**国际环保网站渗透文档**

**站点首页截图**

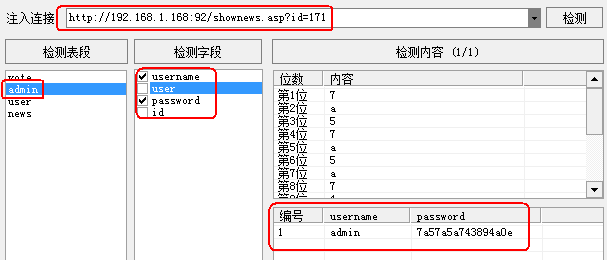
****

**一、SQL注入漏洞**

* + 1. 使用工具进行漏洞测试



注入检测

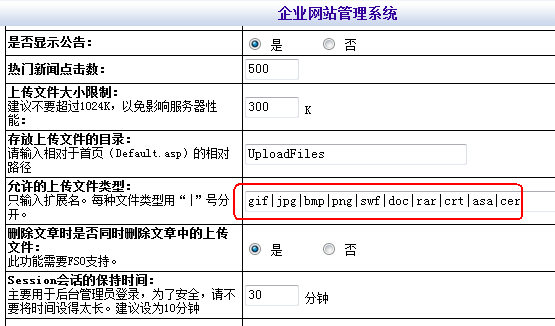


用户名为admin 密码admin

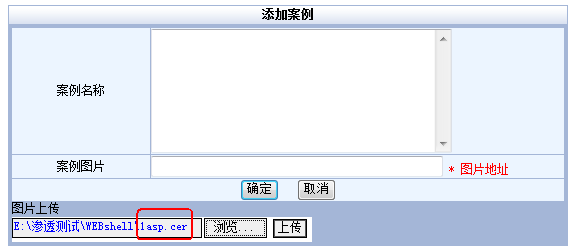
登录后台管理 http://192.168.1.168:92/admin/login.asp



* + 1. 进入后台后，点击系统管理->网站配置，在此处上传.cer格式木马文件



* + 1. 进入后台后，点击成功案例->添加成功案例，在此处上传.cer格式木马文件

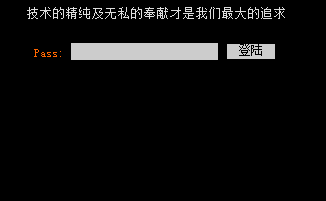


* + 1. 上传成功后，复制图片木马地址



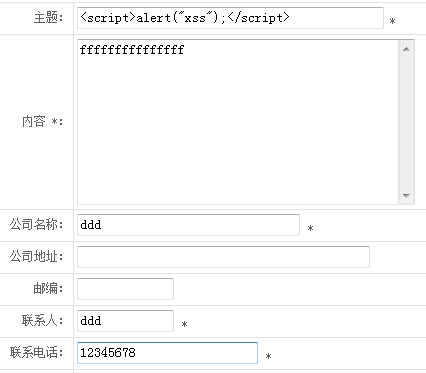
* + 1. 在浏览器中打开该上传的文件

<http://192.168.1.168:92/UploadFiles/200131015479686.cer>

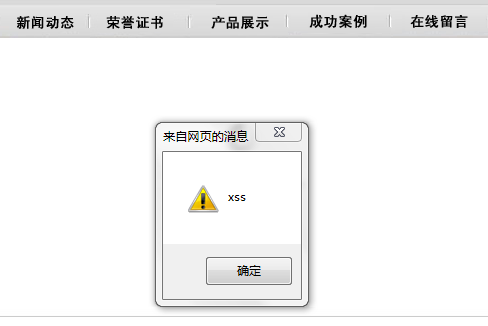


**二、XSS漏洞**

1. 在线留言栏目下主题中插入XSS脚本，<script>alert("xss");</script>



1. 返回带有XSS的提示窗



**三、目录遍历漏洞**

1. 浏览器输入目录遍历地址：http://192.168.1.168:92/admin/JZPeditor/Admin\_UploadFile.asp?id=34&dir=../..



**四、数据库备份漏洞**

1. 先在在线留言标题中插入ASP一句话木马：
2. 登录后台管理-系统管理-数据库备份-备份名称为123.asp



1. 打开一句话木马上传客户端，木马地址处输入备份的数据库地址如下

