Contrast SECURITY

WHITE PAPER

アプリケーションセキュリティの新時代:
IASTによるDASTリプレース

はじめに

動的アプリケーションセキュリティテスト（DAST）は、過去数十年間、主要なアプリケーションセキュリティ（AppSec）のテスト手法であり、ソフトウェアアプリケーションの脆弱性を検出し、対処するために利用されて来ました。DASTは広く利用されているにもかかわらず数多くの制限が存在します。DASTツールは、外部から攻撃を試み攻撃が成功したかどうかをHTTPレスポンスに基づいて判断します。特定の状況では有効ですが、コード内部での動作について詳細な洞察が得られないため、真の脆弱性を見逃してしまうケースが多く見受けられます。

AppSecにおいて検出精度を向上させる為にはアプリケーション内部を可視化し、コードの動作を解析しなければなりません。アプリケーションの内部メカニズムを理解できるツールが必要です。このアプローチが脆弱性の過検出や見逃しを無くし、真の脆弱性を正確に検出するために必要な詳細情報を収集する唯一無二の方法です。

背景：DASTについて

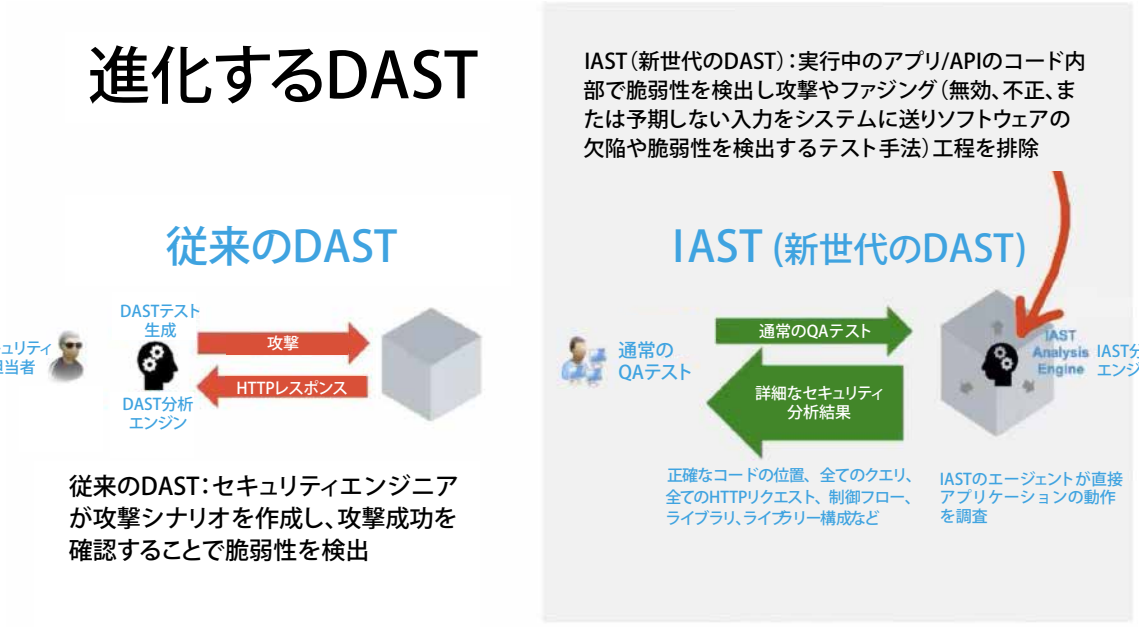
DASTに関する記述は数多くありますがこれらに共通するのは、DASTは実行状態のアプリケーションを分析するセキュリティテスト手法であるということです。米国標準技術局（NIST）の特別資料800-53（改訂5版）のセキュリティアセスメント（SA-11）のガイドライン8では、DASTによる動的テストの重要性が提唱されています。NISTのガイドラインでは、様々な入力や条件に対するソフトウェアコンポーネントの動作にDASTによる動的分析実施が推奨されています。NISTのガイダンスは、実行中のアプリケーションを分析するために多くの異なる方法を推奨しています。

DAST は外部から動作させることが多く、攻撃を可視化しHTTPレスポンスを検査しアプリケーションの反応を観察することで脆弱性を検出します。このような外部からのアプローチは、実行されるコードの複雑なニュアンスや詳細情報を理解することはできません。このため特に複雑なアプリケーションに対するDASTの有効性と精度には限界があります。

次世代のDAST：インテラクティブ・アプリケーション・セキュリティ・テスト(IAST)とは

従来型DASTの限界を考えると、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）と呼ばれる次世代型DASTが急速に普及しています。IASTは実行状態のアプリケーションを分析するAppSecテストですが、アプリケーションの外側からではなく内側から分析します。IASTはエージェントを使用して、アプリケーションの内部操作、ライブラリとのやりとり、バックエンドシステムとの接続等をアプリケーションが動作している間に全てリアルタイムで監視します。

外部スキャン型のDASTとは異なり、IASTはHTTPレスポンスだけでなくコードの動作やクラスメソッド、文字変換、データベースへのクエリーなど様々な情報を確認し脆弱性を高精度で自動的に検出します。この自動化された可視性により従来のDASTや静的アプリケーションセキュリティテスト（SAST）では実現できないほど脆弱性を高精度で特定します。



IAST型のDASTは、かつてない可視性と精度により、AppSecテストをさらに進化させます。内部から行うIAST型アプローチによって提供される詳細情報により、リアルタイムで正確かつ実用的な脆弱性検出結果を得ることが出来、包括的で強力なAppSecを実現します。IAST型のDASTは、従来のDASTよりもはるかに幅広く脆弱性を検出することができます。これには、アプリケーションの外部に全く露出していない可能性のある暗号化された脆弱性も含まれます。また、IAST型のDASTは、実行中のアプリケーションで実際に発生する脆弱な動作パターンのみを高精度で検出します。

IAST型は、脆弱性を発見するために侵入を試みる必要がないことが特徴です。複雑な脆弱性を検出するために、ファジングや侵入攻撃ではなく、通常のアプリケーショントラフィックを使用します。これにより、AppSec担当のセキュリティエンジニアだけでなく、誰でもDASTをご活用出来る様になります。開発者は、通常のWebアプリケーションの機能テストを実施するだけで自動的にコードの脆弱性を検出することができます。自動テストケースを含む全ての機能テストによりセキュリティテストが同時に実施されます。

Contrast Assess：新時代のApp Sec

Contrast Securityは従来のDASTを超える包括的なAppSecツールの必要性から、革新的ソリューションである Contrast Assessの開発に至りました。この最先端のツールはユニークなアプローチによるIAST型のセキュリティテストツールで、アプリケーションの脆弱性をより正確かつ詳細に検出することができます。

Contrast Assessは、エージェントをアプリケーションサーバーに組込めば直ぐに動作します。このエージェント方式によるセキュリティテストのパイオニアです。HTTPレスポンスの分析を行う従来のDASTとは異なりContrastは実行中のアプリケーション内で分析を行います。このエージェントを使用する技術はアプリケーションパフォーマンステストツール市場で何十年も使われており、New Relic、AppDynamics、DataDogのようなツールの基礎技術となっています。

Contrast Assessはコード内部で何が起きているのか全く把握できない従来のDASTツールとは異なり、ソフトウェアの実行中に制御フロー、データフロー、ライブラリの使用状況、危険な関数を追跡し脆弱性を検出します。例えば、Contrastは信頼されていないデータが無害化されないままSQLクエリに直接追加されるなど、危険な動きを検出することができます。この検出機能は非常に高精度で、脆弱性が悪用されることはありません。

Contrast Assessは、DASTを大幅に機能強化したものです。Contrastは従来のDASTのように脆弱性を検出しますが、大きな違いはコード内部を分析しより正確に脆弱性を検出して開発者にリアルタイムでフィードバックすることです。Contrastにスキャンや攻撃は必要有りません。

Contrastが提供するAppSecダッシュボードにはHTTPリクエスト、関連するコードの正確な行、アプリケーションまたはAPIを介したデータフローの正確な内容を含め脆弱性について詳細に詳細に把握することができます。複雑なスケジューリングを伴うスキャンが必要な従来のDASTソリューションとは異なり、Contrastは分散型アプローチであり、数百または数千のアプリケーションで並行実行できるため、開発パイプライン、QA、本番環境における脆弱性を検出することができます。

脆弱性修正方法を提供する機能を備えたContrast Assessは、開発者にとって強力なツールであり、コードの問題を理解し、迅速かつ効率的に修正することができ、フィードバックのループが加速し、AppSecのプロセスがより効率的で費用対効果の高いものになります。

Contrast Assessに代表されるようなAppSecの新時代はセキュリティテスト業界における大きな進化です。このAppSec手法の飛躍的進歩により、企業は従来のDASTの強みを生かしつつ、強力な新機能を追加することで、ソフトウェアアプリケーションをより効果的に保護することができます。ContrastはAppSecを強化し、DASTの要件を満たすための優れたアプローチを提供しています。

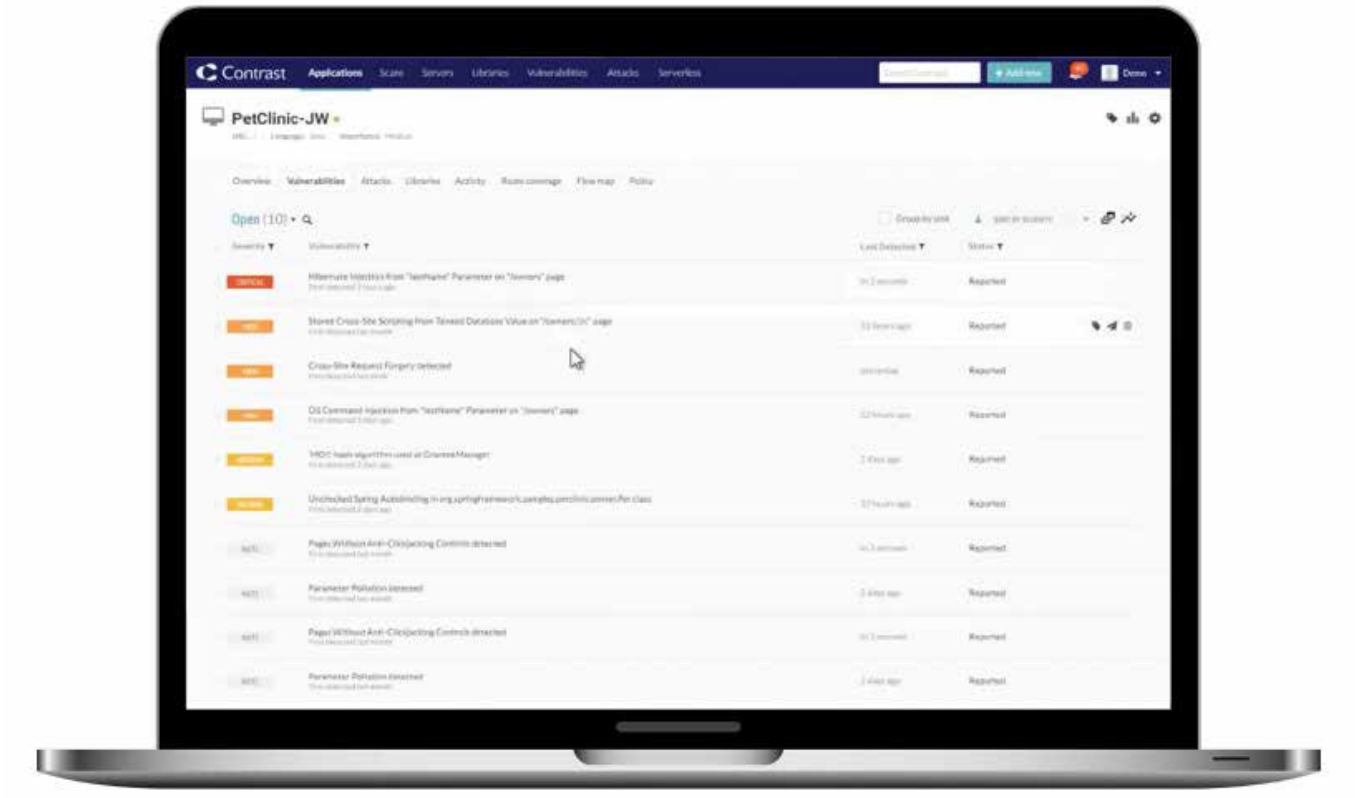
異なる種類のDAST：Contrast Assessの動作

Contrast Assessの機能と効率性を説明するために典型的なSpring Bootアプリケーションであ るPet Clinicを使って、実際に動作しているところを見てみましょう。

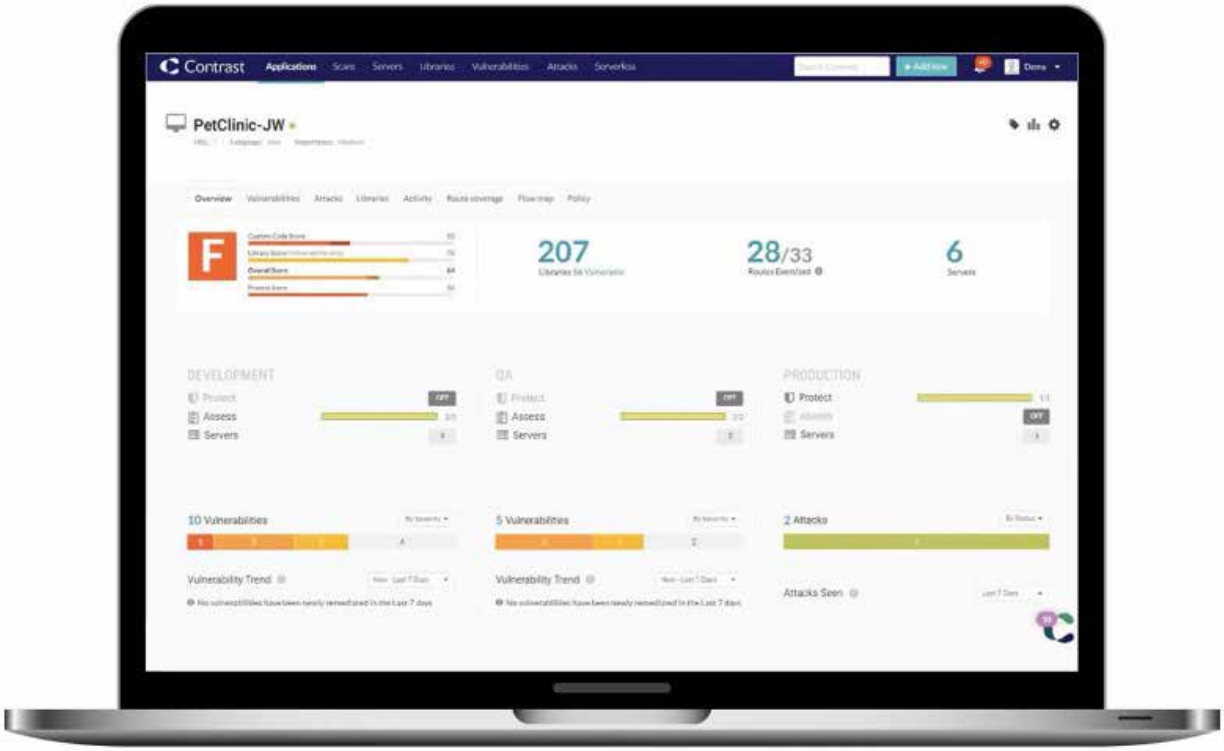
最初のステップでContrastエージェントをアプリケーションスタックに追加します。

Contrastエージェントが追加されるとアプリケーションは通常状態で実行されバックグラウンドでアプリケーションのモニタリングを開始します。

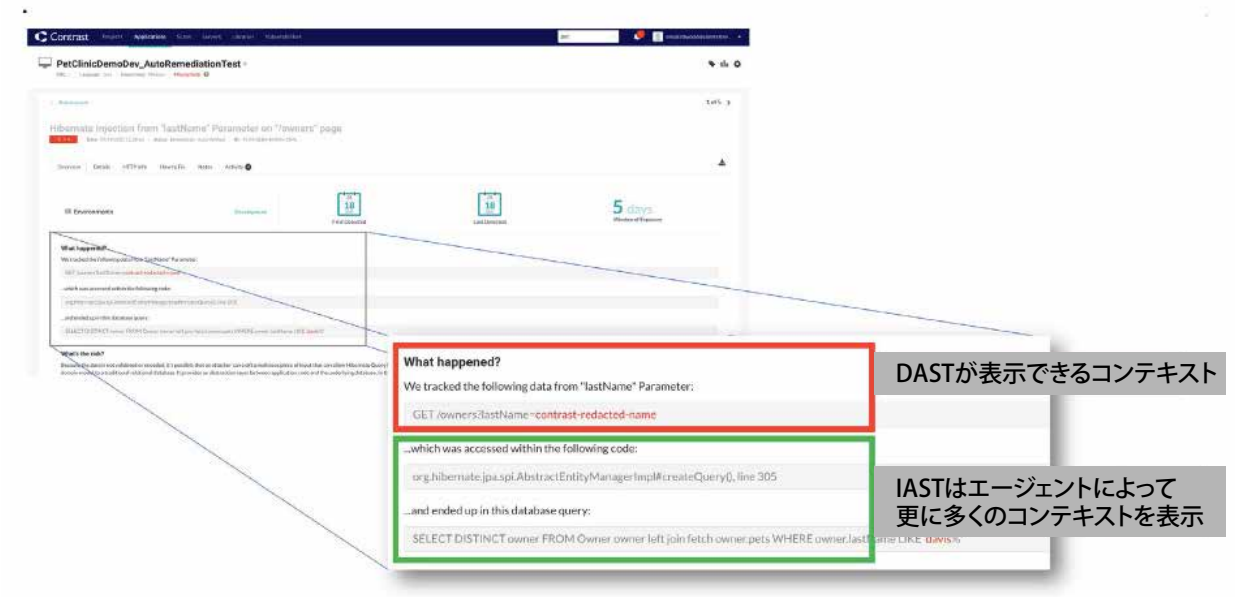
アプリケーションを使用するとContrastは実行中のコードで動作する各リクエストを分析します。 その後脆弱性を検出し、Contrastダッシュボードに報告します。



ダッシュボードには監視対象の全アプリケーションの状況が表示され、使用されるライブラリ、実行されるルートおよびアプリケーションが実行されるサーバーに関する情報が表示されます。



Contrastは脆弱性が検出されると関連する詳細情報を表示します。HTTPリクエスト、そのメソッド、そして適切なエスケープやパラメータ修正されずにクエリ内でどのように使用されたか、など追跡データを表示します。コード行とデータフロー全体の動きが可視化されるため、開発者は脆弱性を理解し、修正することができます。



Contrast Assessは、HTTPリクエストのすべての入力を同時に分析できるため、セキュリティテストに必要な時間を大幅に短縮できます。DASTとIASTを統合することで、Contrast Assessは従来のDASTと次世代AppSecのギャップを効果的に埋めDAST機能に大きな変革をもたらします。高精度、即時フィードバック、複数の攻撃ベクトルを同時にテストする性能を持つContrast Assessは、AppSecにとって強力なツールです。

Contrast Assessと既存QAツールの統合

殆どの企業はDASTを単なる必要要件として使用しています。Contrastはその要件を満たし更に詳細情報を高速に検出することができ従来のDASTに対する厳しい要求は削減されます。この場合、 Burp Suiteのようなシンプルで広く受け入れられているツールを使用し、アプリケーションにContrastを追加することをお勧めします。Burp Suiteは、Webアプリケーションの調査、プローブ、監査のための強力な機能を有しています。Contrastは、Burp Suiteのようなアプリケーションと接続し、アタックサーフェスの詳細なコンテキスト（前後関係)を表示することができます。

このアプローチを採用することでIASTと従来のDASTの両方の利点を活用することができます。IASTの精度とBurp Suiteのようなツールの広範なWebコード分析によりセキュリティテストの包括的な要件を満たします。その結果、より合理的、効率的かつ効果的なAppSecテストプロセスに改善し堅牢なセキュリティ対策を確保しながら、トータルコストを最小限に抑えることができます。

まとめ

AppSecテストの将来を考える上で、Contrast AssessのようなIAST型のDASTは、DASTの長所を有すると同時に、その長所を超える性能であるため活用が推奨されています。アプリケーションの全体像を把握し、内部から脆弱性を浮き彫りにし、優れた精度と詳細情報を提供することができます。従ってIASTは従来のDASTを効果的に置き換えることができ、DASTによる複雑さとトータルコストを削減することができます。

Contrast Securityについて

Contrast Securityは、グローバルビジネスに欠かす事のできないWebアプリケーションのコードを安全にします。最先端で包括的なContrastのアプリケーションセキュリティプラットフォームは、セキュリティの非効率性を取り除き、開発者がセキュアコーディングを実現しながら迅速にアプリケーションをリリースできるようにします。 Contrastのアプリケーションセキュリティプラットフォームは、コード分析と攻撃防御を行うエージェントをWebアプリケーションに直接組み込むことにより、カスタムコードとオープンソースライブラリーの脆弱性を高精度で自動で検出します。開発者に検出された脆弱性と修正方法を提供し、脆弱性を簡単かつ迅速に修正することができます。このプラットフォームによって、開発、テスト、運用担当がより効果的に協力し、デジタルトランスフォーメーション推進を加速することができます。世界の大手企業および公的機関の多くが、開発中のアプリケーションでセキュアーコーディングを実施し、さらに運用中のクラウドおよびオンプレミスアプリケーションを防御するために、Contrastを採用しています。

お問い合わせ：JPNSALES@contrastsecurity.com