

受入試験（指摘事項管理） - 指摘事項 #147

[脆弱性診断]データの不正閲覧

2021/02/22 03:39 - 匿名ユーザー

ステータス:	終了	開始日:	2021/02/22
優先度:	通常	期日:	
担当者:		進捗率:	0%
カテゴリ:		予定工数:	8.00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
アカウントを有している攻撃者が、別権限のデータを不正に閲覧できる可能性があります。
原因は、データに対するアクセス制限が実装されていないためです。
事前にID等の情報を入手する必要がある場合もありますが、推測又は何らかの方法で入手することは可能です。

・検出箇所
(1)
<給与明細書照会>-<給与明細書>
URL
<https://c.economic-app.com/ecclub/kyuyoMeisaiSho>

(2)
<雇用契約書照会>-<PDF>
<https://c.economic-app.com/ecclub/koyoukeiyakusho/handleformall>

<ドキュメント照会>-<PDF>
<https://c.economic-app.com/ecclub/dokumento/handleformall>

・確認方法
(1)
1) 一般権限ユーザーでログインし、自身の給与明細書を閲覧します。
2) 送信されたHTTPリクエストのパラメータ「kohonrenban」および「meisaishoshubetsu」を確認します。
3) 別の一般権限ユーザーでログインします。
4) 自身の給与明細書を閲覧する際に送信されるHTTPリクエストをプロキシツール等でインターセプトします。
5)
下記のようにパラメータ「kohonrenban」および「meisaishoshubetsu」を2)で確認した値に置き換えて送信すると、本来閲覧できない別ユーザーの明細書が閲覧できます。

URL

<https://c.economic-app.com/ecclub/kyuyoMeisaiSho>

HTTPリクエスト

POST /ecclub/kyuyoMeisaiSho HTTP/1.1
Host: c.economic-app.com
(省略)

_token=DS8N49PorZqAZ0rK9KWXh45dHEi1VrMF8ZpzE38t&kohonrenban=<別ユーザーで確認した値>&meisaishubetsu=<別ユーザーで確認した値>

(2)
上記(1)と同様の方法で、パラメータ「currentKey」を置き換えて送信すると、本来閲覧できない別ユーザーの雇用契約書また

はドキュメントを閲覧できます。

URL

<https://c.economic-app.com/ecclub/koyoukeiyakusho/handleformall>

HTTPリクエスト

POST /ecclub/koyoukeiyakusho/handleformall HTTP/1.1

Host: c.economic-app.com

(省略)

repeatToken=1613700922&actionFlag=1¤tKey=<別ユーザーで確認した値>¤tDownloadUrl=https%3A%2F%2Fc.economic-app.com%2Fecclub%2Fkoyoukeiyakusho%2Fmydownload%2F1000_10453_7_000000000013&oldUpdateTime=2021-02-15+11%3A25%3A42.698926&_token=qPbpdnWTt3wNW8IAJXu19jswr14Qgc0n4oXz6Bt9¤tFudoiriyu=

・対処方法
アクセス制限処理を実装してください。

回答・対応内容

ログインユーザーと閲覧しようとしているデータの
「会社コード」と「社員コード」が一致しているか判定し、
一致しない場合、権限エラー画面へ遷移させる。

対応確認いたしました。

履歴

#1 - 2021/02/22 03:39 - 匿名ユーザー

- ステータスを 新規 から 対応中 に変更

#2 - 2021/02/22 08:10 - 匿名ユーザー

- 回答・対応内容を更新

- ファイル データの不正閲覧.xlsx を追加

#3 - 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

#4 - 2021/02/24 08:54 - 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】 データの不正閲覧.xlsx を追加

#5 - 2021/02/25 22:53 - 拓圭 深田

- 回答・対応内容を更新

- 担当者を 菊池 威之 から 拓圭 深田 に変更

- ステータスを 承認済 から 対応済 に変更

#6 - 2021/03/01 04:20 - 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

#7 - 2021/03/01 08:00 - 菊池 威之

- 担当者を 菊池 威之 から 匿名ユーザー に変更

#8 - 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

データの不正閲覧.xlsx	10.2 KB	2021/02/22	匿名ユーザー
【テスト実施後】データの不正閲覧.xlsx	10 KB	2021/02/24	拓圭 深田