AI 辅助渗透测试工具编写

密　　级：公　开

编写日期：2024/5/6

编 写 人：Lewis

修订页

编号	章节名称	修订内容简述	修订日期	修订后版本号	修订人
1	初版		5.6	1.0	Lewis

目录

1 引言

1.1 编写目的

本文档《AI 辅助渗透测试工具编写记录》旨在详细记录和展示 AI 辅助渗透测试工具从概念设计到最终实现的整个过程。文档的主要目的包括：

1. **记录开发历程**：详细记录工具开发的每一步，包括需求分析、系统设计、编码实现、测试验证以及部署上线等，为团队成员提供一个共享知识平台。

2. **展示工作成果**：通过文档形式，向项目干系人（包括但不限于管理层、同事、潜在用户或合作伙伴）展示团队的工作成果和进度。

3. **技术交流与分享**：提供给同行或感兴趣的开发者一个参考，促进技术交流，共同推动 AI 在渗透测试领域的应用和发展。

4. **问题追踪与解决**：记录在开发过程中遇到的问题及其解决方案，帮助团队成员理解问题背景，分析原因，并掌握解决策略。

5. **维护与升级指导**：为工具未来的维护和升级工作提供参考文档，确保工具能够持续适应新的安全威胁和漏洞特征。

6. **风险评估与应对**：评估工具可能带来的安全风险，并提出相应的风险应对措施，确保工具的安全性和可靠性。

7. **知识积累与传承**：作为团队知识管理的一部分，本文档将帮助新团队成员快速了解项目背景、现有工作和未来的发展方向。

8. **项目文档化**：遵循软件开发的最佳实践，通过文档化提高项目的透明度，为项目管理和质量保证提供支持。

9. **成果评估与反馈**：为项目评估和用户反馈提供详细的信息基础，帮助评估工具的有效性和用户满意度。

10. **遵守合规性要求**：确保工具的开发和使用遵守相关的法律法规和行业标准，特别是在信息安全和数据保护方面。

通过本文档，我期望能够为 AI 辅助渗透测试工具的开发和应用提供一个全面、系统的记录。

1.2 背景介绍

为了提高渗透测试的效率和准确性，引入自动化工具已成为行业发展的必然趋势。AI 技术的快速发展，尤其是在模式识别、数据分析和预测建模方面的能力，为渗透测试领域带来了新的机遇。AI 辅助渗透测试工具能够通过学习历史安全数据，自动识别潜在的安全威胁，预测攻击行为，并给出相应的防护建议。

本工具的开发背景基于以下几点考虑：

1. **提升效率**：AI 辅助分析可以大幅减少安全分析师在数据收集、模式匹配和威胁识别上的工作量。

2. **增强准确性**：利用机器学习和深度学习算法，工具能够更准确地识别复杂的攻击模式和未知威胁。

3. **应对复杂性**：随着网络攻击手法的不断进化，AI 的自学习和自适应能力有助于应对新的安全挑战。

4. **实时响应**：AI 辅助工具能够实现对安全事件的快速响应，及时阻断攻击，减少潜在损失。

5. **知识积累**：通过持续学习新的安全事件和威胁情报，AI 辅助工具能够不断优化其分析模型，提升安全防护水平。

6. **资源优化**：在有限的安全专家资源下，AI 辅助工具可以承担更多的重复性工作，让专家能够专注于更复杂的安全分析任务。

7. **合规性要求**：遵守行业标准和法律法规，确保渗透测试过程合法合规，同时 AI 辅助工具的使用也需符合相关的数据保护要求。

综上所述，开发 AI 辅助渗透测试工具是为了结合人工智能的先进技术，提升渗透测试的能力，以更高效、更智能的方式应对日益严峻的网络安全挑战。

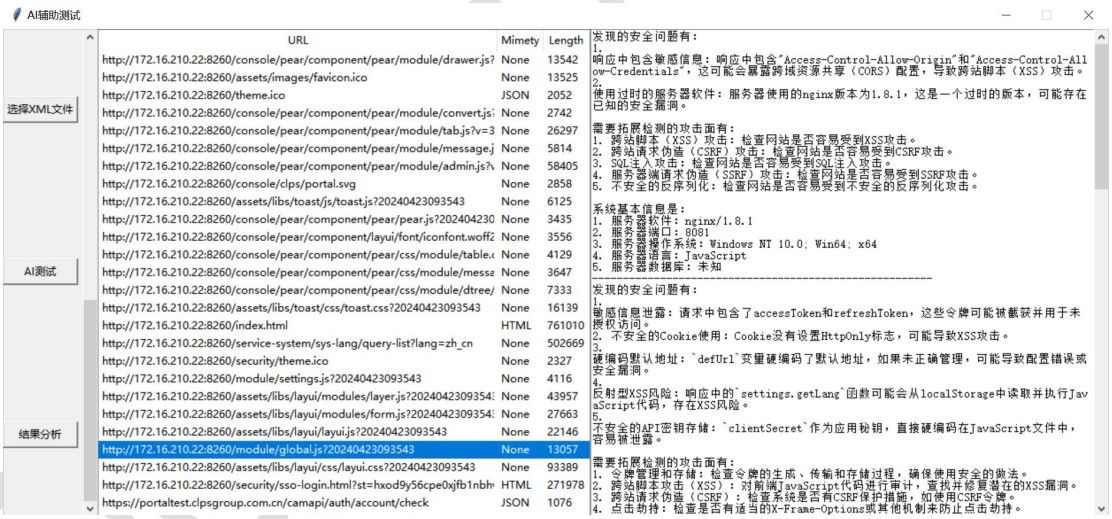
2 工具概述

2.1 工具名称

AI 辅助渗透测试

2.2 功能描述

目前工具实现界面



AI 辅助渗透测试工具旨在通过自动化和智能化手段增强渗透测试的深度与广度。目前，该工具已实现以下核心功能：

1. **网站数据包分析**：工具能够捕获并分析网站的数据包，识别网络流量中的各种协议和潜在问题。

2. **AI 分析网站安全性**：利用机器学习模型，工具可以自动评估网站数据包的安全性，包括但不限于识别常见的安全漏洞和异常行为。

3. **安全问题识别**：工具能够列出发现的安全问题，如 SQL 注入点、跨站脚本（XSS）漏洞、不安全的 HTTP 方法等。

4. **攻击面拓展检测**：除了已知漏洞，工具还能基于 AI 分析结果，提出需要进一步拓展检测的潜在攻击面。

5. **系统基本信息收集**：工具自动收集并展示目标系统的基本信息，如服务器类型、操作系统版本、服务运行状态等。

6. **分析结果保存**：所有分析结果都可以被保存为结构化的报告，方便后续的查阅和分析。

针对未来的开发，我计划添加以下功能：

1. **自定义规则集**：允许用户根据特定需求，自定义安全检测规则，增强工具的灵活性。

2. **主动防御建议**：在识别出安全问题后，工具将提供修复建议或加固措施，帮助用户修复漏洞。

3. **多维数据分析**：集成更复杂的数据分析模块，如异常检测、行为分析等，以识别更隐蔽的安全威胁。

4. **集成第三方情报**：结合威胁情报平台，实时更新安全威胁数据库，提高威胁检测的时效性。

5. **用户交互界面**：开发友好的用户界面，使得非技术用户也能轻松地使用 AI 辅助渗透测试工具。

6. **大规模并行处理**：优化工具的并行处理能力，使其能够处理大规模网络环境和数据集。

7. **移动应用测试支持**：扩展工具的功能，使其支持移动应用的渗透测试。

8. **云服务集成**：提供云服务接口，允许用户在云端进行安全测试，提高工具的可用性

和便捷性。

9. **合规性检查**：确保渗透测试过程遵守相关法律法规和合规性要求。

通过不断完善和扩展功能，我们的 AI 辅助渗透测试工具将能够提供更全面、更深入的安全分析服务，帮助用户更有效地识别和防御网络威胁。

2.3 设计理念

目的

3 开发环境

3.1 编程语言

Python

3.2 依赖库

- tkinter
- xml
- base64
- openai
- time
- re

3.3 开发工具

Notepad--

4 使用说明

4.1 快速开始

1. 安装工具

Python 3.8 或更高版本

必要的 Python 库（如 tkinter, openai 等）

2. 配置工具

在使用本工具之前，请先将 Burpsuite 的数据包日志进行下载

3. 运行工具

使用命令：`python ai_pentest_tool.py` 运行工具

4. 查看结果

分析结果会以流式形式展示在界面中

5. 结果分析

会对 AI 分析结果进行聚合分析

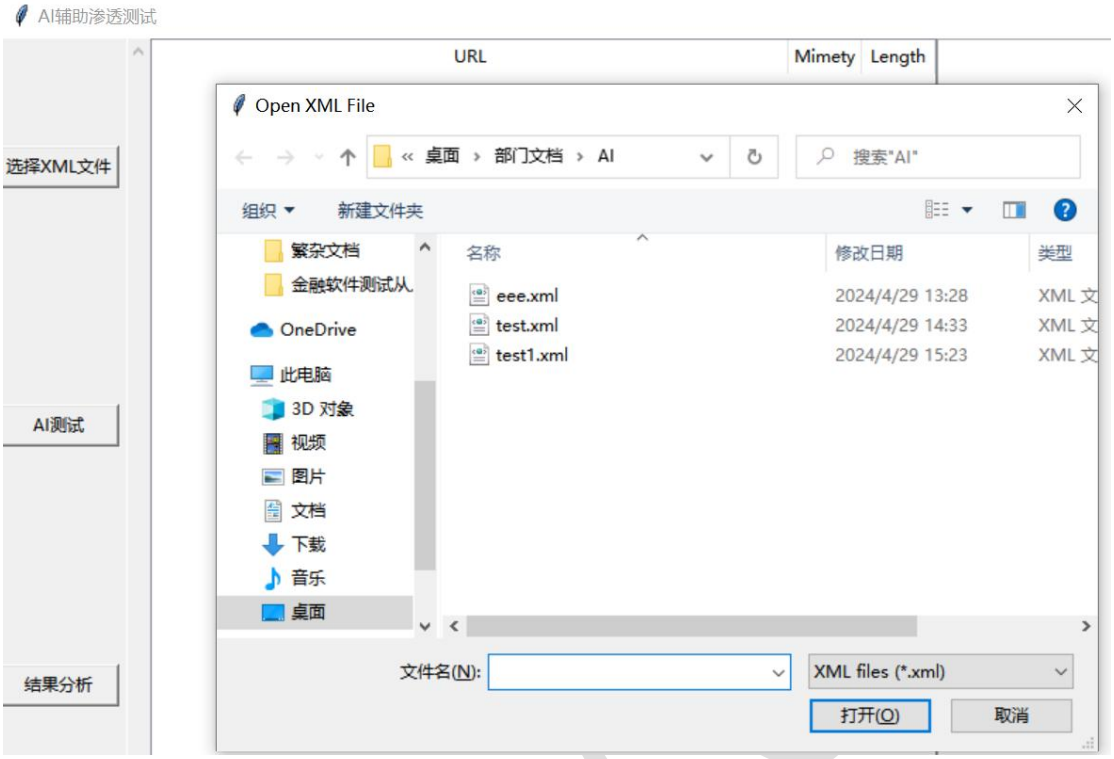
4.2 参数详解

暂无

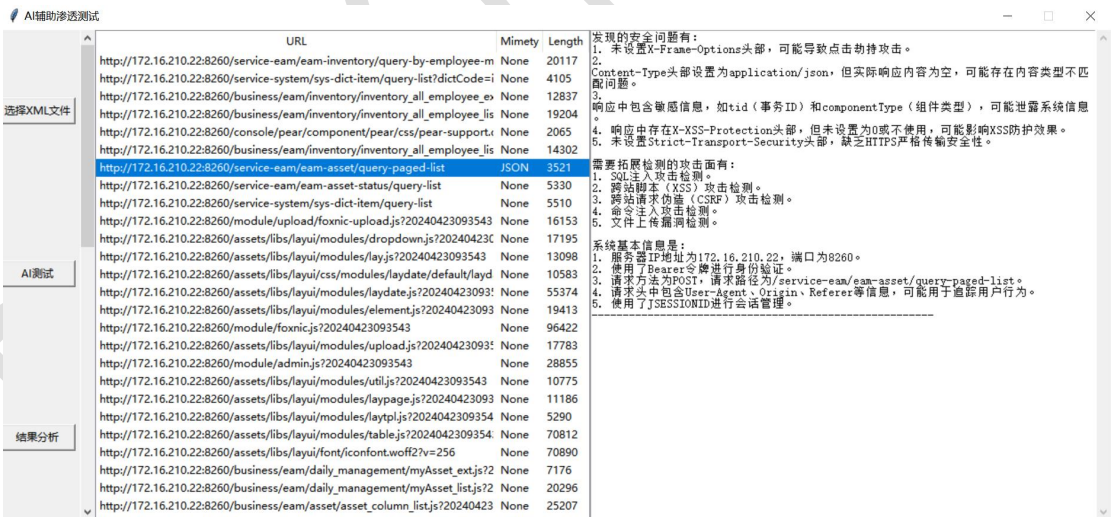
4.3 操作流程

使用命令：`python ai_pentest_tool.py`

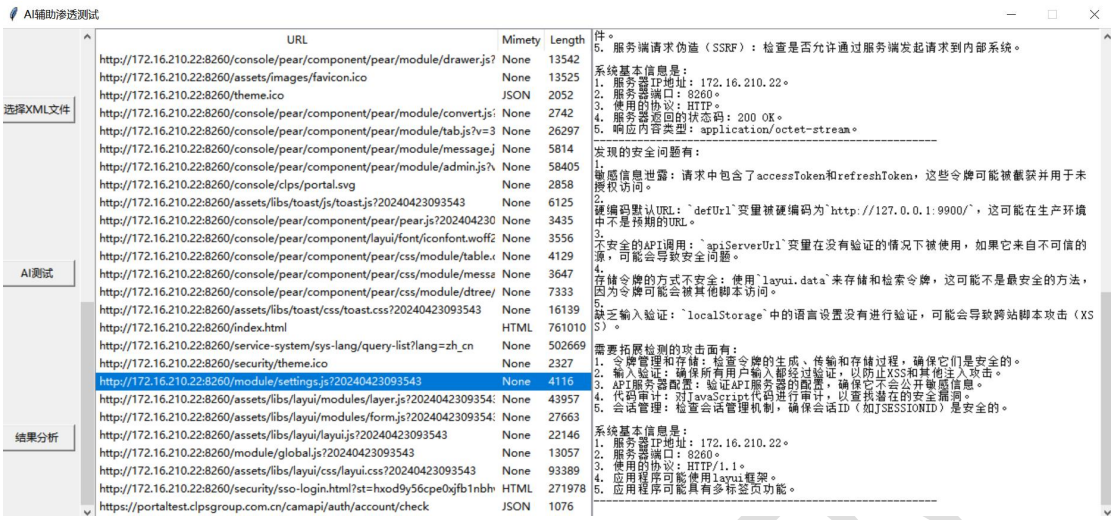
导入 Burpsuite 日志



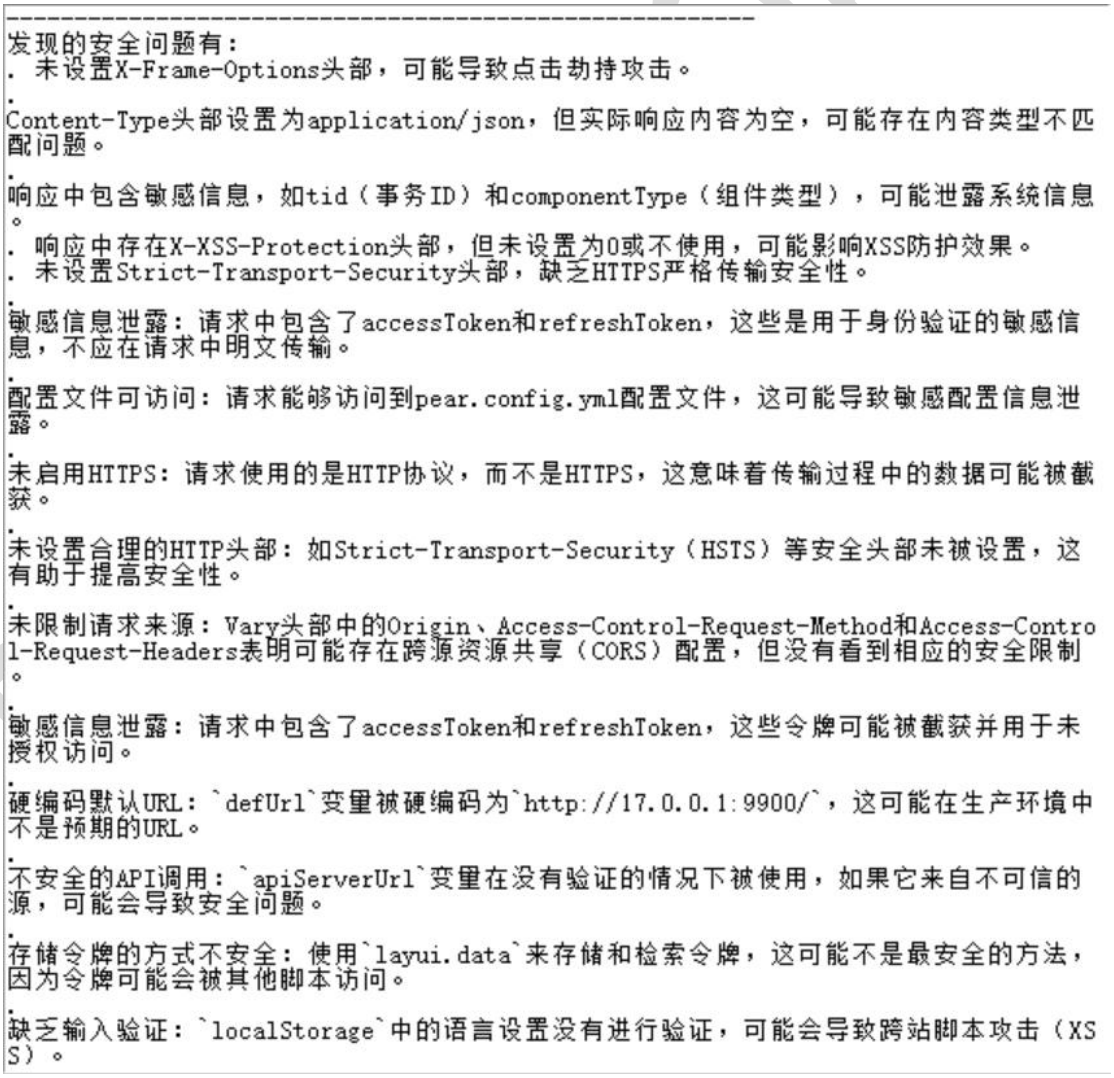
选择特定的链接，再点击“AI 分析”按钮，会自动进行 AI 分析，分析结果会在界面右边流式输出



多个结果可同时呈现在右边界面中



点击“结果分析”可聚合分析多个 ai 分析的结果进行呈现



5 案例分析

5.1 实例演示

以分析[redacted]为例

访问网址，抓取所有的数据包并导出

导入数据包，对经过初步筛选链接进行 AI 辅助测试

URL	Mimety	Length
camapi/auth/login/getSid	None	855
camapi/auth/account/check	None	1004
portal/mob/js/chunk-6001b8e5.f069d58	JSON	4560
portal/mob/js/chunk-505bd9f3.8ac9d03	JSON	9844
portal/mob/js/chunk-70fa09c6.c3b7074f	JSON	13934
portal/mob/js/chunk-vendors.0fddf64f.js	JSON	461621
portal/mob/js/chunk-1e5b0dbc.630075b	JSON	5314
portal/mob/js/app.ae891732.js	None	39802
portal/mob/	HTML	3028
ice-eam/eam-asset/query-list	JSON	3612
ice-eam/eam-asset/query-paged-list	JSON	3905
/pages-index-assetCollection-assetCollec	None	22467
/pages-asset-assetSelection-assetSelecti	None	12942
ice-eam/eam-inventory/query-by-emplo	None	6815
ice-system/sys-dict-item/query-list?dictC	None	4124
/pages-index-assetInventory-assetInvent	None	12825
/pages-index-employeeInventory-emplo	None	9241
/pages-my-myAsset-myAsset.70514bc3.js	None	7226
/pages-asset-assetSelection-assetSelecti	JSON	40819
/pages-employee-myAsset-myAsset~pag	None	12896
rity/sso-login.html?st=vmb30134yxj8qzv	None	171371
/pages-asset-assetSelection-assetSelecti	None	23826
/pages-third-my-my.0990d529.js	None	17292
/pages-asset-assetSelection-assetSelecti	None	16677
/pages-index-report-report~pages-my-r	None	10288
/chunk-vendors.1b8221a2.js	JSON	817195

呈现出所有的分析结果

对结果进行聚合分析，分析结果如下

发现的安全问题有：

. 响应中包含敏感信息：响应中直接显示了错误代码和消息，可能会暴露系统的异常信息，给攻击者提供额外的信息。

. 使用了不安全的 HTTP 连接：在 HTTPS 已经普及的今天，仍然使用 HTTP 连接可能会使得数据在传输过程中被截获或篡改。

. 服务器版本信息泄露：HTTP 响应头中显示了服务器使用的是 nginx/.8.版本，这可能暴露了已知的漏洞信息。

. Cookie 信息泄露：请求中包含了敏感的 Cookie 信息，如 empNo 和 sid，这可能导致会话劫持攻击。

. 不安全的内联脚本：响应内容包含了内联 JavaScript 脚本，这可能允许攻击者执行跨站脚本攻击（XSS）。

. 内容安全策略（CSP）配置不当：CSP 头中设置了 upgrade-insecure-requests，但没有设置更严格的策略，如禁止内联脚本执行。

. 基础 64 编码的图像数据：响应中包含了基础 64 编码的图像数据，这可能被用来隐藏恶意代码。

. 敏感信息泄露：请求中包含了 accessToken 和 refreshToken 等敏感信息，可能存在泄露风险。

. 跨站脚本攻击（XSS）：响应头中设置了 X-XSS-Protection，但没有提供具体的 XSS 防护措施。

. 跨站请求伪造（CSRF）：请求中包含了 JSESSIONID，但没有发现 CSRF 防护措施。

. 内容类型嗅探：响应头中设置了 X-Content-Type-Options: nosniff，但没有提供具体的实现细节。

. 非安全连接：请求是通过 HTTP 协议发送的，而不是 HTTPS，存在中间人攻击风险。

. 响应内容中包含敏感信息：响应中包含了前端的 JavaScript 代码，这可能会暴露应用程序的内部逻辑和实现细节，给攻击者提供可利用的信息。

. 硬编码的 API 路径：请求中包含了硬编码的 API 路径，如果这些路径没有适当的访问控制，可能会被未授权的访问。

. 网站没有启用 HTTPS 协议，存在中间人攻击的风险。

. 网站的服务器使用了较旧的 nginx 版本，可能存在已知的安全漏洞。

. 网站的 ETag 响应头没有使用隐私增强选项 W/，可能会泄露文件的最后修改时间。

. 网站的 Content-Type 为 text/html，但没有使用字符集声明，可能导致跨站脚本攻击。

. 网站的 Referer 头被发送到服务器，可能会泄露用户访问历史。

. 敏感信息泄露：源代码中包含了接口的 URL，可能存在敏感信息泄露的风险。

. 硬编码的接口 URL：接口 URL 直接硬编码在 JavaScript 文件中，不利于接口的管理和更新。

. 缺乏输入验证：在全局请求处理中，对于传入的参数没有进行必要的验证，可能导致注入攻击。

. 密码重置和修改接口存在风险：源代码中包含密码重置和修改的接口，但没有展示相应的安全措施。

. 跨站脚本（XSS）漏洞：在处理错误信息和响应结果时，没有看到对用户输入进行过滤和转义，可能存在 XSS 攻击的风险。

. URL 中的参数可能存在注入风险。

. HTTP 响应头中的 ETag 可能泄露文件信息。

. 网站使用了 HTTP 而不是 HTTPS，存在中间人攻击风险。

. 网站的 Content-Type 为 text/html,但没有设置 X-Content-Type-Options 为 nosniff，可能导致 MIME 类型混淆攻击。

. 网站的脚本文件可能存在跨站脚本（XSS）漏洞。

. 未对请求参数进行过滤和验证，可能存在注入攻击的风险。

. 响应中包含敏感信息,如服务器版本和组件信息,这可能帮助攻击者进行针对性攻击。

. Access-Control-Allow-Origin: * 配置过于宽松，可能导致跨域资源共享（CORS）攻击。

. 连接使用 close，可能存在会话固定攻击的风险。

. 未对请求来源进行限制，可能存在请求伪造攻击的风险。

. 服务器使用了较旧的 Nginx 版本（.8.），可能存在已知的安全漏洞。

. Cookie 中包含了敏感信息（如 empNo），这可能导致会话劫持攻击。

. Content-Security-Policy 仅设置了 upgrade-insecure-requests，安全策略不够全面。

需要拓展检测的攻击面有：

. 会话管理：检查系统的会话管理机制，如是否存在会话固定攻击、会话超时设置是否合理等。

. 输入验证：检查系统是否对输入进行了充分的验证，以防止 SQL 注入、跨站脚本攻击等。

. 错误处理：检查系统的错误处理机制，确保不会泄露敏感信息。

. 跨站请求伪造（CSRF）：检查系统是否采取了足够的措施来防止 CSRF 攻击。

. 跨站脚本（XSS）：检查系统是否对输出进行了编码或过滤，以防止 XSS 攻击。

. 会话管理：检查是否存在会话固定或会话劫持的漏洞。

. 输入验证：检查所有用户输入点，确保没有 SQL 注入、命令注入等漏洞。

. 跨站脚本（XSS）：检查所有用户输入输出点，确保没有 XSS 漏洞。

. 跨站请求伪造（CSRF）：检查是否有 CSRF 保护措施。

. 不安全的直接对象引用（IDOR）：检查是否有直接对象引用的安全问题。

. SQL 注入：检查输入参数是否可能导致 SQL 注入攻击。

. 命令注入：检查输入参数是否可能导致命令注入攻击。
. 文件上传漏洞：检查是否有文件上传功能，以及其安全性。
. 服务端请求伪造（SSRF）：检查是否允许对外发起请求，以及其安全性。
. 访问控制：检查 API 的访问控制机制，是否存在未授权访问的风险。
. API 访问控制：检查 API 路径是否有适当的访问控制，以防止未授权的访问。
. 敏感信息泄露：检查响应内容，确保没有泄露敏感信息，如数据库结构、内部配置等。
. 输入验证：检查前端和后端的输入验证机制，确保没有 SQL 注入、XSS 等安全漏洞。
. 跨站脚本攻击（XSS）：检查前端 JavaScript 代码，确保没有 XSS 漏洞。
. 跨站请求伪造（CSRF）：检查应用程序是否有 CSRF 保护机制。
. 对 HTTPS 协议的强制使用进行测试，以确保数据传输的安全性。
. 对 nginx 服务器的版本进行升级，以修复可能存在的安全漏洞。
. 对 ETag 响应头的使用进行优化，避免泄露敏感信息。
. 对 Content-Type 响应头的字符集声明进行测试，以防止跨站脚本攻击。
. 对 Referer 头的发送进行控制，以保护用户隐私。
. SQL 注入攻击：检查接口是否对输入进行了充分的过滤和转义，防止 SQL 注入。
. 跨站请求伪造（CSRF）：验证应用是否有足够的机制来防止 CSRF 攻击。
. 跨站脚本（XSS）：检查应用是否对用户输入进行了适当的处理，以防止 XSS 攻击。
. 暴力破解：验证密码重置和修改接口是否有限制尝试次数的措施，以防止暴力破解。
. 信息泄露：检查应用是否在前端或后端泄露了敏感的系统信息。
. SQL 注入攻击。
. 文件上传漏洞。
. 跨站脚本（XSS）攻击。
. 跨站请求伪造（CSRF）攻击。
. 会话管理不当。
. SQL 注入攻击检测。
. 跨站脚本（XSS）攻击检测。
. 跨站请求伪造（CSRF）攻击检测。
. 服务器端请求伪造（SSRF）攻击检测。
. 会话管理机制的安全性检测。
. 对 Nginx 服务器进行版本升级和安全补丁更新。
. 检查和改进 Cookie 的安全设置，如使用 Secure 和 HttpOnly 标记。
. 增强 Content-Security-Policy，设置更严格的策略以减少 XSS 和其他注入攻击的风险。
. 验证服务器配置，确保没有不必要的服务运行或开放。
. 检查应用程序的输入验证和输出编码，防止注入攻击。

系统基本信息是：
. 服务器使用了 nginx/.8.版本，这是一个较旧的版本，可能存在已知的安全漏洞。
. 系统使用了 HTTP 协议，而不是更安全的 HTTPS。
. 服务器返回了 401 错误码，表示 token 过期或无效。
. 响应中包含了 Access-Control-Allow-Origin 和 Access-Control-Allow-Credentials 头部，这可能表明系统支持跨源资源共享（CORS）。
. 用户代理为 Chrome/114.0.73.110，表明请求来自一个较新的 Chrome 浏览器。
. 服务器：nginx/.8.

. 响应内容类型：application/javascript
. 响应内容长度：4268 字节
. 响应中包含内联 JavaScript 脚本
. 使用了基础 64 编码的图像数据
. 服务器：使用 nginx/.20.2 作为服务器。
. 编程语言：使用 Java 语言进行开发。
. 数据库：使用 MySQL 数据库。
. 框架：使用 Spring 框架进行开发。
. 容器：使用 Docker 进行部署。
. 使用的服务器软件：nginx/.20.2。
. 响应内容类型：application/javascript。
. 响应内容长度：7478 字节。
. 页面最后修改时间：Fri, 15 Mar 202 06:23:0 GMT。
. 客户端使用的浏览器：Mozilla/.0 (Windows NT 10.0; Win64; x64) AppleWebKit/37.36 (KHTML, like Gecko) Chrome/114.0.73.110 Safari/37.36。
. 网站的域名为 amstest.clps.com.cn。
. 网站使用的服务器软件为 nginx/1.0.。
. 网站的首页返回了 200 OK 的状态码。
. 网站的首页内容类型为 text/html。
. 网站的首页内容长度为 97 字节。
. 使用 AngularJS 框架开发的前端应用程序。
. 应用程序部署在 IP 地址为 17.16.10.93 的服务器上，端口为 8080。
. 应用程序包含登录、薪资、考勤等多个模块。
. 应用程序使用 localStorage 和 sessionStorage 进行数据存储。
. 应用程序支持国际化，使用了 i18n 进行本地化处理。
. 服务器 IP 地址：72.6.20.93。
. 服务器端口：8080。
. 使用了 AngularJS 框架。
. 使用了 jQuery 库。
. 网站标题为"EWQS-薪资查询系统"。
. 服务器使用了 Apache-Coyote/.。
. 响应头中包含了 Access-Control-Allow-Origin: *，表明服务器对跨域请求的处理策略。
. 使用了 HTTP/1.1 协议。
. 响应内容类型为 application/json;charset=UTF-8。
. 服务器返回了 200 OK 状态码，表示请求处理成功。
. 服务器软件：Nginx/.8.
. 服务器域名：
. 响应状态码：04 Not Modified
. 用户代理：Mozilla/5.0 (Windows NT 10.0; Win6; x6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/11.0.5735.110 Safari/537.36
. 支持的响应压缩类型：gzip, deflate

目前可帮助测试人员对系统信息，攻击拓展面以及可能的漏洞进行较为深入的分析

5.2 问题与解决

1. **数据包捕获不完整**

问题描述：在使用工具进行网站数据包分析时，发现捕获的数据包不完整，导致 AI 分析不准确。

期望解决措施：

确认网络连接稳定，检查是否有网络丢包现象。

调整数据包捕获工具的缓冲区大小，以适应高流量场景。

使用更高效的数据包捕获库，如 Scapy 的高级功能。

2. **AI 模型训练数据不足**

问题描述：AI 模型表现不佳，可能是因为训练数据不足或质量不高。

期望解决措施：

收集更多的数据包样本，包括正常流量和攻击流量。

使用数据增强技术，如添加噪声、变速等，来扩充训练集。

采用迁移学习，利用预训练模型作为起点，减少所需训练数据。

3. **工具运行缓慢**

问题描述：在处理大规模数据集时，工具的运行速度明显下降。

期望解决措施：

对代码进行性能分析，找出瓶颈并优化。

使用并行处理或多线程技术来加速数据处理。

在硬件资源允许的情况下，增加 CPU 核心数或内存。

4. **报告生成失败**

问题描述：在分析完成后，工具无法生成或保存分析报告。

期望解决措施：

检查文件系统权限，确保工具有权限写入报告。

验证报告生成模块的逻辑，确保所有必要的数据都被正确处理。

使用异常处理机制，确保在遇到错误时能够给出明确的错误信息。

5. **工具与某些网站不兼容**

问题描述：工具在分析某些特定网站时出现异常，无法正常工作。

解决措施：

分析网站的特性，如使用了特殊的编码或协议。

更新工具以支持这些特性，或为这些网站添加特定的分析规则。

提供用户自定义规则的功能，允许用户根据需要调整分析参数。

6. **用户界面不友好**

问题描述：用户反映工具的用户界面不够直观，难以上手。

期望解决措施：

设计更直观的用户界面，提供清晰的指示和帮助文档。

收集用户反馈，根据用户习惯调整界面布局和操作流程。

提供交互式教程，引导用户完成常见任务。

7. **缺少高级功能**

问题描述：用户需要更高级的分析功能，如自定义规则集或多维数据分析。

期望解决措施：

开发插件系统，允许第三方开发者贡献新的功能。

根据用户反馈，优先开发最需要的高级特性。

定期与用户沟通，了解他们的需求，并据此规划新功能。

通过持续的问题追踪和解决，AI 辅助渗透测试工具能够不断改进，更好地满足用户的需求。

6 附录

暂无