认识 Oauth2

作者：luofeng0603
原文链接：https://ld246.com/article/1683298031956
来源网站：链滴

前言

最近项目中用到了oauth2，所以就来简单研究一下

什么是Oauth

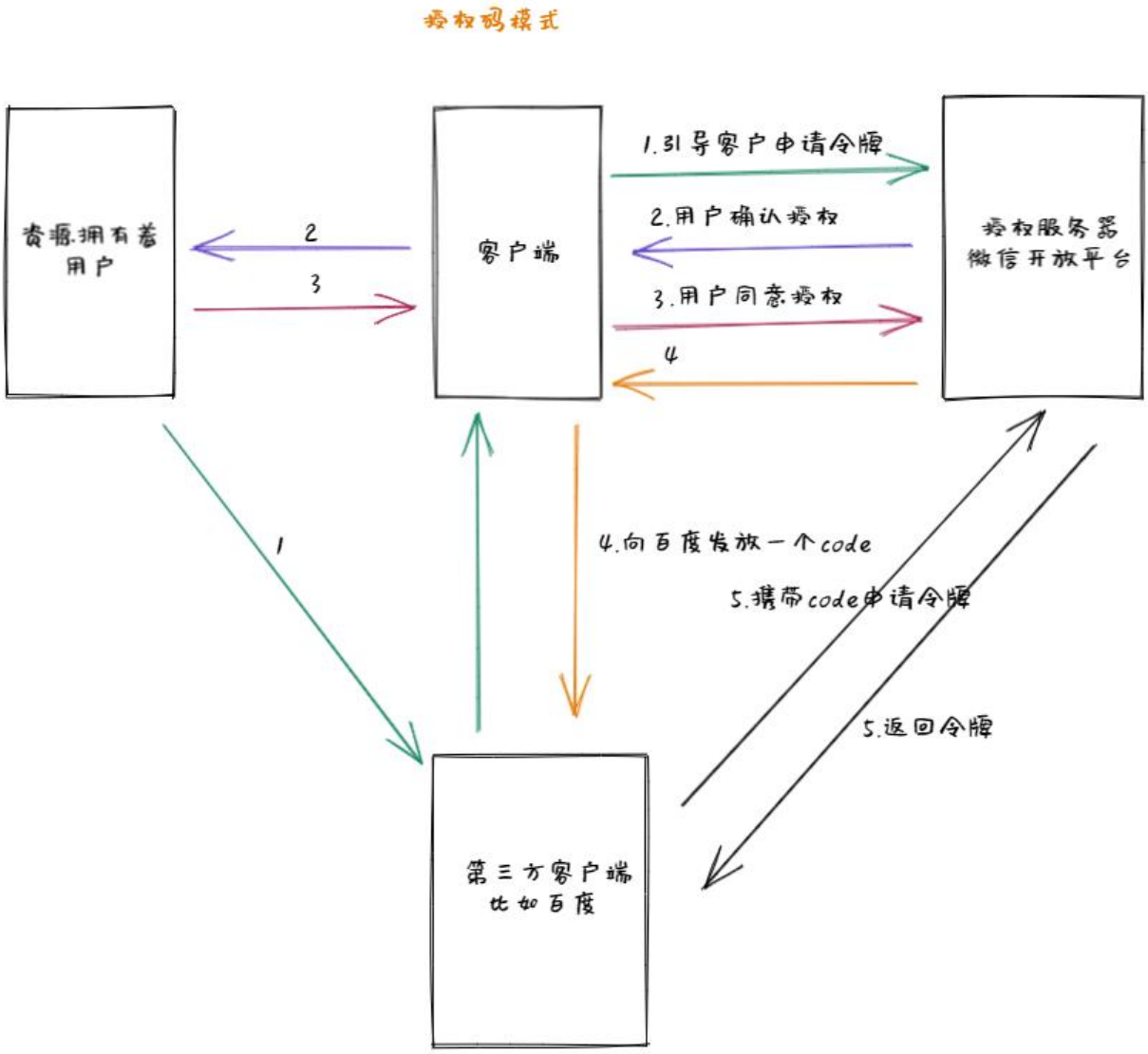
Oauth是一种开放标准，允许用户授权第三方应用程序访问他们存储在另外的服务提供者上的信息，不需要将用户名和密码提供给第三方应用或分享他们数据的所有内容。

简单来说就是允许我们将之前的授权和认证过程交给一个独立的第三方来完成，相当于解耦了。

oauth2.0的四种认证方式

1.授权码模式

授权码模式画个图简单理解一下：



图中的几个参与角色：

资源拥有者，通常就是用户自己了，拥有核心资源，比如微信账号

第三方应用，比如 百度

客户端通常就是浏览器或者手机app

还有一个授权服务器，比如微信开放平台，负责担保

整个流程大概如下：当用户访问百度的时候，百度引导用户去申请一个令牌，也就是去授权服务器申一个令牌， 会返回给用户一个链接，其实是微信开放平台返回的一个链接，这个链接包含了百度的相信息，用户访问了这个链接之后，就可以用微信账号，在开放平台上进行登录，登录之后会有一个确页面，用户可以选择同意授权或者不同意授权， 如果用户选择同意，这个时候会发请求给微信开放平，微信平台就会返回一个code授权码，这个时候百度就拿到这个授权码，但是不能直接使用，而且拿这个授权码去微信开放平台换取token，通过token完成自己的登录逻辑。

这种方式很安全，你看微信都是这么在用的，不过略显复杂。所以还有一种简化模式。

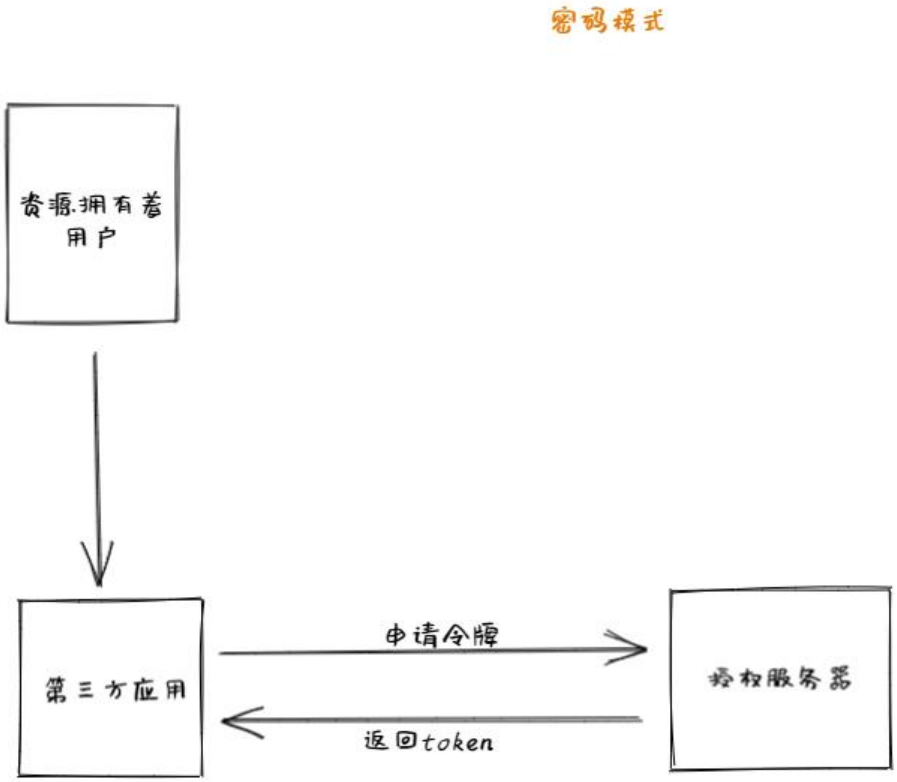
2.简化模式

简化模式就是把授权码模式中的第五步删掉。用户同意之后直接颁发的就是token，不用再拿code去取token了。

简化模式主要是考虑到很多应用没有自己的服务器，所以没办法去做第五步。淘宝开放平台就是使用简化模式。

3.密码模式

这个就比较简单了，看图：



用户把用户名和密码给第三方，第三方拿着你的用户名和密码去获取token。这种模式在互联网上用比较少，资源拥有者对第三应用有绝对的信任才会用这种模式。

4.客户端模式

客户端模式更简单，看图

原文链接：认识 Oauth2

第三方应用给授权服务器一个标识，就是标识自己身份的东西，然后就返回token。

总体来说呢，就授权码最复杂，这种模式里面涉及到了三方互信，资源拥有者/第三方应用/授权服务这三者互不信任，所以两两之间都必须确认。

简化模式呢，授权服务器和第三方应用有信任，所以就省略他们之间的确认。

密码默认呢是在上面的基础上，资源拥有者和第三方之间比较信任，所以又省了一步。

客户端模式代表了这三方都是比较信任的，适合内部应用。