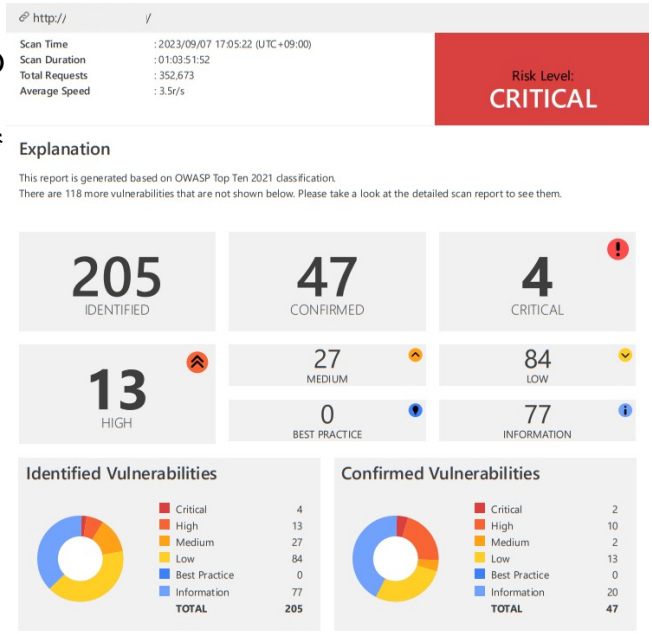
Invicti Web脆弱性スキャナ

高精度・高速・API対応を両立する
統合型のWeb脆弱性対策プラットフォーム

近年、Webアプリケーションは企業活動の中核を担う一方、攻撃手法の高度化や開発スピードの加速により、脆弱性の見落としや修正の長期化が重大なリスクとなっています。特に継続的なリリース環境では、従来型の手動検査だけでは網羅的な対策が困難です。
Invictiは自動化された高精度な脆弱性診断に加え、Proof-Based Scanning™により、検出された脆弱性の実在性についても自動で検証可能です。これにより、継続的なセキュリティ検証と迅速な修正を実現し、Webアプリケーションの安全な運用を支援します。
InvictiにはEssentials／Professional／Ultimateの3プランが展開されており、自社の規模や運用要件に応じて最適な機能レベルを柔軟に選択できるライセンス体系を提供しています。



特長

■ 自動化されたWeb脆弱性スキャン
Invictiは、対象URLのクロール（ページ構造の把握）から入力ポイントの特定、疑似攻撃リクエストの生成・送信、レスポンス解析、脆弱性判定までの一連の診断プロセスを自動化しています。さらに認証が必要な領域へのログイン処理やセッション維持、スキャン結果の整理・レポート生成も自動で実行されるため、運用負荷を抑えつつ高精度な継続診断を実現できます。

■ DAST＋IASTによるハイブリッド検査
動的解析（DAST）に加え、必要に応じてインタラクティブ解析（IAST）を組み合わせることで、実行時の挙動を踏まえたより深い脆弱性検出が可能です。これにより検出の網羅性と現実的なリスク把握が向上し、効率的な優先順位付けにつながります。

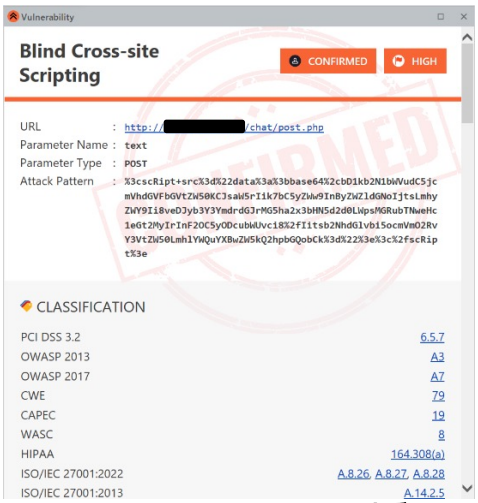
■ 開発プロセス（CI/CD）との統合
InvictiはCI/CDツールやチケット管理システムと連携し、開発ライフサイクルの中にセキュリティ検査を組み込むことが可能です。これによりリリース前後での継続的な検証と迅速な修正対応が実現し、DevSecOpsの推進を支援します。

■ スケーラブルなエンタープライズ対応
大規模環境にも対応可能な設計となっており、多数のWebアプリケーションやAPIを一元管理できます。複数部門・複数システムにまたがるセキュリティ対策を統合的に実施できるため、組織全体でのガバナンス強化に寄与します。

■ 詳細なレポーティングとリスク可視化
検出された脆弱性は、技術者向けの詳細情報から管理者向けのサマリーまで多様な形式でレポート化されます。これにより関係者間での情報共有が円滑になり、修正対応の優先順位付けや経営レベルでの意思決定にも活用できます。

高精度のスキャン

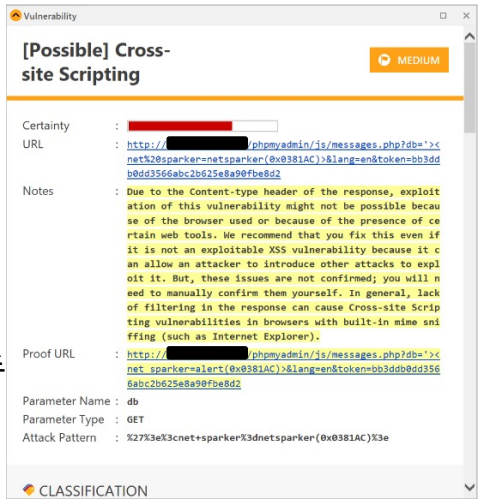
Invictiは、高度なスキャンエンジンと継続的な研究に基づき、実運用環境に即した高精度な脆弱性検出を実現します。単なるパターンマッチングではなく、アプリケーションの挙動やレスポンスを精緻に解析することで、誤検知を抑えつつ本当にリスクとなる脆弱性を的確に特定します。
これにより、開発者やセキュリティ担当者は無駄な検証作業に時間を費やすことなく、優先度の高い対応に集中することが可能になります。
さらにInvictiは、脆弱性検出およびその結果を出力するレポートなどの精度を高める独自技術、Proof-Based Scanning™により、検出した脆弱性の実在性を自動的に検証します。



Proof-Based Scanningによる実在性確認済の脆弱性

■ **Proof-Based Scanning™**

Proof-Based Scanning™は、検出された脆弱性に対して安全な方法で疑似的な攻撃を実施することで、脆弱性が実在するものであるか、誤検知であるか、を自動的に検証します。検証の精度は99.98%（メーカー調べ）に達し、Proof-Based Scanning™により実在性が確認された脆弱性は、右図のように『確認された脆弱性』として報告されます。
そのため、検証済みの脆弱性については、ユーザー自身で誤検知か否かを検証する必要が原則としてなくなり、検出結果の裏付け確認や再現テストの工数を大幅に削減し、迅速かつ確実な修正対応を支援します。
なお、自動検証が行われていない脆弱性については、各脆弱性の詳細確認画面にて、実在性確認済みの脆弱性と区別可能です。未検証の脆弱性の場合、確認画面では脆弱性の実在確度が示されており、手動検証等の対応優先度を検討する際の考慮材料となります。



実在性未確認の脆弱性

スキャン後の対応まで一元化

Invictiは、脆弱性の検出にとどまらず、その後の分析・対応・管理までを単一のプラットフォーム上で一貫して実行できる統合的なアプリケーションセキュリティ（AppSec）環境を提供します。スキャンによって検出された脆弱性は自動的に分類・整理され、技術者向けの詳細レポートから管理者向けのサマリーまで、目的に応じた形式で出力することが可能です。これにより、関係者間での認識齟齬を防ぎながら、迅速かつ的確な対応を促進します。
さらに、脆弱性は深刻度やビジネスへの影響度に基づき優先順位付けされるため、対応すべき課題が明確になり、限られたリソースの中で効率的にリスク低減を進められます。加えて、検出結果は単発で終わることなく、過去のスキャン履歴や対応状況とともに一元的に管理されるため、修正の進捗や再発の有無を継続的に追跡することが可能です。
また複数のWebアプリケーションやAPI、さらには異なる部門・プロジェクトにまたがる診断結果も統合的に可視化されるため、組織全体のセキュリティレベルを俯瞰しながらガバナンスを強化できます。これにより、従来のように複数ツールを組み合わせて運用する必要がなくなり、診断、分析優先順位付け、修正管理、レポーティングまでを一つの基盤で完結させることが可能となります。

出力レポート例
（脆弱性修正状況の比較レポート）

お問い合わせ
ComWorth
株式会社コムワース 通信機器事業部
TEL: 03-3777-0888 FAX: 03-3772-8497
Web: https://www.comworth.co.jp
Mail: info2@comworth.co.jp