HTTP Strict Transport Security (HSTS) Header

a. SSLStrip Saldırısı Nedir?

SSLStrip ya da diğer adıyla HTTPS-to-HTTP-Downgrading kullanıcıların web uygulamasını https üzerinden kullanması gerekirken http üzerinden kullanmasına sebep olan bir saldırı türüdür. Saldırı kabaca lokal ağdaki bir kullanıcı ile web sunucu arasına lokal ağdaki saldırganın MITM yaparak girmesiyle gerçekleşir. Normalde kullanıcılar bir websitesine bağlanmak istediklerinde genellikle adres çubuğuna web sitesinin adresini https ön ekini eklemeden girerler. Bunun sonucunda aradaki adam kullanıcının bağlantı talebini alır, https yapar ve sunucuya öyle gönderir. Fakat bu arada saldırgan kullanıcının paketini şifresiz aldığından içindeki bilgileri okuyabilir. Saldırgan aldığı bağlantı paketini sunucuya https yaparak gönderdikten sonra sunucu https olarak yanıtı saldırgana gönderir. Saldırgan gelen https yanıtını http yaparak kullanıcıya gönderir ve böylece kullanıcı halen http üzerinden web uygulamasını kullanır durumda olur. Nihayetinde saldırgan kullanıcıdan gelen her http paketini okur, web sunucusu ise saldırganla arasında olan https trafiği dolayısıyla bir problem görmez ve bunun sonucunda saldırgan kullanıcıdan gelen her http paketini okuyarak kullanıcı adı & şifre, banka kart numarası & son kullanım tarihi & CVE kodu ve TC Kimlik numarası gibi birçok kritik bilgilere sahip olmuş olur.

Bu saldırının gerçekleşmesini önlemek için web sunucusunu sadece HTTPS kullanacak şekilde yapılandırmak yetmemektedir. Çünkü zaten iletişim önceki senaryoda bahsedildiği gibi lokal ağda aradaki adam olan saldırgan ve sunucu arasında HTTPS üzerinden gerçekleşmektedir. Burada kullanıcıyı HTTPS-to-HTTP-Downgrading saldırısından korumak için kullanıcı tarayıcısını http olarak adres çubuğuna girilen web uygulama adresini https olarak düzeltmeye ve o şekilde bağlantı talebinde bulunmaya zorlamak gerekir. Böylelikle lokal ağda kullanıcı ve sunucu arasına giren saldırgan kullanıcıdan gelen https bağlantı talebini şifreli olarak göreceğinden kullanıcı verilerini elde edemeyecektir.

SSLStrip (HTTPS-to-HTTP-Downgrading) saldırıları hem HTTP ve HTTPS'i beraber kullanan web sitelerini hem de sadece HTTPS kullanan web sitelerini etkileyen bir saldırı türüdür.

> Not:
> "Sadece http kullanan" web siteleri bu saldırının kapsamı dışındadır. Çünkü sadece http kullanan web sitelerinde kullanıcı paketleri zaten şifresiz olarak okunabilmektedir.

Çünkü bu saldırı türü sunucunun davranışına göre (http ve https'i beraber kullanmasına ya da yalnızca https kullanmasına göre) değişen bir saldırı türü değildir. Bu saldırı türü istemcinin davranışına göre değişen bir saldırı türüdür. Eğer istemci HTTPS yerine HTTP üzerinden bağlantı talebinde bulunursa sunucu ister sadece HTTPS kullansın ister HTTP ve HTTPS'i beraber kullansın aradaki saldırgan aldığı paketi https yaparak göndereceğinden sunucu tarafında fark eden bir şey olmayacaktır ve saldırgan kullanıcıdan paketleri http olarak alacağından saldırısını gerçekleştirebilecektir. Bu nedenle istemciye HTTP üzerinden bağlanmak yerine HTTPS üzerinden bağlan direktifi verilmesi gerekmektedir.

b. HTTP Strict Transport Security Başlığı Nedir?

HTTP Strict Transport Security, yani kısaca HSTS kullanıcıların tarayıcı adres çubuğuna http ile girdikleri url'yi https yapan direktifi veren bir response header'ıdır. Böylece kullanıcı istemci tarafında https'e zorlanarak aradaki saldırganın kullanıcı paketlerini şifresiz görüntülemesinin önüne geçilir. HSTS ile SSLStrip saldırılarına karşı korunma akış diyagramı aşağıdaki gibidir

1. İstemci sunucuya "http" bağlantı talebinde bulunur.
2. Sunucu HTTPS'e yönlendirme yapan 302 uyarı nolu yanıtı (HSTS başlığıyla beraber) istemciye gönderir.
3. İstemci HSTS başlığı sayesinde artık sunucu ile sadece HTTPS üzerinden bağlantı kurar.
4. Bağlantı biter.

İlk http talebinde sadece siteye bağlanma isteği yapıldığından kullanıcıya dair bir bilgi yer almaz. Ardından iletişim https üzerinden gerçekleşeceğinden kullanıcıya dair bir bilgi saldırgan tarafından elde edilemez. Dolayısıyla bu süreç boyunca kullanıcının hiçbir bilgisi saldırgan tarafından elde edilemez.

c. SSLStrip Zafiyetinden Nasıl Korunulur?

SSLStrip zafiyetinden korunmak için HSTS response header'ının kullanılması gerekir. HSTS yanıt başlığının syntax'ı şu şekildedir:

Strict-Transport-Security: max-age=<expire-time>; includeSubDomains; preload

max-age	: HSTS direktifinin uygulandığı web sitelerinin tarayıcı cache'in tutulma süresini belirler.
includeSubDomains	: HSTS direktifinin subdomain'lerde de işlemesini sağlar.
preload	: Tarayıcılardaki öntanımlı https siteleri listesine dahil edilmeyi ister. Tarayıcılardaki öntanımlı https siteleri listesi ile tarayıcıdan tanımlı https sitelerine bağlanılmaya çalışıldığında direk https üzerinden bağlantı kurulması sağlanır. Chrome, Firefox, Opera, Safari, IE 11 ve Edge tarayıcıları Chrome'un default listesini temel alırlar.

Strict Transport Security başlığında

max age	=> must be specified (belirtilmek zorundadır)
includeSubDomains	=> must be specified (belirtilmek zorundadır)
preload	=> must be specified (belirtilmek zorundadır)

HSTS header'ını http respsonse header'larına eklemek için

Not: Apache HSTS header'ını uygulamalı olarak eklemek için bkz. Ubuntu Masaüstü / Paketleme için Gözden Geçirilecekler / Sıkılaştırmalar / Apache'de Http Güvenlik Başlıklarını Ekleme.docx

```
# Apache sunucularda apache2.conf dosyasına aşağıdaki satır eklenir.
Header always set Strict-Transport-Security "max-age=31536000; includeSubdomains; preload"

# Nginx sunucularda konfigurasyon dosyasına aşağıdaki satır eklenir.
add_header Strict-Transport-Security "max-age=31536000; includeSubdomains; preload;";
```

IIS sunucularda aşağıdaki adımlar takip edilmelidir.
- IIS Manager açılır.
- Site seçilir.
- Http Response Header simgesi seçilir.
- Actions sütunundaki Add linkine tıklanır.
- Ardından Add Custom Http Response Header dialog penceresine aşağıdaki girdiler girilir.
- name: Strict-Transport-Security
- value: max-age=31536000; includeSubDomains; preload

Not: 31536000 ömrü (saniyesi) 1 yılı ifade eder.

d. Yararlı Linkler

// Chromium HSTS Preload Listesi
https://cs.chromium.org/chromium/src/net/http/transport_security_state_static.json

// HSTS Header'ı Kullanılıyor mu Denetimi (online)
https://securityheaders.io

Kaynaklar

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

https://www.mehmetince.net/hsts-http-strict-transport-security-ile-https-trafik-guvenligi/

https://www.tbs-certificates.co.uk/FAQ/en/hsts-iis.html

https://hstspreload.org/

https://avicoder.me/2016/02/22/SSLstrip-for-newbies/

https://scotthelme.co.uk/hsts-the-missing-link-in-tls/

https://scotthelme.co.uk/hsts-cheat-sheet/