傳單
應用程式交付管理

Fortify Static Code Analyzer

利用 Micro Focus® Fortify Static Code Analyzer 建構更好的程式碼並保護軟體的安全

- **統計資料**
  - 超過 84% 的安全漏洞發生在應用程式層[1]
  - 重大的Web安全弱點幾乎影響了一半的Web應用程式[2]
  - 52% 的 Web 應用程式發生過輸入驗證、跨網站指令碼和 SQL 資料隱碼攻擊 (injection) 的問題[3]
  - 33% 的應用程式從未測試其安全弱點[4]

帶來風險且曝露安全問題的應用程式

軟體開發人員的日常

- 建構新的特性與功能
- 不斷增加的複雜性
- 數不盡的結案日期
- 不斷縮減的預算
- 產品延遲上市

這些描述之所以和軟體開發人員產生共鳴，是因為這正是他們在開發關鍵業務應用程式時所面臨的要求。時至今日，無數的需求造成應用程式的建構更加複雜，開發人員不堪重負，以至於將安全問題置之最後。與此同時，威脅正不斷進化，而且攻擊者專門利用最弱的環節 — 也就是應用程式。Fortify Static Code Analyzer (SCA) 保護組織免於承擔當今最大的安全風險，即執行其業務的應用程式。

Fortify Static Code Analyzer

Fortify SCA 是一種靜態應用程式安全測試 (SAST) 方案，開發團隊和安全專家利用這套工具來分析原始碼的安全漏洞。它可以檢查程式碼，並幫助開發人員毫不費力地以更短的時間來識別問題、確定問題的重要順序並加以解決。

Fortify SCA 讓開發人員能夠：

- 及早並經常掃描原始碼
- 深入每一行程式碼，準確找出程式弱點的根本原因
- 建立結果的關聯性，並確定其優先順序
- 加速開發並縮短掃描時間
- 快速修復安全弱點
- 參考最佳實務以協助開發人員以更安全的方式撰寫程式碼

什麼是「靜態程式碼分析」？

靜態程式碼分析工具能有效找出原始碼的安全弱點。靜態程式碼的分析應在開發生命週期的初期就完成，並在整個應用程式的生命週期中持續執行。在程式開發過程中發生程式碼問題時，它會即時提供回饋意見給開發人員。

為什麼 Fortify SCA 是您理想的選擇

支援完整

Fortify SCA 支援各種開發環境、語言、平台和架構，可在混合的開發和生產環境中執行安全檢查。

- 25 種程式設計語言
- 超過 911,000 個元件級 API
- 可偵測超過 961 個弱點類別
- 支援所有主要平台、建構環境和 IDE

準確度

Fortify SCA 提供準確的結果，並能偵測到其他靜態測試技術找不到的各種問題。Fortify SCA 能排定弱點的優先順序來提供準確的行動計劃，並指定問題的風險等級和分類。這些作業的指導原則，來自一套最大、最完整的安全編碼規則，而這些規則是由 MicroFocus® Security Fortify 軟體安全研究小組所擴充和更新的。

1 *Gartner Magic Quadrant 報告*
2 *2015 Micro Focus 網路風險報告，2015 年 2 月*
3 *同上*
4 *研究報告：行動應用程式開發人員未投入安全問題，2015 年 3 月 20 日*

彈性設計
Fortify SCA 適用您現有的開發環境。它是一套靈活的指令列靜態程式碼分析程式，能透過腳本、外掛程式和 GUI 工具整合到任何環境中，讓開發人員快速輕鬆地啟動和執行。

高效率
更快的掃描時間，對需要加速其應用程式安全計劃的組織帶來不少的好處。Fortify SCA 的增量掃描功能，可提高開發人員的程式設計效率。增量掃描功能只分析前次完全掃描後有變更的部分程式碼，因此可縮短掃描所需要的時間。大幅縮短掃描時間後，開發人員可以更快取得結果，增加掃描的頻率以提高生產力，並加快軟體投入生產環境的時程。

可擴充
應用程式的來源很多，包含內部、外包、第三方、開放原始碼、行動裝置，因此光是從應用程式的數量和複雜性來看，測試與維護企業中所有這些應用程式類型的安全完整性，就是一項挑戰。而 Fortify SCA 支援業界大多數的程式設計語言，能夠識別各種應用程式的風險類型，並隨著業務需求的增長而擴充。

內部部署或隨選服務
Fortify SCA 提供多種傳遞模式，旨在滿足不斷變化的需求和要求。

- 內部部署 — Fortify SCA 適用於企業實地部署、管理和執行靜態應用程式安全測試計畫。
- 隨選服務 — Fortify on Demand 是一種受管理的應用程式安全測試服務，它提供了一種簡單而準確的方法來啟動靜態、動態和行動裝置測試計畫，而無需前期的投入、額外的資源與時間。

支援的程式語言
- ABAP/BSP
- ActionScript/MXML (Flex)
- ASP.NET, VB.NET, C# (.NET)
- C/C++
- Classic ASP (w/VBScript)
- COBOL
- ColdFusion CFML
- HTML
- Java (包括 Android)
- JavaScript/AJAX
- JSP
- Objective-C
- PHP
- PL/SQL
- Python
- T-SQL
- Ruby
- Swift
- Visual Basic
- VBScript
- XML

支援的 IDE
- Eclipse
- IntelliJ Ultimate
- IntelliJ Community Android Studio
- IBM Rational Application Developer (RAD)
- IBM Rational Software Architect (RSA)
- Microsoft Visual Studio

支援的建構工具
- Ant
- Jenkins
- Maven
- MSBuild
- Xcodebuild

Fortify 的軟體安全弱點分類法
弱點類別
在軟體安全方面，大家對於如何判別是否為重大弱點並沒有一致的標準。很多組織對於前幾大弱點自有一套說法，這造成了認知不一致和混淆。為協助開發人員了解會造成安全弱點的常見編碼錯誤類型，Fortify 建立 The Seven Pernicious Kingdoms(七種致命錯誤)以統一組織的弱點，並將其對應 OWASP、SANS、CWE 和 FISMA 等標準。

Fortify Software Security Research Group 是一個全球性的團隊，被業界公認為監控新興威脅的頂尖安全組織之一。該團隊的知識結晶，已貫入 Micro Focus Security Fortify 產品套件的弱點檢查功能，能有效掌握最新的安全威脅。此團隊建立了一套弱點類別分類法 (Vulnerabilities Category Taxonomy)，協助開發人員利用這套規則來了解影響應用程式的安全弱點類型。

深入了解分類法的發展：
www.vulncat.fortify.com/en

關於 Micro Focus Security

Micro Focus 為安全與法規遵循解決方案的領導廠商，能滿足現代企業降低混合環境中的風險並抵禦進階威脅的要求。Micro Focus Security Intelli-gence Platform 以 ArcSight、Fortify 及 Data Security 等市場領先產品為基礎，提供獨特的進階關聯、應用程式保護和網路防禦功能，以保護當今混合式 IT 基礎架構免受先進的網路安全威脅。

深入了解 Micro Focus Security 產品：**www.microfocus.com/securitysolutions**。

更多詳細資訊

Micro Focus Security Fortify 解決方案協助您安心使用軟體來經營企業。

更多資訊請造訪
www.microfocus.com/fortifysca

與我們聯絡：
www.microfocus.com

喜歡本文內容嗎？歡迎分享。

Micro Focus Taiwan facebook

網址：https://www.microfocus.com/zh-tw
電話：+886-2-23760036
電子信箱：taiwan.sales@microfocus.com