Referer ve Referrer-Policy Header

Referer Header

a. Referer Header Nedir?

Referer başlığı bir http request başlığıdır. Referer header'ı bir web sitesindeki linkten bir başka sayfaya atladığımızda atladığımız sayfaya nereden geldiğimizi gösteren link değerini alır. Böylece web site sahipleri uygulamalarına trafiğin nereden geldiğini gözlemleyebilirler. Bir örnek vermek gerekirse scotthelme.co.uk web sitesi sahibi kendisine gelen trafikten 4000 kullanıcının twitter'dan geldiğini gözlemlemiş. Aşağıda bu site sahibinin web sitesine gelen 4000 kullanıcının yaptığı http request'i görmektesin.

Request Headers:

...
Host: scotthelme.co.uk
Referer: https://twitter.com/Scott_Helme/status/760790725
Upgrade-Insecure-Requests: 1
....

Görüldüğü üzere yukarıdaki talebi yapan kullanıcı scotthelme.co.uk sitesine twitter.com/Scott_Helme/status/760790725 sitesinden gelmiştir.

Uygulama

(+) Birebir denenmiştir ve başarıyla uygulanmıştır.

Diyelim ki bir kullanıcı olarak www.includekarabuk.com sitesinde bulunmaktayız. Referer header'ını gözlemlemek adına burp ile tarayıcımız ve sunucu arasına girdiğimizi ve http request'lerin önünü kestiğimizi varsayalım. Ardından www.includekarabuk.com sitesindeki genel kategorisine (linkine) tıklayalım.

HTTP Request:

GET **/kategoriler/genel/** HTTP/1.1
Host: www.includekarabuk.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:58.0) Gecko/20 Firefox/58
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://www.includekarabuk.com/
Cookie: PHPSESSID=n9ti75hr8ae69b5ep00d1l7n94
Connection: close
Upgrade-Insecure-Requests: 1

Görüldüğü üzere Genel kategorisi sayfasını talep ederken geldiğimiz sayfa olarak www.includekarabuk.com olduğu belirtilmiş. Bu talep sonrası Genel kategorisine geliriz. Buradan hareketle başka bir kategoriye tıklayalım. Örneğin Java Programlama'ya:

HTTP Request:

```
GET /kategoriler/javaprogramlama/ HTTP/1.1
Host: www.includekarabuk.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:58.0) Gecko/20 Firefox/58
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://www.includekarabuk.com/kategoriler/genel/
Cookie: PHPSESSID=n9ti75hr8ae69b5ep00d1l7n94
Connection: close
Upgrade-Insecure-Requests: 1
```

Görüldüğü üzere Java Programlama kategorisi sayfasını talep ederken geldiğimiz sayfa olarak www.includekarabuk.com/kategoriler/genel (Yani Genel kategorisi) olduğu belirtilmiş. Dolayısıyla her bir linke tıkladığımızda bir önceki bulunduğumuz link Referer header'ına yerleşmektedir ve böylelikle http request ile sunucuya gitmektedir.

Referer Header ile Doğan Zafiyet

Bir web uygulaması yönlendirme hedef adresi olarak eğer local bir adresi değil de http request header'ı olan referer header'ından gelen adresi kullanırsa open redirection diye adlandırılan bir zafiyete neden olabilir. Çünkü eğer saldırgan hedef web sitesi kullanıcısı ile web sunucusu arasına girerse ve Referer header'ını bir phising sayfası linki yaparsa uygulama kullanıcıyı bir phising sayfasına yönlendirebilir ve oltalama saldırısıyla karşı karşıya bırakabilir.

Örneğin 6 ay önce Moodle web uygulamasında open redirect zafiyeti ortaya çıkmıştır. Şöyle ki Moodle redirect() fonksiyonu get_referer() ile beraber güvensiz bir şekilde [redirect(get_referer())] kullanıyordu. Referer header'ı bir kısıt altına alınmadığından saldırganlar araya girip kullanıcıları rasgele web sitelerine phising amacıyla yönlendirebilmekteydiler. Dolayısıyla kullanıcıların phising saldırısıyla karşı karşıya bırakmamak için web geliştiricileri Referer header'ını bir denetim altına koymak durumundadırlar.

Referer header'ı aynı zamanda kullanıcı gizliliğini de ihlal edebilmektedir. Örneğin Referer header'ı siteler arası atlamalarda kaynak sitede kullanılan kritik parametrelerin diğer siteye aktarımına neden olabilir. Dolayısıyla kullanıcıların gizliliğini ihlal eden bir web uygulaması geliştiricisi olmamak için Referer header'ını bir denetim altına koymak gerekir.

Referer Header ile Doğan Zafiyete Çözüm

İki çözüm yolu vardır:

- Script dili ile kısıt koyma
- Referrer-Policy header'ı ile kısıt koyma

Referer header'ı ile doğan zafiyet web uygulamalarında yönlendirme mekanizmalarının doğrudan Referer header'ından gelen linke göre yönlendirme yapmalarından dolayı ileri geliyordu. Bu problem kodlama ile çözülebilmektedir. Örneğin Moodle için get_referer() fonksiyonu redirect() fonksiyonu ile güvensiz bir biçimde [redirect(get_referer())] kullanıldığından saldırganlar araya

girip Referer'ı değiştirerek kullanıcıları phising sayfalarına yönlendirebiliyordu. Moodle için get_referer() fonksiyonunun çıktısı local bir URI ile replace edilerek güvenlik sorunu çözüme kavuşabilir. Diğer bir yöntem ise http response'da Referrer-Policy header'ı kullanımıdır. Örneğin;

```
Response Header:
        …

        Referrer-Policy:  no-referrer          // Referer header'ı bulunulan web
                                               // uygulaması için istemci tarafında
                                               // komple gönderimi engellenir.
        …
```

Yukarıdaki kullanım ile web uygulaması kullanıcısının tarayıcısına ilgili web uygulamasında bulunduğu sürece asla Referer header'ını ilgili web sunucusuna gönderme demiş oluruz. Böylece phising ya da gizlilik ihlali problemleri hallolmuş olur. Daha spesifik bir Referer kısıtlamasına gitmek için

```
"",
no-referrer,
no-referrer-when-downgrade,
same-origin,
origin,
strict-origin,
origin-when-cross-origin,
strict-origin-when-cross-origin,
unsafe-url
```

değerleri kullanılabilir. Bu çeşitli kısıtlar için daha detaylı bilgiye Referrer-Policy Header başlığında ulaşabilirsin.

Referrer-Policy header'ını web sunucusundan dönen http yanıtlarına eklemek için;

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

```
# Nginx sunucular da konfigurasyon dosyasına
add_header Referrer-Policy "no-referrer";

# Apache sunucular da apache2.conf dosyasına
Header always set Referrer-Policy "no-referrer"

# IIS sunucular da Web.Config dosyasındaki <customHeaders> tag'ları arasına
<system.webServer>
  <httpProtocol>
    <customHeaders>
      <add name="Referrer-Policy" value="no-referrer" />
    </customHeaders>
```

```
  </httpProtocol>
</system.webServer>
```

satırları eklenmelidir ve web sunucu yazılımı yeniden başlatılmalıdır. Böylece http response'larda Referrer-Policy header'ı gelecektir ve kullanıcıların web uygulamasındaki programlama hatasından kaynaklı bir olası phising saldırısıyla karşı karşıya kalmaları önlenmiş olacaktır. Ayrıca geldikleri siteye dair link ve parametreler işlenmediğinden gizlilikleri temin edilmiş olacaktır.

Referrer-Policy Header

a. Referrer-Policy Header Nedir?

Referer başlığı bir http response başlığıdır. Aşağıdaki değerleri alabilir:

```
"",
no-referrer,
no-referrer-when-downgrade,
same-origin,
origin,
strict-origin,
origin-when-cross-origin,
strict-origin-when-cross-origin,
unsafe-url
```

no-referrer
Referrer-Policy header'ı no-referrer ile kullanıldığında bulunulan web uygulamasından yapılan her talepte referer header'ının gönderimi yapılmasın denmiş olur.

```
Response Header:
    …
    Referrer-Policy: no-referrer
    …
```

Örneğin;

Source	Destination	Referrer
https://scotthelme.co.uk/blog1/	http://scotthelme.co.uk/blog2/	NULL
https://scotthelme.co.uk/blog1/	https://scotthelme.co.uk/blog2/	NULL
http://scotthelme.co.uk/blog1/	http://scotthelme.co.uk/blog2/	NULL
http://scotthelme.co.uk/blog1/	http://example.com	NULL
http://scotthelme.co.uk/blog1/	https://example.com	NULL
https://scotthelme.co.uk/blog1/	http://example.com	NULL

same-origin
Referrer-Policy header'ı same-origin ile kullanıldığında bulunulan web uygulamasından başka web uygulamalarına yapılan taleplerde referer header'ının gönderimi yapılmasın denmiş olur. Bulunulan web uygulaması kapsamı içerisinde yapılan taleplerde ise Referer header'ı gönderimi açık olsun denmiş olur.

Response Header:

…
Referrer-Policy: same-origin
…

Source	Destination	Referrer
https://scotthelme.co.uk/blog1/	https://scotthelme.co.uk/blog2/	https://scotthelme.co.uk/blog1/
http://scotthelme.co.uk/blog1/	http://scotthelme.co.uk/blog2/	http://scotthelme.co.uk/blog1/
https://scotthelme.co.uk/blog1/	http://example.com/	NULL
https://scotthelme.co.uk/blog1/	https://example.com/	NULL
https://scotthelme.co.uk/blog1/	http://scotthelme.co.uk/blog2/	NULL

Not: Sonuncu satırda birisi http diğeri https olduğu için ayrı kapsamlarda değerlendirilmektedir.

no-referrer-when-downgrade
Referrer-Policy header'ı no-referrer ile kullanıldığında bulunulan web uygulamasında http den http 'ye gidildiğinde Referer header'ı kullanılsın, http'den https'e gidildiğinde Referer header'ı kullanılsın, https den https'e gidildiğinde yine Referer header'ı kullanılsın, fakat https'den http'ye gidildiğinde Referer header'ı kullanılmasın denmiş olur.

Response Header:

…
Referrer-Policy: no-referrer-when-downgrade
…

Örneğin;

Source	Destination	Referrer
https://scotthelme.co.uk/blog1/	http://scotthelme.co.uk/blog2/	NULL
https://scotthelme.co.uk/blog1/	https://scotthelme.co.uk/blog2/	https://scotthelme.co.uk/blog1/
http://scotthelme.co.uk/blog1/	http://scotthelme.co.uk/blog2/	http://scotthelme.co.uk/blog1/
http://scotthelme.co.uk/blog1/	http://example.com	http://scotthelme.co.uk/blog1/
http://scotthelme.co.uk/blog1/	https://example.com	http://scotthelme.co.uk/blog1/
https://scotthelme.co.uk/blog1/	http://example.com	NULL

Tüm Referrer-Policy değerlerini görüp tercihe uygun olanı seçmek için https://scotthelme.co.uk/a-new-security-header-referrer-policy/ sitesinden detaylıca veya https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy sitesinden öz bir şekilde yararlanılabilir.

Kaynaklar

https://scotthelme.co.uk/a-new-security-header-referrer-policy/

https://blog.qualys.com/securitylabs/2016/01/07/open-redirection-a-simple-vulnerability-threatens-your-web-applications

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3175

https://moodle.org/mod/forum/discuss.php?d=313682
https://blog.appcanary.com/2017/http-security-headers.html#referrer-policy

https://www.ryadel.com/en/iis-web-config-secure-http-response-headers-pass-securityheaders-io-scan/