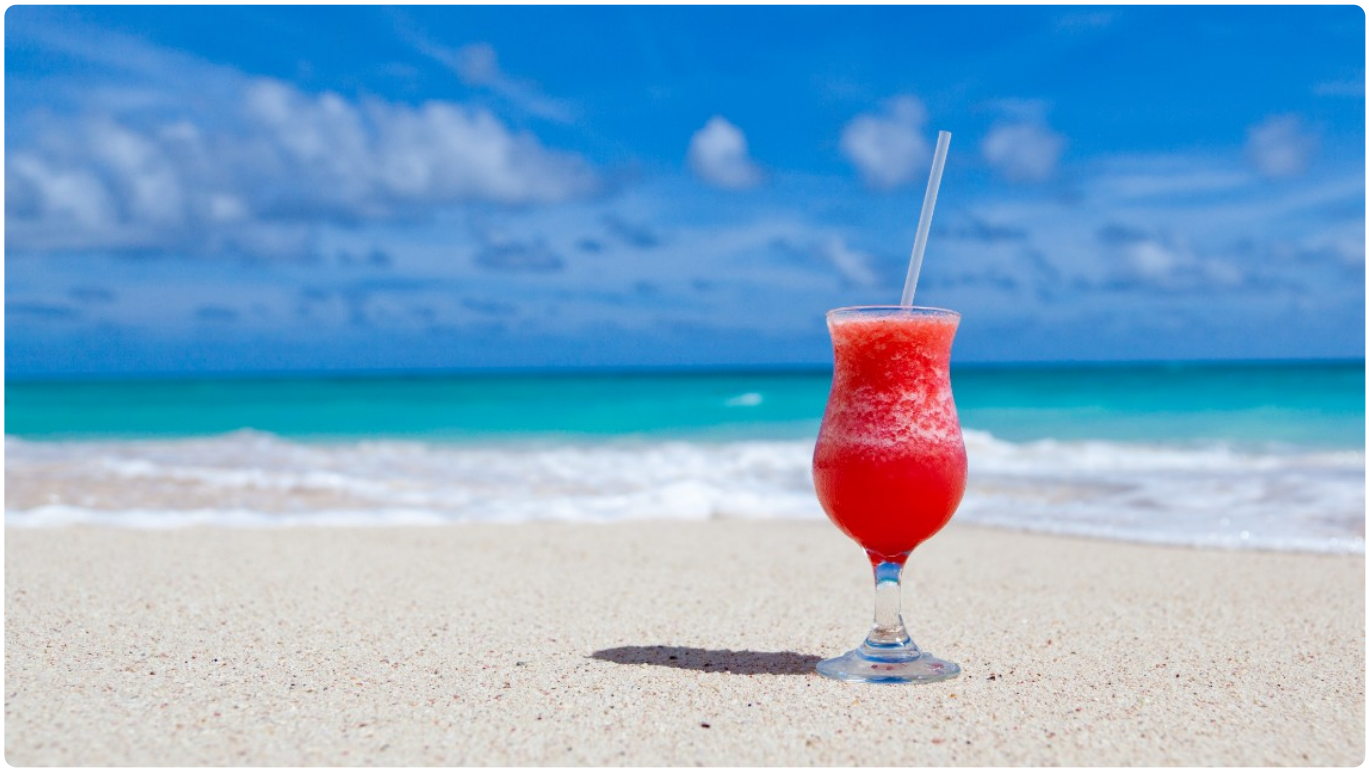
开篇词 | 为什么要学OAuth 2.0?

2020-06-29 王新栋

OAuth 2.0实战课 进入课程 >



讲述：李海明
时长 10:03 大小 9.22M

你好，我是王新栋，是京东的资深架构师，主要负责京东商家开放平台的架构工作。在接下来的时间里，我将带你一起学习 OAuth 2.0 这个授权协议。

我从 2014 年加入京东，便开始接触开放平台相关的技术，主要包括网关、授权两块的内容。在刚开始的几年时间里面，我一直都认为网关是开放平台的核心，起到 “中流砥柱” 的作用，毕竟网关要承载整个开放平台的调用量，同时还要有足够的系统容错能力。

但随着对开放平台理解的不断深入，我们要想在开放平台支持更多样的业务场景，我才发现网关和授权同样重要，相当于开放平台的 “两条腿” 。

而对于授权 “这条腿” ，它不仅要像网关一样要承载访问量，还要同时兼顾业务场景的发展。什么样的业务场景呢？类似的微信登录就是其中之一，越来越多的第三方应用都在向用

户提供使用微信登录的解决方案，来减少用户注册的繁琐操作。而这个解决方案的背后原理，也是我们这门课要讲到的 OAuth 2.0 技术。

OAuth 2.0 是什么?

那，OAuth 2.0 到底是什么呢？我们先从字面上来分析下。OAuth 2.0 一词中的 “Auth” 表示 “授权”，字母 “O” 是 Open 的简称，表示 “开放” ，连在一起就表示 “开放授权” 。这也是为什么我们使用 OAuth 的场景，通常发生在开放平台的环境下。

看到这里，你可能会说应该还有 OAuth 1.0 吧。没错，OAuth 2.0 之前就是 OAuth 1.0。现在，我就来和你说说这两个版本的 OAuth 有什么区别吧。

在 OAuth 1.0 的时候，它有个 “很大的愿望” 就是想用一套授权机制来应对现实中的所有场景，比如 Web 应用场景、移动 App 应用场景、官方应用场景等等，但是这些场景并不是完全相同的。比如官方应用场景，你说还需要让用户来授权吗？如果需要，始终使用一套授权机制给用户带来的体验，是好还是坏呢?

到了 OAuth 2.0 的时候，就解决了 OAuth 1.0 面临的这种“尴尬” 。OAuth 2.0 不再局限于一种授权机制，它扩充了授权许可机制类型，有了授权码许可机制、客户端凭据机制、资源拥有者凭据机制和隐式许可机制。这样的 OAuth 机制就能够很灵活地适应现实中的各种场景，比如移动应用的场景、官方应用的场景，等等。

此外，OAuth 1.0 的弊端还包括安全上的固化攻击等问题，因此 OAuth 1.0 现在已经是废弃状态了。对于我们来讲，直接使用 OAuth 2.0 就可以了。

为什么会有这门课?

但其实呢，OAuth 2.0 并不是一门新的技术，从 2007 年 OAuth 1.0 面世，到 2011 年发布 OAuth 2.0 草案，互联网上已经有很多关于 OAuth 的资料了。所以，在我初次接触 OAuth 2.0 去查阅这些零散的资料时，觉得 OAuth 2.0 很简单啊，不就是授权吗，看两篇文章就够了啊。

但是，看似简单的 OAuth 2.0 却又让我望而却步，在如何使用授权码流程上踌躇不前。比如，在 Web 应用中到底应该怎么使用授权码流程，移动 App 中还能使用授权码流程吗?

当我带着这些问题尝试到网上搜索资料时，那些不成体系的资料着实也让我走了不少弯路。不知道你是不是也被下面问题困扰着：

1. 我要开发一个 Web 应用，当使用 OAuth 2.0 的时候，担心授权码被拦截，却因为没有较好的解决方法而一筹莫展。
2. 我要开发一款移动 App，当使用 OAuth 2.0 的时候，在确定是否需要 Server 端上，花费了大把的时间。

后来我看到《OAuth 2 in Action》这本书，如获至宝。它非常系统地讲解了 OAuth2.0，让我对这个协议框架有了更全面、深刻的认识。也正是这本书给了我足够的勇气，让我能够把自己这些年在开放平台的工作中，所掌握的 OAuth 知识体系梳理一遍。也是在这一刻，我才意识到**只要有了方向，就有了厚度**。

当我开始试着整理出自己这些年掌握的 OAuth 2.0 相关技术、实践，并计划输出的时候，我真真切切地发现，OAuth 2.0 是讲授权没错，但要用对、用好这个协议，绝不是短短两篇文章就能讲清楚的。这也是我做这门课的初衷。

我要结合自己在开放平台上的工作经验以及对 OAuth 2.0 的理解，一次性地给你说透授权这件事儿。同时，我还查阅了诸多资料，包括 OAuth 2 协议规范、OpenID Connect explained等，力求给你带来最贴近本质的 OAuth 2.0 知识的讲解。

这门课是怎么设计的?

在这门课程里，我会分为基础篇和进阶篇两大模块，每个模块都会安排一些实践内容，和你讲清楚 OAuth 2.0。接下来，我就和你解释下为什么要这么安排。

第一部分是基础篇，就是你必须要掌握的 OAuth 2.0 的基础知识。在这一模块中，我会和你细致地讲解授权码许可（Authorization Code）类型的流程，包括 OAuth 2.0 内部组件之间的通信方式，以及授权服务、客户端（第三方软件）、受保护资源服务这三个组件的原理。

在此基础上，我还会为你讲解其他三种常见许可类型，分别是资源拥有者凭据许可（Resource Owner Password Credentials）、隐式许可（Implicit）、客户端凭据许可（Client Credentials）的原理，以及如何选择适合自己实际场景的授权类型。这样一来，

你就能掌握整个 OAuth 2.0 中所有许可类型的运转机制了，并且能够从容地在实际工作环境中使用它们。

为了能够把你带入到 OAuth 2.0 的场景中，方便你理解这些概念、流程，我在讲述这些基础内容的时候，会用一个小明使用第三方“小兔打单软件”来打印自己在京东店铺的订单数据的例子，来贯穿始终。

我可以告诉你的是，学完基础篇的内容，你就可以把 OAuth 2.0 用到实际的工作场景了。

第二部分进阶篇的内容，我会侧重讲一些 OAuth 2.0 “更高级” 的用法，可以让你知道如何更安全地用、扩展地用 OAuth 2.0。

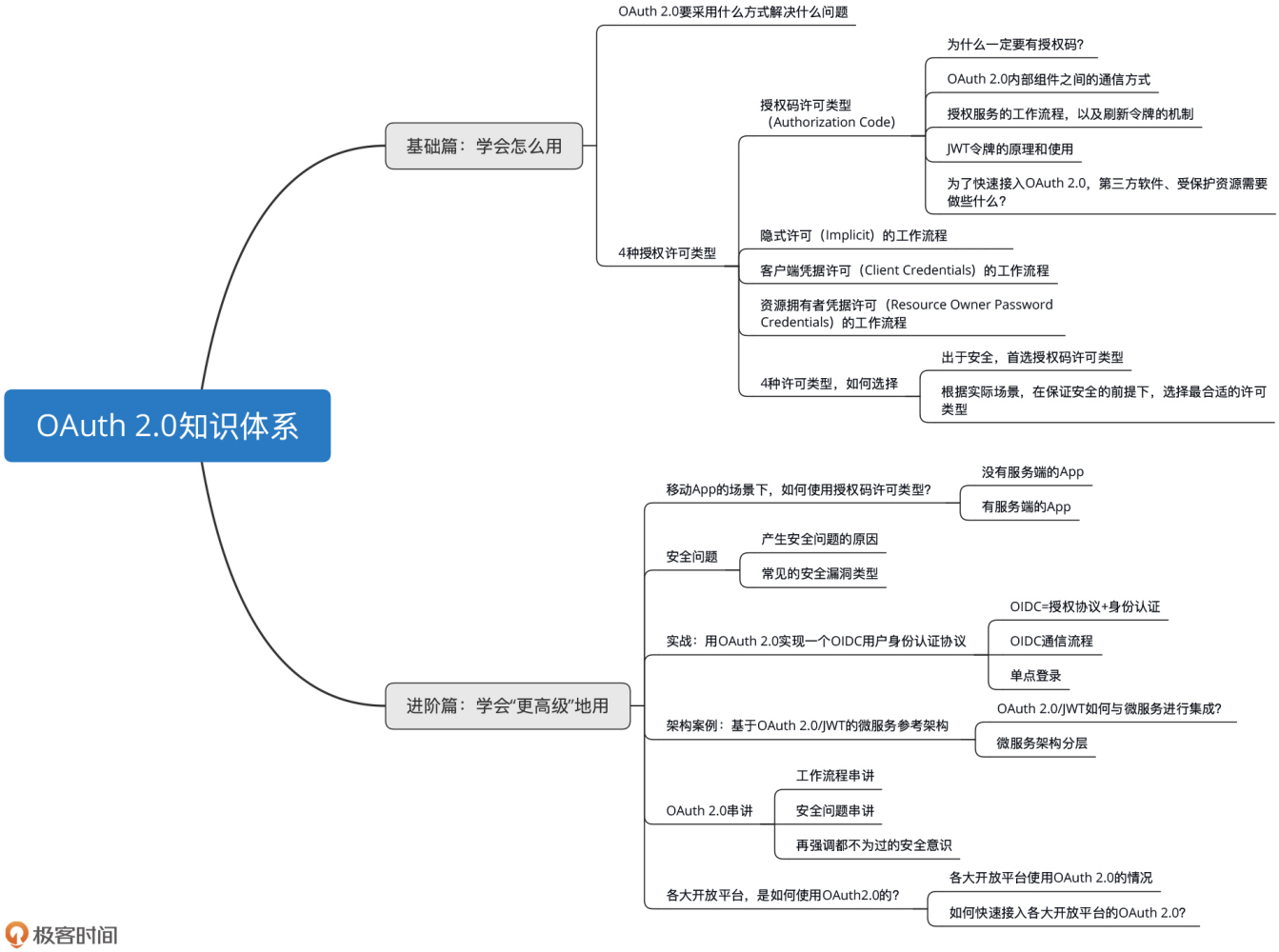
所以，这部分内容会包括如何在移动 App 中使用 OAuth 2.0，因使用不当而导致的 OAuth 2.0 安全漏洞有哪些，以及如何利用 OAuth 2.0 实现一个 OpenID Connect 用户身份认证协议。此外，我还邀请了微服务技术领域的专家杨波老师，给我们分享了一个架构案例，基于 OAuth 2.0/JWT 的微服务参考架构。

最后，为了配合课程的学习，不让理论过于枯燥，也为了学以致用，**我在GitHub上为你准备了一份非常简单、可落地的**通过 Java 语言来实现的代码。

简单的地方在于，代码中除了基本的 Servlet 技术外，我没有引入任何其它的第三方内容。所以，你只要能够理解 Request 和 Response，就能够理解这份代码。

可落地的地方在于，虽然它是一份简单的代码，但它不仅把整个 OAuth 2.0 的组件都跑通了，还包含了实践一个 OIDC 协议的具体实现。当然，我在代码里面还预留了一些 TODO 的地方，你可以结合上下文来自行实践处理。这是一项开源的工程。

在这里，我总结了 OAuth 2.0 的知识体系图，你也可以先了解下整个课程的知识结构。



这样一来，你学完这门课后，便能在互联网的授权领域练就一双“火眼金睛”，可以发现所有使用过 OAuth 2.0 的痕迹，诸如微信登录的场景。这样，即使你不用抓包分析，也能够洞悉它背后的原理，为今后快速熟知互联网的类似场景打下基础。

最后，我还想正式认识一下你。你可以在留言区里做个自我介绍，和我聊聊，你目前学习、使用 OAuth 2.0 的难点、痛点是什么？或者，你也可以聊聊你对 OAuth 2.0、对授权还有哪些独特的思考和体验，欢迎在留言区和我交流讨论。

好了，现在就开启我们的 OAuth 2.0 之旅吧。

下一篇　01 | OAuth 2.0是要通过什么方式解决什么问题?

精选留言 (14)

朱晔
2020-06-29

写留言

分享一个使用Spring Security实现OAuth2三角色+三模式完整例子 https://juejin.im/post/5bdc29e551882517121233f6

展开

2 14

Jaswine
2020-06-29

哈哈哈，看了github上的代码，真的好原生啊，纯servlet和jsp写的，用多了springboot都不知道servlet怎么写了，哈哈哈哈哈

展开

> 作者回复: 本意就是想用“不穿衣服的代码”，排除干扰来讲透OAuth 2.0，我们不能一直依赖框架而忘记了本质的原理性东西，而且 学了咱们这个课程，我们自己实现一个OAuth 2.0框架，一点都不难呢。

7

刘文印@登录易
2020-06-29

谢谢王老师分享，第一时间入手了。我们“登录易”也用了类似的思想，但不是第三方登录，希望王老师帮审核一下有没有漏洞，我邮箱liuwy@gdut.edu.cn，多谢了。

2 1

soul
2020-06-29

希望作者最后能结合所授完成一份实战代码

展开

1

雷霹雳的爸爸
2020-06-29

老师介绍的很实在啊，索性跟着这个课，把oauth2 in action读一遍吧，要不感觉也找不到借口读书...说这话感觉找打...

展开

> 作者回复: 😀 一起学习，我们在学习的时候实际上，我个人认为最高的学习境界方法是做 【主题学习】，比如把OAuth 2.0 这个是一个主题，那么大家就可以同时看好几种资料，来相辅相成，达到自己收获的目的。



1

胡化敏
2020-06-29

jwt 能直接解析，讲讲jwe的实现把

展开


1

1

Blue
2020-06-30

老师您好，我前段时间学习OAuth2.0的痛点就是搞不清楚授权角色的作用，以及为何会产生固定url的交互，更迷糊就是无法有效的区分用户管理系统与OAuth授权中心的关系，在设计上，无法完好的去解耦用户管理系统，与认证授权系统的服务，希望老师能够在后续的课程中着重讲一下如何分离用户管理系统、认证中心、网关这三者之间的联系与区别！

展开


王智
2020-06-30

公司用的OAuth2，前负责人离职了，现在我来负责，但是对这块一点都不熟悉，一头雾水，每次与第三方进行单点登录就是复制前面的代码，然后修修改改，代码越看越不想看，真想重构一波，但是对整个流程又不熟悉，难！！！

展开


bigben
2020-06-30

公司内部微服务调用也需要oauth2吗？有没有更好的解决方法？


一步
2020-06-29

OAuth 2 我之前一直认为是使用在第三方服务端应用接入某个平台的时候使用的。 这个难道还可以使用在 app 或者 Web 端 代替用户名密码直接去做认证的吗？ 这样的话不就把 appid 和 appsecret 给泄露出去了？

作者回复: OAuth 2.0的时候 就充分考虑的现实生成环境中的场景，比如移动App，提出了一种PKCE的模式，大体是通过一个 “挑战码” 来完成的，关于这方面的内容，会在后续的课程中都有讲

解。

马成
2020-06-29

正在着手准备开发一套基于oauth2和jwt机制的用户微服务

作者回复: 太好了，一起学习。

1

约书亚
2020-06-29

希望详细解析一下授权的每一个步骤，如果没有这一步会被如何利用漏洞

作者回复: 在 后面的课程中 我们会有一节课 专门讲解安全的内容，到时候不仅仅 OAuth 2.0 本身的安全问题会讲到，互联网场景的安全比如CSRF XSS 水平越权 等都会涉及，因为OAuth 2.0 也是互联网的场景。

xuyd
2020-06-29

用没有基于spring oauth2的一个例子

展开

作者回复: 目前没有，课程的过程中，本意是想用一套“更干净的代码”，来讲透OAuth 2.0的基本流程，其实OAuth 2.0 学完这个课程之后，只要你掌握了基本的原理流程，搭建一个这样的框架，没有任何难度。

其实在学完这个课程之后使用spring去构建也是没有任何问题的，因为spring也是作为一个 “脚手架” 来使用。

gavin
2020-06-29

感谢老师的分享，用OAuth2.0很久了，一直是基于Spring Security使用password和client模式，来做内部用户（包括app和web端）和第三方用户的身份认证，登录后的访问权限进一步基于身份对应的角色，基于RBAC进行控制，这次跟老师学习一下，看看怎么完善一下，更加符合标准。

展开

作者回复: Spring Security是不错的组件，那么其实最根本的内容还是融入和基于OAuth 2.0本身来实现，我们多交流。

1