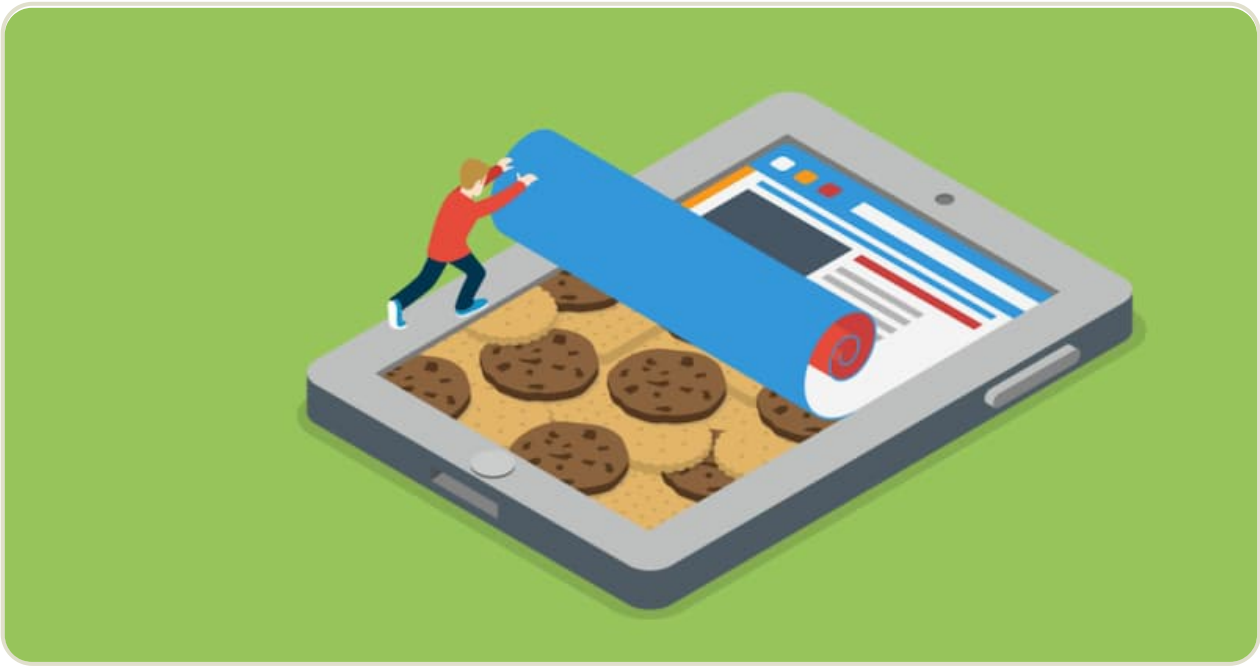
Cookie 的 SameSite 属性

作者： 阮一峰

日期： 2019年9月 9日

Chrome 51 开始，浏览器的 Cookie 新增加了一个 `SameSite` 属性，用来防止 CSRF 攻击和用户追踪。



一、CSRF 攻击是什么？

Cookie 往往用来存储用户的身份信息，恶意网站可以设法伪造带有正确 Cookie 的 HTTP 请求，这就是 CSRF 攻击。

举例来说，用户登陆了银行网站 `your-bank.com` ，银行服务器发来了一个 Cookie。

```
Set-Cookie:id=a3fWa;
```

用户后来又访问了恶意网站 `malicious.com` ，上面有一个表单。

```
<form action="your-bank.com/transfer" method="POST">
  ...
</form>
```

用户一旦被诱骗发送这个表单，银行网站就会收到带有正确 Cookie 的请求。为了防止这种攻击，表单一般都带有一个随机 token，告诉服务器这是真实请求。

```
<form action="your-bank.com/transfer" method="POST">
  <input type="hidden" name="token" value="dad3weg34">
  ...
</form>
```

这种第三方网站引导发出的 Cookie，就称为第三方 Cookie。它除了用于 CSRF 攻击，还可以用于用户追踪。

比如，Facebook 在第三方网站插入一张看不见的图片。

```
<img src="facebook.com" style="visibility:hidden;">
```

浏览器加载上面代码时，就会向 Facebook 发出带有 Cookie 的请求，从而 Facebook 就会知道你是谁，访问了什么网站。

二、SameSite 属性

Cookie 的 `SameSite` 属性用来限制第三方 Cookie，从而减少安全风险。

它可以设置三个值。

- `Strict`
- `Lax`
- `None`

2.1 Strict

`Strict` 最为严格，完全禁止第三方 Cookie，跨站点时，任何情况下都不会发送 Cookie。换言之，只有当前网页的 URL 与请求目标一致，才会带上 Cookie。

```
Set-Cookie: CookieName=CookieValue; SameSite=Strict;
```

这个规则过于严格，可能造成非常不好的用户体验。比如，当前网页有一个 GitHub 链接，用户点击跳转就不会带有 GitHub 的 Cookie，跳转过去总是未登陆状态。

2.2 Lax

Lax 规则稍稍放宽，大多数情况也是不发送第三方 Cookie，但是导航到目标网址的 Get 请求除外。

```
Set-Cookie: CookieName=CookieValue; SameSite=Lax;
```

导航到目标网址的 GET 请求，只包括三种情况：链接，预加载请求，GET 表单。详见下表。

请求类型	示例	正常情况	Lax
链接	`<a href="..."></a>`	发送 Cookie	发送 Cookie
预加载	`<link rel="prerender" href="..."/>`	发送 Cookie	发送 Cookie
GET 表单	`<form method="GET" action="...">`	发送 Cookie	发送 Cookie
POST 表单	`<form method="POST" action="...">`	发送 Cookie	不发送
iframe	`<iframe src="..."></iframe>`	发送 Cookie	不发送
AJAX	`$.get("...")`	发送 Cookie	不发送
Image	`<img src="...">`	发送 Cookie	不发送

设置了 Strict 或 Lax 以后，基本就杜绝了 CSRF 攻击。当然，前提是用户浏览器支持 SameSite 属性。

2.3 None

Chrome 计划将 Lax 变为默认设置。这时，网站可以选择显式关闭 SameSite 属性，将其设为 None 。不过，前提是必须同时设置 Secure 属性（Cookie 只能通过 HTTPS 协议发送），否则无效。

下面的设置无效。

```
Set-Cookie: widget_session=abc123; SameSite=None
```

下面的设置有效。

```
Set-Cookie: widget_session=abc123; SameSite=None; Secure
```

三、参考链接

- Using the Same-Site Cookie Attribute to Prevent CSRF Attacks

- SameSite cookies explained
- Tough Cookies, Scott Helme
- Cross-Site Request Forgery is dead!, Scott Helme

（完）

相关文章

- **2021.05.10:** 软件工程的最大难题

  > 一、引言 大学有一门课程《软件工程》，研究如何组织和管理软件项目。

- **2020.12.13:** 《SSH 入门教程》发布了

  > SSH 是登录 Linux 服务器的必备工具，只要你在做互联网开发，多多少少都会用到它。

- **2020.11.02:** 微信小程序入门教程之四：API 使用

  > 今天是这个系列教程的最后一篇。

- **2020.10.29:** 微信小程序入门教程之三：脚本编程

  > 这个系列教程的前两篇，介绍了小程序的项目结构和页面样式。

Weibo | Twitter | GitHub

Email: yifeng.ruan@gmail.com