WHITE PAPER

アプリケーションセキュリティに対する脅威の軽減

OWASP Top 10

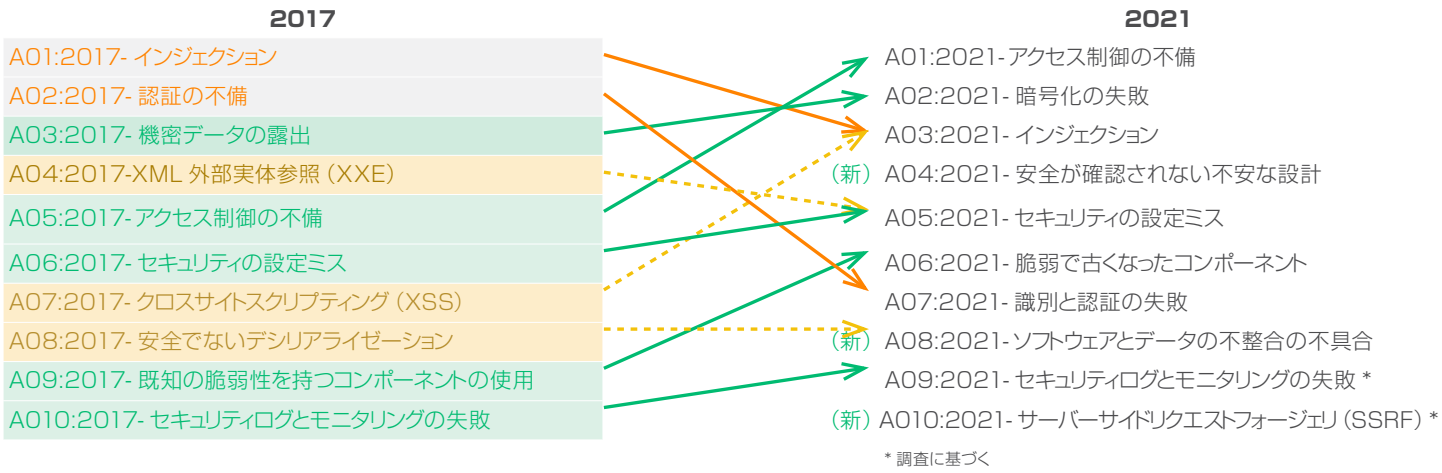
はじめに

Open Web Application Security Project (OWASP) Top 10 は、Web アプリケーションによく見られるセキュリティ上の欠陥を特定した、Webアプリケーションセキュリティ問題に対する意識を高めるための強力なレポートです。世界中のセキュリティ専門家から成るコミュニティによって作成されており、全般的なWebアプリケーションセキュリティプログラムの一環として対処すべき最も重大なWebアプリケーションセキュリティ上の欠陥として広く同意されている問題が反映されています。

OWASP Top10 は、PCI DDS(Payment Card Industry Data Security Standard)や多くの政府規制を含む、幅広い業界標準や要件に影響を与え、その検討に利用されています。OWASP Top 10 の軽減策には、安全なコーディング慣行やコードレビューなど、複数のアプローチがありますが、OWASP Top 10に関わる要件に対処するための主な方法は、やはりWAF(Web アプリケーションファイアウォール)を展開することです。

Top 10 リストの更新

OWASPチームは、脅威情勢の変化、新たなテクノロジーの登場、脅威アクターの戦術の進化に応じて、定期的にTop 10リストを更新しています。2021 年には、新カテゴリの追加、一部のカテゴリ名の変更やカテゴリの統合といった変更を行いました。OWASPによる以下の表には、それらの変更点がまとめられています。



Webアプリケーションセキュリティ上の課題

Webアプリケーションは、今も変わらず脅威アクターにとっての魅力的な標的です。現代組織に必要なビジネス環境を整えるには、一般向けのWebアプリケーションをインターネットに公開しなければなりません。そのようなWebアプリケーションは、顧客情報、クレジットカード情報、従業員情報など、最も機密性の高いデータにつながるバックエンドデータベースに接続するため、脅威アクターにとって格好の標的となっているのです。

Verizonの2022年データ漏洩調査報告書(VDBR)によると、侵害の20%以上に、基本的なWebアプリケーション攻撃(「最初にWebアプリケーションを侵害したのち、数段階のステップ踏むか、追加アクションを行うシンプルなWebアプリケーション攻撃」と定義される)が関わっています[1]。FortiGuard Labs のグローバル脅威レポート 2022年第1四半期版に記載されるように、攻撃者はWebアプリケーションの脆弱性を継続的に探索しています。(次ページの図「テクノロジー別、IPSに最も検知された脆弱性(*2021*年下期)」を参照)

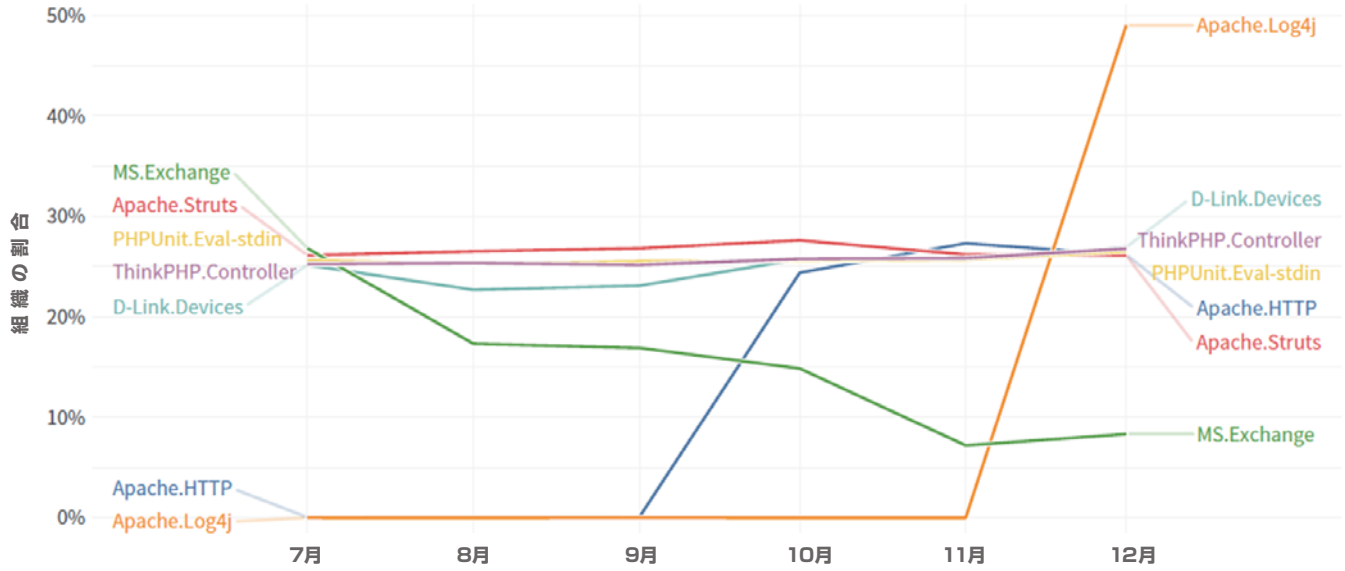


図 1:テクノロジー別、IPS に最も検知された脆弱性（2021 年後期）

一般向けのWebアプリケーションのセキュリティには異なるアプローチが必要です。インターネットへの直接アクセスを安全に遮断できるアプリケーションやサービスとは異なり、Webアプリケーションを効果的に機能させるためには、インターネットアクセスを認めなければなりません。それぞれ数百から、時には数千の要素（URL、パラメータ、cookieなど）から成る複数のアプリケーションとの通信を許可／ブロックするセキュリティポリシーは、どのように定義すればよいでしょうか。要素ごとに異なるポリシーをマニュアルで作成するアプローチは現実的ではなく、Webアプリケーションの数や複雑性が増すにつれて拡張できなくなります。また、Webアプリケーションは頻繁に変更されます。企業は毎月、本番環境のアプリケーション1個あたり平均25件のソフトウェアアップデートを公開しているのです（*Cybersecurity Insider*のアプリケーションセキュリティに関する2021年レポートを参照）[2]。

FortiWeb の Web アプリケーションと API のためのセキュリティ：多層型アプローチ

FortiWebのポジティブセキュリティモデルである多層型アプローチには、1）優れた脅威検知と 2）運用効率の向上という2つの重要なメリットがあります。特定の保護対象アプリケーションに高度な2層式の機械学習を適用して異常な振る舞いを検知するFortiWebの機能によって、先例のない未知のエクスプロイトをブロックすることができます。これは、アプリケーションを狙うゼロデイ攻撃に対する最高の保護です。

FortiWebは、包括的なアプリケーションセキュリティモデルを作成することで、SQLインジェクションやクロスサイトスクリプティングといったアプリケーション層を狙う攻撃を含む、あらゆる既知または未知の脆弱性を防御することができます。運用面では、FortiWebの機械学習によって、誤検知の修正やWAFルールのマニュアル調整など、時間のかかる作業が解消されます。FortiWebはアプリケーションの進化に合わせてモデルを継続的に更新するため、精度がそれほど高くないWAFソリューションに多い、WAFルールの手動チューニングと誤検知対応という時間のかかる作業を行う必要性がなくなり、コードを素早く本番環境に実装することができるのです。

FortiWeb製品ラインは、ポジティブおよびネガティブのセキュリティモデルに基づき、既知の攻撃とゼロデイ攻撃を防御します。FortiGuard Labsの脅威インテリジェンスをベースとするアナリティクスと高度な機械学習機能を融合し、アプリケーションを狙う攻撃からの防御をサポートします。 FortiGuard Labsのアナリティクスは、SQLインジェクションやクロスサイトスクリプティングなど、さまざまな攻撃を防ぐための高度な技法を利用し、FortiWebの機械学習は、アプリケーションの実際の使用状況をモデリングし、悪意のある異常を探します。

FortiWebはアプリケーションの可用性を確保しながら機密データを保護し、極めて多様なセキュリティモジュールとテクノロジーを利用して、OWASP Top 10に対処できる柔軟かつ信頼性の高いセキュリティを実現します。多層型のセキュリティアプローチにより、高度な攻撃をブロックします。双方向のトラフィック解析に基づくポジティブおよびネガティブのセキュリティモジュールと、機械学習による振る舞いベースの埋め込み型異常検知エンジンを統合したFortiWebは、ネットワークの再構築やアプリケーションの変更を要求することなく、幅広い脅威からの保護を提供します。

FortiGuard Labs に支えられるソリューション

FortiWebには、既知のアプリケーション層攻撃やアプリケーションロジック攻撃を防御するための完全なアプリケーションシグネチャディクショナリが搭載されています。高度なエンジンがインバウンドとアウトバウンドの双方向のトラフィックをスキャンし、事前に定義された既知のエクスプロイトと一致する要素を探し出します。また、このソリューションが提供する強化された柔軟なエンジンでは、お客様が正規表現エンジンを使用して独自のシグネチャを記述できるようになっています。つまり、あらゆるアプリケーションや脆弱性に対するシグネチャを新規作成またはカスタマイズすることが可能なのです。

FortiWebのシグネチャディクショナリは、既知および潜在的なセキュリティ脅威に対する保護を研究するフォーティネットのグローバルセキュリティ研究チームの研究結果に基づき動的な保護を提供するセキュリティサブスクリプションサービス「FortiGuard Labs」を介して、定期的かつ自動的に更新されています。

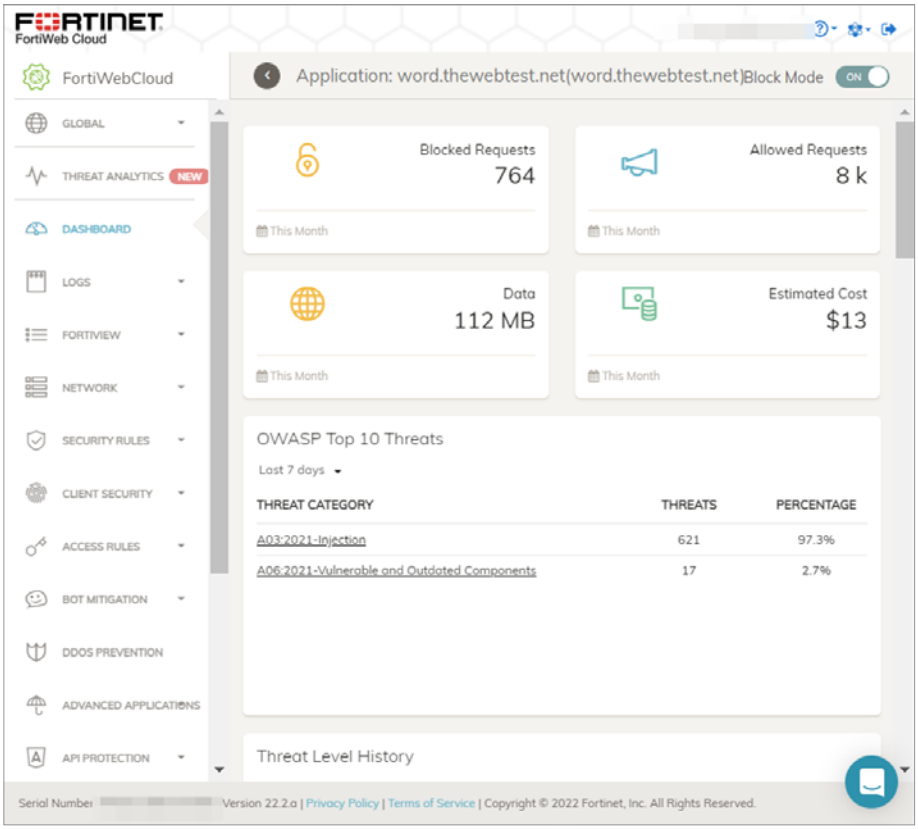


図 2:OWASP Top 10 脅威ダッシュボード要素

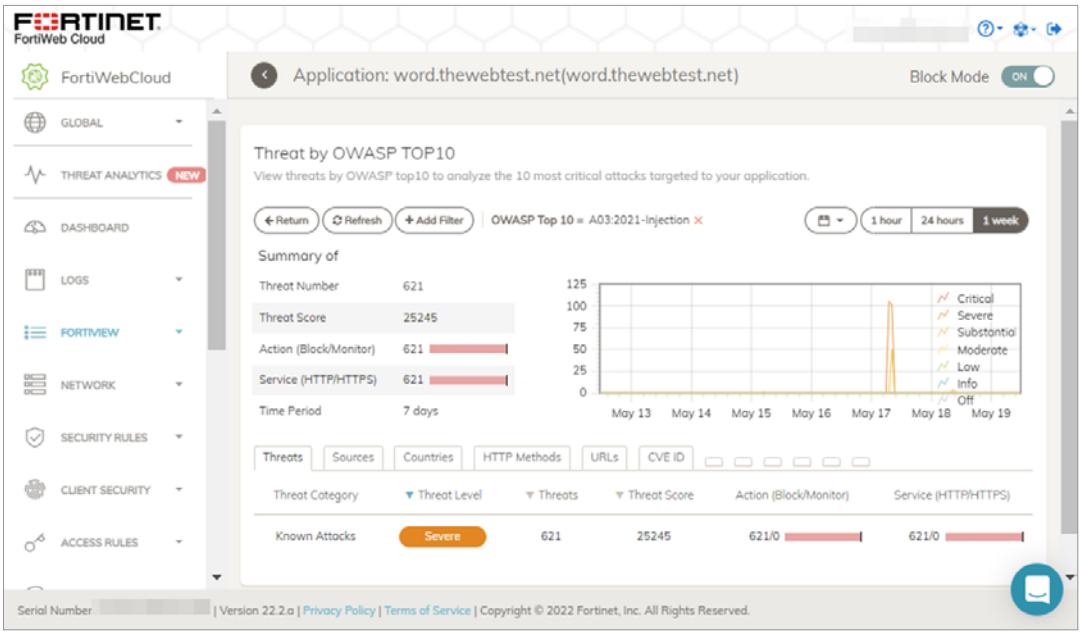


図 3:FortiWeb Cloud における「A03:2021 インジェクション」アラートの例

データ漏洩防止と情報開示

お客様は、機密データのマスキングに関する既定のカスタムポリシーを利用して、FortiWeb に記録された機密データが不正なアクセスから保護されるように確保することができます。機密データのマスキングは、OWASP Top 10に対する重要な軽減策の1つとして非常に重大なタスクです。

システムへのアクセスが許可されている場合でも、データ自体がマスキングされるため、貴重な機密情報を読み取ることはできません。既定のポリシーを利用する以外に、ログ内の他のフィールドも自動的にマスキングされるように、独自のカスタムポリシーを作成することも可能です。

OWASP Top 10 と FortiWeb の軽減策

2021年のOWASP Top 10と、それに対するFortiWebの軽減策を下の表にまとめました。

OWASP Top 10	説明	FortiWeb の軽減策
1. アクセス制御の不備	アクセス制御の不備は、ユーザーが本来意図されていないリソースにアクセスできる状況を意味します。リソースへのアクセス権は、必ず最小権限の原則に基づき付与し、権限のないユーザーによるアクセスは拒否されるべきです。	• FortiWeb の認証を実施するほか、正しいユーザーグループを使用することで、強力なアクセス制御メカニズムを構築します。 • FortiWeb API Gateway を利用して、API キーの検証、ユーザー管理、URL の非表示、API へのアクセス制限を行います。 • FortiWeb 攻撃シグネチャを有効にし、権限昇格を引き起こす可能性のあるディレクトリトラバーサル、強制ブラウジング、機密ファイルへのアクセスを防ぎます。 • FortiGuard Labs のクレデンシャルスタッフィング防御サービスを使用します。
2. 暗号化の失敗	アプリケーションは、機密データ、特にプライバシー規制や金融に関する規制（GDPR や PCI DSS など）の対象となるデータを扱うため、転送中のデータと静止中のデータに適切な保護を提供する必要があります。	• FortiWeb を利用し、HTTP でアクセスできるアプリケーションにも TLS 暗号化通信を強制します。可能であれば、HSTS と Secure 属性を使用します。 • FortiWeb ではより強力な暗号法のみを使用し、クライアントサイド通信とサーバーサイド通信を保護します。 • FortiWeb の攻撃シグネチャを有効にし、etc や passwd などの機密ファイルへの直接アクセスを防止します。 • FortiWeb のシグネチャを利用し、ヘッダーなどからの機密データの漏えいを阻止します。 • cookie の暗号化を有効にします。 • FortiWeb ログ内のすべての機密フィールドをマスキングし、管理者も含め、誰も機密データを読み取れないように確保します。

OWASP Top 10	説明	FortiWeb の軽減策
3. インジェクション	最も古く、現在も広範に蔓延している攻撃の 1 つです。攻撃者は、アプリケーションによって無害化されないことを期待して、リクエストに悪意のあるコードを注入します。コードが無害化されなければ、ユーザーが所有していないデータを取得するなどの不正な行動を行います。 インジェクション攻撃で非常に一般的な形式は SQL インジェクションですが、LDAP、OS コマンド、メールヘッダーのインジェクションなど、他にも多数のインジェクション攻撃があります。 OWASP Top 10 2021 年版からインジェクションのカテゴリに追加されたクロスサイトスクリプティングは、非常に危険ながら一般的な攻撃です。	• FortiWeb の攻撃シグネチャを有効にし、インジェクション攻撃とクロスサイトスクリプティング攻撃を防ぎます。 • 機械学習ベースの異常検知を有効にし、ゼロデイインジェクション攻撃を防ぎます。インジェクション攻撃は、アプリケーションのロジックに含まれる脆弱性の悪用を試みる攻撃であり、必ずしもコード自体の脆弱性（入力の検証や無害化を行わないなど）ではないため、この攻撃に関しては異常検知による保護が重要になります。 • API 保護のための機械学習を有効にし、API をゼロデイ攻撃から自動的に保護します。別の方法として、アップロードされたスキーマに基づき、XML や JSON スキーマの検証を実施します。
4. 安全が確認されない不安な設計	2021 年版の OWASP Top 10 から加わったこの新カテゴリは、設計やアーキテクチャ上の欠陥に関わるリスクに焦点を当てたものです。主に SDLC に関わる欠陥であり、実装面から修正できるものではありません。 定義上、特定の攻撃の防御を目的として必要なセキュリティ制御が構築されたことはないため、安全でない設計を完璧な実装によって修正することは不可能です。	FortiWeb ソリューションの対応範囲外：安全でない設計を防ぐためには、プログラミングに関するベストプラクティスに従い、安全なソフトウェア開発ライフサイクル（SSDLC）を確立してください。
5. セキュリティの設定ミス	セキュリティの設定ミスとは、アプリケーションに必要なセキュリティ制御がすべて実装されていない状態を意味します。例えば、導入時にデフォルトのユーザーアカウントやパスワードが無効にされていない、不要なソフトウェアコンポーネントが有効になっている、クラウドアクセス権が正しく設定されていないなどの欠陥が、セキュリティ設定のミスに分類されます。 OWASP Top 10 2021 年版では、以前は別のカテゴリに分類されていた XML 外部実体参照（XXE）もセキュリティの設定ミスに含められました。XML XXE 攻撃では、XML パーサーが正しく設定されていない場合に、外部エンティティの参照を含む XML 入力が利用・悪用されます。	• FortiWeb の攻撃シグネチャを有効にし、機密情報を読み取ろうとする試みを検知するほか、既知のデフォルトのシステム URL へのアクセスをブロックします。 • External Entity、Entity Expansion、XInclude など、禁止される XML エンティティに対する FortiWeb の保護を有効にし、XML XXE 攻撃を防ぎます。 • FortiWeb の認証層を追加し、すべてのユーザーに認証を強制します。 • ファイルセキュリティを強制し、特定のファイルタイプへのアクセスをブロックします。
6. 脆弱で古くなったコンポーネント	脆弱で古くなったコンポーネントとは、コンポーネント、モジュール、ライブラリ、ソフトウェアパッケージに含まれる既知の脆弱性（別称 CVE）を意味します。 その多くは、サードパーティーまたはオープンソースのパッケージに含まれるものであり、利用者側が管理できるものではありませんが、標準的なソフトウェア機能を実現するために、大多数のアプリケーションに広く展開および統合されています。OpenSSL がその一例です。 これらのコンポーネントに含まれる脆弱性は、他の脆弱性と同様に、アプリケーションにとっての潜在的な脅威であり、標準的なインジェクション攻撃、XSS、バッファオーバーフローなどのエクスプロイトを利用して悪用される可能性があります。Log4J 脆弱性は、このカテゴリの良い例です。	• FortiWeb の攻撃シグネチャを有効にし、既知の CVE を悪用しようとする試みを検知します。 • 標準的な脆弱性評価ツールを使って定期的にアプリケーションをスキャンし、既知の脆弱性を探します。FortiWeb にこのツールを統合し、仮想パッチを自動的に適用する機能を実現します。
7. 識別と認証の失敗	識別と認証の失敗とは、認証関連の攻撃を防ぐために極めて重要な、ユーザーの本人確認、認証、セッション管理に関係している欠陥です。このカテゴリは 2021 年のリストで 2 位から 7 位に降格しました。 クレデンシャルスタッフィング攻撃、ブルートフォース攻撃、セッションハイジャック、セッションの固定化などのエクスプロイトが、このカテゴリに該当します。	• クライアント管理を有効にし、FortiWeb がすべてのユーザーセッションを追跡できるようにします。 • クレデンシャルスタッフィングからの保護を有効にし、漏洩が確認されたことのある認証情報がユーザーログインに使われていないことを確認します。 • セッションの固定化に対する保護を有効にし、セッションタイムアウトを強制します。 • cookie を “signed” または “encrypted” に設定し、セッションハイジャックを防ぎます。 • FortiWeb の攻撃シグネチャを有効にします。

OWASP Top 10	説明	FortiWeb の軽減策
8. ソフトウェアとデータの不整合の不具合	ソフトウェアとデータの不整合の不具合とは、整合性違反に脆弱なコードやインフラを意味します。例えば、信頼できないソースやリポジトリから提供されるプラグイン、ライブラリ、モジュールを利用しているアプリケーションは正しく検証されておらず、改ざんや破損の可能性があるため、このカテゴリに該当します。この不具合が原因で悪意のあるコードがインストールされた場合、攻撃者にアプリケーションを悪用される可能性があります。2020 年に発生し、世界で数千の組織に影響を与えた SolarWinds サプライチェーン攻撃の主な原因は、この不具合です。 ソフトウェアとデータの不整合の不具合は、ソフトウェアの整合性そのものに関わる問題であるため、それ自体を WAF で防ぐことはできません。しかし、WAF によって、この不具合に起因する脆弱性の悪用を防ぐことができます。	• アプリケーション固有の管理インターフェイスやその他の機密性の高い URL に FortiWeb の認証を適用します。 • FortiWeb の攻撃シグネチャを有効にし、バッファオーバーフローやコマンドインジェクションなどの攻撃タイプを防御します。
9. セキュリティログとモニタリングの失敗	セキュリティログとモニタリングの失敗は、以前は「不十分なロギングとモニタリング」と呼ばれていました。この欠陥は、アプリケーションによるセキュリティリスクの検知と対応能力の弱さに関係しています。 不審なアクティビティのロギングは、あらゆるセキュリティシステムに不可欠な機能です。ロギングとモニタリングなしに、侵害を検知することはできません。	• FortiWeb ソリューションには、イベントを迅速に理解し、時間の経過とともに発生する様々な攻撃の相関関係を分析し、管理者が最も深刻な脅威に即座に集中できるようにサポートする、高度なモニタリングおよびロギング機能が搭載されています。 • 攻撃ログでは、違反がハイライトされ、一貫性のある読みやすい形式で説明されています。 • 管理者は、FortiView の機能を利用し、ソース IP、ジオ IP、ヘッダー、URL をはじめとする様々な基準に従ってログを細かく分類することができます。 • 脅威アナリティクスを使用します。脅威の検知と対応を簡素化し、WAF アラートのセキュリティ調査を高速化します。機械学習を利用して、すべての Web アプリケーションにおける攻撃を分析し、共通の特徴やパターンを特定のうえ、意味のあるセキュリティインシデントに分類します。 • トラフィックログをリモートサーバーに転送し、安全な保管と将来的なセキュリティ調査をサポートします。
10. サーバーサイドリクエストフォージェリ	2021 年に新たに加わったサーバーサイドリクエストフォージェリ（SSRF）とは、Web アプリケーションがユーザー指定の URL に基づき、その URL を検証することなく、リモートリソースからデータを取得することに関わる脆弱性です。攻撃者は、アプリケーションに意図されていないリソースにアクセスするリクエストを強制的に送ることができ、多くのケースにおいてセキュリティ制御を逃れています。 SSRF 攻撃に成功された場合、データの流出、機密データの漏洩、データの盗難につながる可能性があります。	• 攻撃シグネチャを有効にし、既知のアプリケーションにおける SSRF 攻撃を防ぎます。 • 機械学習ベースの異常検知を有効にし、ゼロデイ SSRF 攻撃を防ぎます。

まとめ

OWASP Top 10 は、組織が現在のアプリケーションセキュリティ体制を評価し、リスク軽減の優先順位を判断する際の出発点となるものです。セキュリティの基本指標として、多くの標準化団体に幅広く採用されており、アプリケーションセキュリティのための取り組みをサポートしてくれます。

FortiWebは、APIの発見と保護、ボット対策、高度な脅威検知とともに、OWASP Top 10の軽減に必要なセキュリティを提供します。

[1] 2021年版DBIRからの所見, Verizon.
[2] アプリケーションセキュリティレポート, Cybersecurity Insiders, 2021.

フォーティネットジャパン合同会社
〒106-0032
東京都港区六本木7-7-7 Tri-Seven Roppongi 9階
www.fortinet.com/jp/contact

お問い合わせ

Copyright© 2022 Fortinet, Inc. All rights reserved. この文書のいかなる部分も、いかなる方法によっても複製、または電子媒体に複写することを禁じます。この文書に記載されている仕様は、予告なしに変更されることがあります。この文書に含まれている情報の正確性および信頼性には万全を期しておりますが、Fortinet, Inc.は、いかなる利用についても一切の責任を負わないものとします。Fortinet®、FortiGate®、FortiCare®、およびFortiGuard® はFortinet, Inc. の登録商標です。その他記載されているフォーティネット製品はフォーティネットの商標です。その他の製品または社名は各社の商標です。

WP-ky-OWASP-Top-10-202208-R1