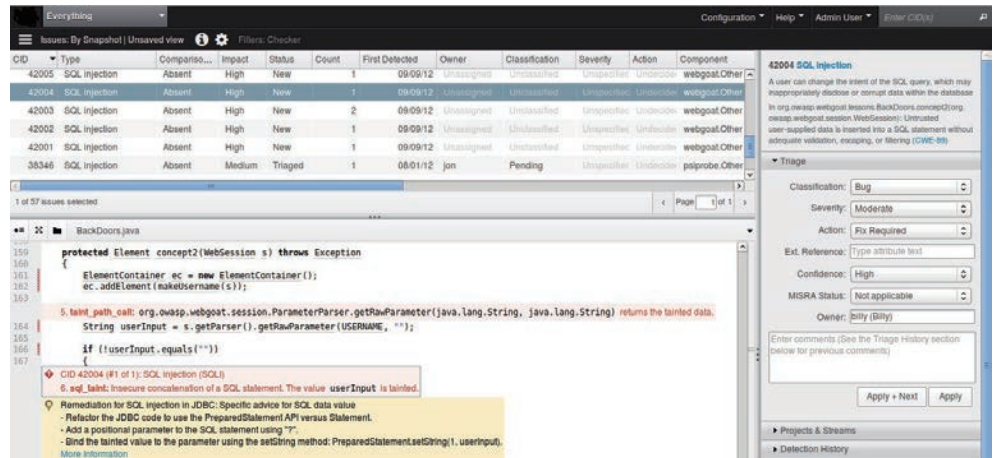


Coverity® 綜合靜態分析與應用安全測試 (SAST) ®

Synopsys 靜態分析軟體 (Coverity®) 是一款精確的綜合靜態分析與應用安全測試 (SAST) 平臺，它可以在編寫代碼時發現關鍵的缺陷和安全弱點，防止它們變成安全漏洞、故障或維護缺陷。



切實可行的修復指南幫助開發人員快速解決潛在的安全漏洞。

產品概述

Coverity 利用精確和有效的修復指南，基於專利技術以及對 100 億行專用和開源代碼的十年研發和分析經驗，可以識別出開發期間的關鍵品質缺陷和潛在安全漏洞，有助於降低風險和整體項目成本。

關鍵特點

深入和精確的分析

- Coverity 可以無縫集成任何構建系統，生成源代碼的高保真度說明和註釋，以確保深入理解其行為。
- Coverity 可以提供完整的路徑覆蓋範圍，確保每一行代碼和每一條潛在的執行路徑經過測試。它可以利用多種專利技術，確保深入、精確的分析。
- 通過深入理解源代碼和底層框架，Coverity 平臺可以提供高度精確的分析結果，使開發人員不再浪費時間管理大量的誤報結果。這會幫助他們能夠有效地將安全性構建到開發生命週期中

快速和大規模的分析

- Coverity 旨在徹底適應您的現有工作流，它具備以下功能：
- 並行分析允許 Coverity 同時運行高達十六個內核，交付的性能比序列分析高出 10 倍。
- 增量分析支援分析加速，只重新分析發生變動或受變動影響的代碼，而非每次分析整個代碼庫。
- Coverity 可以擴展，在地理分布式環境中容納數千名開發人員，並且輕鬆分析超過 1 億行代碼的項目。

高效的問題管理和修復

- 利用該平臺的協作式問題管理界面 Coverity Connect，開發人員可以訪問必要的訊息，獲得精確的修復指南，工具可為他們展示修復缺陷的正確方式和修復代碼的最佳位置，無需深入的安全專業知識。
- Coverity Connect 提供源代碼導航，識別通向缺陷的準確路徑，並自動識別共享代碼之間發生的每個缺陷。
- 缺陷可以自動分配到適合的開發人員加以解決，用戶可以快速查看所有未解決的安全問題、OWASP 10 大問題、CWE 和 PCI 相關的問題。

軟體開發生命週期 (SDLC) 集成

- Coverity 平臺可以快速集成所使用的關鍵工具和系統，從而支援開發流程（例如源代碼控制管理、構建和持續集成、錯誤跟蹤、集成開發環境 (IDE) 和應用生命週期管理(ALM) 解決方案）。
- Coverity 是一款開放式平臺，允許開發人員將第三方分析結果導入工作流，利用軟體缺陷和風險單一視圖查看和管理所有類型的缺陷。

促進採用和緩解風險

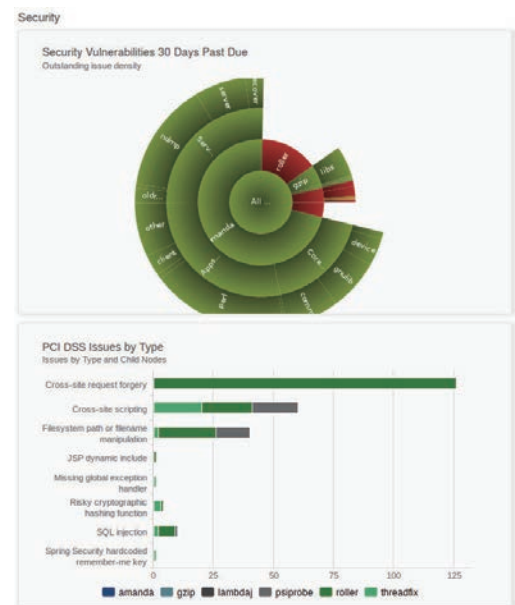
Coverity Policy Manager 幫助企業定義和強制實施始終如一的標準，支援各個開發團隊的代碼安全、品質和測試。它可以全面觀察團隊、項目或組件是否符合這些標準，並基於缺陷和測試相關預定義標準，創建可以衡量的階段關卡。Coverity Policy Manager 的定制化視圖可以選擇開發指標和閾值，從而與具體目標保持一致。支持嵌入式、企业级和移动应用。

擴展漏洞檢測

Coverity Extend 是一種易用的軟體開發包 (SDK)，允許開發人員檢測獨有的缺陷類型。這個 SDK 是為編寫程式分析器或檢查器提供的一個框架，幫助他們識別自定義或特定領域的缺陷。定制化檢查器還有助於滿足企業安全要求和行業標準或指導方針的合規要求。

解決源頭的安全問題

- 為您的開發人員提供他們所需的訊息，以便快速和高效地排除故障並修復關鍵缺陷
- 確保開發流程的品質和安全，以免後期發現缺陷，減少返工和上市延遲付出的成本
- 避免現場或生產過程中的軟體故障和安全漏洞，減少由此產生的高昂成本和品牌損失等風險



Coverity 的 Policy Manager 能夠幫助用戶輕鬆監控和報告狀態、風險以及趨勢。

支援語言和框架

C/C++	C#	Java
JavaScript	PHP	Python
ASP .NET	Objective-C	JSP
Node.js	Ruby	Android
Swift	Fortran	

支援平臺

Windows	Linux	Mac OS X	Solaris
AIX	HP-UX	NetBSD	FreeBSD

支援的編譯器部分列舉

• VisualDSP++ • ARM C/C++ • Borland C++ • Clang • Cosmic C • Freescale Codewarrior • GNU GCC/G++ • Green Hills C/C++/EC++ • HI-TECH PICC • HP aCC • IAR C/C++	• IBM XLC • Intel C++ • Keil Compilers • Marvell MSA • QNX C/C++ • Renesas C/C++ • SNC C/C++ • SNC GNU C/C++ • Sony ORBIS SDK • Sony PS4 • STMicroelectronics GNU C/C++ • STMicroelectronics ST Micro C/C++	• S Sun (Oracle) CC • Synopsys Metaware C and C++ • TI Code Composer • Visual Studio • Wind River C/++ • JDK for Mac OS X • OpenJDK • Sun/Oracle JDK • CEVA XC4500
---	---	--

SDLC集成

SCM	IDE/CI	問題跟蹤
• Accurev • Clearcase • CVS • Git • Hg (Mercurial) • Perforce • SVN • TFS SCM	• Android Studio • Eclipse • IBM RTC • IntelliJ, Webstorm, Rubymine, PhpStorm, PyCharm • QNX Momentics • MS Visual Studio • Wind River Workbench • Jenkins • TFS	• JIRA • Bugzilla



關鍵檢查

API 使用錯誤	整數處理問題
最佳實踐編碼錯誤	整數溢位
構建系統問題	記憶體 – 損壞
緩沖區溢位	記憶體 – 非法訪問
類層次不一致	空指針間接引用
代碼可維護性問題	路徑操作
並發數據訪問沖突	性能低效
控制流問題	程式掛起
跨站腳本 (XSS)	競爭條件
跨站請求偽造 (CSRF)	資源泄露
死鎖	違規
錯誤處理問題	安全最佳實踐違規
硬編碼證書	安全配置錯誤
表達錯誤	SQL 註入
不安全的數據處理	未初始化成員

Coverity 能夠為開源社區提供服務而備感自豪，超過 4000 個項目目前正在使用我們免費的 Coverity Scan，項目包括 Linux、Python、PostgreSQL、Firefox、OpenSSL、Perl、Apache Hadoop 以及更多。

Synopsys 的與眾不同之處

Synopsys 公司為您構建完整、安全、高品質的 SDLC 和供應鏈提供了最全面的解決方案。我們綜合利用領先的測試技術、自動化分析能力和領域專家來創建一系列的強大產品和服務，從而允許企業開發定制的程式，用於在開發流程的早期階段檢測到並修復缺陷和漏洞，最大限度地降低風險並提高生產力。Synopsys 是應用安全測試領域公認的領導者，在針對物聯網、DevOps、CI/CD 和雲計算等新技術和新趨勢來調整和應用最佳實踐方法方面占據得天獨厚的優勢。我們的工作不會止步於測試結束。我們還提供在線和部署幫助、針對性的修復指導、以及各種培訓解決方案，以幫您優化投資回報。無論您的軟體開發流程是剛剛開始，還是已經取得了一定的進展，我們的平臺都能幫您確保軟體應用的完整性，為您發展業務奠定堅實基礎。

欲了解更多訊息，請訪問：www.synopsys.com/software。

Synopsys, Inc.
185 貝裏街, 6500 號房
舊金山, CA 94107 USA

美國銷售電話：800.873.8193
國際銷售電話：+1 415.321.5237
電子信箱：sig-info@synopsys.com