# Referrer Policy 介绍

 2017-08-11 00:34 2017-08-11 01:09 [HTTP](https://caixw.io/tags/http.html)[安全](https://caixw.io/tags/security.html) caixw

当用户在浏览器上点击一个链接时，会产生一个 HTTP 请求，用于获取新的页面内容，而在该请求的报头中，会包含一个 Referrer，用以指定该请求是从哪个页面跳转页来的，常被用于分析用户来源等信息。但是也有成为用户的一个不安全因素，比如有些网站直接将 sessionid 或是 token 放在地址栏里传递的，会原样不动地当作 Referrer 报头的内容传递给第三方网站。

所以就有了 [Referrer Policy](https://www.w3.org/TR/referrer-policy/)，用于过滤 Referrer 报头内容，目前是一个候选标准，不过已经有部分浏览器支持该标准。具体的可查看[这里](https://www.caniuse.com/" \l "search=referrer)。

## 指令值

目前包含了以下几种指令值：

enum ReferrerPolicy {

"",

"no-referrer",

"no-referrer-when-downgrade",

"same-origin",

"origin",

"strict-origin",

"origin-when-cross-origin",

"strict-origin-when-cross-origin",

"unsafe-url"};

### 空字符串

按照浏览器的默认值执行。默认值为 [no-referrer-when-downgrade](https://caixw.io/posts/2017/referrer-policy.html" \l "no-referrer-when-downgrade)。部分标签可重定义此安全策略。

### no-referrer

从字面意思就可以理解，不传递 Referrer 报头的值。

### no-referrer-when-downgrade

当发生降级（比如从 https:// 跳转到 http:// ）时，不传递 Referrer 报头。但是反过来的话不受影响。通常也会当作浏览器的默认安全策略。

| 原地址 | 跳转地址 | Referrer |
| --- | --- | --- |
| https://example.com?token=123 | https://example.com/path | https://example.com?token=123 |
| http://example.com?token=123 | http://example.com/path | http://example.com?token=123 |
| http**s**//example.com | http://example.com/path | 无（协议降级） |
| http://example.com?token=123 | http**s**://example.com/path | http://example.com?token=123 |

### same-origin

同源，即当协议、域名和端口（如果有一方指定的话）都相同，才会传递 Referrer。

| 原地址 | 跳转地址 | Referrer |
| --- | --- | --- |
| https://example.com?token=123 | https://example.com/path | https://example.com?token=123 |
| http://example.com?token=123 | http://example.com/path | http://example.com?token=123 |
| http**s**//example.com | http://example.com/path | 无（协议不同） |
| http://example.com?token=123 | http**s**://example.com/path | 无（协议不同） |
| http://example.com?token=123 | http://example.com:88/path | 无（端口不同） |
| https://example.com?token=123 | https://caixw.io | 无（域名不同） |

### origin

将当前页面过滤掉参数及路径部分，仅将协议、域名和端口（如果有的话）当作 Referrer。

| 原地址 | 跳转地址 | Referrer |
| --- | --- | --- |
| https://example.com?token=123 | https://example.com/path | https://example.com |
| http://example.com?token=123 | http**s**://example.com/path | http://example.com |
| https://example.com?token=123 | https://caixw.io | https://example.com |

### strict-origin

类似于 [origin](https://caixw.io/posts/2017/referrer-policy.html" \l "origin)，但是不能降级。

| 原地址 | 跳转地址 | Referrer |
| --- | --- | --- |
| https://example.com?token=123 | https://example.com/path | https://example.com |
| http://example.com?token=123 | http**s**://example.com/path | http://example.com |
| http://example.com?token=123 | http://caixw.io | http://example.com |
| https://example.com?token=123 | http://caixw.io | 无 |

### origin-when-cross-origin

跨域时（协议、域名和端口只有一个不同）和 [origin](https://caixw.io/posts/2017/referrer-policy.html" \l "origin) 模式相同，否则 Referrer 还是传递当前页的全路径。

| 原地址 | 跳转地址 | Referrer |
| --- | --- | --- |
| https://example.com?token=123 | https://example.com/path | https://example.com?token=123 |
| http://example.com?token=123 | http**s**://example.com/path | http://example.com?token=123 |
| http://example.com?token=123 | http://caixw.io | http://example.com |

### strict-origin-when-cross-origin

与 [origin-when-cross-origin](https://caixw.io/posts/2017/referrer-policy.html" \l "origin-when-cross-origin) 类似，但不能降级。

| 原地址 | 跳转地址 | Referrer |
| --- | --- | --- |
| https://example.com?token=123 | https://example.com/path | https://example.com?token=123 |
| https://example.com?token=123 | https://caixw.io | https://example.com |
| http**s**://example.com?token=123 | http://example.com/path | 无 |
| http**s**://example.com?token=123 | http://example.com/ | 无 |

### unsafe-url

任意情况下，都发送当前页的全部地址到 Referrer，最宽松和不安全的策略。

## 传递方式

### Referrer-Policy 报头

推荐的方式，直接在 Referrer-Policy 报头中设置。

Referrer-Policy: origin;

### Meta

通过指定 name 值为 referrer 的 meta 标签，也可以达到相同的效果：

<meta name="referrer" content="strict-origin" />

content 可以是上面的指定的值，也可以是下面这几种旧的指令值，会自动作相应的转换，但不推荐这些旧的指令值：

| Legacy | Referrer |
| --- | --- |
| never | [no-referrer](https://caixw.io/posts/2017/referrer-policy.html" \l "no-referrer) |
| default | [no-referrer-when-downgrade](https://caixw.io/posts/2017/referrer-policy.html" \l "no-referrer-when-downgrade) |
| always | [unsafe-url](https://caixw.io/posts/2017/referrer-policy.html" \l "unsafe-url) |
| origin-when-crossorigin | [origin-when-cross-origin](https://caixw.io/posts/2017/origin-when-cross-origin) |

### 标签属性

* a 和 link 标签可以通过属性 rel 指定 noreferrer，仅对当前链接有效；
* a、area、link、iframe 和 img 还可以通过 referrerpolicy 指定仅针对当前链接的设置。

## 参考

[Referrer Policy](https://www.w3.org/TR/referrer-policy/)

[Referrer-Policy](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy)

[浏览器的同源策略](https://developer.mozilla.org/zh-CN/docs/Web/Security/Same-origin_policy)