# 1.什么是Auth2

目前最流行的授权机制，用来授权第三方应用，获取用户数据。简单说，OAuth 就是一种授权机制。数据的所有者告诉系统，同意授权第三方应用进入系统，获取这些数据。系统从而产生一个短期的进入令牌（token），用来代替密码，供第三方应用使用。

# 2.OAuth 2.0 的核心

OAuth 的核心就是向第三方应用颁发令牌。OAuth 2.0 规定了四种获得令牌的流程。你可以选择最适合自己的那一种，向第三方应用颁发令牌。

# 3. OAuth 2.0获取令牌的方式

授权码（authorization-code）

隐藏式（implicit）

密码式（password）：

客户端凭证（client credentials）

不管哪一种授权方式，第三方应用申请令牌之前，都必须先到系统备案，说明自己的身份，然后会拿到两个身份识别码：客户端 ID（client ID）和客户端密钥（client secret）。这是为了防止令牌被滥用，没有备案过的第三方应用，是不会拿到令牌的。

# 4.Oauth2.0四种授权方式的应用场景

**1.授权码（authorization code）方式**，指的是第三方应用先申请一个授权码，然后再用该码获取令牌。

这种方式是**最常用的流程**，**安全性也最高**，它适用于那些有后端的 Web 应用。授权码通过前端传送，令牌则是储存在后端，而且所有与资源服务器的通信都在后端完成。这样的前后端分离，可以避免令牌泄漏。

**2. 隐藏式（implicit）方式,** 这种方式**允许直接向前端颁发令牌**。这种方式没有授权码这个中间步骤，所以称为（授权码）"隐藏式"（implicit），有些 Web 应用是纯前端应用，没有后端。这时就不能用上面的方式了，必须将令牌储存在前端。

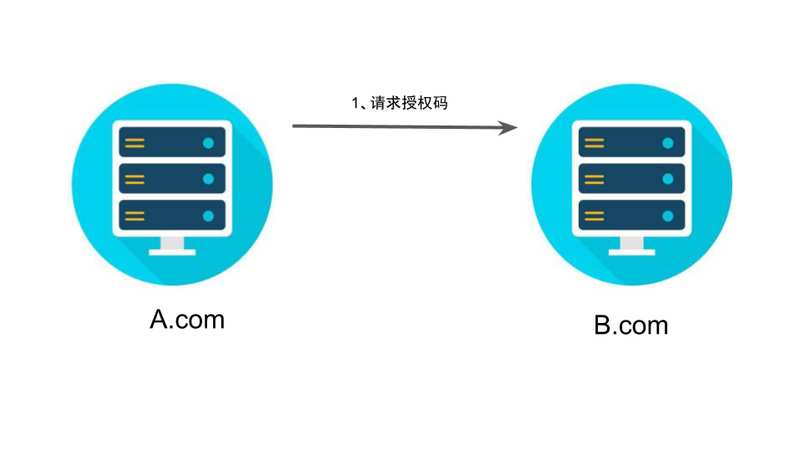
**3. 密码式（password）,** 如果你高度信任某个应用，OAuth也允许用户把用户名和密码，直接告诉该应用。该应用就使用你的密码，申请令牌，这种方式称为"密码式"（password）。

**4.凭证式（client credentials）**，适用于没有前端的命令行应用，即在命令行下请求令牌。

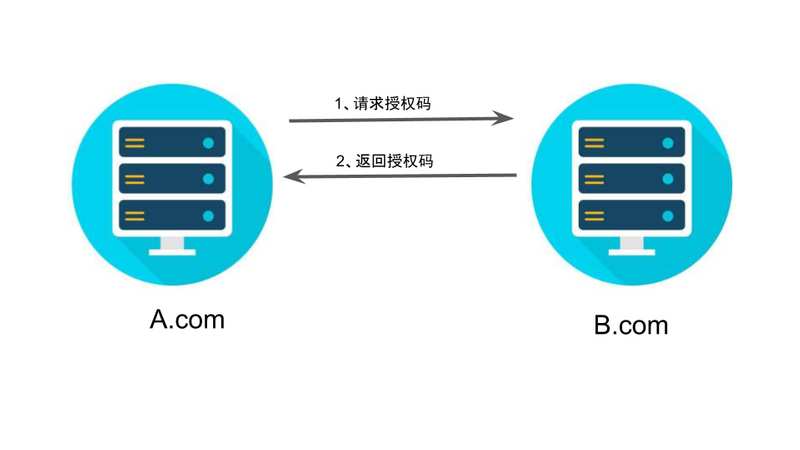
如何实现

授权码方式

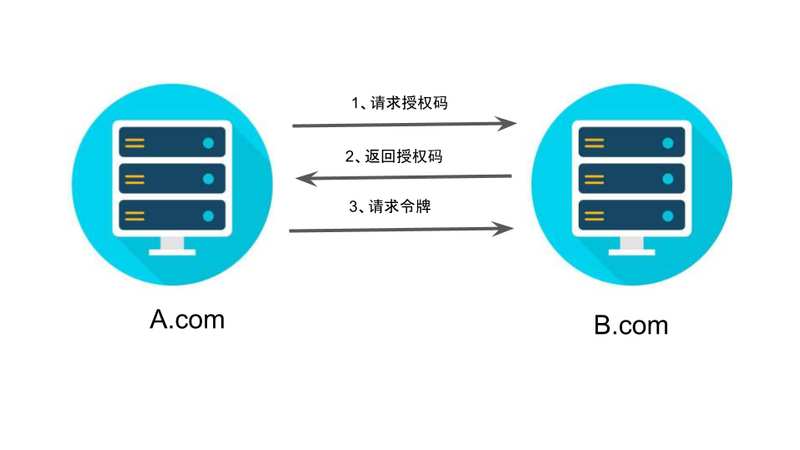
1. 第一步，A 网站提供一个链接，用户点击后就会跳转到 B 网站，授权用户数据给 A 网站使用。



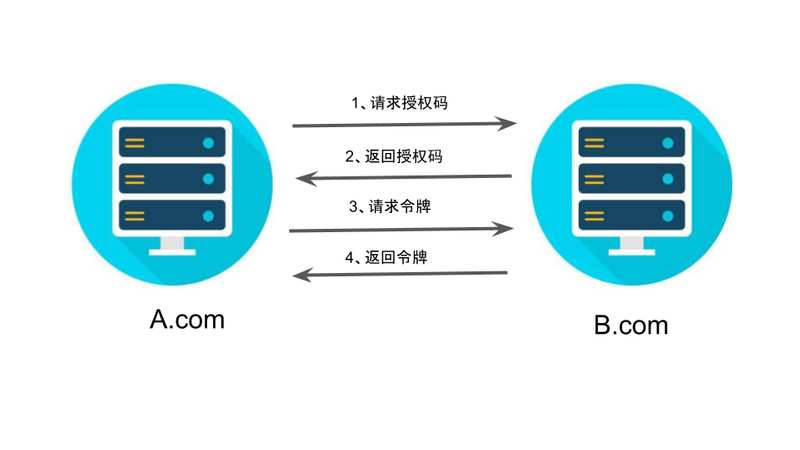
1. 用户跳转后，B 网站会要求用户登录，然后询问是否同意给予 A 网站授权。用户表示同意，这时 B 网站就会跳回redirect\_uri参数指定的网址。跳转时，会传回一个授权码；



1. A 网站拿到授权码以后，就可以在后端，向 B 网站请求令牌。



1. B 网站收到请求以后，就会颁发令牌。



# 5.SpringCloud整合Auth2

# 6.相关资料:

<http://www.ruanyifeng.com/blog/2019/04/oauth-grant-types.html>

<https://www.cnblogs.com/cjsblog/p/9174797.html>