登录注册中的cookie

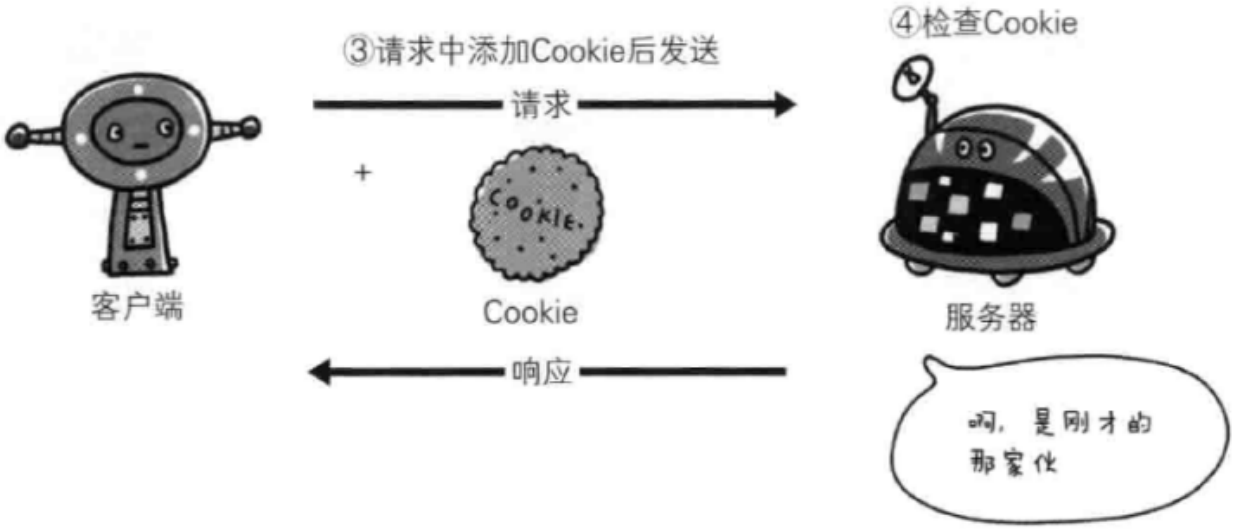
cookie 俗称夹心饼干。它是服务器和浏览器之间传递的少量数据。

cookie的主要作用：

因为HTTP协议是无状态的，对于一个浏览器发出的多次请求，WEB服务器无法区分是不是来源于同一个浏览器。所以，需要额外的数据用于维护会话。
Cookie 正是这样的一段随HTTP请求一起被传递的额外数据。

Cookie技术通过在请求和响应报文中写入Cookie信息来控制客户端的状态。Cookie会根据从服务器端发送的响应报文内一个叫做 Set-Cookie 的首部字段信息，通知客户端保存Cookie。当下次客户端再次向该服务器发送请求时，客户端会自动在请求报文中加入Cookie值。服务器端发现客户端发送过来的Cookie后，会去检查究竟是从哪一个客户端发来的连接请求，然后对比服务器上的记录，最后得到之前的状态信息。
简单过程如下示例图：
1）第1次没有Cookie信息状态下发送请求

2）第2次存在Cookie信息状态后发送请求：



上面示图展示了发生Cookie交互的情景，HTTP请求报文和响应报文的内容如下：

1）请求报文（没有Cookie信息的状态）

GET /reader/ HTTP/1.1

Host: hackr.jp

2）响应报文（服务器端生成Cookie信息）

HTTP/1.1 200 OK

Date: Thu, 12 Jul 2012 05:45:32 GMT

Server: Apache

< Set-Cookie: sid=1342077140226724; path=/; ..... >

Content-Type: text/plain; charset=UTF-8

3)请求报文（自动发送保存着的Cookie信息）

GET /image/ HTTP/1.1

Host: hackr.jp

Cookie: sid=1342077140226724

Cookie存在哪里

Cookie是存在硬盘上， IE存cookie的地方和Firefox存cookie的地方不一样。不同的操作系统也可能存cookie的地方不一样。

不同的浏览器会在各自的独立空间存放Cookie, 互不干涉

你也可以这样找, 打开IE，点击Tools->Internet Options->General Tab下的->Browsing history下的Setting按钮，弹出的对话框中点击View files.

cookie的主要属性：

1、name COOKIE的名字

2、value COOKIE对应的值

3、domain 域名 就是说这个COOKIE对应哪一个域名有效

4、path 路径 ， COOKIE对应的哪一个路径才会有效

5、expires/Max-Age 字段为此cookie超时时间。若设置其值为一个时间，那么当到达此时间后，此cookie失效。不设置的话默认值是Session，意思是cookie会和session一起失效。当浏览器关闭(不是浏览器标签页，而是整个浏览器) 后，此cookie失效。

从服务器端，发送cookie给客户端，是对应的Set-Cookie。包括了对应的cookie的名称，值，以及各个属性。

从客户端发送cookie给服务器的时候，是不发送cookie的各个属性的，而只是发送对应的名称和值。

例如：

GET /spec.html HTTP/1.1

Host: www.example.org

Cookie: name=value; name2=value2

举一个例子，看看我们的浏览器怎么样去决定要带哪些COOKIE值，假设浏览器有如下COOKIE值

Set-Cookie: id=123456789; expires=Wed, 25-Apr-2018 06:04:48 GMT; domain = 119.29.100.135 path=/pro/

如下四个请求：

1、http://119.29.100.138:/pro/

2、http://119.29.100.135:/pro/

3、http://119.29.100.135:/pro/test/

4、http://119.29.100.135:/pro11/

结果：

2、3访问的时候会带上对应的COOKIE id =123456789

1、不会带上因为域名不对

4、不会带上因为路径不对

不同的网站会有不同的cookie文件

网站自动登陆的原理

我们以”博客园自动登陆“的例子，来说明cookie是如何传递的。

大家知道博客园是可以自动登陆的。 如下图，这个是什么原理呢?

假如我已经在登陆页面输入了用户名，密码，选择了保存密码，登陆。

（这时候，其实在你的机器上保存好了登陆的cookie, 不信你可以按照上节介绍方法去你的电脑上找下博客园的cookie）

当我下次访问博客园流程如下。

1. 用户打开IE浏览器，在地址栏上输入www.cnblogs.com.
2. IE首先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发给Web服务器。
3. Web服务器返回博客园首页（你会看到你已经登陆了）。

截获Cookie，冒充别人身份

通过上面这个例子，可以看到cookie是很重要的，识别是否是登陆用户，就是通过cookie。 假如截获了别人的cookie是否可以冒充他人的身份登陆呢？ 当然可以， 这就是一种黑客技术叫Cookie欺骗。
利用Cookie 欺骗， 不需要知道用户名密码。就可以直接登录，使用别人的账户做坏事。
我知道有两种方法可以截获他人的cookie，
1. 通过XSS脚步攻击， 获取他人的cookie.
2. 想办法获取别人电脑上保存的cookie文件（这个比较难）

拿到cookie后，就可以冒充别人的身份了。