

Code Sight™ IDE Plug-in

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, 从而实现在左移
- 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
 - Apache Hadoop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

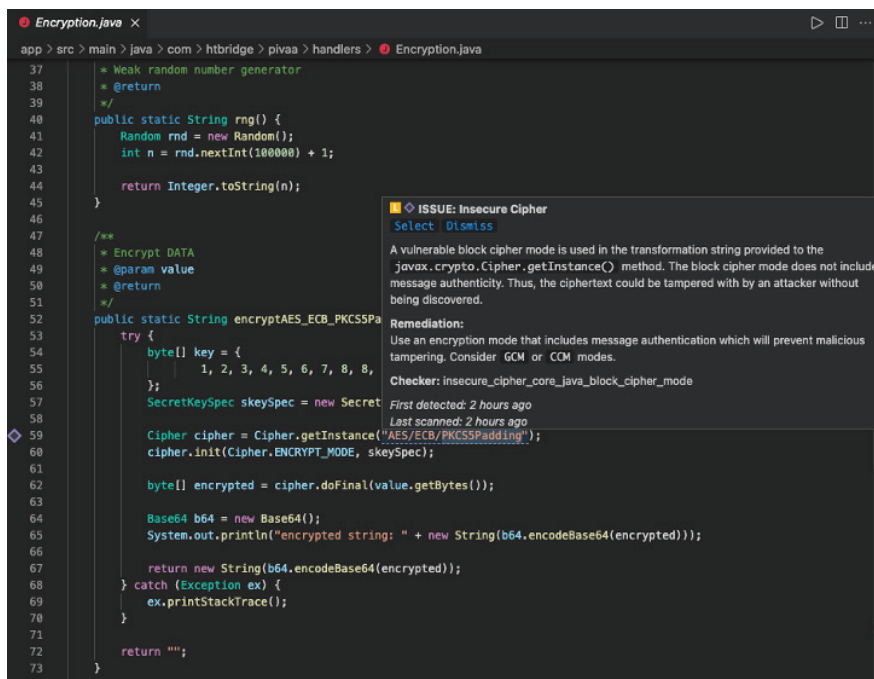
概述

Code Sight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 workflow。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。

Code Sight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。



```
Encryption.java x
app > src > main > java > com > htbridge > pivaa > handlers > Encryption.java
37  * Weak random number generator
38  * @return
39  */
40  public static String rng() {
41      Random rnd = new Random();
42      int n = rnd.nextInt(100000) + 1;
43
44      return Integer.toString(n);
45  }
46
47
48  /**
49   * Encrypt DATA
50   * @param value
51   * @return
52   */
53  public static String encryptAES_ECB_PKCS5Pa
54      try {
55          byte[] key = {
56              1, 2, 3, 4, 5, 6, 7, 8, 8,
57          };
58          SecretKeySpec keySpec = new Secret
59
60          Cipher cipher = Cipher.getInstance("AES/ECB/PKCS5Padding");
61          cipher.init(Cipher.ENCRYPT_MODE, keySpec);
62
63          byte[] encrypted = cipher.doFinal(value.getBytes());
64
65          Base64 b64 = new Base64();
66          System.out.println("encrypted string: " + new String(b64.encodeBase64(encrypted)));
67
68          return new String(b64.encodeBase64(encrypted));
69      } catch (Exception ex) {
70          ex.printStackTrace();
71      }
72
73      return "";
74  }
```

ISSUE: Insecure Cipher
Select Dismiss

A vulnerable block cipher mode is used in the transformation string provided to the `javax.crypto.Cipher.getInstance()` method. The block cipher mode does not include message authenticity. Thus, the ciphertext could be tampered with by an attacker without being discovered.

Remediation:
Use an encryption mode that includes message authentication which will prevent malicious tampering. Consider GCM or CCM modes.

Checker: insecure_cipher_core_java_block_cipher_mode

First detected: 2 hours ago
Last scanned: 2 hours ago

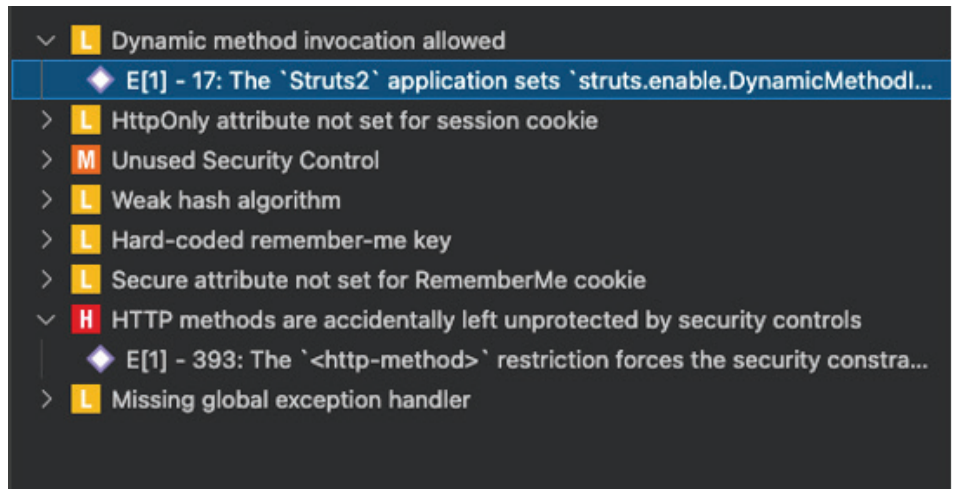
Code Sight 标准版的功能

集成静态分析

- Code Sight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

- Code Sight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® Static Analysis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。

Black Duck与众不同

Black Duck® 提供业界最全面、最强大、最值得信赖的应用安全解决方案组合。我们拥有无与伦比的专业知识和经验,来帮助世界各地的组织机构快速保护其软件,在其开发环境中高效集成安全性以及使用新技术进行安全创新。作为软件安全领域公认的领导者、专家和创新者, Black Duck拥有您构建可信软件所需的一切。如预了解更多信息,请访问www.blackduck.com。

©2024 Black Duck Software, Inc. 版权所有,保留所有权利。Black Duck 是 Black Duck Software, Inc.在美国和其他国家/地区的商标。本文提及的所有其他名称均为其各自所有者的商标或注册商标。2024年9月。