# **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**: 教育用動画コンテンツサービス
* **バージョン/リリース日**: v1.0.0 / 2025年7月1日
* **検査環境**: 開発環境
* **検査範囲**: EC2 / LP

### **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、Amazon Inspector
* **実施期間**: 2025年6月30日
* **担当チーム**: インフラチーム

## **2. 検査手法**

* EC2
  + 検査ツール:Amazon Inspector
    - Nameタグを指定
    - IAMRole: AmazonSSMManagedInstanceCore の付与
    - 評価テンプレート
      * Common Vulnerabilities and Exposures (CVE)
      * CIS Operating System Security Configuration Benchmarks
      * AWS Security Best Practices
      * Runtime Behavior Analysis
  + 対象
    - 開発環境 App用EC2
* S3
  + 検査ツール:OWASP ZAP
    - 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://xxxxx.cloudfront.net
  + 認証の有無:
    - 認証なし
  + その他設定:
    - なし

## **3. 検査結果**

### **3.1 EC2**

* **検出された脆弱性数**: 0

#### 3.1.1 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 |  |  |  |  |  |

### 3.2 S3

* **検出された脆弱性数**: 1
* **脆弱性の危険度分布**:
  + High: 0件
  + Meidum: 1件
  + Low:0件
  + Info:0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。

#### 3.2.1 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 | - |

## **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。

**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**

Amazon Inspector レポート結果(.pdf)

OWASP ZAPのレポート出力結果（.pdf)