

sonar ATS Web アプリケーション脆弱性診断結果

1 診断概要

2025年8月1日から8月13日、及び8月25日に、株式会社RSコネクト様によるセキュリティ診断を実施しました。

本資料にて診断結果を公開します。

2 診断結果サマリ

今回の診断では、脆弱性は検出されませんでした。

3 診断対象

sonar ATS の以下の機能について診断を実施しました。

No.	ページ・機能名	診断対象の操作・遷移
1	CMS 掲示板	タイトルと本文の入力、ファイル添付を行える
2	CMS 掲示板	作成ボタンクリックでスレッドの作成ができる
3	CMS ブログ	
4	CMS プロフィール 共有 プロフィール の一覧	「プロフィールの作成」クリックで「6」の画面へ遷移
5	CMS プロフィール 共有 プロフィール の一覧	一覧内右端の「参照」クリックで「9」の画面へ遷移
6	CMS プロフィール 共有 プロフィール の編集	アンケート情報という見出し横の「編集」クリックで「7」の画面へ遷移
7	CMS プロフィール 共有 アンケート情報編集	入力後「確認ボタン」クリック
8	CMS プロフィール 共有 アンケート情報編集	確認画面から「保存ボタン」クリック
9	CMS プロフィール 共有 プロフィール 参照	
10	Connector ログイン画面	id/pw 入力してログイン
11	Connector パスワード設定画面	メールアドレス、パスワード入力後、「保存」ボタン押下で保存
12	人材リクエスト 一覧画面	リストアイテム押下で「人材リクエスト 詳細画面」に遷移

13	人材リクエスト 一覧画面	リストメニュー「:」>「編集」押下で「人材リクエスト 編集画面」に遷移
14	人材リクエスト 一覧画面	「申請」ボタン押下で「人材リクエスト 申請フォーマット選択」画面へ遷移
15	人材リクエスト 募集中一覧画面	リストアイテム押下で「人材リクエスト 詳細画面」に遷移
16	人材リクエスト 詳細画面	「鉛筆アイコン」ボタン押下で、「人材リクエスト 編集画面」に遷移
17	人材リクエスト 詳細画面	コメント欄入力、ステータス選択し、「送信」ボタン押下でコメント送信
18	人材リクエスト 詳細画面	「求人票作成」ボタン押下で、求人票作成画面に遷移
19	人材リクエスト 申請フォーマット選択画面	対象フォーマットを押下し、項目入力画面に遷移
20	人材リクエスト 新規申請画面	各項目を入力・もしくは選択し、「申請確認」ボタンを押下でリクエスト申請画面に遷移
21	人材リクエスト リクエスト申請確認画面	「修正」ボタン押下で、項目入力画面に遷移
22	人材リクエスト リクエスト申請確認画面	「申請」ボタン押下で、申請完了
23	人材リクエスト リクエスト申請確認画面 > 完了	「詳細を確認する」ボタン押下で、申請したリクエストの詳細画面へ遷移
24	人材リクエスト リクエスト申請確認画面 > 完了	「一覧へ戻る」ボタン押下で、人材リクエスト一覧画面に遷移
25	人材リクエスト 編集画面	各項目を修正・もしくは再選択、「申請確認」ボタンを押下し、編集確認画面に遷移
26	人材リクエスト 編集確認画面	「修正」ボタン押下で、編集画面に遷移
27	人材リクエスト 編集確認画面	「申請」ボタン押下で、申請完了
28	人材リクエスト 編集画面 リクエスト申請確認 完了	「詳細を確認する」ボタン押下で、申請したリクエストの詳細画面へ遷移
29	人材リクエスト 編集画面 リクエスト申請確認 完了	「一覧へ戻る」ボタン押下で、人材リクエスト一覧画面に遷移
30	求人票 一覧画面	リストアイテム押下で「求人票 詳細画面」に遷移
31	求人票 一覧画面	リストメニュー「:」>「編集」押下で「求人票 編集画面」に遷移
32	求人票 一覧画面	「申請」ボタン押下で「求人票 申請フォーマット選択」画面へ遷移
33	求人票 詳細画面	「鉛筆アイコン」ボタン押下で、「求人票 編集画面」に遷移
34	求人票 詳細画面	コメント欄入力、ステータス選択し、「送信」ボタン押下でコメント送信

35	求人票 詳細画面 > ATS 連携	「sonar ATS に連携」ボタン押下で「連携先を選択」モーダル表示
36	求人票 詳細画面 > ATS 連携 > 連携先選択	「プロジェクト No」を選択>「新規求人を作成」を選択し、「連携」ボタンを押下で送信し、ダイアログ表示
37	求人票 詳細画面 > ATS 連携解除	「連携解除」ボタン押下で「連携解除」モーダル表示
38	求人票 詳細画面 > ATS 連携解除	「解除」ボタン押下で「解除」が実行されモーダル非表示
39	求人票 新規申請画面 フォーマット選択	対象フォーマットを押下し、項目入力画面に遷移
40	求人票 新規申請画面 項目入力	各項目を入力・もしくは選択し、「申請確認」ボタンを押下で求人票申請確認画面に遷移
41	求人票 新規申請確認画面	「修正」ボタン押下で、項目入力画面に遷移
42	求人票 新規申請確認画面	「申請」ボタン押下で、申請完了
43	求人票 新規申請確認画面> 完了	「詳細を確認する」ボタン押下で、申請した求人票の詳細画面へ遷移
44	求人票 新規申請確認画面> 完了	「一覧へ戻る」ボタン押下で、求人票一覧画面に遷移
45	求人票 編集画面	各項目を修正・もしくは再選択、「申請確認」ボタンを押下し、求人票 編集確認画面に遷移
46	求人票 編集確認画面	「修正」ボタン押下で、編集画面に遷移
47	求人票 編集確認画面	「申請」ボタン押下で、申請完了
48	求人票 編集画面 申請確認 完了	「詳細を確認する」ボタン押下で、申請した求人票の詳細画面へ遷移
49	求人票 編集画面 申請確認 完了	「一覧へ戻る」ボタン押下で、求人票一覧画面に遷移
50	社内ジョブボード 社内公募一覧画面	リストアイテム押下で「社内ジョブボード 公募詳細画面」に遷移
51	社内ジョブボード 公募詳細画面	「応募」ボタン押下で、sonar ATS 対応求人へ遷移
52	人材リクエストフォーマット 一覧	「作成」押下で「人材リクエストフォーマット 新規作成」画面へ遷移
53	人材リクエストフォーマット 一覧	リストアイテム押下で「人材リクエストフォーマット 編集、詳細画面」へ遷移
54	人材リクエストフォーマット 新規作成	各項目を入力・もしくは選択し、登録ボタンを押下し、一覧画面に遷移
55	人材リクエストフォーマット 詳細・編集画面	各項目を入力・もしくは選択し、登録ボタンを押下し、一覧画面に遷移
56	求人フォーマット 一覧	「作成」押下で「求人フォーマット 新規作成」画面へ遷移
57	求人フォーマット 一覧	リストアイテム押下で「求人フォーマット 編集、詳細画面」へ遷移

58	求人フォーマット 新規作成	各項目を入力・もしくは選択し、登録ボタンを押下し、一覧画面に遷移
59	求人フォーマット 詳細・編集画面	各項目を入力・もしくは選択し、登録ボタンを押下し、一覧画面に遷移
60	ユーザーアカウント画面	「パスワード再設定」ボタン押下でパスワード設定メール送信、メールから「パスワード設定画面」へ
61	事業年度設定画面	事業年度名、開始日入力し「登録」ボタン押下で、登録
62	ユーザーアカウント一覧画面	「招待」ボタン押下で「ユーザーアカウント一覧画面 > ユーザー招待」画面遷移
63	ユーザーアカウント一覧画面 > ユーザー招待	名前、メールアドレス入力後、「招待」ボタン押下でアカウント登録され、「ユーザーアカウント一覧」画面遷移
64	ユーザーアカウント一覧画面 > 部署変更	リストアイテムチェックボックス選択でアクションメニュー表示> 「部署変更」ボタン押下で部署選択画面表示
65	ユーザーアカウント一覧画面 > 部署変更	組織選択後、「保存」ボタン押下で「ユーザーアカウント一覧」画面へ
66	ユーザーアカウント一覧画面 > ロール変更	リストアイテムチェックボックス選択でアクションメニュー表示> 「ロール変更」ボタン押下でロール選択画面表示
67	ユーザーアカウント一覧画面 > ロール変更	ロール追加後、「保存」ボタン押下で「ユーザーアカウント一覧」画面へ
68	ユーザーアカウント一覧画面 > 利用停止	リストアイテムチェックボックス選択でアクションメニュー表示> 「利用停止」ボタン押下で、利用停止され、ユーザーアカウント一覧に遷移

4 診断内容

診断項目は日本セキュリティオペレーション事業者協議会および OWASP が公表している「Web アプリケーション脆弱性診断ガイドライン」に準拠しています。

1. 目視による WEB アプリケーションの挙動確認
2. 脆弱性診断ツールによる全体的な脆弱性診断
3. フォームへの入力による挙動確認
4. アクセス制御の確認
5. セッション管理状態の確認
6. クロスサイト・スクリプティング (XSS) の脆弱性診断
7. バッファオーバーフロー
8. システムコマンドや、SQL コマンド挿入の欠陥診断
9. WEB アプリケーションのエラー出力の確認
10. 安全ではない設定管理

修正履歴

- 修正日 : 2025 年 10 月 21 日
 - 2025 年 8 月 28 日に掲載した内容に以下の内容を追加しました。
 - 「1. 診断概要」に、2025 年 8 月 1 日から 13 日に実施した旨を追加
 - 「3. 診断対象」に No.の項目を追加
 - 「3. 診断対象」に 2025 年 8 月 1 日から 13 日に実施した機能を追加。対象機能は、No.10～No.68