Terashia ｜ Webアプリ脆弱性診断

【サンプル】開発者向け修正依頼書

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。

項目	内容
お客様	架空の顧客 A 社（サンプル）
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）
診断期間	2026-11-16 〜 2026-11-18
報告日	2026-11-20
レポート番号	SAMPLE-2026-001
確認担当	Terashia 技術担当

この文書の使い方

- 各項目は、Terashia の技術者が確認した**確認済みの事実**です（ツールの検出をそのまま載せたものではありません）。
- 「修正方針の候補」は一般的な対策の例です。実装に合わせて選んでください。
- 「受け入れ基準」を満たしたら修正完了とし、再診断で確認します。
- 末尾の「追加検証が必要な事項」は**未確定**です。修正の前に、事実かどうかの確認をお願いします。

一覧

ID	発見事項	重大度	箇所数	対応の目安
TF-1CB359DC	SQL インジェクション	高	1	2 週間以内
TF-4C30E6C3	Content-Security-Policy（CSP）が未設定	中	3	1 か月以内
TF-5303E1C6	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
TF-EC75D5A5	セキュリティ関連ヘッダーの不足	低	2	次回の改修時
TF-AD174075	Cookie の安全属性の不足	低	1	次回の改修時
TF-67D79FB0	エラー情報の露出	低	1	次回の改修時

SAMPLE

TF-1CB359DC SQL インジェクション

- **重大度:** 高（ツールの判定: 高、確度: 中）
- **分類:** CWE-89 / A03:2021 Injection
- **状態:** 確認済み（Terashia 技術担当、2026-11-18T15:00:00+09:00）

脆弱性の技術的説明

ユーザー入力が SQL 文に文字列連結で組み込まれ、引用符や SQL 構文で問い合わせの意味を変えられる状態です。

対象箇所

メソッド	URL	パラメータ
GET	`https://app.example.com/api/reservations/search?keyword=test`	keyword

検証証拠

- 技術者の確認: 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。
- 検出したツール: zap（40018: SQL Injection）
- 応答に含まれていた証拠（抜粋）:

```
https://app.example.com/api/reservations/search?keyword=test: SQLSTATE[42000]: Syntax error or access violation
```

再現条件

対象パラメータに引用符（'）や論理式（' OR '1'='1 など）を含む値を送り、応答の差（エラー、件数、ログイン成否、応答時間）を確認します。

修正方針の候補

1. プレースホルダ（プリペアドステートメント）か ORM のパラメータ束縛で問い合わせを組み立てる
2. 文字列連結で SQL を組み立てている箇所をすべて洗い出して置き換える
3. データベース接続ユーザーの権限を必要最小限にする

受け入れ基準

- [ ] 対象パラメータに引用符・SQL 構文を含む値を送っても、エラーや結果件数の変化が起きない
- [ ] 該当箇所のコードがパラメータ束縛になっていることをレビューで確認できる
- [ ] 同じ実装パターンの他の箇所も修正済みである

参考情報

- https://owasp.org/Top10/A03_2021-Injection/
- https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html
- https://cwe.mitre.org/data/definitions/89.html

SAMPLE

TF-4C30E6C3 Content-Security-Policy（CSP）が未設定

- **重大度:** 中（ツールの判定: 中、確度: 高）
- **分類:** CWE-693 / A05:2021 Security Misconfiguration
- **状態:** 確認済み（Terashia 技術担当、2026-11-18T15:10:00+09:00）

脆弱性の技術的説明

応答に Content-Security-Policy ヘッダー（または安全な値）がありません。

対象箇所

メソッド	URL	パラメータ
GET	`https://app.example.com/`	—
GET	`https://app.example.com/login`	—
GET	`https://app.example.com/reservations`	—

検証証拠

- 技術者の確認: 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。
- 検出したツール: zap（10038: Content Security Policy (CSP) Header Not Set）、nuclei（http-missing-security-headers: HTTP Missing Security Headers（content-security-policy））

再現条件

対象 URL の応答ヘッダーに Content-Security-Policy が含まれるかを確認します。

修正方針の候補

1. Content-Security-Policy を設定し、script-src を自社と必要な配信元に限定する
2. まず Content-Security-Policy-Report-Only で影響を確かめてから適用する

受け入れ基準

- [ ] 主要なページの応答に、インラインスクリプトを許可しない CSP が含まれる

参考情報

- https://developer.mozilla.org/ja/docs/Web/HTTP/CSP
- https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html

SAMPLE

TF-5303E1C6 公開不要な管理・監視用の画面や情報の露出

- **重大度:** 中（ツールの判定: 中、確度: 中）
- **分類:** CWE-200 / A05:2021 Security Misconfiguration
- **状態:** 確認済み（Terashia 技術担当、2026-11-18T15:20:00+09:00）

脆弱性の技術的説明

監視用エンドポイント（/metrics など）や設定・デバッグ用の URL が、認証なしで応答しています。

対象箇所

メソッド	URL	パラメータ
GET	`https://app.example.com/actuator/env`	—

検証証拠

- 技術者の確認: /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）。
- 検出したツール: nuclei（springboot-env: Spring Boot Actuator - Environment Exposure）
- 応答に含まれていた証拠（抜粋）:

```
https://app.example.com/actuator/env: activeProfiles
```

再現条件

対象 URL へ認証なしでアクセスし、内部情報が返るかを確認します。

修正方針の候補

1. 監視・デバッグ用のエンドポイントは、社内ネットワークか認証の内側へ移す
2. 本番環境で不要なものは無効化する

受け入れ基準

- [ ] 認証なしのアクセスで、監視・設定・デバッグ情報が返らない（401/403/404）

参考情報

- https://owasp.org/Top10/A05_2021-Security_Misconfiguration/

SAMPLE

TF-EC75D5A5 セキュリティ関連ヘッダーの不足

- **重大度:** 低（ツールの判定: 低、確度: 高）
- **分類:** CWE-693 / A05:2021 Security Misconfiguration
- **状態:** 確認済み（Terashia 技術担当、2026-11-18T15:35:00+09:00）

脆弱性の技術的説明

応答に、X-Frame-Options / frame-ancestors、X-Content-Type-Options、Strict-Transport-Security、Permissions-Policy などのヘッダーが不足しているか、サーバーの版情報が含まれています。

対象箇所

メソッド	URL	パラメータ
GET	`https://app.example.com/`	—
GET	`https://app.example.com/`	x-content-type-options

検証証拠

- 技術者の確認: Strict-Transport-Security と X-Content-Type-Options が無いことを確認しました。
- 検出したツール: zap（10021: X-Content-Type-Options Header Missing）、nuclei（http-missing-security-headers: HTTP Missing Security Headers（strict-transport-security））

再現条件

対象 URL の応答ヘッダーを確認します（curl -I など）。

修正方針の候補

1. Web サーバーかアプリの共通ミドルウェアで、推奨ヘッダーをまとめて付与する
2. Server / X-Powered-By などの版情報を応答から外す

受け入れ基準

- [ ] 主要なページの応答に推奨ヘッダーが含まれ、版情報が含まれない

参考情報

- https://owasp.org/www-project-secure-headers/
- https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Headers_Cheat_Sheet.html

SAMPLE

TF-AD174075 Cookie の安全属性の不足

- **重大度:** 低（ツールの判定: 低、確度: 中）
- **分類:** CWE-1275 / A05:2021 Security Misconfiguration
- **状態:** 確認済み（Terashia 技術担当、2026-11-18T15:30:00+09:00）

脆弱性の技術的説明

Cookie に HttpOnly / Secure / SameSite 属性の一部がありません。

対象箇所

メソッド	URL	パラメータ
POST	`https://app.example.com/login`	SESSIONID

検証証拠

- 技術者の確認: 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。
- 検出したツール: zap（10054: Cookie without SameSite Attribute）
- 応答に含まれていた証拠（抜粋）:

```
https://app.example.com/login: Set-Cookie: SESSIONID
```

再現条件

対象の応答の Set-Cookie ヘッダーの属性を確認します。

修正方針の候補

1. セッション Cookie に HttpOnly・Secure・SameSite=Lax 以上を付ける

受け入れ基準

- [ ] セッション Cookie の Set-Cookie に 3 つの属性が含まれる

参考情報

- https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html

SAMPLE

TF-67D79FB0 エラー情報の露出

- **重大度:** 低（ツールの判定: 低、確度: 中）
- **分類:** CWE-209 / A05:2021 Security Misconfiguration
- **状態:** 確認済み（Terashia 技術担当、2026-11-18T15:40:00+09:00）

脆弱性の技術的説明

例外のスタックトレースやフレームワークのデバッグ情報が、応答本文に含まれています。

対象箇所

メソッド	URL	パラメータ
GET	`https://app.example.com/api/reservations/abc`	—

検証証拠

- 技術者の確認: 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。
- 検出したツール: zap（90022: Application Error Disclosure）
- 応答に含まれていた証拠（抜粋）:

```
https://app.example.com/api/reservations/abc: at app.reservation.ReservationController.show (/srv/app/src/...)
```

再現条件

対象 URL に不正な値を送り、応答にスタックトレースや内部パスが含まれるかを確認します。

修正方針の候補

1. 本番環境ではデバッグ表示を無効化し、利用者には汎用のエラーメッセージだけを返す
2. 詳細はサーバー側のログにだけ残す

受け入れ基準

- [ ] 不正な入力を送っても、応答にスタックトレース・内部パス・SQL 文が含まれない

参考情報

- https://cheatsheetseries.owasp.org/cheatsheets/Error_Handling_Cheat_Sheet.html
- https://cwe.mitre.org/data/definitions/209.html

SAMPLE

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、技術者が今回の範囲で確定できなかったものです。修正の前に、事実かどうかの確認をお願いします。

ID	事項	ツールの判定	未確定の理由	対象の例
TF-D54E5A8A	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。	`https://app.example.com/assets/js/jquery-1.12.4.min.js`

SAMPLE

参考情報（対応不要）

ID	事項	内容
TF-C088B30D	使用技術の特定（情報）	使っている技術や仕組みが外部から判別できます（それ自体は問題ではありません）。

SAMPLE

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。誤検知として除外した検出は 1 件です。

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
- 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