受入試験（指摘事項管理） - 指摘事項 #144

[脆弱性診断]クロスサイトリクエストフォージェリ

2021/02/18 04:00 - 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：中

・解説
クロスサイトリクエストフォージェリ(CSRF)が検出されました。
CSRFは、攻撃者が正規のユーザに特定の処理を強制的に実行させることが可能な脆弱性です。
攻撃者が本脆弱性を悪用することで、サイトを不正利用することが可能です。

・検出箇所
<雇用契約書一括ダウンロード>-<削除する>
URL
https://c.ecomic-app.com/ecclub/KoyouKeiyakushoIkatsuDownLoad/KoyouKeiyakushodownload/doAction

<雇用契約書一括ダウンロード>-<選択項目の回答期限を変更する>
URL
https://c.ecomic-app.com/ecclub/KoyouKeiyakushoIkatsuDownLoad/KoyouKeiyakushodownload/doAction

<EC NEWS登録>-<新規登録>-<登録する>
URL
https://c.ecomic-app.com/ecclub/eco/ecnews/toukou

<EC NEWS登録>-<投稿一覧>-<編集>
URL
https://c.ecomic-app.com/ecclub/eco/ecnews/henshu

<EC NEWS登録>-<投稿一覧>-<削除>
URL
https://c.ecomic-app.com/ecclub/eco/ecnews/toukouichiran/sakujo

<コミュニケーションボード登録>~~<新規登録>~~<登録する>
URL
https://c.ecomic-app.com/ecclub/communication/toukou

<ドキュメント一括ダウンロード>-<削除する>
URL
https://c.ecomic-app.com/ecclub/DokyumentoIkatsuDownLoad/Dokyumentodownload/doAction

---2/15追加----------
<コミュニケーションボード管理>~~<投稿一覧>~~<編集>
URL
https://c.ecomic-app.com/ecclub/communication/toukou

<コミュニケーションボード管理>~~<投稿一覧>~~<削除>
URL
https://c.ecomic-app.com/ecclub/communication/toukouichiran/sakujo

<ドキュメント一括ダウンロード>~~<公開日時を変更する>~~<変更する>
URL

https://c.ecomic-app.com/ecclub/DokyumentoIkatsuDownLoad/Dokyumentodownload/doAction

<拠点管理者追加>-<登録>
URL
https://c.ecomic-app.com/ecclub/kyoten/kanrisha/tsuika/koshin

---

・確認方法
※例は、<EC NEWS登録>-<新規登録>-<登録する>を使用しております。
その他の箇所も同様の方法で確認可能です。

1) 有効なアカウントでログイン後、下記のURLにアクセスします。
---
https://c.ecomic-app.com/ecclub/eco/ecnews/toukou?_token=&subject=%e8%a8%ba%e6%96%ad&text_main=%e8%a8%ba%e6%96%ad%e6%9c%ac%e6%96%87&upload_file=
---

2) 目的の処理が正常に完了します。

・対処方法
送信されてきたリクエストが正規のユーザの意図する内容であるかを検証する処理を追加してください。
例) ワンタイムトークンの利用、Refererヘッダの検証など

回答・対応内容

例えば、EC NEWS登録の場合、画面上で登録するとPost(@csrf)で送られるが、
Getも許可してしまっている為、下記のURLのGetでの登録ができてしまう。
ecclub/eco/ecnews/toukou?_token=&subject=%e8%a8%ba%e6%96%ad&text_main=%e8%a8%ba%e6%96%ad%e6%9c%ac%e6%96%87&upload_file=

Routing(web.php)で、更新や削除処理にもかかわらずGetを許可している操作をPostのみに修正する対応を行う。

テストについては、laravelのバリデーションエラーはGetでリダイレクトされる為、その点も考慮してテストする。

対応確認いたしました。

履歴

#1 - 2021/02/18 07:03 - 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 04:41 - 匿名ユーザー

- 回答・対応内容 を更新

- 予定工数 を 16.00時間 にセット

- ファイル クロスサイトリクエストフォージェリ.xlsx を追加

#4 - 2021/02/20 09:10 - 匿名ユーザー

- ファイル を削除 (クロスサイトリクエストフォージェリ.xlsx)

- ファイル クロスサイトリクエストフォージェリ.xlsx を追加

#5 - 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

#6 - 2021/03/01 04:24 - 拓圭 深田

- 回答・対応内容 を更新

#7 - 2021/03/01 04:24 - 拓圭 深田

- 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

#8 - 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

#9 - 2021/03/08 07:50 - 匿名ユーザー

- ファイル を削除 (クロスサイトリクエストフォージェリ.xlsx)

- ファイル クロスサイトリクエストフォージェリ.xlsx を追加

#10 - 2021/03/18 12:40 - 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

クロスサイトリクエストフォージェリ.xlsx	12.2 KB	2021/03/08	匿名ユーザー