

Syhunt Dynamic Augmentedは、セキュリティテストを完全に自動化し、あらゆる種類のアプリケーションから組織のWebインフラをプロアクティブに保護するWebアプリケーションセキュリティスキャナーです。

Augmented Dynamic Analysisにより、推論攻撃、帯域内攻撃、帯域外攻撃を含むセキュリティ脅威を解決



ダイナミックアプリケーションセキュリティテスト

- 推論攻撃、帯域内攻撃、帯域外攻撃など、70以上のカテゴリーに分類される**5700以上**の動的なWebアプリケーションのセキュリティ脆弱性。
- あらゆる種類のライブWebアプリケーション、特にASP.NET(# & VB Net)で書かれたWebアプリケーションをスキャンします。**ASP.NET (C#とVB.Net)、Java (JEE / JSP)、JavaScript、Node.js、Lua、Perl、PHP、Python、Ruby**で書かれたWebアプリケーションをスキャンします。
- Webアプリケーション層の完全な侵入テストを実行できる。
- アプリケーション層の完全な侵入テストを行うことができる。
- **ディープクロール**(スパイダリング)、完全な自動ウェブサイト構造マッピング、エントリーポイントの特定(すべてのリンク、フォーム、XHRリクエスト)、**HTML5とJS**のサポート。
- 様々なサーバ(**Apache、Tomcat、IIS、Nginx**など)、プラットフォーム(Windows、Unixなど)で動作する様々なフレームワークを使用したWebサイトのテストに最適です。

カバレッジと統合

- Webアプリケーションセキュリティの最も重要な脆弱性トップ10、PHPトップ5脆弱性、その他のOWASPリスト、XSS(クロスサイトスクリプティング)、SQLインジェクション、ファイルインクルージョン、コマンド実行などを静的および動的解析によりスキャンします。
- 17種類以上のデータベースを対象としたSQL Injectionの脆弱性を検出します。
- 継続的インテグレーション(CI)と課題追跡のための**GitHub、GitLab、Jenkins、JIRA**、仮想脆弱性パッチのための**Imperva、F5 BIG-IP ASM、ModSecurity**と統合されています。

帯域外アプリケーションセキュリティテスト

- コマンド実行、リモートファイル挿入、サーバーサイドリクエストフォージェリ、SQLインジェクション、XXEインジェクションの見えない、帯域外の亜種を検出します。
- このような脆弱性は、従来のDASTでは検出することができません。
- スキャン期間中、脆弱なターゲットWebサーバーから強制的に送られてくるリクエストをリスニングします。
- 脆弱性のあるターゲットWebサーバーからのデータ流出を実証します。
- **偽陽性はゼロ**で返されます。

報告書作成

- 特定された脆弱性の詳細、グラフ、統計、CVEや**CWE**などのリファレンスを含む包括的なレポートを作成します。
- **CVSS3** Vectors：脆弱性の深刻度を伝え、対応の緊急性や優先度を決定するのに役立つもので、特定した欠陥をCVSSスコアに基づいて分類しています。OWASP Top 10、OWASP PHP Top 5、CWE/SANS Top 25、WASC Threatに関連したコンプライアンス情報。
- 分類、PCI DSS基準など。脆弱性の時間的な進化を表示。**HTML、PDF、JSON、XML、テキスト、CSV**など、複数のファイル形式で利用可能。

Syhuntの詳細については、<https://www.syhunt.jp>をご覧ください。