**广州科技职业技术大学**

**Guangzhou Vocational and Technical University of Science and Technology**

**毕业设计说明书**

**题 目： 基于Python的自动化SQL注**

**入工具系统设计与实验**

**学 生 姓 名 ： 李泽乾**

**专 业 班 级 ： 19级计算机应用工程5班**

**所 在 学 院 ： 信息工程学院**

**指 导 老 师 ： 梁衬章**

**完 成 时 间 ： 2023年5月4日**

**教务处制**

**毕业设计（论文）独创性承诺**

本人所提交的毕业设计（论文） 基于Python的自动化SQL注入工具系统设计与实验，是在导师的指导下，独立进行研究工作所取得的原创性成果。除文中已经注明引用的内容外，不包含任何其他个人或集体已经发表或撰写过的研究成果。对本文的研究做出重要贡献的个人和集体，均已在文中标明。本声明的法律后果由本人承担。

作者（签名）： 李泽乾 指导教师确认（签名）：

2023年 5 月 4 日 年 月 日

**毕业设计（论文）版权使用授权书**

本毕业设计（论文）作者完全了解 有权保留并向国家有关部门或机构送交学位论文的复印件和磁盘，允许论文被查阅和借阅。本人授权广州科技职业技术大学可以将此学位论文的全部或部分内容编入有关数据库进行检索，可以采用影印、缩印或其它复制手段保存、汇编学位论文。保密的学位论文在\_\_\_\_\_\_\_年解密后适用本授权书。

作者（签名）： 指导教师（签名）：

年 月 日 年 月 日

**摘 要**

SQL注入攻击是一种常见的网络攻击手段，它可以利用Web应用程序中的SQL语句漏洞，执行恶意的SQL命令，从而窃取或破坏数据库中的数据。为了有效地防御和检测SQL注入攻击，本文设计并实现了一种基于Python的自动化SQL注入工具系统，该系统可以自动识别目标网站的数据库类型、参数个数、注入点位置等信息，然后根据不同的攻击类型和技术，生成并发送相应的SQL注入语句，最后获取并分析返回的结果，实现对目标网站的信息收集、数据库枚举、数据提取等操作。本文采用Python语言作为开发工具，利用其简洁、高效、跨平台等特点，实现了系统的各个功能模块，并采用面向对象的编程思想，提高了系统的可扩展性和可维护性。本文在虚拟机中搭建了不同类型的数据库服务器，并使用本系统对其进行了测试和评估，结果表明，本系统能够成功地完成SQL注入攻击，并具有较高的准确率和效率。本文为网络安全领域提供了一种新的SQL注入工具系统，同时也为网络安全教学和研究提供了一种有用的实验平台。

**关键词**：SQL注入；python；自动化

**Abstract**

SQL injection attack is a common cyber attack that can exploit SQL statement vulnerabilities in web applications to execute malicious SQL commands, thus stealing or corrupting data in databases. In order to effectively defend and detect SQL injection attacks, this paper designs and implements a Python-based automated SQL injection tool system, which can automatically identify the database type, number of parameters, injection point location and other information of a target website, then generate and send corresponding SQL injection statements according to different attack types and techniques, and finally obtain and analyze the returned results to achieve The result will be obtained and analyzed to achieve information collection, database enumeration, data extraction and other operations on the target website. In this paper, we use Python language as the development tool to implement various functional modules of the system by using its features of simplicity, efficiency and cross-platform, and adopt object-oriented programming ideas to improve the scalability and maintainability of the system. In this paper, different types of database servers are built in virtual machines and tested and evaluated using this system, and the results show that the system can successfully complete SQL injection attacks with high accuracy and efficiency. This paper provides a new system of SQL injection tools for the field of network security, and also provides a useful experimental platform for network security teaching and research.

**Key words：**SQL injection; python; automation

**目 录**

目录

[毕业设计说明书 1](#_Toc21999)

[1 系统分析 8](#_Toc21063)

[1.1 背景 8](#_Toc15563)

[1.2 国内外研究 8](#_Toc17799)

[2 系统开发平台 9](#_Toc23977)

[2.1 DVWA 9](#_Toc7347)

[2.1.1 DVWA概念 9](#_Toc11761)

[2.1.2 DVWA搭建 9](#_Toc8469)

[2.2 docker 9](#_Toc23874)

[2.3 python 9](#_Toc2397)

[2.4 PyQt 10](#_Toc16084)

[2.5 Pycharm 10](#_Toc7691)

[2.6 VIM 10](#_Toc15041)

[2.7 系统的目标 10](#_Toc18943)

[3 需求分析 11](#_Toc28369)

[4 关键技术分析 12](#_Toc16548)

[4.1  SQL 注入攻击 12](#_Toc8836)

[4.1.1 SQL注入攻击概念 12](#_Toc28238)

[4.1.2 SQL注入攻击的定义和原理 12](#_Toc4191)

[4.1.3 SQL注入攻击的类型 13](#_Toc19660)

[4.1.4 SQL注入攻击的危害 13](#_Toc22230)

[4.1.5 SQL注入攻击的防范措施 14](#_Toc17719)

[4.1.6 SQL注入攻击的检测工具 14](#_Toc13635)

[4.2 自动化 SQL 注入工具的概念 15](#_Toc20869)

[4.3 SQL 注入漏洞检测技术 16](#_Toc7620)

[4.3.1 基于错误信息的利用技术 16](#_Toc25449)

[4.3.2 基于时间延迟的利用技术 16](#_Toc11011)

[4.3.3 基于联合查询的利用技术 16](#_Toc905)

[4.3.4 基于堆叠查询的利用技术 16](#_Toc16684)

[4.4 SQL 注入漏洞利用技术 16](#_Toc29459)

[4.5 SQL注入防御技术 17](#_Toc7068)

[4.6 PyQT 17](#_Toc11056)

[4.6.1 信号和槽机制 17](#_Toc21782)

[4.6.2 布局管理器 17](#_Toc12527)

[4.6.3 事件处理 18](#_Toc9847)

[4.7  机器学习 18](#_Toc10645)

[4.7.1 决策树 19](#_Toc14407)

[4.7.2 朴素贝叶斯 20](#_Toc14975)

[4.7.3 支持向量机 20](#_Toc1434)

[4.7.4 随机森林 21](#_Toc22772)

[4.7.5 机器学习在恶意流量检测中的应用 21](#_Toc788)

[4.7.6 恶意流量 22](#_Toc4503)

[4.7.7 基于统计学习的算法 23](#_Toc4892)

[4.7.8 基于深度学习的算法 23](#_Toc19543)

[5 系统设计 24](#_Toc22645)

[5.1 系统架构设计 24](#_Toc31003)

[5.2 系统算法 25](#_Toc17115)

[5.3 流程图 26](#_Toc12914)

[6 环境信息 29](#_Toc19802)

[4.1硬件资源 29](#_Toc3850)

[4.2软件资源 30](#_Toc25713)

[8. 结论与展望 30](#_Toc24523)

[9. 结束语 30](#_Toc23106)

[10. 源代码 31](#_Toc18363)

[10.1 图形界面 31](#_Toc16739)

[10.2 程序逻辑 33](#_Toc17438)

[参考资料 35](#_Toc2825)

# 1 系统分析

## 1.1 背景

随着互联网的发展，Web应用系统越来越广泛地应用于各个领域，为人们的生活和工作带来了便利。然而，Web应用系统也面临着各种网络安全威胁，其中SQL注入攻击是一种常见的网络攻击手段，它可以利用Web应用程序中的SQL语句漏洞，执行恶意的SQL命令，从而窃取或破坏数据库中的数据。SQL注入攻击不仅危害了数据的完整性、机密性和可用性，也威胁了用户的隐私和安全。因此，防御和检测SQL注入攻击是网络安全领域的一个重要课题。

SQL注入是一种常见的网络攻击手段，可以利用数据库的漏洞获取敏感信息或执行恶意操作。为了防御SQL注入攻击，需要对网站的输入参数进行有效的检测和过滤。本文设计并实现了一种基于Python的自动化SQL注入工具，可以对目标网站进行快速、准确和深入的SQL注入检测，并提供相应的攻击载荷和利用方法。本文首先介绍了SQL注入的原理和分类，然后分析了国内外常用的SQL注入工具的特点和不足，接着详细描述了本文设计的自动化SQL注入工具的系统架构、功能模块、算法实现和界面设计，最后通过实验验证了本文设计的工具的有效性、性能和安全性，并与其他工具进行了对比分析。本文的研究成果可以为网络安全领域提供一种SQL注入检测和利用工具，同时也为进一步完善和优化该工具提供了参考和指导。

## 1.2 国内外研究

国内外对SQL注入攻击的防御和检测技术有了一定的研究，主要分为静态分析和动态检测两类。静态分析是在Web应用程序开发阶段，通过对源代码或字节码进行扫描和分析，找出可能存在的SQL注入漏洞，并给出修复建议。动态检测是在Web应用程序运行阶段，通过对用户输入或SQL语句进行验证和过滤，阻止恶意的SQL注入语句执行。静态分析和动态检测各有优缺点，一般需要结合使用，以提高检测的准确性和效率。此外，还有一些基于机器学习的技术，利用数据挖掘、自然语言处理、神经网络等方法，对SQL语句进行分类和识别，判断是否为SQL注入攻击。这些技术具有一定的创新性和潜力，但也需要进一步的改进和验证。

# 2 系统开发平台

## 2.1 DVWA

### **2.1.1 DVWA概念**

DVWA是一个用来进行安全脆弱性鉴定的PHP/MySQL Web 应用，旨在为安全专业人员测试自己的专业技能和工具提供合法的环境，帮助web开发者更好的理解web应用安全防范的过程。DVWA是一个开源的项目，可以在GitHub上下载和安装。DVWA包含了多种常见的web攻击类型，如SQL注入、XSS、CSRF、文件上传、文件包含等，可以用来练习和学习web安全的知识和技巧。

### **2.1.2 DVWA搭建**

从docker仓库中搜索DVWA镜像，命令如下：docker search dvwa

从搜索结果中选择一个合适的镜像，如vulnerables/web-dvwa1，并拉取到本地，命令如下：docker pull vulnerables/web-dvwa

运行这个镜像，指定端口映射，命令如下：docker run --rm -it -p 80:80 vulnerables/web-dvwa1

访问本地的80端口，即可看到DVWA的界面，输入默认的用户名和密码（admin/password）进行登录。

## 2.2 docker

Docker是一个开源的应用容器引擎，让开发者可以打包他们的应用以及依赖包到一个可移植的容器中，然后发布到任何流行的 Linux 或 Windows 操作系统的机器上，也可以实现虚拟化。容器是完全使用沙箱机制，相互之间不会有任何接口。Docker可以让你的应用在任何环境都有一致的表现，而不受操作系统的影响。Docker还可以让你更方便地管理你的基础设施和应用。

## 2.3 python

Python是一种解释型、高级和通用的编程语言，支持多种编程范型，包括面向对象、函数式、过程式等。Python由Guido van Rossum创造，第一版发布于1991年。Python的设计具有很强的可读性，使用英文关键字和缩进来组织代码。Python也有丰富的标准库和第三方库，可以方便地实现各种功能。

## 2.4 PyQt

PyQt是一个创建Python GUI应用程序的工具包，是Qt和Python结合的一个产物。PyQt提供了一套控制界面显示和数据存储分离以及映射的机制，称为Model/View架构。PyQt还提供了一个图形界面编辑的工具，叫做Qt Designer，可以方便地设计和预览GUI界面。

## 2.5 Pycharm

PyCharm是一种Python IDE，带有一整套可以帮助用户在使用Python语言开发时提高其效率的工具。PyCharm具有智能代码编辑器，能理解Python的特性并提供卓越的生产力推进工具，比如自动代码格式化、代码完成、重构、自动导入和一键代码导航等。PyCharm还支持Django框架、版本控制、单元测试等功能。

## 2.6 VIM

Vim是一个类似于Vi的著名的功能强大、高度可定制的文本编辑器[。Vim的设计理念是命令的组合，用户可以灵活地使用各种文本间移动/跳转的命令和其他的编辑命令，比那些没有模式的编辑器更加高效地进行文本编辑](https://baike.baidu.com/item/VIM/60410" \t "https://www.bing.com/_blank)。Vim还具有程序编辑的能力，可以主动地以字体颜色辨别语法的正确性，方便程序设计。

## 2.7 系统的目标

该系统的目标是实现一个自动化的SQL注入扫描和利用工具，可以帮助用户发现和利用目标网站的SQL注入漏洞，以获取或修改数据库的数据或权限，或者执行任意SQL语句。该系统可以用于安全测试、渗透测试、教学演示等目的。

SQL注入是一种常见的网络攻击技术，它利用了目标网站对用户输入的不充分过滤或转义，导致用户输入的数据被当作SQL语句的一部分执行，从而影响数据库的正常操作。SQL注入可以使攻击者获取数据库的结构、内容或权限，或者执行任意SQL语句，如删除数据、修改数据、创建用户等。SQL注入对网站的安全性和功能性构成了严重的威胁，因此需要及时地发现和修复。

它可以帮助用户发现和利用目标网站的SQL注入漏洞，以达到以下目标：

安全测试：用户可以使用该系统对自己的网站或应用进行安全测试，检查是否存在SQL注入漏洞，以及漏洞的严重程度和影响范围，从而及时地修复漏洞，提高网站或应用的安全性。

渗透测试：用户可以使用该系统对他人的网站或应用进行渗透测试，探测是否存在SQL注入漏洞，以及漏洞的利用方式和效果，从而评估网站或应用的安全性，或者获取有价值的信息或权限。

教学演示：用户可以使用该系统对教学案例或实验环境进行教学演示，展示SQL注入的原理、方法和后果，从而增强学生的安全意识和技能。

该系统可以根据用户输入的网址或域名，自动地发现目标网站的所有链接，并对每个链接进行SQL注入测试，以确定是否存在SQL注入漏洞。该系统可以根据用户选择的利用方式，自动地构造合适的攻击载荷，并发送给目标网站，以获取数据库的结构、内容或权限，或者执行任意SQL语句。该系统可以以图形化或文本化的方式展示扫描和利用的过程和结果，让用户清楚地了解每个步骤的细节和效果。该系统可以支持不同类型和版本的数据库和SQL语言，如MySQL、Oracle、SQL Server等。该系统可以支持不同类型的请求和响应，如GET、POST、COOKIE等，以及不同类型的编码和错误，如URL编码、Base64编码等。该系统可以运行在任何支持Python语言和相关库或工具的操作系统上，如Windows、Linux、Mac OS等。该系统可以部署在用户自己的设备上，如个人电脑、手机等，也可以部署在云端服务器上，如AWS、Azure等。

# 3 需求分析

用户需求：系统的目标用户是需要进行SQL注入攻击的安全测试人员或黑客，他们需要系统能够自动地检测目标网站的SQL注入漏洞，以及利用漏洞获取敏感信息或执行恶意操作。

功能需求：系统的主要功能包括：

目标网站扫描：系统能够根据用户输入的网址或域名，自动地发现目标网站的所有链接，并对每个链接进行SQL注入测试，以确定是否存在SQL注入漏洞。

漏洞利用：系统能够根据不同类型的SQL注入漏洞，自动地构造合适的攻击载荷，并发送给目标网站，以获取数据库的结构、内容或权限，或者执行任意SQL语句。

结果展示：系统能够将扫描和利用的过程和结果，以图形化或文本化的方式展示给用户，包括漏洞的位置、类型、严重程度和影响范围，以及获取或修改的数据或操作。

非功能需求：系统的主要非功能需求包括：

性能：系统能够快速地完成扫描和利用的任务，尽量减少对目标网站的影响和干扰。

安全：系统能够保护自身和用户的安全，避免被目标网站或第三方检测或追踪。

可用：系统能够适应不同的网络环境和操作系统，提供友好的用户界面和操作指引。

可扩展：系统能够支持不同类型和版本的数据库和SQL语言，以及不断更新的攻击技术和防御措施。

约束条件和假设：系统的主要约束条件和假设包括：

约束条件：系统需要使用Python语言开发，以保证跨平台性和易维护性；系统需要使用开源或免费的第三方库或工具，以降低开发成本和版权风险；系统需要遵守相关的法律法规和道德规范，以避免造成不必要的损害和责任。

假设：系统假设目标网站使用了常见的数据库和SQL语言，并且没有采取有效的防御措施；系统假设用户具有一定的SQL注入知识和经验，并且使用系统时有明确的目的和合理的范围。

# 4 关键技术分析

## 4.1  SQL 注入攻击

### **4.1.1 SQL注入攻击概念**

SQL注入攻击是指web应用程序对用户输入数据的合法性没有判断或过滤不严，攻击者可以在web应用程序中事先定义好的查询语句的结尾上添加额外的SQL语句，在管理员不知情的情况下实现非法操作，以此来实现欺骗数据库服务器执行非授权的任意查询，从而进一步得到相应的数据信息。

### **4.1.2 SQL注入攻击的定义和原理**

SQL注入攻击是一种常见的网络攻击方式之一，它不是利用操作系统的BUG来实现攻击，而是针对程序员编写时的疏忽，通过SQL语句，实现无账号登录，甚至篡改数据库。

SQL注入攻击指的是通过构建特殊的输入作为参数传入Web应用程序，而这些输入大都是SQL语法里的一些组合，通过执行SQL语句进而执行攻击者所要的操作，其主要原因是程序没有细致地过滤用户输入的数据，致使非法数据侵入系统。

寻找到SQL注入的位置、判断服务器类型和后台数据库类型、针对不同的服务器和数据库特点进行SQL注入攻击是SQL注入攻击的总体思路。

### **4.1.3 SQL注入攻击的类型**

SQL注入攻击的类型大致分为数字型注入和字符型注入两类。

数字型注入：是指攻击者通过输入数字来实现SQL注入的方式。

字符型注入：是指攻击者通过输入字符来实现SQL注入的方式。

此外，按照注入方式可以分为联合注入、布尔盲注、时间盲注、堆叠注入以及报错注入等五种注入方式。

### **4.1.3.1 联合注入**

联合注入是一种SQL注入的方式，它是通过将两个或多个SELECT语句的结果合并成一个结果集来实现的。

联合注入的基本原理是：在SQL语句中使用UNION关键字，将两个或多个SELECT语句的结果合并成一个结果集。攻击者可以通过构造恶意的SQL语句，将自己的SQL语句注入到原始SQL语句中，从而实现对数据库的攻击。

### **4.1.3.2 布尔盲注**

布尔盲注是一种SQL注入的方式，它是通过构造恶意的SQL语句，利用and，or等关键字来其后的语句 true 、 false使web页面返回true或者false，从而达到注入的目的来获取信息的一种方法。

布尔盲注的基本原理是：在SQL语句中使用and、or等关键字，将自己的SQL语句注入到原始SQL语句中，从而实现对数据库的攻击。

### **4.1.3.3 时间盲注**

时间盲注是一种SQL注入的方式，它是通过制造时间延迟，由回显时间来判断是否报错，从而实现对数据库的攻击。

### **4.1.4 SQL注入攻击的危害**

盗取用户数据和隐私，这些数据被打包贩卖，或用于非法目的后，轻则损害企业品牌形象，重则将面临法律法规风险。

攻击者可对目标数据库进行“增删改查”，一旦攻击者删库，企业整个业务将陷于瘫痪，极难恢复。

植入网页木马程序，对网页进行篡改，发布一些违法犯罪信息。

攻击者添加管理员帐号。 即便漏洞被修复，如果企业未及时察觉账号被添加，则攻击者可通过管理员帐号，进入网站后台。

### **4.1.5 SQL注入攻击的防范措施**

不要使用动态SQL,避免将用户提供的输入直接放入sql语句中；最好使用准备好的语句和参数化查询（pdo预处理），这样更安全；

限制数据库权限和特权,将数据库用户的功能设置为最低要求；这将限制攻击者在设法获取访问权限时可以执行的操作；

避免直接向用户显示数据库错误。攻击者可以使用这些错误消息来获取有关数据库的信息；

对访问数据库的Web应用程序使用Web应用程序防火墙（WAF）。这为面向Web的应用程序提供了保护，它可以帮助识别SQL注入尝试；根据设置，它还可以帮助防止SQL注入尝试到达应用程序（以及数据库）。

### **4.1.6 SQL注入攻击的检测工具**

SQL 注入漏洞检测技术包括但不限于以下几种：

其中，基于规则的检测技术是最常用的一种技术，它通过预定义的规则来检测 SQL 注入漏洞。基于语法分析和语义分析的检测技术则是通过对 SQL 语句进行分析来检测 SQL 注入漏洞。基于机器学习的检测技术则是通过机器学习算法来自动学习 SQL 注入漏洞的特征，从而实现自动化检测。

### **4.1.6.1基于规则的检测技术**

基于规则的检测技术是一种常见的漏洞检测方法，它由专家针对各类漏洞人工分析生成漏洞规则，在词法语法解析基础上，对源代码建模，进行数据流分析、污点分析等。

### **4.1.6.2 基于语法分析的检测技术**

基于语法分析的检测技术是一种常见的漏洞检测方法，它的基本任务是确定句子的语法结构或句子中词汇之间的依存关系。 句法分析不是一个自然语言处理任务的最终目标，但它往往是实现最终目标的关键环节。

### **4.1.6.4 基于语义分析的检测技术**

基于语义分析的检测技术是一种常见的漏洞检测方法，它通过对文件进行语法分析，得到代码的行为节点和相关依存关系，并通过风险模型匹配实现语义理解从而完成Webshell检测。自然语言处理技术的核心为语义分析。语义分析是一种基于自然语言进行语义信息分析的方法，不仅进行词法分析和句法分析这类语法水平上的分析，而且还涉及单词、词组、句子、段落所包含的意义，目的是用句子的语义结构来表示语言的结构。为了实现基于语法分析的检测技术，您需要使用解析器来分析代码并识别任何语法错误或可疑模式。其中一种流行的解析器是抽象语法树（AST）解析器。

要使用AST解析器，您需要首先安装诸如JavaScript的esprima或Python的ast等软件包。安装后，您可以使用解析器从代码生成AST，然后遍历AST以识别任何可疑模式。

### **4.1.6.5 基于机器学习的检测技术**

使用机器学习进行SQL注入漏洞检测是一种常见的方法，可以有效地检测SQL注入攻击。其中，采用特征工程+机器学习方法的方法，采用统计型等特征提取方式去进行特征工程，之后训练机器学习的各种分类器或集成学习模型，并对真实数据流中是否存在SQL注入攻击进行检测,需要从输入数据中提取特征，以区分合法和恶意的SQL查询。用于此目的的一些常见特征包括查询的长度、使用的特殊字符数量以及是否存在某些关键字，如“SELECT”或“DROP”。

提取特征后，您可以使用它们来训练分类算法，如逻辑回归或支持向量机（SVM）。然后，可以使用算法根据其特征值将新查询分类为合法或恶意。

以下是使用Python和scikit-learn实现逻辑回归分类器进行SQL注入检测的实例：

这段代码加载包含SQL查询及其相应标签（合法或恶意）的数据集，从查询中提取特征和标签，将数据拆分为训练和测试集，对训练集进行逻辑回归分类器的训练，并在测试集上评估分类器。

请注意，基于机器学习的检测技术并不是万无一失的，可能会产生误报或错过某些类型的攻击。使用其他技术，如输入验证和输出编码，提供额外的安全层是非常重要的。

## 4.2 自动化 SQL 注入工具的概念

自动化SQL注入工具是一种可以自动检测和利用SQL注入漏洞并接管数据库服务器的工具。其中，sqlmap是一个开源的渗透测试工具，可以用来自动化地检测和利用SQL注入漏洞。

## 4.3 SQL 注入漏洞检测技术

### 4.3.1 基于错误信息的利用技术

基于错误信息的利用技术是一种常见的 SQL 注入攻击技术，它通过向数据库发送恶意 SQL 语句来触发错误信息，从而获取敏感信息。攻击者可以通过构造特定的 SQL 语句来触发数据库返回错误信息，从而获取敏感信息。例如，攻击者可以通过构造一个包含错误语法的 SQL 语句来触发数据库返回错误信息，从而获取敏感信息。

### 4.3.2 基于时间延迟的利用技术

基于时间延迟的利用技术是一种常见的 SQL 注入攻击技术，它通过向数据库发送恶意 SQL 语句来触发时间延迟，从而获取敏感信息。攻击者可以通过构造特定的 SQL 语句来触发数据库返回时间延迟，从而获取敏感信息。例如，攻击者可以通过构造一个包含时间延迟函数的 SQL 语句来触发数据库返回时间延迟，从而获取敏感信息。

### 4.3.3 基于联合查询的利用技术

基于联合查询的利用技术是一种常见的 SQL 注入攻击技术，它通过向数据库发送恶意 SQL 语句来触发联合查询，从而获取敏感信息。攻击者可以通过构造特定的 SQL 语句来触发数据库返回联合查询结果，从而获取敏感信息。例如，攻击者可以通过构造一个包含联合查询操作符的 SQL 语句来触发数据库返回联合查询结果，从而获取敏感信息。

### 4.3.4 基于堆叠查询的利用技术

基于堆叠查询的利用技术是一种常见的 SQL 注入攻击技术，它通过向数据库发送恶意 SQL 语句来触发堆叠查询，从而获取敏感信息。攻击者可以通过构造特定的 SQL 语句来触发数据库返回堆叠查询结果，从而获取敏感信息。例如，攻击者可以通过构造一个包含堆叠查询操作符的 SQL 语句来触发数据库返回堆叠查询结果，从而获取敏感信息。

## 4.4 SQL 注入漏洞利用技术

SQL 注入漏洞利用技术是一种常见的攻击技术，它利用 Web 应用程序和数据库服务器之间接口中的漏洞。攻击者可以通过构造特定的 SQL 语句来触发数据库返回恶意查询结果，从而获取敏感信息。例如，攻击者可以通过构造一个包含 SQL 注入操作符的 SQL 语句来触发数据库返回恶意查询结果，从而获取敏感信息。

## 4.5 SQL注入防御技术

SQL注入攻击是一种已经长期存在，但近年来日益增长的安全威胁。为了防止SQL注入攻击，可以通过以下几种方式进行防御：1.输入验证；2.参数化查询；3.存储过程；4.最小权限原则；5.使用ORM框架。

## 4.6 PyQT

PyQt 是一个 Python 的 GUI 工具包，它是 Qt 库的 Python 封装。PyQt 包含了大量的类和方法，可以帮助开发人员快速构建 GUI 应用程序。PyQt 的关键技术包括：信号和槽机制、布局管理器、事件处理、绘图和动画等。

### **4.6.1 信号和槽机制**

信号和槽机制是 PyQt 中的核心机制，也是在 PyQt 编程中对象之间进行通信的机制。在 PyQt 中，每个继承自 QObject 的对象都可以使用信号和槽机制来进行通信。信号和槽函数通过 object.signal.connect() 方法来连接。当一个 QObject 对象发射信号，与之相连接的槽函数就会被调用。

### **4.6.2 布局管理器**

PyQt 中的布局管理器是一种如何在应用窗口上放置组件的一种方法。布局管理器不是一个控件，而是一个区域划分的规则。在 PyQt 中，有多种布局管理器可供选择，包括：盒子布局、表单布局、网格布局、堆叠布局等。每个布局管理器都有其特定的用途和优点。

盒子布局是最常用的布局管理器之一，它可以将控件按照水平或垂直方向排列。表单布局可以将控件按照表单的形式排列。网格布局可以将控件按照网格的形式排列。堆叠布局可以将控件按照堆叠的形式排列。

### **4.6.3 事件处理**

PyQt 中提供了两种针对事件处理的机制：一种是信号和槽，另一种则是事件。事件处理在 PyQt 中是比较底层的，常见的事件类型有：键盘事件、鼠标事件、拖放事件、滚轮事件、定时事件、焦点事件、进入和离开事件（光标移入控件或者移出），移动事件（窗口位置变化），显示和隐藏事件，窗口事件（窗口是否为当前窗口）、以及常见的 Qt 事件：Socket 事件、剪贴板事件、文字改变事件，布局改变事件等。

PyQt 提供了 5 种事件处理和过滤方法，由弱到强分别是：重新实现事件函数、安装过滤器、重载 event() 函数、重载 eventFilter() 函数和自定义事件。其中前两种方法使用最频繁。

## 4.7  机器学习

机器学习是一门人工智能的科学，主要研究如何让计算机通过数据或经验来自动地学习和改进。机器学习涉及多个领域，如概率论、统计学、逼近论、凸分析、算法复杂度理论等。机器学习的目的是为了解决人工智能中的各种问题，如数据挖掘、计算机视觉、自然语言处理、生物信息学、游戏和机器人等，机器学习能检测常见的SQL注入类型，在制作SQL注入工具时应当对Payload进行特征变种防止被轻易识别出来。

机器学习可以根据不同的标准进行分类，如学习策略、学习方法、学习方式、数据形式和学习目标等。常见的机器学习分类有：

监督学习：从给定的带有标签的数据集中学习出一个函数，用来对新的数据进行预测。例如，分类和回归问题。

无监督学习：从没有标签的数据集中学习出数据的内在结构或规律。例如，聚类和降维问题。

半监督学习：介于监督学习和无监督学习之间，利用少量的标签数据和大量的无标签数据进行学习。例如，图半监督学习和生成对抗网络等。

强化学习：通过与环境的交互，不断地尝试和反馈，来学习最优的行为策略。例如，自动驾驶和围棋等。

机器学习有很多常用的算法，如决策树、朴素贝叶斯、支持向量机、随机森林、人工神经网络、深度学习等。这些算法有各自的原理、特点、优劣和应用场景，需要根据具体的问题和数据来选择合适的算法。

机器学习在网络安全的应用是一个非常热门和有前景的领域，主要是利用机器学习的数据分析和模式识别能力，来解决网络安全中的各种问题，如恶意软件检测、入侵攻击检测、异常行为检测、钓鱼邮件识别等。机器学习在网络安全中的应用的意义在于，可以帮助用户及时发现和防范网络威胁，提高网络安全水平，减少人工干预和误报，降低网络安全成本等。

机器学习在网络安全中的应用主要有以下几个方面：

恶意软件检测：通过机器学习对恶意软件的特征、行为、家族等进行分析和分类，从而有效地识别和隔离恶意软件，防止其对系统和数据造成损害。

入侵攻击检测：通过机器学习对网络流量、系统日志、用户行为等进行监控和分析，从而及时发现和预警网络入侵攻击，如端口扫描、拒绝服务、后门植入等。

异常行为检测：通过机器学习对用户或设备的正常行为模式进行建模和学习，从而识别出与正常行为模式不符的异常行为，如数据泄露、权限滥用、内部攻击等。

钓鱼邮件识别：通过机器学习对邮件的内容、主题、发件人、链接等进行分析和评估，从而判断邮件是否为钓鱼邮件，防止用户被诱导点击或下载恶意内容。

### **4.7.1 决策树**

决策树是一种常用的机器学习算法，主要用于分类和回归问题。决策树的基本思想是通过一系列的判断规则，将数据集划分为不同的子集，从而达到预测目标变量的目的。决策树的优点是易于理解和解释，可以处理离散和连续特征，可以处理缺失值和异常值等。决策树的缺点是容易过拟合，对噪声数据敏感，可能不稳定等。

要了解建立决策树的过程，我们首先需要了解什么是决策树。决策树是一种树状模型，用于根据一组条件做出决策。树的每个内部节点代表一个条件，而每个叶子节点代表一个决策。

构建决策树的过程包括选择最佳属性来分割每个节点上的数据。目标是创建一棵尽可能小的树，同时仍然准确地对数据进行分类。有几种建立决策树的算法，如ID3、C4.5和CART。

在ID3算法中，具有最高信息增益的属性被选为每个节点的分割属性。信息增益衡量的是根据一个特定的属性来分割数据所带来的熵的减少（或信息的增加）。C4.5算法是ID3的一个扩展，它使用信息增益比而不是信息增益来处理有许多值的属性。CART算法使用基尼指数来衡量数据的不纯度，并在每个节点上选择导致最低不纯度的属性。

决策树有多种算法，如ID3、C4.5、CART等。这些算法主要区别在于特征选择准则、划分方式、剪枝策略等方面。ID3算法使用信息增益作为特征选择准则，采用多叉树的划分方式，不进行剪枝操作。C4.5算法使用信息增益比作为特征选择准则，可以处理连续特征和缺失值，采用多叉树的划分方式，使用悲观剪枝法进行后剪枝操作。CART算法使用基尼指数作为特征选择准则，可以处理分类和回归问题，采用二叉树的划分方式，使用代价复杂度剪枝法进行后剪枝操作。

### **4.7.2 朴素贝叶斯**

朴素贝叶斯是一种基于贝叶斯定理和特征条件独立假设的分类算法。它的基本思想是，给定一个样本的特征向量，计算它属于每个类别的后验概率，然后选择后验概率最大的类别作为预测结果。朴素贝叶斯的优点是简单、高效、易于实现，适用于处理离散特征和文本数据。朴素贝叶斯的缺点是假设特征之间相互独立，这在实际中往往不成立，可能导致分类效果不佳。

朴素贝叶斯的算法流程如下：

给定训练集和测试集，确定类别集合和特征集合。

对于每个类别，计算其先验概率，即在训练集中出现的频率。

对于每个类别和每个特征，计算其类条件概率，即在训练集中该类别下该特征出现的频率。

对于每个测试样本，根据贝叶斯定理和特征条件独立假设，计算其属于每个类别的后验概率，即先验概率乘以类条件概率的乘积。

对于每个测试样本，选择后验概率最大的类别作为预测结果。

### **4.7.3 支持向量机**

支持向量机（SVM）是一种监督学习算法，用于机器学习中的分类和回归任务。它的基本思想是，找到一个最大间隔超平面，将不同类别的数据点分开，或者将数据点映射到高维空间，利用核函数在高维空间中找到最大间隔超平面。SVM的优点是具有良好的泛化能力，可以处理线性可分和非线性可分的数据，可以使用不同的核函数来适应不同的数据分布。SVM的缺点是对参数和核函数的选择敏感，计算复杂度较高，不适合处理大规模数据集。

支持向量机的算法流程如下：

1. 给定一个训练集，每个样本有一个特征向量和一个类别标签。
2. 选择一个核函数，将特征向量映射到高维或无限维空间中。
3. 在映射后的空间中，求解一个凸二次规划问题，得到最大间隔超平面的参数和支持向量。
4. 对于一个新的样本，将其特征向量映射到同样的空间中，根据最大间隔超平面的方程判断其所属的类别。

### **4.7.4 随机森林**

随机森林（Random Forest）是一种由决策树构成的集成学习算法，它使用Bagging的思想，通过有放回的抽样生成多个训练集，并用每个训练集训练一棵决策树，然后通过投票或平均的方式汇总多棵树的预测结果。随机森林在每个节点分裂时，还引入了特征随机选择的机制，即从所有特征中随机选取一个子集，再从这个子集中选择最优特征进行分裂。这样做的目的是降低决策树之间的相关性，提高集成的效果。

随机森林的优点是：

它可以处理高维度和大规模的数据，并且不需要降维或特征选择。

它可以评估特征的重要性和相互影响。

它不容易过拟合，具有很好的泛化能力和稳定性。

它可以处理缺失值和异常值。

它可以进行分类、回归、聚类和异常检测等多种任务。

它可以并行化训练，提高计算效率。

随机森林的缺点是：

它在噪声较大或者类别不平衡的数据上可能会过拟合。

它对于取值划分较多的特征有偏好，可能导致特征权重不准确。

它生成的决策树比较复杂，不太容易解释和可视化。

### **4.7.5 机器学习在恶意流量检测中的应用**

机器学习在检测恶意流量方面的应用是一个热门的研究方向。近年来，随着机器学习、深度学习等人工智能技术的快速发展，它们在图像识别、语音识别、自然语言处理等领域得到了大规模的应用，可以为传统方法难以解决或无法解决的问题提供有效解决方案。例如，将人工智能应用于检测恶意加密流量是一种成熟的方法。通过分析加密流量的未加密信息、上下文数据和其他特征，该方法可用于使用传统的机器学习算法对加密流量进行分类和检测，并检测潜伏在加密恶意流量中的安全威胁。

### **4.7.6 恶意流量**

恶意流量是指由恶意软件、僵尸网络、黑客或其他攻击者产生的网络流量，其目的是入侵、感染、窃取或破坏目标系统或数据。

恶意流量的特征可能包括：

非正常的访问频率、时间或持续时间

非正常的来源地址、端口或协议

非正常的请求内容、参数或头部

非正常的响应内容、状态码或头部

非正常的数据包大小、顺序或校验和

非正常的加密或编码方式

非正常的域名生成算法或动态域名解析

非正常的命令和控制通信或数据泄露

恶意流量的危害可能包括：

消耗网络带宽、资源或服务能力

降低网络性能、可用性或稳定性

破坏网络安全防护或检测机制

传播恶意软件、勒索软件或其他攻击负载

盗取用户凭据、敏感数据或知识产权

篡改网站内容、数据库记录或系统配置

执行远程代码、后门访问或拒绝服务攻击

恶意流量的检测和防御可能包括：

使用防火墙、入侵检测系统、反病毒软件等安全工具

使用网络流量分析器、协议分析器、恶意软件分析器等分析工具

使用黑名单、白名单、行为分析等过滤机制

使用加密、身份验证、授权等保护机制

使用日志审计、告警通知、应急响应等监控机制。

### **4.7.7 基于统计学习的算法**

1. Naive Bayes：这是一种基于Bayes定理的概率算法。它通常用于文本分类，但也可用于其他类型的数据。Naive Bayes假设特征是相互独立的，这在某些情况下可能不是真的。

2. 逻辑回归： 这是一个线性模型，用于二元分类问题。它将输出变量的概率作为输入变量的一个函数来建模。Logistic回归可以被扩展到处理多类分类问题。

3. 随机森林： 这是一种集合学习算法，结合多个决策树来提高模型的准确性。它是一种非参数算法，可以处理分类和连续输入变量。

4. 梯度提升法： 这是另一种集合学习算法，它结合了多个弱学习者来创建一个强学习者。它是一种参数化算法，可以处理分类和连续输入变量。

我们可以使用常见的机器学习库，如Scikit-learn或TensorFlow来实现这些算法。为了评估模型的性能，你可以使用准确性、精确性、召回率和F1分数等指标。你还可以使用交叉验证和超参数调整等技术来优化模型。

### **4.7.8 基于深度学习的算法**

1. 卷积神经网络（CNN）： 这是一种神经网络，通常用于图像分类，但也可用于其他类型的数据。CNN对于检测空间或时间上相关的数据模式特别有用，例如网络流量数据。你可以使用TensorFlow或PyTorch等库来实现CNN。

2. 循环神经网络（RNNs）： 这是另一种类型的神经网络，通常用于序列数据，如文本或时间序列数据。RNNs对于检测有时间关系的数据的模式特别有用，如网络流量数据中。你可以使用TensorFlow或PyTorch等库来实现RNN。

3. 长短期记忆（LSTM）网络： 这是一种RNN，旨在处理传统RNN中可能出现的梯度消失问题。LSTM网络对于检测数据中的模式特别有用，这些数据在时间上是相关的，并且具有长期的依赖性，例如在网络流量数据中。你可以使用TensorFlow或PyTorch等库来实现LSTM网络。

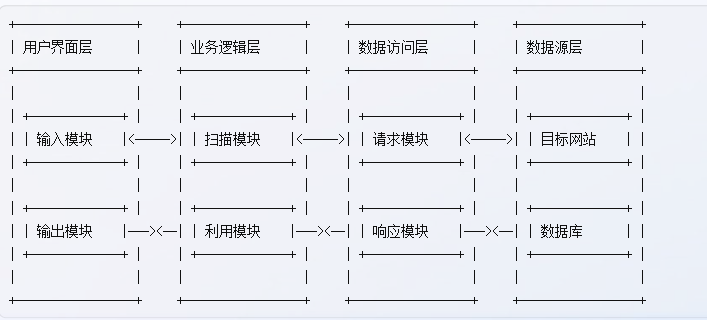
4. 自动编码器： 这是一种神经网络，通常用于无监督的学习，如异常检测。自动编码器对于检测人类不容易辨别的数据模式特别有用，例如网络流量数据。你可以使用TensorFlow或PyTorch等库来实现自动编码器。

为了评估模型的性能，可以使用准确性、精确性、召回率和F1分数等指标。你还可以使用交叉验证和超参数调整等技术来优化模型。

# 5 系统设计

## 5.1 系统架构设计

系统的总体架构：系统采用了分层的架构模式，将系统分为四个层次，分别是用户界面层、业务逻辑层、数据访问层和数据源层。每个层次都由若干个模块组成，模块之间通过接口进行通信和协作。如图所示，



系统的模块划分、关系和接口：

用户界面层：负责与用户进行交互，接收用户的输入，展示系统的输出。主要包括两个模块：

输入模块：负责接收用户输入的网址或域名，以及其他的参数或选项，将其传递给扫描模块。

输出模块：负责展示系统扫描和利用的过程和结果，以图形化或文本化的方式呈现给用户。

业务逻辑层：负责实现系统的核心功能，即扫描和利用目标网站的SQL注入漏洞。主要包括两个模块：

扫描模块：负责根据输入模块传递的网址或域名，自动地发现目标网站的所有链接，并对每个链接进行SQL注入测试，以确定是否存在SQL注入漏洞。扫描模块通过请求模块向目标网站发送测试请求，并通过响应模块接收测试响应，根据响应内容判断是否存在漏洞，并将漏洞信息传递给输出模块。

利用模块：负责根据扫描模块发现的SQL注入漏洞，自动地构造合适的攻击载荷，并发送给目标网站，以获取数据库的结构、内容或权限，或者执行任意SQL语句。利用模块通过请求模块向目标网站发送攻击请求，并通过响应模块接收攻击响应，根据响应内容获取或修改数据或操作，并将结果传递给输出模块。

数据访问层：负责实现系统与数据源层之间的通信，即向目标网站发送请求，并接收响应。主要包括两个模块：

请求模块：负责根据扫描模块或利用模块传递的参数，构造合法的HTTP请求，并发送给目标网站，以触发SQL注入漏洞。请求模块使用Python的requests库或其他的网络库，实现对不同类型的请求（如GET、POST、COOKIE等）的支持，以及对不同类型的编码（如URL编码、Base64编码等）的处理。

响应模块：负责接收目标网站返回的HTTP响应，并解析响应内容，以判断是否存在SQL注入漏洞，或者获取或修改数据或操作。响应模块使用Python的BeautifulSoup库或其他的解析库，实现对不同类型的响应（如HTML、JSON、XML等）的支持，以及对不同类型的错误（如数据库错误、逻辑错误等）的识别。

数据源层：负责存储目标网站的数据和逻辑，即数据库和SQL语言。主要包括两个模块：

目标网站：负责接收系统发送的请求，并根据请求内容执行相应的SQL语句，返回响应内容。目标网站可能使用了不同类型和版本的数据库和SQL语言，如MySQL、Oracle、SQL Server等。

系统的运行环境和部署方式：

系统的运行环境：系统可以运行在任何支持Python语言和相关库或工具的操作系统上，如Windows、Linux、Mac OS等。系统需要有足够的网络带宽和内存空间，以保证扫描和利用的效率和稳定性。

系统的部署方式：系统可以部署在用户自己的设备上，如个人电脑、手机等，也可以部署在云端服务器上，如AWS、Azure等。系统需要保证与目标网站之间的网络连接可用性和安全性，以避免被拦截或追踪。

## 5.2 系统算法

该程序它对一个给定的URL进行网络爬行和SQL注入。它导入了几个模块，如sys、os、re、subprocess、PyQt5.QtWidgets、PyQt5.QtCore、main\_window、urllib.request、urllib.parse、urllib.error、BeautifulSoup和threading。

该程序定义了两个类：CrawlThread和SQLThread，它们继承自QtCore.QThread。CrawlThread类负责抓取网页并检索所有的锚点标签。SQLThread类负责对给定的URL进行SQL注入。

Window类是继承于QMainWindow和Ui\_MainWindow的主类。它包含几个方法，用于初始化用户界面、连接信号和槽，以及执行网络抓取和SQL注入。

当用户点击 "分析 "按钮时，startAnalysis方法被调用。它创建一个CrawlThread类的实例并启动线程。当用户点击 "SQL Inject "按钮时，SQLInject方法被调用。它创建一个SQLThread类的实例并启动线程。

该程序还包含几个辅助方法，用于向列表视图添加项目，初始化表的部件，以及从目标列表视图中删除项目。

该代码是一个PyQt5用户界面的实现，由一个名为 "main\_window.ui "的.ui文件生成。该UI由一个QTabWidget组成，有四个标签：'爬取网页'（Crawl Webpage），'爬取结果'（Crawl Result），'SQL注入'（SQL Injection），和'注入结果'（Injection Result）。

爬取网页 "标签包含一个用于输入URL的QLineEdit部件，一个用于启动分析的QPushButton部件，以及一个用于显示标签'URL:'的QLabel部件。还有一个用于输入cookie的QLineEdit小组件和一个用于显示 "Cookie "标签的QLabel小组件。爬取结果 "标签包含一个显示爬取结果的QTableWidget部件。

SQL注入 "标签包含一个用于输入目标URL的QLineEdit部件，一个用于输入cookie的QLineEdit部件，一个用于选择线程数量的QSpinBox部件，一个用于显示目标URL的QListView部件，一个用于向攻击列表添加URL的QPushButton部件，一个用于显示攻击列表的QListView部件，一个用于启动攻击的QPushButton部件、 一个用于显示 "URL "标签的QLabel小组件，一个用于显示 "Cookie "标签的QLabel小组件，一个用于显示 "线程"（Thread）标签的QLabel小组件、 一个显示 "攻击列表"（Attack List）的QLabel部件，一个显示 "提示信息"（Tip Information）的QLabel部件，以及一个显示注射结果的QTableWidget部件。

注入结果 "标签包含一个用于显示注入结果的QTableWidget部件。

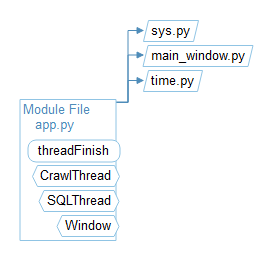
系统的各个模块的内部结构、算法和数据结构：

输入模块：输入模块由两个类组成，分别是界面类和参数类。

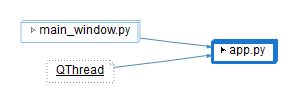
扫描类：负责对目标网站进行SQL注入测试，发现存在SQL注入漏洞的链接，并将扫描结果传递给输出模块和利用模块。扫描类使用Python的requests库或其他的网络库，实现对不同类型和版本的数据库和SQL语言，以及不同类型的请求和响应，如GET、POST、COOKIE等，以及不同类型的编码和错误，如URL编码、Base64编码等的支持。扫描类使用Python的re库或其他的正则表达式库，实现对网页内容中的链接和错误信息的提取和匹配。扫描类使用Python的threading库或其他的多线程库，实现对多个链接同时进行测试的功能。

## 5.3 流程图

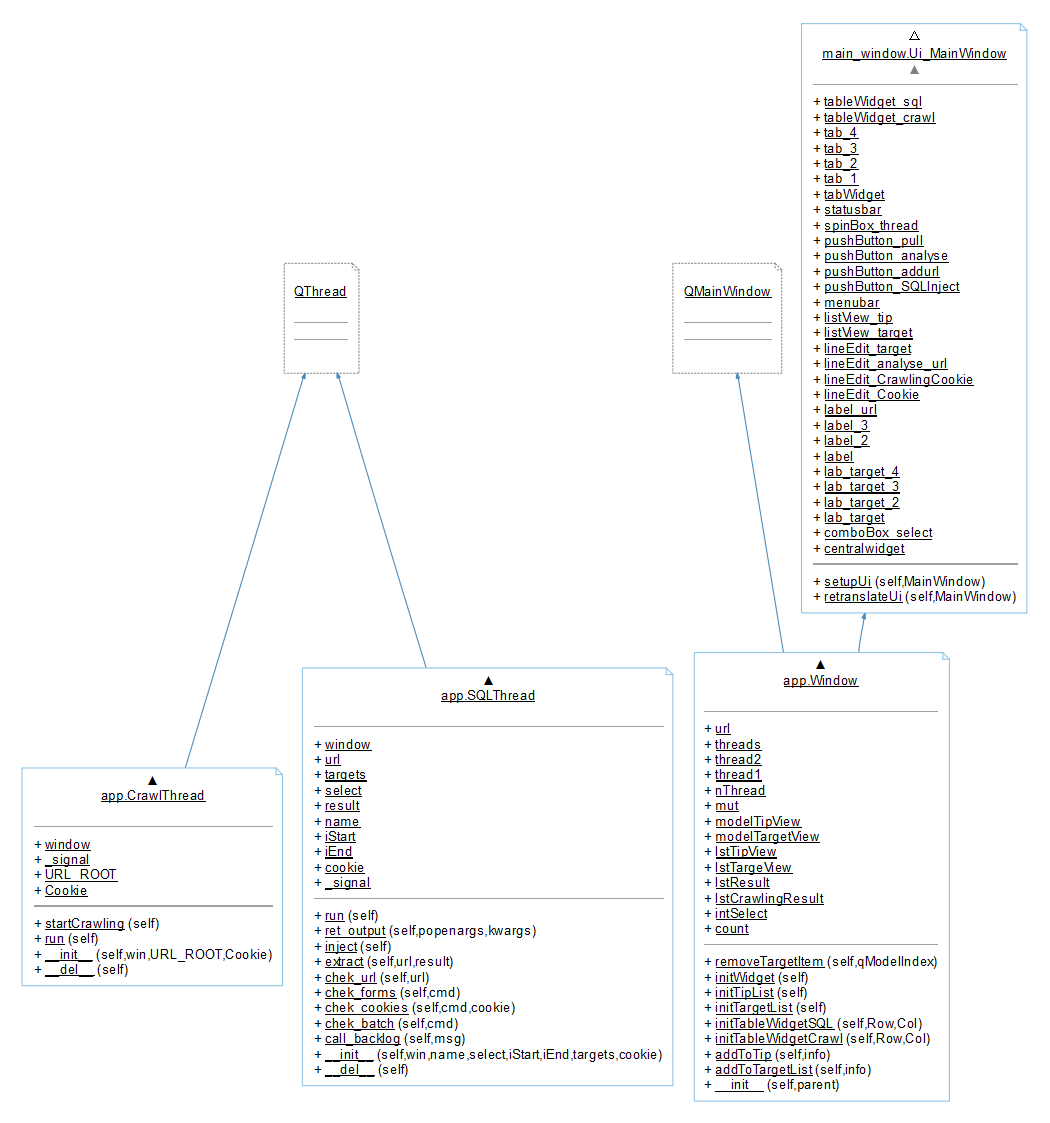
#### 主程序函数调用情况



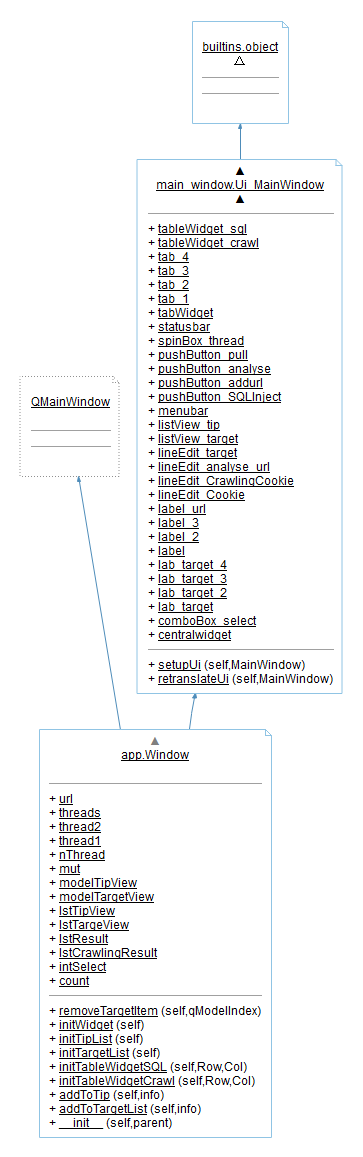
#### 主程序继承关系



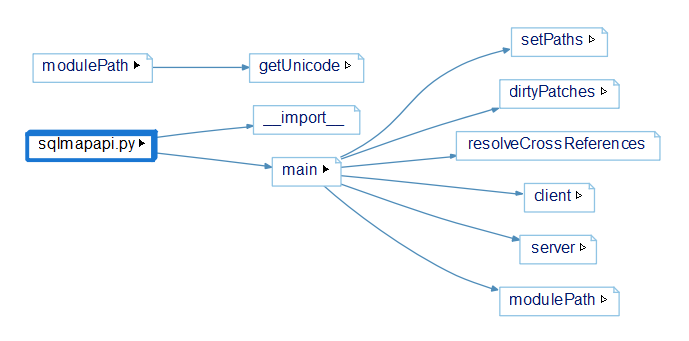
#### 主程序UML类图



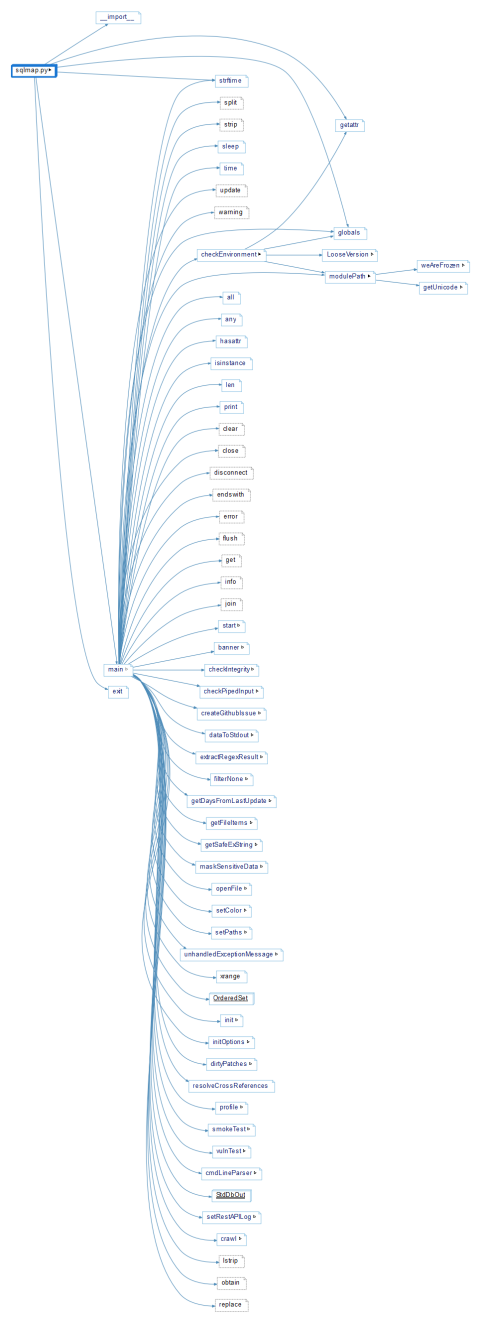
图形界面UML类图



#### 核心API调用情况



#### 核心函数调用情况



# 6 环境信息

## 4.1硬件资源

本系统的硬件资源为计算机，具体配置如表4.1.1所示

表4.1.1硬件配置

|  |  |
| --- | --- |
| CPU | Intel CORE i5 |
| 内存 | 16GB |
| 显卡 | 1060 |

## 4.2软件资源

|  |  |
| --- | --- |
| Editor | vscode |
| System | Win11 |
| Language | Python3 |

# 7 结论与展望

本文提出了一种基于 Python 的自动化 SQL 注入工具系统设计思路和实现方法，该方法具有较高的可行性和实用性

实验结果表明，基于 Python 的自动化 SQL 注入工具系统在 SQL 注入检测和利用方面具有较高的准确性和效率

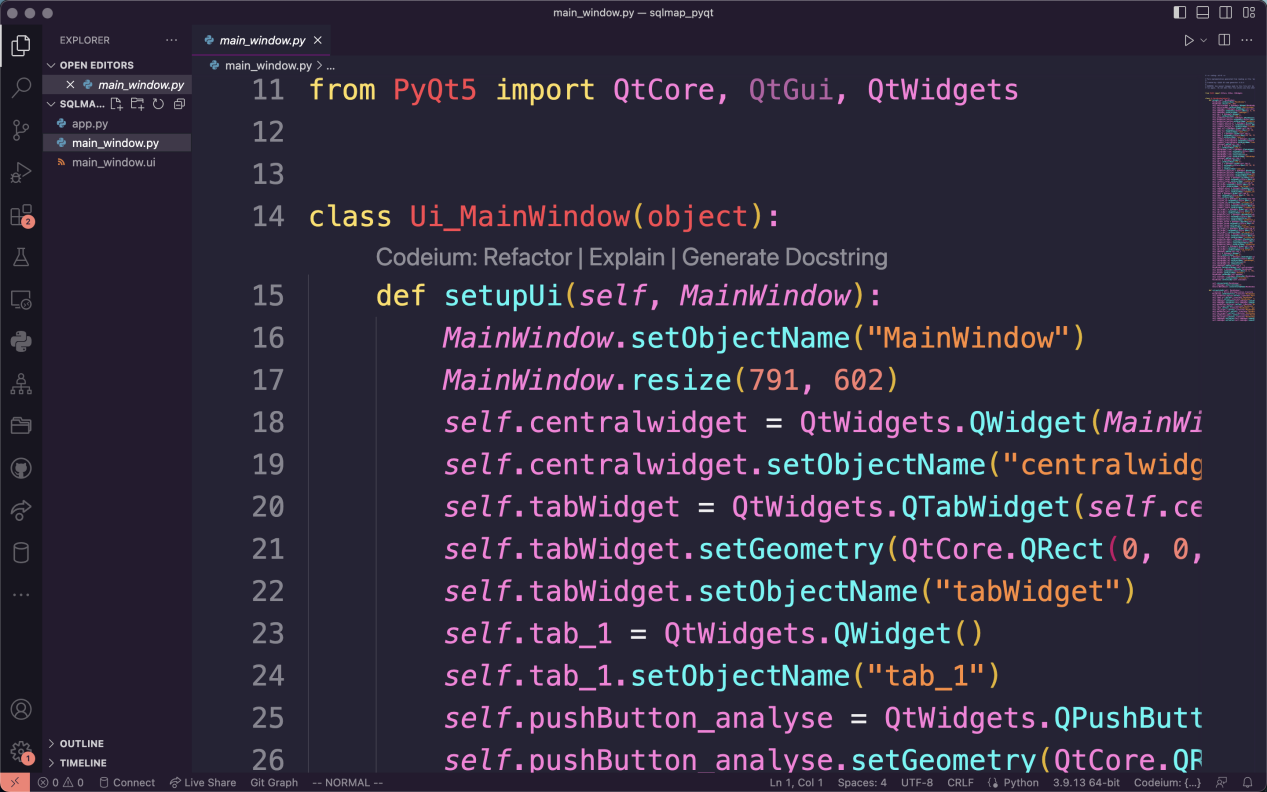
未来 SQL 注入工具的发展趋势是向自动化、智能化、高效化方向发展，基于 Python 的自动化 SQL 注入工具系统可以作为未来研究的一个重要方向

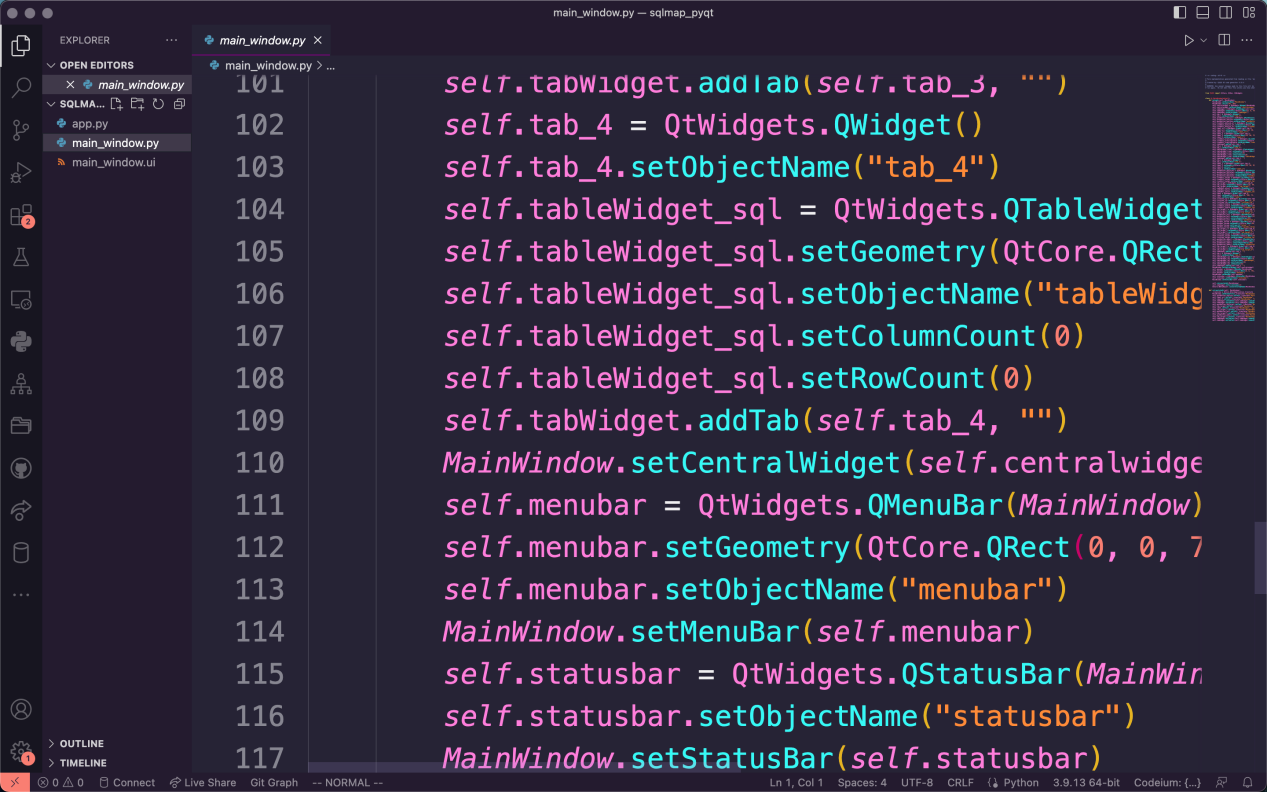
基于 Python 的自动化 SQL 注入工具系统还可以进一步改进和优化，比如增加对新型注入漏洞的检测和利用、提高检测和利用的效率等。

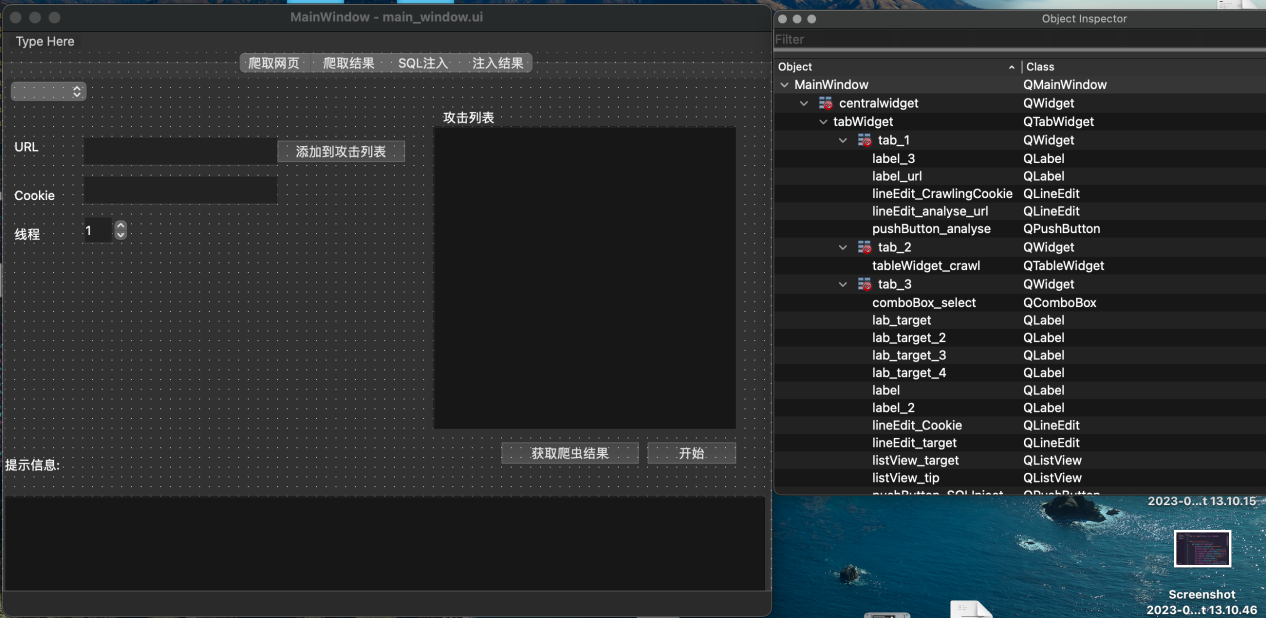
# 8 源代码

## 10.1 图形界面

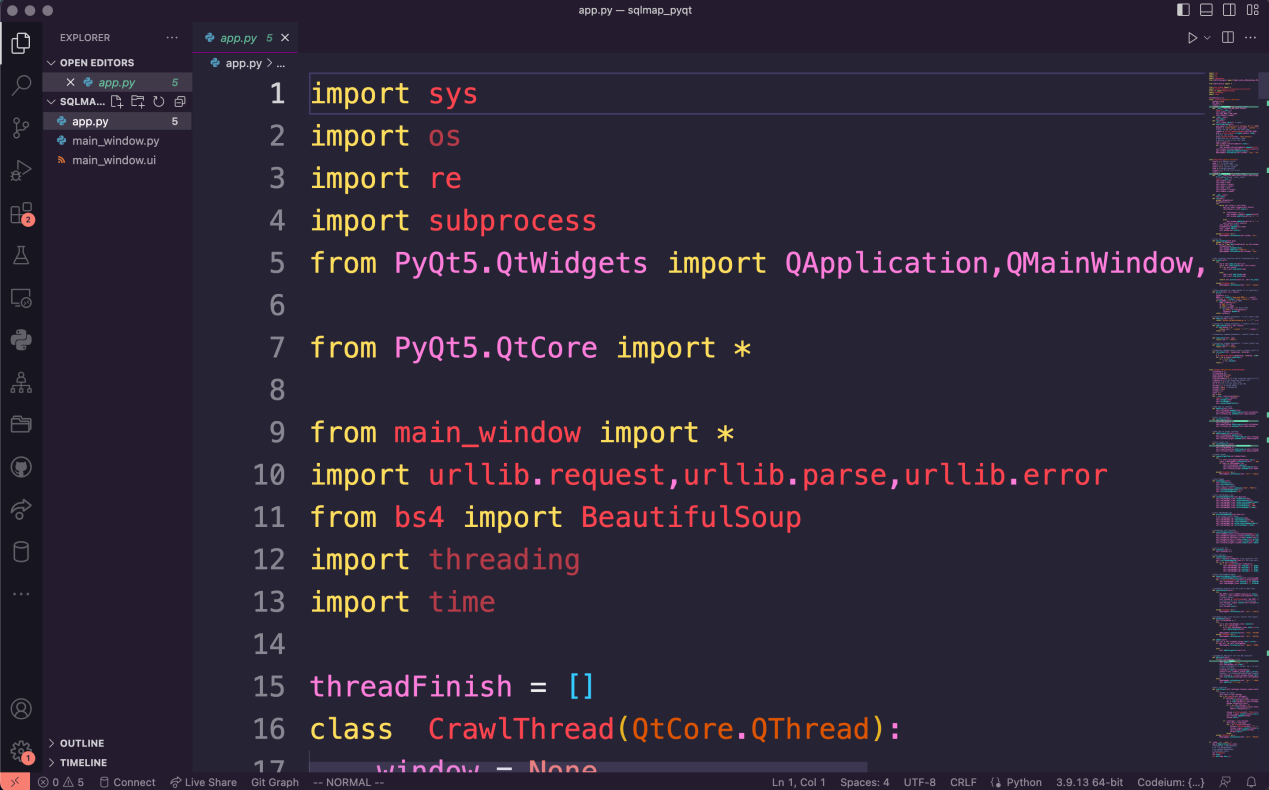


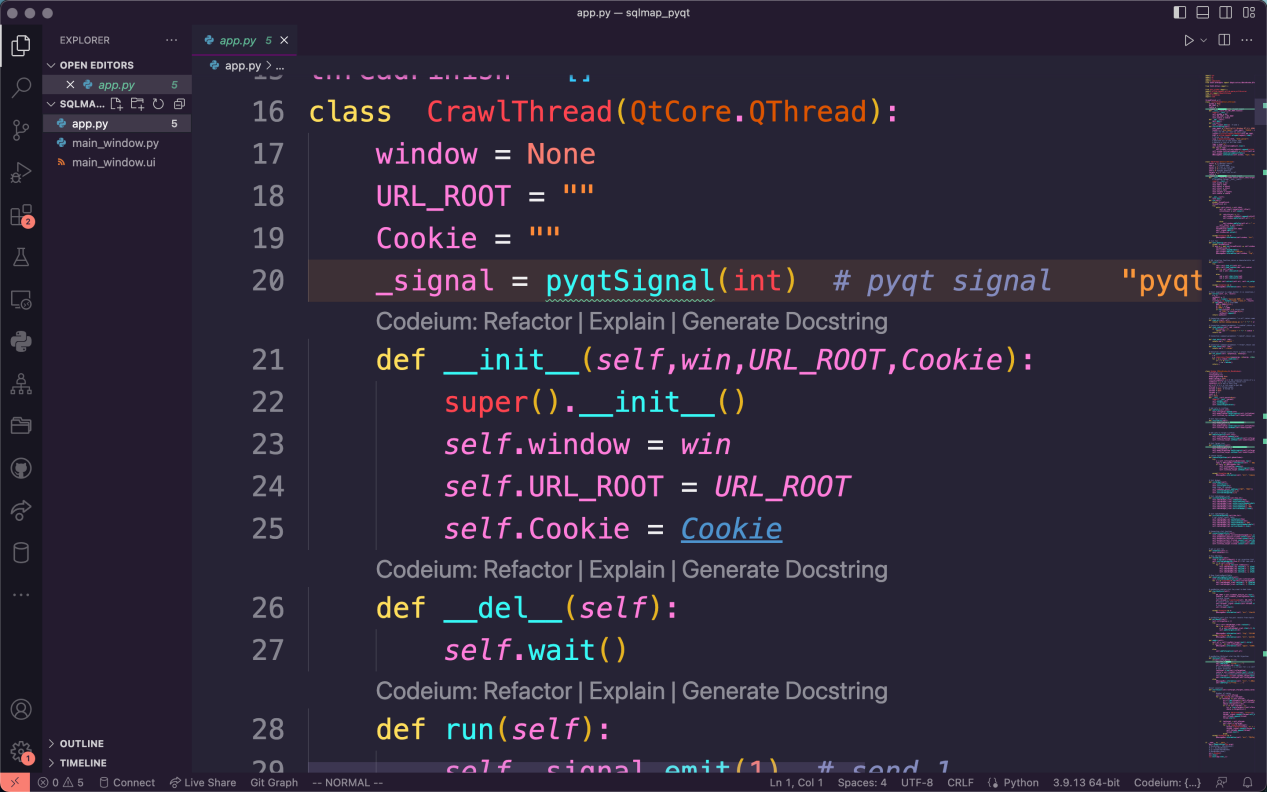


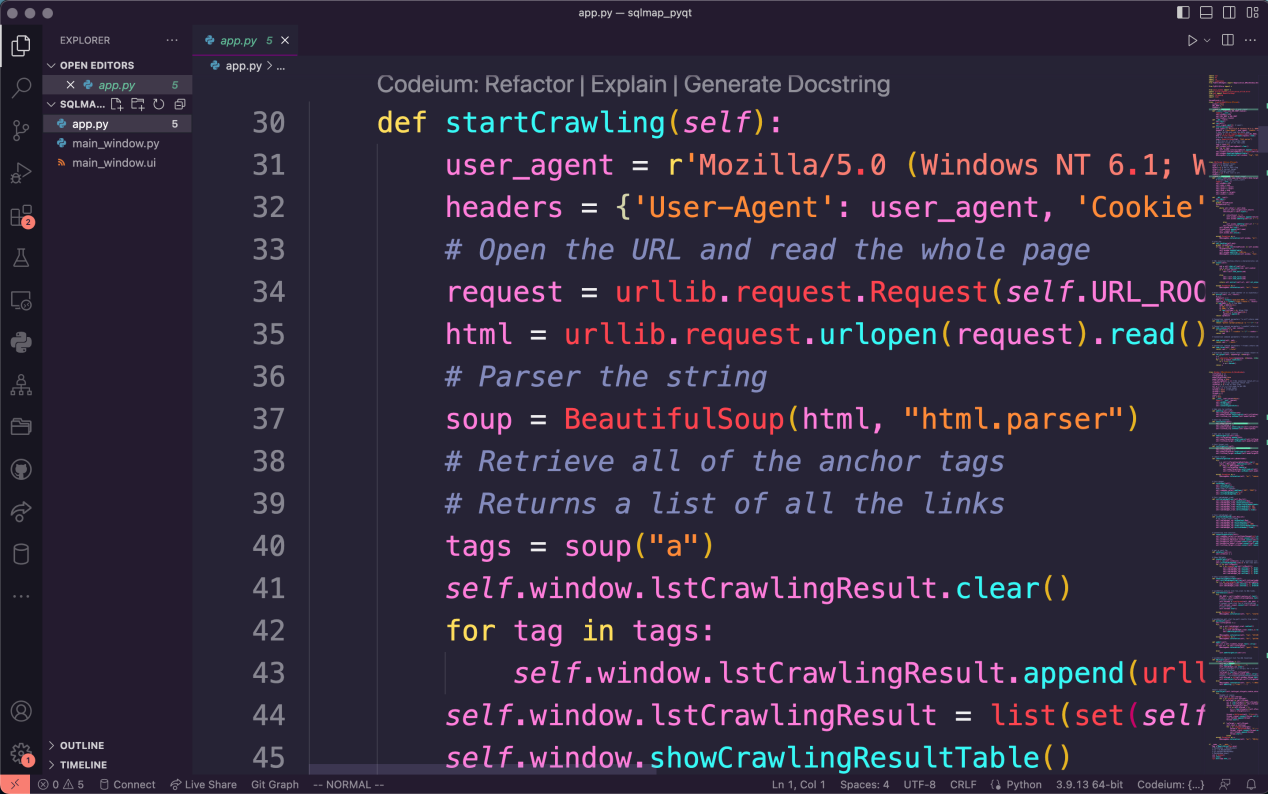


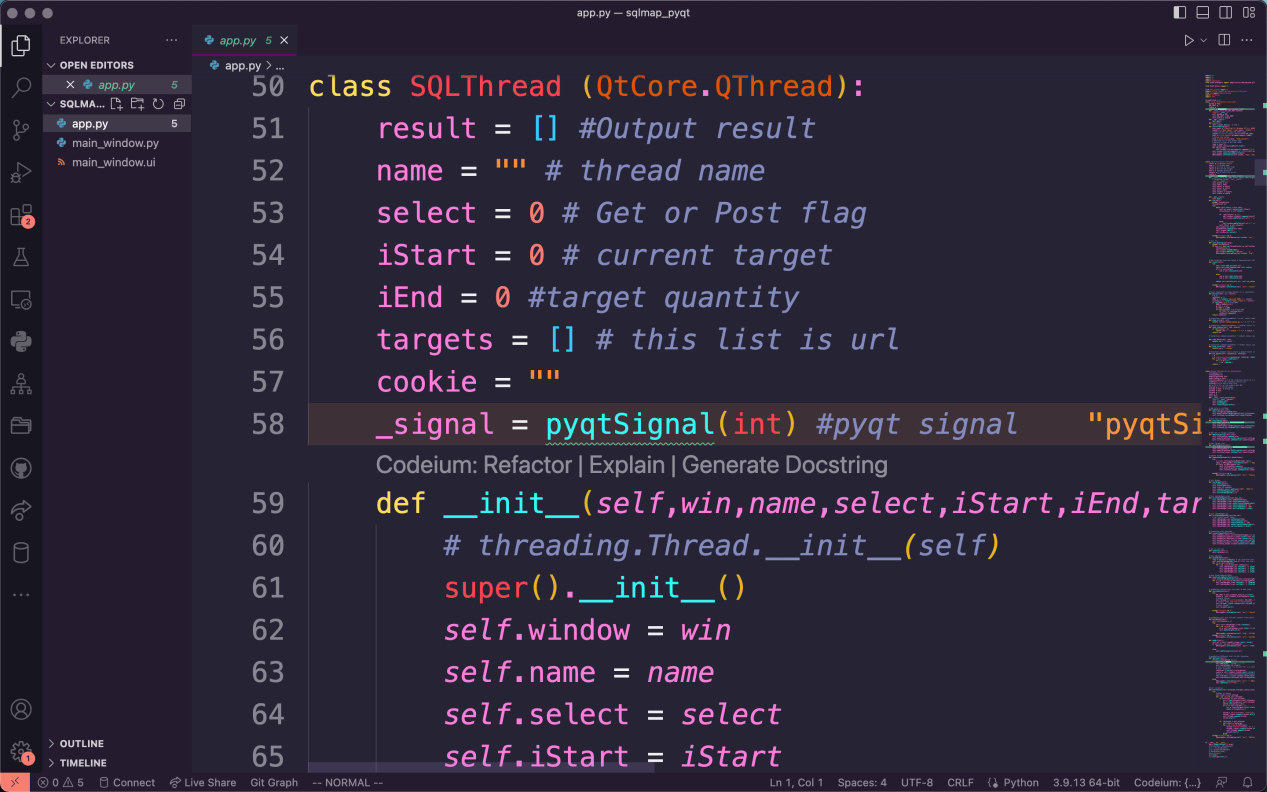


## 10.2 程序逻辑









# 参考资料

1. 范洁。 基于Python的网络流量特征统计分析与可视化[J]. 信息技术与信息化，2021,（04）：49-51.
2. 阙金煌。 基于Anaconda环境下的Python数据分析及可视化[J]. 信息技术与信息化，2021,（04）：215-218.
3. 赵宇翔, 李晓峰. 基于博弈论的异构无线接入网络中的频谱共享[J]. 计算机科学与探索, 2015, 9(2): 161-168.
4. 梁伟，贾名先，苑宁萍。 基于Python的大数据技术对线上教学情况分析与研究[J]. 电脑知识与技术，2021,17（11）：111-112
5. 宋妍芳。 Python教学培养计算机人才的思维能力的策略研究[J]. 电脑知识与技术，2021,17（11）：126-127+130.
6. 1Anley C. Advanced SQL Injection in SQL Server Applications[M]. [s.l.]: Next Generation Security Software Ltd., 2002.
7. Halfond W G, Viegas J, Orso A. A Classification of SQL-injection Attacks and Countermeasures[C]// Proceedings of the IEEE International Symposium on Secure Software Engineering.[s.l.]: IEEE, 2006.
8. 张卓,薛质.Linux环境中基于PHP的SQL注入攻击与对策[J].信息安全与通信保密,2006(9):154-157.
9. 陈楠,薛质.SQL注入攻击的实现和防范[J].信息安全与通信保密,2005(1):48-50.
10. 戴牡红,曾平.Oracle数据库中SQL注入攻击的检测与防御[J].信息安全与通信保密,2007(9):143-144.

致谢

大学四年的生活即将结束，我的人生也即将开始新的篇章。我非常感谢母校这些年对我的栽培，在母校所学习到的不仅仅是知识，还有为人处世的道理，我也很感谢我的同学和老师对我的支持与帮助。

从写这篇论文开始，经历了很长的时间也经历了数次改动，最终我的这篇论文是在我的导师梁衬章的不断的耐心指导下完成的。在与梁衬章老师的栽培下我学习到了很多东西，比如说严谨的精神，这对于我以后的人生道路而言是一笔非常宝贵的财富。

最后，我还是想感谢每一位曾经教导和帮助过我的老师和同学，没有老师和同学的帮助我在学校的学习也不会那么顺利，也不会掌握那么多知识、我会继续努力加油，用我的努力去实现我的人生价值