

セキュリティ診断レポート - 表示サンプル

架空データによる表示例です。実サイトの診断結果や文章レビューの実績ではありません。

対象: <https://sample.example.com/> (サンプル用)

作成日: 2026-10-22 / 商品: 日本語レポート・PDF付き 2,980円 (税込)

まず行うこと

担当者がHTTP応答ヘッダーを確認し、サイトの構成に応じてクリックジャッキング対策とMIME判定制限を設定します。

検出の概要 (架空)

Critical 0件 / High 0件 / Medium 0件 / Low 1件

業務影響: 情報の一部が外部から確認できる可能性があります。ヘッダー不足だけで、情報漏洩や不正操作が成立すると断定できません。

今回の表示例: 応答ヘッダーの一部が設定されていない状態。

CVE: 特定のCVEには該当しません。CVSS・EPSS・KEVは適用外です。

推奨対策 (表示例)

1. サイトの構成と、iframeへの埋め込みが必要なページを確認します。
2. 必要に応じてContent-Security-Policyのframe-ancestorsとX-Content-Type-Optionsを設定します。
3. 変更後に主要画面の動作とヘッダーを確認し、再診断します。

設定値はCDN・Webサーバー・既存機能を確認して決めます。

再確認と文章レビュー

実運用ではCritical / Highを再確認します。このLowの表示例は対象外です。再現しない場合も、修正済みとは断定しません。

実商品ではMuseのwriterと独立reviewerが説明文を確認します。本サンプルは編集済みの表示例です。

実行範囲・情報の時点

採用範囲: 固定コーパスの署名付きHTTPテンプレート4,352件。元のHTTP 11,703件から選別しています。このサンプルではテンプレートを実行していません。

GET/HEAD・同一オリジンに限定。リダイレクト・コード・ブラウザ操作・POST・内部ネットワーク・新規脆弱性・認可ロジックは対象外です。検出0件でも安全を保証しません。

NVD / CISA KEV / EPSS / JVN: この表示サンプルでは未取得です。実商品では各情報源の取得日・版・取得失敗や古さを明示します。

参考資料: <https://owasp.org/www-project-secure-headers/>

レポートはスキャン時点の記録です。対策の適用判断と動作確認は、対象システムの管理者が行ってください。