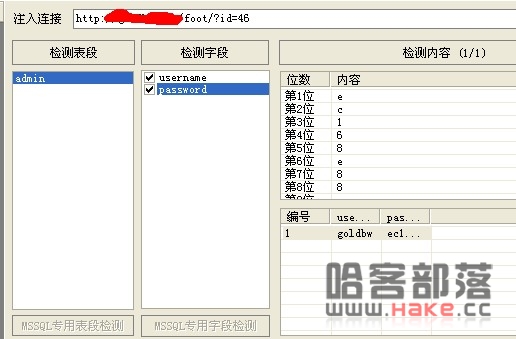
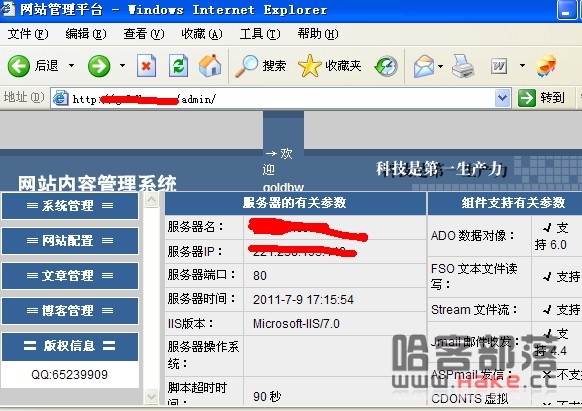
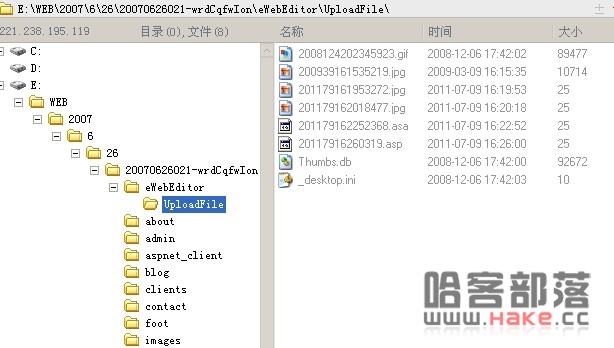
几天闲的没事干  在网上瞎逛游发现了个学院商城    反正没事干渗透个玩玩    
   
在网页上翻腾了半天   发现这个是叫shopxp网上购物系统的程序  现在好办了  网上找0day呗    网上看到一篇<http://www.tmdsb.com/2011/07/shopxp-into-the-online-shopping-system-v7-4-latest-0day/> shopxp网上购物系统v7.4最新注入0day  
成功利用0day拿下  后台密码账号  
   
然后一进后台   全部都是  你的权限不够   
   
  看到备份了都不能用   
哎~~~~  看看能不能旁注吧  放到   
御剑1.3.1 一统的扫   
   
然后是批量注入点  扫着吧  我睡午觉去了     
一个小时以后·~~~~    
打开电脑  一看扫完了  还不少   选最后一个吧  （个人习惯）  
      
上啊D检测 吧  拿下   
   
后台账号密码    后台标准路径  省事了  
还是iis7.0的  
   
在添加文章那里看到很熟悉的编织器   看代码  找ewebeditor的路径  
7.jpg   
看到这原来在根目录啊    
上eWebEditor/admin\_login.asp熟悉的界面出来了   
   
随后admin admin   RP不错进去了    
剩下的就是添加asa  结果在这里出问题了 请求筛选模块被配置为拒绝该文件扩展名。  
     
愁了  看来只能想方法  传asp的格式了  想了想貌似在那篇文章里看到过用asaspp   
   
就可以上传asp格式的了  成功菜刀  
     
然后上传大马  不知道为什么  老是被杀   一想  直接  上传aspx的大马  试试  用哈客的  aspx大马成功上传   但是不能执行exe的文件   现在  还没提到权  有大牛想试试的话  在群里发QQ乎我 我吧马发过去