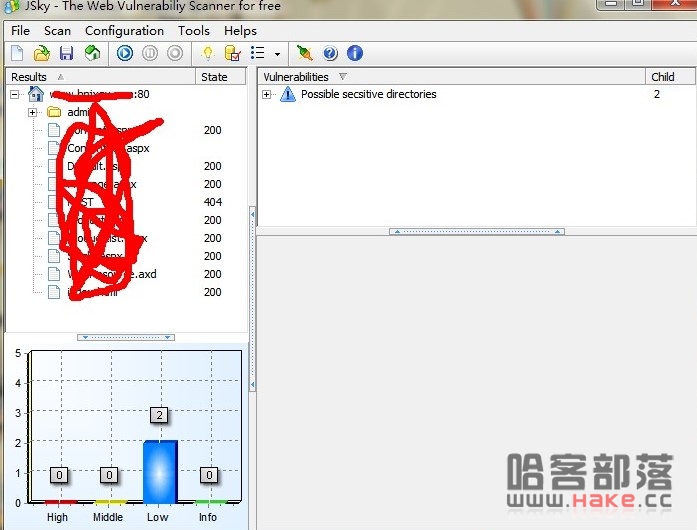
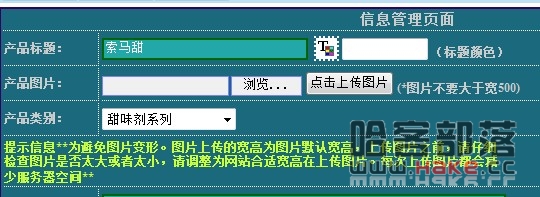
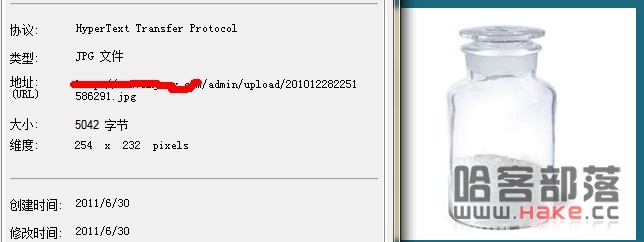
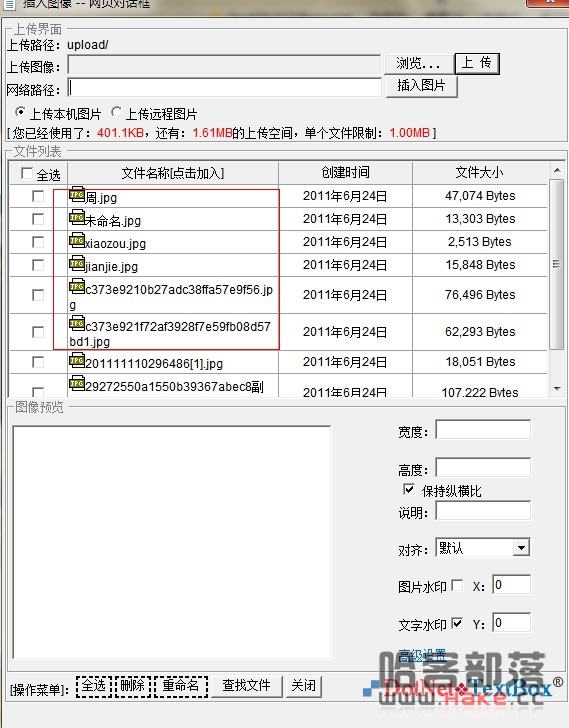
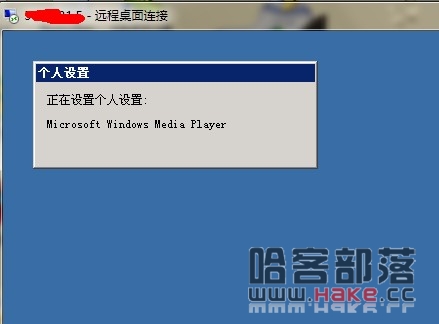
作者：blue 【NST90】（以后署名都用这个）  
  
  
昨晚心情不是很好，于是就放下复习资料，上网随便浏览网页。  
无意中看到一个食品添加剂的企业网站，看到想起之前发生的食品安全问题，加上心情本来就不怎么好，于是我就来火了  
想搞了它，挂个TXT上去泄泄愤。  
说干就干，首先用JSKY一顿狂扫，说真的，JSKY这个软件很不错的，能扫出一些漏洞，并能扫出网站的目录（并不是扫出所有的目录，是看字典的），我最喜欢用它扫网站的后台的，几乎弹无虚发啊。扯远了，继续，看JSKY扫完的截图。  
   
神马能用的漏洞都木有。开骂了一句，关了，再进首页看看  
在网站上磨蹭了好久，都木有发现可用的信息，也不知道网站是神马整站程序来的。  
认真想想，刚刚JSKY不是扫出网站的后台了吗，进去看看，或者能发现是神马整站程序都不一定的哦。  
敲入admin  
   
眼前的一幕让我大吃了一惊。  
直接进了后台？？  
当时有点不相信自己的眼睛，这情况，我还木有遇到过啊，真是千年难得一遇的后台啊！！  
当时我就不是特别的激动，因为，可能是蜜罐。  
不管它蜜不蜜罐的，先看看再说。  
找到了一个上传图片的地方，先试试上传，看看这个后台是不是真的蜜罐，试着直接上传个ASP的吧，限制了。  
   
   
应该就不是蜜罐了吧。  
然后点开旁边那个产品的图片属性看看文件名有木有重命名，如果木有就能用解析漏洞了。  
   
结果真的重命名了。杯具  
然后再发现下面有个编辑器，还有个上传图片的地方，点开看看  
   
很惊奇的发现，里面的文件都木有重命名啊，于是就屁颠屁颠的上传asp;.jpg的文件。  
   
结果看到这个，我那个崩溃啊！！！！  
你说你是不是坑爹的啊，那个编辑器里提示明明还有1兆多的容量，你说内存不足，啥意思啊！！！  
算了，接受事实吧，再去其他地方看看有木有可利用的。  
全部东西都点完了，木有发现可利用的东西。  
迷惑中突然灵光一闪，刚刚下面那个上传的地方的路径好像是跟那个重命名了的产品图片一样的。  
于是就去确定一下，好像真的是相同的。于是就跑去上面那里上传asp;.jpg的图片，然后再到下面的编辑器那里打开看看。  
哇，果真有啊！！  
   
  
于是就用了上面那个重命名的路径去访问  <http://xxxxxx/admin/upload/xxxx;.asp.jpg>  
结果木有显示那个熟悉的界面啊！！！  
然后试着把admin出掉试试，还是木有啊！！！  
冷静下来想想，那个编辑器就是插入图片的，插进文章那里，再看源码，肯定能找到真正的路径了吧！  
于是还真的发现了。  
   
明显和之前那个重命名的产品图片的路径不一样啊，那为什么又能在哪里上传，在编辑器这里找到呢？？迷惑中，哎，不管了，是我RP大爆发吧，哈哈  
复制链接，打开。出现了那熟悉的界面，哇哈哈。  
然后先挂个TXT泄愤先  
   
然后就是提权，提权没啥亮点，本来这个网站就是.net 的，于是就上传了个ASPX马，找到一个常用的目录，用一个面参数的PR提权成功。  
   
没啥技术含量，大牛勿喷