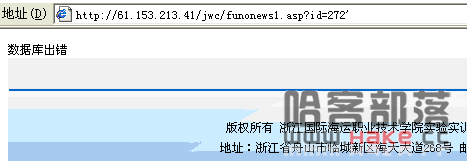
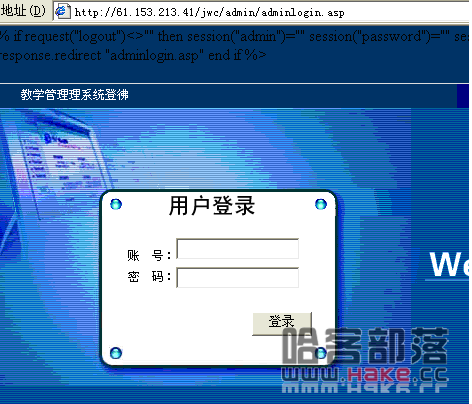
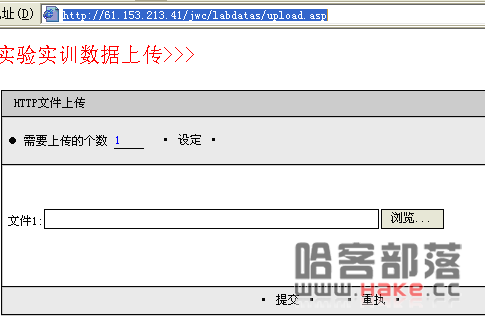
去年的一次渗透，没什么技术含量，只是觉得其中有几个地方新手朋友们可以当作收集一点经验，老鸟请飘过~~  
  
其中的地址，已经不能用了，那学校换了。所以只能看看了，再说是去年的事了。嘿~~

群里一朋友叫帮忙看一站点，网站是：[http://61.153.213.41](http://61.153.213.41/) 打开是邮件服务器软件 cmailserver webmail 5.4.6。我在这上面没看出什么来，就用wwwscan扫了一下后台。

很快就扫到了一个<http://61.153.213.41/jwc/a.asp> 打开看里面全是a，这个肯定是被人搞过的。把后面的a.asp删了就进到了浙江国际海运职业技术学院教学管理的站点上了，如图：  
   
    随便点点看，有个“实验实训”是新的，我们去看看，点开发现里面只有一篇文章，看来的确是新加的版块。点开这个文章看看，  
   
然后，加个‘来看看：  
   
再来，and 1=1 、and 1=2 返回了不一样的结果，确定有注入了。    
   接下来就是 and exists(select \* from admin)猜有没有admin这表了，返回正常。然后把\*换成usernmae结果返回错误，说明没有这个字段，换成user返回正常，呵呵，继续。。。再换成password返回正常。这下直接得到了表admin字段user、password。嘿~~~感觉挺简单的！！接着来猜长度，order by 10 猜到12时出错，说明是11。接着就  
And 1=2 union select 1,2,3,4,5,6,7,8,9,10,11from admin  
   
然后直接把 2，3替换成user、password,结果出错了，那么我就只替换pssword呢，结果爆出来了：  
   
因为一般的后台名是admin,所以有密码一般就足够了。爆出来的密码一看，不是cmd5加密的啊，这是雷池那加密的，网上有这个解密工具，解密后的密码是admin12345,我XX 弱口令啊，这时后台也扫出来了：  
[http://61.153.213.41/jwc/](http://61.153.213.41/jwc/a.asp)admin/adminlogin.asp，还扫出来了一个上传地址：<http://61.153.213.41/jwc/labdatas/upload.asp>。  
   
进后台一看，太简单了，也懒的看的太仔细，就先看看扫出来的另一个上传地址：<http://61.153.213.41/jwc/labdatas/upload.asp>  
 

试着传一个图片格式的小马，居然出错了，然后试试传一个真图片，居然还是出错，如下图：

   
看出错代码，类型不匹配，这应该是少了个什么参数。查看一下它的源文件如下：

<pclass="style1">实验实训数据上传>>></p>

<tablewidth="673" border="0">

<tr>

<tdwidth="667"><form name="form1" method="post"action="upfile.asp?xy=" enctype="multipart/form-data">

<label></label>

<p>

<input type="hidden"name="act" value="upload"></p>

他的提交地址action="upfile.asp?xy="后面没参数啊，难怪会出错了，怎么办呢，这里我就试着本地构造上传了，构造如下：

<pclass="style1">实验实训数据上传>>></p>

<tablewidth="673" border="0">

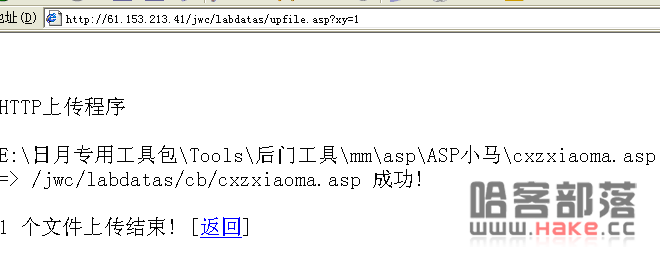
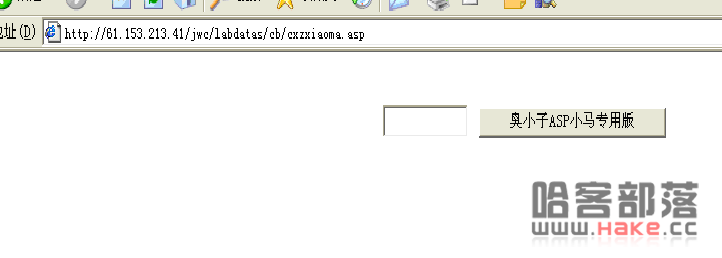
<tr>

<tdwidth="667"><form name="form1" method="post"action="<http://61.153.213.41/jwc/labdatas/upfile.asp?xy=1>" enctype="multipart/form-data">

<label></label>

<p>

<input type="hidden"name="act" value="upload"></p>

把完整的提交地址补全，后面缺少的参数，我试着补齐，也不知道补什么，随便补个1吧。本地提交一个asp的小马：  
   
居然上传无过滤，且上传成功了。我X，这也是RP么，  
   
上传大马，这些就不写了，把这个小马地址丢给了群里的那个朋友，闪人！