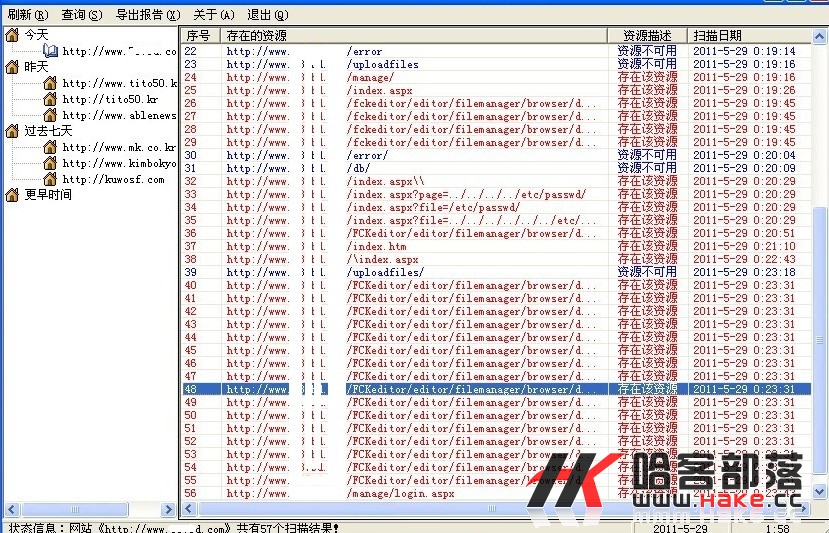
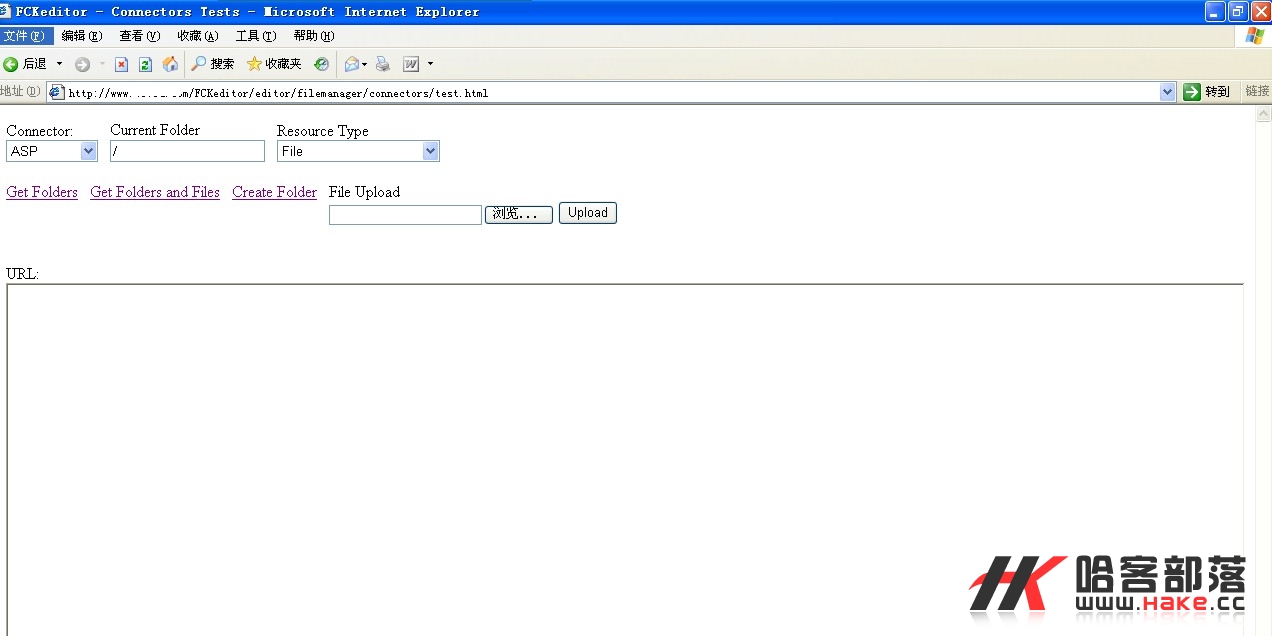
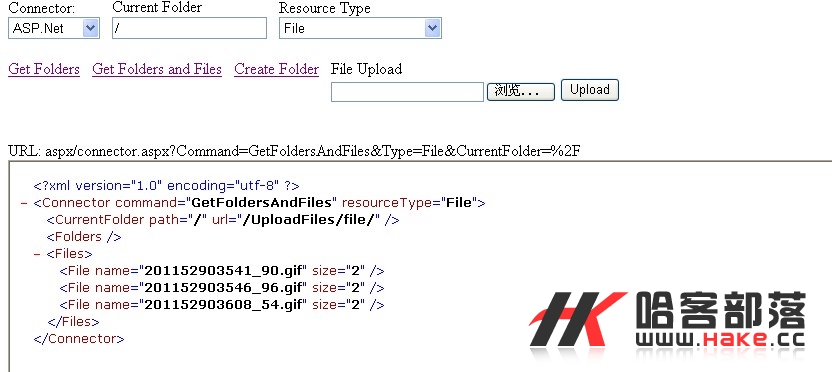
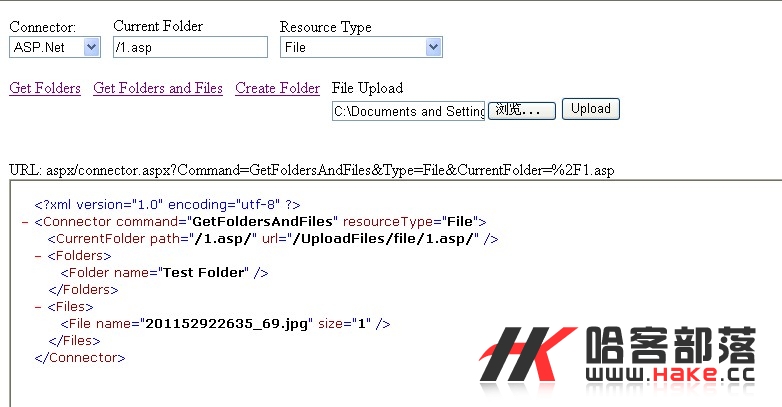
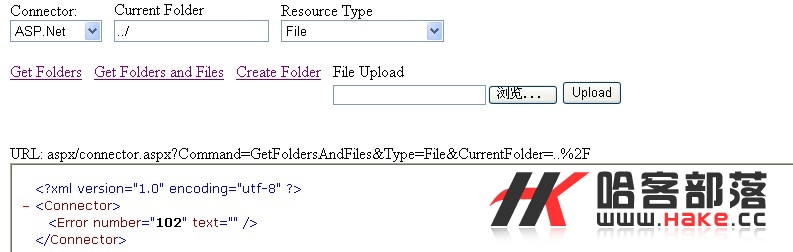
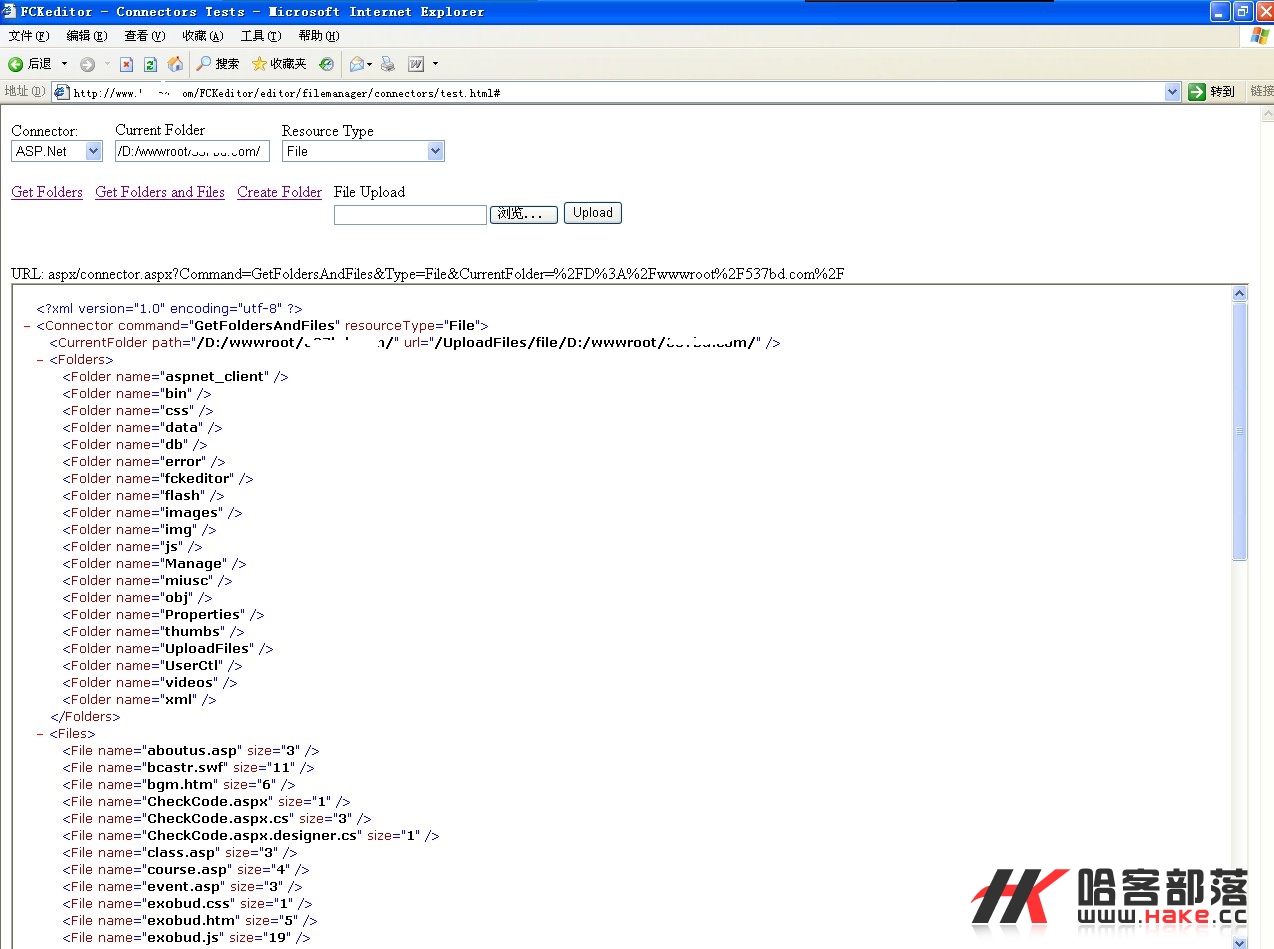
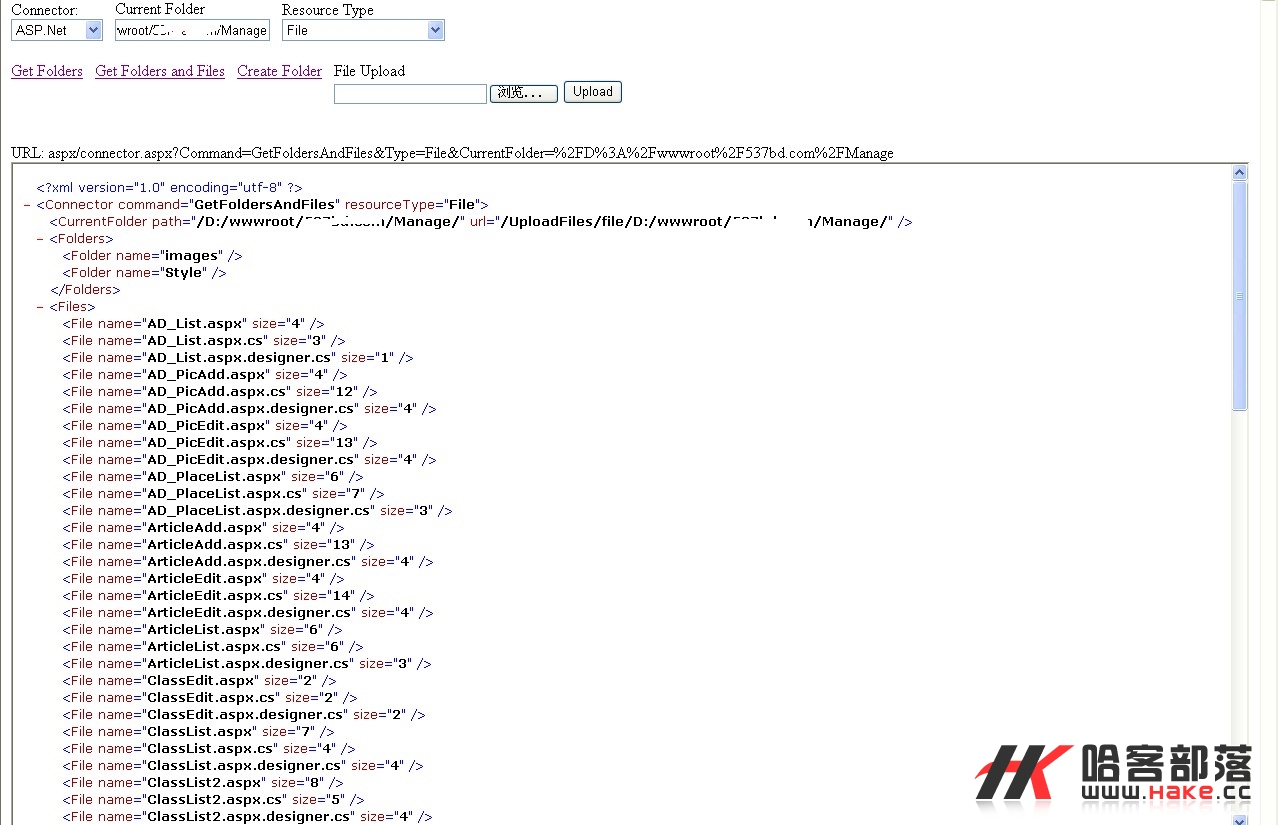
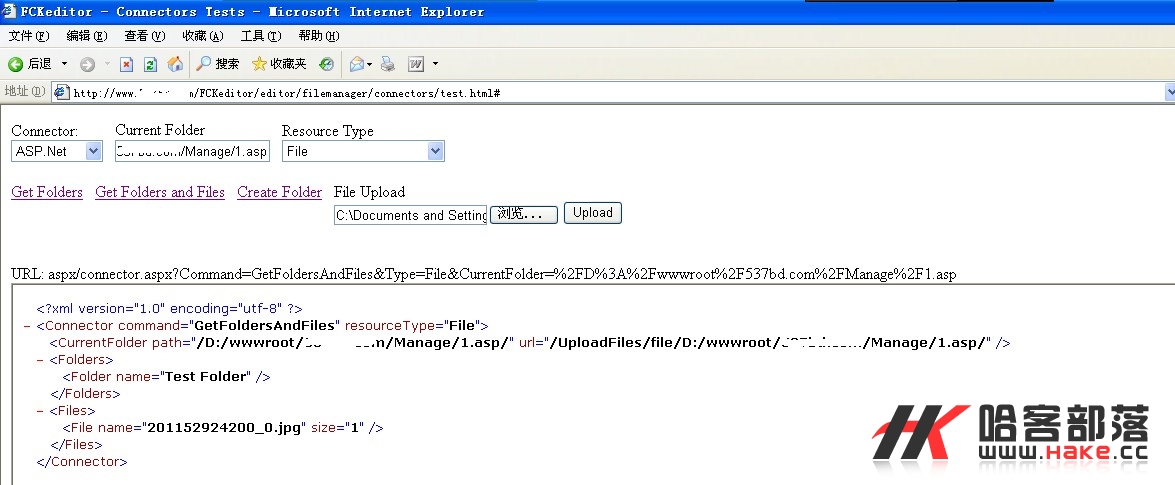
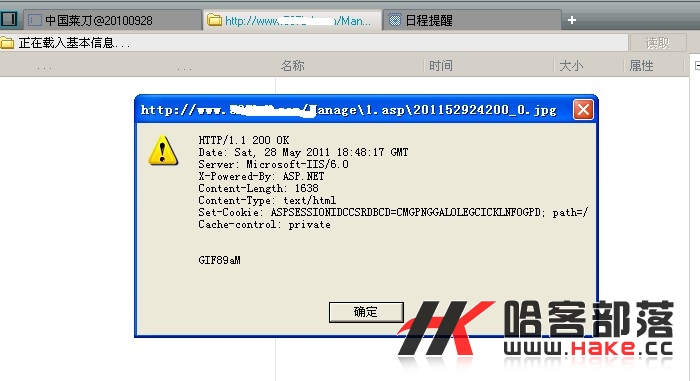
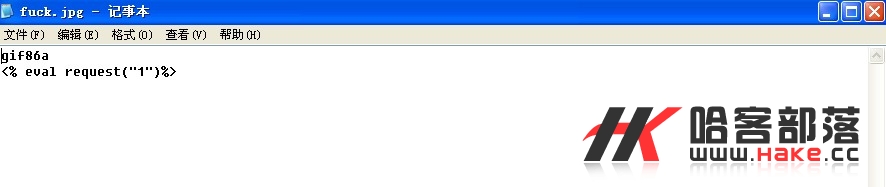
本帖最后由 无名小卒 于 2011-5-29 04:45 编辑  
  
**图/文**  
**作者：残剑   ,   无名小卒**

**From：哈客部落核心组原创详细的图文结合文章（转载请注重版权：From:哈客部落）**

各位黑阔你们好，今天我和残剑在工作室做事的时候，有个兄弟发个街舞的站来叫我们帮他看看！  
诶，由于关系不错所以事忙完了就帮忙啦！~~  诶 。。。   
呵呵，其实我们写出来是因为咱两兄弟研究出了一个比较新的FCK上传小技巧！！贴出来让大家学习学习。    
初步探测主站是用ASPX程序搭建的,  
随后手工测试了一下主站的安全,没啥常见的漏洞。  
接着就用神器多线程去扫描网站的敏感目录了.  
   
  
发现了可爱的fck编辑器。  
接着就测试了fck的常用目录,终于是找到了一个fck的test上传页面  
  
   
  
这种一看就是使用高版本的fck,所以一开始就打算使用fck二次上次漏洞把网站搞定的。  
但是,悲剧发生了  
  
   
  
上传后网站自动重命名进行了处理。  
没事。我们还有方法,  
那就是传说中的新建.asp文件夹。利用iis解析漏洞把网站拿下  
  
   
  
但是悲剧再一次发生了。访问一句话页面的时候,页面提示没有权限运行。看来管理员在iis上对目录做了设置,不允许任何脚本运行。看来管理对网站还是挺有心的嘛。  
但是不能就这样放弃了。我就在想能不能换个目录进行上传呢??  
想着想着就做了.  
于是在Current Folder里填写../进行跳跃目录尝试。后来发现想法过于天真了  
  
   
  
没办法.还是从主站下手吧。在主站逛荡逛荡,随手在网站的动态连接文件showzew.aspx?id=1前加了一个~。  
爆出了网站的目录。这时候心生出了一个淫荡的想法,在Current Folder填入网站的目录会咋样呢??  
于是,想着想着就做了.  
  
   
  
居然爆出了网站的所有文件。这可真是天大的惊喜啊!!意外,绝对是意外...  
  
   
  
接着进入网站管理目录新建一个.asp的文件夹上传我们的小马。  
  
   
  
正高兴的用菜刀连接的时候,悲剧再一次出现了。  
  
   
  
菜刀提示连接错误。看了一下错误gif89am。想了想应该是程序验证文件头.  
.于是更改一句话小马的文件头,提交上传。  
  
   
最后成功拿到shell  
   
  
好啦！  文章到此结束啦！~~