OWASP Top 10（2021年版）への対応策

OWASP Top10（2021年版）のリスクに対する弊社の対応策　　対象サービス：イーベ！　記入：株式会社フラッグシステム

No	名前	弊社の対応策
A01:2021	アクセス制御の不備	ユーザー、フォーム提出者、一般の閲覧者、開発者、カスタマーサポートなどの各役割に応じて適切なアクセス制御策を採用しております。不正な操作によるアクセス制御の回避に対する防衛策も講じています。
A02:2021	暗号化の失敗	安全な通信とデータの保存には、適切な暗号化技術を採用しています。ネットワーク間の通信には適切なSSL/TLSを使用し、ファイルストレージやデータベースも適切な暗号化領域に保存しています。
A03:2021	インジェクション	クライアントからの入力に対しパラメータ化、適切な検証、エスケープ等の手段を用いて、インジェクション攻撃を予防しています。
A04:2021	安全が確認されない不安な設計	設計フローには、初期段階からセキュリティを考慮したアプローチが取られています。セキュリティリスクアセスメントの実施を通じて、設計が安全であることを確認します。
A05:2021	セキュリティの設定ミス	外部によるセキュリティアセスメントを実施し、脆弱性のある設定を回避します。設定の変更管理とセキュリティ視点でのレビュープロセスを行っています。また、常に最新のセキュリティパッチとアップデートを適用し、最新のセキュリティ設定を維持します。
A06:2021	脆弱で古くなったコンポーネント	必要最小限のコンポーネントのみを使用し、不要なものは除外します。定期的なコンポーネントのアップデートにより、古く脆弱性のあるコンポーネントが使用されていないことを確認します。
A07:2021	識別と認証の失敗	防御策として、多要素認証、パスワードポリシー、自動化攻撃からの保護などを採用しています。また、セッションのなりすましを防ぐための適切な管理を行っています。
A08:2021	ソフトウェアとデータの整合性の不具合	信頼できるリポジトリを使用してライブラリや依存関係を管理します。また、CI/CDパイプラインに自動化されたテストや検証ツールを組み込み、整合性を確保します。
A09:2021	セキュリティログとモニタリングの失敗	全てのシステムとアプリケーションに適切なログ記録とモニタリングを設定し、異常な行動やセキュリティインシデントを早期に発見できるよう取り組んでいます。
A10:2021	サーバーサイドリクエストフォージェリ(SSRF)	クライアントからの入力に対して、パラメータ化、適切な検証、エスケープなどの手法を用いてインジェクション攻撃を防止しています。さらに、ネットワークのインプットは必要最低限のソース、ポート、宛先に制限します。ログを記録し、不正なネットワークフローを監視します。

記入日　2023/07/07