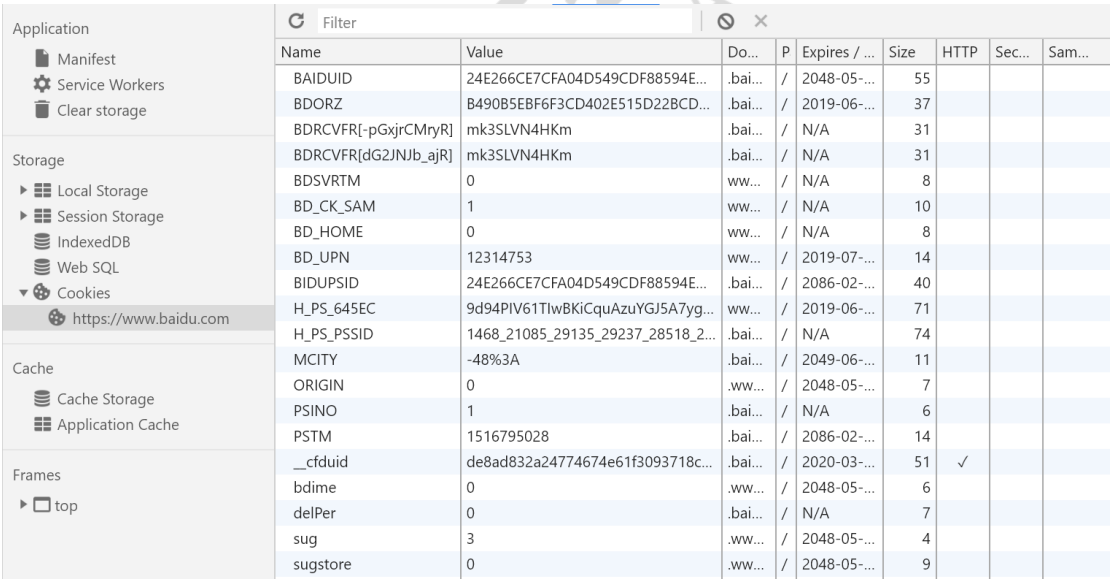
对于 Cookie 你了解多少

ookie 在 web 开发中时常被用到，也是面试官喜欢问的一块技术，很多人只知其一不知其二，谈起 web 存储，都会答 localStorage、sessionStorage、还有就是 cookie，然后一些区别啊什么的倒背如流，cookie 的优缺点也了然于心，但是当你看完这块内容之后，你会对 cookie 有另外独到的见解，希望以后问到这块技术，或者项目中遇到这个你都会处理，我在实习的过程中，一直在用，所以它真的不是口头说说的那么简单，让我们进入 cookie 的世界。

cookie 是什么?

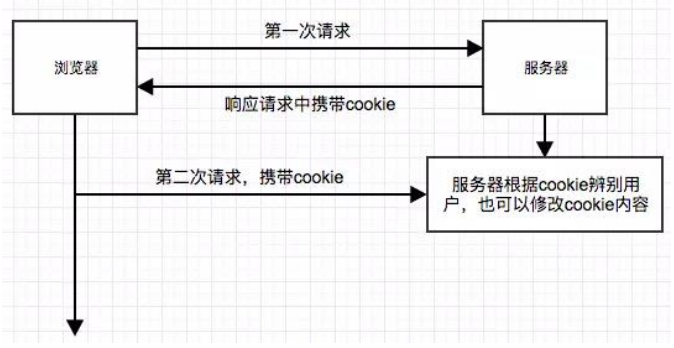
这个讲起来很简单，了解 http 的同学，肯定知道，http 是一个不保存状态的协议，什么叫不保存状态，就是一个服务器是不清楚是不是同一个浏览器在访问他，在 cookie 之前，有另外的技术是可以解决，这里简单讲一下，就是在请求中插入一个 token，然后在发送请求的时候，把这个东西带给服务器，这种方式是易出错，所以有了 cookie 的出现



Name	Value	Do...	P	Expires / ...	Size	HTTP	Sec...	Sam...
BAIDUID	24E266CE7CFA04D549CDF88594E...	.bai...	/	2048-05-...	55			
BDORZ	B490B5EBF6F3CD402E515D22BCD...	.bai...	/	2019-06-...	37			
BDRCVFR[-pGxjrCMryR]	mk3SLVN4HKm	.bai...	/	N/A	31			
BDRCVFR[dG2JNJb_ajR]	mk3SLVN4HKm	.bai...	/	N/A	31			
BDSVRTM	0	ww...	/	N/A	8			
BD_CK_SAM	1	ww...	/	N/A	10			
BD_HOME	0	ww...	/	N/A	8			
BD_UPN	12314753	ww...	/	2019-07-...	14			
BIDUPSID	24E266CE7CFA04D549CDF88594E...	.bai...	/	2086-02-...	40			
H_PS_645EC	9d94PIV61TIwBKiCquAzuYGJ5A7yg...	ww...	/	2019-06-...	71			
H_PS_PSSID	1468_21085_29135_29237_28518_2...	.bai...	/	N/A	74			
MCITY	-48%3A	.bai...	/	2049-06-...	11			
ORIGIN	0	.ww...	/	2048-05-...	7			
PSINO	1	.bai...	/	N/A	6			
PSTM	1516795028	.bai...	/	2086-02-...	14			
__cfduid	de8ad832a24774674e61f3093718c...	.bai...	/	2020-03-...	51	✓		
bdime	0	.ww...	/	2048-05-...	6			
delPer	0	.bai...	/	N/A	7			
sug	3	.ww...	/	2048-05-...	4			
sugstore	0	.ww...	/	2048-05-...	9			

cookie 是什么，cookie 就是一种浏览器管理状态的一个文件，它有 name，也有 value，后面那些看不见的是 Domain、path 等等，我们后面会介绍

cookie 原理



第一次访问网站的时候，浏览器发出请求，服务器响应请求后，会将 cookie 放入到响应请求中，在浏览器第二次发请求的时候，会把 cookie 带过去，服务端会辨别用户身份，当然服务器也可以修改 cookie 内容。

cookie 的属性

name
这个显而易见，就是代表 cookie 的名字的意思，一个域名下绑定的 cookie，name 不能相同，相同的 name 的值会被覆盖掉，有兴趣的同学可以试一试，我在项目中切实用到过
value
这个就是每个 cookie 拥有的一个属性，它表示 cookie 的值，但是我在这里想说的不是这个，有以下几种说法，如下：
1.cookie 的值必须被 URL 编码。
2.对 cookie 的值进行编码不是必须的，还举了原始文档中所说的，仅对三种符号必须进行编码：分号、逗号和空格。
3. 由于 cookie 规定是名称/值是不允许包含分号，逗号，空格的，所以为了不给用户到来麻烦，考虑服务器的兼容性，任何存储 cookie 的数据都应该被编码。

domain

这个是指的域名，这个代表的是，cookie 绑定的域名，如果没有设置，就会自动绑定到执行语句的当前域,还有值得注意的点,统一个域名下的二级域名也是不可以交换使用 cookie 的，比如，你设置 www.baidu.com 和 image.baidu.com,依旧是不能公用的
path
path 这个属性默认是'/'，这个值匹配的是 web 的路由，举个例子：
//默认路径
www.baidu.com
//blog 路径
www.baidu.com/blog

cookie 的有效期

Expires / Max-Age
2048-05-27T03:42:15.000Z
2019-06-29T02:34:39.337Z

什么是有效期，就是图中的 Expires 属性，一般浏览器的 cookie 都是默认储存的，当关闭浏览器结束这个会话的时候，这个 cookie 也就会被删除，这就是上图中的——session(会话储

存)。
如果你想要cookie存在一段时间，那么你可以通过设置Expires属性为未来的一个时间节点，Expires 这个是代表当前时间的，这个属性已经逐渐被我们下面这个主人公所取代——Max-Age
Max-Age，是以秒为单位的，Max-Age 为正数时，cookie 会在 Max-Age 秒之后，被删除，当 Max-Age 为负数时，表示的是临时储存，不会生出 cookie 文件，只会存在浏览器内存中，且只会在打开的浏览器窗口或者子窗口有效，一旦浏览器关闭，cookie 就会消失，当 Max-Age 为 0 时，又会发生什么呢，删除 cookie，因为 cookie 机制本身没有设置删除 cookie，失效的 cookie 会被浏览器自动从内存中删除，所以，它实现的就是让 cookie 失效。

Secure

这个属性译为安全，http 不仅是无状态的，还是不安全的协议，容易被劫持，打个比方，你在手机端浏览网页的时候，有没有中国移动图标跳出来过，闲言少叙，当这个属性设置为 true 时，此 cookie 只会在 https 和 ssl 等安全协议下传输

提示：这个属性并不能对客户端的 cookie 进行加密，不能保证绝对的安全性

HttpOnly

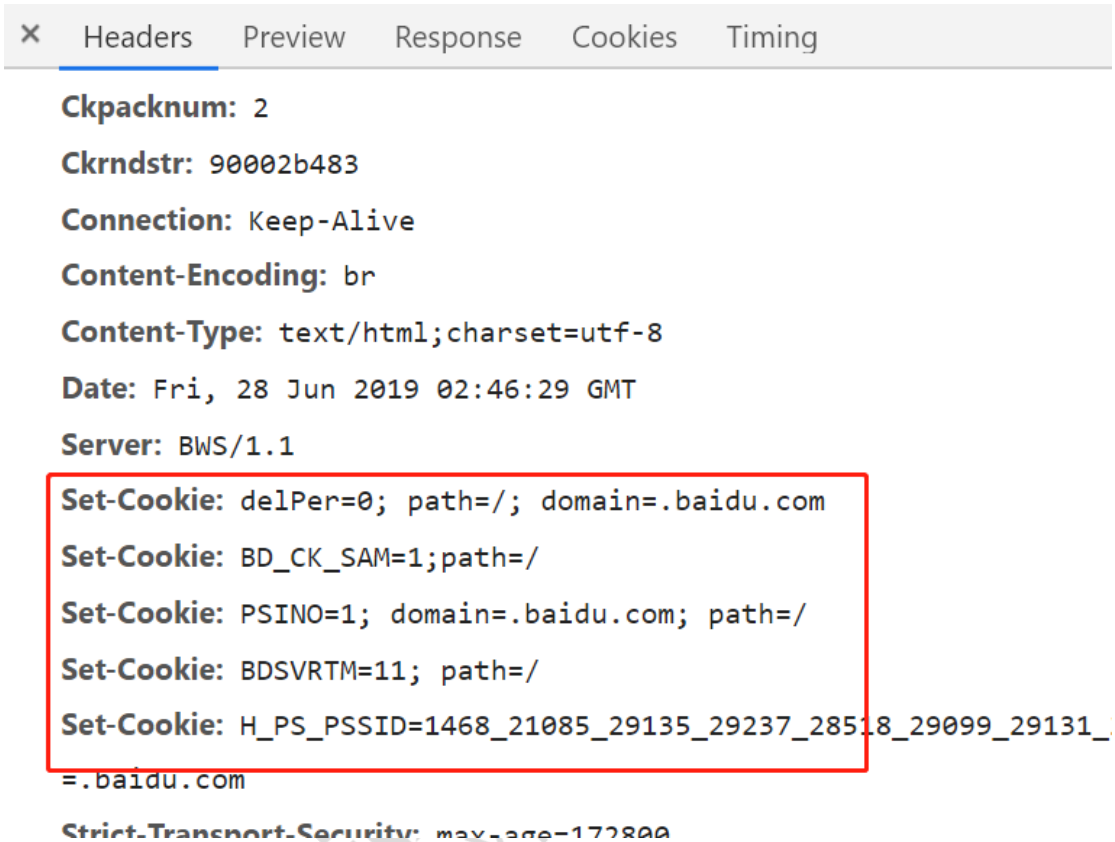
这个属性是面试的时候常考的，如果这个属性设置为 true，就不能通过 js 脚本来获取 cookie 的值，能有效的防止 xss 攻击,看 MDN 的官方文档：

> To prevent cross-site scripting (XSS) attacks, `HttpOnly` cookies are inaccessible to JavaScript's `Document.cookie` API; they are only sent to the server. For example, cookies that persist server-side sessions don't need to be available to JavaScript, and the `HttpOnly` flag should be set.

关于 js 操作 cookie
document.cookie 可以对 cookie 进行读写，看一下两条指令：

```
//读取浏览器中的 cookie
console.log(document.cookie);
//写入 cookie
document.cookie='myname=laihuamin;path=/;domain=.baidu.com';
```

服务端如何去设置 cookie
关于怎么设置 cookie，我们只要打开控制台，看一个 http 的请求头和响应头中的东西即可明白：



服务端就是通过 setCookie 来设置 cookie 的，注意点，要设置多个 cookie 时，得多写几个 setCookie。对于 cookie 的发送，是浏览器的默认行为，当我们进行请求时。自动携带 cookie。