ホワイトペーパー

OWASP Top 10 API セキュリティリスクに対する防御計画

API の一般的な脆弱性と脅威への対処における Akamai の役割

OWASP Top 10 API セキュリティリスク		Akamai による保護
API1:2023	オブジェクトレベルの認可の不備（BOLA）	✓
API2:2023	認証の不備（BA）	✓
API3:2023	オブジェクト・プロパティ・レベルの認可の不備（BOPLA）	✓
API4:2023	制限のないリソース消費	✓
API5:2023	機能レベルの認可の不備（BFLA）	✓
API6:2023	機密性の高いフローへの制限のないアクセス	✓
API7:2023	サーバーサイド・リクエスト・フォージェリ（SSRF）	✓
API8:2023	セキュリティの設定ミス	✓
API9:2023	不適切なインベントリ管理	✓
API10:2023	API の安全でない使用	✓

API は、エンタープライズのデジタル製品、サービス、クラウド環境で中心的役割を担っています。また、アプリケーション開発において組織がマイクロサービスベースのアーキテクチャへの移行を進める中で、API はアプリケーションの構築と接続の標準にもなっています。しかしながら、データと重要なシステムに繰り返しアクセスする API は、収益拡大の推進力であると同時に運用上のリスクをもたらす存在になりました。

それは、公開された API や設定ミスのある API は至るところにあり、簡単に侵害でき、多くの場合保護されていないためです。そして、たった 1 つの API が侵害されただけで数百万もの記録が盗まれる可能性があります。

組織の 78% が 1 年間で API のセキュリティインシデントを経験した、と報告している状況を踏まえれば、API の保護が優先事項であることは明らかです。しかし、API アタックサーフェスは格好の標的として急浮上しており、そのスピードは、ほとんどのエンタープライズが以下の点について理解を深めてきた速度をはるかに上回ります。

API のリスク

API 攻撃の手法

API セキュリティの制御と機能

API のアタックサーフェスは、どのようなもので構成されるのでしょうか。端的に言えば、多くの組織が認識しているよりもはるかに広い範囲が対象となります。API に対するこれまでの解釈は、たとえばマシンツーマシン API やサードパーティ API などの場合、マイクロサービスベースのアーキテクチャの一部としてモバイルサービスや Web アプリケーションサービスにまで広げることができ、またそうすべきです。つまり、そうしたアーキテクチャ内の 1 つの Web リクエストは、さまざまなマイクロサービスの一連の呼び出しの中の 1 つとして機能する API になります。

78%

1 年間で API のセキュリティインシデントを経験した、と報告している組織の割合。API の保護が優先事項であることは明らかです。

2023 年 6 月 5 日、その活動が高く評価されている Open Worldwide Application Security Project（OWASP）は、2019 年にリリースされた最初の Top 10 API セキュリティリスクのリストに対する初の大規模アップデートを発表しました。この最新版リストでは、こうした API 呼び出しのそれぞれがどのようにしてセキュリティホールとプライバシーリスクの原因となり得るか、以下の点を含めて説明しています。

不十分なデータ検証

設定エラー

実装の欠陥

セキュリティコンポーネント間の統合ギャップ

OWASP が特定した主なリスクと、Akamai の API セキュリティソリューションがそのリスクを緩和する方法について、詳細をご確認ください。

問題は、API の完全なインベントリを作成していると主張する組織でさえ、深刻なギャップがあることです。

呼び出しに応じてどの API が機微な情報を返すのか、把握しているのは **10 社中 4 社**にすぎません。

API1:2023 — オブジェクトレベルの認可の不備（BOLA）

オブジェクトレベルの認可の不備（BOLA）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。この脆弱性は、リソースに直接アクセスし、予期されたアプリケーションのワークフローを迂回して、機微な情報に不正アクセスするチャンスを攻撃者に与える恐れがあります。組織は、クライアントからのリクエストで渡されたオブジェクト ID だけに依存しないようにすることで、このリスクを軽減できます。または、推測不可能なランダムな ID をオブジェクトに使用することで、すべてのオブジェクトに対して強固な検証を行うことも有効です。必要に応じて実際のオブジェクト ID にマスク処理を行い、セキュリティのレイヤーを追加することができます。

Akamai の役割

Akamai の警戒監視システムは脅威を追跡し、BOLA の悪用が試みられた場合にアラートを生成することで、迅速な対策と対応を可能にしています。

Akamai のリスク緩和策：

- BOLA 悪用の試みを特定
- API オブジェクトとプロパティ間の関係だけでなく、受け取った入力（一連のパラメーターなど）に基づいて、BOLA 悪用の影響を受けやすい API エンドポイントを分類する
- BOLA 悪用の試みまたは成功を検知してアラートを生成する

API2:2023 — 認証の不備（BA）

認証の不備とは、認証プロセスにおける幅広い脆弱性を指します。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。一般に、認証の不備による脆弱性を利用する攻撃者は、脆弱なパスワードやセッションリプレイなど、システムの抜け穴を悪用します。認証の不備による脆弱性への対策としては、強力なパスワードポリシー、キーローテーション、強力なトークン署名、暗号化キーなど、堅牢な認証と機密管理のメカニズムを確立することが有効です。このような厳格なポリシーを組織全体で徹底することで、リスクを大幅に軽減することができます。

Akamai の役割

Akamai は、脆弱な認証ポイントの特定と修正、自動化された攻撃の阻止、および悪用の試みに対する予防的な警告により、API セキュリティを強化します。

Akamai のリスク緩和策：

- 認証を必要としない API エンドポイント、または認証のベストプラクティスに従っていない（例：脆弱なトークン署名や暗号化キー、期限切れ認証トークンの受け入れなど）API エンドポイントを特定する
- ボット管理機能により、自動化された辞書攻撃や Credential Stuffing 攻撃から保護する
- Akamai の API Gateway 機能により、強力なトークン署名を使用して JSON Web Tokens の認可を処理する
- BUA 悪用の試みを検知してアラートを生成する

API3:2023 — オブジェクト・プロパティ・レベルの認可の不備（BOPLA）

オブジェクト・プロパティ・レベルの認可の不備（BOPLA）とは、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つながる、セキュリティ上の欠陥です。

この欠陥は、攻撃者に不用意に過剰なデータを提供する可能性があり、そのデータはさらなる脆弱性の発見や機微な情報のマイニングに使用される可能性があります。これには、管理者レベルのアクセスに限定されたプロパティが、権限のないユーザーによって操作され、システムの完全性がさらに損なわれるというシナリオも考えられます。セキュリティを維持し、攻撃者による余分な情報の入手や操作を防ぐためには、適切なアクセスレベルとデータ流出を設定して、潜在的な攻撃者がこれらの不備を悪用するのを阻止することが重要です。

Akamai の役割

Akamai の包括的な戦術を活用することで、企業は API エンドポイントとその関連プロパティを特定してカタログ化し、BOPLA のリスクを緩和することができます。

Akamai のリスク緩和策：

- 個人を特定できる情報（PII）など、すべてのエンドポイントとそれらが公開する API プロパティを識別し、ラベル付けを行う
- 文書化されていない API やシャドウ API のエンドポイント、オブジェクト、プロパティ、および異常なプロパティを特定する
- データのサニタイズ（無害化）を確実に行うため、許容可能で定義されたパラメーターとプロパティにセキュリティポリシーを適用する
- 完全な OpenAPI（Swagger）仕様に基づくセキュリティポリシーを適用し、明確に定義された API エンドポイントとメソッドのみが API オブジェクトとプロパティにアクセスできるようにする
- BOPLA 悪用の試みを検知してアラートを生成する

API4:2023 — 制限のないリソース消費

制限のないリソース消費（「API リソース枯渇」と呼ばれることもあります）とは、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る脆弱性の一種です。この脆弱性を見落とすと、サービス妨害（DoS）攻撃を行おうとする攻撃者に絶好の機会を与える恐れがあり、その結果、正規のユーザーがシステムを利用できなくなる可能性があります。このような悪用はビジネスに深刻な影響を及ぼしかねません。サービス停止の期間や範囲によっては、サービス可用性や顧客満足度の低下、収益損失につながります。サービスの損失を防ぐためには、API リクエストのレートと返されるデータのサイズを制限する対策を講じることが重要です。

Akamai の役割

Akamai は、次のような方法で、制限のないリソース消費の脅威から API を保護します。

- 危険な状態にあるエンドポイントを特定し、ボリューム型攻撃の試みに対してリアルタイムアラートを提供する
- 過剰なエラー、ログイン試行、リスクを示唆する変則的なふるまいを検出する

Akamai のリスク緩和策：

- レート制限に不備があるか、大規模なボリューム型辞書攻撃や Credential Stuffing 攻撃を受けている API エンドポイントを特定する
- ボリューム型攻撃を抑制またはブロックするワークフローを開始する
- ボリューム型攻撃の試みに対してアラートを生成する

API5:2023 — 機能レベル認可の不備（BFLA）

機能レベル認可の不備（BFLA）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場合があります。アクセス制御の方法が不適切であったり、古かったりすると、不正アクセスを適切に制限できず、攻撃者が機微な情報やシステム全体にアクセスできてしまう可能性があります。このリスクを緩和するため、組織は最小権限の原則を採用し、すべての機能、特に管理機能には、適切な権限を持つユーザーのみがアクセスできるようにすることができます。

Akamai の役割

Akamai は、行動のタイムラインを追跡し、機密性の高い機能にセキュリティポリシーを適用し、キーのローテーションと取り消しを管理して、疑わしい試みがあれば即座に警告を発することで、組織の BFLA 防止および対応戦略を強化します。

Akamai のリスク緩和策：

- ユーザー、API キー、アクセストークン、セッション ID などをキャプチャすることで、API エンドポイントアクセスの行動タイムラインを特定する
- Akamai API Gateway により、キーローテーションまたは公開されたキーの取り消しを適用する
- 管理機能に不審なアクセスがあった場合にアラートを生成する

API6:2023 — 機密性の高いフローへの制限のないアクセス

機密性の高いビジネスフローへの制限のないアクセスは、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。これは不正アクセスや悪用につながり、組織に重大な損害をもたらす可能性があります。一般的に悪用に関わる行為には、API が支えるビジネスモデルの把握、機微なビジネスフローの特定、これらのフローへの抜け穴の悪用などがあります。こうしたことが、正当なユーザーが製品を購入できなくなるなどの影響につながります。

Akamai の役割

Akamai の包括的な API 保護ソリューションでお客様のビジネスを保護し、機密エンドポイントを特定し、リアルタイムで悪用アラートを発して、専門家によるコンサルティングでお客様の重要なデータと業務を保護します。

Akamai のリスク緩和策：

- 決済フローや PII を扱うエンドポイントなど、機密性の高い API エンドポイントを特定する
- データ窃取やデータ不正操作、これらの機密 API エンドポイントでの不審な試みに至るまで、想定されるさまざまな悪用に対してアラートを生成する

API7:2023 — サーバーサイド・リクエスト・フォージェリ

サーバーサイド・リクエスト・フォージェリ（SSRF）を使用すると、攻撃者はサーバー側のアプリケーションを誘導して、攻撃者が選択した任意のドメインに HTTPS リクエストを送ることができます。典型的な SSRF 攻撃では、攻撃者がサーバーを欺いて内部リソースにリクエストを送信し、ファイアウォールを回避して内部サービスにアクセスします。これにより、データの漏洩やリモートコードの実行が発生する恐れがあります。このリスクを緩和するためには、ユーザー入力を検証、フィルタリング、またはサニタイズし、サーバーが発信できる接続を制限して、重要なサービスとのみ通信できるようにすることが重要です。

Akamai の役割

お客様は、信頼できる API 接続の異常検知、効果的なキー管理、SSRF の悪用試行に関する即時通知を提供する Akamai を使用して、セキュリティ体制を強化できます。

Akamai のリスク緩和策：

- SSRF 攻撃をターゲットとした Web アプリケーションと API 保護ポリシーによる保護を適用する
- API Gateway により、キーローテーションまたは公開されたキーの取り消しを適用する

API8:2023 – セキュリティ設定のミス

セキュリティ設定のミスとは、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。その原因は、安全ではないデフォルト設定、不完全または場当たり的な設定、オープン・クラウド・ストレージ、HTTP(S) ヘッダーの誤設定、機微な情報を含む詳細なエラーメッセージです。リスクを緩和するため、組織は、アプリケーションと API のあらゆる面でセキュリティ管理が正しく設定されているかを確認することが重要です。そのためには、定期的な更新、徹底したテスト、継続的な監視を実施し、設定ミスを速やかに特定して修正する必要があります。

Akamai の役割

Akamai は、シャドウ／不正／ゾンビ API エンドポイントの特定や、セキュリティのベストプラクティスとの整合、堅牢な HTTPS 実装の達成、セキュリティ設定のミスに対する即時アラートの受信を支援し、お客様の知見を高めます。

Akamai のリスク緩和策：

- 低レベル環境（テスト環境やステージング環境など）を公開する可能性のあるシャドウ API エンドポイントを特定する
- セキュリティ設定のベストプラクティスと標準に照らし合わせて、API エンドポイント、オブジェクト、プロパティを特定し、適合させる
- 適切な HTTPS リクエストとレスポンス、正しい HTTP ヘッダーの設定や削除、Cross-Origin Resource Sharing（CORS）とキャッシュ制御ヘッダーの完全な制御の徹底など、API セキュリティのベストプラクティスを通じてセキュリティポリシーを適用する
- 適切で安全な暗号スイートなど、SSL/TLS を介して適切な HTTPS 実装を適用する
- 設定ミスや、API セキュリティのベストプラクティスと標準への違反に対してアラートを生成する

API9:2023 — 不適切なインベントリ管理

不適切なインベントリ管理は、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、シャドウ 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。このことは、古いコンポーネント、未使用のページや API、機密情報の不必要な流出につながる恐れがあります。サービス管理の整備が不十分だと、システムが脅威に対して脆弱になり、攻撃者が同じデータベースに接続された未知の API を通じて機微な情報やサーバーにアクセスする可能性もあります。アクセス制御と定期的な監査は、組織のサービスのコンポーネントが頻繁に変更されるのを避けるためには不可欠です。

Akamai の役割

Akamai は、API トラフィックを継続的に監視し、隠れた API エンドポイントやリスクとなる可能性のある API の探索をサポートすることで、組織における安全なデータ保存、高度な脅威分析、悪用の可能性に関する即時のアラートを実現しています。

Akamai のリスク緩和策：

- 一般に公開されている API を対象とする垂直方向（North-South）の API エンドポイントや、水平方向（East-West）の内部 API エンドポイントなど、お客様の環境を流れる公開 API トラフィックを継続的に監視する
- 低レベル環境（テスト環境やステージング環境など）や文書化されていない非推奨の API バージョンを公開する可能性のあるシャドウ API エンドポイントを特定する
- リスクスコアリングとデータ分類に基づいて、最新の API インベントリを作成する
- データ窃取やデータ不正操作、これらの機密 API エンドポイントでの不審な試みに至るまで、想定されるさまざまな悪用に対してアラートを生成する

API10:2023 — API の安全でない使用

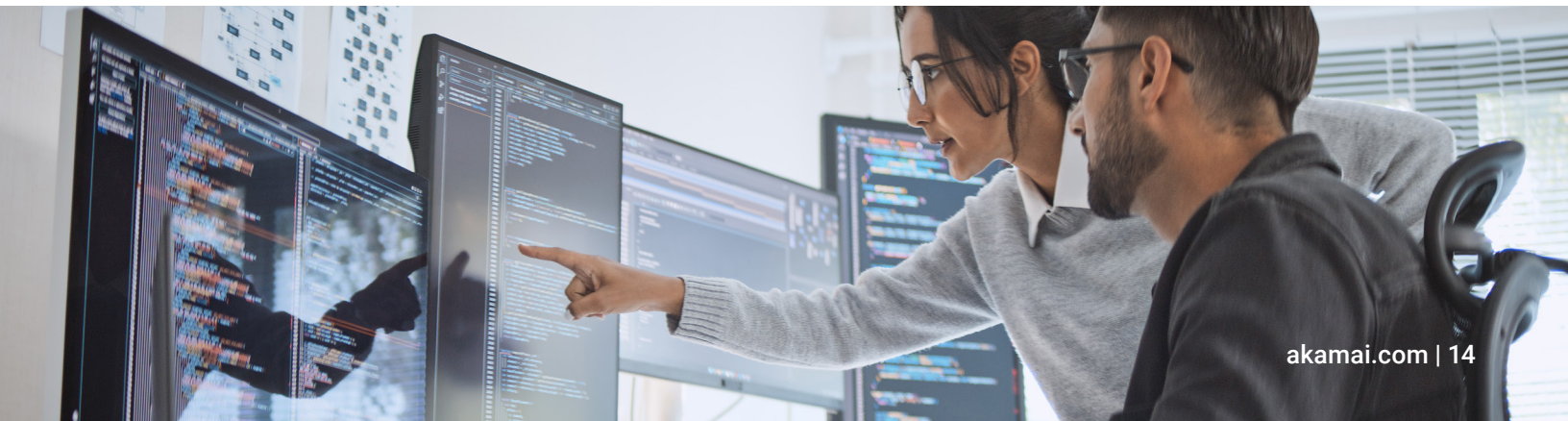
API の安全でない使用とは、適切なセキュリティ対策を伴わないサードパーティ API の使用に関連するリスクを指します。組織は、サービスや機能を拡張するために、サードパーティの API への依存度を高めているため、これらの API は通常デフォルトで信頼されています。ここに、重大なセキュリティ脆弱性につながる危険性が潜んでいます。適切な暗号化、データ検証、サニタイズ、リソース消費制限を実装しないと、組織は重大な脆弱性に晒される可能性があります。これらのリスクを緩和するために、組織はネットワーク経由で送信されるすべてのデータに対して暗号化を実施し、すべてのデータ入力を検証してサニタイズし、リソース消費に合理的な制限を設定することができます。

Akamai の役割

Akamai のモニタリング、アラート、コンサルティングサービスにより、お客様のサービスを監視および検証して、セキュリティを確保することにより、お客様のシステムを継続的に保護します。

Akamai のリスク緩和策：

- B2B やサードパーティ統合を促進する東西方向およびアウトバウンド API を含む、お客様の環境を流れるすべての公開 API トラフィックを継続的に監視する
- データ窃取やデータ不正操作、これらの機密 API エンドポイントでの不審な試みに至るまで、想定されるさまざまな悪用に対してアラートを生成する
- 攻撃グループが収集した、さまざまな API 攻撃をターゲットとした Web アプリケーションと API 保護ポリシーによる保護を適用する



OWASP によるその他のセキュリティリスク

2023 年の OWASP Top 10 API セキュリティリスクは、この非営利団体が 2019 年に発表したリストに対する初の大規模アップデートです。しかしながら、当初のリストは今見返しても示唆に富む内容であり、その中で議論しているその他のセキュリティリスク（インジェクション攻撃など）は現在の状況においても依然として重要な意味を持っています。

Akamai のセキュリティリスク緩和策：

- 署名の照合と異常の検知により、API インジェクションに対して脆弱なエンドポイントとインジェクションの試みを特定する
- API リクエストの JSON および XML 検査と、SQLi、XSS、CMDi、RFI、LFI などのさまざまなインジェクション攻撃のスキャンによって、セキュリティポリシーを適用する
- インジェクション攻撃に対してアラートを生成する

さらに、OWASP は、OWASP Top 10 Web アプリケーション・セキュリティ・リスクなど、他のトップ 10 セキュリティリスクのリストも発表しています。Akamai のセキュリティポートフォリオは、このようなセキュリティリスクの緩和にも役立ちます。

お気軽にお問い合わせください。

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 TOP 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 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、1 日数百万の Web アプリケーションおよび API 攻撃、数十億のボット要求、数兆ものAPI リクエストから知見を得るプラットフォームを提供しています。

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、DDoS 攻撃、API ベースの攻撃から組織を保護します。また、Akamai Managed Security Service は、24 時間体制の監視、セキュリティ管理、脅威の緩和を提供します。

Akamai のセキュリティポートフォリオの詳細については、当社 Web サイトをご覧ください。パートナーとして当社が貴社のビジネスに最善の保護をどのように確立できるのか、詳しくご検討されたい場合は、今すぐ Akamai の営業担当者にお問い合わせください。

Akamai のセキュリティは、パフォーマンスや顧客体験を損なうことなく、ビジネスを推進するアプリケーションをあらゆる場面で保護します。当社のグローバルプラットフォームの規模と脅威に対する可視性を活用して、お客様と Akamai が提携し、脅威を防止、検知、緩和することで、ブランドの信頼を構築し、ビジョンを実現できます。Akamai のクラウドコンピューティング、セキュリティ、コンテンツデリバリーの各ソリューションの詳細については、akamai.com および akamai.com/blog をご覧いただくか、X（旧 Twitter）と LinkedIn で Akamai Technologies をフォローしてください。公開日：2024 年 9 月。