# **セキュリティテスト報告書**

## **1. 概要**

### **1.1 検査対象**

* **対象アプリケーション名**: ドローン生産部品在庫管理システム
* **バージョン/リリース日**: v1.5.3 / 2024年11月1日
* **検査環境**: テストサーバ
* **検査範囲**: Webアプリケーション全体

### **1.2 検査目的**

・クライアント企業様アプリの脆弱性診断を行いセキュリティリスクを特定すること。  
・リスクに対する対策要否を確認すること。

### **1.3 検査実施概要**

* **検査ツール**: OWASP ZAP
* **実施期間**: 2024年12月14日
* **担当チーム**: インフラチーム

## **2. 検査手法**

* **検査ツール「OWASP ZAP」の設定**:
  + プロキシ設定: 127.0.0.1:8085
  + テストモード: 動的スキャン
* **対象URL/エンドポイント**:
  + https://fnb8gpdqqr.ap-northeast-1.awsapprunner.com/
* **認証の有無**:
  + 認証なし
* **その他設定**:
  + なし

## **3. 検査結果**

### **3.1 全体概要**

* **検出された脆弱性数**: 9
* **脆弱性の危険度分布**:
  + High: 0件
  + Meidum: 2件
  + Low:3件
  + Info:4件

※OWASP ZAPレポートのうち、確度(Confidence)については記載を省略する。

### **3.2 検出結果一覧**

| **No.** | **脆弱性名** | **危険度** | **検出箇所** | **修正**  **要否** | **備考** |
| --- | --- | --- | --- | --- | --- |
| 1 | Content Security Policy ヘッダの不備 | Medium | 全般 | 要検討 | - |
| 2 | X-Frame-Optionsヘッダの不備 | Medium | 全般 | 要検討 | - |
| 3 | サードパーティのJavaScriptファイルの利用 | Low | 全般 | 要検討 | - |
| 4 | HSTSヘッダの不備 | Low | 全般 | 要検討 | - |
| 5 | X-Content-Type-Optionsヘッダの不備 | Low | 全般 | 要検討 | - |
| 6 | コメントによる情報漏えい | Info | - | 対応 不要 | 誤検出の可能性あり |
| 7 | Modern Web Application | Info | - | 対応 不要 | - |
| 8 | Cache-Controlヘッダの不備 | Info | 全般 | 要検討 | - |
| 9 | User-Agent情報によるレスポンスの差異 | Info | - | 対応  不要 | 誤検出の可能性あり |

## **4. 脆弱性詳細**

### **4.1 脆弱性名:** Content Security Policy ヘッダの不備

* **危険度**:Medium
* **概要**:
  + レスポンスにCSPヘッダがない。
* **検出箇所**:
  + URL: /
* **影響**:
  + クロスサイト・スクリプティングやクリックジャッキングの被害を緩和・軽減できない可能性がある。
* **修正案**:CSPヘッダを設定する。

### **4.2 脆弱性名:** X-Frame-Optionsヘッダの不備

* **危険度**:Medium
* **概要**:
  + レスポンスにX-Frame-Optionsヘッダがない。
* **検出箇所**:
  + URL: /
* **影響**:
  + クリックジャッキングの被害を緩和・軽減できない可能性がある。
* **修正案**:X-Frame-Optionsヘッダを設定する。

### **4.3 脆弱性名:** サードパーティのJavaScriptファイルの利用

* **危険度**:Low
* **概要**:
  + サードパーティのJavaScriptファイルを利用している。
* **検出箇所**:
  + URL: /
* **影響**:
  + 安全でないJavaScriptファイルが読み込まれていると不正なプログラムを実行される可能性がある。
* **修正案**:サードパーティのJavaScriptファイルの提供元を確認する。

### **4.4 脆弱性名:** HSTSヘッダの不備

* **危険度**:Low
* **概要**:
  + レスポンスにHSTSヘッダがない。
* **検出箇所**:
  + URL: /
* **影響**:
  + ユーザーにHTTPS通信を強制できない可能性がある。
* **修正案**:HSTSヘッダを設定する。

### **4.5 脆弱性名:** X-Content-Type-Optionsヘッダの不備

* **危険度**:Low
* **概要**:
  + レスポンスにX-Content-Type-Optionsヘッダの不備がない。
* **検出箇所**:
  + URL: /
* **影響**:
  + ブラウザによるMIMEスニッフィングを抑止できない可能性があります。
* **修正案**:X-Content-Type-Optionsヘッダを設定する。

### **4.6 脆弱性名:** コメントによる情報漏えい

* **危険度**:Info
* **概要**:
  + HTMLやJavaScriptなどにコメント記載が疑われる。
* **検出箇所**:
  + URL: /
* **影響**:
  + コメントが実際に存在した場合、攻撃者に有益な情報を提供する。
* **修正案**:不要なコメントは削除。

### **4.7 脆弱性名:** Modern Web Application

* **危険度**:Info
* **概要**:
  + このアプリケーションは最新のWebアプリケーションである。
* **検出箇所**:
  + URL: /
* **影響**:
  + なし
* **修正案**:不要。

### **4.8 脆弱性名:** Cache-Controlヘッダの不備

* **危険度**:Info
* **概要**:
  + レスポンスにCache-Controlヘッダがない。
* **検出箇所**:
  + URL: /
* **影響**:
  + 対象画面が機微情報などを含む場合、クライアントや中間機器にキャッシュ情報を破棄させることができない。
* **修正案**:Cache-Controlヘッダを設定する。

### **4.9 脆弱性名:** User-Agent情報によるレスポンスの差異

* **危険度**:Info
* **概要**:
  + 予期しないUser-Agent情報を受け入れる可能性がある。
* **検出箇所**:
  + URL: /
* **影響**:
  + クライアント側で改ざんされる可能性のあるユーザエージェント情報を信頼している可能性がある。
* **修正案**:仕様通りであるかどうかの確認。

## **5. 対応方針**

### **5.1 緊急対応が必要な脆弱性**

高危険度の脆弱性を優先的に修正する

### **5.2 修正の担当チーム**

* **アプリレベルの脆弱性**: バックエンドチームへエスカレーション
* **インフラレベルの脆弱性**: インフラチームが対応

### **5.3 修正期限**

* **高危険度**: 1週間以内
* **中危険度**: 2週間以内
* **低危険度**: 次回リリースまで

## **6. まとめ**

* **総評**:
  + 検出された脆弱性は想定内であり、修正可能である。
* **次回対応予定**:
  + 修正後の再検査を実施する。

## **7. 添付資料**

* OWASP ZAPのレポート出力結果（.pdf)
* OWASP ZAPのセッションファイル(.session)