SYNOPSYS®

Code Sight

编写代码时快速高效地查找修复应用安全缺陷

优势

易于使用

- 通过直观的IDE扩展UI，仅需几分钟即可完成安装，并开始修复代码和开源依赖问题
- 自动扫描功能，可以针对打开、保存或编辑的文件中的代码问题发送警报更可靠的代码

Better code

- 在签入代码之前修复问题，从而实现左移
- 解决源代码、开源依赖、API调用、加密、基础架构即代码等方面的问题
- 直接在IDE中提供的清晰准确的修复指南，告知需要修复什么以及如何修复提高生产力

提高生产力

- 通过针对IDE优化的扫描实现实时代码分析
  - WebGoat只需3秒
  - ApacheHadoop只需10秒（800个文件和100万行代码）
- 通过尽早发现缺陷 — 而不是在后期下游测试期间 — 来避免代价高昂的返工

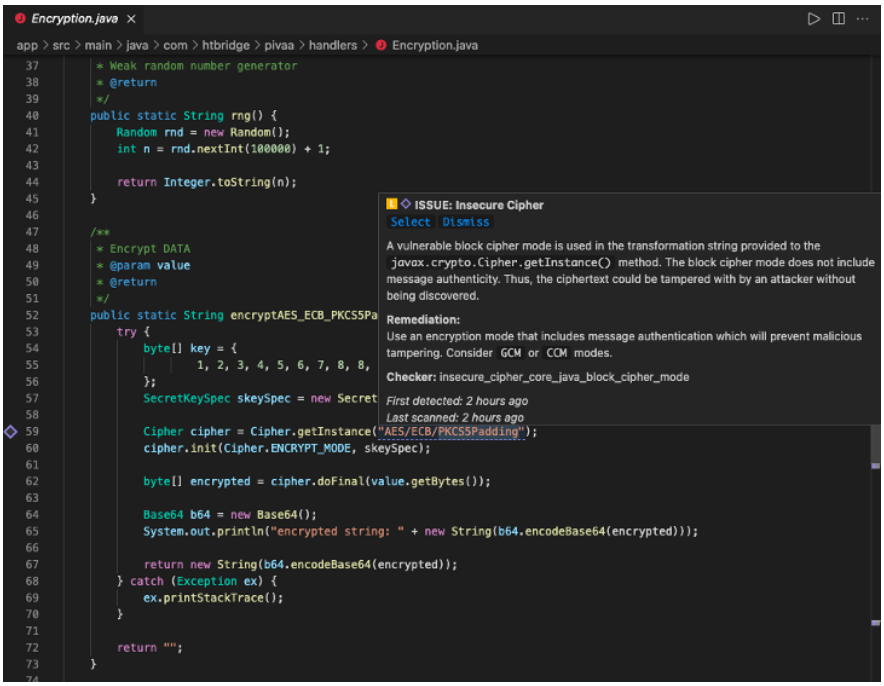
概述

CodeSight™是基于IDE的应用安全解决方案，可以帮助您在编写代码时快速高效地发现并修复安全问题，无需切换工具或中断工作流。 Code Sight将静态应用安全测试(SAST)和软件组成分析(SCA)结合在一起，可以针对以下问题提供实时警报和查看：

- 代码中的安全漏洞(CWE)
- 开源依赖项中的已知漏洞(CVE)
- 不安全的基础架构即代码(IaC)配置
- 潜在的机密/敏感数据泄露风险
- 易受攻击的API使用

Code Sight速度极快，可在几秒内分析大型代码库。 IDE中直接提供的详细修复指南可以帮助您快速修复问题，编写更可靠的代码。

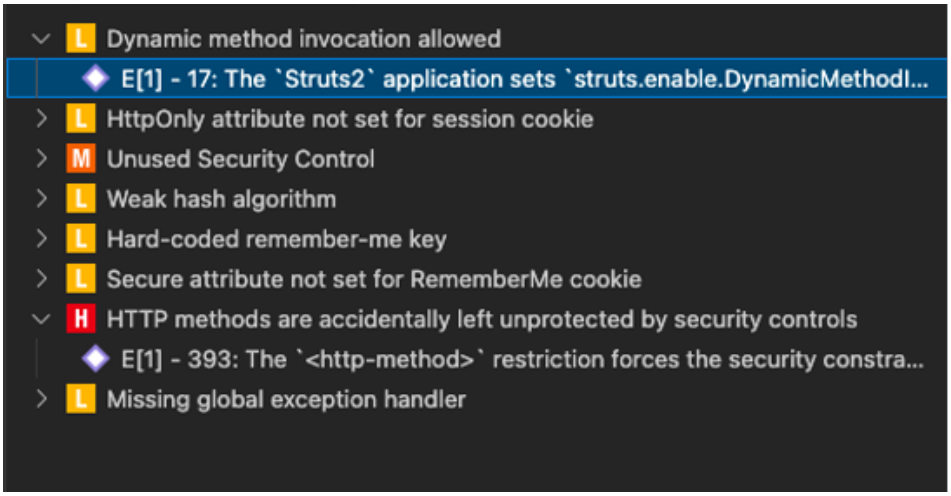
CodeSight还补充和提高了集成在CI管道或作为QA一部分执行的集中式AST分析的效力。 它使您能够在签入代码之前修复缺陷，从而避免因直到后期下游测试才发现漏洞而导致代价高昂的返工。



CodeSight标准版的功能

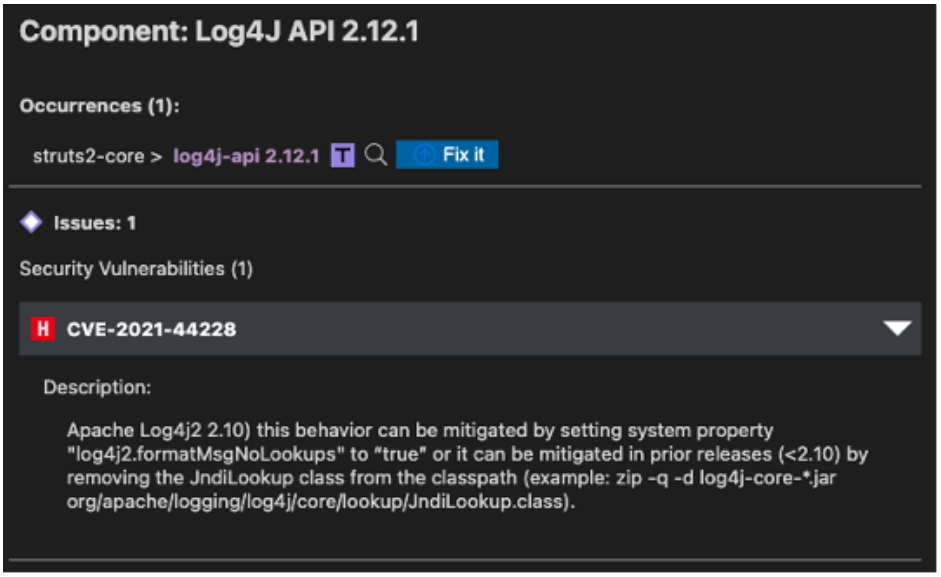
集成静态分析

- CodeSight可以在编写代码时自动扫描和分析源代码和基础架构即代码文件。
- 检测到的问题将直接在编辑器窗口突出显示，以便于识别。
- 只需将鼠标悬停在突出显示的代码行上，便可以看到包括问题描述和修复指南在内的详细信息。
- 只需一步单击操作，便可以对多个漏洞应用推荐的代码修复。



集成软件组成分析

- CodeSight能够识别出直接的和间接的开源依赖项中的已知安全漏洞。
- 直接在IDE中查看漏洞描述以及CVE和/或Black Duck Security Advisory ID。
- 基于CVSS评分的严重级别信息可以帮助快速决定优先解决哪些问题。
- 修复指南可以帮助您选择问题组件的下一个无漏洞或低风险版本。



Code Sight标准版 | 技术指标

IDE和语言

IDE

- Visual Studio Code

语言

- Java
- JavaScript
- TypeScript

IaC平台和文件格式

平台

- AWS CloudFormation
- ELK
- Helm
- Kubernetes
- Terraform

文件格式

- HCL (Terraform)
- HTML
- JSON
- JSX
- Properties
- TOML
- TSX
- Vue
- XML
- YAML

当与Coverity® SAST或Black Duck® SCA结合使用时，Code Sight可以提供额外的语言和IDE支持。

本文适用于Code Sight标准版2022.1.0及更高版本。

新思科技与众不同

新思科技提供集成解决方案，可以改变您构建和交付软件的方式，在应对业务风险的同时加速创新。 我们提供市场上最全面的业界领先的软件安全产品和服务组合，并可与第三方和开源工具互操作，从而允许企业利用现有投资来构建最能满足其需求的安全程序。 只有新思科技能够满足您在构建可信软件时的一切需求。

有关新思科技软件完整性小组的更多信息，请访问我们的网站：www.synopsys.com/software.。

Synopsys, Inc.
690 E Middlefield Road
Mountain View, CA 94043 USA

美国销售热线：800.873.8193
国际销售热线：+1 415.321.5237
电子邮件：sig-info@synopsys.com