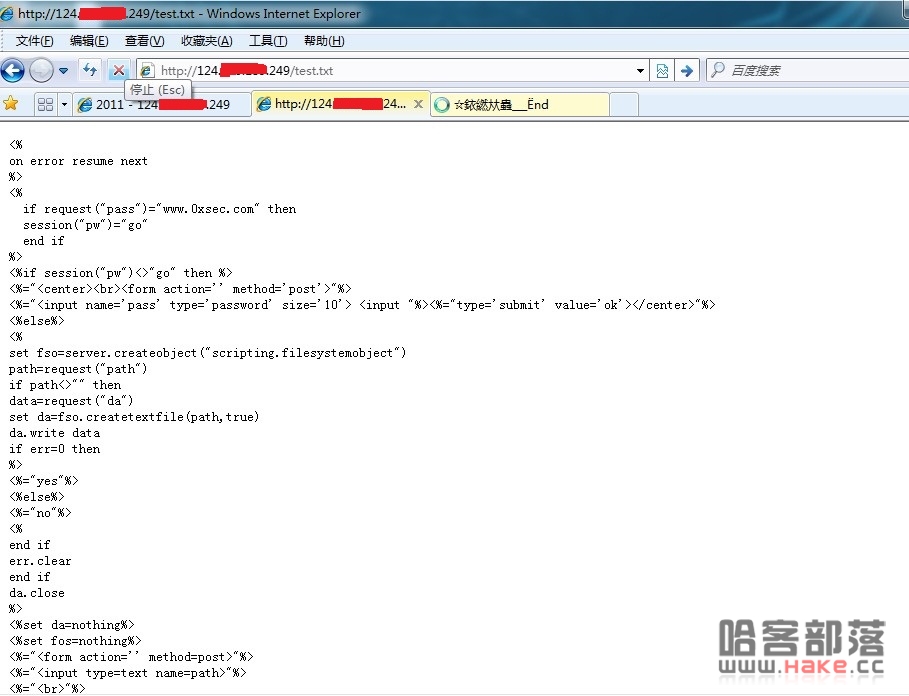
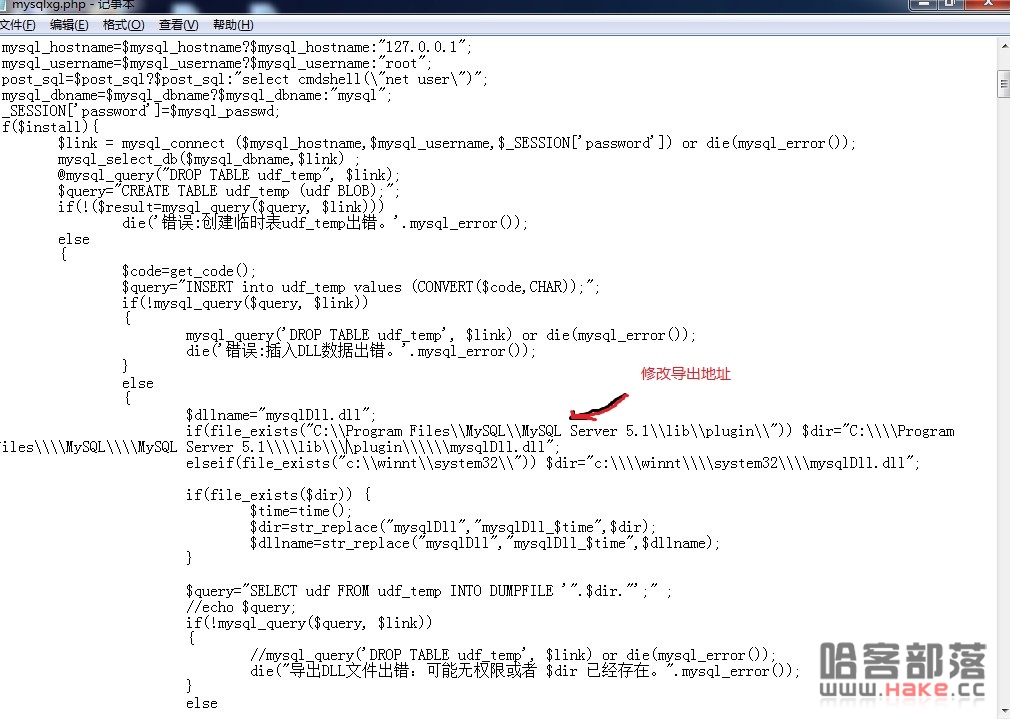
作者：小蛋  
目标[www.xxx.com](http://www.xxx.com/) 主站无明显漏洞，独立服务器无法旁注，C段试试，拿起IISputscaner扫描发现，两个iis6为PUT  
   
虽然unsupport,也有成功几率，用老兵的IISREAD，对124.x.x.249 put一个文件，如图  
   
成功PUT，打开连接  
   
然后就是move成ASP,但是无法成功,copy也失败，我们可以move为一个1.asp;1.jpg的文件，貌似还要NC发个包，这里有个简单方法，直接用IE以文件夹方式打开，如图  
   
直接，拖进去1.asp;1.jpg就可以了（注：这里就算你拖asp结尾的文件也不可以）  
   
然后就是提权了，大概看了下主机，有可写目录，支持aspx，systeminfo下主机信息，，300多个补丁，各种溢出，各种提，无果，翻了N久目录，找到root，苍天有眼，这里发现mysql为5.1，残剑有篇文章，记得讲过查看方法，就是利用PHP马，连接数据库查看版本信息，这里就不介绍了，上传udf.php前，本地修改下导出目录，如图   
   
OK，添加用户，登陆服务器  
   
接下来就是嗅探，很庆幸在一个网段，很郁闷，目标主机很少更新，嗅探不到有价值信息。  
  
大牛勿喷,不足之处还多多包涵