MICRO FOCUS

データシート
Fortify Static Code Analyzer

Fortify Static Code Analyzer

コードの品質向上とソフトウェアの保護

アプリケーションがもたらすリスクとセキュリティ上の弱点

ソフトウェア開発者が直面する現実

- 新しい特長や機能の構築
- ますます増大する複雑さ
- いくつもの締め切りや納期
- 縮小する予算
- 製品 (開発-市場投入) の遅れ

これらは、ソフトウェア開発者がクリティカルなビジネスアプリケーションを構築する際に直面する課題です。ソフトウェア開発者には、これらの課題への取り組みや対処が常に求められています。今日のアプリケーション開発では、開発者は数えきれないほどのさまざまな要件への対応に追われているため、セキュリティ対策は後手に回りがちです。その間にも、脅威は刻々と進化を続けており、敵はアプリケーションという弱点を突く攻撃に専念しています。Fortify Static Code Analyzer (SCA) は、組織のビジネスを動かしているアプリケーションという今日の最大のセキュリティリスクから組織を保護するのに役立ちます。

Fortify Static Code Analyzer

Fortify SCAは、開発グループやセキュリティプロフェッショナルがソースコードのセキュリティ脆弱性を分析するのに使用する、静的アプリケーションセキュリティテスト (SAST) ソリューションです。Fortify SCAでコードをレビューすることで、開発者は問題の発見、優先順位付け、および解決をすばやく簡単に行うことができます。

Fortify SCAで開発者ができること:

- ソースコードを早い段階から何度もスキャン
- 脆弱性の根本原因をコード行レベルで特定
- 結果の関連付けと優先順位付け
- 開発を迅速化し、スキャン時間を短縮
- セキュリティ脆弱性をすばやく修正
- 開発者がより安全なコードを作成するのに役立つベストプラクティスを確認

静的コード分析とは

静的コード分析では、ソースコード内のセキュリティ脆弱性を効率的に見つけることができます。静的コード分析は開発サイクルの早い段階で行い、アプリケーションのライフサイクルを通じて継続的に使用する必要があります。静的コード分析を行うことで、開発中にコードに発生した問題点が開発者にすばやくフィードバックされます。

Fortify SCAをお勧めする理由

包括的

Fortify SCAは、幅広い開発環境、言語、プラットフォーム、およびフレームワークをサポートしているため、開発と本番の混在環境でセキュリティレビューを行うことができます。

- 25のプログラミング言語
- 911,000を超えるコンポーネントレベルのAPI
- 961を超える脆弱性カテゴリの検出
- すべての主要なプラットフォーム、ビルド環境、IDEのサポート

統計データ

- セキュリティ違反の84パーセント以上が、アプリケーションレイヤーで発生している[1]
- すべてのWebアプリケーションの半分近くが、重大なWebセキュリティ脆弱性の影響を受けている[2]
- Webアプリケーションの52パーセントが、入力検証、クロスサイトスクリプティング、SQLインジェクションに関する問題を経験している[3]
- アプリケーションの33パーセントが、セキュリティ脆弱性に関するテストをまったく受けていない[4]

1 Gartner Magic Quadrant Report
2 「Micro Focus Cyber Risk Report 2015」、2015年2月
3 同上
4 調査:「Mobile Application Developers Not Investing in Security」、2015年3月20日

高精度

Fortify SCAで生成される結果は精度が高く、他の静的テストテクノロジーでは検出できない幅広い問題点を見つけることができます。Fortify SCAでは、精度の高いアクションプランを提供するため、脆弱性の優先順位付けが行われ、リスクランクとカテゴリ分類付きで問題点が示されます。Fortify SCAは、すべての内容が網羅された最大規模のセキュリティコーディングルールに基づいています。このセキュリティコーディングルールは、Micro Focus® Security Fortifyソフトウェアセキュリティリサーチグループが拡張および改訂を行っています。

柔軟

Fortify SCAは、既存の開発環境に合わせて使用できます。Fortify SCAは柔軟なコマンドラインの静的コード分析ツールで、スクリプト、プラグイン、およびGUIツールを介してあらゆる環境に組み込むことができるため、開発者はすばやく簡単に静的コード分析を実行できます。

効率的

アプリケーションセキュリティプログラムの迅速化を必要としている組織は、スキャン時間の短縮を図ることができます。Fortify SCAでは、増分スキャンを行うことができるため、開発者がプログラミングの生産性を向上させるのに役立ちます。増分スキャンでは、前回のフルスキャン以降に変更されたコード部分のみを分析することで、スキャンの実行に要する時間を短縮できます。スキャン時間が大幅に短縮されるため、開発者は結果をすばやく得ることができます。また、スキャンを行う頻度を増やして生産性を向上させ、ソフトウェアを本稼働させるまでの時間を短縮することができます。

スケーラブル

社内開発、アウトソース、サードパーティ製、オープンソース、モバイルなど、さまざまなソースのアプリケーションが存在します。また、非常に多くの複雑なアプリケーションが作成されているため、これらのすべてのアプリケーションタイプのセキュリティをテストして完全な状態を維持するのは非常に困難です。Fortify SCAは、業界内のほとんどのプログラミング言語をサポートしており、あらゆるタイプのアプリケーションでリスクを発見することができます。また、ビジネスの要求に合わせて拡張することもできます。

オンプレミスまたはオンデマンド

Fortify SCAは、変化するニーズや要件に対応できるように設計された複数のデリバリモデルで提供されます。

- オンプレミス ― Fortify SCAは、静的アプリケーションセキュリティテストプログラムをオンサイトに導入して使用します。
- オンデマンド ― Fortify on Demandは、精度の高い静的、動的、およびモバイルテストを容易に実行できるマネージド・アプリケーションセキュリティ・テストサービスで、先行投資や追加リソースなしに使用できます。

サポートされる言語

- ABAP/BSP
- ActionScript/MXML (Flex)
- ASP.NET、VB.NET、C# (.NET)
- C/C++
- Classic ASP (VBScriptを使用)
- COBOL
- ColdFusion CFML
- HTML
- Java (Androidを含む)
- JavaScript/AJAX
- JSP
- Objective-C
- PHP
- PL/SQL
- Python
- T-SQL
- Ruby
- Swift
- Visual Basic
- VBScript
- XML

サポートされるIDE

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

サポートされるビルドツール

- Ant
- Jenkins
- Maven
- MSBuild
- Xcodebuild

Fortifyによるソフトウェアセキュリティ脆弱性の分類

脆弱性のカテゴリ

ソフトウェアセキュリティについては、重大な脆弱性の定義に関する明確な基準はありません。多くの組織が最も重要な脆弱性に関する独自の解釈を発表しており、くい違いや混乱が生じる原因になっています。開発者がセキュリティ脆弱性につながる一般的なコーディングの誤りを理解できるように、Fortifyは脆弱性を体系化して、OWASP、SANS、CWE、FISMAなどの基準との対応関係を示した「Seven Pernicious Kingdoms」を作成しました。

Fortifyソフトウェアセキュリティリサーチグループは、新たに発生する脅威の監視を行う最も優れたセキュリティ組織の1つとして業界で認められたグローバル規模のチームです。ここで収集された知識は、最新の脅威を抑止する脆弱性チェックの形でMicro Focus Security Fortify Suite製品に反映されます。このチームは、「Vulnerabilities Category Taxonomy (脆弱性カテゴリ分類)」を作成しています。この分類は、開発者がアプリケーションに影響を与えるセキュリティ脆弱性のタイプを理解するための基準としても役立ちます。

詳細情報: Evolution of a Taxonomy: **vulncat.fortify.com/en**

Micro Focusのセキュリティについて

Micro Focusは、ハイブリッド環境でのリスクの軽減と、高度な脅威に対する防御を必要とするエンタープライズ向けにセキュリティおよびコンプライアンスソリューションを提供する世界有数のプロバイダーです。業界をリードするArcSight、Fortify、およびData Securityの製品に基づくMicro Focus Security Intelligenceプラットフォームは、他に類を見ない高度な相関、アプリケーションの保護、およびネットワークセキュリティを提供し、今日のハイブリッドITインフラストラクチャーを高度なサイバー脅威から守ります。

Micro Focusのセキュリティ製品の詳細については、**microfocus.com/securitysolutions**を参照してください。

関連情報

Micro Focus Security Fortifyソリューションは、ビジネスを動かしているソフトウェアの信頼性を確保するのに役立ちます。Fortify Static Code Analyzerの詳細については、**microfocus.com/fortifysca**を参照してください。

詳細情報

microfocus.com/fortifysca

www.microfocus.com

Micro Focus
英国本社
United Kingdom
+44 (0) 1635 565200

米国本社
Rockville, Maryland
+1 301 838 5000
+1 877 772 4450

www.microfocus.com

マイクロフォーカスエンタープライズ株式会社
0120 923 333

www.microfocus-enterprise.co.jp