

../SYHUNT/DYNAMIC



ウェブアプリケーションセキュリティスキャナー

Syhunt Dynamic® (旧名Sandcatスキャナー) 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セキュリティの脅威から組織のWebインフラを積極的に保護するWebアプリケーションセキュリティスキャナーです。

主な特長

Syhunt DynamicとURLを入力するだけで、簡単に利用できます。

- 800以上の動的なWebアプリケーションのセキュリティチェックを実行します。
- 70種類のウェブ攻撃-を含む。
- 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。
- OWASPの最も重要なWebアプリケーションセキュリティ脆弱性トップ10とPHPトップ5の脆弱性 特定のWebアプリケーションやサーバーに影響を及ぼす既知の脆弱性について、数千もの追加動的チェックを実行します。
- Webサイト全体の構造を自動的にマッピングし、インジェクションやディレクトリ、認証のブルートフォースチェックを実行するディープクロウリング(スパイダリング)を実行します。
- あらゆる種類のウェブアプリケーションをスキャン



ディープクロウラー

Syhunt Dynamicは、Webサイト全体の構造 (すべてのリンク、フォーム、XHRリクエスト、その他のエントリポイント) をマッピングし、幅広い攻撃のシミュレーション/数千のリクエストの送信により、カスタムでユニークな脆弱性を見つけます。スキャナーは、Chrome、Firefox、IEのように動作し、ユーザーのインタラクション(キープレス、マウスクリックなど)までもシミュレートします。

アドバンストインジェクター

SQL インジェクション、XSS、ファイルインクルージョン、その他多くのウェブアプリケーション脆弱性クラスをテストします。スキャン実行中、Syhunt はウェブアプリケーションにデータを注入し、その後、アプリケーションコードが脆弱であるかどうかを判断するために、アプリケーションのレスポンスを分析します。

あらゆる種類のウェブ環境をスキャンする

Syhunt Dynamic は、あらゆるウェブ環境を、あらゆる場所でサポートするために必要な、柔軟性と汎用性を備えています。複雑で大規模なWebサイトをインテリジェントに処理し、異なるWeb環境と技術に自動的に適応するように設計されています。Webサイトのスパイダリングや脆弱性調査において、Syhunt Dynamicは最新のHTML 5対応Webブラウザをエミュレートし、すべてのWebアプリケーションを完全にテストすることができます。Syhunt のブラウザエミュレーション機能セットには以下が含まれます。

- インテリジェントなHTMLパース（ウェブブラウザのように不正なHTMLを処理する）
- JavaScriptエミュレーション（Chrome、Firefox、IEとして動作可能）、XHRリクエスト対応 ユーザーインタラクションシミュレーション（キープレス、マウスクリックなど）。
- HTML 5対応、CSS 3対応 自動フォーム入力・フォームログイン
- プロセス分離/マルチプロセススキャン（開始する各ウェブサイトのスキャンは、オペレーティングシステム上で異なるプロセスです。）
- クッキー対応
- HTTPS対応（SSL 2 / SSL 3 / TLS 1）証明書対応
- Basic & NTLM認証サポート HTTP 1.0および1.1サポート
- Keep-Alive対応 HTTPリダイレクト対応



Syhunt Dynamic scannerがサポートする主要技術の一部をご紹介します。



詳細なレポートを作成する

Syhunt Dynamicは、脆弱性の詳細を含む包括的なレポートを生成する機能を備えています。攻撃に対するアプリケーションの応答を調査した後、ターゲットURLが脆弱であることが判明した場合、レポートに追加されます。Syhunt Dynamicのレポートには、チャート、統計、コンプライアンス情報も含まれており、さまざまな対象者向けにカスタマイズされたレポートテンプレートのセットも用意されています。Syhuntの完全なレポートには通常以下が含まれます。

- CVE、NVD、CWE、Bugtraq、OSVDBなどの脆弱性情報およびリファレンス。CVSS3/CVSS2 スコアとベクトル情報。
- 比較情報 - 過去のスキャンセッションデータを比較することで、脆弱性を時系列で進化させることができます。
- コンプライアンス情報 - OWASP Top 10、PHP Top 5、CWE/SANS Top 25、Payment Card Industry (PCI) など。

現在、Syhunt Dynamic は、HTML、PDF、XML、Text、CSV、RTF、XLS、DOC、NBEなどのフォーマットでレポートを作成し、データをエクスポートすることが可能です。結果はいつでもHTMLや複数の利用可能なフォーマットに変換でき、新規、変更なし、削除された脆弱性を判断するために比較することができます。



上位の脆弱性をチェックする

Syhunt Dynamicは、Webアプリケーションに対して攻撃者が使用するトップレベルの脆弱性をスキャンすることができます。

OWASPトップ10

OWASP Top Ten は、早急な対処が必要な脆弱性のリストです。これらの脆弱性は、攻撃者によって積極的に狙われているため、既存のコードも直ちにチェックする必要があります。OWASP財団は、Webアプリケーションを保護するための最低基準として、OWASP Top Tenを採用することを企業に推奨しています。

SANSトップ20

SANS Top 20には、セキュリティ上の欠陥を修正するために有効なステップバイステップの手順と追加情報へのポイントが含まれています。SANS Instituteは、より重大な脅威や、より最新で便利な保護方法が確認された場合、リストと説明書を更新します。これは、コミュニティの合意文書です。

コンプライアンス監査

Syhunt Dynamicは、以下のようなコンプライアンスに関する最も差し迫った問題に対処するための支援を提供します。

- 医療保険の相互運用性と説明責任に関する法律 (HIPAA)
- グラム・リーチ・ブライリー (GLBA)
- PCI (Payment Card Industry) データセキュリティ基準
- CA-SB1
- Sarbanes-Oxley

CVE と CWE

Syhunt Dynamicは、CVE (Common Vulnerabilities and Exposures) と CWE (Common Weakness Enumeration) を完全にサポートしており、Webアプリケーションに関連するCWEトップエントリをスキャンすることができます。

Syhuntは、Mitre CorporationのCVE-互換製品・サービスリストにも掲載されています。Mitre Corporationは、この規格自体の作成者である。



手作業でテストしていたら見逃していたようなSQLインジェクションやXSSの脆弱性を数多く発見することができました。Syhuntの最も良い使い方の1つは、ソースコード解析とダイナミックスキャナーを組み合わせ、本当の問題に素早くズームインすることです。

Arthur Donkers、セキュリティ 役員



Syhuntのようなツールは、アプリケーションの脆弱性をより簡単に検出することができ、もはや「ハッカー」レベルのスキルセットを必要としません。

SCマガジン

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

