2018开源静态分析工具-第一部分-python

niexinming / 2018-10-22 22:27:45 / 浏览数 2054 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-1-python-348e9c1af1cd
翻译：聂心明
我对静态分析工具的态度是即爱也恨。我喜欢他们，我使用他们并且在他们运行停止之前，我都无法交付产品。并且我讨厌他们，因为我目前对"安全和合规"的工作定义的相

这篇文章包含4种编程语言，这四种语言在我们公司中非常重要，但这并不意味着我们不用其他的语言。但这至少可以让我们对这些语言有一个很好的了解。我发现静态扫描
下面的语言我都会讲到，这篇文章我先讲python

- python
- java
- go
- JavaScript

目标不是那么完全，但是却很实用

精确度：这个工具会有很多误报吗？以至于工程师最好的办法就是禁用它。
实践性：这个工具会给我很多可实践的建议和例子吗？
集成性：我能和我现有的工具搭配使用吗？
可维护性：我不知道未来会发生什么，但是这个工具的可维护性怎么样？或者它是否有足够好的文档，以至于可以让我自己可以维护它？

资源：
这里有一份资源列表，里面包含了更多语言的静态分析工具:
https://github.com/mre/awesome-static-analysis

python

从静态分析的角度来看，python是一个有趣的语言，它有AST包，但是很多代码可以在运行时被改变。围绕"pythonic"化的想法是存在的并且频繁的代码检查可能会发现一

1. 检查你的requirements.txt

在2018年，几乎所有的python代码被运行和部署在虚拟环境中。这意味着，上游的依赖全部被记录在requirements.txt中。如果你没有这样做，请停下来，然后按照下面的
http://docs.python-guide.org/en/latest/dev/virtualenvs/

我们使用safety（ https://github.com/pyupio/safety
）去检查我们的requirements.txt，到目前为止，他已经发现了很多有漏洞的上游库。只要可能，我们尽可能要使用最新版本的包。但是我不推荐这种方法。这虽然增加了很
精确性：你能信任 https://github.com/pyupio/safety-db ？
实践性：这是伟大的，通常只要PyPi包升级是可用的，我们就能升级。
集成性：文件可以被方便的导入并且我们仅仅在我们的项目中运行一些的指令就可以了，只要发现有漏洞的包，它都会让项目的创建停止，并且报告错误。这也给工程师提供

```
safety check -r $TOPDIR/requirements.txt --full-report --json > $TOPDIR/safety-report.json
if [[ $open_vulnerabilities -gt 0 ]]; then
  echo "$open_vulnerabilities open known vulnerabilities exist in packages, failing build"
  safety check -r $TOPDIR/requirements.txt --full-report
  exit 1
fi
```

可维护性：如果safety-db可行的话，我不知道为什么有些人或者有些组织不想拥有它。而且，为啥PyPI不做这个事情。

2.检查你的代码

所以上游的任何代码都没已知的漏洞，很好。现在让我在我的代码上运行bandit（ https://github.com/openstack/bandit
）。这个工具可以解析你的python代码并且允许你去选择要检查的错误类型。如果有一些误报，你可以用#nosec忽略这块代码。

准确性：我发现在我测试的代码中都是相对准确的。
实践性：这给要特别注意，无论怎样，工具提供多种方式去导出成不同的格式并且可以用`-lll`提高严格性，并且可以用`-iii`提高可信度。所以你如果想看最严格的情况和最

```
bandit -lll -iii -r dir
```

集成性：你可以使用`-f`这个标志把结果导出成csv,html,json,screen,txt或者xml。如果你想去分类，解说，或者导入JIRA中，这个功能都是非常有用的。
可维护性：这看上去对我非常友好，这个项目被Openstack 管理并且它支持在自己的AST中做hook。所以我能看到更多新的应用场景。
明天，我将讨论关于Java代码静态分析工具的古往今来。

上一篇：Phar与Stream Wrapp... 下一篇：soap导致的SSRF
1. 0 条回复

- 动动手指，沙发就是你的了！

登录 后跟帖

先知社区

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