# 金和-c6 carcardinfo-aspx sql注入

## 漏洞描述

金和-c6 carcardinfo-aspx sql注入,攻击者可通过此漏洞获取数据库敏感信息，从而为下一步攻击做准备。

## 漏洞复现

1. Fofa

app="金和网络-金和OA"



1. 界面如下



1. Nuclei

id: need\_to\_change

info:

name: need\_to\_change

author: m0be1

severity: high

http:

- raw:

- |

GET /c6/JHSoft.Web.Vehicle/CarCardInfo.aspx/ HTTP/1.1

Host: {{Hostname}}

Cache-Control: max-age=0

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_15\_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 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-HK;q=0.9,zh;q=0.8

Connection: close

matchers:

- type: dsl

dsl:

- status\_code==200 && contains\_all(body,"选择牌照")

## 修复建议

1. 升级到安全版本

2、如非必要，禁止公网访问该系统。

3、设置白名单访问。