Nerdesin Ey Referer

Bedirhan Urgun, Aralık 2009, WGT E-Dergi 3. Sayı

http://www.webguvenligi.org web sitesini açıp okuyan bir kullanıcı, sayfa içindeki e-dergi linkine tıkladığında http://dergi.webguvenligi.org sitesine yapılacak HTTP GET isteği aşağıdaki gibidir.

```
GET /default.aspx HTTP/1.1
Host: dergi.webguvenligi.org
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.9.0.15)
Gecko/2009101601 Firefox/3.0.15 (.NET CLR 3.5.30729)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en-gb;q=0.7,tr;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Proxy-Connection: keep-alive
Referer: http://www.webguvenligi.org/
```

Bu HTTP GET isteğinde Referer [1] başlığının değeri kullanıcının dergi.webguvenligi.org adresine giderken, aslında www.webguvenligi.org adresini kullandığını anlatmaktadır. Bu başlığın sağladığı faydalara veya zararlara birden fazla perspektiften bakabiliriz;

1. Web Sitesi Yöneticileri: Referer başlığı web site yöneticilerine sayfalarını ziyaret eden kullanıcılarının hangi kaynaklardan geldiklerini gösterir. Bu da sitenin ziyaret sayısını ve performansını arttırmaları için çok önemli bir bilgidir.
2. Kullanıcılar: Referer başlığı tarayıcı tarafından otomatik olarak isteklere eklendiğinden kullanıcıların hangi siteyi ziyaret ederken yönlendirildikleri hedef siteye gönderilmiş olur.
3. Saldırganlar: Zararlı linklerini (CSRF/XSS/Kötü amaçlı iframeler/.) koydukları sayfaları ziyaret eden kullanıcılar, hedef siteye linklere tıklayarak veya otomatik olarak yönlendirildiklerinde kaynak web siteleri Referer başlığı sayesinde hemen yakalanabilir.
4. Geliştiriciler: Artık çok iyi bilinse de, geliştiriciler bazı yetkilendirme kontrollerini bu başlığın değerini kullanarak gerçekleştirilebilirler. CSRF kontrolleri [2] de bu kullanım alanlarına bir örnektir.

Bu yazıda Referer HTTP başlığının tarayıcı tarafından isteklere otomatik olarak eklenmesini **önleyecek** veya **önlemeye yetmeyecek** tekniklerden bahsedilecektir.

meta refresh

Literatürde en çok bahsedilen teknik olarak HTML meta elementi gözükmektedir. Meta elementi Refresh değeri ile kullanıldığında url parametresindeki değer tarayıcı tarafından istendiğinde Referer başlığı HTTP isteğine eklenmeyecektir. Önemli bir not, meta elementi

sadece head elementi içinde değil body elementi içinde de kullanıldığında tarayıcılar tarafından çalıştırılabilmektedir.

HTML

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
 <head>
 <meta http-equiv="refresh" content="0;url=http://www.webguvenligi.org/" />
<title>
</title>
</head>
<body>
Meta Refresh Referer Stripping
</body>
</html>
```

HTTP İSTEK

```
GET / HTTP/1.1
Host: www.webguvenligi.org
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.9.0.15)
Gecko/2009101601 Firefox/3.0.15 (.NET CLR 3.5.30729)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en-gb;q=0.7,tr;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
```

iframe

Tarayıcı bir üst kapsamın adresini kullandığından iframe kullanılarak Referer başlığının kaldırılması mümkün olmamaktadır.

HTML

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
 <head>
 <title></title>
 </head>
 <body>
  <iframe src="http://www.webguvenligi.org/" />
 </body>
</html>
```

HTTP İSTEK

GET / HTTP/1.1
Host: www.webguvenligi.org
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.9.0.15) Gecko/2009101601 Firefox/3.0.15 (.NET CLR 3.5.30729)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://www.attacker.com/metarefresh/second.html

javascript

script HTML elementinin farklı şekillerde kullanılması ile Referer önlenmesi pek mümkün gözükmemektedir.

HTML 1

```
<script src="http://www.webguvenligi.org/"></script>
```

HTML 2

```
<script>
 var i = new Image();
 i.src = "http://www.webguvenligi.org/";
</script>
```

HTML 3

```
<script>
 document.write("<img src='http://www.webguvenligi.org/' />");
</script>
```

HTML 4

```
<iframe src="javascript:document.location='http://www.webguvenligi.org/'" />
```

HTTP İSTEK

GET / HTTP/1.1
Host: www.webguvenligi.org
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.9.0.15) Gecko/2009101601 Firefox/3.0.15 (.NET CLR 3.5.30729)
Accept: */*
Accept-Language: en-us,en-gb;q=0.7,tr;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7

Keep-Alive: 300
Connection: keep-alive
Referer: http://www.attacker.com/metarefresh/third.html

javascript + iframe + biraz sihir

iframe ve script elementleri ile yapamadığımızı ikisini farklı bir şekilde birleştirerek yapabilmemiz mümkün olabilmektedir. (setTimeout metodunu kullanmak gerekli gözüküyor)

HTML

```
<iframe src="javascript:t=setTimeout('i=new
Image();i.src=\'http://www.webguvenligi.org/\'',1000);" />
```

HTTP İSTEK

```
GET / HTTP/1.1
Host: www.webguvenligi.org
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.9.0.15)
Gecko/2009101601 Firefox/3.0.15 (.NET CLR 3.5.30729)
Accept: image/png,image/*;q=0.8,*/*;q=0.5
Accept-Language: en-us,en-gb;q=0.7,tr;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
```

https -> http

Kaynak sayfa HTTP'den farklı bir protokole sahipse (HTTPS/DATA/FTP/.) tarayıcılar Referer başlığını eklememektedir. Burada sadece HTTPS kaynağı örneklenmiştir.

Kaynak: **https**://www.webguvenligi.org
Hedef: **http**://dergi.webguvenligi.org/default.aspx

HTTP İSTEK

```
GET /default.aspx HTTP/1.1
Accept: */*
Accept-Language: en-gb,tr;q=0.5
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727; .
3.0.4506.2152; .NET CLR 3.5.30729; MS-RTC LM 8)
Host: dergi.webguvenligi.org
Proxy-Connection: Keep-Alive
```

xhr

AJAX ile yapılan isteklerde de Referer başlığının otomatik olarak eklenmesi söz konusudur. Kaldı ki Same Origin Policy [3] nedeniyle başka bir domain'e istek yapmak yasaklanmıştır.

HTML

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
 <head>
 <title></title>
 </head>
 <body>
<script type="text/javascript">
var xmlhttp;
function loadXMLDoc(url)
{
xmlhttp=GetXmlHttpObject();
.
xmlhttp.open("GET",url,true);
xmlhttp.send(null);
}

function GetXmlHttpObject()
{
.
}
...
loadXMLDoc("http://www.attacker.org/");
</script>
 </body>
</html>
```

HTTP İSTEK

```
GET / HTTP/1.1
Host: www.attacker.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.9.0.15)
Gecko/2009101601 Firefox/3.0.15 (.NET CLR 3.5.30729)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en-gb;q=0.7,tr;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://www.attacker.com/metarefresh/fourth.html
```

flash

Same Origin Policy XHR'e göre daha az kısıtlayıcı olsa da Flash ile yapılan isteklerde de Referer başlığının otomatik olarak eklenmesi söz konusudur.

ACTIONSCRIPT

```
<?xml version="1.0" encoding="utf-8"?>
<mx:Application xmlns:mx="http://www.adobe.com/2006/mxml" layout="absolute"
initialize="redirect()">
 <mx:Script>
  <![CDATA[
   import flash.net.navigateToURL;

   private function redirect() :void{
    var request:URLRequest = new URLRequest();
    request.url = "http://www.webguvenligi.org/";
    navigateToURL(request, "_top");
   }
  ]]>
 </mx:Script>
</mx:Application>
```

HTTP İSTEK

```
GET / HTTP/1.1
Host: www.webguvenligi.org
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.9.0.15)
Gecko/2009101601 Firefox/3.0.15 (.NET CLR 3.5.30729)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en-gb;q=0.7,tr;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://www.attacker.com/metarefresh/refresh/refresh.html
```

hiderefer / unrefer

Referer başlığını otomatik olarak eklemeyi önlemenin diğer bir yöntemi de hiderefer.com ve unrefer.com gibi sitelerdir. Temelinde meta refresh tekniğini kullansalar da bu da diğerlerinden farklı bir teknik olarak anlatılabilir.

HTML

```
<title>HideRefer.com Anonym Link</title>
<meta http-equiv="refresh" content="1; URL=http://www.webguvenligi.org/">
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
```

HTTP İSTEK

```
GET / HTTP/1.1
Host: www.webguvenligi.org
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.9.0.15)
Gecko/2009101601 Firefox/3.0.15 (.NET CLR 3.5.30729)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en-gb;q=0.7,tr;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Proxy-Connection: keep-alive
```

hiderefer.com Tarafından Kullanılan HTML

```
<iframe src="http://hiderefer.com/?http://www.webguvenligi.org/" />
```

Bu gibi servisleri ve teknikler kullanıldığında dikkat edilmesi gereken bir nokta vardır. Eğer hedef sitesi framebusting kodu kullanıyorsa, iframe veya frame ile açılan sayfada bu kod parçası çalışacak ve hedef siteye yapılan ikinci istekte Referer başlığı tekrar eklenecektir. Bu kapsamda Referer HTTP başlığının kullanıcının tarayıcısından çıkmaması için en iyi yollar meta refresh, https->http gibi gözükmektedir.

Referanslar

[1] http://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html
[2] http://seclab.stanford.edu/websec/csrf/
[3] https://developer.mozilla.org/en/Same_origin_policy_for_JavaScript