

受入試験（指摘事項管理） - 指摘事項 #166

[脆弱性診断]Cookie へのセキュリティ属性の未設定

2021/03/04 08:20 - 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:	1.00時間
機能名:	全般	要マニュアル反映:	はい
原因区分:	脆弱性診断		

説明

指摘事項

危険度

低

解説

HttpOnly 属性およびSecure 属性が設定されていないCookie 変数が検出されました。HttpOnly 属性が設定されている場合、JavaScript によるCookie 操作が禁止されます。これにより、第三者によって悪意のあるJavaScript が挿入された場合にもCookie 値の改ざんや漏えいを防ぐことが可能です。Secure 属性が設定されている場合、非暗号化通信<http://>ではCookie 値が送信されず暗号化通信<https://>でのみCookie 値が送信されるため、通信を盗聴する第三者へのCookie 値の漏えいを防ぐことが可能です。

検出箇所
・ HttpOnly 属性
ホスト
c.economic-app.com
Cookie 変数
XSRF-TOKEN
・ Secure 属性
ホスト
c.economic-app.com
Cookie 変数
XSRF-TOKEN
ec_club_session

回答・対応内容

Apacheのhttpd.confに下記を設定する。

Header edit Set-Cookie ^(.*)\$ \$1;HttpOnly;Secure

→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 08:29 - 匿名ユーザー

- 指摘事項 を更新

#2 - 2021/03/04 08:29 - 匿名ユーザー

- 指摘事項 を更新

#3 - 2021/03/04 08:31 - 匿名ユーザー

- 指摘事項 を更新

#4 - 2021/03/04 12:07 - 匿名ユーザー

- 予定工数 を 1.00時間 にセット

#5 - 2021/03/05 03:48 - 菊池 威之

- ステータス を 新規 から 対応中 に変更

#6 - 2021/03/05 08:25 - 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

- 要マニュアル反映 を いいえ から はい 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

#7 - 2021/03/08 02:01 - 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 #166 [脆弱性診断]Cookie へのセキュリティ属性の未設定.xlsx を追加

#8 - 2021/03/08 02:14 - 匿名ユーザー

- ファイル を削除 (対応後確認_指摘事項 #166 [脆弱性診断]Cookie へのセキュリティ属性の未設定.xlsx)

- ファイル 対応後確認_指摘事項 #166 [脆弱性診断]Cookie へのセキュリティ属性の未設定.xlsx を追加

#9 - 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 #166 [脆弱性診断]Cookie へのセキュリティ属性の未設定.xlsx)

- ファイル 対応後確認_指摘事項 #166 [脆弱性診断]Cookie へのセキュリティ属性の未設定.xlsx を追加

#10 - 2021/03/09 01:43 - 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

#11 - 2021/03/10 03:37 - 菊池 威之

- 担当者を 菊池 威之 から 匿名ユーザー に変更

#12 - 2021/03/18 12:41 - 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 #166 [脆弱性診断]Cookie へのセキュリティ属性の未設定.xlsx 2021/03/08

匿名ユーザー