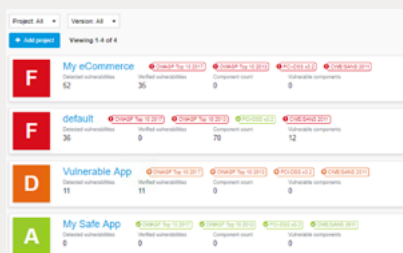


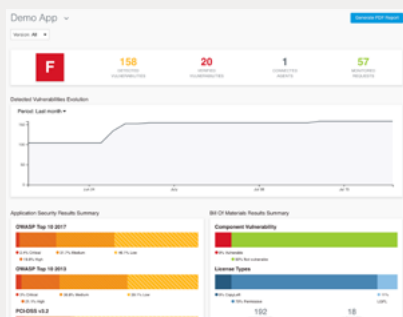
Seeker

インタラクティブ・アプリケーション・セキュリティ・テスト (IAST)

脆弱性を正確に特定・
検証できる使いやすい
エンタープライズ・
クラスの IAST



セキュリティ脆弱性ステータスに基づいて
プロジェクトのセキュリティを格付け評価。



重大なセキュリティ脆弱性が一目で分かる
包括的なダッシュボード・ビュー。

概要

シノプシスのインタラクティブ・アプリケーション・セキュリティ・テスト (IAST) ソリューション Seeker は、Web アプリケーションのセキュリティ状態を最大限に可視化し、OWASP Top 10、PCI DSS、GDPR、CWE/SANS Top 25 などのコンプライアンス規格に照らし合わせて脆弱性トレンドを洗い出します。また、Seeker には機微なデータを特定し、これらが安全に取り扱われているかどうかを追跡する機能もあり、これらの情報が強力な暗号化で保護されていないログ・ファイルやデータベースに格納されるのを防ぐことができます。Seeker は CI/CD ワークフローにシームレスに統合できるため、DevOps のスピードで迅速に IAST セキュリティ・テストを実行できます。

一般的な IAST ソリューションにはセキュリティ脆弱性を特定する機能しかありませんが、Seeker は特定したセキュリティ脆弱性 (XSS や SQL インジェクションなど) を検証し、悪用の可能性を判定する機能もあるため、リスク度に応じてどの順番に脆弱性を修正すればよいかをただちに分かります。Seeker は独自の特許技術により、数十万もの HTTP(S) リクエストを高速に処理して脆弱性を特定しながらも、誤検知はほぼゼロに抑えています。このため、セキュリティ・チームは本当に脅威となる検証済みセキュリティ脆弱性への対応を優先させることができ、生産性の飛躍的な向上とビジネス・リスクの軽減を図ることができます。Seeker を導入することは、Web アプリケーションへの自動ペネトレーション・テストを 24 時間体制で実行してくれる専属チームを持つと同じ効果があります。

Seeker は実行中のアプリケーション内部にエージェントを配置するコード・インストールメンテーションの手法を採用しており、大規模なエンタープライズ環境におけるセキュリティ要件にもスケールアップに対応します。また、面倒な設定なしに高精度な結果が得られるのも Seeker の特長です。脆弱性に関する詳細な解説、具体的な修正アドバイス、スタック・トレース情報を提示しながらどのコード行に脆弱性が存在するかを Seeker が指摘してくれるため、セキュリティの専門知識を持たない開発者にもご利用いただけます。

Seeker は Web アプリケーションに適用されるすべてのタイプのテストを常時監視し、自動 CI ビルド・サーバーおよびテスト・ツールとシームレスに統合します。Seeker はこれらのテスト (人手によるログイン・ページの QA や自動機能テストなど) を利用して、複数のセキュリティ・テストを自動で生成します。

Seeker には、シノプシスのソフトウェア・コンポジション解析 (SCA) ソリューション Black Duck Binary Analysis も付属しており、サードパーティおよびオープンソースのコンポーネント、既知の脆弱性、ライセンス・タイプ、およびその他の潜在的なリスクを洗い出すことができます。Seeker と Black Duck の解析結果は同じビューに表示され、Jira へ自動的に送信できるため、通常の開発ワークフローの一環としてトリアージできます。

Seeker は 1 つのアプリケーションを構成する複数のマイクロサービスを一括評価できるため、マイクロサービス・ベースのアプリケーション開発に最適です。

具体的な結果を常時、迅速に提供

解析結果には、脆弱性への対処に必要なすべての情報が含まれます。

- リスクに関する明確な解説
- 実行時のメモリー値およびコンテキスト
- 技術的な説明
- 脆弱性が見つかったコード行
- コンテキストを考慮した具体的な修正ガイダンス

データフローおよび悪意により挿入されたパラメータ(動的 SQL 連結など)の影響は、複数の詳細なペインに表示されます。この結果には、検出された脆弱性が自動検証によって悪用可能と判定されたか、誤検知として削除されたかも表示されます。

Seeker は Black Duck Binary Analysis も統合しています。

- アプリケーションのバイナリを SCA 解析に送信するだけで、解析結果が Seeker のダッシュボードにアップロードされます。

アクティブな検証機能を備えた唯一のエンタープライズ・クラス IAST ソリューション

Seeker 独自のアクティブ検証機能は数十万もの HTTP(S) リクエストを処理し、検出した脆弱性から誤検知をすばやく削除して提示するため、ユーザーが誤検知を目にすることはほとんどありません。更にテスト・カバレッジを高めるため、Seeker にはパラメータ特定機能があります。これは、使われていないパラメータを検出し、悪意のある値を用いてこれらを再テストする機能で、アプリケーションの攻撃・サーフェス(攻撃対象領域)、隠れパラメータ、バックドアをより広範に調査できます。

これには以下の利点があります。

- セキュリティ・チームと開発チーム双方の生産性が飛躍的に向上。
- 少ないリソースでダイナミック・アプリケーション・セキュリティ・テスト (DAST) や人手によるペネトレーション・テストが実行でき、全体的なコストが削減。

Vulnerability	Severity	#	Last Detected	Status
SQL Injection [Key: ECOMMERCE-48] <input checked="" type="checkbox"/> Seeker-Verified URL: /wvsep/active/SQL-Injection/Sirjec... Parameter: msg Code location: o.a.c.d.DelegatingStatement.execu...	Critical	2	a few seconds ago	Detected
SQL Injection [Key: ECOMMERCE-47] <input checked="" type="checkbox"/> Seeker-Verified URL: /wvsep/active/SQL-Injection/Sirjec... Parameter: password Code location: o.a.c.d.DelegatingStatement.execu...	Critical	2	a few seconds ago	Detected
Cross-site Scripting [Key: ECOMMERCE-52] <input checked="" type="checkbox"/> Seeker-Verified URL: /wvsep/active/Reflected-XSS/RXSS... Parameter: userInput Code location: o.a.j.JspWriterImpl.print() 452	High	2	a few seconds ago	Detected
Weak Hash [Key: VULN_APP-1] <input checked="" type="checkbox"/> Seeker-Verified URL: None Parameter: None Code location: js.MessageDigest.digest()	Low	3	3 minutes ago	Detected
Weak Hash [Key: ECOMMERCE-2] <input checked="" type="checkbox"/> Seeker-Verified URL: None Parameter: None Code location: js.MessageDigest.digest()	Low	5	10 minutes ago	Detected
Weak Hash [Key: ECOMMERCE-46] <input checked="" type="checkbox"/> Seeker-Verified URL: /wvsep/active/SQL-Injection/Sirjec... Parameter: None Code location: c.s.d.ConnectionPoolManager.getC...	Low	1	10 minutes ago	Detected
Weak Hash [Key: ECOMMERCE-34] <input checked="" type="checkbox"/> Seeker-Verified URL: /wvsep/... Parameter: None Code location: js.MessageDigest.digest()	Low	1	11 minutes ago	Detected

導入から運用までが簡単

Seeker は、主にソフトウェア開発ライフサイクル (SDLC) の統合テスト /QA ステージでソフトウェア開発ライフサイクル (SDLC) の運用展開の直前まで、インストールメンテナー手法とランタイム解析を使用して、Web アプリケーションのセキュリティ脆弱性を常時監視、検出、検証します。アプリケーションはオンプレミス、マイクロサービス・ベース、またはクラウド・ベースのものを対象にできます。Seeker は最新のアプリケーション開発メソドロジーとテクノロジーをサポートしています。アプリケーション・コードが動作する各ティアまたはノード (Docker コンテナ、仮想マシン、クラウド・インスタンスなど) にエージェントを導入するだけで、動作中のアプリケーションで実行されるすべてのアクションを追跡できます。解析結果はすぐに取得でき、特別なスキャンは必要ありません。

Seeker はコードを 1 行ずつ解析するだけでなく、データフローとランタイム・コード実行の相関をリアルタイムに取得します。また、すべてのアプリケーション・ティアおよびコンポーネントを対象にコードと重要なユーザー・データの相互作用も確認します。このテクノロジーは、他のテクノロジーでは検出できない複雑な脆弱性やロジックの欠陥を含め、クリティカルなデータに対して本当に脅威となる脆弱性を特定します。

Seeker と e ラーニングの統合は、開発者と DevOps チームに臨機応変なヘルプとトレーニングを提供します。それによって脆弱性に関する深い理解を得て、リアルタイムに修正することが可能になります。

導入後、即活用が可能な Seeker

- **CI/CD ワークフローにシームレスに適合。** ネイティブ統合と Web API により、オンプレミス、クラウド・ベース、マイクロサービス・ベース、コンテナ・ベース開発に使用している既存のツールとシームレスに統合します。
- **短時間で簡単にデプロイ可能。** Seeker のリアルタイム解析は、導入直後から誤検知がほぼゼロに抑えられます。
 - 面倒な設定や調整が不要で、すぐに高精度な結果を取得可能
 - Web サイトのログイン資格情報や特別なスキャンが不要
 - 入力バリデーション・ライブラリとカスタム関数を考慮したアクティブ検証により、入力をサニタイズ (SQL インジェクション脆弱性など)
 - 大規模なエンタープライズ環境にもスケーラブルに対応
- **あらゆるタイプのテスト手法に適合。** Seeker には非介入型のパッシブ監視機能もあり、既存のテスト・オートメーション、手動または機能テスト、自動 web クローラーなどと組み合わせて利用できます。

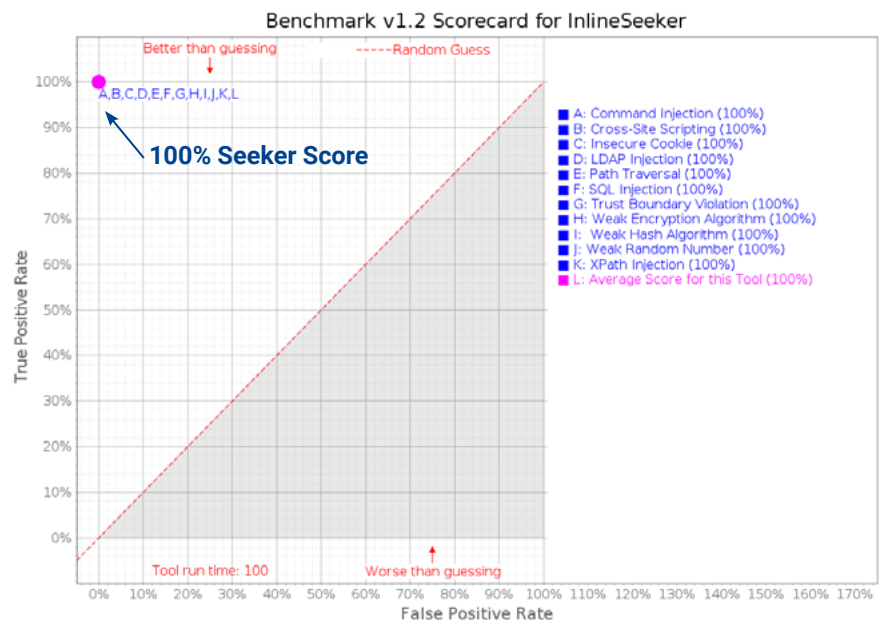
Web アプリケーションの URL 検出およびカバレッジ

自動 URL マッピング機能では、どこまでテストが完了したかがグラフィカルに表示され、Web アプリケーションのテスト・カバレッジを一目で把握できます。同じアプリケーションの異なるバージョン間でカバレッジの違いを容易に比較できます。

機微なデータのトラッキング

Seeker は、機微なデータのトラッキング機能においても業界をリードしています。この機能は、ユーザーが「Sensitive (機微なデータ)」と指定した情報 (クレジットカード番号、ユーザー名、パスワードなど) が、暗号化されていないログやデータベース、ファイルに保存されていないかを常時監視します。これにより、PCI DSS のデータ暗号化に関するセクションや、GDPR (EU 一般データ保護規則) などの業界標準規格・規制へのコンプライアンスが容易になります。しかも、人手による検査に比べて生産性が飛躍的に向上し、時間、コスト、リソースも節約されます。

OWASP ベンチマークで最高スコアを達成



Seeker | 技術スペック

対応言語

- ASP.NET
- C#
- Clojure
- Gosu
- Groovy
- Java
- JavaScript (Node.js)
- Scala (Lift を含む)
- VB.NET

対応プラットフォーム

言語 / テスト・プラットフォーム

- Java
 - すべての Java EE サーバー
 - GlassFish
 - JBoss
 - Tomcat
 - WebLogic
 - WebSphere
- .NET (2.0 以降)
 - IIS
- Node.js (6 以降)
 - Express
 - Hapi
 - Koa

ランタイム / フレームワーク

- .NET/CLR
 - ASP.NET MVC
 - Enterprise Library
 - Entity Framework
 - NHibernate
 - Ninject
 - NVelocity
 - OWASP ESAPI
 - SharePoint
 - Spring.NET
 - Telerik
 - Unity
- Java/JVM
 - Enterprise JavaBeans (EJB)
 - Grails
 - GWT
 - Hibernate
 - OWASP ESAPI
 - Play
 - Seam
 - Spring
 - Struts
 - Vaadin
 - Velocity

テクノロジー

- データベース
 - DB2
 - HSQLDB
 - MongoDB
 - MS SQL
 - MySQL
 - Oracle
 - PostgreSQL
 - SQLite
- アプリケーション・タイプ
 - Ajax
 - JSON
 - マイクロサービス
 - モバイル (HTTP/S)
 - RESTful
 - SPA (Single Page Application)
 - Web (HTML5 を含む)
 - Web API
 - Web サービス

クラウド・プラットフォーム

- Azure PaaS
- AWS
- Google Cloud
- Pivotal Cloud Foundry

シノプシスの特色

シノプシスのソフトウェア インテグリティ グループは、企業が安全で高品質のソフトウェアを構築し、リスクを最小限に抑えながらスピードと生産性の最大化に貢献します。シノプシスは、アプリケーション・セキュリティのリーダーであり、静的解析、ソフトウェア・コンポジション解析、動的解析ソリューションを提供しており、独自のコード、オープンソース・コンポーネント、およびアプリケーションの動作における脆弱性や不具合を迅速に見つけて修正します。

詳しくは、www.synopsys.com/jp/software をご覧ください。

日本シノプシス合同会社
〒158-0094 東京都世田谷区玉川
2-21-1 二子玉川ライズオフィス

TEL: 03-6746-3600
Email: sig-japan@synopsys.com