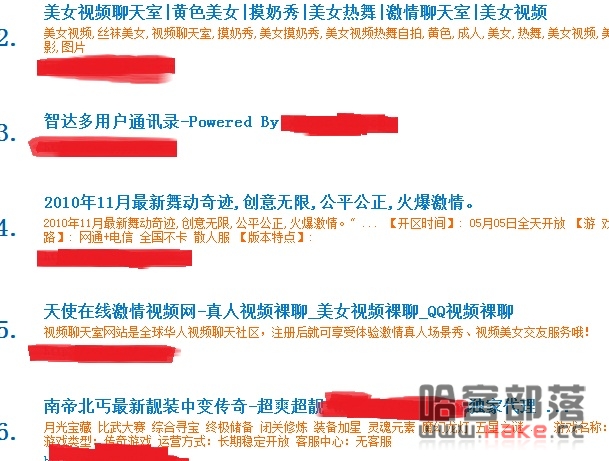
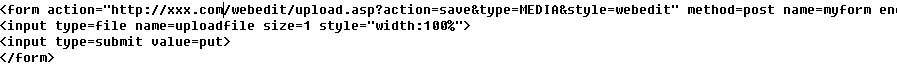
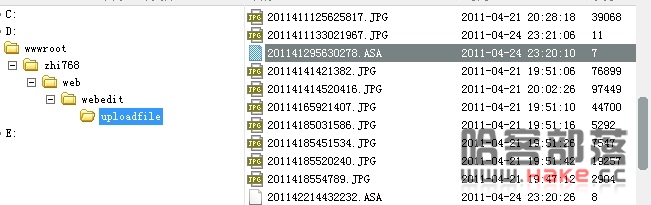
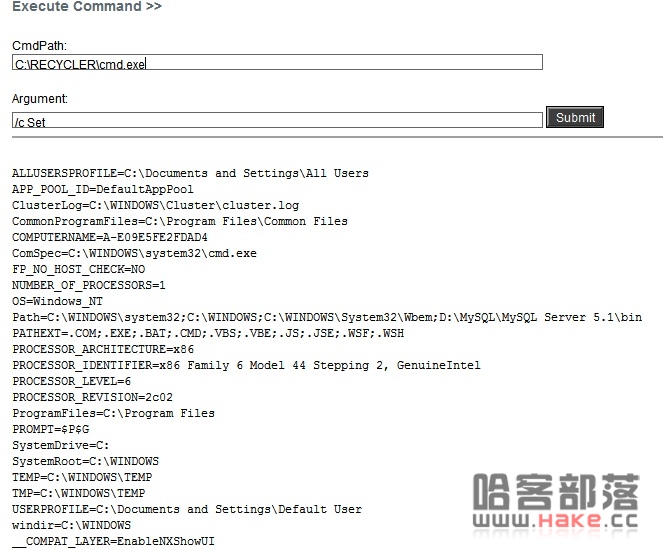
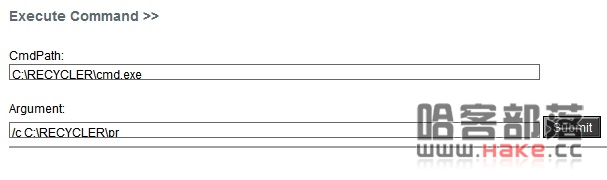
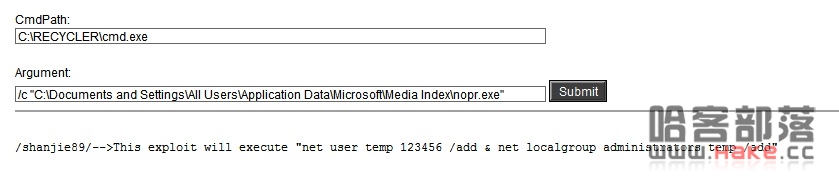
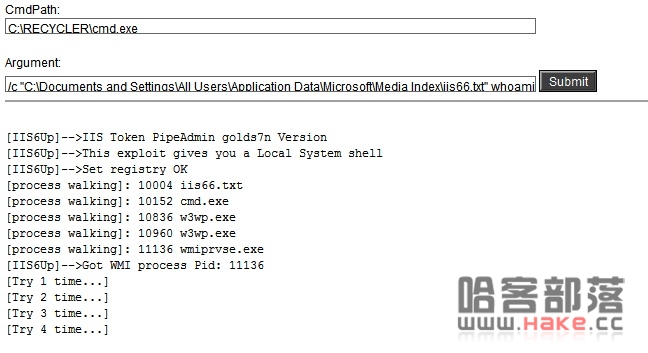
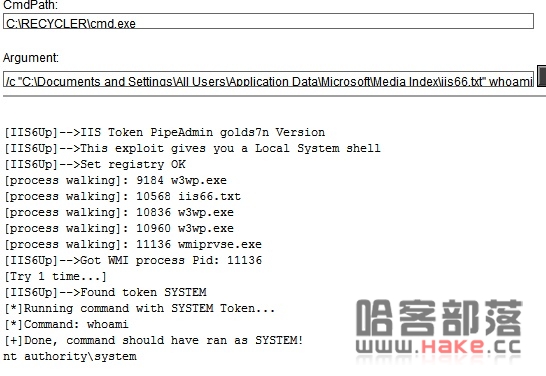
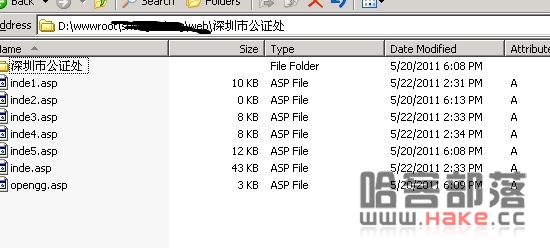
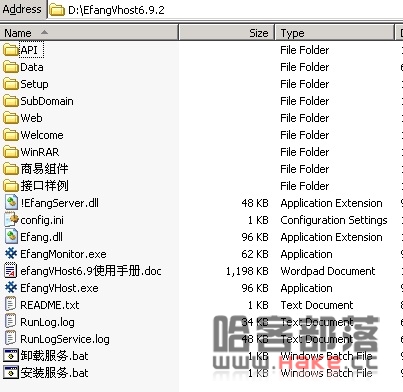
无意中发现一词霸的钓鱼站点，决定渗透一翻。  
  
首页做的挺炫的，估计能迷惑到不少人，这种站按经验来看，无非就是  
  
几个HTML页面，外加一个MDB数据库存受害人的信息。因此自然想到旁注。  
  
  
上面的站不多但是每一个好鸟，都是些非法站点。  
  
  
  
接下来就是寻找目标的过程了，由于站不多，而且都是钓鱼性质的，好不容易发现了一个站  
  
的开源源码，顺利下载了数据库，结果解不出MD5，难道以前被人黑过，尝试了下cookie欺骗，  
  
还是没能进后台，后来发现一个后台可以直接万能密码进入，有一老版本的eweb，无后台，  
  
不过该版本可以在本地构造asa上传  
  
  
  
  
方法就是把上传页面源码保存到本地为html文件，然后按如下修改即可。  
  
上传过程中发现居然还会对文件头进行检测，用图片合并了一个一句话进去，成功上传，  
  
然后菜刀连接之。。。  
  
  
目标站支持ASPX，直接上ASPX马儿，首先看了下回收站，居然可以写入，测试了下  
居然还能执行，很久没遇到此等好事了！！  
  
  
传了个IIS脚本把密码跑出来，发现根本没用，压根能知道目标站的路径而已。  
  
因为这些用户名都是随机数字，密码也是随机，没星外那等好事，这密码也跟FTP关联不起来，  
  
因为服务器用的serv-u，先不管用的什么虚拟主机软件吧，老规矩，用RP试试PR^\_^  
  
  
结果传到回收站目录的都执行不起来，按理说应该是有执行权限才对啊。  
  
看来这个问题只能进服务器才能搞清楚了，估计还是权限问题  
  
  
用星外的思路，随手找了几个目录，zend,php，结果发现经典的media index目录  
  
可以写入，而且可以执行，我比较懒，一般直接用无参数版，这样懒得纠结路径缩写之类的  
  
问题，回显结果告诉我没有成功....  
  
  
别泄气，试试t00ls版的，看到这个结果，估计很多人跟我一样  
  
以为失败  
  
  
再执行一次，所以说多收集几个版本看来还是派的上用场的。  
  
然后就是dump出hash，直接管理登陆.....  
  
  
找到目标站  
  
  
原来是一个叫易方的虚拟主机软件，以前也没接触过，google一下，  
  
貌似也没人研究过  
  
后来发现这套软件什么都是加密的，后台管理密码居然是35位：  
g460AE3C5FB9641765CB2E68B06E4FA2845  
不解中，另外serv-u，mysql密码均无法破解出来，啥也没收获啊。  
不过发现用户的密码都是以明文存的。  
总体看来还是比较顺利的....留下的就是研究这套软件了....  
  
寻思着，要是没有PR提权，估计我后来也就歇菜了...所以对此虚拟主机软件的研究  
  
还在继续中，希望有经验的朋友分享一下，有兴趣的朋友也可以下载研究：  
  
http://www.efang.com.cn/download.asp  
  
