4.24汇报

PentestAgent

- 主要目的为将源代码中使用到的**GPT模型**均替换为**DeepSeek模型**

ReconAgent

API替换

- 核心改动：将 OpenAI 原生 API 替换为 DeepSeek API
- 由于Deepseek的API设计与OpenAI类似，因此可以直接使用OpenAI SDK兼容方式，但是必须**指定** `base_url`

```
# 初始化DeepSeek客户端
self.client = OpenAI(
    api_key="sk-cba71d6e422f4f06a37ea31fb2f4ac37",
    base_url="https://api.deepseek.com"
)
```

源码在ReconAgent部分只有一个`ReconAgent`类，直接使用OpenAI的客户端库来创建和管理**Assistant**、**Thread**、**Message**等，但是在DeepSeek中并没有像Assistant这样的东西

实现类似功能的做法：定义了两个类：`DeepSeekAssistant`和`ReconAgent`。

- `DeepSeekAssistant`是对DeepSeek API的一个封装，用于**模拟**OpenAI的Assistant功能。
- `ReconAgent`是主控类，负责管理对话线程、消息发送、运行线程以及与DeepSeek API的交互。

线程与状态管理的重构

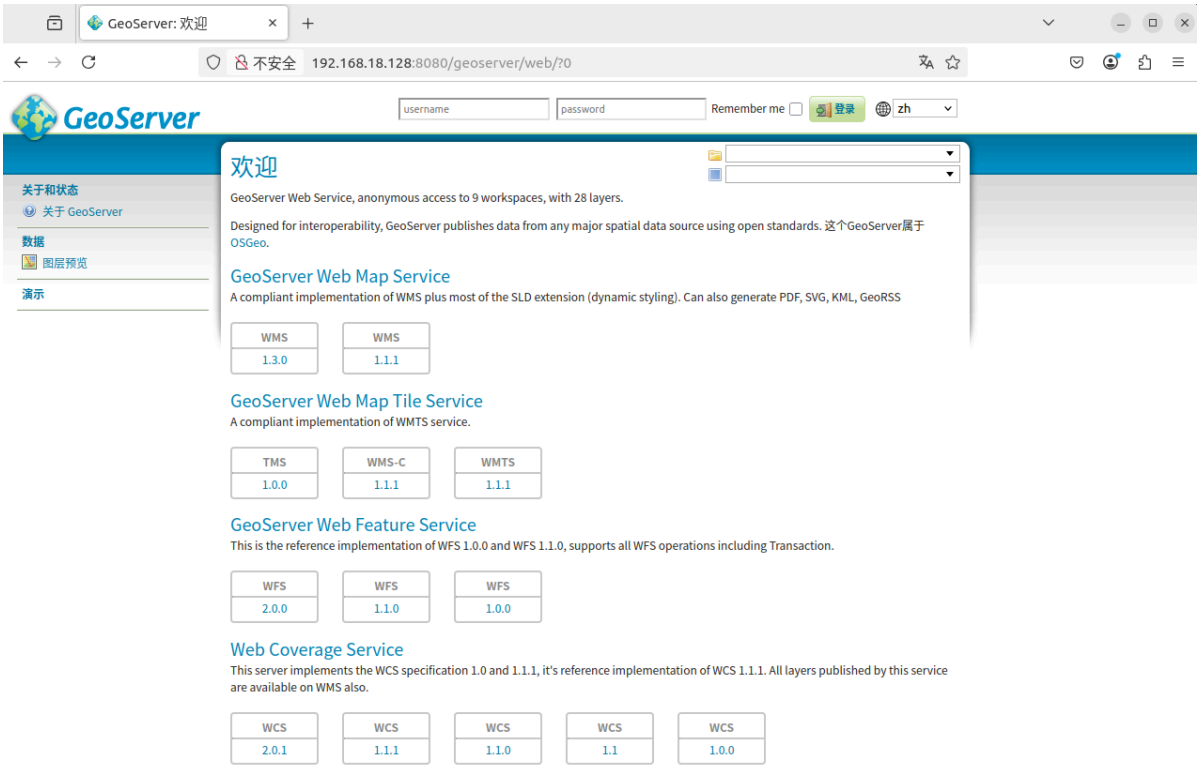
- 核心改动：从依赖 OpenAI 原生 Thread 对象转为本地模拟线程生命周期。
- 实现 init_thread、send_message、run_thread 等方法，完全自行管理线程状态（如 running/completed/failed）
- 添加本地持久化逻辑（如 _save_persistent_state 和 _load_persistent_state），将线程、助手配置保存到 JSON 文件。
- 移除对 OpenAI Thread ID 的依赖，改为基于 topic 的本地映射（thread_map）

修改后的效果

第一步：在目标机器上构建靶场

```
WARN[0000] /home/yyk/桌面/vulhub/vulhub-master/geoserver/CVE-2023-25157/docker-compose.yml: `version` is obsolete
[+] Running 3/3
 ✔ Network cve-2023-25157_default       Created
 ✔ Container cve-2023-25157-postgres-1  Started
 ✔ Container cve-2023-25157-web-1       Started
root@yyk-virtual-machine:/home/yyk/桌面/vulhub/vulhub-master/geoserver/CVE-2023-25157#
```

在浏览器中检验其是否可访问；`url:http://192.168.18.128:8080`



第二步：提供目标IP至ReconAgent，然后执行代码

```
try:
    # 初始化智能体
    agent = ReconAgent()
    topic = "geoserver_CVE-2023-25157"
    target_ip = "192.168.18.128:8080"
```

```
2025-04-21 04:07:56,456 [INFO] __main__ - 创建新助手: 渗透测试侦察专家
2025-04-21 04:07:56,456 [INFO] __main__ - 侦察智能体初始化完成
2025-04-21 04:07:56,456 [INFO] __main__ - 初始化新线程，主题: geoserver_CVE-2023-25157，ID: f3aefa2f-5b03-4994-bba0-e8203fa59e0b
2025-04-21 04:07:56,456 [INFO] __main__ - 初始消息已发送: 我需要利用目标主机 192.168.18.128:8080
2025-04-21 04:07:56,456 [INFO] __main__ - ═══ 迭代 1/10 ═══
2025-04-21 04:07:57,486 [INFO] httpx - HTTP Request: POST https://api.deepseek.com/chat/completions "HTTP/1.1 200 OK"
2025-04-21 04:08:04,679 [INFO] __main__ - 主题 geoserver_CVE-2023-25157 运行完成，生成响应长度: 211
2025-04-21 04:08:04,679 [INFO] __main__ - AI原始响应:
```json
{
    "analysis": "None",
    "next_step": "First, perform a basic Nmap scan to identify the operating system and open ports on the target host.",
    "executable": "nmap -O -p 8080 192.168.18.128"
}
```
```

```
2025-04-21 04:08:04,679 [INFO] __main__ - 执行命令: nmap -O -p 8080 192.168.18.128
2025-04-21 04:08:04,679 [INFO] __main__ - 执行系统命令: nmap -O -p 8080 192.168.18.128
2025-04-21 04:08:16,272 [INFO] __main__ - 命令输出（647 字节）
2025-04-21 04:08:16,272 [INFO] __main__ - ═══ 迭代 2/10 ═══
2025-04-21 04:08:17,064 [INFO] httpx - HTTP Request: POST https://api.deepseek.com/chat/completions "HTTP/1.1 200 OK"
2025-04-21 04:08:26,712 [INFO] __main__ - 主题 geoserver_CVE-2023-25157 运行完成，生成响应长度: 471
2025-04-21 04:08:26,712 [INFO] __main__ - AI原始响应:
```json
{
    "analysis": "The Nmap scan indicates that port 8080 is open and running an HTTP proxy service. The target host is likely running a Linux kernel between versions 4.15 and 5.8.",
    "next_step": "Perform a detailed service and version detection scan on port 8080 using Nmap scripts to identify the specific HTTP service and its version.",
    "executable": "nmap -sV -p 8080 --script=http-enum,http-title,http-server-header,http-headers 192.168.18.128"
}
```
```

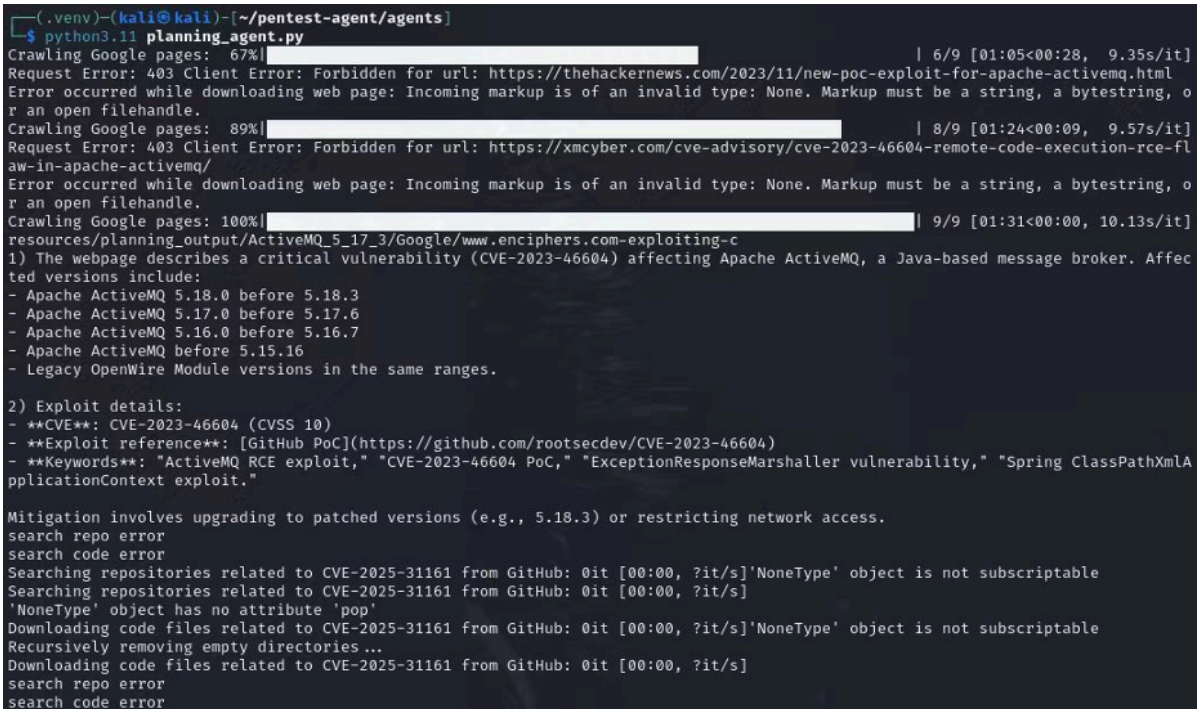
```
    "next_step": "The reconnaissance phase is complete. Next steps would be to: 1) Research known vulnerabilities in GeoServer 2.22.1 and Jetty 9.4.48, 2) Attempt to access restricted resources if credentials are available, 3) Check for misconfigurations in the exposed services.",
    "executable": "None"
}
```

2025-04-21 04:09:53,035 [INFO] __main__ - 未检测到有效命令，进入总结阶段
2025-04-21 04:09:53,404 [INFO] httpx - HTTP Request: POST https://api.deepseek.com/chat/completions "HTTP/1.1 200 OK"
2025-04-21 04:10:22,708 [INFO] __main__ - 主题 geoserver_CVE-2023-25157 运行完成，生成响应长度: 1946
2025-04-21 04:10:22,708 [INFO] __main__ - ═══ 最终侦察总结 ═══
2025-04-21 04:10:22,709 [INFO] __main__ - 执行完成，总耗时: 146.32秒
```
```

```
"analysis": {
    "8080": {
        "service": "Jetty",
        "version": "9.4.48.v20220622",
        "web_application": {
            "name": "GeoServer",
            "version": "2.22.1",
            "authentication": {
                "method": "Spring Security",
                "login_url": "/geoserver/j_spring_security_check",
                "form_fields": ["username", "password", "_spring_security_remember_me"]
            },
            "content": {
                "workspaces": ["cite", "it.geosolutions", "ne", "nurc", "sde", "sf", "tiger", "topp", "vulhub"],
                "layers": 28,
                "services": ["WMS", "WMTS", "WFS", "WCS"]
            },
            "vulnerability_notes": {
                "GeoServer_2.22.1": "Check for known vulnerabilities in this version",
                "Jetty_9.4.48": "Check for vulnerabilities in this Jetty version"
            }
        }
    }
```


PlanningAgent

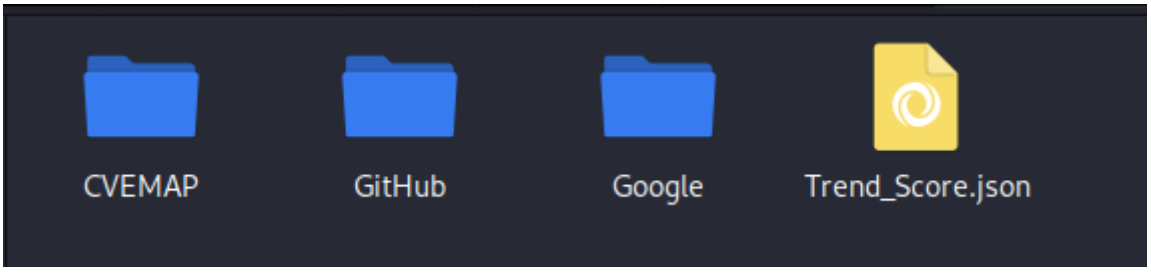
- 通过 DeepSeekLLM 类封装 API 调用,支持DeepSeek



- 由 `cvemap_product` 函数获取到的cve数据将储存为cvemap.json文件

```
{
  "cve_id": "CVE-2024-36401",
  "cve_description": "GeoServer is an open source server that allows users to share and edit geospatial data
y unauthenticated users through specially crafted input against a default GeoServer installation due to unsaf
ttribute names for feature types in a way that unsafely passes them to the commons-jxpath library which can e
eature types (i.e., Application Schema data stores) but is incorrectly being applied to simple feature types
ulnerability has been confirmed to be exploitable through WFS GetFeature, WFS GetPropertyValue, WMS GetMap, W
n\nVersions 2.22.6, 2.23.6, 2.24.4, and 2.25.2 contain a patch for the issue. A workaround exists by removing
unning GeoServer 2.25.1). This will remove the vulnerable code from GeoServer but may break some GeoServer fu
  "severity": "critical",
  "cvss_score": 9.8,
  "cvss_metrics": {
    "cvss31": {
      "score": 9.8,
      "vector": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H",
      "severity": "critical"
    }
  },
  "weaknesses": [
    {
      "cwe_id": "CWE-95",
      "cwe_name": "Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')"
    },
    {
      "cwe_id": "CWE-94",
      "cwe_name": "Improper Control of Generation of Code ('Code Injection')"
    }
  ],
  "epss": {
    "epss_score": 0.94418,
    "epss_percentile": 0.99976
  },
  "cpe": {
    "cpe": "cpe:2.3:a:geoserver:geoserver:*:*:*:*:*:*:*:*",
    "vendor": "geoserver",
    "product": "geoserver"
  },
  "reference": [
    "https://github.com/Linxloop/fork_POC",
    "https://github.com/bigb0x/CVE-2024-36401"
```


程序完成运作之后将会得到以下四个文件



目前存在的问题

- google信息收集过程中，某些网站可能存在反爬机制，可能导致某些关键信息的缺失
- GitHub在利用CVE_ID进行检索漏洞利用信息的过程中也会产生信息的缺失
- **结果分析阶段**使用到的doc_handler中利用到Llama_Index中的**RAG**，但是目前llama_Index中并**未集成DeepSeek**（目前处于解决该问题阶段）