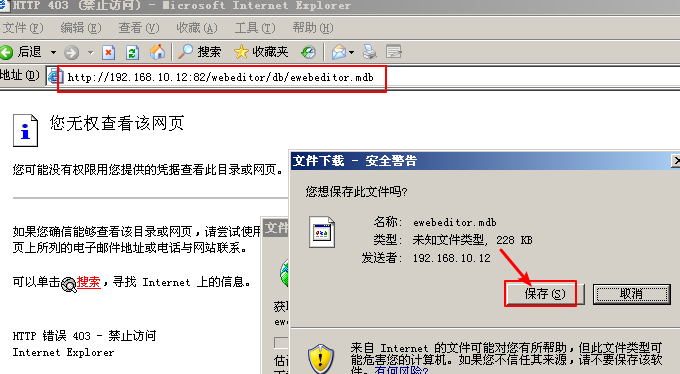
将Ewebeditor 编辑器上传到IIS服务器上，使用浏览器访问主页



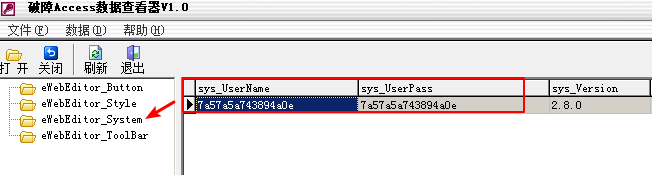
使用扫描工具扫描后台，默认的地址是编辑器目录下的 admin\_login.asp



默认账号密码是 admin admin ，如果不行可以尝试访问默认数据库位置，直接下载数据库



然后使用破障查看账号密码即可，如果是hash也可以去解密一下



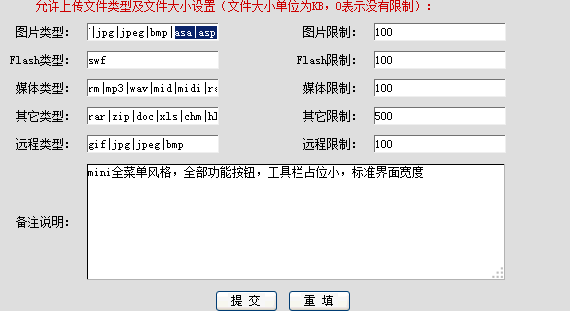
在刚刚的登录页面输入账号密码admin admin 后可以看到如下界面，点击样式管理



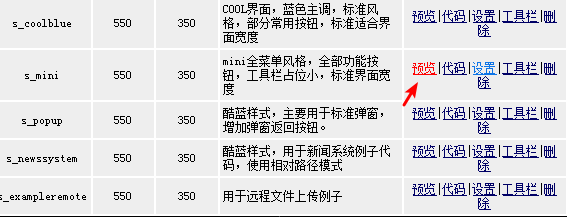
然后随便找个样式点击设置



在允许上传图片的类型上添加两个后缀 .asp .asa ，然后点击提交，注意如果这里没有提交，可以自己创建一个样式，然后改后缀，添加一个上传图片的插件。

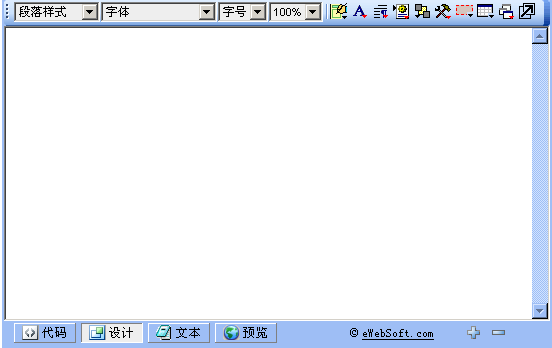


提交完后，点击预览，但是这里显示不全，蛋疼的是只有IE6.0才可以正常使用

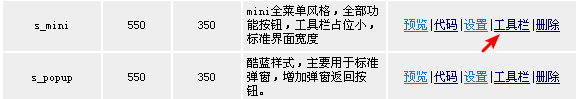


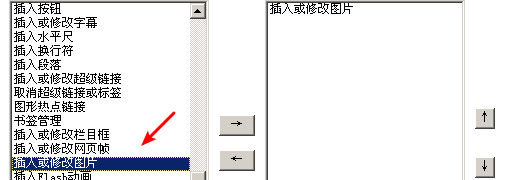


所以这里使用win2003自带的浏览器IE6.0来访问，登录账号密码访问上面的界面

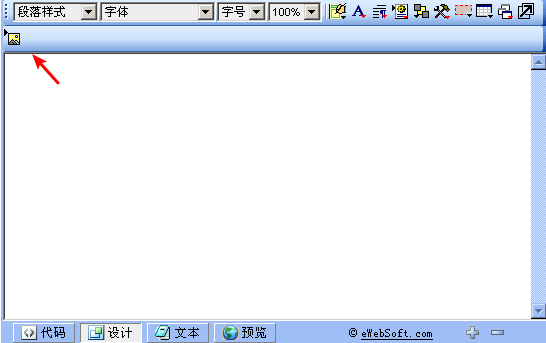


很可惜，迷你版没有上传插件，所以这里还需要自己添加一个上传图片的插件

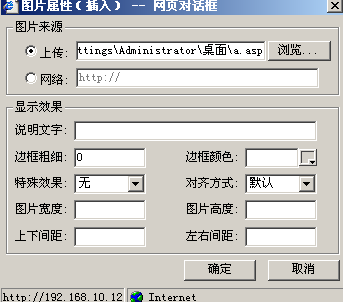




保存设置后，点击预览



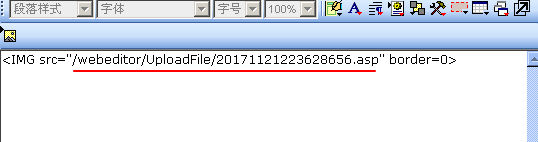
然后将图片asp木马直接改名成a.asp上传上去



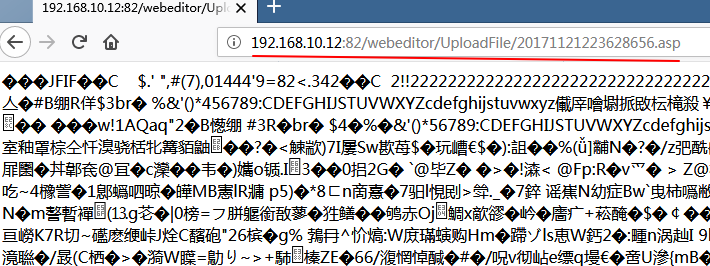
注意：如果这里不允许使用asp上传的话，也可以将木马换成a.asa一样也可以被解析成木马



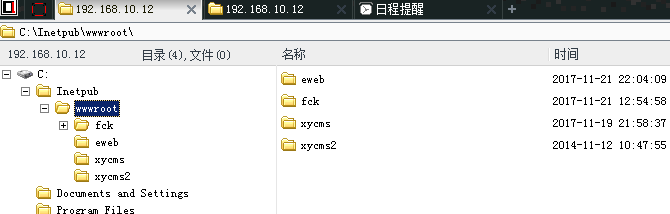
上传好后，点击顶部的代码，查看图片所上传的位置



将图片位置复制，使用浏览器访问



然后使用菜刀连接即可。



**Ewebeditor目录便利漏洞**



进入后台，点击文件上传接口，然后选择样式目录中随便选择一个



将URL中的id=22 改成 id=&dir=.. 然后回车



可以发现跑到上级目录了，如果点击返回上一级就

继续访问参数： id=&dir=../..



这时候应该是到了wwwroot下，可以看到旁站了，尝试点击旁站访问下



旁站的源代码全部暴露，这样就可以去搞旁站了，当然也可以继续访问上级目录

继续访问参数： id=&dir=../../../.. 一直到C盘根目录后就出不去了



虽然可以列举和浏览任意位置的文件，但是无法查看文件内容和下载这些文件

