第三者機関によるセキュリティ監査

本資料は株式会社 World Wide System が提供するサービスのセキュリティを確保するため第三者機関によるセキュリティ監査結果を記載したものです。

プロダクトブランド	SmartPR シリーズ
プロダクト名	SmartKuji
バージョン	Ver4.1.0

1.概要

２０２２年１１月１４日に、GMO サイバーセキュリティ by イエラエ株式会社にて脆弱性診断を実施いたしました。本資料にて監査結果を公開いたします。

2. 監査結果サマリー

今回の監査では６件の脆弱性が検出されました。

検出された脆弱性は、全て対策を講じた上で２０２２年１２月１２日から提供しております。また、過去設置分についてはお客様指定の日時にて改修対応をいたします。

3.監査対象について

監査対象のリクエスト名は以下の通りです。

・Web アプリケーション診断対象一覧(管理画面)

1. TOP
2. TOP＞ID/Pass を入力＞ログイン

・Web アプリケーション診断対象一覧(メールアドレス)

1. TOP
2. TOP＞キャンペーンに参加する＞メールアドレスを入力＞送信
3. TOP＞キャンペーンに参加する＞メールアドレスを入力＞送信＞キャンペーンページトップに戻る＞キャンペーン参加 URL 通知：URL 押下
4. TOP＞キャンペーンに参加する＞メールアドレスを入力＞送信＞キャンペーンページトップに戻る＞キャンペーン参加 URL 通知：URL 押下#2
5. TOP＞キャンペーンに参加する＞メールアドレスを入力＞送信＞キャンペーンページトップに戻る＞キャンペーン参加 URL 通知：URL 押下＞1 回くじがひけるよ：Start＞賞品受け取り用フォーム 再アクセス URL 通知：URL 押下
6. TOP＞キャンペーンに参加する＞メールアドレスを入力＞送信＞キャンペーンページトップに戻る＞キ

ャンペーン参加 URL 通知：URL 押下＞1 回くじがひけるよ：Start＞賞品受け取り用フォーム 再アクセス URL 通知：URL 押下＞送付先情報入力フォーム：住所自動入力

7. TOP＞キャンペーンに参加する＞メールアドレスを入力＞送信＞キャンペーンページトップに戻る＞キャンペーン参加 URL 通知：URL 押下＞1 回くじがひけるよ：Start＞賞品受け取り用フォーム 再アクセス URL 通知：URL 押下＞送付先情報入力フォーム：住所自動入力＞確認
8. TOP＞キャンペーンに参加する＞メールアドレスを入力＞送信＞キャンペーンページトップに戻る＞キャンペーン参加 URL 通知：URL 押下＞1 回くじがひけるよ：Start＞賞品受け取り用フォーム 再アクセス URL 通知：URL 押下＞送付先情報入力フォーム：住所自動入力＞確認＞戻る
9. TOP＞キャンペーンに参加する＞メールアドレスを入力＞送信＞キャンペーンページトップに戻る＞キャンペーン参加 URL 通知：URL 押下＞1 回くじがひけるよ：Start＞賞品受け取り用フォーム 再アクセス URL 通知：URL 押下＞送付先情報入力フォーム：住所自動入力＞確認＞送信
10. TOP＞キャンペーンに参加する＞メールアドレスを入力＞送信＞キャンペーンページトップに戻る＞キャンペーン参加 URL 通知：URL 押下＞1 回くじがひけるよ：Start＞賞品受け取り用フォーム 再アクセス URL 通知：URL 押下＞送付先情報入力フォーム：住所自動入力＞確認＞送信＞キャンペーンページトップに戻る＞当選通知：URL 押下

・Web アプリケーション診断対象一覧(シリアル)

1. TOP
2. TOP＞キャンペーンに参加する＞シリアルナンバーを入力＞送信
3. TOP＞キャンペーンに参加する＞シリアルナンバーを入力＞送信#2

４．検証観点について

以下の観点で監査いただきました。

検証観点	詳細
作業者によるマニュアル診断	ツール診断では検出出来ない診断項目を攻撃者の観点からすべて手動で確認します。個別では些細な脆弱性だとしても、合わさることにより大きなセキュリティリスクに繋がる可能性について監査します。
ツールによる自動診断	ツールが得意としている診断対象への網羅的な診断を行い、設定不備やセキュリティ対策漏れによる Web アプリケーションの脆弱性を監査します。

5.検出された脆弱性について

・検出された脆弱性への対応

検出された脆弱性は、改修いたしております。

・検出された脆弱性について

６件の脆弱性が検出されました。

検出された脆弱性	SQL インジェクション
リスクレベル評価	高
リスクレベル基準	・システムやその利用者にとって重要と考えられるデータや、大量の個人データの漏洩、改ざんにつながる脆弱性など

検出された脆弱性	クロスサイトスクリプティング
リスクレベル評価	中
リスクレベル基準	・情報漏洩や改ざん等につながるが、攻撃成立のために被害者自身による操作を要する受動的攻撃や、攻撃者には制御不能な前提条件を要する脆弱性 ・システムへの能動的な攻撃が可能だが、高レベルの影響に至らない脆弱性

検出された脆弱性	不用意な情報公開
リスクレベル評価	低
リスクレベル基準	・その脆弱性の単独の悪用では重大事に至らないと考えられる、軽微なシステム情報の出力など ・現実的でない前提条件を要するなど、実際の攻撃が困難な脆弱性

検出された脆弱性	不用意な情報公開
リスクレベル評価	低
リスクレベル基準	・その脆弱性の単独の悪用では重大事に至らないと考えられる、軽微なシステム情報の出力など ・現実的でない前提条件を要するなど、実際の攻撃が困難な脆弱性

検出された脆弱性	Secure 属性のないセッション管理用 Cookie
リスクレベル評価	低
リスクレベル基準	・その脆弱性の単独の悪用では重大事に至らないと考えられ

	る、軽微なシステム情報の出力など ・現実的でない前提条件を要するなど、実際の攻撃が困難な脆弱性

検出された脆弱性	キャッシュ制御の不備
リスクレベル評価	低
リスクレベル基準	・その脆弱性の単独の悪用では重大事に至らないと考えられる、軽微なシステム情報の出力など ・現実的でない前提条件を要するなど、実際の攻撃が困難な脆弱性

検出された脆弱性	X-Frame-Options ヘッダの推奨事項
リスクレベル評価	低
リスクレベル基準	・その脆弱性の単独の悪用では重大事に至らないと考えられる、軽微なシステム情報の出力など ・現実的でない前提条件を要するなど、実際の攻撃が困難な脆弱性