

Web アプリケーション 脆弱性診断報告書

提出先 株式会社サンプル商事 御中

サンプルレポート

本書は架空の企業・システムを想定したサンプルです。記載の社名・ドメイン・IP アドレス・担当者名・数値は実在しません。

株式会社セキュア DX
セキュリティ事業部

1. エグゼクティブサマリ

1.1 診断概要

項目	内容
案件名	サンプル商事様 Web アプリケーション脆弱性診断
診断対象	サンプルオーダー（B2B-EC サイト）
対象 URL	https://stg.shop.example.jp/（本番環境 www.shop.example.jp は診断対象外）
対象環境	ステージング環境（本番同等構成）
診断方式	ブラックボックス（リモート診断）
診断期間	7 営業日
使用ツール	Burp Suite Professional、Chrome DevTools、Nmap（ssl-enum-ciphers）
除外事項	DoS/DDoS 試験、およびデータの破壊・改変を伴う試験は、事前合意に基づき実施していない
診断担当 / 品質レビュー	山田太郎 / 佐藤一郎

1.2 総合評価

総合評価: 高 (High)

本診断の結果、合計 11 所見の脆弱性・設定不備・推奨事項を検出した。これに加え、複数の所見が組み合わさることで**高 (High)** 相当のリスクとなる複合所見を 1 件（WebAP-C01）識別した。

最も重大な所見は、商品検索 API の **SQL インジェクション**（WebAP-001、**高 (High)**）である。認証済みユーザーであれば検索キーワードを通じて任意の SQL 文を実行でき、会員情報・注文情報の取得やデータの改ざんにつながる。個人情報漏洩に直結するため、即時の修正を推奨する。また、商品検索画面では反射型クロスサイトスクリプティング（WebAP-002）も確認されており、入力値の検証と出力エスケープの見直しが必要である。

次に、パスワードリスト型攻撃に対する防御の不在（WebAP-C01）がある。ログイン試行回数の制限がなく（WebAP-004）、多要素認証が未実装であり（WebAP-005）、かつ有効なログイン ID が URL パラメータから取得可能な状態（WebAP-006）にある。これら 3 つの条件が同時に揃うこと

で、外部から流出した ID・パスワードの組み合わせを用いた攻撃を事実上無制限に試行できる状態となっている。

また、API レスポンスへの過剰なデータ公開（WebAP-003）では、ユーザー情報 API が画面表示に不要な権限構造・営業担当者情報・組織内部情報を返却しており、ソーシャルエンジニアリングの足がかりとなるリスクが確認された。

一方、CSRF、IDOR、権限昇格、SSRF などの脆弱性は検出されず、JWT 署名検証、価格改ざん防止、数量バリデーションなど、セキュリティ上重要な機能は適切に実装されている。ただし、これらは本診断の範囲・手法・実施時点において問題を確認できなかったことを示すものであり、脆弱性が存在しないことを保証するものではない（4.2 参照）。

1.3 検出脆弱性の統計

深刻度	所見数
緊急 (Critical)	0
高 (High)	1 + 複合所見 1
中 (Medium)	5
低 (Low)	2
情報 (Info)	3
合計	11 所見 + 複合 1

※ 複合所見（WebAP-C01）は個別所見の重複カウントではなく、組み合わせにより生じる追加リスクの評価である。

1.4 推奨対応の優先度

優先度は深刻度（技術的な危険度）の順位ではなく、対応の緊急性・影響範囲・実現容易性を総合的に勘案した **対応時期の目安** である。

優先度	該当所見
優先度 1（即時対応）	WebAP-001
優先度 2（1 ヶ月以内）	WebAP-002、WebAP-003、WebAP-004、WebAP-005、WebAP-006
優先度 3（3 ヶ月以内）	WebAP-007、WebAP-008
優先度 4（次回改修時）	WebAP-009、WebAP-010
推奨事項	WebAP-011

2. 診断範囲と手法

2.1 診断対象

項目	内容
サイト名	サンプルオーダー
URL	https://stg.shop.example.jp/
種別	B2B-EC サイト（法人向け消耗品発注システム）
技術スタック	Next.js（React）、Node.js
認証方式	JWT、アクセストークン（30 分）＋リフレッシュトークン（14 日間）
テストアカウント	一般ユーザー、グループ管理者（貴社よりご提供）

2.2 診断手法

78 項目・10 カテゴリ（認証、認可、セッション管理、入力検証、暗号化、構成管理、ビジネスロジック等）の診断チェックリストに基づき、以下の 3 フェーズで診断を実施した。

フェーズ	内容	手法
Phase A	自動スキャン	Burp Scanner による自動スキャン
Phase B	スキャナ＋手動併用	ツール結果の手動検証・誤検知排除
Phase M	手動診断	認証・認可・ビジネスロジック・セッション管理の手動テスト

3. 検出脆弱性の詳細

本章では主要な所見を深刻度の高い順に記載し、その他の所見は 3.7 に一覧で示す。

章番号	所見 ID	所見名	深刻度
3.1	WebAP-001	SQL インジェクション	高 (High)
3.2	WebAP-C01	パスワードリスト型攻撃に対する防御の不在【複合所見】	高 (High)
3.3	WebAP-002	クロスサイトスクリプティング (反射型)	中 (Medium)
3.4	WebAP-003	API レスポンスへの過剰なデータ公開	中 (Medium)
3.5	WebAP-004	アカウントロック・レート制限の欠如	中 (Medium)
3.6	WebAP-005 / WebAP-006	多要素認証の未実装 / URL パラメータへのユーザーID 含有	情報 (Info)
3.7	WebAP-007～WebAP-011	その他の所見 (一覧)	中 (Medium) ～情報 (Info)

3.1 WebAP-001: SQL インジェクション

項目	内容
深刻度	高 (High)
CVSS スコア	8.8 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
CWE / OWASP	CWE-89 (Improper Neutralization of Special Elements used in an SQL Command) / A03:2021 — Injection
検出箇所	GET /api/v2/items/search?q=...

概要

商品検索 API の q パラメータに入力した値が、適切にエスケープされずに SQL 文へ組み込まれていることを確認した。認証済みユーザーであれば、検索キーワードを通じてデータベースに対して任意の SQL 文を実行できる状態にある。

再現手順

- ログイン済み状態で商品検索 API にシングルクォートを含むキーワードを送信し、データベースエラーを示す応答 (HTTP 500) が返ることを確認

2. 常に真となる条件式を付加したキーワードを送信し、検索結果が本来と異なる件数（全件）で返ることを確認
3. 応答時間に差が生じる条件式を送信し、時間ベースの判定でも脆弱性が成立することを確認

※ 脆弱性の存在確認にとどめ、実データの取得やデータの改変は行っていない。

想定リスク

- 会員情報（氏名・住所・メールアドレス・ログイン ID）や注文情報の全件取得による個人情報漏洩
- データの改ざん・削除、認証の迂回、DB アカountの権限によってはサーバー上でのコマンド実行
- B2B-EC サイトとして取引先情報を扱うため、漏洩時の事業影響と信用上の損害は極めて大きい

推奨対策

- 【最優先】プレースホルダ（バインド変数）を使った SQL 文の組み立てに修正する。ORM を利用している場合も生 SQL の連結箇所がないか確認する
- アプリケーションから利用する DB アカountの権限を必要最小限（参照専用等）にする
- データベースエラーの詳細を画面・API 応答に表示しない
- 修正後、他の検索・絞り込み系 API にも同様の実装がないか横展開で確認する

参考情報

- CWE-89: <https://cwe.mitre.org/data/definitions/89.html>
- IPA 安全なウェブサイトの作り方（SQL インジェクション）: <https://www.ipa.go.jp/security/vuln/websecurity/sql.html>

3.2 WebAP-C01: パスワードリスト型攻撃に対する防御の不在【複合所見】

項目	内容
深刻度	高（High）（複合評価）
CVSS スコア	7.9（複合評価、CVSS v3.1 ベース。単一ベクトルでは複合条件を表現できないためベクトルは省略）
構成所見	WebAP-004、WebAP-005、WebAP-006

概要

本所見は、以下の 3 つの個別所見が同時に存在することにより、パスワードリスト型攻撃（クレデンシャルスタッフィング）を事実上無制限に試行できる状態にあることを報告するものである。個別所見の深刻度はいずれも中（Medium）または情報（Info）であるが、複合条件下でのリスクを高（High）と評価した。

条件	該当所見	単独深刻度
有効なログイン ID が外部から取得可能	WebAP-006（URL パラメータへのログイン ID 含有）	情報（Info）
ログイン試行回数に制限がない	WebAP-004（アカウントロック・レート制限の欠如）	中（Medium）
パスワード以外の認証要素がない	WebAP-005（多要素認証の未実装）	情報（Info）

深刻度判定根拠

CVSS は所見単体の評価基準であり、複数の欠落が重なった場合の実質的なリスクを表現できない。本件では、攻撃者が URL パラメータやリファラーログから有効なログイン ID を収集したうえで、外部から流出したパスワードリストを用いて無制限にログインを試行できる。成功した場合、パスワード以外に認証を阻止する手段が存在しない。B2B-EC サイトとして取引情報・発注機能を扱うシステムであり、アカウント乗っ取り時の事業影響（不正発注、取引情報の漏洩、取引先への二次被害）を考慮し、複合条件下でのリスクを高（High）と評価した。

想定リスク

- 攻撃者が URL パラメータ・リファラーログ・プロキシログ等から有効なログイン ID を収集する（WebAP-006）
- 外部から流出したパスワードリスト（他サービスの漏洩データベース等）を入手する
- 収集したログイン ID に対し、パスワードリストの組み合わせを自動送信する（WebAP-004: 試行回数制限なし）
- パスワードが一致した場合、他に認証を阻止する手段がないためログインが成功する（WebAP-005: MFA 未実装）
- 攻撃者は被害者のアカウントとして取引情報の閲覧、不正発注、プロフィール変更等が可能となる

推奨対策

本所見は 3 つの個別所見の組み合わせであるため、いずれか 1 つの対策でもリスクは大幅に低減する。以下の優先順で対策を推奨する。

1. 【最優先】ログイン試行回数の制限を実装する（WebAP-004 の対策参照）。攻撃の試行回数を制限することで、パスワードリスト型攻撃の実行可能性を直接的に低減する
2. 【推奨】管理者権限アカウントから段階的に MFA を導入する（WebAP-005 の対策参照）。パスワードが一致しても第二認証要素で阻止できる
3. 【推奨】ログイン ID を URL パラメータから除外する（WebAP-006 の対策参照）。有効な ID の収集を困難にする

参考情報

- CWE-307: <https://cwe.mitre.org/data/definitions/307.html>
- OWASP — Credential Stuffing: https://owasp.org/www-community/attacks/Credential_stuffing

3.3 WebAP-002: クロスサイトスクリプティング（反射型）

項目	内容
深刻度	中 (Medium)
CVSS スコア	6.1 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)
CWE / OWASP	CWE-79 (Improper Neutralization of Input During Web Page Generation) / A03:2021 — Injection
検出箇所	商品検索画面 /items?q=...

概要

商品検索画面において、URL パラメータ q の値が HTML エスケープされずに「"○○" の検索結果」として画面に出力されている。スクリプトタグやイベントハンドラを含むキーワードを指定した URL を開くと、閲覧者のブラウザ上で任意のスクリプトが実行される。

再現手順

1. q パラメータに `<img src=x onerror=alert(document.domain)>` を含む URL を作成
2. ログイン済みブラウザで当該 URL を開く
3. ダイアログが表示され、スクリプトが実行されることを確認

想定リスク

- 細工した URL を取引先担当者にメール等で送り付け、開かせることで、ログイン中のセッションを利用した不正操作（発注、プロフィール変更）や画面の改ざん、フィッシングサイトへの誘導が

可能になる

- 本所見は WebAP-003（営業担当者情報の露出）およびメール送信ドメイン認証の不備と組み合わせることで、標的型攻撃の成功率を高める

推奨対策

- 画面出力時に HTML エスケープを徹底する（フレームワークのテンプレート機能を利用し、生 HTML 挿入を避ける）
- 多層防御として Content-Security-Policy ヘッダーを設定する（WebAP-007 参照）
- 修正後、他の入力値を画面に反映する箇所（絞り込み条件、エラーメッセージ等）にも同様の実装がないか確認する

参考情報

- CWE-79: <https://cwe.mitre.org/data/definitions/79.html>
- IPA 安全なウェブサイトの作り方（クロスサイト・スクリプティング）: <https://www.ipa.go.jp/security/vuln/websecurity/cross-site-scripting.html>

3.4 WebAP-003: API レスponsへの過剰なデータ公開

項目	内容
深刻度	中 (Medium)
CVSS スコア	5.0 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N)
CWE / OWASP	CWE-200 / API3:2023 — Broken Object Property Level Authorization
検出箇所	GET /api/v2/account/profile

概要

ユーザー情報取得 API のレスポンスに、画面表示に不要な内部システム情報が大量に含まれている。なお、本所見は自身のアカウント情報の API レスポンスに過剰な情報が含まれるものであり、他ユーザーの情報を取得できる状態（IDOR）ではない。露出するフィールドに営業担当者の氏名・メールアドレス・営業所情報が含まれており、標的型フィッシングの素材として悪用可能なことから **中 (Medium)** と判定した。

検出された過剰情報（抜粋）

分類	フィールド名	レスポンス例	問題点
権限・アクセス制御	permissions	[{"funcId":"F0012","enabled":true}, ...]（計 24 個）	機能別の権限フラグが全件公開。無効化されている機能 ID の特定が可能
権限・アクセス制御	modules	["MOD001","MOD002", ...]	機能モジュール構成が露出。非公開 API エンドポイントを推測可能
営業担当者情報	repEmail / officeEmail	[@example.net]（テスト値） / [@example.co.jp]	営業担当者・社内システム用メールアドレスの露出。本番環境では実際の業務メールアドレスが格納されると推定される
営業担当者情報	officeTel / officeAddress	0120-000-000 / 東京都千代田区サンプル1-2-3	営業所の電話番号・所在地。電話による偽装・なりすましに利用可能
営業担当者情報	deptName / repCode	営業事業部 / A-017	部署名と内部コード。組織構造のマッピングが可能

想定リスク

1. 標的型フィッシング: 営業担当者情報（メールアドレス・営業所名・住所・電話番号）を使った、顧客や社内関係者へのなりすましメール送信。NW 診断で確認されたメール送信ドメイン認証の不備（NW-005）と組み合わせることで実行可能性が高まる（総合サマリー報告書 3.1 参照）
2. 権限昇格: permissions と modules から非公開 API・管理機能の推測と攻撃（実際の成功は本診断では確認されていない）
3. 組織偵察: 内部コード体系から組織構造のマッピング

推奨対策

- 【優先度: 高】API レスポンスをフロントエンド表示に必要なフィールドのみに限定（DTO/シリアライザによるホワイトリスト方式）
- 【優先度: 高】permissions、modules、営業担当者・営業所の連絡先をレスポンスから速やかに除外。フロントエンド表示で参照しているフィールドがないことを事前に確認する
- 【設計改善】DB エンティティをそのままレスポンスに含めず、用途別のレスポンス DTO を設計

参考情報

- OWASP API Security Top 10 — API3:2023: <https://owasp.org/API-Security/editions/2023/en/0xa3-broken-object-property-level-authorization/>

3.5 WebAP-004: ログイン試行に対するアカウントロック・レート制限の欠如

項目	内容
深刻度	中 (Medium)
CVSS スコア	5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)
CWE	CWE-307 (Improper Restriction of Excessive Authentication Attempts)
検出箇所	POST /api/v2/auth/login
関連所見	WebAP-C01 (複合所見)、WebAP-005、WebAP-006

概要

ログイン API に対して連続 30 回の認証失敗を実行したが、アカウントロック・レート制限・CAPTCHA 表示等の防御機構が動作することを確認できなかった。すべて同一の HTTP 401 レスポンスであり、試行回数による応答内容・応答時間の変化は確認されなかった。本所見は単独では**中 (Medium)** だが、WebAP-005 および WebAP-006 と組み合わせることで、パスワードリスト型攻撃を事実上無制限に試行できる状態となる (WebAP-C01)。

推奨対策

- 一定回数 (5 回程度) の認証失敗後にアカウントを一時ロック (15~30 分)。ただしアカウントロックのみでは正規利用者をログインできなくする「ロックアウト DoS」が可能になるため、IP アドレスベースのレート制限 (同一 IP から 1 分間に 20 回以上の試行を制限) と併せた設計を推奨する
- 連続失敗後に CAPTCHA 表示、認証失敗ログの記録と異常検知アラート
- 多要素認証 (MFA) の導入 (WebAP-005 参照)。特に管理者権限アカウントについては優先的な導入を推奨する

参考情報

- CWE-307: <https://cwe.mitre.org/data/definitions/307.html>

3.6 WebAP-005 / WebAP-006: 複合所見を構成する情報 (Info) 所見

WebAP-005: 多要素認証 (MFA) の未実装 — 情報 (Info) /CWE-308/ログイン認証全般

認証はログイン ID+パスワードの単一要素認証のみ。パスワードが漏洩した場合にアカウント乗っ取りを防ぐ手段がない。WebAP-004 および WebAP-006 と組み合わせることで、パスワードリスト型

攻撃への耐性が大幅に低下する（WebAP-C01 参照）。管理者権限アカウントから段階的に MFA を導入することを推奨する。

WebAP-006: URL パラメータへのユーザー ID 含有 — 情報（Info） / CWE-598 / GET /api/v2/coupons?accountId=...

URL クエリパラメータにログイン ID（accountId）が含まれている。単体では認証に使用できないが、ブラウザ履歴・リファラー・プロキシログへの漏洩リスクがあり、パスワードリスト型攻撃の足がかりとなる（WebAP-C01 参照）。ログイン ID を URL クエリパラメータから除外し、サーバー側でセッション情報からユーザーを識別する方式に変更することを推奨する。

3.7 その他の所見（一覧）

所見 ID	所見名	深刻度	概要と推奨対策
WebAP-007	セキュリティヘッダーの未設定 （CSP / HSTS / X-Frame-Options）	中（Medium）	フロントエンド側で 3 つの主要ヘッダーが未設定。フレームワークの設定で一括設定し、CSP は Report-Only で運用してから本適用することを推奨。WebAP-002（XSS）の多層防御としても有効
WebAP-008	TLS 設定の脆弱性 （Forward Secrecy 未対応）	中（Medium）	使用中の暗号スイートが Forward Secrecy をサポートしない。ECDHE 系暗号スイートの優先、TLS 1.3 の有効化を推奨（NW 診断報告書 NW-004 と同時対応）
WebAP-009	サーバー情報の露出（X-Powered-By）	低（Low）	フレームワーク名がヘッダーで開示されている。poweredByHeader: false の設定を推奨
WebAP-010	パスワードポリシーの不備	低（Low）	最小長 4 文字、最大長 16 文字。NIST SP 800-63B に基づき最小長 8 文字以上、最大長 64 文字以上への変更を推奨
WebAP-011	security.txt の未設置	情報（Info）	RFC 9116 に基づき /.well-known/security.txt に脆弱性報告の連絡先を設置することを推奨

4. 補足情報

4.1 検出されなかった主要な脆弱性カテゴリ

以下の主要な脆弱性カテゴリについては、本診断において検出されなかった。ただし、検出されなかったことは脆弱性が存在しないことを保証するものではない（4.2 参照）。

- クロスサイトリクエストフォージェリ（CSRF）：JWT Bearer 認証の現行実装では Cookie 依存の CSRF 攻撃は成立しない
- 他ユーザーリソースへの不正アクセス（IDOR）、垂直権限昇格、SSRF
- JWT 署名検証の不備：alg:none 攻撃およびアルゴリズム混同攻撃を試行し、いずれもサーバー側で拒否されることを確認
- 価格改ざん：各リクエストで価格を改変して送信したが、サーバー側の価格が適用されることを確認

4.2 診断の限界事項

- 本診断はステージング環境に対する外部からのブラックボックス診断であり、ソースコード・データベースへの直接アクセスは行っていない。サーバーサイドの内部実装（パスワードハッシュ方式、ログ出力内容等）は検証対象外である
- 本報告書は診断期間・手法・アクセス権限の範囲内で検出された事項を報告するものであり、記載のない脆弱性が存在しないことを保証するものではない。誤検知・未検知の可能性を排除できない
- ステージング環境が本番環境と同等の構成である旨は貴社よりご申告いただいた情報に基づく。本番環境固有の構成・設定に起因する事象は本診断の対象外である
- 一部の検証項目（パスワードリセット、在庫整合性、注文二重送信等）はテスト環境の制約により完全な検証ができなかった。貴社での内部確認を推奨する
- DoS/DDoS 試験、およびデータの破壊・改変を伴う試験は、事前合意に基づき実施していない

4.3 今後の推奨事項

- 本報告書の所見対応後、再診断の実施を推奨（優先度 1・2 の所見は対策完了後 3 ヶ月以内）
- 定期的な脆弱性診断の実施（年 1 回以上）と、開発プロセスへのセキュリティテスト組み込み（SAST/DAST）を推奨
- ソースコード診断（ホワイトボックス診断）の実施を推奨。ブラックボックス診断では内部実装に起因する脆弱性の検出に限界がある

5. お問い合わせ窓口

本報告書の内容に関するご質問、対策実施に関するご相談は、以下までお問い合わせください。

項目	内容
会社名	株式会社セキュア DX
部門	セキュリティ事業部
担当者	山田太郎
メール	sample@example.com
Web サイト	https://www.secure-dx.co.jp/

付録: 参考規格・ガイドライン

- OWASP Testing Guide v4.2 / OWASP Top 10 (2021) / OWASP API Security Top 10 (2023)
- CWE (Common Weakness Enumeration) / CVSS v3.1
- NIST SP 800-63B (Digital Identity Guidelines)
- IPA 安全なウェブサイトの作り方
- RFC 6797 (HSTS) / RFC 9116 (security.txt)

※ 用語集・CVSS スコアの評価基準は「別紙: 診断対象・評価基準・用語集」を参照。