Test HTTP Strict Transport Security (HTTP Sıkı Aktarım Güvenliğini Test Etme)

Summary (Özet)

HTTP Sıkı Taşımacılık Güvenliği (HSTS) özelliği, bir web uygulamasının tarayıcıyı özel bir yanıt başlığının kullanımıyla, şifrelenmemiş HTTP kullanarak belirtilen etki alanı sunucularına asla bir bağlantı kurmaması gerektiğini bildirmesini sağlar. Bunun yerine, siteye HTTPS aracılığıyla erişmek için tüm bağlantı isteklerini otomatik olarak oluşturmalıdır. Ayrıca kullanıcıların sertifika hatalarını geçersiz kılmalarını da önler.

Bu güvenlik önleminin önemini göz önünde bulundurarak, web sitesinin web tarayıcısı ile sunucu arasında şifrelenmiş tüm verilerin yol kaplamasını sağlamak için bu HTTP başlığını kullandığını doğrulamak ihtiyatlıdır.

HTTP sıkı taşıma güvenlik başlığı iki direktif kullanır:

- `max-age` Tarayıcının tüm HTTP isteklerini otomatik olarak HTTPS'ye dönüştürmesi gereken saniye sayısını belirtmek için.
- `includeSubDomains`: İlgili tüm alt-domanların HTTPS kullanması gerektiğini belirtmek gerekir.
- `preload` Resmi olmayan: Domain(ler) ön yükleme listelerinde olduğunu ve tarayıcıların HTTPS olmadan asla bağlanmaması gerektiğini belirtmek.
    - Bu, tüm büyük tarayıcılar tarafından desteklenir, ancak spesifikasyonun resmi bir parçası değildir. (Daha fazla bilgi için hstspreload.org adresine bakın.)

İşte HSTS başlığı uygulamasına bir örnek:

`Strict-Transport-Security: max-age=31536000; includeSubDomains`

Bu başlığın web uygulamaları tarafından kullanılması, aşağıdaki güvenlik sorunlarının üretilip üretilemeyeceğini bulmak için kontrol edilmelidir:

- Saldırganlar ağ trafiğini kokluyor ve şifrelenmemiş bir kanal aracılığıyla aktarılan bilgilere erişiyor.
- Saldırganlar, güvenilmeyen sertifikaları kabul etme sorunu nedeniyle orta saldırıda bir manipülatörü istismar ediyor.
- Tarayıcıda yanlışlıkla bir adrese giren kullanıcılar HTTP yerine HTTP'yi veya HTTP protokolünü yanlışlıkla kullandığını gösteren bir web uygulamasında bir bağlantıya tıklayan kullanıcılar.

Test Objectives (Test Hedefleri)

- HSTS başlığını ve geçerliliğini gözden geçirin.

How to Test (Nasıl Test Edilir)

HSTS başlığının varlığı, sunucunun yanıtını ele geçiren bir proxy aracılığıyla veya aşağıdaki gibi kıvırcık kullanarak doğrulanabilir:

```
$ curl -s -D- https://owasp.org | grep -i strict
Strict-Transport-Security: max-age=31536000
```

References (Referanslar)

- OWASP HTTP Katı Ulaştırma Güvenliği
- OWASP Appsec Dayatoryal Dizisi - Bölüm 4: Sttrict Transport Security
- HSTS Şartname