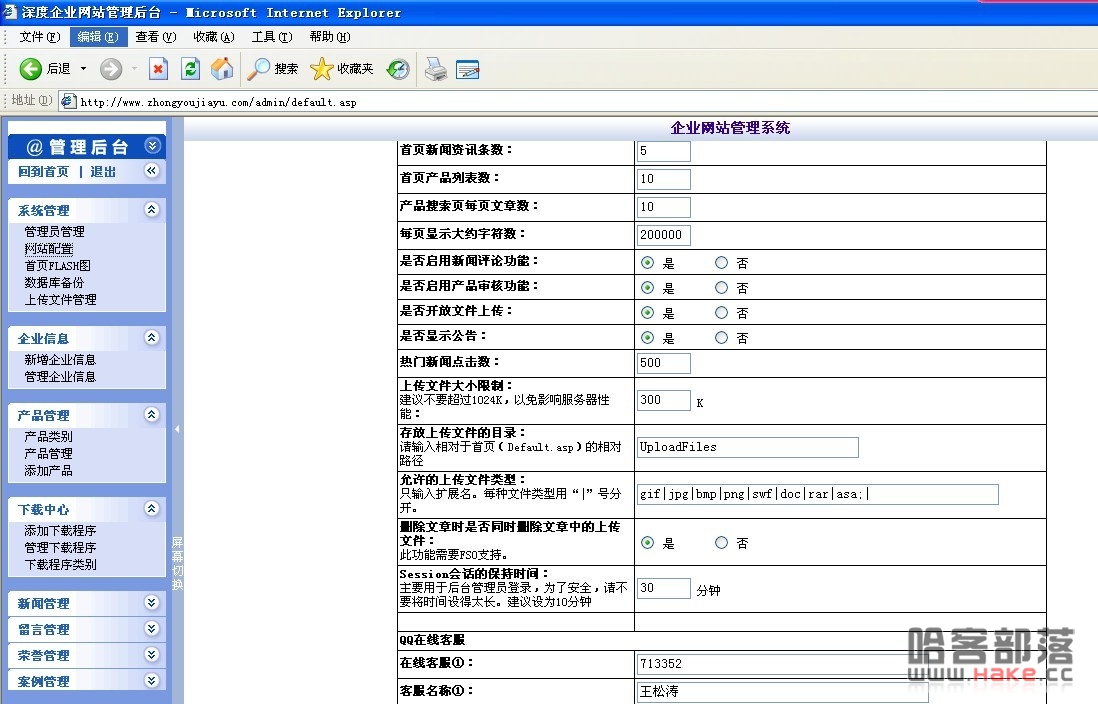
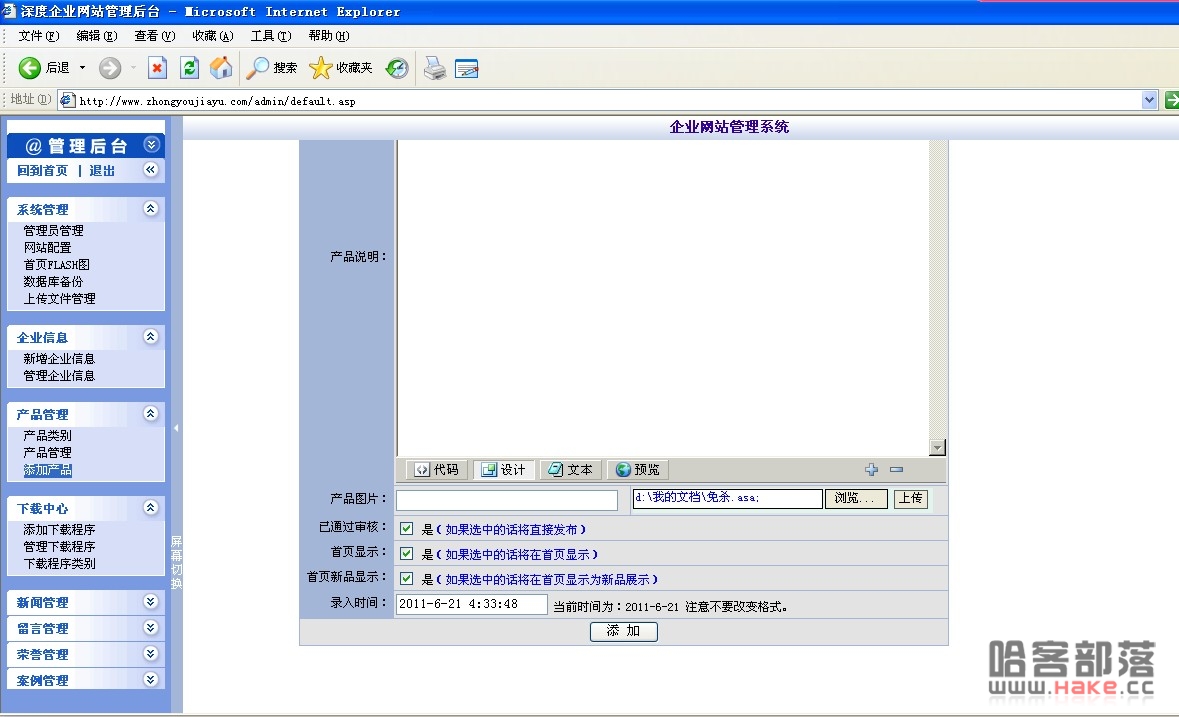
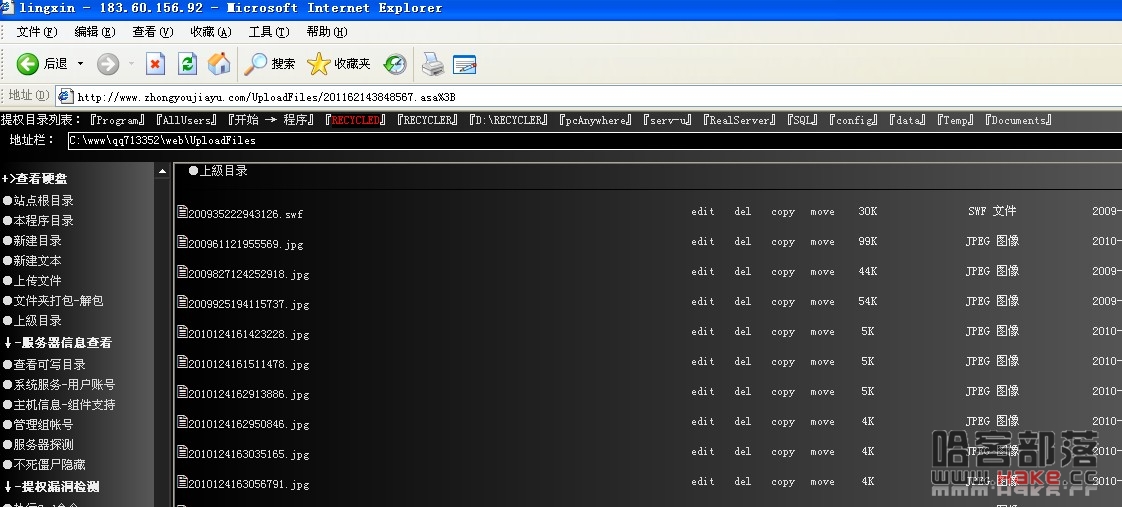
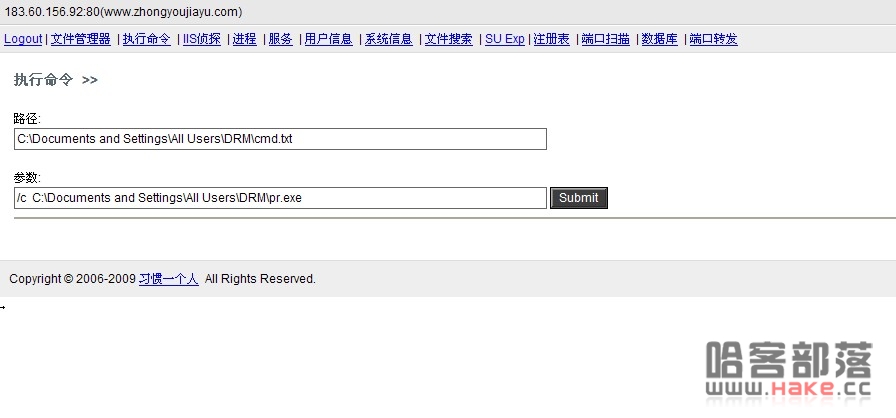
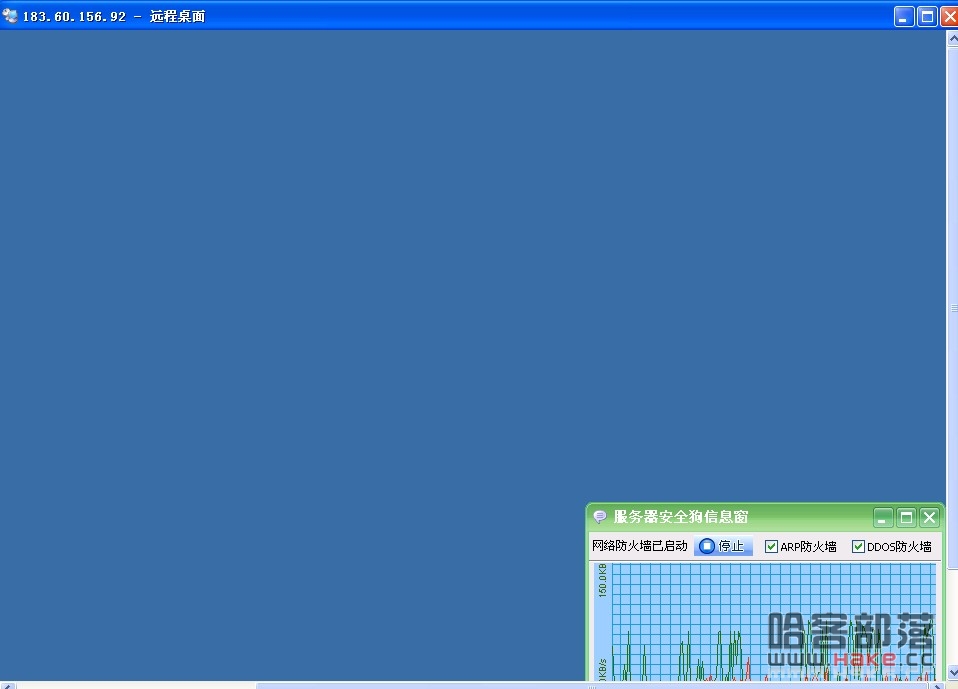
 今天下午群里发了一个网站后台，发现是良精的程序，直接中转注入，顺利拿到后台账号密码(刚拿到群里也有人把后台账号密码发出来了).  
   登入后台，网站配置，**允许的上传文件类型：添加asa;格式，**  
  
   
  
然后找一个上传图片的地方，这里我就直接[添加产品](http://www.zhongyoujiayu.com/admin/ProductAdd.asp)，来到一个可以上传图片的界面，上传asa格式木马，  
  
  
  
   
  
  
  
上传后，顺利拿到shell  
   
  
  
  
命令行组建都没删，且支持.net脚本，看来提权希望瞒大的，  
  
这里我就直接上传.net脚本，执行set命令，返回拒绝访问，估计系统路径cmd做了限制，  
  
找了个可写的目录，C:\Documents and Settings\All Users\DRM\，上传cmd.txt，  
  
成功执行命令，systeminfo 发现系统只打了一个补丁，上传PR，执行没反应  
  
   
PR放自定义路径看看，  
   
可以执行命令，但是 命令参数好像没执行，  
  
换其他提权工具也一样，都是参数不执行  
  
换个免参数的PR试试,顺利添加用户 ，成功连接到服务器  
  
   
  
至此，提权结束。  
  
  小菜第一次写文章，做得不好的地方，请大家指出