



下载APP



结束语 | 把学习当成一种习惯

2020-08-04 王新栋

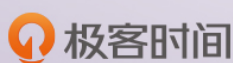
OAuth 2.0实战课

[进入课程 >](#)**王新栋**

京东资深架构师

你好，我是王新栋。

你不知道的是，在你坚持学习的时候，有很多人都掉了队，站在终点回头去看，不知不觉中你就成为了极少数人。放大到整个人生去看，只要持续走极少数人走的路，你就能成为极少数人。


**讲述：李海明**

时长 08:20 大小 7.65M



你好，我是王新栋。

当你来到这节课的时候，我们的课程已经接近尾声，相信你在课程的学习中都有所收获。在最后的这节课，我想跟你谈一谈如何学习 OAuth 2.0 这门技术。

在谈起如何学习这个话题的时候，我很愿意跟你分享我的一些经历和经验。我个人认为，**学习从来都不是一件容易的事情，夸张一点讲有点“反人性”**。你想啊，谁不愿意，在工作忙碌了一天，晚上回家多陪陪家人；又有谁不愿意，到了周末去找几个朋友打打篮球或者陪女朋友看看电影呢。但是，学习一定要养成一种习惯。我在《程序员思维修炼》本书中读到这么一段话，分享给你：

知识投资也是一样。你需要定期投资最低限度的时间量。养成一种习惯，如果需要的话。躲到你的家庭办公室里去或者走进有无线网络的咖啡厅。并非每期学习都同样富有成效，但是只要定期安排学习，长期来看一定会成功。如果你一直在等待空闲时间或者等待灵感的突现，那么它永远都不会发生。

在具备了上面所述的“定力”以后，我再和你谈一谈具体的学习方法。

我按照层次由低到高把学习分为**基础学习、分析学习和主题学习**：

基础学习，就是从知识点最基本的理论开始学习；

分析学习，就是对知识的结构脉络做梳理，并带着问题去学习；

主题学习，就是对同一个知识点，分别找到不同的资料来学习。

这样看，基础学习和分析学习属于“点”的学习，而主题学习就属于“面”的学习，整体下来就是从点到面构建知识网络的过程。接下来，我就和你说说 OAuth 2.0 的学习，是怎么对应到这三个层次的。

在基础学习的过程中，我们要学习 OAuth 2.0 的四种基本角色，包括资源拥有者（也就是用户）、客户端（也就是第三方软件）、授权服务、受保护资源服务；还要学 OAuth 2.0 的四种基本授权许可类型，包括授权码许可类型、隐式许可类型、客户端凭据许可类型、资源拥有者凭据许可类型。

当确定了基础学习阶段的学习范围之后，我们就要将这些角色带入到每个许可类型中，让这些角色“转起来”，这时你就可以像我一样用小明使用小兔打单软件的例子串起整个 OAuth 2.0 的工作流程。

在分析学习的过程中，我们就需要将 OAuth 2.0 的知识体系结构进行一个梳理，同时把学习时遇到的问题都列出来，然后逐一分析。这些问题可能是：为什么授权码许可流程一定要有授权码，为什么授权码许可一定要有两次重定向，如何管理 JWT 格式的令牌的生命周期，当访问令牌失效了一定要让用户重新授权吗，刷新令牌会一直有效吗，ID 令牌和访问令牌之间有联系吗，等等。

在主题学习的过程中，我们可以把要重点理解的内容当成一个主题，去“横向”地学习。怎么才能叫做横向呢？比如，要知道 PKCE 到底解决了什么问题，那么你就可以把 PKCE

当成一个主题来学习，你要去查阅跟它相关的任何资料，可以找 OAuth 2.0 的官方文档，可以看咱们的专栏，也可以看其它与之相关的书籍等等。总之，这是你的一个“研究方向”。

在掌握了基础学习、分析学习和主题学习这三个层次的学习方法之后，我还有一招儿，就是配合“**输出倒逼输入**”来加强学习效果。

有一天我在图书馆看书时，回想起自己这些年在公司内外做分享和写书的经历，猛然间脑子里面蹦出了“输出倒逼输入”这个词儿，一下子想通了输出对于技术学习的重要性。再后来，我刷朋友圈里别人分享的文章时，也看到了这个词。再到后来，我在读《如何阅读一本书》时，看到了其中有这样一句话“阅读与写作的互惠”，又再次印证了这一点。

那我再分享自己的一个小故事吧。有一年 618 刚结束，京东大学的同事就来找我，问我愿不愿意做一次 618 大促备战的复盘分享，而且要在一周内准备好要分享的内容。虽然时间很紧张，我也不知道自己要分享什么内容，甚至连思路都还不清晰，但我还是毫不犹豫地答应了下来。输出倒逼输入嘛。

在接下来的准备时间里，我从要备战内容的点点滴滴，到系统黄金流程的识别过程，再到人员的培训，分别进行了梳理，逐渐形成了自己的一套备战方法论，完成了那次的大促复盘分享，也获得了同事们的很多正反馈。

你看，要不是因为有“输出”的逼迫感，我可能就不会去做这个复盘，也不会沉淀自己的方法论。正所谓备战在平时，后来我和团队就把这套备战方法论落到了日常工作中，时刻保证着系统的稳定运行。

这就让我无比坚信，“输出倒逼输入”是一个绝好的学习方式。

那具体到我们的课程中，该怎么运用这个方法呢？

最简单的，自然就是留言了。永远不要觉得看完文章就是学会了，要知道，任何一种思想都不可避免地带有局限性，想要拥有更高维度的见解，前提是你见识过足够多、足够好的东西。

因此，你要多输出自己的想法，抛出引子，比如你对某些内容的深入思考、你在工作中积累的独特经验，甚至是你对我的一些观点的质疑，等等。我和其他同学看到了你的留言，也会和你讨论，我们的思想交叠碰撞，你的知识厚度必定会有所增加。

除了零碎的留言，你还可以进行系统的梳理，制作一些思维导图、PPT，或者是写成文章，在公司内部做一场分享。最后，你得到的是一套知识体系，同时也可以增加你在公司里的“出镜率”，这不是一举多得呢？

当然，这种方式绝不仅限于咱们课程的学习，希望你总能积极地向外传达你的想法。带着惊喜的输出亮相，理所当然地会得到未知的惊喜。

到这里，我们相伴而行的时光也就接近尾声了，接下来，我们要回归各自的赛道了。在此之前，我很想很想跟你说一句“敬佩”。

你不知道的是，在你坚持学习的时候，有很多人都掉了队，站在终点回头去看，不知不觉中你就成为了极少数人。放大到整个人生去看，只要持续走极少数人走的路，你就能成为极少数人。

“将每一个忙碌、充实的日子，累积成酣畅淋漓的生命”，希望我们都能活到淋漓，与你共勉。

我在这里为你准备了一份 [📄 毕业问卷](#)，题目不多，希望你能花两分钟填一下。我非常期待能听你和我说一说，你对这个课程的想法和建议。今天虽然是结课，但我还会继续关注你的留言，也希望你能继续学习这个课程的内容，并会通过留言区和你互动。最后，再次和你一声“感谢”。

**王新栋**

京东资深架构师

感谢一起走过的这段时间，非常想听听你对我和这门课程的反馈与建议。在 2020 年 8 月 17 日前提交问卷，将有机会获得



原创 | 正则表达式快捷速查
超大鼠标垫 价值 **¥49**

或



极客时间课程阅码
价值 **¥99**

填写问卷 

提建议

更多课程推荐

Elasticsearch

核心技术与实战

>>> 快速构建分布式搜索和分析引擎

阮一鸣

eBay Pronto 平台技术负责人



涨价倒计时 🕒

现仅 **¥99** 8月15日涨价至 **¥199**

© 版权归极客邦科技所有，未经许可不得传播售卖。页面已增加防盗追踪，如有侵权极客邦将依法追究其法律责任。

上一篇 期末测试 | 一套习题，测试你的掌握程度

精选留言 (14)

💬 写留言

**Geek_883762**

2020-08-04

当老师说再见的时候，我哭了。

展开 ∨



👍 1

**carol**

2020-08-04

马上买了一本《程序员思维修炼》，哈哈

展开 ∨

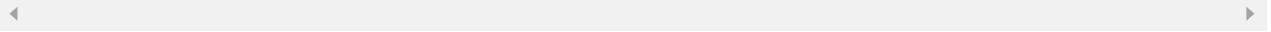
作者回复: 哈哈 一起变得更加优秀

**zeroki**

2020-08-07

“鉴权”是建议在开放平台的网关做呢，还是授权服务做呢？

作者回复: 放在网关来做，读取授权服务的接口或者是直接操作授权服务的数据存储。

**Tim Zhang**

2020-08-07

老师 不是很理解你回答的刷新逻辑在授权服务。

前提 我的oauth服务是我自己写的，并非第三方服务。

我一个请求首先访问了网关，网关进行了鉴权，然后请求打到了后面api，但是actoken过期了，需要拿着refreshtoken去刷新actoken，难道不是受保护资源自己去调用我的oauth服务拿actoken么？这个逻辑如果每个受保护资源自己做，那是不是每个受保护资源都...
展开 ∨

**AgCl**

2020-08-07

老师，看到留言，我有点疑惑，我们这边正想用oauth2的实现，如果网关做了验证和粗粒度的授权

但是资源服务器可能有更细粒度的权限管理，如果用的是spring security 的框架，资源服务器获取到用户id, 然后我们自己初始化好securityContextHolder的内容；这样的话是不是我们直接网关就做转发，资源服务器自己去做token的验证以及权限验证，谢谢老师
展开 ∨

**Tim Zhang**

2020-08-06

请问下假设2个服务 a和b，首先调用a的/a，然后a会调用b的/b，在网关层只能针对/a进行权限校验，/a执行完毕后调用/b，这个时候已经不会访问到网关了，请问权限校验是否只能在/b的应用上通过横切逻辑类似filter进行校验过滤

展开 ∨

**Tim Zhang**

2020-08-06

请问下既然网关层scope与api进行鉴权了，那么访问都后端api的时候，是否还要通过rbac进行hasRole hasAuthority进行每个api验证

展开 ∨



Tim Zhang

2020-08-06

老师，还有疑问，求解答

1、scope与api的映射表，缓存在网关，网关进行鉴权。那么如果粒度很细，一个api(url 路径+ http方法)就需要对应一个scope，那么可能有成千上万个api，都需要在表里面定义么

2、网关已经校验过了scope，并且通过，请求调用到了受保护资源的某个api，还需要...

展开 ∨

作者回复: 1、这个数量参照要按照accesstoken的角度来讲，每一个accesstoken对应一个scope，如果按照上面所述的，就是一对一对多的关系，这些数据都存储在redis中。

2、在网关做了OAuth的鉴权也包括scope的校验，受保护资源不需要在做类似的验证，但是越权访问，也就是之前我们讲到的数据归属判断，是一定要在受保护资源内部逻辑中去做。

3、刷新token的逻辑在授权服务系统中实现，不在网关层。



Tim Zhang

2020-08-05

请教一下 refreshtoken的刷新以及一些重定向可以全部交给spring security，但是这部分逻辑应该实现在网关 还是每个受保护资源都需要实现一下

展开 ∨

作者回复: 如果有多个受保护资源，在做“鉴权”的时候，可以统一放在网关内部实现。

支持refreshtoken的逻辑是在授权服务上面进行的，如果使用了security，则是在框架内职责模块上实现。



在路上

2020-08-04

感谢老师的精彩讲解，现在每次授权登录时，都想到老师讲些的后台流程。



**tt**

2020-08-04

感谢老师，收获满满，对OAuth2.0的理解更扎实了

展开 ▾

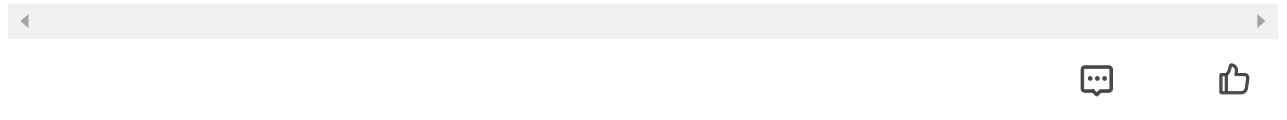
作者回复: 感谢支持

**Alex**

2020-08-04

感谢老师，跟着重新梳理了一遍OAuth2.0的知识体系。学习要坚持，复利的效果十分惊人。

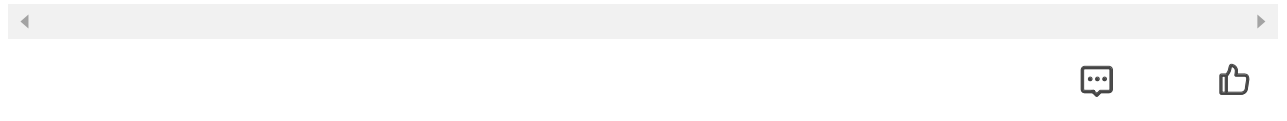
作者回复: 感谢支持，一起进步

**Adong0678**

2020-08-04

当把具象的事物能用自己简短语言总结概括出来，说明真正理解，掌握了。具体的事物会被更迭，但思想永远闪闪发光！传授知识者，都应尊称老师，十分感谢王老师！

作者回复: 感谢支持，抽象是看清了事物的本质，大家一起进步

**inrtyx**

2020-08-04

难说再见，谢谢老师

展开 ▾

作者回复: 我会一直在的 ^_^

