链滴

理解 Cookie 机制

作者：someone38063

原文链接：https://ld246.com/article/1558414101632

来源网站：链滴

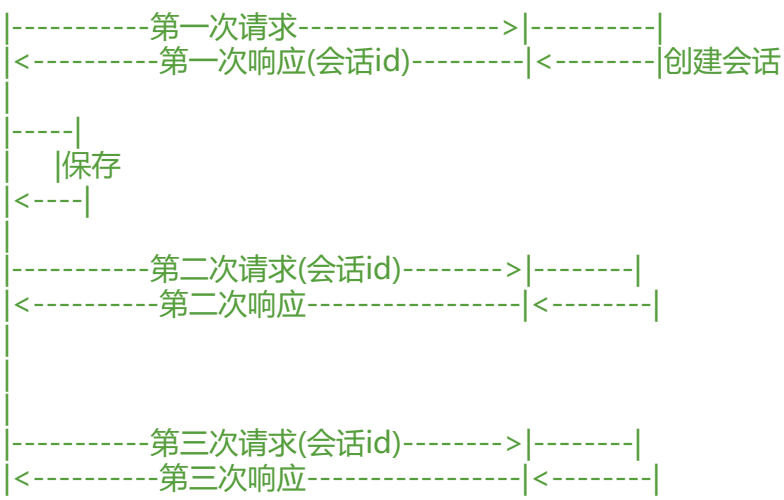
Cookie是一个很重要的客户端数据来源，也可以实现扩展性很好的会话

HTTP协议是无状态的

- 对于浏览器的每一次请求，服务器都会单独处理，不与之前或之后的请求发生关联
- 即使同一个浏览器发送了3个请求，服务器也会独立处理这3个请求，服务器并不知道3个请求来自一个浏览器
- 服务器需要识别浏览器请求，就必须弄清楚浏览器的请求状态。既然HTTP协议是无状态的，那就服务器和浏览器共同维护一个状态，这就是会话机制

#会话机制

浏览器 服务器



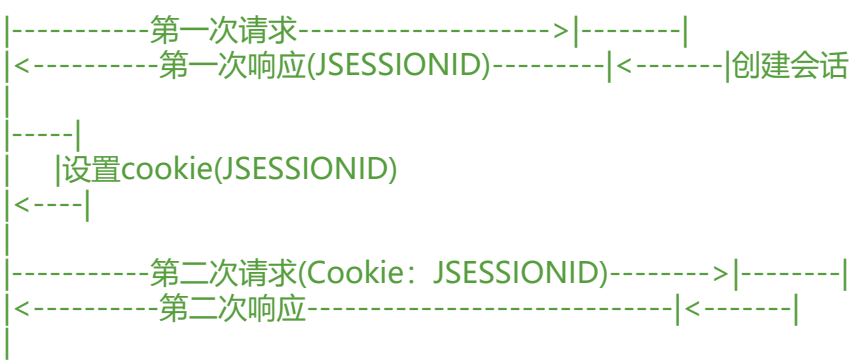
1. 浏览器第一次请求服务器时，服务器创建一个会话，并将会话的id作为响应的一部分发送给浏览器
2. 浏览器存储会话id，并在后续第二次和第三次请求中带上会话id。服务器取得请求中的会话id就知是不是同一个用户了

这样一来，后续请求就与第一次请求产生了关联

Cookie机制

服务器在内存中保存会话对象，浏览器可以使用Cookie机制保存会话id

浏览器 服务器



原文链接：理解 Cookie 机制

Cookie机制是一种会话机制。Cookie是浏览器用来存储少量数据的一种机制，数据以"key=value"式存储，浏览器发送HTTP请求时，自动附带cookie信息

Cookie是什么

- Cookie是一小段文本信息，伴随着用户请求和页面在浏览器和Web服务器之间传递
- Cookie是一种HTTP Header，以"key=value"的形式组成，例如：ip_country=CN
- 两个Cookie之间用分号隔开，比如ip_country=CN;mbox=check#true#1499311989

Cookie的作用

Cookie最主要的作用是用来做用户认证，还可以用于保存用户的一些其他信息

Cookie也可以用用于互联网精准广告定向技术

实例

通过Fiddler抓包观察上海科技馆网站的登录，来理解登陆的过程和Cookie机制

1. 启动fiddler，启动浏览器打开 http://piaoweb.sstm.org.cn/；输入用户名和密码并登录

抓包后可以看到浏览器把用户名发送给了Web服务器；Web服务器会验证用户名和密码的正确性，后通过"Set-Cookie"给浏览器发送3个Cookie，其中一个是用来保存登陆信息的

2. 打开"用户中心"： http://piaoweb.sstm.org.cn/user/center/orderlist

抓包后可以看到，HTTP Request中会带上Cookie(即上一步中Web服务器返回的Cookie)，这样We服务器就认为浏览器是登陆状态

Cookie的属性

从Fiddler的抓包中，可以看到Web服务器返回了下面一段数据给浏览器

cookie_user_token=83AC4E4F5A788CA4E70C62707CE400DE; Expires=Tue, 21-May-2019 04:1:05 GMT; Path=/; HttpOnly

1. Expires属性：Expires的值是一个时间，代表过期时间。即超过这个时间该Cookie就失效了(如果指定Expires time，即表示关闭浏览器/页面的时候，Cookie就应该被浏览器上除了)
2. Path属性：表示Cookie所属的路径，asp.net默认为"/"，就是根目录。

在同一个服务器上的目录如下：/test/、/test/cd/、/test/dd/。假设一个Cookie1的Path为/test/，Cokie2的Path为/test/cd/，那么test下的所有页面都可以访问到Cookie1.而/test/dd/的子页面不能访

Cookie2。因为Cookie只能让其Path路径下的页面访问。

3. HttpOnly属性：将一个Cookie设置为HttpOnly后，通过Javascript脚本将无法读取到Cookie信息这能有效地防止XSS攻击

(一般来说，跟登陆相关的Cookie必须设置为HttpOnly)

Cookie分类

可以大致分为2类：会话Cookie和持久Cookie

- 会话Cookie是一种临时的Cookie，它记录了用户访问站点，它记录了用户访问站点时的设置和偏；关闭浏览器，会话Cookie就被删除了
- 持久Cookie存储在硬盘上，不管浏览器退出或计算机重启，持久Cookie都继续存在。持久Cookie过期时间

Cookie保存在哪里

Cookie是存在硬盘上的，不同浏览器，不同操作系统存储Cookie的地方可能不一样

网站自动登陆的原理

很多网站都有自动登陆的功能，以"博客园自动登录"为例来说明Cookie是如何传递的

在登录页面输入用户名密码，选择保存密码单击登录(这时你的机器上已保存好了登陆的Cookie)

1. 打开浏览器输入 www.cnblogs.com
2. 浏览器会在硬盘中查找关于cnblogs.com的Cookie，然后把Cookie放到HTTP Request中，再把Request发送给Web服务器
3. Web服务器返回页面，这时你会看到自己已经登陆了