Terashia ｜ Webアプリ脆弱性診断

【サンプル】経営者向けレポート

これは説明用のサンプルです。対象・会社名・検出内容はすべて架空で、実在の企業や診断実績とは関係ありません。

お客様	架空の顧客 A 社（サンプル）	**報告日**	2026-11-20
診断対象	架空のオンライン予約システム（サンプル）	**診断期間**	2026-11-16 〜 2026-11-18
プラン	スタンダード診断（サンプル）	**レポート番号**	SAMPLE-2026-001

総合評価

早急な対応が必要です

重大度「高」以上の問題を確認しました。外部から悪用されるおそれがあるため、優先して修正してください。

0	1	2	3	1
緊急	高	中	低	情報

技術者が確認した件数（確認済みの事実）。このほか、追加検証が必要な事項 1 件、誤検知として除外した検出 1 件があります。

優先して対応すべきこと

1. **SQL インジェクション** 高（目安: 2 週間以内）
   入力欄に細工した文字列を送ると、データベースへの命令を書き換えられるおそれがあります。
2. **Content-Security-Policy（CSP）が未設定** 中（目安: 1 か月以内）
   画面に読み込むスクリプトの出どころを制限する設定がありません。
3. **公開不要な管理・監視用の画面や情報の露出** 中（目安: 1 か月以内）
   本来は社内向けの監視情報や設定情報が、インターネットから見える状態です。

本レポートは、合意した範囲・期間・方法で行った診断の結果です。**脆弱性がゼロであることを保証するものではありません。** 診断していない機能・期間外の変更・未知の攻撃手法によるリスクは残ります。詳しくは「未検査項目と残存リスク」をご覧ください。

SAMPLE

1. 診断概要

お客様から許可をいただいた範囲で、外部から Web アプリケーションへアクセスし、一般的な攻撃手法で悪用されうる弱点（脆弱性）がないかを、複数の自動診断ツールと技術者の確認で調べました。

自動診断ツールの検出は、技術者が 1 件ずつ確認しています。本レポートには、技術者が確認した事項（**確認済み**）と、追加の検証が必要な事項（**未確定**）を分けて記載しています。

2. 診断対象・実施日

診断対象	架空のオンライン予約システム（サンプル）
対象範囲	・https://app.example.com/ 配下の公開画面と予約 API（ログイン前の機能） ・会員ログイン後の予約・マイページ機能（テスト用アカウント 1 件）
実施期間	2026-11-16 〜 2026-11-18
確認担当	Terashia 技術担当
使用ツール	zap baseline、nuclei default、zap api

3. 検査範囲と制限

・お客様が用意した検証環境（本番と同じ版）を対象にし、本番環境には診断を行っていません
・サービス停止・データ破壊・大量のリクエストにつながる検査は行っていません
・管理者用の画面・権限は今回の範囲外です
・ソースコード・サーバー設定の確認（ホワイトボックス診断）は含みません

4. 発見事項のサマリー

No.	発見事項	重大度	箇所数	対応の目安
1	SQL インジェクション	高	1	2 週間以内
2	Content-Security-Policy（CSP）が未設定	中	3	1 か月以内
3	公開不要な管理・監視用の画面や情報の露出	中	1	1 か月以内
4	セキュリティ関連ヘッダーの不足	低	2	次回の改修時
5	Cookie の安全属性の不足	低	1	次回の改修時
6	エラー情報の露出	低	1	次回の改修時

このほか、対応不要の参考情報が 1 件あります（開発者向け修正依頼書に記載）。

5. リスクの説明と事業への影響

「事業への影響」は、この種類の問題で一般的に想定される影響です。実際の被害の有無を確認したものではありません。

SAMPLE

1. SQL インジェクション 高

どういう問題か: 入力欄に細工した文字列を送ると、データベースへの命令を書き換えられるおそれがあります。

事業への影響: 顧客情報や注文データの漏えい・改ざん、ログインの迂回につながる可能性があり、個人情報保護法上の報告義務や信用低下に直結します。

確認済み 検索キーワードに引用符を含めると SQL エラーが返り、論理式を含めると全件が返ることを検証環境で再現しました。（確認: Terashia 技術担当）

2. Content-Security-Policy（CSP）が未設定 中

どういう問題か: 画面に読み込むスクリプトの出どころを制限する設定がありません。

事業への影響: 単独で被害が出るものではありませんが、XSS などが見つかったときの被害を抑える防御が無い状態です。

確認済み 主要な画面の応答に Content-Security-Policy ヘッダーが無いことを確認しました。（確認: Terashia 技術担当）

3. 公開不要な管理・監視用の画面や情報の露出 中

どういう問題か: 本来は社内向けの監視情報や設定情報が、インターネットから見える状態です。

事業への影響: 内部構成や利用状況、場合によっては秘密情報が漏れ、攻撃の手がかりや直接の被害につながる可能性があります。

確認済み /actuator/env が認証なしで応答し、環境変数名とフレームワークの設定値が表示されることを確認しました（秘密の値は伏せ字でした）。（確認: Terashia 技術担当）

4. セキュリティ関連ヘッダーの不足 低

どういう問題か: ブラウザ側の防御を有効にする設定（応答ヘッダー）の一部がありません。

事業への影響: 単独で被害が出るものではありませんが、クリックジャッキングや情報漏えいの被害を抑える防御が弱い状態です。

確認済み Strict-Transport-Security と X-Content-Type-Options が無いことを確認しました。（確認: Terashia 技術担当）

5. Cookie の安全属性の不足 低

どういう問題か: ログイン状態を保つ Cookie に、盗まれにくくする設定が足りない可能性があります。

事業への影響: 他の問題と組み合わさると、ログイン状態の乗っ取りにつながる可能性があります。

確認済み ログイン後のセッション Cookie に SameSite 属性が無いことを確認しました。（確認: Terashia 技術担当）

6. エラー情報の露出 低

どういう問題か: エラー時に、内部の構成がわかる情報を画面に表示しています。

事業への影響: 攻撃者が内部構成（使用技術・ファイルの場所・SQL 文など）を知り、攻撃の手がかりにする可能性があります。

確認済み 予約 ID に文字列を指定すると、スタックトレースと内部のファイルパスが表示されることを確認しました。（確認: Terashia 技術担当）

6. 対応優先順位

優先度	発見事項	推奨する対応期限

SAMPLE

高	SQL インジェクション	2 週間以内
中	Content-Security-Policy（CSP）が未設定	1 か月以内
中	公開不要な管理・監視用の画面や情報の露出	1 か月以内
低	セキュリティ関連ヘッダーの不足	次回の改修時
低	Cookie の安全属性の不足	次回の改修時
低	エラー情報の露出	次回の改修時

期限は目安です。公開範囲・利用者数・取り扱う情報の重要度に応じて、開発会社と相談のうえ決めてください。

7. 今後の推奨アクション

1. 同封の「開発者向け修正依頼書」を開発会社へ渡し、修正の見積りと予定を確認してください。
2. 修正後、同じ範囲で再診断を行い、修正が有効であることを確認してください。
3. 個人情報を扱う画面が多いため、年 1 回または大きな改修の後に定期診断を行ってください
4. 機能追加や大きな改修のたびに、診断の対象と時期を見直してください。

8. 未検査項目と残存リスク

- 管理者画面と、管理者権限での操作
- 決済代行サービスとの連携部分（外部サービスのため対象外）
- メール送信・ファイルアップロードの悪用（今回の範囲外）
- サーバー・ネットワーク機器・クラウド設定そのもの
- 診断期間の後に行われた変更

本診断は脆弱性が存在しないことを保証するものではありません。上記の未検査項目、診断後の変更、未知の攻撃手法によるリスクは残ります。

9. 追加検証が必要な事項（未確定）

以下は確認済みの事実ではありません。自動診断ツールの検出のうち、今回の範囲では技術者が再現・否定のどちらも確定できなかったものです。追加の検証で判断します。

事項	ツール判定	未確定の理由
既知の脆弱性を持つ部品の利用	中	応答から古い版の jQuery を検出しましたが、実際に読み込まれる画面と影響する機能の利用有無を外部からは確定できません。開発会社に依存関係の版の確認をお願いします。

10. レポートの利用条件

- 本レポートはお客様の社内での改善と、お客様が委託する開発会社への共有を目的としています
- 第三者（取引先・投資家など）へ提示する場合は、診断の範囲・期間・制限を省略せずに提示してください。本レポートは対象の安全性を証明・保証するものではありません

SAMPLE

・本レポートには攻撃に悪用されうる情報が含まれます。共有先を必要最小限にしてください

発行: Terashia（2026-11-20 生成）

SAMPLE