

Web 資産の戦略的保護により
ビジネス目標をサポート



Rational software

IBM Rational AppScan ライフサイクル・ソリューション: ソフトウェア開発プロセスに Web アプリケーション・セキュリティーを組込む



オンラインの脆弱性がもたらすビジネス・リスク

今日の多くの組織が、ビジネス・プロセスの実行や、サプライヤーとの取引の実行、またこれまでになく高度なサービスを顧客に提供するために、Web ベースのソフトウェアとシステムに依存しています。適切に統制のとれている組織内では、オンラインでのデプロイメントが予定されているすべてのアプリケーションにセキュリティーを組み込むことは、ソフトウェアやシステムのデリバリーのビジネス・プロセスで不可欠の部分となります。しかし残念ながら、多くの企業は、競合相手に一歩でも先んじようとするばかりに、新しい製品やサービスの市場投入を急ぎ、これらの懸念事項に十分な対応を行っていません。そして、その結果生じる脆弱性により、ハッカーが企業や個人の情報にアクセスしたり、盗んだりすることのできる大いなるチャンスが生まれ、ビジネス全体がリスクにさらされる可能性があるのです。

IBM Rational® AppScan® は、組織がこの重要な課題に対処するために必要な可視性とコントロールを獲得するための、市場をリードする Web アプリケーション・セキュリティー・ソリューションです。

- IBM Rational AppScan Standard Edition
(デスクトップ・アプリケーションとして利用可能)

この包括的なソリューションは、スキャン、レポート作成、および推奨される修正の提示機能を備えており、アプリケーション開発者、品質保証 (QA) チーム、侵入テスト担当者、セキュリティー監査担当者、シニア・マネージャーといったさまざまなユーザーが行うあらゆるタイプのセキュリティー・テストに対応します。

IBM Rational Software Delivery Platform の他のライフサイクル・ソリューションと同様に、Rational AppScan 製品においても、主要な QA ツールや統合開発環境 (IDE) との事実上シームレスな統合により、ユーザーは使い慣れたテクノロジー環境において作業を行うことができます。また、継続的なセキュリティー監査を実行することができ、ソフトウェア・デリバリー・チームが基礎から Web アプリケーションにセキュリティーを組み込むことができるため、アプリケーションをデプロイする前にビジネス・リスクの緩和を図ることができます。

重要な Web ベースのビジネス資産を保護する

複雑な Web サイトのための包括的なセキュリティー保護を提供する Rational AppScan Standard Editionは、Web サイトをスキャンおよびテストして、Web アプリケーション・セキュリティー・コンソーシアム (WASC) の脅威種別により特定されたものを含む、一般的な Web アプリケーション脆弱性の有無をチェックします。Rational

AppScan ソリューションには、最新の Web 2.0 テクノロジーに対応した堅固なアプリケーション・スキャンを提供する、広範囲にわたる強力で柔軟な中核機能が搭載されています。例えば、Flash および先進的な Java™ Scriptのサポート拡張、Ajax プログラミング言語の包括的なサポート (JavaScript オブジェクト記法 (JSON) や Web サービス・パラメーターのための専用テストを含む) などです。

スキャンの効率性と操作性のための Rational AppScan の中核機能:

- アプリケーション・ツリー、階層型のセキュリティー問題結果リスト、開発者のための修復ビュー、詳細ペインを選択できる使いやすいユーザー・インターフェース
- アプリケーション・パラメーターを分析して、開発プロセスの妨げとならない関連テストのみを選択することができる、適応力の高いテスト・プロセス
- CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart) による複数手順の認証、複数要素による認証、ワンタイム・パスワード、USB (ユニバーサル・シリアル・バス) キー、スマート・カード、相互認証などの、Web アプリケーションにおける複数手順の認証手続きに対応したテストが可能な、複合認証のサポート
- 必要に応じて自動再ログインを実行する高度なセッション管理
- スキャン完了前にユーザーが問題に対処できる、リアルタイムの結果表示

- クレジット・カードや、その他の数値列のパターン検索規則

カスタマイズとコントロールのための Rational AppScan の中核機能:

- テスト機能を拡張する強力なアドオンを作成し、共有し、読み込むことができるようにする Rational AppScan eXtensions Framework テクノロジー
- Rational AppScan に Python スクリプトの機能を組み合わせて、ユーザー・インターフェースの制約なしにユーザーがスキャン機能を活用できるようにする Pyscan。これにより、セキュリティ担当者や侵入テスト担当者がこれまで利用できなかったレベルのカスタマイズが可能になります。
- Rational AppScan の Software Development Kit (SDK)は、大規模なスキャンからカスタマイズしたテストまで、各種のアクションを起動する機能を提供します。SDK のインターフェースは、スキャン・エンジンをカスタマイズして使用できるよう設計されており、Rational AppScan eXtensions Framework と Pyscan のオプションの利用を可能にします。

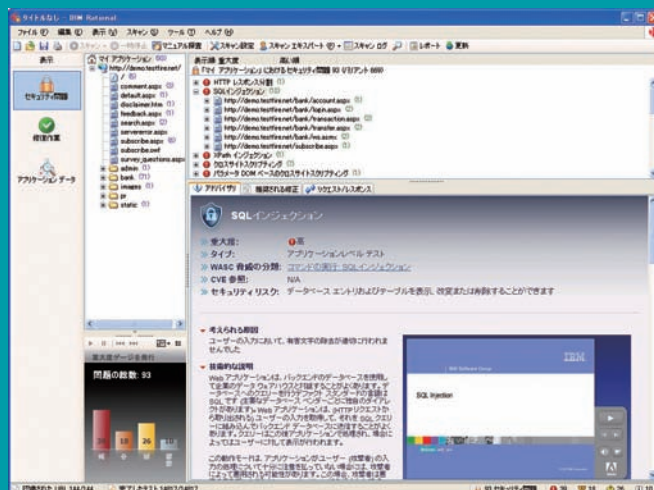
脆弱性検出のため Rational AppScan の中核機能:

- グローバル検索機能は、テストレスポンスを分析し、SSL 証明書の有効性や、クロス・サイト・リクエスト・フォージェリ (CSRF) のような問題を検知します。
- Open Web Application Security Project (OWASP) トップ10 および System Administration Networking and Security Institute (SANS) トップ 20 の脆弱性に対応したハッカー・シミュレーション
- Rational AppScan 製品の起動時に自動的に更新される、最新の脅威に関するアップデート
- 侵入テスト担当者やセキュリティ・コンサルタントによる Web アプリケーションの開発、テスト、デバッグを支援する、バンドルされたユーティリティ・スイート

レポート作成と修復のための Rational AppScan の中核機能:

- 米国標準技術局 (NIST) Special Publication 800-53、OWASP トップ 10 (2007 年に更新)、個人情報保護法、PCI データ セキュリティ標準 を含む、40 を超えるグローバルな法令順守問題および標準に関連するテスト。

- Rational AppScan バージョン 7.7 では、これらに加えて FERPA (Family Education Rights and Privacy Act: 家庭教育の権利とプライバシーに関する法律)、FIPPA (Freedom of Information and Protection of Privacy Act: 情報公開とプライバシー保護に関する法律)、および PABP (Payment Application Best Practices: 支払アプリケーション・ベスト・プラクティス) にも対応しています。
- 脆弱性のある HTML コードをピン・ポイントで特定して問題を説明する、検証の強調表示。差分機能により、変更された HTML コードが明確に表示されます。
- NET、J2EE、Hypertext Preprocessor (PHP) の推奨される修正および開発者タスク・リストを含む修復レポート。これらのレポートでは、アプリケーションに関連する問題、インフラストラクチャーの問題、またはその両方を表示すること、また今後の検討のために、バリエーションを削除する、または脆弱ではないというマークを付けることも可能です。
- HTML コメント内の機密データ、疑わしいコンテンツにまつわる HTTP アクティビティなどの項目を列挙した、不審コンテンツに関する詳細なレポート
- 脆弱性データベースの CVE (Common Vulnerabilities and Exposures) ID を含むアドバイザリー
- Rational AppScan の内部ブラウザからスクリーン・ショットを取り込みます。特定のテストから秘密情報を取り除いた情報を電子メール用に解凍、圧縮、および暗号化し、サポートに送付することができます。また、誤ってAppScanがフォールス ポジティブと判断されたインシデントを IBM Rational AppScan セキュリティ調査チームに報告することも可能です。これにより、製品の正確性を継続的に改善できます。



IBM Rational AppScan のセキュリティ・アドバイザリービュー



