

原创 如何用clang analyzer定制静态分析规则（2）创建定制规则库篇

2017-04-21 17:27:06 喜欢冒险的松鼠 阅读量 609 更多

版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。

本文链接：<https://blog.csdn.net/u012448058/article/details/70332536>

如何用clang analyzer定制静态分析规则（2）创建定制规则库篇

在上一篇《工程配置篇》里，我们已经了解了如何下载llvm和clang的源码，如何生成Xcode工程并完成编译，现在就开始定制自己的静态分析规则。首先要明确的两点，一是clang自己的build target基本是静态链接的，但我们要做的是独立发布、独立加载的规则库，必须做成动态链接。二是全依赖clang提供的能力，考虑到开发、调试的方便，规则库工程将被建立在clang工程下。

我们实现的机制是应用了clang plugin机制，可参考<http://clang.llvm.org/docs/ClangPlugins.html>。具体到静态分析规则开发，可以使用更简单的check plugin，详细原理会在后面阐述，此处暂只先说工程搭建。

1、CMake配置

clang analyzer的源码在

```
1 ~/projects/analyzer/llvm/tools/clang/lib/StaticAnalyzer
```

规则库工程就建立在这里。

为了跟其他target保持一致，先创建CMake配置：

target名：clangSquirrelCheckers

规则库包含文件列表：

SuspiciousSizeofChecker.cpp（规则路径：“ squirrel.defect.SuspiciousSizeof”）

```
1 ~/projects/analyzer/llvm/tools/clang/lib/StaticAnalyzer
2 |-- CMakeLists.txt
3 |-- Checkers
4 |   |-- .....
5 |   `-- .....
6 |-- Core
7 |   |-- .....
8 |   `-- .....
9 |-- Frontend
10 |   |-- .....
11 |   `-- .....
12 |-- README.txt
13 `-- SquirrelCheckers
14     |-- CMakeLists.txt
15     `-- SuspiciousSizeofChecker.cpp
```

```
1 #~/projects/analyzer/llvm/tools/clang/lib/StaticAnalyzer/SquirrelCheckers/CMakeLists.txt
2
3 IF (${CMAKE_SYSTEM_NAME} MATCHES "Darwin")
4     SET(CMAKE_SHARED_LINKER_FLAGS "-undefined dynamic_lookup")
5 ENDIF()
6
7 add_clang_library(clangSquirrelCheckers
8     SuspiciousSizeofChecker.cpp
9
10     SHARED
11 )
```

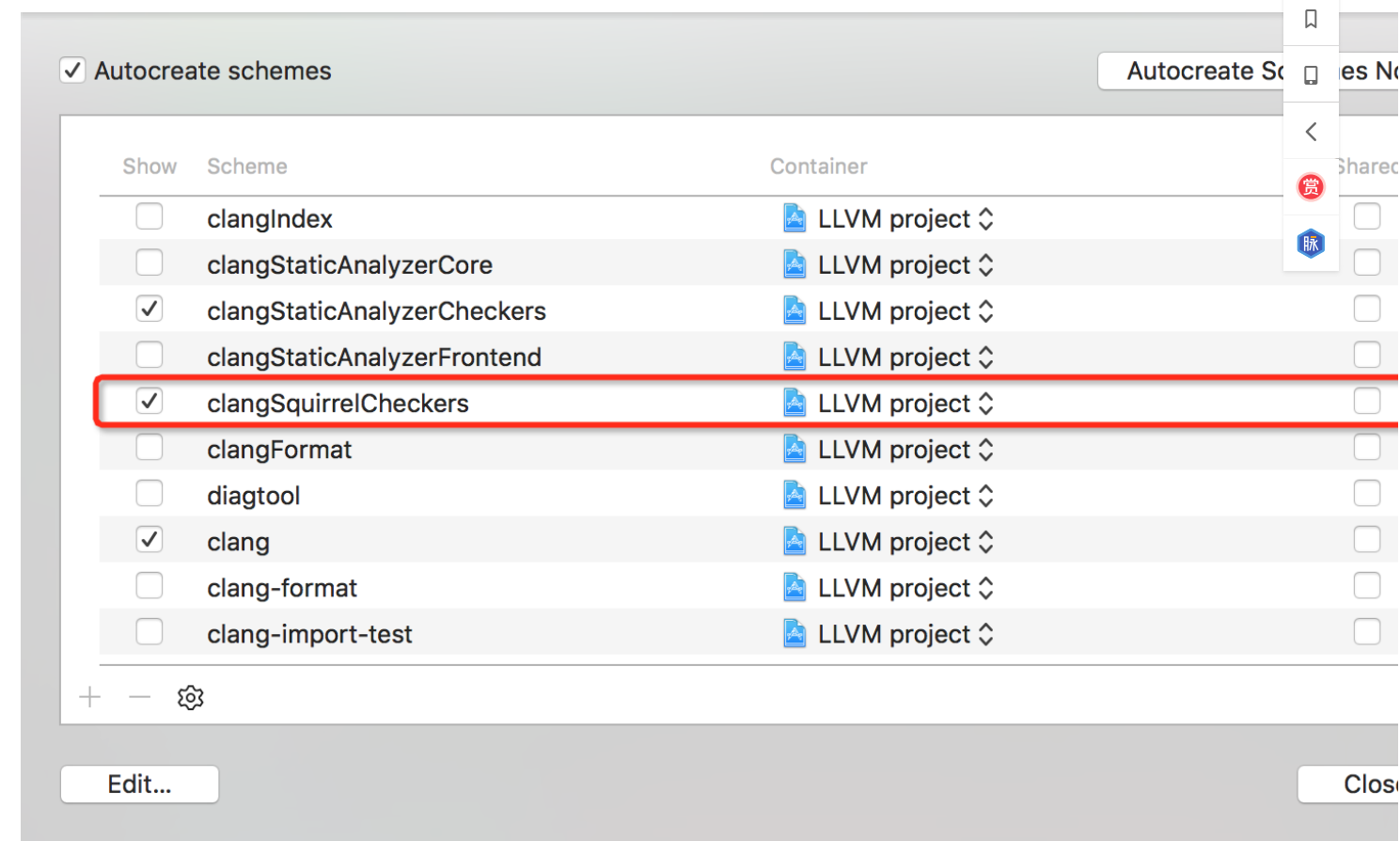
这里要备注的是，add_clang_library是clang定义的一个宏，在

```
1 ~/projects/analyzer/llvm/tools/clang/cmake/modules/AddClang.cmake
```

我们需要创建动态链接的.dylib，所以使用了SHARED。

2、Xcode工程

按照前文《工程配置篇》里的步骤，Xcode工程打开时会多了一个scheme clangSquirrelCheckers。



直接Build，在Debug/lib（根据Build configuration）下就可以得到libclangSquirrelCheckers.dylib

3、使用

clang的plugin可以通过 `-load ooxx.dylib` 来加载。之后，便像内置扫描规则一样使用。例如：
可以检查定制规则是否正常加载

```
1 clang -cc1 -load ~/projects/analyzer/build/Debug/lib/libclangSquirrelCheckers.dylib -analyzer-checker-help
```

可以直接用于扫描

```
1 clang -cc1 -load ~/projects/analyzer/build/Debug/lib/libclangSquirrelCheckers.dylib -analyze ooxx.cpp
```

4、源码

本系列文章源码可见 <https://github.com/squirrel-explorer/eagleeye-ios>。

2、3年经验的切图仔，如何把开发思维提前 5 年？



beswkwangbo

106篇文章

排名:千里之外

关注



电影旅行敲代码

77篇文章

排名:千里之外

关注



adream307

500篇文章

排名:1000+

关注

Clang 静态分析(Static Analyzer)工具使用的总结 - bes..._CSDN博客

clang static analyzer源码分析(三) - 电影旅行敲代码 - CSDN博客

MySQL命名、设计及使用规范-----来自标点符的《MySQL命名、设计及使用规范》

阅读数 225

原文地址: http://www.biaodianfu.com/mysql-best-practices.html 最近在看MySQL相关的内容... 博文 | 来自: BuildingJiang...

深入研究Clang（三） libclang

阅读数 1万+

libclang是一个提供了C接口的一个库，它让你可以轻松的把clang作为一个库去使用，这样的做法带来... 博文 | 来自: SHINING的博客

[Linux]使用Clang实现代码静态分析 - weixin_33755557的博客 - ...

如何用clang analyzer定制静态分析规则(1)工程配置篇 -..._CSDN博客

使用XCode Clang(静态分析器)发现内存泄露

阅读数 88

XCode中引入了静态分析器,用于发现普通编译错误以外的错误选择Build->BuildandAnalyze... 博文 | 来自: weixin_34226...

数据分析师究竟有多少大企在抢？

优秀的数据分析程序员需要具备什么样的技术水平~ 学院 | 讲师: CSDN

深入研究Clang(十一) 使用libclang遍历AST

阅读数 3861

之前在本系列的第三篇（深入研究Clang（三） libclang）介绍过libclang，内容相对简单，也没有实际... 博文 | 来自: SHINING的博客

如何基于规则引擎打造规则库

阅读数 8993

规则引擎是面向技术人员的工具。目前技术人员为什么会选择规则引擎来使用，主要是基于如下情形来... 博文 | 来自: joeyshi的专栏

浅谈GCC/Clang生成和链接静态库/动态库

阅读数 7230

为了方便下面的讲解，先写两个C++源文件，代码如下：12345//add.cppint add(int a, int b){ retu... 博文 | 来自: x_studying的...

clang++编译器使用

阅读数 1万+

编译过程通常的程序需要经过预处理阶段，编译阶段，汇编阶段,链接阶段-预处理阶段：预处理阶段对... 博文 | 来自: bleedingfight...

cmake 查看编译选项

阅读数 1276

cmake.-LH 博文 | 来自: 犯了错的小孩

羡慕AI高薪岗！为什么这类程序员不建议大家转型？

被众多开发工程师羡慕的AI程序员为啥这么高薪！30w只是白菜价有啥要求？ 学院 | 讲师: CSDN

clang static analyzer源码分析（一）

阅读数 9374

引子clang静态代码分析是clang相对于gcc一个比较能够引起关注的点，特别是clang静态代码分析基于... 博文 | 来自: 电影旅行敲代码

《自己动手设计数据库》第11章 定义和建立业务规则

阅读数 1573

根据业务需要定义和建立业务规则，并将其体现在数据库中 博文 | 来自: TROUBLE I A...

clang static analyzer源码分析（二）

阅读数 3631

clangstaticanalyzer源码分析（二），主要介绍ExplodedGraph的概念以及对clangstaticanalyzer进... 博文 | 来自: 电影旅行敲代码

clang语法检查设置

阅读数 2053

clang语法检查设置使用clang进行语法检查非常方便，不用像pclint那样需要一大堆的配置。控制台命... 博文 | 来自: robin_chenyu...

Python从小白到大牛

图书视频源代码讲师专属答疑群

关闭

🔊


🔇


https://blog.csdn.net/u012448058/article/details/70332536


4/9


windows平台下clang_checker的使用	阅读数 1865
Windows平台下ClangChecker的使用写在最前为什么要写这篇博客呢，因为最近的一个项目涉及到了...	博文 来自: tuqinag的专栏
这个双十一，程序员应该屯点什么课？	
CSDN课程《Python数据分析高效特训》，专题模块+班主任督学+直播强化训练	学院 讲师: CSDN
parasoft Jtest 使用教程：代码规范静态分析Suppressions（禁止）概念解析	阅读数 764
今天给大家带来parasoftJtest中非常重要的代码规范静态分析Suppressions（禁止）两点概念解析，...	博文 来自: zjj32的博客
初学者的静态分析挑战writeup2	阅读数 36
题目来源至https://www.malwaretech.com/beginner-malware-reversing-challenges所有挑战都是...	博文 来自: onionsec
Clang 之旅--实现一个自定义检查规范的 Clang 插件	阅读数 36
Clang之旅系列文章：Clang之旅--使用Xcode开发Clang插件Clang之旅--[翻译]添加自定义的attribut...	博文 来自: weixin_33832...
Clang中的重构操作规则需求(RefactoringActionRuleRequirement)简介	阅读数 49
1.Clang中目前存在的重构操作规则需求继承关系如下：一个重构操作规则需求(RefactoringActionRul...	博文 来自: 梦在哪里的博客
程序员实用工具网站	阅读数 17万+
目录1、搜索引擎2、PPT3、图片操作4、文件共享5、应届生招聘6、程序员面试题库7、办公、开发软...	博文 来自: 不脱发的程序猿
反转！BAT编程吸金榜来了，AI程序员刷爆了.....	
2019年BAT等大厂积极布局AI领域，程序员转行学AI的门槛是什么？怎么转？	学院 讲师: CSDN
程序员真是太太太太有趣了！！	阅读数 5万+
网络上虽然已经有了很多关于程序员的话题，但大部分人对这个群体还是很陌生。我们在谈论程序员的...	博文 来自: 程序猿DD
1行Python代码制作动态二维码	阅读数 1万+
目录1、普通二维码2、艺术二维码3、动态二维码在GitHub上发现了一个比较有意思的项目，只需要一...	博文 来自: 不脱发的程序猿
全球最厉害的 14 位程序员！	阅读数 8652
来源 ITWorld整理自网络全球最厉害的14位程序员是谁？今天就让我们一起来了解一下吧，排名不分先...	博文 来自: GitHubDaily
从入门到精通，Java学习路线导航	阅读数 6万+
引言最近也有很多人来向我“请教”，他们大都是一些刚入门的新手，还不了解这个行业，也不知道从何...	博文 来自: wangweijun
我花了一夜用数据结构给女朋友写个H5走迷宫游戏	阅读数 15万+
起因又到深夜了，我按照以往在csdn和公众号写着数据结构！这占用了我大量的时间！我的超越妹妹严...	博文 来自: bigsai
程序员连拿3份Offer，每份工资竟超出原来薪资5万，这几点分享给你！	
作为一名老码农！Python 116K 超过 C++，薪酬排行第一	学院 讲师: CSDN
别再翻了，面试二叉树看这 11 个就够了~	阅读数 6万+
写在前边数据结构与算法：不知道你有没有这种困惑，虽然刷了很多算法题，当我去面试的时候，面试...	博文 来自: 一个不甘平凡...
接班马云的为何是张勇？	阅读数 3万+
上海人、职业经理人、CFO背景，集齐马云三大不喜欢的张勇怎么就成了阿里接班人？作者 王琳本文经...	博文 来自: CSDN资讯
什么是大公司病（太形象了）	阅读数 7822
点击蓝色“五分钟学算法”关注我哟加个“星标”，天天中午12:15，一起学算法作者 南之鱼来源 芝麻...	博文 来自: 程序员吴师兄...
让程序员崩溃的瞬间（非程序员勿入）	阅读数 21万+
今天给大家带来点快乐，程序员才能看懂。来源：https://zhuanlan.zhihu.com/p/470665211.公司实...	博文 来自: strongerHuang
离职了	阅读数 4072
这是我毕业后的第一份工作...面试时，HR小姐姐告诉我...然鹅...我入职之后才发现：对标阿里的只有加...	博文 来自: 嵌入式Linux


<div>nginx学习，看这一篇就够了：下载、安装。使用：正向代理、反向代理、负载均衡。常用命令...</div> <div>文章目录前言一、nginx简介1. 什么是 nginx 和可以做什么事情2.Nginx 作为 web 服务器3. 正向代理4...</div>	阅读数 3788	博文
<div>动画：用动画给面试官解释 TCP 三次握手过程</div> <div>作者 小鹿 来源 公众号：小鹿动画学编程 写在前边 TCP 三次握手过程对于面试是必考的一个，所以...</div>	阅读数 3万+	博文
<div>JAVA实现商品信息管理系统</div> <div>任务与实现 超市商品管理系统 题目要求 超市中商品分为四类，分别是食品、化妆品、日用品和饮料。...</div>	阅读数 2918	博文
<div>500行代码，教你用python写个微信飞机大战</div> <div>这几天在重温微信小游戏的飞机大战，玩着玩着就在思考人生了，这飞机大战怎么就可以做的那么好，...</div>	阅读数 5万+	博文
<div>2019诺贝尔经济学奖得主：贫穷的本质是什么？</div> <div>2019年诺贝尔经济学奖，颁给了来自麻省理工学院的 阿巴希·巴纳吉（Abhijit Vinayak Banerjee）、...</div>	阅读数 1万+	博文
<div>linux：最常见的linux命令（centOS 7.6）</div> <div>最常见，最频繁使用的20个基础命令如下： 皮一下，这都是干货偶，大佬轻喷 一、linux关机命令： 1....</div>	阅读数 1万+	博文
<div>只因写了一段爬虫，公司200多人被抓！</div> <div>“一个程序员写了个爬虫程序，整个公司200多人被端了。” “不可能吧！” 刚从朋友听到这个消息的...</div>	阅读数 10万+	博文
<div>别在学习框架了，那些让你起飞的计算机基础知识。</div> <div>我之前的文章，写的大部分都是与计算机基础知识相关的，这些基础知识，就像我们的内功，如果在...</div>	阅读数 5万+	博文
<div>java学习路线导航【教学视频+博客+书籍整理】</div> <div>在博主认为，学习java的最佳学习方法莫过于视频+博客+书籍+总结，前三者博主将淋漓尽致地挥毫于...</div>	阅读数 7613	博文
<div>五款高效率黑科技神器工具，炸裂好用，省时间</div> <div>loonggg读完需要4分钟速读仅需2分钟感觉我好久好久没有给大家分享高质量的软件和插件了。今天周...</div>	阅读数 2万+	博文
<div>程序员必须掌握的核心算法有哪些？</div> <div>由于我之前一直强调数据结构以及算法学习的重要性，所以就有一些读者经常问我，数据结构与算法应...</div>	阅读数 6万+	博文
<div>SQL基本语法入门 看这里就够了</div> <div>SQL执行顺序 第一步：执行FROM 第二步：WHERE条件过滤 第三步：GROUP BY 分组 第四步：执行...</div>	阅读数 4584	博文
<div>如何优化MySQL千万级大表，我写了6000字的解读</div> <div>这是学习笔记的第2138篇文章 千万级大表如何优化，这是一个很有技术含量的问题，通常我们的直觉...</div>	阅读数 3万+	博文
<div>面试最后一问：你有什么问题想问我吗？</div> <div>尽管，我们之前分享了这么多关于面试的主题： 高薪必备的一些Spring Boot高级面试题 面试必问：设...</div>	阅读数 3万+	博文
<div>python 程序员进阶之路：从新手到高手的100个模块</div> <div>在知乎和CSDN的圈子里，经常看到、听到一些 python 初学者说，学完基础语法后，不知道该学什么...</div>	阅读数 4万+	博文
<div>Python——画一棵漂亮的樱花树（不同种樱花+玫瑰+圣诞树喔）</div> <div>最近翻到一篇知乎，上面有不少用Python（大多是turtle库）绘制的树图，感觉很漂亮，我整理了一下...</div>	阅读数 3万+	博文
<div>Linux/C/C++ 不可错过的好书</div> <div>来源：公众号【编程珠玑】 作者：守望先生 ID：shouwangxiansheng 前言 经常有读者让我推荐书籍...</div>	阅读数 8171	博文
<div>史上最强Tomcat8性能优化</div> <div>文章目录授人以鱼不如授人以渔目的服务器资源Tomcat配置优化Linux环境安装运行Tomcat8AJP连接...</div>	阅读数 2万+	博文
<div>单点登录（SSO）</div> <div>一、SSO（单点登录）介绍 SSO英文全称Single SignOn，单点登录。SSO是在多个应用系统中，用户...</div>	阅读数 1万+	博文


0




















《Python从小白到大牛》

图书视频源代码讲师专属答疑群

关闭





阅读数 2万+

今天这篇文章，讲通过对话的形式，让你由浅入深知道，为什么 Https 是安全的。一、对称加密 —...

博文

阅读数 9898

启动与停止 启动mysql服务 `sudo /usr/local/mysql/support-files/mysql.server start` 停止mysql服务...

博文

阅读数 1万+

可能很多人在大一的时候，就已经接触了递归了，不过，我敢保证很多人初学者刚开始接触递归的时候...

博文

阅读数 1万+

数据结构与算法是我在大学里第一次接触到的，当时学了很多其他安卓、网页之类的，一开始就感觉纳...

博文

阅读数 1万+

从业五年多，辗转两个大厂，出过书，创过业，从技术小白成长为基层管理，联合几个业内大牛回答下...

博文

阅读数 5万+

最近，有关程序员因为参与某些项目开发导致被起诉，甚至被判刑的事件发生的比较多：某程序员因为...


博文

阅读数 1万+

什么是TCP/IP协议? 计算机与网络设备之间如果要相互通信,双方就必须基于相同的方法.比如如何探测...

博文

c# mvc 上传 文件 c#扫描软件 c# 文字打印左右反转 c#byte转换成数字 c# 音量调节组件 c# wpf 界面 c# 读取证书文件的
内容 c# 单例模式 工厂模式 c# dgv 树结构 c#继承 反序列化



喜欢冒险的松鼠

TA的个人主页 >

私信

关注

原创	粉丝	获赞	评论	访问
4	0	0	0	4374

等级:

博客 1

周排名:
 47万+

积分:
 84

总排名:
 46万+

最新文章

如何用clang analyzer定制静态分析规则
 (1) 工程配置篇

从lombok到UAST – 浅谈Android Lint的
 AST Parser (2)

从lombok到UAST – 浅谈Android Lint的
 AST Parser (1)

《Python从小白到大牛》
图书·视频·源代码·讲师专属答疑群
关闭

分类专栏

静态代码扫描

3篇

归档

2017年4月

3篇

2017年3月

1篇

热门文章

如何用clang analyzer定制静态分析规则（1）工程配置篇

阅读数 2078

从lombok到UAST – 浅谈Android Lint的AST Parser（1）

阅读数 1022

从lombok到UAST – 浅谈Android Lint的AST Parser（2）

阅读数 671

如何用clang analyzer定制静态分析规则（2）创建定制规则库篇

阅读数 607



数据可视化



CSDN学院



CSDN企业招聘

QQ客服

kefu@csdn.net

客服论坛

400-660-0108

工作时间 8:30-22:00

关于我们 | 招聘 | 广告服务 | 网站地图

百度提供站内搜索 京ICP备19004658号

©1999-2019 北京创新乐知网络技术有限公司

网络110报警服务


经营性网站备案信息


北京互联网违法和不良信息举报中心


中国互联网举报中心


家长监护


版权申诉


0




















《Python从小白到大牛》

图书视频源代码讲师专属答疑群

关闭



