[脆弱性診断]設定推奨ヘッダの未設定

2021/03/04 08:17 - 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:	2.00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

Strict-Transport-Security、X-Content-Type-Options、X-Frame-Options、Cache-Control の各ヘッダが適切に設定されていないことを確認しました。

・ Strict-Transport-Security

ブラウザに暗号化通信(HTTPS)を用いて通信を行うよう指示するレスポンスヘッダです。同ヘッダが有効になっている場合、ブラウザ内部で非暗号(<http://~>)を暗号化通信(<https://~>)に変換して送信するため、ネットワーク上に平文の通信内容を送信されることがなくなります。ただし、初回アクセス時に非暗号(<http://~>)でアクセスした場合、ヘッダ設定前であるため、通信は保護されないことに注意してください。

・ X-Content-Type-Options

Internet Explorer(IE) 8 以降に対して、HTTP レスポンスボディからのコンテンツタイプ推測の禁止を指示するレスポンスヘッダです。これにより、IE におけるコンテンツタイプ推測によるクロスサイトスクリプティング(XSS)攻撃を防ぐことが可能です。同ヘッダはIE 以外のブラウザでも実装されており、スクリプトやスタイルをインポートする際のコンテンツタイプ推測を制御するために利用されます。レスポンスがJSON 形式データの場合、同ヘッダはレスポンスデータを不正に奪取するJSONP インジェクション攻撃に対して有効です。

・ X-Frame-Options

FRAME 又はIFRAME タグなどによるフレームの中でのページ読み込み動作を制御するレスポンスヘッダです。同ヘッダが設定されていないレスポンスは、無制限にページ読み込みを許可しています。攻撃者は、制限のないページ読み込みを悪用し、クリックジャック攻撃()を仕掛けてくるおそれがあります。
クリックジャック攻撃
 攻撃者は、スタイルシートを駆使しフレーム読み込みしたページ(本来のページ)を覆い隠す擬似ページを作成します。被害者が騙されてこの擬似ページの処理を完了させるだけで、本来のページの処理も被害者の気づかないうちに完了させる攻撃です。

・ Cache-Control

ブラウザやプロキシ等のキャッシュ動作を制御するレスポンスヘッダです。
同ヘッダにno-store ディレクティブが設定されていない場合、プロキシ等にてレスポンスをキャッシュされ、再利用される可能性があります。
機密情報が含まれている場合は情報の漏洩につながる可能性があります。

検出箇所

・ Strict-Transport-Security

ホスト
c.ecomic-app.com

・ X-Content-Type-Options

ホスト
c.ecomic-app.com

・ X-Frame-Options

ホスト
c.ecomic-app.com

・ Cache-Control

ホスト
c.ecomic-app.com

回答・対応内容

Apacheのhttpd.confに下記を設定する。

・ Strict-Transport-Security

```
---  
Header always set Strict-Transport-Security "max-age=63072000"  
---
```

・ X-Content-Type-Options

```
---  
Header always append X-Content-Type-Options "nosniff"  
---
```

・ X-Frame-Options

```
---  
Header always append X-FRAME-OPTIONS "DENY"  
---
```

・ Cache-Control

```
---  
FileETag None  
RequestHeader unset If-Modified-Since  
Header set Cache-Control no-store  
---
```

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 08:25 - 匿名ユーザー

- 指摘事項を更新

#2 - 2021/03/04 08:25 - 匿名ユーザー

- 指摘事項を更新

#3 - 2021/03/04 08:28 - 匿名ユーザー

- 指摘事項を更新

#4 - 2021/03/04 08:30 - 匿名ユーザー

- 指摘事項を更新

#5 - 2021/03/04 08:30 - 匿名ユーザー

- 指摘事項を更新

#6 - 2021/03/04 12:07 - 匿名ユーザー

- 予定工数を2.00時間にセット

#7 - 2021/03/05 02:21 - 菊池 威之

- ステータスを新規から対応中に変更

#8 - 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

- 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

#9 - 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#165 [脆弱性診断]設定推奨ヘッダの未設定.xlsx を追加

#10 - 2021/03/08 10:15 - 匿名ユーザー

- ファイルを削除(対応後確認_指摘事項#165 [脆弱性診断]設定推奨ヘッダの未設定.xlsx)

- ファイル 対応後確認_指摘事項#165 [脆弱性診断]設定推奨ヘッダの未設定.xlsx を追加

#11 - 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

#12 - 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

#13 - 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 #165 [脆弱性診断]設定推奨ヘッダの未設定.xlsx 744 KB

2021/03/08

匿名ユーザー