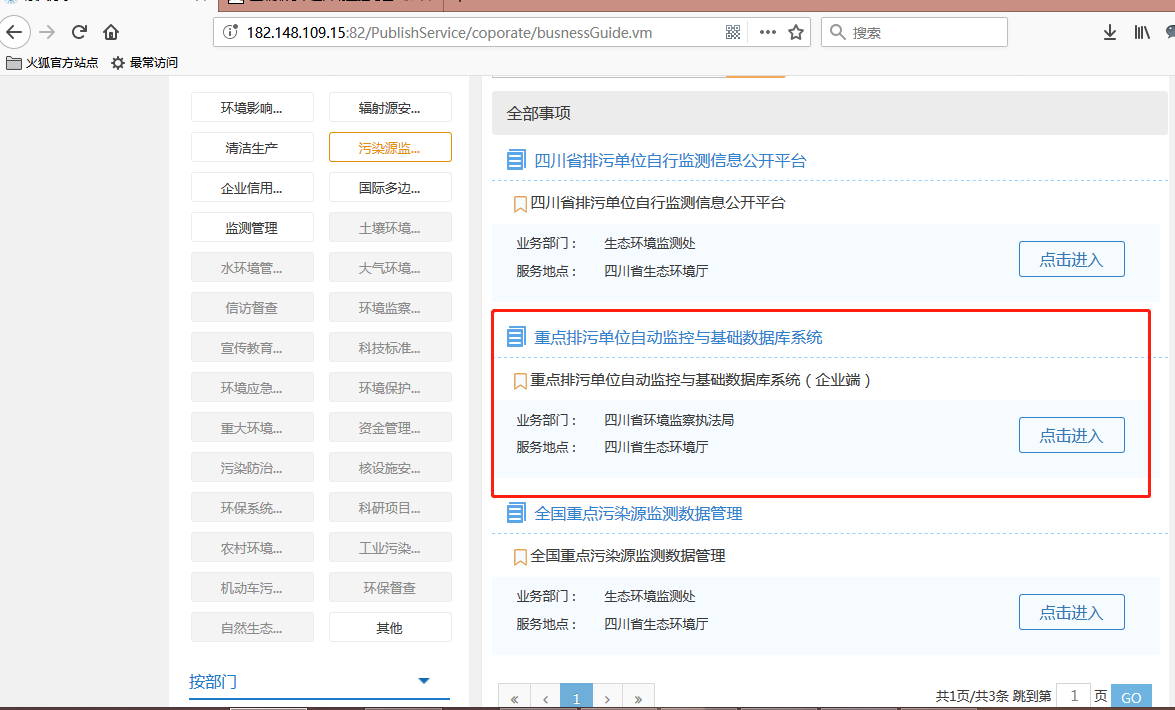
漏洞名称：xss

影响站点：http://182.148.109.179:8888/amOnline/app/AppMain.page

# http://182.148.109.179:8888/amOnline/app/AppMain.page

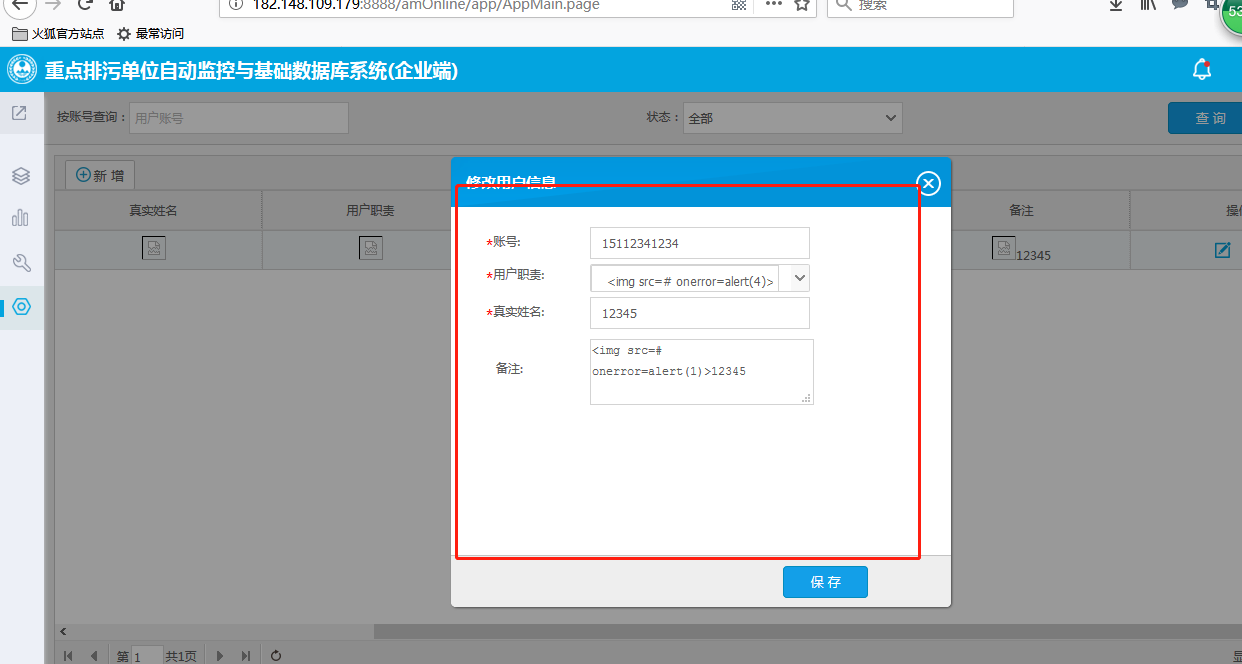
Payload： %3Cimg+src%3D%23+onerror%3Dalert(1)%3E

测试过程：点击重点排污单位自动监控与基础数据库系统



在账户管理这里点击修改信息

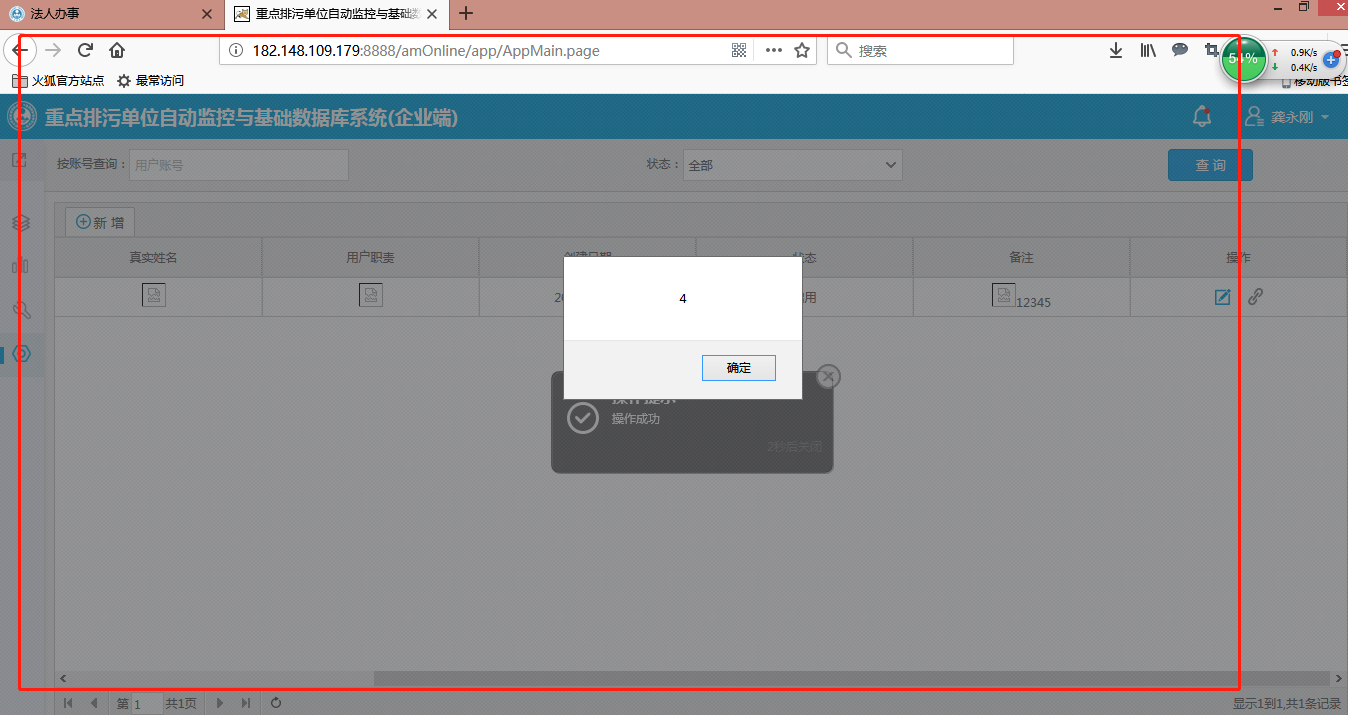




用burp进行抓包，修改这里的4个参数search\_usernam、search\_true\_name、search\_describ、search\_userType为payload：

%3Cimg+src%3D%23+onerror%3Dalert(1)%3E

可以看到成功弹窗



漏洞危害：攻击者可以利用此漏洞构造url引诱他人点击此链接，然后获取他人的cookie，从而登陆用户账户，进一步控制整个系统

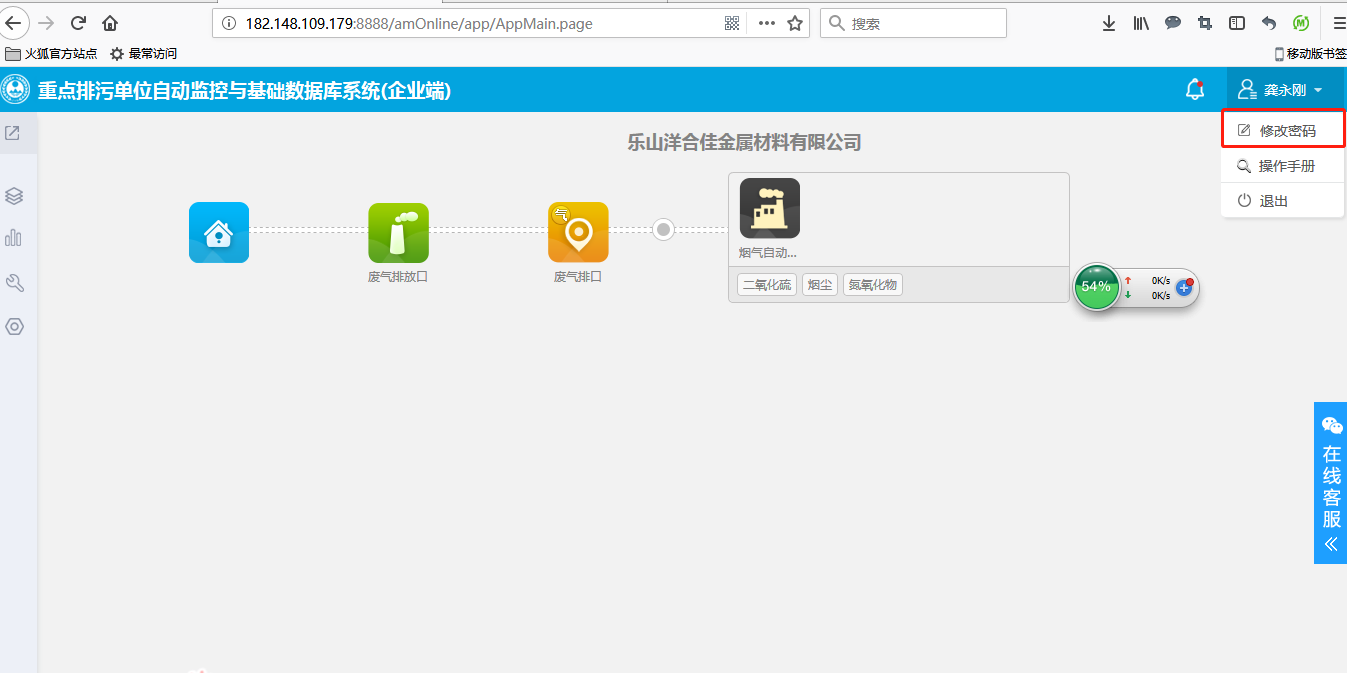
修复建议：对4个参数search\_usernam、search\_true\_name、search\_describ、search\_userType参数的输入进行过滤，将危险的script等字符进行过滤； 对4个参数search\_usernam、search\_true\_name、search\_describ、search\_userType参数的输出进行html实体编码，防止恶意script脚本被成功解析执行

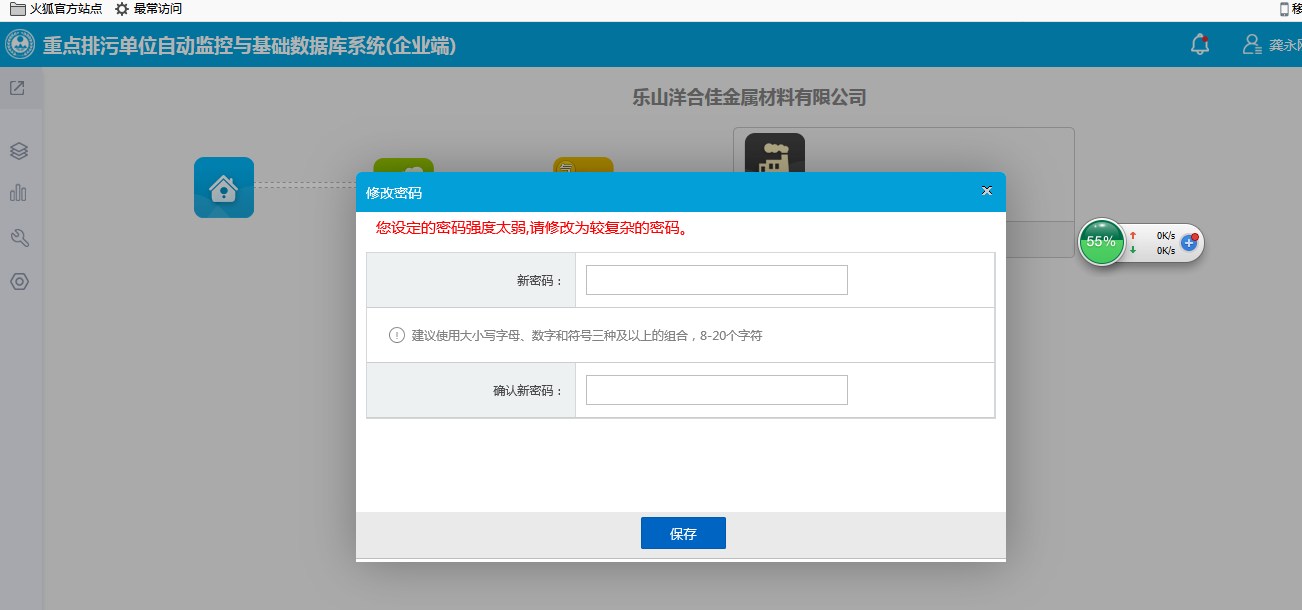
Csrf漏洞

<http://182.148.109.179:8888/amOnline/app/AppMain.page>

测试过程：

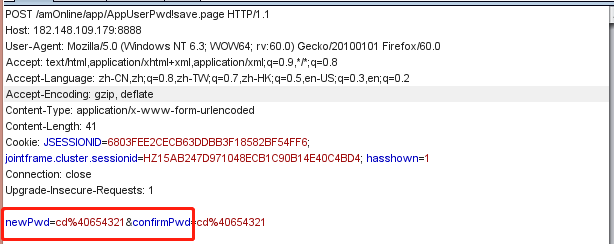
在界面上看到修改密码接口，点击修改密码



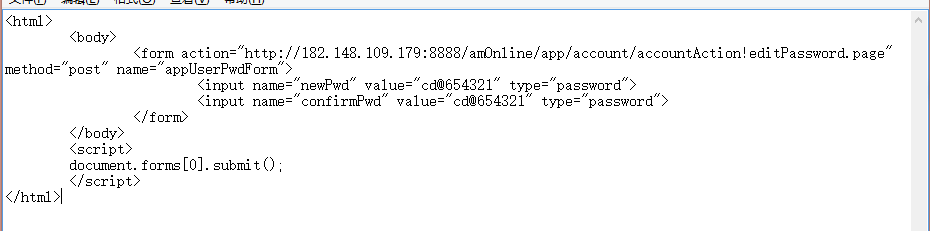


发现不需要输入原密码等操作

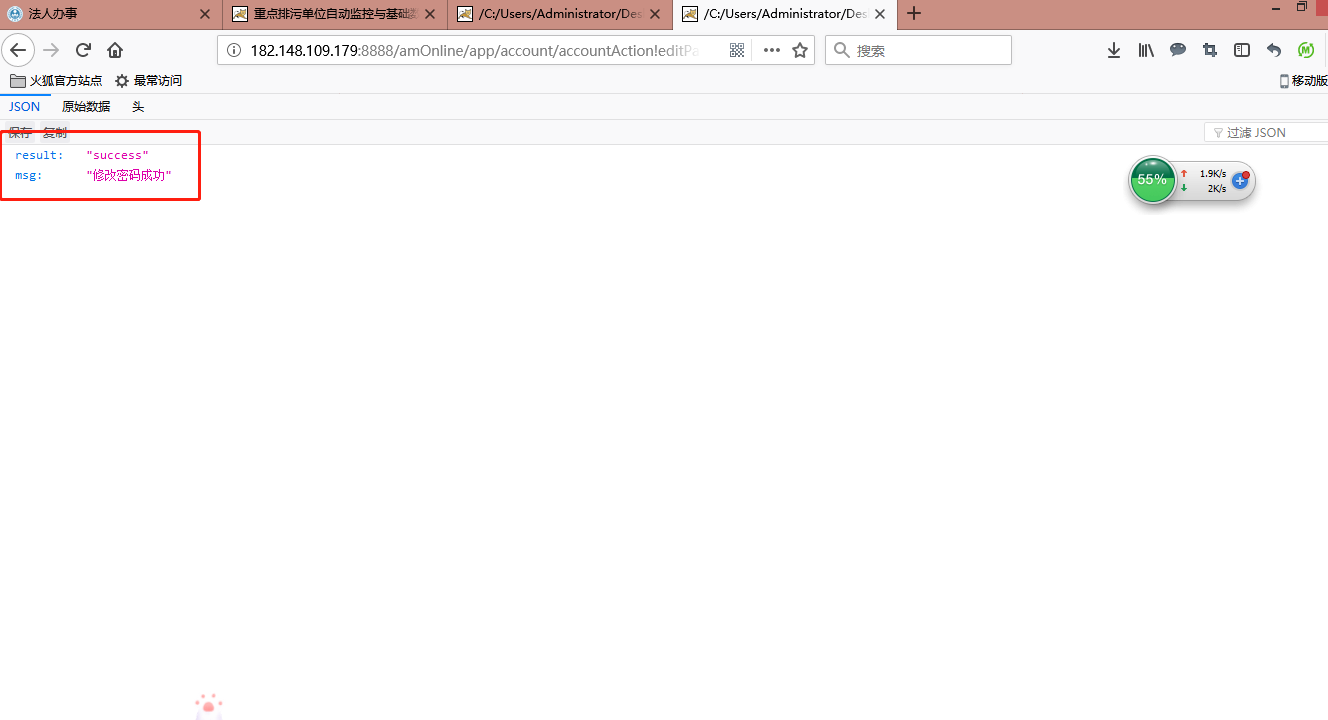
于是查看源码，发现提交的post数据有2个 newPwd&confirmPwd



构造form表单



在本地打开，发现更改密码成功



漏洞影响：攻击者可以伪造一个form表单，诱使受害者点击html文件或地址，然后可以任意修改受害者的账户密码，从而登陆受害者账户

修复建议：对referer字段进行校验，比如只允许同域名下的referer等；对修改密码的url添加随机token；修改密码的时候应该先确认原密码是否正确，或者添加验证码等验证操作