# 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

## 2.1、OAuth 1.0的认证流程

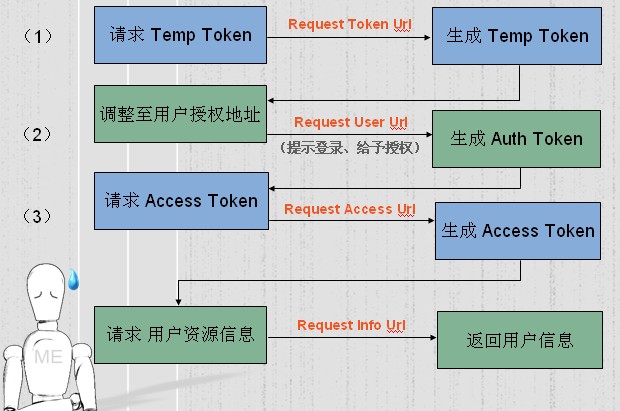
　　在OAuth 1.0认证中会用到三个重要的Url：

　　第一个：Request Token Url，获取未授权的Token的Url；

　　第二个：User Authorization Url，请求用户对Token进行授权的Url；

　　第三个：Request Access Url，使用Token获取Access Token的Url。

上面是认证流程中用到的三个Url，在下面的流程示意图中会体现到，这是我讲解OAuth幻灯片的一页，直接截图下来进行讲解：



　　第一步：网站向认证平台请求一个未授权的Token，这个Request Token Url是前面说的第一个Url；

　　第二步：跳转至用户授权页面，提示用户进行登录，并进行授权，返回获得已授权的Token，用到的User Authorization Url是前面说的第二个Url；

　　第三步：通过已授权的Token，向认证平台请求Access Token(数据令牌)，用到的Request Access Url是前面说的第三个Url，返回后到这步整个认证流程就结束了，最后一步，是通过数据令牌等参数，调用接口获取用户信息，不完全算认证的流程。（

## 2.1、OAuth2.0的认证流程

　　在OAuth2.0的处理流程，主要分为以下四个步骤：

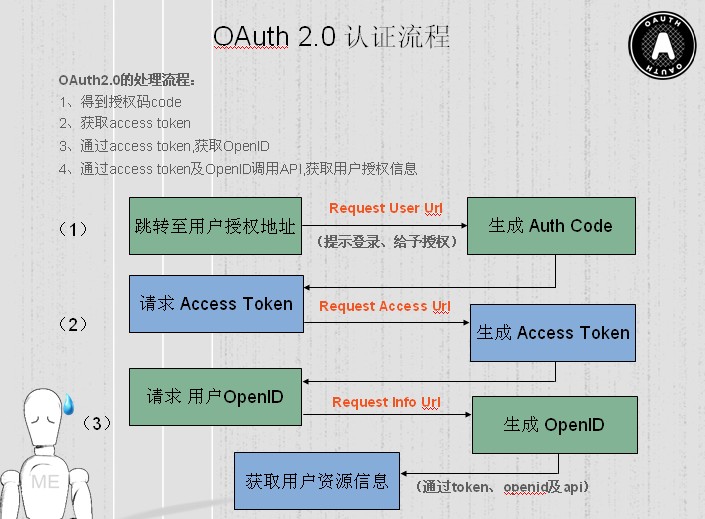
　　1）得到授权码code

　　2）获取access token

　　3）通过access token，获取OpenID

　　4）通过access token及OpenID调用API，获取用户授权信息

上面是流程的大概四个步骤，在下面的流程示意图中会得到体现，这是我制作的一个幻灯片的流程图（文章最后会附上制作的OAuth幻灯片分享给大家），这里就直接截图下来进行讲解：



　　第一步：首先直接跳转至用户授权地址，即图示 Request User Url ，提示用户进行登录，并给予相关资源授权，得到唯一的Auth code，这里注意的是code只有10分钟的有效期，对于安全考虑，相对于OAuth 1.0省了一步获取临时的Token，并且有效期也进行了控制，比1.0认证简化了很多，并安全一些；

　　第二步：得到授权code后，这一步就是请求access token，通过 图示 Request access url ，生成得到数据Token；

　　第三步：通过Access Token请求OpenID，OpenID是用户在此平台的唯一标识，通过图示 Request info url 请求，然后得到OpenID；

　　第四步：通过第二步得到的数据Token、第三步得到的OpenID及相关API，进行请求，获取用户授权资源信息。（我喜欢简洁明了，OAuth2.0认证流程就是这样，相信通过图示及讲解都能明白，若有不明白之处请留言）

# 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