外部共有版　技術詳細版　診断時点 2026年10月

Webシステム
セキュリティ診断報告書

改修前のWebアプリケーションを対象に、認証・認可、データ処理、ファイル管理、実行環境を診断した。優先度は、機密性・完全性・可用性への想定影響と、コード上で確認した到達性を基に設定した。

診断範囲と手法

手法	確認内容と範囲
ソースコードレビュー	対象コードを棚卸しし、主要経路を抽出した。要求入力から認証・認可判定、データベース参照、更新、応答出力までのデータフローを追跡した。
ローカル隔離検証	業務データベースを代替した環境で実装の一部を実行し、架空データによる出力、検索条件の組立て、認証・再設定処理などの挙動を観察した。
運用環境の確認範囲	公開環境の到達性、Webサーバーの実効設定、全画面の動的試験、過去のアクセスログの調査は追加確認の対象。実際の侵入や情報流出の有無は未判定。

最優先の指摘

ID・分類	深刻度	証拠の範囲
S01 公開データ取得の認可不備	重大	コード確認・隔離観察
S02 オブジェクト単位の認可不備	高	コード確認・一部の隔離観察
S03 管理機能の認可不備	高	コード確認。公開経路は要確認。
S04 SQLインジェクションリスク	重大	コード確認・SQL組立ての隔離観察

重大・高・中は診断時の相対評価。CWEは弱点の種類を示す参考分類であり、CVSSの数値は付与していない。

最優先指摘の技術詳細

認可の強制箇所とSQLの組立てを重点確認した。確認根拠は、診断時に実際に観察した範囲を示す。

S01　公開データ取得の認可不備

重大 CWE-862 コード確認・隔離観察

原因・根拠　汎用データ取得処理で、参照対象・返却項目を公開用に限定するサーバー側の認可が不足。隔離環境では、未認証状態で機密属性に相当する架空値が応答に含まれた。

想定影響　公開経路から処理に到達できる場合、利用者情報や認証関連情報の機密性が損なわれる。

対策・判定　公開対象と返却項目を用途ごとの許可リストで固定。公開データの取得は成功し、許可外の項目は応答に含まれないことを確認する。

S02　オブジェクト単位の認可不備（IDOR）

高 CWE-639 コード確認・一部の隔離観察

原因・根拠　一部の取得・更新処理で、要求されたレコードと利用者の所属・当事者関係を照合していない。隔離検証では、利用者の条件を伴わない参照処理を観察した。

想定影響　権限外のメッセージや添付の取得、削除・状態変更につながるおそれがある。

対策・判定　各操作にレコード単位の認可を強制し、更新条件にも適用する。当事者の操作が成功し、別利用者による取得・更新が拒否されることを確認する。

S03　管理機能の認可不備

高 CWE-862 コード確認・公開経路は要確認

原因・根拠　一部の管理機能で、データ参照・出力・取込の実行前に管理者ロールを必須とする判定がないことをコードで確認した。

想定影響　公開設定と利用者の権限次第で、管理データの取得や業務データの改変が可能になる。

対策・判定　処理の入口でサーバー側の役割確認を行う。未認証・一般利用者の要求で、応答へのデータ混入やデータベースの更新が起きないことを確認する。

S04　SQLインジェクションリスク

重大 CWE-89 コード確認・SQL組立ての隔離観察

原因・根拠　検索条件をSQL文の組立てに直接使用しており、文とデータが分離されていない。隔離検証では、通常の検索文字列がバインドなしでSQL文に含まれることを確認した。

想定影響　検索条件の改変や権限外の参照が想定される。更新などの影響範囲はDB権限と実行方式に依存する。

対策・判定　値をパラメーターとしてバインドし、並び順・列は許可リスト、件数は型と上限で制御する。通常入力で検索が成功し、入力がSQL文の構造を変えないことを確認する。

認証とセッションの指摘

資格情報の保存、復旧手続き、認証後の権限が切り替わる箇所を確認した。

S07　計算コストの低いパスワードハッシュ

高 CWE-916 コード確認・文字数制約の隔離観察

原因・影響　ソルトなしの高速ハッシュを保存に使用し、文字数の上限も短い。保存値が漏えいした場合、オフラインでのパスワード推測に弱い。

対策・判定　パスワード用ハッシュ関数を採用し、登録・変更・取込・再設定で共通化する。旧形式の利用者がログインでき、成功後に新形式へ移行することを確認する。

S08　本人確認前のパスワード更新

高 コード確認

原因・影響　一部の再設定で、メールによる本人確認の前に資格情報が更新される。第三者からの申請やメール配送失敗で、正規利用者がログインできなくなるおそれがある。

対策・判定　申請と変更確定を分離し、有効なトークン確認後に更新する。申請・配送失敗時に既存パスワードが維持されることを確認する。

S09　再設定トークンと権限の分離不足

高 コード確認・一部の隔離観察

原因・影響　再設定リンクの秘密管理が他の資格情報に依存し、使用済み状態の管理と再設定専用の権限分離が不足していた。資格情報の漏えい時に影響が波及し得る。

対策・判定　独立した乱数トークンのハッシュを用途・対象・期限とともに保存し、消費を原子的に確定する。期限切れ・再利用を拒否し、通常の認証状態を付与しないことを確認する。

S10　セッション管理の不統一

高 コード確認・Cookieの実効設定は要確認

原因・影響　認証経路によってセッションIDの再生成や資格情報変更時の失効処理が異なる。一部の経路では認証前のIDや変更前の認証状態が残るおそれがある。

対策・判定　ログイン・追加認証の完了時にIDを再生成し、資格情報変更時に旧セッションを失効させる。実応答でCookieの保護属性を確認する。

S11　認証・再設定の試行回数制限の不足

高 CWE-307はログイン試行に対応 周辺防御は要確認

原因・影響　ログイン失敗や再設定要求をアプリ側で制限する処理が不足し、連続したパスワード推測や再設定メールの連続要求が可能になるおそれがある。

対策・判定　アカウントと接続元を考慮した一時制限を設ける。上限に達した連続・並行要求の拒否と、所定条件での制限解除を確認する。

入力・ファイル・公開設定の指摘

コード上の指摘と、公開サーバーの設定や稼働構成で確認すべき項目を示す。

ID・深刻度	技術的な指摘と根拠	対策方針
S05 高 **XSS**	要求値・保存値の一部で、HTML出力先に応じたエンコードが不足。コードで確認。CWE-79。	HTML本文、属性、URLなど、出力先の文脈ごとにエンコードと検証を適用する。
S06 高 **CSRF**	一部の状態変更で要求の正当性の確認が不足。コードと一部の隔離観察で確認。CWE-352。	状態変更に適切なHTTPメソッドとセッションに紐づくCSRFトークンを必須化する。
S12 高 **アップロードと一時ファイル**	保存先、ファイル形式、所有者の検証に課題。公開環境の配信制限は要確認。	非公開保管と認可付き配信を採用し、一時ファイルを利用者に紐づくサーバー側IDで管理する。
S13 高 **診断用ファイルの公開範囲**	機密情報を扱う診断用ファイルの配置をコード側で確認。本番での公開状況を優先確認。	配布対象を棚卸しし、秘密情報・ログ・診断用ファイルを公開範囲から除外する。
S14 中 **エラー出力とHTTP応答**	詳細エラーが画面に表示される構成を確認。保護ヘッダーの実効値は要確認。	利用者向け応答を一般化し、詳細を内部ログに記録する。配信時の保護ヘッダーを点検する。
S15 高 **実行環境の保守**	引継ぎ資料に保守期限を過ぎた実行環境の記録がある。本番の稼働版とパッチ適用状況は要確認。	実行環境の版と適用済み修正を台帳化し、保守対象の構成への移行を計画する。
S16 中 **依存ライブラリ**	旧版のJavaScriptライブラリを確認。ページごとの利用箇所と影響範囲は要確認。	実際に読み込まれる依存を棚卸しし、更新と画面の回帰試験を行う。
S17 中 **CSVの数式解釈**	利用者入力が表計算ソフトで数式として解釈され得る。コードで確認。	対象ソフトで文字列として扱われるよう出力を制御し、通常データへの影響も確認する。

S13の公開状況は優先して確認する。OS・実行環境の保守は、アプリケーション改修と並行して計画する。

改修後の再診断計画

診断時点で設定した合格条件。実際の適用範囲と本番反映後の検証結果は、別紙のセキュリティ対策実施報告書を参照する。

対応する指摘	合格条件
S01-S03 アクセス制御	未認証・別利用者・異なる所属・権限不足の要求を拒否し、応答とデータベースに副作用がない。権限のある利用者の参照・更新・出力は成功する。
S04-S06 入力と更新	正当な検索入力が利用でき、SQL文の構造が入力で変化しない。画面出力はブラウザーでデータとして扱われ、不正なトークンでの更新は拒否される。
S07-S11 認証と復旧	旧パスワードからの移行、失効済みリンクの拒否、セッションの再生成・失効、一時制限と復帰を確認する。追加認証の完了前は管理権限を付与しない。
S12-S14 ファイルと配信	権限外の添付取得、保存先外への操作、公開経路からの診断ファイル取得を拒否する。エラー応答に接続情報や内部パスが含まれない。
S15-S17 保守と出力	本番の実行環境と依存の版・更新状況を照合する。主要画面と出力の回帰、CSVの文字列扱い、バックアップからの復元を確認する。

公開環境で追加確認する項目

公開ルートと別経路からの到達性、実効のCookie・TLS・HTTPヘッダー、アプリのDB権限、公開フォームの設定、アクセスログの保存範囲を確認する。ログ確認と診断結果は、実際の被害の有無を判断する際の別個の証拠として扱う。

診断資料と分類の参照先

対象固有の評価は、改修前の内部診断記録と隔離検証結果に基づく。以下のMITRE CWEは一般的な弱点分類の参照先。

CWE-862 **CWE-639** **CWE-89** **CWE-79** **CWE-352** **CWE-916** **CWE-307**