

HABILIS SECURITY / CONFIDENTIAL

VPS・Webアプリ セキュリティ診断 報告書

診断品質と成果物の形式を示すサンプル
(デモラボ実測 / 実在の顧客環境ではありません)

顧客	サンプルFX株式会社 御中（架空）
対象	Habilis Demo Lab（意図的に脆弱な検証環境）
実施期間	2026年10月24日
報告日	2026年10月24日
版	2.0
実施	Habilis（デモラボ検証） / 提携パートナー契約・保険・法務レビューは準備中。締結までは非破壊の確認のみ提供
区分	CONFIDENTIAL / SAMPLE

本サンプルは、意図的に脆弱なローカルラボで取得した実測結果です。実在の企業・IP・取引口座・顧客データとは関係ありません。実案件では、認証情報・個人情報をマスキングし、顧客の許可なく公表しません。

1. エグゼクティブサマリー

総合評価

High 5件 / Medium 2件 / Low 1件 / 管理策の確認 1件

最も優先すべき3つは以下。

1. 管理画面のアクセス制御 bypass (High)

クライアント側の `role` Cookie を `admin` に変更するだけで、一般ユーザーが管理画面に到達できた。

2. IDOR (High)

一般ユーザーのセッションで、他人のユーザー情報を取得できた。

3. SQLインジェクション (High)

`id=1 OR 1=1` で、商品テーブルの全件を取得できた。

経営判断に必要な影響

本ラボは意図的に脆弱な検証環境であり、実在の顧客データは含まない。

ただし、同じ設計が本番に存在する場合、以下につながる。

- 管理画面からの設定変更・顧客情報の閲覧
- 他人のアカウント情報の取得
- データベース内の情報の一括取得
- サーバー側からの内部サービスへの到達
- 不正なファイルの設置
- パスワード総当たりの踏み台化

30日以内の推奨アクション

- 管理画面の認可をサーバー側セッションで判定する
- オブジェクト取得時に所有者チェックを入れる
- SQLをパラメータ化する
- 外部URL取得に許可リストを設ける
- アップロードの拡張子・内容・保存先を制限する
- ログインにレート制限・ロックアウトを入れる
- CSP等のセキュリティヘッダを設定する
- 修正後に再確認する

対象

- Habilis Demo Lab (<http://127.0.0.1:18080>)
- Web/APIの認証、認可、入力検証、SSRF、ファイルアップロード、レート制限、セキュリティヘッダ
- 検証用Windowsホストの読み取り専用チェック (RDP、Firewall、Defender、起動項目、更新、ログ)

除外

- 実在の顧客システム、取引口座、決済基盤
- 外部インターネット上の第三者システム
- DoS / 負荷テスト
- マルウェア、WebShell、ランサムウェア
- データの持ち出し・大量取得
- ソーシャルエンジニアリング、物理、Wi-Fi
- クラウド事業者・取引所の基盤

制約

- 非破壊
- ループバックのみ
- SQLiは読み取り専用のBoolean
- アップロードはテキストのみ
- XSSは画面表示のみ
- SSRFはlocalhostのみ
- 実認証情報は使用しない

3. 方法論

PTES / OWASP Testing Guide / OWASP ASVS / CIS Benchmarks を参考に、以下の順で実施した。

1. 資産・入口の整理

ログイン、管理画面、API、検索、アップロード、URL取得機能を列挙。

2. 低リスク検証

未認証・一般ユーザー・改ざんCookieの3視点で認証/認可を確認。

3. 入力検証

SQLi、XSS、SSRF、ファイルアップロードを、安全なペイロードで確認。

1件の他ユーザー情報、3件の商品、内部トークン1件など、最小限の証拠に留めた。

5. 証拠化

HTTPステータス、応答ヘッダ、応答本文、スクリーンショット、再現手順を保存。

6. 誤検知レビュー

対照リクエストと比較し、単なる仕様か脆弱性かを判定。

7. 報告・修正・再確認

優先度、担当、期限、再確認方法を整理。

4. 所見一覧

ID	重大度	CVSS	タイトル	状態
H-01	High	8.1	クライアント制御のrole Cookieによる管理画面バイパス	Open
H-02	High	7.5	IDOR: 他人のユーザー情報を取得	Open
H-03	High	8.1	Boolean SQLインジェクション	Open
H-04	High	8.1	SSRF: 内部エンドポイントへ到達	Open
H-05	High	7.5	制限なしファイルアップロード	Open
M-01	Medium	6.1	反射型XSS	Open
M-02	Medium	5.3	ログインのレート制限・ロックアウトなし	Open
L-01	Low	3.1	セキュリティヘッダの欠如	Open

CVSSは参考値。実案件では、到達可能性・影響・既存の緩和策を確認して再評価する。

5. 詳細所見

H-01: クライアント制御のrole Cookieによる管理画面バイパス

- 重大度: High / CVSS: 8.1
- 対象: GET /admin
- 概要: 管理画面の認可が、クライアント側で変更可能な role Cookie に依存している。一般ユーザーでログイン後、role=admin に変更すると管理画面に到達できた。
- 証拠:
 - 一般ユーザー (role=user) : 403

- スクリーンショット: `evidence/lab_admin_bypass.png`
- **影響:** 管理機能の不正利用、顧客情報の閲覧、設定変更（推定。本検証では管理機能の全操作は未検証）。
- **修正:**
 - 認可判定をサーバー側セッション/トークンのロールで行う。
 - `role` Cookie を認可に使わない。署名・暗号化・HttpOnly・SameSiteを適切に設定する。
 - 管理画面の全エンドポイントにサーバー側の認可チェックを入れる。
- **再確認:** 一般ユーザーで `/admin` が403、管理者のみ200。Cookie改ざんが無効。

H-02: IDOR（他人のユーザー情報を取得）

- **重大度:** High / **CVSS:** 7.5
- **対象:** `GET /api/user/{id}`
- **概要:** ログイン済みであれば、パスの `id` を変えるだけで他人の情報を取得できた。セッションのユーザーIDと取得対象の所有者チェックがない。
- **証拠:**
 - aliceのセッションで `/api/user/1` → alice
 - 同じセッションで `/api/user/2` → bob（`bob@example.test`）
 - 生データ: `evidence/LAB-02_idor.json`
- **影響:** 顧客情報の閲覧、アカウント列挙、なりすましの足がかり。
- **修正:**
 - 取得対象がセッション所有者に属するか、毎回サーバー側で確認する。
 - 管理者以外は `id` を直接指定させない。必要な場合は推測困難なID+認可。
 - 自動テストに「他人のIDで403」を追加する。
- **再確認:** 一般ユーザーが他人のIDで403、自分のIDのみ200。

H-03: Boolean SQLインジェクション

- **重大度:** High / **CVSS:** 8.1
- **対象:** `GET /api/items?id=`
- **概要:** `id` をSQL文字列に直接埋め込んでいる。 `1 OR 1=1` で全件取得できた。
- **証拠:**
 - `id=1` → 1件
 - `id=1 OR 1=1` → 3件
 - 実行クエリ: `SELECT id,name,price FROM items WHERE id = 1 OR 1=1`
 - 生データ: `evidence/LAB-03_sql_i.json`

のみで、書き込み系SQLは未実施（推定）。

- **修正:**
 - プレースホルダ/パラメータ化クエリを使う。
 - DBユーザーの最小権限化。
 - WAFは補助。根本はクエリの修正。
 - 入力の型検証（整数IDなら整数に変換）。
- **再確認:** `1 OR 1=1` が1件扱い、または400。エラーにSQL情報を出さない。

H-04: SSRF（内部エンドポイントへ到達）

- **重大度:** High / **CVSS:** 8.1
- **対象:** `GET /api/fetch?url=`
- **概要:** 利用者が指定したURLをサーバー側で取得する。内部エンドポイント `http://127.0.0.1:18080/internal/secret` に到達し、デモ用トークンを取得できた。
- **証拠:**
 - 応答: `DEMO-INTERNAL-TOKEN-NOT-REAL`
 - 生データ: `evidence/LAB-05_ssrf.json`
- **影響:** クラウドメタデータ、内部API、管理画面への到達。認証情報の取得（推定。本検証ではクラウドメタデータは未検証）。
- **修正:**
 - 取得先を許可リストで制限する。
 - `127.0.0.1`、`169.254.169.254`、内部ドメイン、リダイレクト先を拒否する。
 - 名前解決後のIPも検証する。必要なら専用の外向きプロキシ経由。
- **再確認:** 内部URLが400/403、外部の許可先のみ200。

H-05: 制限なしファイルアップロード

- **重大度:** High / **CVSS:** 7.5
- **対象:** `POST /upload`
- **概要:** 拡張子・Content-Type・内容・保存先の制限がない。テキスト `proof.txt` を保存し、`/uploads/proof.txt` から再取得できた。
- **証拠:**
 - アップロード: `201`
 - 再取得: `200`、内容一致
 - 証拠: `evidence/LAB-06_upload.txt`

ル/WebShellは未検証)。

- **修正:**
 - 許可する拡張子・MIME・サイズを制限する。
 - 内容を検証し、実行権限のない場所に保存する。
 - ファイル名をランダム化し、元の名前を使わない。
 - 配信時に `Content-Disposition: attachment` と `X-Content-Type-Options: nosniff`。
- **再確認:** 実行ファイルが拒否され、テキストのみ許可される。

M-01: 反射型XSS

- **重大度:** Medium / **CVSS:** 6.1
- **対象:** `GET /search?q=`
- **概要:** 検索語がHTMLエスケープされずに反射する。 `<img onerror=...>` が実行され、画面に `XSS EXECUTED` が表示された。
- **証拠:** `evidence/lab_xss_executed.png`、`evidence/LAB-04_xss.html`
- **影響:** セッション窃取、フィッシング、画面改ざん、CSRFの補助（推定。本検証ではCookie窃取は未実施）。
- **修正:**
 - コンテキストに応じた出力エスケープ。
 - CSPを設定し、インラインスクリプトを制限。
 - 入力のサニタイズだけに依存しない。
- **再確認:** ペイロードが文字列として表示され、実行されない。

M-02: ログインのレート制限・ロックアウトなし

- **重大度:** Medium / **CVSS:** 5.3
- **対象:** `POST /login`
- **概要:** 10回連続で失敗しても、429/423、遅延、CAPTCHA、ロックアウトがない。
- **証拠:** `evidence/LAB-07_rate_limit.json`
- **影響:** パスワード総当たり、Credential Stuffing、アカウント列挙（推定。負荷をかける試行は未実施）。
- **修正:**
 - IP・アカウント単位のレート制限。
 - 失敗回数に応じた遅延・ロック・CAPTCHA。
 - MFA、通知、不審ログインの検知。
- **再確認:** 一定回数で429/423、または遅延。

- 重大度: Low / CVSS: 3.1
- 対象: 全応答
- 概要: CSP、X-Content-Type-Options、Referrer-Policy、Permissions-Policy がない。
- 証拠: evidence/LAB-08_headers.json
- 影響: XSSの影響拡大、MIMEスニッフィング、リファラ漏えい（推定）。
- 修正: 各ヘッダを設定。CSPは段階的に導入。
- 再確認: ヘッダの付与を確認。

6. 確認できた管理策

- 未認証の /admin は 403。認証自体は存在する。
- ログインにはセッションIDが発行される。
- ただし、認可の判定がクライアントCookieに依存しており、bypass が可能だった。

「認証がある」と「認可が正しい」ことは別、という点が今回の最重要示唆。

7. 修正チェックリスト

優先	項目	担当	期限	状態
1	管理画面の認可をサーバー側で判定	開発	3日	
2	IDORの所有者チェック	開発	3日	
3	SQLのパラメータ化	開発	3日	
4	SSRFの許可リスト	開発	7日	
5	アップロード制限	開発	7日	
6	XSSのエスケープ/CSP	開発	7日	
7	ログインのレート制限	開発/運用	14日	
8	セキュリティヘッダ	開発	14日	
9	再確認	Habilis/パートナー	30日	

- 対象: H-01～H-05、M-01～M-02、L-01
- 方法:
 - 同じリクエストを再送し、403/400/エスケープを確認
 - 管理画面の全エンドポイントで一般ユーザー/管理者の差分を確認
 - SQLiペイロードが無効化されていることを確認
 - SSRFの内部URL・リダイレクト・名前解決後のIPを確認
 - アップロードの拒否と保存先の権限を確認
- 合格:
 - High/Mediumが再現しない
 - 新たな回帰がない
 - 残リスクを合意する

9. 品質保証と限界

品質保証

- 同一環境・同ースクリプトの連続2回で同一結果（環境非依存の再現性は未検証）
- 8所見の誤検知レビュー
- 外部通信・破壊・持ち出し・DoS・マルウェアなし
- 証拠と再現手順を保存
- 報告書のPeer Review（予定）

限界

- 本レポートはデモラボの結果であり、実在の顧客環境の安全性を示すものではない。
- テスト時点の評価であり、将来の侵害を防ぐ保証ではない。
- CVSSは参考値。実環境の影響は別途評価する。
- 独立した第三者による再現は未実施。
- ソーシャルエンジニアリング、物理、クラウドIAM、大規模APIは範囲外。

10. 免責

本報告書は、合意された範囲・時点の情報に基づく。

特定の脆弱性や侵入の成功、将来のサイバー攻撃の防止、事業継続、売上を保証するものではない。

スコープ・手法・成果物の未提供がある場合、未提供分の返金または再実施を行う。
「脆弱性が見つからなかった」「攻撃が防御された」ことは返金理由に該当しない。

付録A. テスト一覧

ID	テスト	結果
LAB-00	未認証の管理画面	403（対照）
LAB-01	role Cookie改ざん	200（bypass）
LAB-02	IDOR	他人の情報を取得
LAB-03	Boolean SQLi	全3件を取得
LAB-04	反射型XSS	DOM実行
LAB-05	SSRF	内部トークン取得
LAB-06	ファイルアップロード	保存・再取得
LAB-07	レート制限	10回401、制限なし
LAB-08	セキュリティヘッダ	4種欠如

付録B. 証拠ファイル

- evidence/LAB-00_admin_anon.html
- evidence/LAB-01_login_headers.json
- evidence/LAB-01_admin_tampered.html
- evidence/LAB-02_idor.json
- evidence/LAB-03_sqli.json
- evidence/LAB-04_xss.html
- evidence/LAB-05_ssrf.json
- evidence/LAB-06_upload.txt
- evidence/LAB-07_rate_limit.json
- evidence/LAB-08_headers.json
- evidence/lab_admin_bypass.png
- evidence/lab_xss_executed.png
- evidence/vps_checks.json
- evidence/repeatability_check.json

END OF SAMPLE

以下は、意図的に脆弱なデモラボで取得した証拠です。実在の顧客環境ではありません。

Admin console

DEMO ONLY. 管理画面に到達しました。

ID	Email	Role
1	alice@example.test	user
2	bob@example.test	user
3	admin@example.test	admin

H-01: 一般ユーザーのセッションで `role=admin` に改ざんし、管理画面に到達した状態。

Search

Results for: 

[Home](#)

M-01: 検索語の未エスケープにより、DOM上で **XSS EXECUTED** が表示された状態。

本サンプルは診断商品の品質と成果物の形式を示すためのものです。実在の企業・IP・取引口座とは関係ありません。 Habilis / 坂井 大騎 / sakai@habilis.io / <https://habilis.io/security>