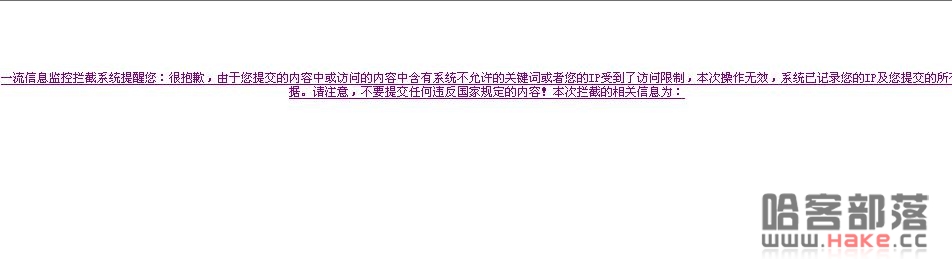
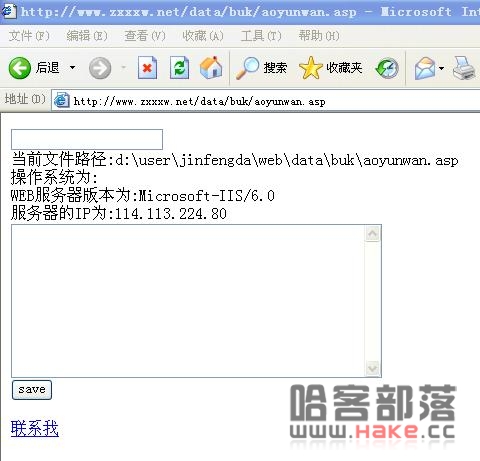
哇咔咔  这可是我的处女做！希望通过审核、我希望和大家交流和学习呢！  
  
话说某日虐天兄扔一个网站过来说要我和谐下、我打开一看、晕 信息网站 、不是CMS   
  
随便看了一下、这个网站貌似有监控拦截系统  
  
这种监控拦截系统最恶劣了、啥都拦截、什么一句话木马 大马小马通吃 BT的很  
  
无奈用google看看吧？应该是个注入  
  
  
屁颠屁颠的打开了 试一下能注入不？悲剧！拦截了  
  
依然google 找找后台吧  
  
  
intext:管理员 intext:密码 等等也是一样、有的是出来一堆没有是的  
纠结了、既然google不行了、那就用工具扫一下目录吧。  
jsky太慢了、我这256内存也用不起啊、就用wwwscan吧  
还真扫出来东西了  
  
  
  
/admin1/admin\_login.asp就是后台了、  
还有备份的数据库 data/buk/cnmai.mdb  
哈哈。直接拿下管理员密码、 可是是md5加密的、cmd5收费？哎。别的又解不出来只好去饭客求助（朋友都说哈客的md5解密很强大！可是我没号！呜呜呜）  
最后进入后台。后台更变态、一律是各种过滤- -也没上传的地方  
有人可能会说一句话木马。拦截呀拦截！  
  
在各个地方试了一句话木马 最后在公告插入一句话 然后备份数据库拿下了shell  
  
  
  
我md5还花了2饭票呢、希望管理通过，以后渗透也方便多了！嘿嘿