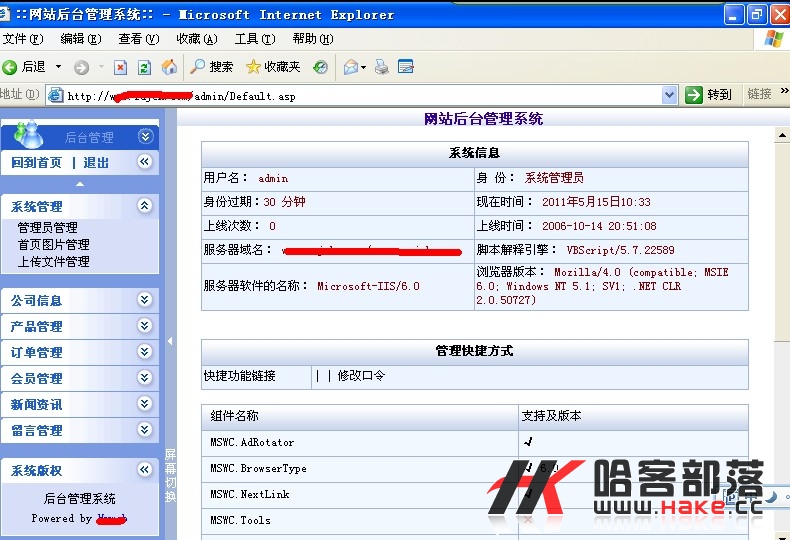
**文/图 残剑**

今天帮一朋友看一个后台。叫我帮忙拿shell,,

这不是刚起床嘛。那就活动活动筋骨把~~~



这后台乍一看像是良精的程序。Admin admin 弱口令进入之。



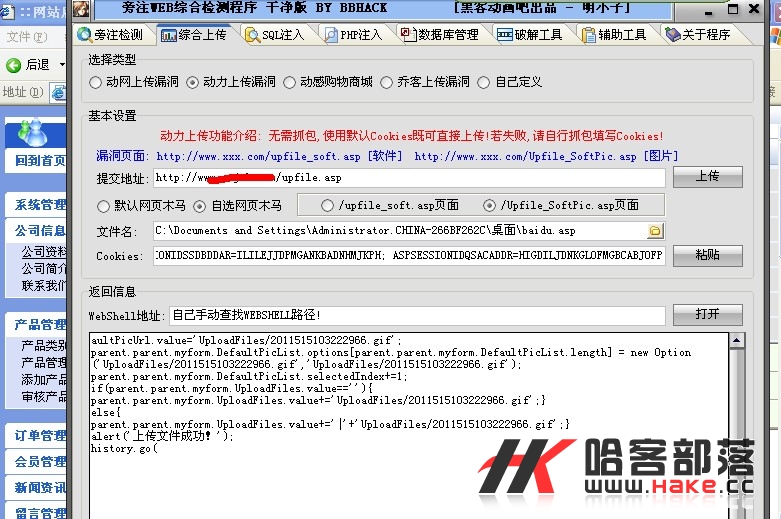
可是仔细看了一下。并没有良精后台传说中的页面,,连良精的通杀拿shell的配置页面/admin/SiteConfig.asp都消失的无影无踪。我估计这是良精的改版或者页面被管理员删除了。





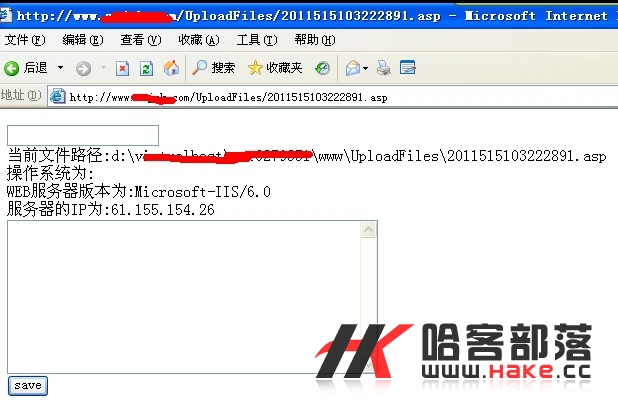
看到一上传页面。抓包上传之。

可是不管是用神马类型的方式上传。显示的结果都是gif后缀。



这时候翻到文件上传管理,发现了文件管理中有asp的文件。访问之确实是我刚才上传的小马





最后说一句撒。细心决定一切。很多过程我都一笔带过,图片很好的说明了我的方法。不解释不解释！~~~