受入試験（指摘事項管理） - 指摘事項 #143

[脆弱性診断]権限昇格

2021/02/18 03:56 - 匿名ユーザー

ステータス:	終了	**開始日:**	2021/02/18
優先度:	通常	**期日:**	
担当者:		**進捗率:**	0%
カテゴリ:		**予定工数:**	16.00時間
機能名:	全般	**要マニュアル反映:**	いいえ
原因区分:	脆弱性診断		

説明

指摘事項

・危険度：高

・解説
ユーザに対して仕様上許可されていない操作が実行可能であることが確認されました。
データの不正な閲覧や登録更新削除が行われる可能性があります。

・対象
（1）
社員情報アップロード
https://c.ecomic-app.com/ecclub/shain
給与アップロードチェック
https://c.ecomic-app.com/ecclub/kyuyokoukai

（2）
雇用契約一括ダウンロード＜検索結果をダウンロードする＞
https://c.ecomic-app.com/ecclub/KoyouKeiyakushoIkatsuDownLoad/KoyouKeiyakushodownload/csvDownload
雇用契約一括ダウンロード＜選択項目のダウンロードする(PDF)＞
https://c.ecomic-app.com/ecclub/KoyouKeiyakushoIkatsuDownLoad/KoyouKeiyakushodownload/pdfDownload
給与明細一括ダウンロード＜選択項目をダウンロードする＞
https://c.ecomic-app.com/ecclub/kyuyoMeisaiIkatsuDownLoad/KyuyoMeisaidownload/selectPdfDownLoad
各種アップロード取込履歴画面＜CSVダウンロード＞
https://c.ecomic-app.com/ecclub/torikomirireki/ichirancsv
ドキュメント一括ダウンロード＜検索結果をダウンロードする＞
https://c.ecomic-app.com/ecclub/DokyumentoIkatsuDownLoad/Dokyumentodownload/csvDownload
ドキュメント一括ダウンロード＜選択項目をダウンロードする（PDF）＞
https://c.ecomic-app.com/ecclub/DokyumentoIkatsuDownLoad/Dokyumentodownload/pdfDownload

・確認方法
（1）
1) ログイン画面にて、一般従業員ユーザーとしてログインします。
2) ブラウザに対象URLを入力し遷移します。
3) 権限が低い一般従業員ユーザーで人事担当者・設定担当者権限が必要な該当ページへアクセス可能であることが確認できます。

（2）
1) 設定担当者権限ユーザーとしてログインします。
2) 対象画面に遷移してダウンロード操作を実行し、送信されたリクエストURL（パラメータを含む）をコピーします。
3) ログアウトし、一般従業員ユーザーとしてログインします。
4) コピーしたURLをブラウザに入力し遷移します。
5)
権限が低い一般従業員ユーザーで人事担当者・設定担当者権限が必要なファイルダウンロードが可能であることが確認できます。

・対処方法
画面上でのメニューやリンクの有無ではなく
実際の操作の実行時にユーザの権限をチェックしてください。

回答・対応内容

メニューに表示されている画面以外にURL直書きで遷移しようとした場合、権限エラー画面を遷移させるよう修正。

→Controller層でロール情報の機能IDリストをチェックし、対象画面IDが無い場合に権限エラー画面へ遷移
※Postのみが許可されているURLについては、先にそちらのチェックがなされる為、権限エラー画面に遷移するよう修正。

対応確認いたしました。

履歴

#1 - 2021/02/18 07:01 - 菊池 威之

- 原因区分 を 脆弱性診断 にセット

#2 - 2021/02/18 07:07 - 菊池 威之

- ステータス を 新規 から 対応中 に変更

#3 - 2021/02/19 04:42 - 匿名ユーザー

- 予定工数 を 16.00時間 にセット

#4 - 2021/02/20 06:43 - 匿名ユーザー

- 回答・対応内容 を更新

#5 - 2021/02/20 06:48 - 匿名ユーザー

- 回答・対応内容 を更新

#6 - 2021/02/20 09:10 - 匿名ユーザー

- ファイル 権限昇格.xlsx を追加

#7 - 2021/02/22 08:10 - 匿名ユーザー

- 回答・対応内容 を更新

#8 - 2021/02/24 01:11 - 匿名ユーザー

- 担当者 を 匿名ユーザー から 拓圭 深田 に変更

- ステータス を 対応中 から 対応済 に変更

#9 - 2021/03/01 04:19 - 拓圭 深田

- 回答・対応内容 を更新

- 担当者 を 拓圭 深田 から 菊池 威之 に変更

- ステータス を 対応済 から 承認済 に変更

- ファイル 【テスト実施後】権限昇格.xlsx を追加

#10 - 2021/03/01 08:01 - 菊池 威之

- 担当者 を 菊池 威之 から 匿名ユーザー に変更

#11 - 2021/03/18 12:39 - 菊池 威之

- ステータス を 承認済 から 終了 に変更

再診断結果OKにてクローズします。

ファイル

権限昇格.xlsx	12.5 KB	2021/02/20	匿名ユーザー
【テスト実施後】権限昇格.xlsx	13.5 KB	2021/03/01	拓圭 深田