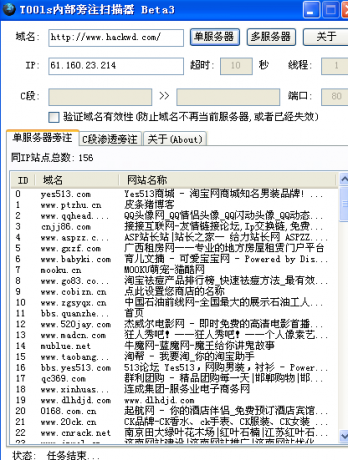
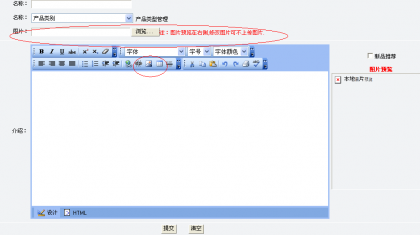
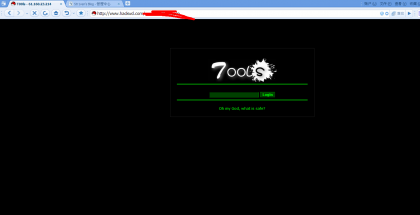
今天放假，上网时间挺长的，于是和朋友一起搞站，朋友找了个站，叫黑旗基地，这类黑客站点一般主站都很安全，于是乎打算旁注，扫了一下同ip站点。 156个，蛮多的（对于俺这种小菜喜欢旁站多的，入手地方也就多了嘛）。  
[](http://www.hackver.com/content/uploadfile/201105/dc0087269034d5b22e7006d05260278e20110501070718.png)   
  
开始找了几个公司的网站（一般公司的站点安全性都比较差），没过多长时间通过注入拿到了一个后台，发现上传的地方被人删掉了，看来是有朋友来过呀，郁闷的很，无奈只好再去找，找了几个站，注入，弱口令等方法均无果，这时候朋友发来了一个aspx的旁站，弱口令轻松进去了，进入后台发现系统比较简洁，仅有个添加产品，点了进去发现有2处上传的地方。  
[](http://www.hackver.com/content/uploadfile/201105/dc0087269034d5b22e7006d05260278e20110501070605.png)   
点了下图片的图标，跳出上传的对话框，直接先上传一个asp文件尝试，失败，对文件进行了限制。在尝试一下其他后缀，均无果，服务器用有iis6.0，这时候想到了iis6.0的解析漏洞，看看能否成功，把文件名改成.asp;.jpg这类的形式可以以脚本的形式运行，直接将小马改成xm.asp;.jpg进行上传，谁知道图片显示上传成功却在任务栏上没有显示，奇怪了，难道是没有图像就不在任务栏显示？ 这我怎么看路径访问呀，于是在电脑cmd下输入copy /b 1.jpg 2.txt 3.asp，成功合成了一个图片一句话木马（有些人可能我问为啥不生成大马，因为太大了。。。），之后上传，成功，任务栏上出现了图片。  
[](http://www.hackver.com/content/uploadfile/201105/dc0087269034d5b22e7006d05260278e20110501065825.png)   
之后查看属性，成功，获得一句话木马地址，菜刀连接之，之后就是提权了，上传一个asp大马继续看。  
首先看了下网站目录d:\host\wwroot，貌似是星外分支，组建不支持ws，脚本探测一下，支持aspx，这就好办了，找到可读可写目录C:\Documents and Settings\All Users\Application Data\Microsoft\Media Index\（想必这个目录大家都知道），可以执行命令。  
既然这个目录可读可写，那胜利的曙光就不远了。  
上传读iis帐号密码的脚本，执行命令/c “C:\Documents and Settings\All Users\Application Data\Microsoft\Media Index\cscript.exe” d:\freehost\xxxxx\iis.vbs成功获取用户名密码。  
[](http://www.hackver.com/content/uploadfile/201105/dc0087269034d5b22e7006d05260278e20110504235250.png)   
服务器我就不登陆了，直接ftp上传一个shell，收工！  
[](http://www.hackver.com/content/uploadfile/201105/dc0087269034d5b22e7006d05260278e20110501071235.png)   
  
之后发现黑旗原来也有朋友来过，还留了一句话。。。。。  
  
文章没什么技术含量，博各位看官一笑。  
  
  
写两篇技术文章