

受入試験（指摘事項管理） - 指摘事項 #164

[脆弱性診断] リファラーヘッダのオープンリダイレクト

2021/03/04 08:06 - 匿名ユーザー

ステータス:	終了	開始日:	2021/03/04
優先度:	通常	期日:	
担当者:		進捗率:	100%
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			
低			
解説			
リダイレクト先にリファラーヘッダの値が使用されていることが確認されました。リファラーヘッダの値を改ざんすることにより、被害者を任意のURL へリダイレクトさせることが可能です。			
検出箇所 URL			
https://c.ecomic-app.com/ecclub/eco/ecnews/toukou			
https://c.ecomic-app.com/ecclub/kyuyokokaibidetail			
https://c.ecomic-app.com/ecclub/kyuyokokaibidetail/update			
https://c.ecomic-app.com/ecclub/KoyouKeiyakusho/katsuDownLoad/KoyouKeiyakushodownload/doAction			
https://c.ecomic-app.com/ecclub/koyouKeiyakusyoTenpuretoUpload/update			
https://c.ecomic-app.com/ecclub/koyouKeiyakusyoTenpuretoUpload/upload			
https://c.ecomic-app.com/ecclub/koyoukeiyakusho/handleformall			
https://c.ecomic-app.com/ecclub/kyoten/kanrisha/tsuika/koshin			
回答・対応内容			
検出箇所 URLで、referrerを送信しないよう修正する。			
Viewで下記のmetaタグを設定する。			
<meta name="referrer" content="never">			
→ 対応後の確認結果を添付			

対応確認いたしました。			

履歴

#1 - 2021/03/04 08:27 - 匿名ユーザー

- 指摘事項 を更新

#2 - 2021/03/04 08:30 - 匿名ユーザー

- 指摘事項 を更新

#3 - 2021/03/04 12:06 - 匿名ユーザー

- 予定工数 を 8.00時間 にセット

#4 - 2021/03/05 02:20 - 菊池 威之

- ステータス を 新規 から 対応中 に変更

#5 - 2021/03/05 08:24 - 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

- 進捗率 を 0 から 100 に変更

- ステータス を 対応中 から 対応済 に変更

#6 - 2021/03/08 02:36 - 匿名ユーザー

- 回答・対応内容 を更新

- ファイル 対応後確認_指摘事項 #164 [脆弱性診断]リファラーヘッダのオープンリダイレクト.xlsx を追加

#7 - 2021/03/08 10:16 - 匿名ユーザー

- ファイル を削除 (対応後確認_指摘事項 #164 [脆弱性診断]リファラーヘッダのオープンリダイレクト.xlsx)

- ファイル 対応後確認_指摘事項 #164 [脆弱性診断]リファラーヘッダのオープンリダイレクト.xlsx を追加

#8 - 2021/03/09 01:42 - 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

#9 - 2021/03/10 03:36 - 菊池 威之

- 担当者 を 菊池 威之 から 匿名ユーザー に変更

#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

対応後確認_指摘事項 #164 [脆弱性診断]リファラーヘッダのオープンリダイレクト.xlsx2021/03/08

匿名ユーザー