Apache'de Http Güvenlik Başlıklarını Ekleme

(+) Bu yazı birebir denenmiştir ve başarıyla uygulanmıştır.

Belli başlı http güvenlik başlıkları vardır. Bunlar arasında

```
Content-Security-Policy          // Yeni tarayıcılar için XSS önleyici header
X-XSS-Protection                 // Eski tarayıcılar için XSS önleyici header
X-Frame-Options                  // Clickjacking önleyici header
X-Content-Type-Options           // Sunucudan gelen dosyayı belirtilen uzantıyla
                                 // çalıştırma kısıtı
Referrer-Policy                  // Referer request header'ını denetim altına
                                 // alarak Open redirect sonucu phising'i önler,
                                 // ayrıca kaynak siteden gelen parametrelerin
                                 // aktarımı sonucu kullanıcının gizliliğini ihlal
                                 // etmeyi engeller.
Set-cookie                       // Ortaya çıkabilecek olası zafiyetlere karşı
                                 // (örn; xss'e karşı) çerez güvenliğini sağlar
                                 // ve çerezin üçüncü parti sunuculara gidişini
                                 // önler.
Strict-Transport-Security        // Hem http hem de https kullanan web uygula-
                                 // maları için sslstrip saldırılarını önler. Erişim
                                 // http ise http, https ise https üzerinden akar.
                                 // Https ken http üzerinden akmaz. Engellenir.
```

gibi header'lar mevcuttur. Bu http güvenlik başlıklarının http response'da yer alabilmesi için önce bir apache modülü olan mod_headers'ın enable edilmesi gerekmektedir.

```
> sudo a2enmod headers
> sudo service apache2 restart
```

Ardından apache'nin konfigurasyon dosyasına aşağıdaki satırlar eklenmelidir.

```
> sudo gedit /etc/apache2/apache2.conf
```

Eklenecek Satırlar:

```
Header add Content-Security-Policy "style-src * 'unsafe-inline'; script-src * 'unsafe-inline' 'unsafe-eval'; img-src *; connect-src: *; frame-src: *; object-src: *"
Header set X-XSS-Protection "1; mode=block"
Header set X-Frame-Options "SAMEORIGIN"
Header set X-Content-Type-Options "nosniff"
Header set Referrer-Policy "no-referrer"
Header edit Set-Cookie ^(.*)$ "$1; HttpOnly; Secure; SameSite=strict"  // Mevcut cookie'ye bayrakları ilave eder.
Header set Strict-Transport-Security "max-age=31536000; includeSubdomains; preload"
```

Böylece http response paketlerinde yukarıdaki header'lar yer alacaktır ve istemci taraflı güvenlik sağlanmış olacaktır.

Uygulama

Ubuntu 14.04 ana makinasındaki localhost'a telnet yapalım ve varsayılan header'ları bir görüntüleyelim.

> telnet localhost 80

HEAD / HTTP/1.0

HTTP/1.1 200 OK
Date: Wed, 09 Aug 2017 06:53:19 GMT
Server: Apache/2.4.7 (Ubuntu)
Connection: close
Content-Type: text/html;charset=UTF-8
Connection closed by foreign host.

Şimdi sistemimizdeki apache'yi yapılandıralım ve http güvenlik başlıklarını ekleyelim.

> sudo gedit /etc/apache2/apache2.conf

Eklenecek Satırlar:

Header add Content-Security-Policy "style-src * 'unsafe-inline'; script-src * 'unsafe-inline' 'unsafe-eval'; img-src *; connect-src: *; frame-src: *; object-src: *"
Header set X-XSS-Protection "1; mode=block"
Header set X-Frame-Options "SAMEORIGIN"
Header set X-Content-Type-Options "nosniff"
Header set Referrer-Policy "no-referrer"
Header edit Set-Cookie ^(.*)$ "$1; HttpOnly; Secure; SameSite=strict"
Header set Strict-Transport-Security "max-age=31536000; includeSubdomains; preload"

Ardından dosyayı kaydedip apache'yi restart'layalım.

> service apache2 restart

Böylece localhost'a telnet yaptığımızda dönen http response'da http güvenlik başlıkları da gelecektir.

> telnet localhost 80

HEAD / HTTP/1.0
HTTP/1.1 200 OK
Date: Mon, 14 Aug 2017 12:37:07 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Content-Type-Options: nosniff
Header add Content-Security-Policy "style-src * 'unsafe-inline'; script-src * 'unsafe-inline' 'unsafe-eval'; img-src *; connect-src: *; frame-src: *; object-src: *"
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Referrer-Policy: no-referrer
örn; Set-Cookie: MoodleSession=nk7qifj0q9i7; HttpOnly; Secure; SameSite=strict
Strict-Transport-Security: max-age=31536000; includeSubdomains; preload
Connection: close
Content-Type: text/html;charset=UTF-8

Connection closed by foreign host.

Not: Localhost'ta çerez olmadığından Set-Cookie header'ı görünmeyecektir. Fakat bu header pentest yaptığım egitim.sge.gov.tr'ye eklendiğinde yukarıdaki şekilde görünecektir. Yani mevcut cookie'ye HttpOnly, Secure ve SameSite bayrakları eklenecektir.

Uyarı

Eğer uygulama 404 gibi hata mesajları döndüğünde de güvenlik başlıkları http response'larda yer alsın istiyorsan apache2.conf dosyasına eklediğin satırlara aşağıdaki gibi always keyword'ü eklemelisin.

> sudo gedit /etc/apache2/apache2.conf

Eklenecek Satırlar:

Header **always** add Content-Security-Policy "style-src * 'unsafe-inline'; script-src * 'unsafe-inline' 'unsafe-eval'; img-src * data: 'unsafe-inline'"
Header **always** set X-XSS-Protection "1; mode=block"
Header **always** set X-Frame-Options "SAMEORIGIN"
Header **always** set X-Content-Type-Options "nosniff"
Header **always** set Referrer-Policy "no-referrer"
Header **always** set Strict-Transport-Security "max-age=31536000; includeSubdomains; preload"

[UYARI]
Egitim.sge.gov.tr'ye yaptığım testte Set-Cookie başlığına always 'i eklediğimde ve telnet
ile egitim sge'ye HEAD talebi yaptığımda gelen yanıtta HttpOnly, Secure ve SameSite
bayrakların yer almadığı görülmüştür. Always'i kaldırdığımda ise bayrakların geldiği
görülmüştür. O nedenle always'i Set-Cookie'de kullanma.
Header **always** set Set-Cookie ^(.*)$ "$1; HttpOnly; Secure; SameSite=strict"

Böylece hata mesajı dönen http response'larda da güvenlik başlıkları gelecektir.

Not: Konfigasyon dosyasında always olmadığında telnet ile HEAD / HTTP/1.0 talebi sonrası http güvenlik başlıkları gelmişken HEAD / HTTP/1.**1** talebi sonrası hata döndüğünden http talepleri gelmemiştir. Konfigurasyon dosyasına always keyword'leri eklendiğinde ise telnet ile hem HEAD / HTTP/1.0 talebi yaptığımızda hem de HEAD / HTTP/1.1 talebi yaptğımızda http güvenlik başlıkları gelmiştir.

Yararlanılan Kaynak

https://stackoverflow.com/questions/16385541/content-security-policy-invalid-command

https://www.keycdn.com/blog/http-security-headers/

https://stackoverflow.com/questions/39502968/apache-difference-between-header-always-set-and-header-set

https://serverfault.com/questions/880894/how-can-i-add-in-apache-referrer-policy-header

https://geekflare.com/httponly-secure-cookie-apache/

https://blog.appcanary.com/2017/http-security-headers.html#hsts

https://zaclee.net/apache/errors-apache/invalid-command-header

https://serverfault.com/questions/524966/how-do-i-get-apache2-to-parse-without-error-header-directives-in-a-htaccess

https://www.maketecheasier.com/securing-apache-ubuntu-2/