AKAMAI チェックリスト

OWASP トップ 10 API セキュリティ

API は、特にマイクロサービスベースのアーキテクチャへの移行が進む中においては、最新のアプリケーションの構築と接続の標準になっています。そのため、Open Worldwide Application Security Project (OWASP) で特定された一般的な API セキュリティリスクから、組織を保護することが重要です。2023 年度版のリストをご覧いただき、API セキュリティ確保の方法を意思決定する際にお役立てください。

Akamai の OWASP API トップ 10 の対応範囲

- **API1:2023 – オブジェクトレベルの認可の不備 (BOLA)：**この脆弱性は、特定のオブジェクト ID にアクセスする際にクライアントの認可が適切に検証されていない場合に存在します。
- **API2:2023 – 認証の不備 (BA)：**認証の不備は、認証プロセスにおける幅広い脆弱性を指しています。この脆弱性によってシステムが攻撃者に晒されてしまい、弱点が悪用され、API オブジェクト保護が侵害されます。
- **API3:2023 – オブジェクトプロパティレベルの認可の不備 (BOPLA)：**このセキュリティ上の欠陥では、API エンドポイントがその機能に求められている以上にデータプロパティを不必要に公開してしまい、最小権限の原則を無視することに繋がります。
- **API4:2023 – 制限のないリソース消費：**これは、API リソースの枯渇と呼ばれる脆弱性の一種です。この脆弱性は、API が特定の時間内で提供するリクエストの数やデータの量を制限しないことで起こります。
- **API5:2023 – 機能レベル認可の不備 (BFLA)：**このリスクは、API エンドポイントのアクセス制御モデルの実装が不適切な時に起こることがあります。
- **API6:2023 – 機密性の高いフローへの制限のないアクセス：**このリスクは、API が、十分なアクセス制御を行わないまま、ビジネスロジックのような重要な操作を公開する場合に発生します。
- **API7:2023 – サーバーサイドリクエストフォージェリ (SSRF)：**この攻撃を使用すると、攻撃者はサーバーサイドアプリケーションを操って、攻撃者が選んだ任意のドメインへの HTTPS リクエストを実行することができます。
- **API8:2023 – セキュリティの設定ミス：**これは、セキュリティ制御のセットアップが不適切である状態を指します。この状態では、システムが攻撃に対して脆弱なままになってしまいます。
- **API9:2023 – 不適切なインベントリ管理：**これは、API を管理するすべての組織にとっての課題です。API セキュリティソリューションは既知の API を保護できますが、廃止された API、レガシー API、古い API などの未知の API には、パッチが適用されず、攻撃に対して脆弱である場合があります。
- **API10:2023 – API の安全でない使用：**適切なセキュリティ対策を講じずにサードパーティー API を使用することに関連するリスクを指します。

2019 年と 2023 年の OWASP トップ 10 API セキュリティリスクの違いについて詳しくは、このブログ記事をご覧ください。

Akamai と協力する

組織とそのセキュリティベンダーは緊密に連携し、人、プロセス、テクノロジー全体を調整して、OWASP トップ 10 API セキュリティリスクに記載されているセキュリティリスクに対して強固な防御策を講じる必要があります。

Akamai について

Akamai は、業界をリードするセキュリティソリューション、経験豊富なエキスパート、Akamai Connected Cloud により、毎日数百万の Web アプリケーション攻撃、数十億のボット要求、数兆の API 要求から知見を収集します。Akamai の Web アプリケーションおよび API のセキュリティソリューションは、最先端の Web アプリケーション攻撃、分散型サービス妨害 (DDoS) 攻撃、API ベースの攻撃から組織を保護します。

 | サポート | 公開日：2023 年 8 月