

サンプル商事株式会社 様

診断報告書

プラン：AI診断

実施日：2026年10月10日

対象：example-sample-shop.jp

※本書は架空のサイトを例にした見本です。実在の企業・サイトとは関係ありません。

1 何が起こるのか

お客様や利用者の情報が、外部に漏れる可能性があります

今回の診断の範囲で、至急対応が必要な問題が1件、早めの対応をおすすめする問題が1件見つかりました。試した攻撃8種類のうち、問題が見つかったのはこの2種類です。

2 何から直すか

No.1	至急対応	お問い合わせフォームに、不正な指示を混ぜて送ってしまう箇所がある	担当：制作・開発会社
No.2	早めに対応	一部のページで、別のサイトに見せかけた表示を差し込める可能性がある	担当：制作・開発会社

3 誰に何を頼めばいいか

サイトの制作・開発会社へ

No.1・No.2の修正を依頼してください。技術付録をそのまま渡せば伝わります。

→ 付録（技術担当者向け）

次回の診断

上記の修正後、または新しい機能を追加したときに、再度の診断をおすすめします。目安は半年後です。

→ 時期：修正後・機能追加時

4 技術担当者向けの付録

付録：技術担当者向け（再現手順は別途お渡しします）

No.1 SQLインジェクション [CWE-89] High (8.6)

対象 お問い合わせフォーム (/contact の message)

対策 入力値をブレースホルダ（パラメータ化クエリ）で処理する。入力値の検証を追加する。

No.2 蓄積型クロスサイトスクリプティング [CWE-79] Medium (6.1)

対象 商品レビュー投稿欄 (/review の body)

対策 出力時にHTMLエスケープを行う。
Content-Security-Policy を設定する。

本診断は、AIによるサイバー攻撃を想定した耐性テストです。決まったチェックリストをすべて検査するものではなく、すべての弱点の発見を保証するものではありません。深刻度(CVSS)は診断時に算出した参考値です。再現に必要な詳細手順は、別途、安全な方法でお渡しします。

実施した確認の一覧

今回の診断で試した攻撃の種類と、その結果です。問題が見つからなかった項目も記載しています。

確認した攻撃の種類	結果	補足
SQLインジェクション（データベースへの不正操作）	問題あり	No.1 として報告
クロスサイトスクリプティング（表示の乗っ取り）	問題あり	No.2 として報告
OSコマンドインジェクション	問題なし	
認証・ログイン回りの不備	対象外	今回はログイン前のみ診断
アクセス制御の不備（他人の情報の閲覧）	対象外	今回はログイン前のみ診断
パス・トラバーサル（非公開ファイルの閲覧）	問題なし	
サーバーの情報漏えい（設定ファイル等）	問題なし	
なりすまし投稿（CSRF）	問題なし	