脅威の分類

- 機能の悪用
- アプリケーション・コード実行
- アプリケーションの設定ミス
- autocomplete 属性
- ブルートフォース
- バッファオーバーフロー
- キャッシュ可能なセンシティブな応答
- クリックジャッキング
- コンテンツ・スプーフィング
- クロスサイト・リクエスト・フォージェリ
- クロスサイト・スクリプティング
- サービス拒否
- ディレクトリ・リスティング
- フィンガープリンティング
- フレーマブル・リソース
- HTTP レスポンス分割
- 不適切な入力確認
- 情報漏洩
- 安全でないインデックス化
- 自動化の停止が不適切
- 不適切な許可
- 不適切なパスワードポリシーの実装
- 不適切なパスワード回復
- 不適切なプロセス検証
- 不適切なセッション有効期限
- 不十分なトランスポート層の保護
- LDAP インジェクション
- メール・コマンド・インジェクション
- セキュア・ヘッダーの欠落
- HttpOnly 属性のないセッション・クッキー
- OS コマンド・インジェクション
- OS コマンドの実行
- パス・トラバーサル
- 推測可能なリソースの位置
- クエリー言語インジェクション
- リモート・ファイル・インクルード
- ルーティングの迂回
- サーバーの設定ミス
- セッション ID の固定化
- 証明書とセッションの推測
- SQL インジェクション
- SSI インジェクション
- パッチ未適用のソフトウェア
- 安全でないセッション・クッキー
- URL リダイレクトの悪用
- XML 外部実体参照
- XML インジェクション
- XPath インジェクション
- XQuery インジェクション

OWASP Top 10

- A1 - アクセス制御の不備
- A2 - 暗号化の失敗
- A3 - インジェクション
- A4 - 安全が確認されない不安な設計
- A5 - セキュリティの設定ミス
- A6 - 脆弱で古くなったコンポーネント
- A7 - 識別と認証の失敗
- A8 - ソフトウェアとデータの整合性の不具合
- A9 - セキュリティログとモニタリングの失敗
- A10 - サーバーサイドリクエストフォージェリ (SSRF)

* 製品ラインごとの互換性リストについては
お問い合わせください。

シノプシスの特色

シノプシスがご提供する統合型ソリューションは、ソフトウェア開発とデリバリのあり方を根底から変革し、ビジネス・リスクに対処しながらイノベーションを加速することを可能にします。シノプシスのソリューションにより、開発者はスピードを落とすことなくセキュアなコードを作成することができます。開発および DevSecOps チームはスピードを犠牲にすることなく、開発パイプライン内でテストを自動化できます。セキュリティ・チームは先手を打ったリスク管理が可能となり、組織にとって最も重要な問題の修正に集中できます。シノプシスは業界随一のノウハウを活かし、最適なセキュリティ・イニシアティブの立案と実行をご支援します。信頼性の高いソフトウェアの構築に必要なものをワンストップでご提供できるのは、シノプシスだけです。

詳しくは、www.synopsys.com/jp/software をご覧ください。

日本シノプシス合同会社 ソフトウェア インテグリティ グループ
〒 158-0094 東京都世田谷区玉川
2-21-1 二子玉川ライズオフィス
TEL: 03-6746-3600
Email: sig-japan@synopsys.com
www.synopsys.com/jp/software