

## テクノロジー

当社のイノベーションへのコミットメントにより、当社は最適な Web サイトのセキュリティを提供することができます。

GamaSec は、Web サイトおよび Web アプリケーションの脆弱性を識別するための業界最先端のクラウドベース (SaaS) ソリューションを提供します。競合他社とはまったく異なるテクノロジーバックボーンを基礎にして構築された GamaSec は、従来のシグネチャベースのスキヤナを超えて、より詳細できめ細かい検査に基づいて、より現実的な脆弱性を発見します。

GamaSec は、スキャンされたオブジェクトを操作してマルウェア攻撃の可能性を効果的に検出する多層型の脅威分析手法を組み込んでいます。ヒューリスティック技術は、悪意のある Web コンテンツを完全に分類して革新的なマルウェア検出を提供する Malicious Content Detection エンジンと組み合わせられています。

GamaSec スキャナーは Web アプリケーション環境全体を探索し、その構造と内容を登録します。次に、実際のハッキング方法を模倣して、次のような攻撃に対して脆弱なあらゆる点の詳細を特定して明らかにします。

- SQL インジェクション攻撃 - データベースサーバに任意の SQL を実行させようとしています。
- クロスサイトスクリプティング攻撃 - 第三者の Javascript を出力するようプログラムに強制しようとしています。
- パラメータ操作攻撃 - アプリケーションの検証とフィルタリングへの入力进行操作しようとしています。
- コードインジェクション攻撃 - 任意のコードを実行しようとしています。
- 隠しタグの問題 - 隠しタグを使用してフォームにハードコードされた、価格などの機密情報の取得を試みます。

Web スキャナーは、さまざまな脆弱性を発見するために使用される可能性があります。検出後、実際には脆弱なデータを保護するためのソリューションをお勧めします。

### GamaScan がカバーするアプリケーション脆弱性攻撃

- SQLI インジェクション

- ブラインド SQL インジェクション
- インストールパスの開示
- 正味例外
- コマンド実行
- PHP コードインジェクション
- Xpath インジェクション
- CRLF インジェクション
- ディレクトリトラバーサル開示
- スクリプト言語エラー
- URL リダイレクト
- リモートファイルインクルード
- LDAP インジェクション
- クッキー操作
- ソースコード
- クロスサイトスクリプティング
- クロスフレームスクリプティング
- 内部 IP 開示

#### GamaScan がカバーする一般テスト

- Web サーバー
- Web サーバーテクノロジー
- HTTP メソッド
- バックアップファイル
- ディレクトリ列挙
- ディレクトリインデックス
- ディレクトリアクセス
- ディレクトリ許可
- 機密ファイル/共通ファイル
- 第三者の申し込み

GamaScan は、お客様の Web サイトでセキュリティの脆弱性とマルウェアの検出を識別するだけでなく、最も適切な解決策をお勧めします。修正または回避策の解決策は、遅すぎる場合ではなく、必要なときに識別および実装されます。