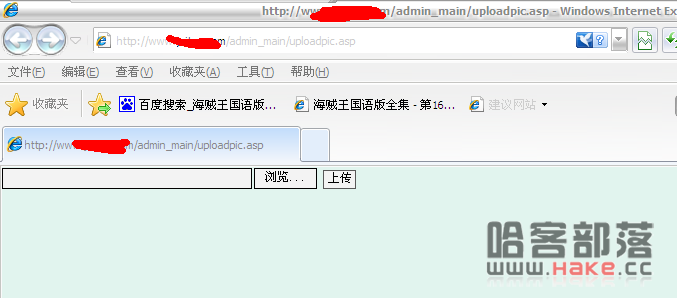
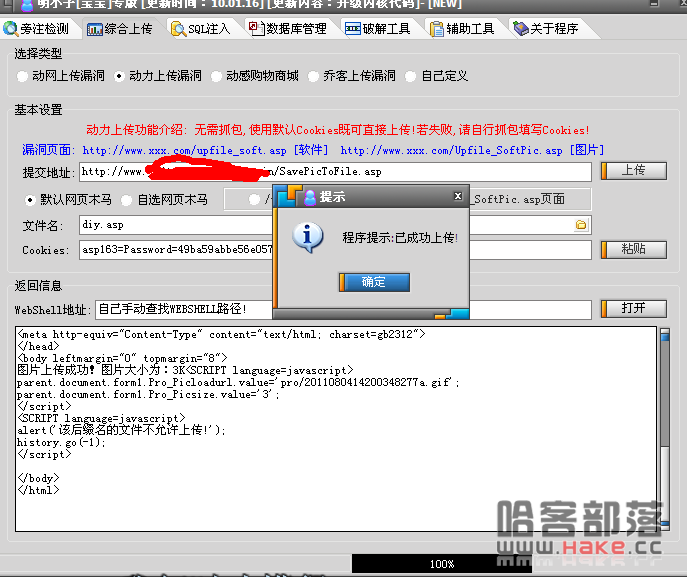
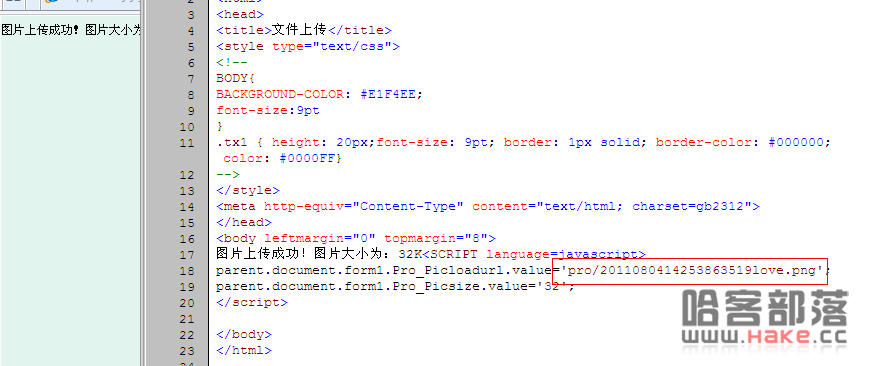
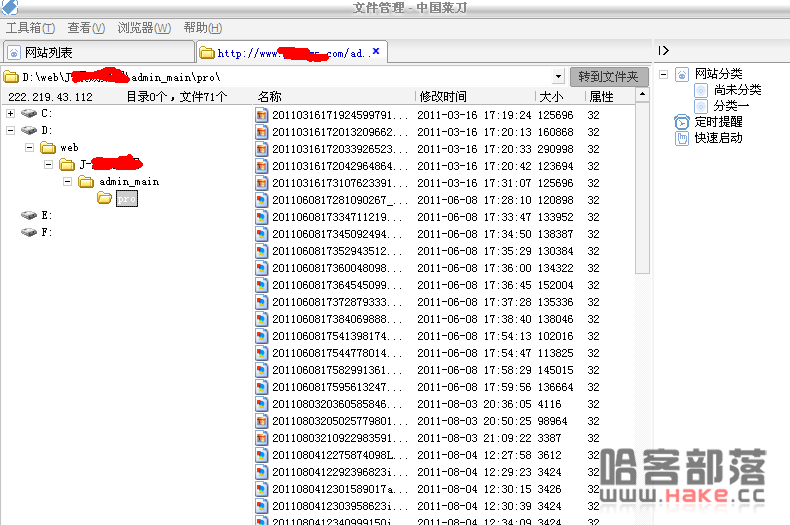
今天一朋友甩给我一个网站, 说是他公司的,注入无表名,只有个上传点, 叫我帮忙抓包试试看。  
   
  
好吧， 那就打开看看，很常见的一个上传。  
  
   
  
OK ， 试试简单的ASP文件上传无果，上个图片抓个包，拿到明小子上传试试，提示成功，  
但是访问是不存在的。  
   
  
这就蛋疼了，返回上传点继续看。  再上传个文件名love.png的图片瞧瞧看。  
  
   
上传成功， 而且在源码看地址时候发现，只要文件是以英文开头的，他只是在原来的名字前加上日期编码进行重命名。 看到这大家想到什么？ 对， IIS6.0解析漏洞， 马上上传个以love.asp;.jpg命名的网马. 上传成功。返回地址是：pro/2011080414294227060love.asp;.jpg。好吧， 访问一下，shit！ 不存在  
  
  
  
   
以为网马被杀, 换了好几个都是这样, shit! 再想想, 是不是过滤了文件里面的代码 ?  看到桌面有个图片一句话，想想就顺便传一下，图片名字也没去改，默认muma.asp.jpg。提示上传成功， 但是访问依然是不存在。好吧， 干你娘， 是不是名字太长了不让我访问啊我草。  回想一下，之前上传一个love.png图片 是成功的，然而上传了love.asp;.jpg还有muma.asp.jpg却不行， 两个文件名共同点就是ASP。好吧，测试一下是不是,上传mumaasp.jpg试试，  访问成功， 看到度娘的logo。  
   
不是过滤ASP ，  干你娘的， 想想之前传的love.asp;.jpg还有muma.asp.jpg还有一个共同点，就是有2个"."号,问题估计就是出在这里了, 重新命名一个图片木马, 一般来说，在众多IIS解析漏洞下利用的马马都是 XX.asp;.jpg,在分号后又多了一个后缀。想了下，记得II6.0下的解析漏洞原理是分号后面的全部无视，就搞了个名为love.asp;gif , 只有一个“.”号, 多了个分号, 好吧, 测试下，上传打开。表示很成功， 看到了熟习的百度logo，看来猜想是对的， 只要文件名有2个“.”以上包括2个，系统提示上传成功，但是根本是没上传！妇产科，  好了， 试试这个文件名有没起到IIS解析的效果(不知道你们有没见过，反正我是没见过，如果有，那就是我孤陋寡闻了。)。菜刀连之。 表示很OK 。  
   
  
  
整个过程就是这样， 主要是细心的观察，也没多大技术含量，但是就是那么让人蛋疼。  
  
  
抠字不容易，小菜写个文章也不容易， 管理给个原创吧， thank you.