# OAuth协议

## 网上好文：

[OAuth 2.0 的一个简单解释](http://www.ruanyifeng.com/blog/2019/04/oauth_design.html)

[理解OAuth 2.0](http://www.ruanyifeng.com/blog/2014/05/oauth_2_0.html)

[GitHub OAuth 第三方登录示例教程](http://www.ruanyifeng.com/blog/2019/04/github-oauth.html)

[一张图搞定OAuth2.0](https://www.cnblogs.com/flashsun/p/7424071.html)

[OAuth2.0实战之微信授权篇](https://www.imooc.com/article/17696)

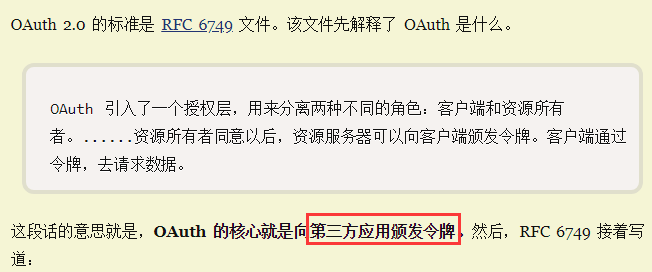
## 京东链接：

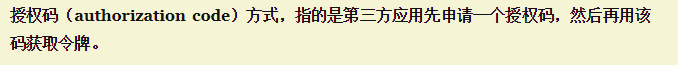
宙斯系统：跳转第三方应用

<http://open.jd.com/home/home#/doc/common?listId=880>

京东不允许直接将openId给第三方用户

## 概念：





## 问答：

1. 我个人感觉需要输入账号密码的都属于四大授权模式中的密码模式吧？授权码模式的过程中是“用户是否同意给予客户端授权”这么一个步骤，你讲得很好，但我感觉豆瓣这个应该是密码模式：

你的理解是不对的，需要输入账号和密码属于那种模式，得看你是把密码输入在豆瓣的页面，还是QQ的页面。如果输入给豆瓣，豆瓣再传给QQ做校验，那是密码模式。但这个案例是从豆瓣页面点击跳转到QQ页面，在QQ页面输入密码，这个密码是不经过豆瓣服务器的，这个是授权码模式。虽然都是输入了用户名密码，但这是有本质区别的。

1. 为什么auth2.0中access\_token不能被直接返回，code可以

因为浏览器的redirect\_uri是一个不安全的信道，虽然HTTPS安全但是可能会存在浏览器的cache或者log文件中，这就给攻击者盗取access\_token带来了很多机会。但authorization\_code不像access\_token那么敏感。因为交换access\_token不仅需要authorization\_code还需要认证client的身份（即app\_id，app\_secret等）

1. 认证失败的自定义异常

[Spring Security Oauth2 自定义 OAuth2 Exception](https://blog.csdn.net/dandandeshangni/article/details/80472147)

# Nonce

# [nonce和timestamp在Http安全协议中的作用](https://www.cnblogs.com/sheseido/p/5944195.html)