OAuth2.0认证和授权原理

什么是OAuth授权？

**一、什么是OAuth协议**

OAuth(开放授权)是一个开放标准。

允许第三方网站在用户授权的前提下访问在用户在服务商那里存储的各种信息。

而这种授权无需将用户提供用户名和密码提供给该第三方网站。

OAuth允许用户提供一个令牌给第三方网站，一个令牌对应一个特定的第三方网站，同时该令牌只能在特定的时间内访问特定的资源。

**二、OAuth的原理和授权流程**

OAuth的认证和授权的过程中涉及的三方包括：

服务商：用户使用服务的提供方，一般用来存消息、储照片、视频、联系人、文件等(比如Twitter、Sina微波等)。

用  户：服务商的用户

第三方：通常是网站，该网站想要访问用户存储在服务商那里的信息。

比如某个提供照片打印服务的网站，用户想在那里打印自己存在服务商那里的网络相册。

在认证过程之前，第三方需要先向服务商申请第三方服务的唯一标识。

OAuth认证和授权的过程如下:

1、用户访问第三方网站网站，想对用户存放在服务商的某些资源进行操作。

2、第三方网站向服务商请求一个临时令牌。

3、服务商验证第三方网站的身份后，授予一个临时令牌。

4、第三方网站获得临时令牌后，将用户导向至服务商的授权页面请求用户授权，然后这个过程中将临时令牌和第三方网站的返回地址发送给服务商。

5、用户在服务商的授权页面上输入自己的用户名和密码，授权第三方网站访问所相应的资源。

6、授权成功后，服务商将用户导向第三方网站的返回地址。

7、第三方网站根据临时令牌从服务商那里获取访问令牌。

8、服务商根据令牌和用户的授权情况授予第三方网站访问令牌。

9、第三方网站使用获取到的访问令牌访问存放在服务商的对应的用户资源。

**三、目前支持OAuth的网站有哪些？**

t.sina.com.cn

t.qq.com

t.sohu.com

t.163.com

www.douban.com

www.twitter.com

www.facebook.com

Google Buzz

文件来源于： <http://www.6zou.net/tech/what_is_oauth.html>

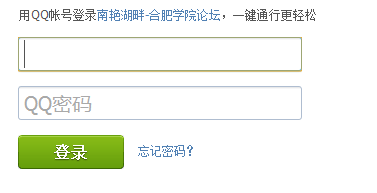
所谓OAuth（即Open Authorization，开放授权），它是为用户资源授权提供了一种安全简单的标准，也就是说用户在访问第三方web或应用的时候，第三方不会知道用户的信息（登录密码等），现在基本都支持OAuth2.0版本了。

首先来看看我们在第三方使用oauth流程如下：

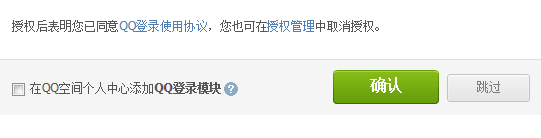
第一步：用户登录第三方网站，使用qq登录。



第二步：点击登录后，会跳到qq平台提示输入用户名和密码。



第三步：如果用户名和密码正确，会提示是否接受授权，如果授权成功，第三方网站就能访问你的资源了，qq头像、用户名等

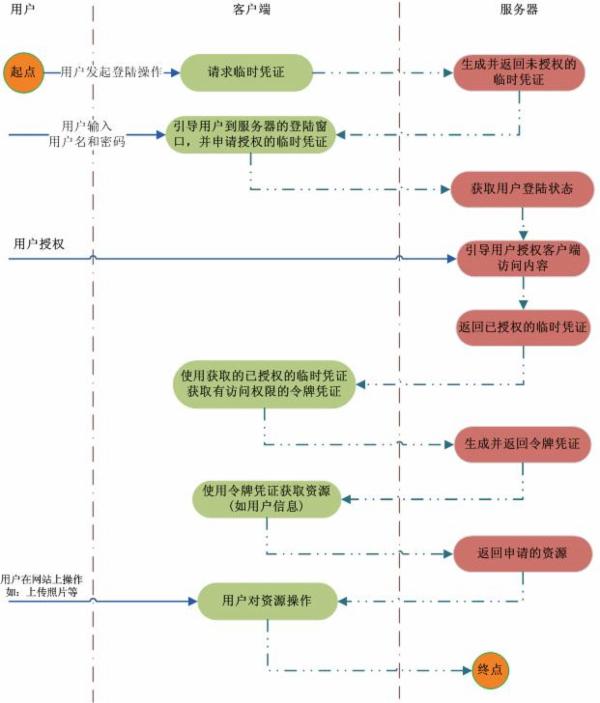


认证和授权过程（包括三方）

1、服务提供方，用户使用服务提供方来存储受保护的资源，如照片，视频，联系人列表。

2、用户，存放在服务提供方的受保护的资源的拥有者。

3、客户端，要访问服务提供方资源的第三方应用，通常是网站。在认证过程之前，客户端要向服务提供者申请客户端标识。

       用户访问客户端的网站，想操作用户存放在服务提供方的资源。

客户端向服务提供方请求一个临时令牌。

服务提供方验证客户端的身份后，授予一个临时令牌。

客户端获得临时令牌后，将用户引导至服务提供方的授权页面请求用户授权。在这个过程中将临时令牌和客户端的回调连接发送给服务提供方。

用户在服务提供方的网页上输入用户名和密码，然后授权该客户端访问所请求的资源。

授权成功后，服务提供方引导用户返回客户端的网页。

客户端根据临时令牌从服务提供方那里获取访问令牌。

服务提供方根据临时令牌和用户的授权情况授予客户端访问令牌。

客户端使用获取的访问令牌访问存放在服务提供方上的受保护的资源。