**电气公司网站渗透文档**

**站点首页截图**

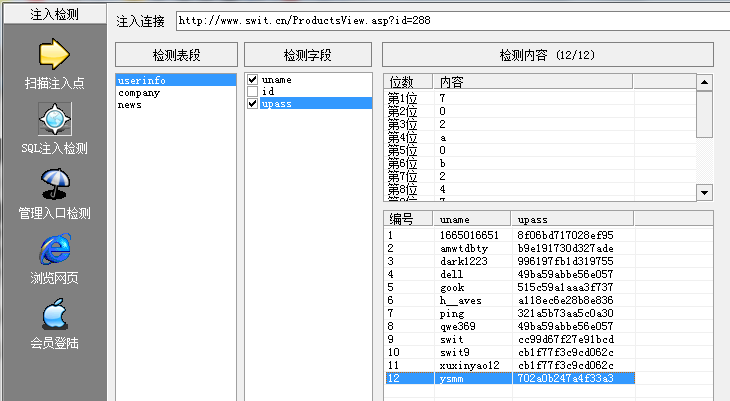
****

**一、SQL注入漏洞**

* + 1. 使用工具进行漏洞测试

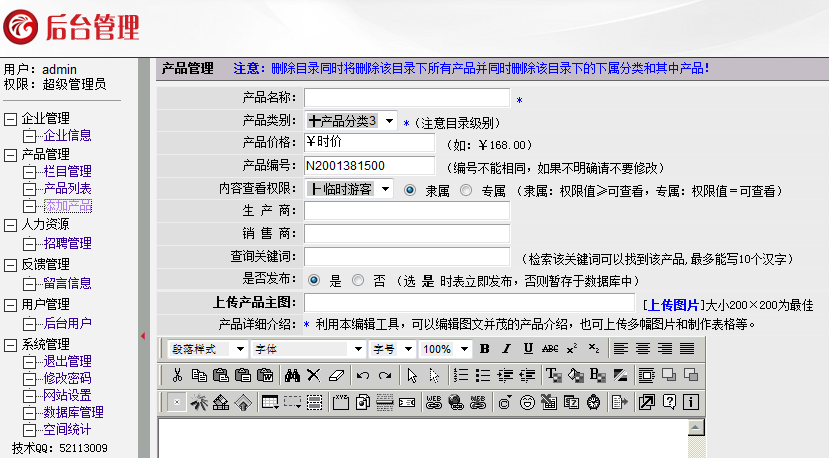


破解



选择用户名：admin 密码:admin888

http://192.168.1.168:93/System/index.asp



**二、XSS漏洞**

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

<http://192.168.1.168:93/FeedbackAdd.asp>



1. 登录后台管理点击留言信息，返回带有cookie的提示窗



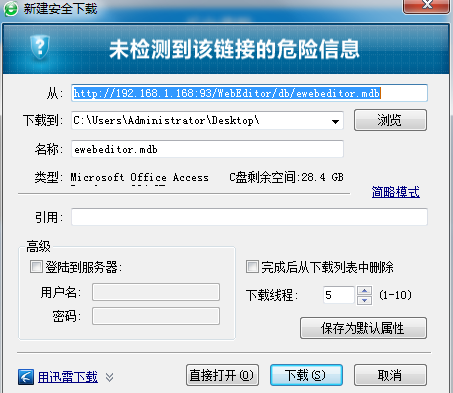
**三、编辑器漏洞**

1. 联系我们-QQ图标，右键属性，可以看到当前网站使用的编辑器是webeditor



1. 打开编辑器默认的数据库地址，下载数据库并查看编辑器的用户名密码

<http://192.168.1.168:93/WebEditor/db/ewebeditor.mdb>



1. 编辑器默认管理地址：<http://192.168.1.168:93/webEditor/admin_login.asp>，注意需要先成功登录网站后台管理后，才能登录编辑器后台管理，用户名admin密码admin



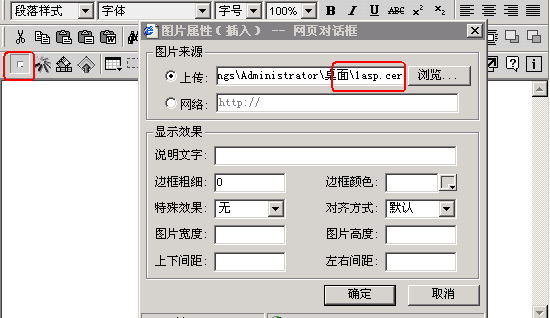
1. 点击样式管理



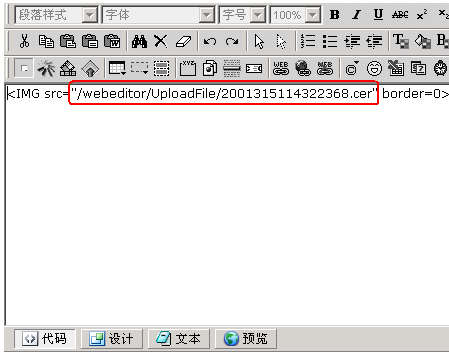
1. 默认样式不允许编辑，点击后面的拷贝，生成一个新的样式表standard，并进行设置，在图片类型中增加asa、cer类型

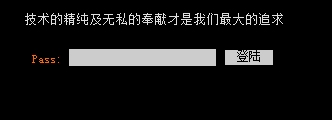


1. 设置完成后，点击预览，点击插入图片，浏览木马并上传



1. 上传完成后，点击“代码”按钮，查看上传路径，并在浏览器中打开该木马





**四、目录遍历漏洞**

1. 浏览器输入目录遍历地址：/webEditor/admin\_uploadfile.asp?id=14&dir=../../../

