R15-4润乾报表-企业级报表工具-文件上传

漏洞描述:

润乾报表平台 dataSphereServlet 接口存在任意文件上传漏洞,未经身份攻击者可通过该漏洞上传恶意后门文件,执行任意指令,最终可导致服务器失陷。

网站图片:





HTTP Status 404 - /demo/reportJsp/showRe

type Status report

message /demo/reportJsp/showReport.jsp

description The requested resource is not available.

Apache Tomcat/7.0.77

网络测绘:

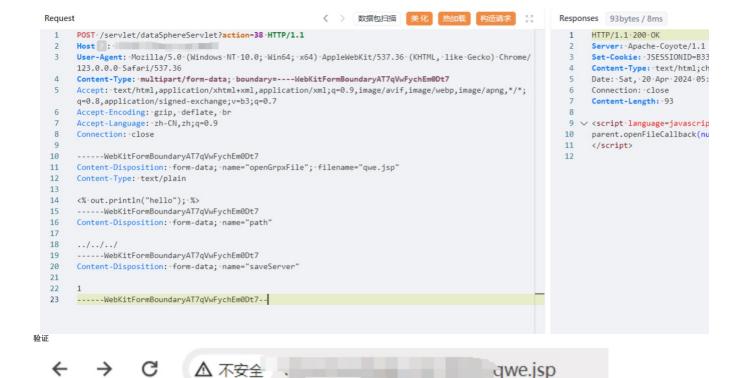
Hunter 语法:

鹰图指纹: app.name="润乾报表平台"

漏洞复现:

payload:

效果图:



hello

Windows IP ??

?????? ???: