Hisa 静态分析工具需求说明

(第三周期)

撰写者：南京大学 程珂

南京大学 陈昊东

南京大学 施超烜

南京大学 吴晓阳

南京大学 周若衡

目录

1. 引言

1.1 编写目的

本项目基于演化模型进行开发，第三版需求说明书是对项目第二周期(2020/5/7~2020/5/27)需求说明的补充和改进，同时也包括了基于项目第二周期的阶段性成果以及提出的新的需求。第三版需求说明的编写目的在于对第二周期的后续工作进行补充以及对第三迭代周期的工作进行指导。帮助编码人员更好的理解第二周期的目标从而准确高效的完成第三周期的任务。与此同时还可以辅助我们与用户的交流，从而从用户的角度得到更有效的反馈。

1.2 需求说明(第三周期)概述

需求说明(第三版)在项目背景、预期的读者和建议、项目前景、项目功能概述、用户类及其特征等内容上与第一版无区别，因此不再重复编写。

本版需求说明第 2 节介绍了对于第 2 周期需求说明的改进和补充，旨在记录在项目的进展过程中，随着开发人员对项目难点、重点和用户需求的理解加深，从而对第二版需求中的部分内容进行的更改和细化。在第 2 节中，我们详细列出了更新的原因和修改/添加的位置及更新后的新内容。

本版需求说明第 3 节介绍了在项目的第三个迭代周期中需要完成的新的功能及其与用户交互的效果，旨在第三个迭代周期中对开发人员做出指导，使其更加容易理解各个功能的实现效果，从而高效准确的完成开发任务。同时也向用户和上级检查人员和用户展示我们对需求的理解，以便从上级评测人员和用户得到有效的反馈和修改意见。

本版需求说明第 4 节介绍了项目第三周期的预期目标和最终结项验收的工作。

2 改进

2.1 概述

在第 2 节中，我们详细介绍团队在第二周期开发的过程中对第二版需求说明做出的改进：我们将第二周期的结束时间从 6 月 7 日提前至 5 月 27 日，更改了用户项目的输入形式，修改了事件列表中的相应内容，修改了命令集设计，增加了交互式命令行模块，增加了对 Text 输出格式的支持，改进了 Html 报告的设计，并根据功能的变更更新了用户用例图，还细化了软件文档规范。

2.2 第二周期提前结束

由于在第一周期过后团队成员对核心框架的理解已经较为深入，熟悉了一系列工具的使用和演化模型一个周期内的步骤，因此第二周期的开发进度超过预期，所以团队决定将第二周期的结束日期从 6 月 7 日提前至 5 月 27 日，并从 5 月 27 日开始进行第三周期的需求分析工作。

2.3 用户输入形式变更

将用户的输入形式由一个或多个文件路径变更为输入项目的 compile_commands.json 文件，用户可自行选择需要被检测的 C++文件。

变更原因：以文件为路径作为输入仅仅能检测只依赖标准头文件的项目，为了增加 HiSA 对大规模项目的支持，需要用户提供待检测项目的编译信息。为了方便用户使用 HiSA，我们在用户手册中列举了可行的生成 compile_commands.json 文件的方式以指导用户使用 HiSA。

2.4 事件列表变更

对命令行版本的事件列表，进行如下更改

操作	事件	触发	事件源	行为	响应	事件宿
删：(1)	用户查看检测历史记录	用户输入查看历史记录的命令	用户	从数据库中读取用户检测历史，将历史记录中每一次检测的检测时间，各项检测选项，项目所在地址，报告输出地址等信息整理成历史记录条目，依次输出	用户检测历史记录	用户
删：	用户删除历史记录	用户输入删除历史记录的命令和选择需要删除的命令范围	用户	从数据库中删除用户相应的检测历史信息	删除后的历史记录	用户
原：(1)	用户创建检测项目	用户打从命令行输入项目检测命令并输入项目基本	用户	在用户的项目列表中添加一个项	用户项目	用户

		信息		目，并在其中保存用户输入的基本信息	列表中的项目	
原：(2)	用户上传项目文件	用户从命令行输入项目文件所在地址	用户	Load 项目文件，并在数据库中插入相应信息	上传成功或失败的结果信息	用户
改：(1)	用户输入项目对应的 compile_commands.json 文件	compile_commands.json 文件所在路径	用户	检测该地址对应文件是否存在，尝试 load 并返回 load 结果	文件是否找到的信息	用户
改：(2)	用户选择需要检测的 C++文件	项目中需要检测的一个或多个 C++文件所在路径，如果省略该项，则默认检测 compile_commands.json 文件中包含的所有文件	用户	检测该地址对应文件是否存在，尝试 load 并返回 load 结果	文件是否找到的信息	用户

2.5 命令集变更

在第二周期的开发过程中我们将命令集设计进行了改进，新的命令集如下表所示：

Command	Description
-help	打印帮助信息
-g	开启 god mode
-debug	开启 debug mode
-debug --output-path path	指定生成的 ExplodedGraph 的文件路径，仅 debug 模式下有效
-debug --trim-exploded-graph	只打印缺陷报告的路径，仅 debug 模式下有效
-debug --show-analysis-progres	打印分析的进度，仅 debug 模式下有效
-debug --exploded-graph	打印 ExplodedGraph，仅 debug 模式下有效
-input file1 file2 ...	指定输入文件，若留空则检查 compile_commands.json 内所有源文件
-compilation-database-path path	指定 compile_commands.json 路径
-output --path path	指定输出路径
-output --format format1 format2 ...	指定输出格式，目前支持 json,console,text,html
-output --info opt1 opt2 ...	指定输出包含的信息，目前支持 time,checker,desc,stats，若指定 time 则默认添加-stats
-enable-checker	指定开启的检测器，若留空则禁用所有检测器

checker1 checker2 ...	
-checker-list	列举现有支持的检测器

变更原因：由于在开发的过程中对部分核心功能进行了拓展，原来设计的命令集不足以支持更多的功能，并且第二周期需求说明中命令集的设计不够规范，部分命令(eg. -o,-s,-dz)语义不清晰且难以理解。经过团队讨论决定在兼容原命令集功能的前提下改进命令集。

2.7 交互式命令行模块

在原命令行版本中新增交互式命令行模块，命令行版本提供用户使用终端输入命令直接调用和采用交互式命令两种交互模式。交互式命令行的命令集设计如下表所示：

命令	子命令	描述
help	\	打印帮助信息
quit	\	退出程序
info	help	打印 info 命令的帮助信息
info	analyzer-opt	获取 Analyzer Options
info	output-opt	获取 Output Options
info	checker	获取 Checker List 及其状态
info	src	获取当前将会分析的文件列表
info	available-src	获取当前可进行分析的文件列表
set	help	打印 set 命令的帮助信息
set	debug-output-path path	设置生成的 ExplodedGraph 的文件路径，仅 debug 模式下有效
set	compilation-database	设置 compile_commands.json 路径

	path	
set	output-format format1 format2 ..	设置输出格式，目前支持 json,console,text,html
set	output-path path	设置输出路径
enable	help	打印 enable 命令的帮助信息
enable	gmode	开启 God Mode
enable	analyzer-stats	开启分析器统计
enable	debug	开启 Debug Mode
enable	debug-analysis-progress	开启分析进度显示（默认开启 Debug Mode）
enable	debug-exploded-graph	开启 Exploded Graph 打印（默认开启 Debug Mode）
enable	debug-trim-exploded-graph	开启对 Exploded Graph 路径裁剪（默认开启 Debug Mode）
enable	output-time	开启时间信息输出
enable	output-checker	开启 Checker 信息输出
enable	output-description	开启缺陷描述信息输出
enable	output-stats	开启统计信息输出
enable	checkername	开启对应 Checker
disable	help	打印 disable 命令的帮助信息
disable	gmode	关闭 God Mode
disable	analyzer-stats	关闭分析器统计

disable	debug	关闭 Debug Mode
disable	debug-analysis-progress	关闭分析进度显示
disable	debug-exploded-graph	关闭 Exploded Graph 打印
disable	debug-trim-exploded-graph	关闭对 Exploded Graph 路径裁剪
disable	output-time	关闭时间信息输出
disable	output-checker	关闭 Checker 信息输出
disable	output-description	关闭缺陷描述信息输出
disable	output-stats	关闭统计信息输出
disable	checkername	关闭对应 Checker
analyze	analyze \<filename\>	运行分析器，若指定文件名则分析指定文件，否则按文件列表进行分析
reset	help	打印 reset 命令的帮助信息
reset	analyzer-opt	重置 Analyzer Options
reset	output-opt	重置 Output Options
reset	checker	重置 Checker 状态
reset	src	重置文件列表
addsrc	filename	将文件加入至文件列表
delsrc	filename	从文件列表中移除对应文件
show	help	打印 show 命令的帮助信息
show	summary	打印上一次分析的总结报告
show	all	打印上一次分析的分析报告，包含各个文

		件的分析和总结报告

变更原因：原本命令行版本仅支持从控制台打开直接输入完整命令，交互性较差。为了提高命令行版本的交互性，团队决定开发交互式命令行模块并集成进命令行版本中。

2.8 Text 输出格式

在 htm，json 输出格式的基础上新增了 txt 文件的报告输出格式。

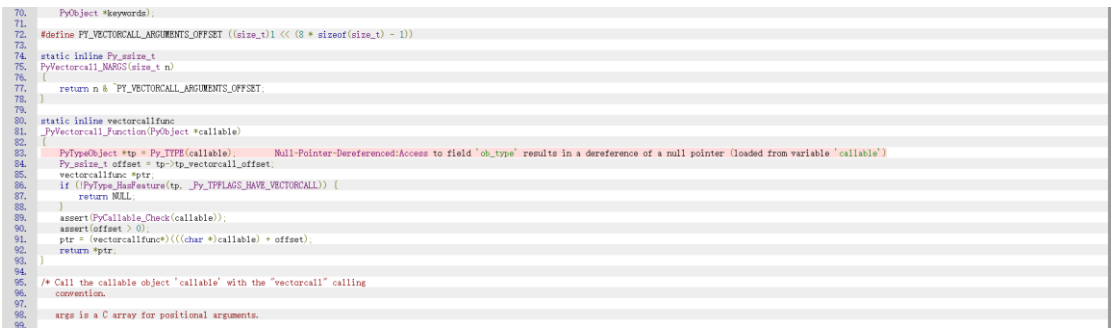
变更原因：增加更多输出格式以满足用户的多种需求

2.9 Html 报告重设计

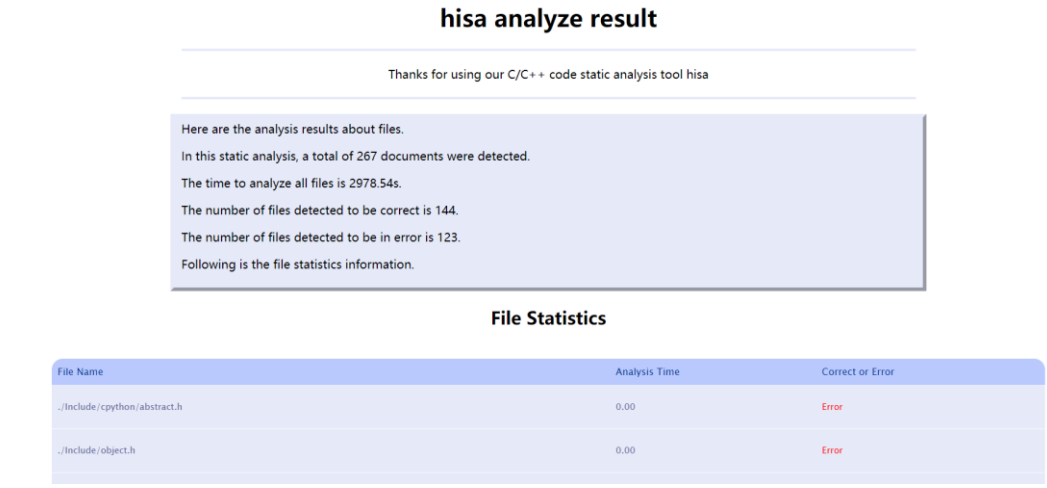
在第二周期需求说明的 HTML 报告的基础上对 HTML 报告进行了重设计，界面更加简洁美观，并支持索引跳转到具体代码。

更改后的 html 报告主页如下图所示：

跳转到具体代码：

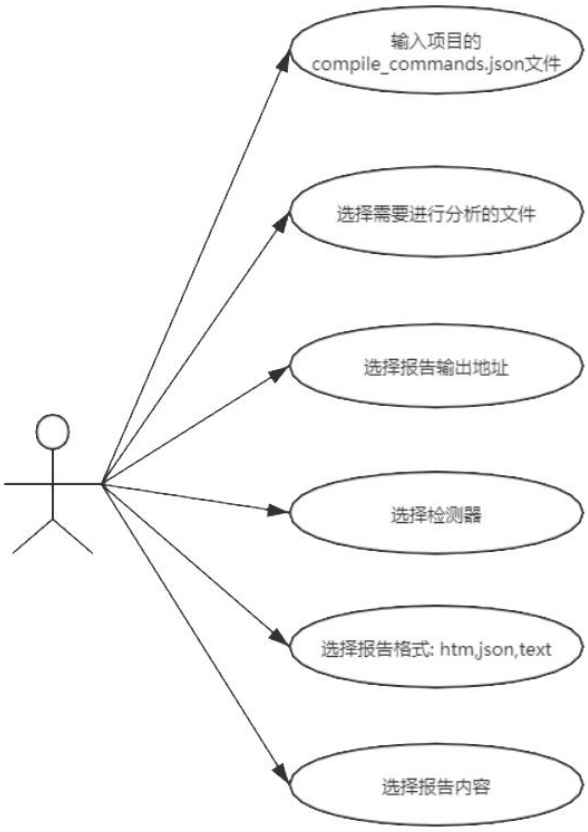


统计信息界面：



变更原因：为了提高 html 报告查看的便捷性，团队成员决定支持从错误信息跳转到具体代码的功能，同时为了使得报告界面更加简洁，将统计信息和缺陷列表划分为两个不同的页面，并在它们之间提供相互跳转的功能。

2.10 用户用例图变更



变更原因：因为变更了用户的输入并新增了报告格式，所以用户与 HiSA 的交互发生了变化。

2.11 细化软件文档规范

对于第一版需求说明中的**代码文档规范**，我们提出了更加具体的指标：每个模块都必须存在相应的设计文档，其中包括类图，时序图或控制流程图。

3 新的需求

3.1 新需求概述

在本节中，我们对于在第三个迭代周期(2020/5/27~2020/6/30)中预计要新增的功能进行需求说明。1. 核心增强与拓展：增强 HiSA 的核心检测功能，使得其具有能够在有限时间内检测百万行级别大项目的能力。2. Gui 功能的拓展：在第三周期中 Gui 将支持历史记录，中英文语言转换，自动从项目文件夹中检索 compile_commands.json 文件，并提供用户选择需要检测的 C++文件的界面，增加恢复默认设置的功能，新增功能的事件列表与界面设计将会在 3.3 给出。3. 官方网站的开发与搭建，支持在线下载 HiSA，查看用户手册，查看开发者手册与 API 文档的功能，具体的事件列表与界面设计将会在 3.4 给出。

3.2 核心功能增强

在第三个周期中，HiSA 需要增强其核心检测能力，需要通过对万行，十万行，百万行级别项目的测试。在这一过程中需要核心开发人员不断修复和增强核心框架与检测器的功能。这一过程并不影响用户与 HiSA 的交互过程，因此无需绘制新的事件列表。

3.3 Gui 功能拓展

在第三周期中，Gui 将支持历史记录，中英文语言转换，自动从项目文件夹中检索 commands.json 文件，并提供用户选择被检测 C++文件的界面，增加恢复默认设置的功能。在此给出事件列表和 Gui 设计，以指导第三周期中相关模块的开发者。

3.3.1 事件列表

Gui 拓展功能事件列表					
历史记录					
事件	触发	事件源	行为	响应	事件宿
用户查看历史记录	用户点击 Settings → History	用户	History 模块从 history.txt 文件中读取历史记录,HistoryDialog 将读取到的历史记录展示在界面中	HistoryDialog 界面，其中包含了当前的历史检测记录	用户
用户清空历史记录	用户点击 HistoryDialog 界面中的 Clear History 按钮	用户	HistoryDialog 清空历史记录表并调用 History 模块将 history.txt 文件清空	清空历史记录后的 HistoryDialog	用户
用户查看一	用户选中该	用户	HistoryDialog 将	包含用户所选	用户

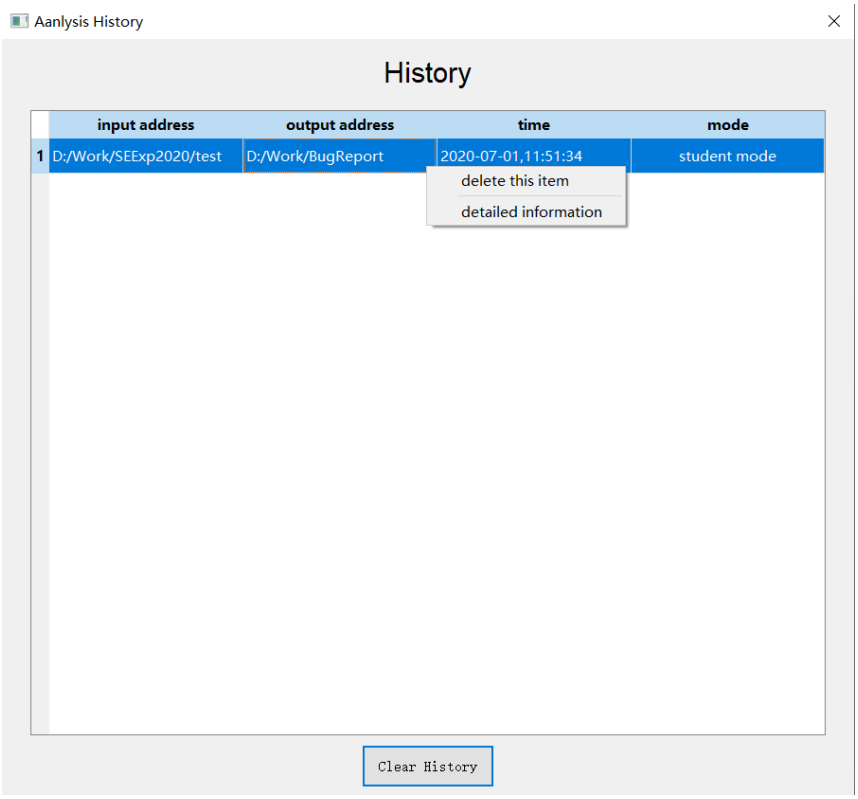
条历史记录详情	HistoryDialog 界面中一个条目并右键选择 detailed Information 选项		History 模块中的对应信息传入 Detailed InforDialog 中并展示给用户	历史记录详细信息的 Detailed InfoDialog	
用户删除一条历史记录	用户选中该 HistoryDialog 界面中一个条目并右键选择 delete this item 选项	用户	HistoryDialog 将用户选中的条目从自己的 TableView 中删除并调用 History 模块将对应条目从 history,txt 文件中删除	删除选中历史记录条目后的 HistoryDialog	用户
中英文转换					
事件	触发	事件源	行为	响应	事件宿
用户将 Gui 界面语言转换为中文	用户点击菜单栏中的 Settings → Language → Chinese	用户	将界面中的所有控件名，提示内容与帮助内容都变更为中文	中文界面	用户
用户将 Gui 界	用户点击菜单	用户	将界面中的所有	英文界面	用户

面语言转换为英文	栏中的设置→语言→英文		控件名，提示内容与帮助内容都变更为英文		
自动检索 compile_commands.json 文件					
事件	触发	事件源	行为	响应	事件宿
用户准备开始缺陷检测	用户单击 Go!按钮准备开启缺陷检测	用户	检索用户输入的项目文件夹目录是否合法，如果合法则检索项目文件夹中所有的.json 文件，并将找到的 json 文件列表展示给用户	项目中所有 compile _commands. json 的文件列表	用户
用户选择项目中需要被检测的 C/C++文件					
事件	触发	事件源	行为	响应	事件宿
用户选择项目中需要被检测的 C/C++文件	用户选中 compile _commands. json 文件后单击 Affirm 按钮	用户	解析用户选中的 compile _ commands .json 文件，抽取其中的 Cpp/C 文件整理为文件树结构展	项目的 Cpp/C 文件文件树	用户

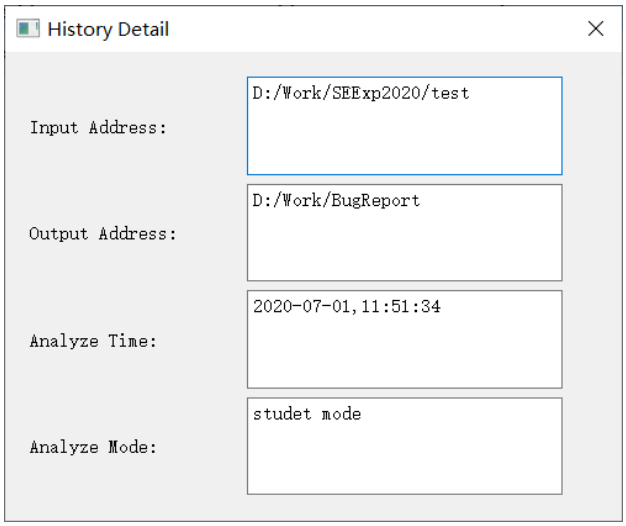
			示给用户		
恢复默认设置					
事件	触发	事件源	行为	响应	事件宿
用户恢复默认设置	用户点击菜单栏中的 设置→恢复默认设置	用户	将界面语言转换为英文，将所有选项设置为初始化时的默认选项	初始化默认界面	用户

3.3.2 界面设计

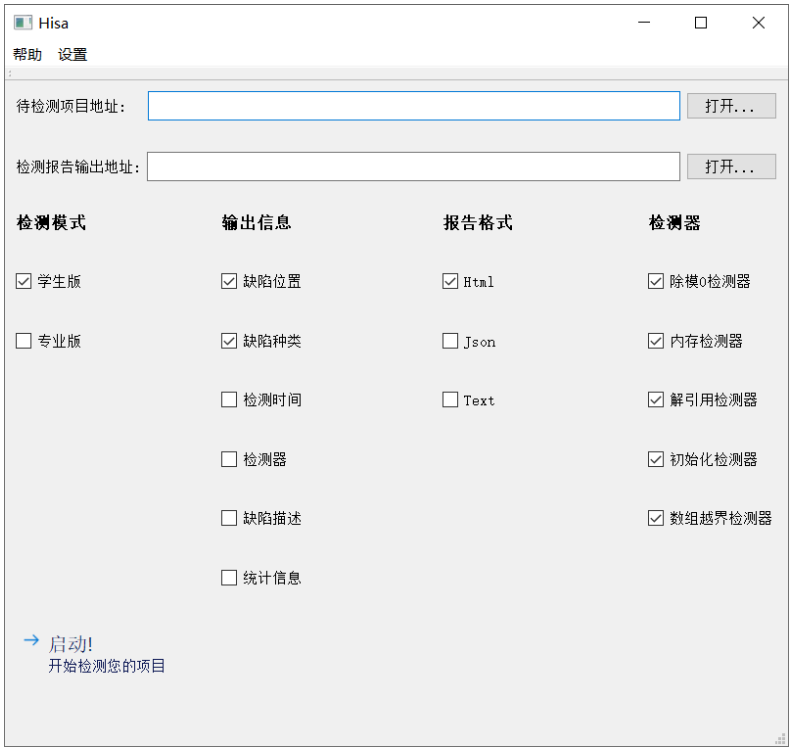
历史记录界面：



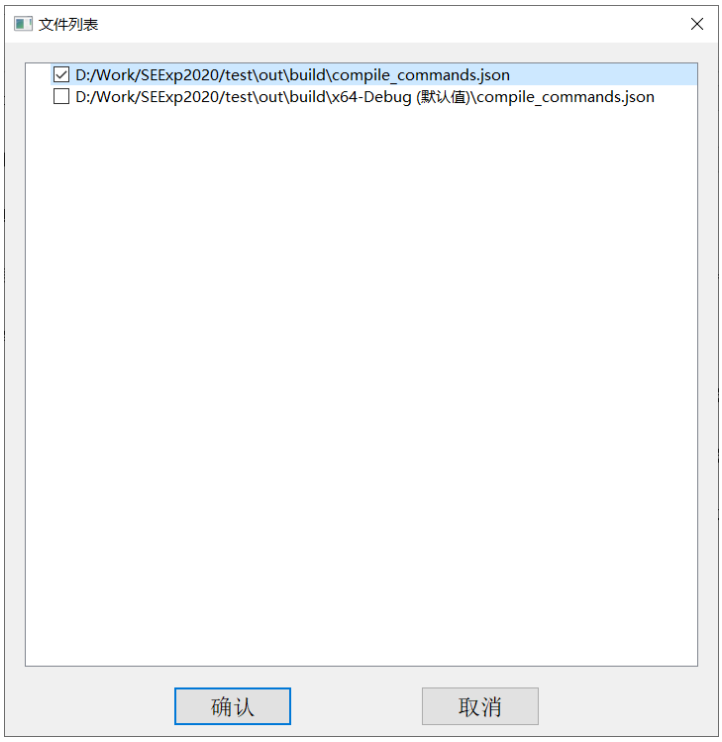
详细历史记录信息界面：



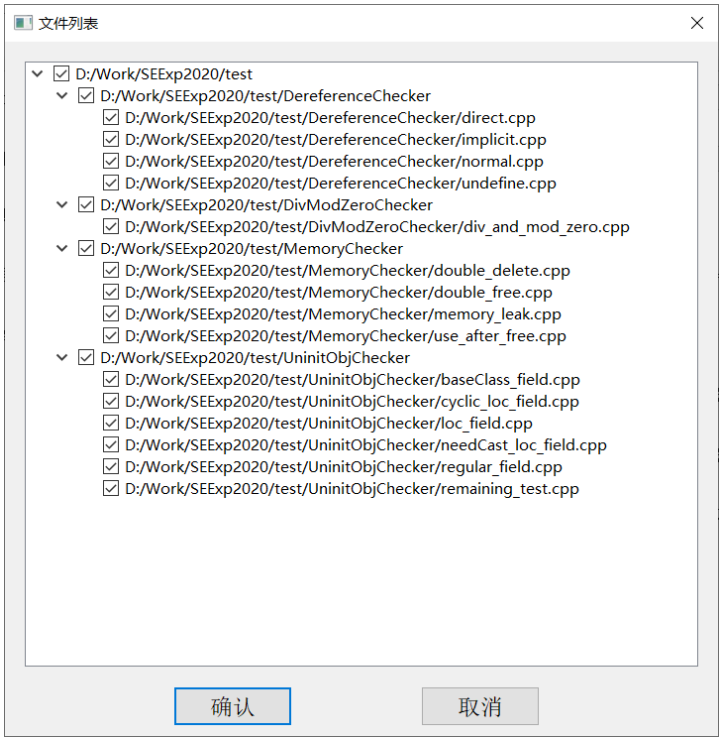
中文 Gui 界面：



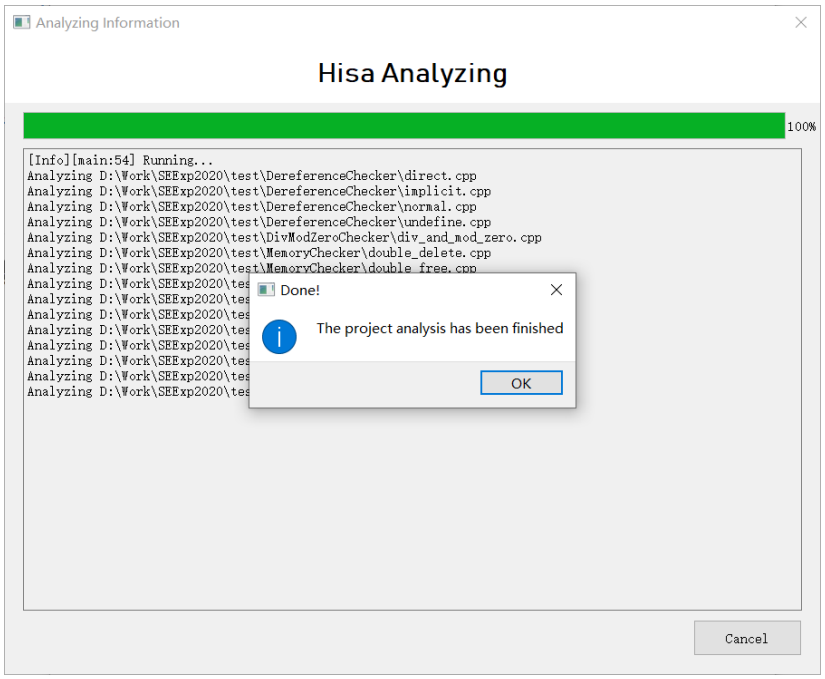
compile_commands.json 文件选择界面：



C++/C 文件选择界面：



进度条界面：



3.4 官方网站

在第三周期中我们将进行官方网站的开发与搭建，支持在线下载 HiSA，查看用户手册，查看开发者手册与 API 文档等功能。在此给出事件列表和 Gui 设计，以指导第三周期中相关模块的开发者。

3.4.1 事件列表

事件	触发	事件源	行为	响应	事件宿
用户准备下载 HiSA	用户点击主页中的 **下载** 键	用户	跳转到下载页面	下载页面	用户
用户下载 HiSA	用户在下载页面点击需要下载的版本	用户	将文件传输到用户本地	用户选中的 HiSA 版本	用户
用户打开使用	用户点击主页	用户	跳转到使用手册	使用手册选择	用户

手册选择页面	中的 **使用手册** 键		选择界面	界面	
用户打开 API 文档页面	用户点击使用手册选择界面中的 **API 文档** 键	用户	跳转到 API 文档界面	API 文档界面	用户
用户打开开发者手册页面	用户点击使用手册选择界面中的 **开发者手册** 键	用户	跳转到开发者手册页面	开发者手册页面	用户
用户打开 Gui 使用手册页面	用户点击使用手册选择界面中的 **Gui 使用手册** 键	用户	跳转到 Gui 使用手册页面	Gui 使用手册页面	用户
用户打开命令行使用手册界面	用户点击使用手册选择界面中的 **命令行使用手册** 键	用户	跳转到命令行使用手册界面	命令行使用手册界面	用户
用户返回上一页	用户点击浏览器左上角的回退健	用户	如果用户当前在主页，那么不做任何操作，否则跳转到当前页面	主页或当前页面的上一页	用户

			的上一页		

3.4.2 界面设计

主页设计：

下载选择界面：

使用手册选择界面：

软件使用手册

使用手册

- GUI使用手册
- 命令行使用手册
- 开发者手册

命令行用户手册界面：

- 通过二进制文件安装hisa
  - Windows
  - Linux
- 从源码构建hisa
  - Windows
  - Linux
- 命令行
  - 命令列表
  - 使用示例
    - 我只想打印帮助信息或现有的检查器列表
    - 我想检测我的项目源码，它位于/proj/src
    - 但我不想检测所有的文件，只想检测其中几个源文件
    - 我还希望能输出全面的信息
    - 可我只想检测特定的缺陷
    - 我是Checker的开发者，我该如何debug我的Checker?
    - 我想使用Clang Static Analyzer
- 交互式命令行环境REPL
  - 命令列表
  - 使用示例
  - 行为约定

通过二进制文件安装hisa

Windows

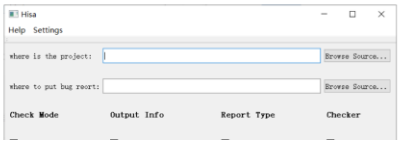
在windows已经安装clang/llvm的前提下，下载二进制文件压缩包后，将exe可执行文件解压缩后即可运行。

Gui 用户手册界面：

- Gui
  - 界面概览
  - 帮助
  - 设置
    - 语言转换
    - 历史记录
    - 恢复默认设置
  - 使用示例:
    - Windows下生成compile_commands.json
    - 选择输入输出地址
    - 自定义设置
    - 进行分析
  - 异常
    - execution error/执行错误

Gui

界面概览



开发者手册界面：

开发者手册

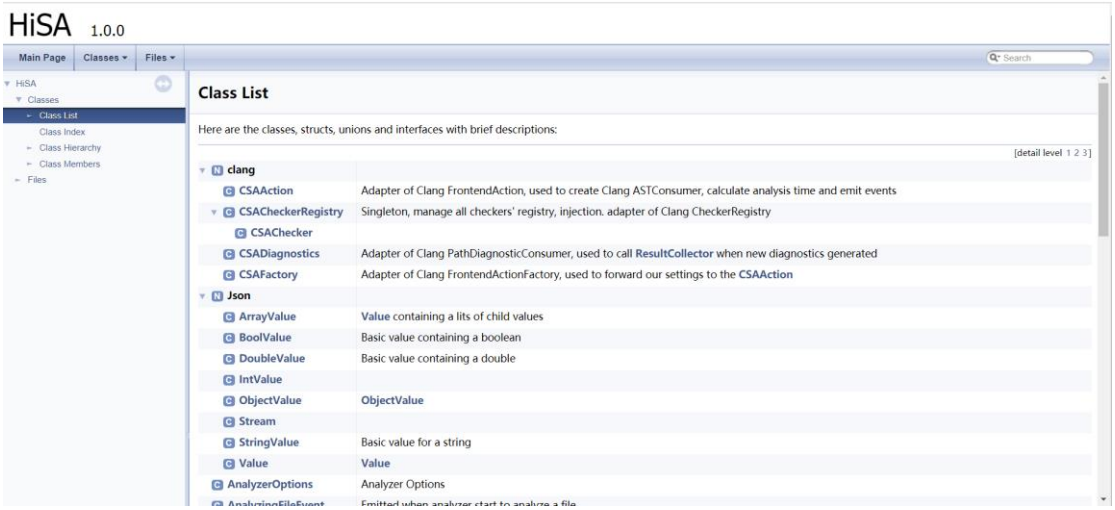
以下简称Clang Static Analyzer为CSA，相关接口见API文档

框架

设计原则

- 屏蔽Clang繁琐的调用流程，使得在基于本框架开发时仅需要CSA相关知识
- Make Life Easier

API 文档：



介绍界面：

4 结语

4.1 第三周期预期目标

第三周期的预期目标为：增强项目的核心检测功能，使其可以在有限时间内完成对百万行级别 C++/C 项目的检测。同时完成 Gui 功能的拓展和官方网站的开发。并对新增功能编写详细的设计文档并完成相应的测试工作。

4.2 项目未来发展方向

在第三周期结束后项目会进入收尾阶段，团队成员将着手整合之前编写的文档资料，准备各自的答辩材料和最终的项目验收材料，做好准备进入项目答辩阶段。