2018开源静态分析工具-第三部分-go

niexinming / 2018-10-26 07:58:00 / 浏览数 3055 安全工具 工具 顶(0) 踩(0)

翻译自： https://medium.com/@prasincs/open-source-static-analysis-for-security-in-2018-part-3-go-8018507568bb
翻译：聂心明
在过去三年里，我一直用GO做全职开发，期间只休息了一小段时间。我非常喜欢这个语言，因为它有很好的系统类型，安全，支持并发高和我不断处理的性能问题。我最喜
https://blog.cloudflare.com/building-the-simplest-go-static-analysis-tool/ ）。它对各种开发环境都很友好，无论工程师们使用的是Vi，VS
Code，Goland，Emacs，都可以使用goimports，使用gofmt格式化代码，并且你也会看到，可以使用类似的工具去分析静态代码。

Gometalinter

Go Metalinter（ https://github.com/alecthomas/gometalinter ）是本文的TLDR版本--如果你喜欢kitchensink带给你的一切体验，用go
metalinter也足够可以检查所有的代码。当你用VS Code写Go项目的时候，VS Code也会安装一系列不错的工具。下面的代码是教你如何使用metalinter。

```
go get alecthomas/gometalinter
#Install the packages
gometalinter --install
gometalinter ./...
```

如果你不喜欢shebang的方法，我将介绍一些其他的工具

gas

Go AST Scanner（ http://github.com/GoASTScanner/gas
）是一个非常好的项目，它可以帮你找到你项目中是否使用MD5，或者你的项目中使用了rand而不是crypto/rand这个包。还可以发现其他类似的东西。
你可以运行下面的代码快速的使用这个工具

```
go get github.com/GoASTScanner/gas/cmd/gas/...
gas ./...
```

另外，你也可以过滤不同的错误类型，如果你希望使用gas标记一些事情，你可以使用#nosec这个标记来避免警告。通常，你最好为#nosec添加一些注释，目的是告诉下一

safesql

Safesql (https://github.com/stripe/safesql)可以检测出有sql注入的代码--确保用户输入的数据不会导致sql注入攻击。

goreportcard

总之，当我使用 Goreportcard（ https://github.com/gojp/goreportcard
）检查开源项目的时候，我觉得这个项目很浮夸。它会运行几个工具给你的项目打分，然后输出为一个web页面。
我用它检查过一个重要的开源项目，这个开源项目的分数是96%。它不会让你的项目变的更安全，但是如果能得到100%也是很开心的。

go vet/test

`go vet` 是我最喜欢的用go写的工具，但是它在`go 1.10`这个环境中会遇到很多问题，这样会打乱你的测试。

dingo-hunter

我没有在特别复杂地非学术项目上运行过 dingo hunter（ https://github.com/nickng/dingo-hunter ）
，但这个是一个静态分析器，用来建模并发和寻找死锁。它模型的核心代码是Haskell，并且背后还有一些我不能理解的数学计算的模块。
你可以在 https://github.com/mre/awesome-static-analysis 找到更多用于go语言的静态分析器，你也可以自己写一个，这其实很容易。:)

上一篇：CVE-2018-4338：在MA... 下一篇：安恒杯秋季选拔赛部分题目WP

1. 0 条回复
   - 动动手指，沙发就是你的了！

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板