**Bilgi Sistemleri ve**

**Güvenliği**

**175541008**

**Bekir Öndeş**

**Özet**

Invicti, bu web sitesinde BREACH (Browser Reconnaissance & Exfiltrasyon yoluyla Adaptive Compression of

Hypertext) saldırısının mümkün olduğunu tespit etti.

BREACH saldırısını mümkün kılan unsurlar nedeniyle, SSL/TLS korumalı trafik savunmasız kalır ve web sitesindeki bilgileri ortaya çıkarmak için saldırıya uğrayabilir.

Hangi SSL/TLS sürümünü kullanırsanız kullanın, saldırılar yine de mümkündür. Saldırılar, TLS katmanı sıkıştırması gerektirmez ve herhangi bir şifre paketine karşı çalışabilirler.

**Etkisi**

SSL/TLS korumalı bir bağlantı kullansanız bile, saldırgan kurbanın şifreli trafiğini görüntüleyebilir ve kurbanın (görünmez çerçeveler kullanarak) savunmasız web sunucusuna HTTP istekleri göndermesine neden olabilir. Bu adımları izleyerek bir saldırgan web sitesinden bilgi çalabilir ve aşağıdakileri yapabilir:

 Ortaya çıkardıkları kısmi düz metni bir kurbanın isteklerine enjekte edin

 Şifrelenmiş trafiğin boyutunu ölçün

**Düzeltmek için,**

Netsparker, hedef web sayfası bunu kolaylaştıran aşağıdaki koşulları karşıladığı için Olası bir İhlal Saldırısı sorunu bildirdi:

 HTTP düzeyinde sıkıştırma kullanan bir sunucudan sunulur (ör. gzip)

 HTTP yanıt gövdelerinde kullanıcı girdisini yansıtır

 HTTP yanıt gövdelerinde hassas bilgiler (CSRF belirteci gibi) içerir

Sorunu azaltmak için aşağıdaki çözümleri öneriyoruz:

1. Mümkünse, HTTP düzeyinde sıkıştırmayı devre dışı bırakın

2. Hassas bilgileri kullanıcı girişinden ayırın

3. Güvenlik açığı bulunan sayfaları CSRF belirteci ile koruyun. SameSite Cookie özniteliği bu sorunu azaltacaktır, çünkü bu sorundan yararlanmak için bir saldırgan, kurbanı görünmez çerçeveler kullanarak hedef bir web sitesini ziyaret etmeye zorlar. SameSite cookie özelliği eklendiğinde, hedefe ait cookie'ler üst düzey navigasyon içermeyen bir istek ile gönderilmeyecektir.

4. Yanıtlara rastgele sayıda bayt ekleyerek trafiğin uzunluğunu gizleyin.

5. Dakikada beş kez maksimum sayfaya ulaşılması için bir hız sınırı ekleyin.

6 / 114

**Özet**

Invicti, HTTP Katı Aktarım Güvenliği (HSTS) ilkesinin etkinleştirilmediğini belirledi.

Hedef web sitesi yalnızca HTTPS'den değil, aynı zamanda HTTP'den de sunuluyor ve HSTS politika uygulamasından yoksun.

HTTP Strict Transport Security (HSTS), bir web sunucusunun, uygun kullanıcı aracılarının (bir web tarayıcısı gibi) kendisiyle yalnızca güvenli (HTTPS) bağlantılar kullanarak etkileşime gireceğini beyan ettiği bir web güvenlik politikası mekanizmasıdır. HSTS Politikası, sunucu tarafından kullanıcı aracısına "Strict-Transport-Security" adlı bir HTTP yanıt başlığı alanı aracılığıyla iletilir. HSTS Politikası, kullanıcı aracısının sunucuya yalnızca güvenli bir şekilde erişeceği bir süre belirtir.

Bir web uygulaması kullanıcı aracılarına HSTS Politikası yayınladığında, uyumlu kullanıcı aracıları aşağıdaki gibi davranır:

 Web uygulamasına atıfta bulunan güvenli olmayan (HTTP) bağlantıları otomatik olarak güvenli (HTTPS) bağlantılara dönüştürün. (Örneğin, <http://example.com/some/page/>, sunucuya erişmeden önce https://example.com/some/page/ olarak değiştirilecektir.)

 Bağlantının güvenliği sağlanamıyorsa (örneğin sunucunun TLS sertifikası kendinden imzalıysa), kullanıcı aracıları bir hata mesajı gösterir ve kullanıcının web uygulamasına erişmesine izin vermez.

**Düzeltme**

Web sunucunuzu HTTP isteklerini HTTPS'ye yönlendirecek şekilde yapılandırın.

yani Apache için httpd.conf dosyasında değişiklik yapmalısınız. Daha fazla konfigürasyon için lütfen Dış Referanslar bölümüne bakın.

# yük modülü

LoadModule headers\_module modülleri/mod\_headers.so

# tüm HTTP'yi HTTPS'ye yönlendir (isteğe bağlı)

<SanalAna Bilgisayar \*:80> SunucuAlias \*

Yeniden YazmaMotoru Açık

RewriteRule ^(.\*)$ https://%{HTTP\_HOST}$1 [yönlendirme=301]

</SanalAna Bilgisayar