社外秘 / CONFIDENTIAL

SECURITY ASSESSMENT REPORT

Webアプリケーション
脆弱性診断 報告書

対象システム：会員向けポータルサイト（本番環境）

文書番号	ITS-VA-2026-041	版数	第 1.0 版
発行日	2026年9月12日	診断種別	手動診断＋ツール診断（グレーボックス）
お客様	株式会社サンプル 御中	機密区分	社外秘（取扱注意）
発行元	IT.Skill／岐阜県大垣市　https://it-skill.jp		

本報告書はサンプルです。記載の診断結果・URL・企業名はすべて架空であり、実在の組織・システムとは関係ありません。

改訂履歴

版数	発行日	改訂内容	作成／承認
1.0	2026-09-12	初版発行	IT.Skill

目次

1. 診断概要 P.2
2. 実施方針と準拠基準 P.2
3. 診断結果サマリ P.3
4. 総合所見 P.3
5. 指摘事項の一覧 P.4
6. 指摘事項の詳細 P.4
7. 是正計画と再診断 P.6
付録A. 診断範囲・免責事項・用語 P.6

1. 診断概要

診断の目的	本番リリース済みの会員ポータルについて、外部・認証済みの両面から実装上の脆弱性を洗い出し、リスクの大きい順に是正方針を提示する。
診断対象	https://portal.example.co.jp/（会員ログイン／マイページ／問い合わせ／管理画面）　※ステージング環境で実施
診断範囲	Webアプリケーション層（画面遷移・API・認証認可・入力処理）。ネットワーク／物理／ソーシャルは範囲外。
診断期間	2026年9月8日 ～ 2026年9月11日（実働3人日）
診断手法	グレーボックス（一般ユーザー権限のアカウント貸与）。手動診断を主とし、OWASP ZAP による自動スキャンを補助的に併用。
実施者	IT.Skill

2. 実施方針と準拠基準

本診断は、以下の公開された基準・ガイドラインに沿って項目を設計し、検出事象の深刻度は CVSS v3.1 の基本評価基準（Base Score）に基づいて算定した。

基準・ガイドライン	本診断での用途

OWASP Top 10（2021）	診断観点の網羅性の確認（A01〜A10 に対応付け）
OWASP ASVS 4.0	認証・セッション・アクセス制御・入力検証の検証項目
CVSS v3.1	各指摘の深刻度スコア／深刻度レーティングの算定
ISO/IEC 27001:2022 附属書A（A.8.8 技術的脆弱性の管理 ／ A.8.25 セキュア開発 ／ A.8.28 セキュアコーディング）	是正・記録・再発防止の位置づけ（ISMS運用への接続）

深刻度は次の基準で色分けする。緊急 CVSS 9.0-10.0 ／ 高 7.0-8.9 ／ 中 4.0-6.9 ／ 低 0.1-3.9 ／ 情報 参考情報。

3. 診断結果サマリ

0	1	2	2	5
緊急 Critical	高 High	中 Medium	低 Low	指摘 合計

認証境界の内側で情報が漏れうる指摘（SQLインジェクション／アクセス制御不備）が確認された。緊急に該当する事象は無いが、High 1件は個人情報の一括漏えいに直結しうるため、最優先での是正を推奨する。

4. 総合所見

本システムは、通信の暗号化（TLS1.2以上）やパスワードのハッシュ保存など、基本的な防御は実装されている。一方で、**入力値をSQL文へ組み立てる箇所**と**他人のIDを指定した際の権限チェック**に不備が残っており、いずれも「認証は通っているが、本来見えてはならないデータが見える」種類のリスクである。これらは機能追加の過程で個別に実装された画面に集中しており、共通の入力処理・認可処理を経由していないことが根本原因と考えられる。恒久対策として、クエリの組み立てをORM／プレースホルダに一本化し、認可判定を共通ミドルウェアへ集約することを併せて提言する。

5. 指摘事項の一覧

ID	指摘事項	深刻度	CVSS	是正状況
VA-01	SQLインジェクション（検索パラメータ）	高	8.6	未対応
VA-02	アクセス制御不備（IDOR／他会員の明細参照）	中	6.5	未対応
VA-03	ログイン試行回数の制限なし（ブルートフォース）	中	5.3	未対応
VA-04	セキュリティヘッダーの不足（HSTS／CSP等）	低	3.1	未対応
VA-05	詳細なエラー情報の露出（スタックトレース）	低	2.6	未対応

6. 指摘事項の詳細

VA-01　SQLインジェクション

高　CVSS 8.6

会員検索の `keyword` パラメータに、SQL文の一部として解釈される入力が可能

対象	`GET /members/search?keyword=`
OWASP / 分類	A03:2021 – Injection
CVSS v3.1	8.6　`AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:N`

概要・影響

検索キーワードがエスケープ処理されずSQL文へ連結されているため、任意の条件式を注入できる。会員テーブル全件（氏名・メール・電話番号）の抽出、および他テーブルへの横断参照が可能で、**個人情報の一括漏えいに直結する。**

再現手順（証跡）

```
① 一般会員でログインし、会員検索画面を開く
② keyword に次を入力して送信：
   ' OR '1'='1' --
③ 本来1件も一致しないはずが、全会員 1,284 件が表示される
④ UNION 句により users テーブルのメール列が取得可能なことを確認
   （PoC は影響を最小化するため件数取得のみに留め、データは保全しない）
```

推奨対策

- 文字列連結によるクエリ生成を廃止し、**プレースホルダ（バインド機構）またはORM**に統一する。
- 入力値は「検索語」として扱い、SQLの構文要素として解釈させない。
- DB接続アカウントの権限を当該機能に必要な範囲へ最小化する（多層防御）。

参照

OWASP Cheat Sheet: SQL Injection Prevention ／ CWE-89

VA-02　アクセス制御不備（IDOR）

中　CVSS 6.5

URLの注文IDを差し替えると、他会員の購入明細が閲覧できる

対象	`GET /mypage/orders/{order_id}`
OWASP / 分類	A01:2021 – Broken Access Control（CWE-639）
CVSS v3.1	6.5　`AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N`

概要・影響

注文明細の表示時に「そのログインユーザーの注文かどうか」の所有者チェックが行われていない。連番のIDを変更するだけで、他会員の氏名・配送先住所・購入内容が閲覧できる。

再現手順（証跡）

```
① 自アカウントの注文 /mypage/orders/10432 を開く
② order_id を 10431 → 10420 と変更
③ いずれも別会員の明細（宛名・住所・金額）が表示される
```

推奨対策

- 明細取得時に `WHERE order_id=? AND user_id=<ログインユーザー>` の条件で所有者を必ず検証する。
- 認可判定を各画面に散在させず、共通ミドルウェア／デコレータへ集約する。

VA-03　ログイン試行回数の制限なし

中　CVSS 5.3

ログインAPIに回数制限・ロックアウトが無く、総当たり攻撃が可能

対象	`POST /login`
OWASP / 分類	A07:2021 – Identification and Authentication Failures
CVSS v3.1	5.3　`AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N`

概要・影響

同一アカウントへ短時間に数百回のログイン試行を行ってもロックや遅延が発生しない。弱いパスワードの会員が乗っ取られるおそれがある。

推奨対策

- 連続失敗に対するアカウントロック／指数バックオフ、IP単位のレート制限を導入する。
- 重要操作には多要素認証（MFA）を検討する。

VA-04 / VA-05　低リスク（まとめ）

低

VA-04 セキュリティヘッダー不足（CVSS 3.1）： `Strict-Transport-Security` / `Content-Security-Policy` / `X-Content-Type-Options` が未設定。中間者攻撃やクリックジャッキングの耐性が下がる。→ リバースプロキシまたはアプリ側で付与。

VA-05 エラー情報の露出（CVSS 2.6）： 例外発生時にスタックトレースとフレームワークのバージョンが画面に表示される。→ 本番は共通エラーページへ集約し、詳細はサーバーログにのみ出力する。

7. 是正計画と再診断

下表の優先度・期限は推奨案である。是正完了後、対象箇所に限定した再診断（無償・1回）を実施し、本報告書に「是正状況」列と再診断結果を追記して確定版とする（ISO/IEC 27001 A.8.8 に基づく脆弱性管理記録として保管可能）。

ID	深刻度	推奨期限	是正の要点
VA-01	高	7日以内	プレースホルダ／ORMへ統一
VA-02	中	14日以内	所有者チェックの共通化
VA-03	中	30日以内	レート制限・ロックアウト
VA-04/05	低	次回リリース	ヘッダー付与・エラー集約

付録A. 診断範囲・免責事項・用語

範囲外の事項

ネットワーク機器・OS・ミドルウェアのパッチ適用状況、DoS/DDoS耐性、物理セキュリティ、フィッシング等のソーシャルエンジニアリングは本診断の対象外である。

免責事項

本診断は合意した範囲・期間における非破壊的な手法で実施したものであり、対象システムに存在する全ての脆弱性を検出することを保証するものではない。本報告書に基づく是正・運用の最終判断はお客様の責任において行われるものとする。本報告書は取扱注意（社外秘）とし、第三者への開示にはIT.Skillの同意を要する。

主な用語

用語	説明
CVSS	Common Vulnerability Scoring System。脆弱性の深刻度を0.0〜10.0で表す共通指標。
IDOR	Insecure Direct Object Reference。ID等を差し替えて他人の資源を参照できる不備。
グレーボックス	一般利用者相当の権限・情報を与えた状態で行う診断方式。

診断実施者：IT.Skill
発行日：2026年9月12日
連絡先：https://it-skill.jp／お問い合わせフォーム