セキュリティを強化する7つの便利なHTTPヘッダ

Nobuhiro Makita (牧 田 延 大), 2015-31-08

Webアプリケーションの開発・展開を行っている人々にとって、セキュリティ確保は大きな関心事の1つだといえます。そのためのベストプラクティスやフレームワーク、ガイドラインを提供しているのがOWASP（Open Web Application Security Project）です。OWASPのWikiサイト（OWASP.org）には、Webアプリケーションのセキュリティ確保のための様々な情報がありますが、それらの中でも即効性の高いのが「便利なHTTPヘッダのリスト（List of useful HTTP headers）」だといえるでしょう。

このページには、アプリケーションのHTTPレスポンスに追加することで、事実上無料でセキュリティを強化できるHTTPヘッダが7種類掲載されています。

これらの中でまず活用したいのが、以下の2つのHTTPヘッダです。

X-XSS-Protection

最近のWebブラウザには、クロスサイトスクリプティング（XSS）に対するフィルタ機能が装備されています。「X-XSS-Protection」はこのフィルタ機能を強制的に有効にするというものです。通常であればXSSフィルタはデフォルトで有効に設定されているはずですが、ユーザがこの設定を無効にした場合には、このHTTPヘッダがXSSの防止に役立ちます。

X-Content-Type-Options

Webブラウザは本来、サーバから送られてきたHTTPレスポンスに記述されている「Content-Type」に基づいて、HTTPレスポンスをどのように処理するのかを決定します。　例えば「Content-Type:text/plain」であれば、Webブラウザはこれをテキストとして扱い、レスポンスの中にスクリプト記述があってもスクリプトとしては実行しません。しかしWebブラウザの中には、HTTPレスポンス全体を検査（sniffing）してコンテンツ タイプを判断し、「Content-Type」を無視した動作を行うものも存在します。このような実装はWebアプリケーション開発者の意図しない動作を引き起こし、セキュリティ上の問題につながると指摘されてきました。このsniffingを防止するのが「X-Content-Type-Options」です。「X-Content-Type-Options : nosniff」とすることでsniffingをやめさせ、「Content-Type」に合致しない動作を回避できます。

また以下のヘッダもセキュリティ強化に役立ちますが、実際に利用した際に問題が発生しないかどうか、慎重に検討する必要があります。

Public-Key-Pins

Webブラウザに、特定の暗号鍵と特定のWebサーバとの紐付（pinning）を行わせます。これによって偽造証明書を検出しやすくなるため、偽造証明書による中間者攻撃の回避に役立ちます。

Strict-Transport-Security

Webブラウザに対し、現在接続しているドメインへの次回以降のアクセスにおいて、HTTPSの使用を強制します。これも中間者攻撃の回避に役立ちます。

X-Frame-Options / Frame-Options

またはの内部にページを表示しないように指定できます。これによってクリックジャッキングを防止できるようになります。クリックジャッキングとは、一見無害なページの上に＜iframe＞等の透過レイヤーによって悪意のあるページを「見えないように表示」させ、ユーザが意図していないボタンクリック等を引き起こすという攻撃です。ただしこのHTTPオプションによって＜frame＞＜iframe＞の機能が制限されるため、これらの機能を活用しているアプリケーションは正常に動作しない可能性があります。

Content-Security-Policy / X-Content-Security-Policy / X-Webkit-CSP

ロード可能なスクリプトを制限する、インライン記述のスクリプトの実行を禁止する、等のポリシーを設定し、それをWebブラウザに強制させます。XSSを含む幅広い攻撃の防止に役立ちます。

Content-Security-Policy-Report-Only

1つ上のCSPと同様ですが、ポリシーを強制せず、ポリシー違反が起きた時のレポーティングのみを行います。

HTTPヘッダをWebアプリケーションに自動追加する方法

これらのHTTPヘッダを全てのWebアプリケーションに追加するのは大変な作業ですが、F5が2015年5月に発表した「F5 LineRate」を利用すれば簡単になります。F5 LineRateは安価なソフトウェア型ロードバランサであり、プロキシとして機能するバーチャルサーバにスクリプトを追加することで、様々な機能を実装できます。

例えば上記ヘッダのうち、「X-Frame-Options」「X-XSS-Protection」「X-Content-Type-Options」を自動的に追加するスクリプトは、以下のように記述できます。

```
 "use strict";

var vsm = require("lrs/virtualServerModule"),

   virtualServerName = "myVirtualServer";

vsm.on("exist", virtualServerName, function(vs) {
   vs.on("request", insertUsefulHeaders);
 });

function insertUsefulHeaders(servReq, servResp, cliReq) {
   cliReq.on("response", function(cliResp) {
      cliResp.bindHeaders(servResp);
      servResp.setHeader("X-Frame-Options", "deny");
      servResp.setHeader("X-XSS-Protection", "1; mode=block");
      servResp.setHeader("X-Content-Type-Options: nosniff");
      cliResp.fastPipe(servResp);
   });
   servReq.bindHeaders(cliReq);
   servReq.fastPipe(cliReq);
 }
```

スクリプトの行数はわずか20行。追加されるヘッダ記述の容量も100バイト程度しかありません。これによってアプリケーションのセキュリティは、大幅に強化されるはずです。

なお、F5 LineRateのStarter Editionは、無料でダウンロードして試すことができます。ぜひ無料ライセンスを取得し、その威力を体感してください。

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com