**1. 我把密码献给你**

小梁开发了一个“信用卡管家”的程序 ， 可以自动从邮箱中读取信用卡相关邮件，分析、汇总，形成一个报表。

小梁找到信用卡达人张大胖试用 ： “你的信用卡那么多，看看我这个程序吧， 保准你会爱死它。”

张大胖尝试了几下说： “咦，你这个程序要读取我的网易邮箱啊，那需要用户名/密码吧”

“是啊 ， 你把密码告诉输入程序不就行了， 我的程序替你加密保存，保证不会泄露。”

“得了吧你， 我可不会告诉你我的密码， 为了方便记忆， 我的密码都是通用的， 万一泄露了就完蛋了”

小梁说：“这样吧，我不保存，我就访问邮箱的时候使用一次， 用完就扔！”

“你以为你是阿里巴巴啊， 有信用背书， 你只是个小网站， 我把密码献给你，总是觉得不安全。就是我信任你，别人能信任你吗？”

小梁想想也是， 这是一个巨大的心理障碍， 每个人都要誓死捍卫自己的密码啊。

**2. Token**

过了一周， 小梁兴致勃勃地把张大胖拉来看“信用卡管家”的升级版。

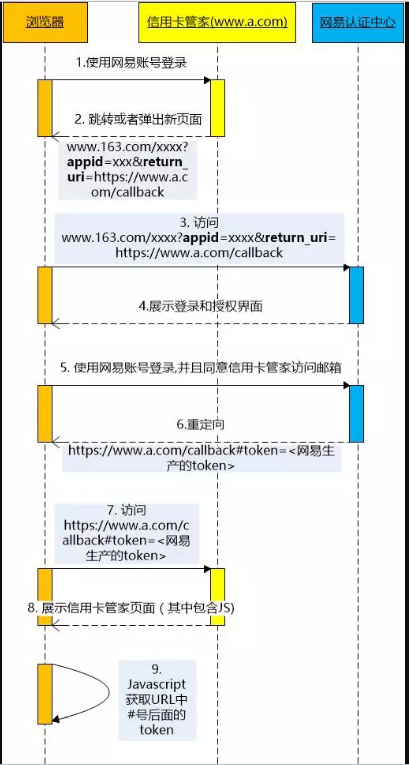
“升级为2.0了啊， 这次不用问你要网易邮箱的用户名和密码了”

“那你怎么访问我的邮箱？”

“很简单，我提供了一个新的入口，使用网易账号登录， 你点了以后，其实就会重定向到网易的认证系统去登录， 网易的认证系统会让你输入用户名和密码，并且询问你是否允许信用卡管家访问网易邮箱， 你确认了以后，就再次重定向到我的‘信用卡管家’网站， 同时捎带一个‘token’ 过来， 我用这个token 就可以通过API来访问网易邮箱了。 在这个过程中， 我根本不会接触到你的用户名和密码，怎么样， 这下满意了吧？”

“你说得轻松， 你这个信用卡管家是个小网站，还没有什么名气， 网易怎么会相信你这个网站呢？”

“我当然要先在网易注册一下啊， 他们会给我发个app\_id 和app\_secret， 我重定向到网易的时候需要把这个东西发过去， 这样网易就知道是‘信用卡管家’这个应用在申请授权了。”



张大胖说： “ 你这重定向来重定向去的， 实际上不就是为了拿到一个token 吗？”

“对啊，因为你不信任我的信用卡管家， 不让它保存你的密码，只好用token的方法了 , 它是网易认证中心颁发的，实际上就代表了你对信用卡管家访问邮箱的授权，所以有了这个token 就可以访问你的邮箱了”

"对了" 张大胖问题， “你为什么用Javascript的方式来读取token啊”

“这样我的后端服务器就不用参与了，工作都在前端搞定， 你注意到那个URL中的#号了吗？ www.a.com/callback#token=<网易返回的token>”

张大胖说： “我知道啊，这个东西叫做hash fragment, 只会停留在浏览器端， 只有Javascript 能访问它，并且它不会再次通过http request 发到别的服务器器， 我想这是为了提高安全性吧。”

小梁说： “没错， 那个token非常非常重要，得妥善保存，不能泄露！”

“可是在第6步通过重定向，这个token 以明文的方式发送给了我的浏览器， 虽然是https ，不会被别人窃取，可是浏览器的历史记录或者访问日志中就能找到， 岂不暴露了？”

小梁说： “这个.... ， 我说你这个家伙，安全意识很强烈嘛， 让我想想，有没有更安全的方式。"

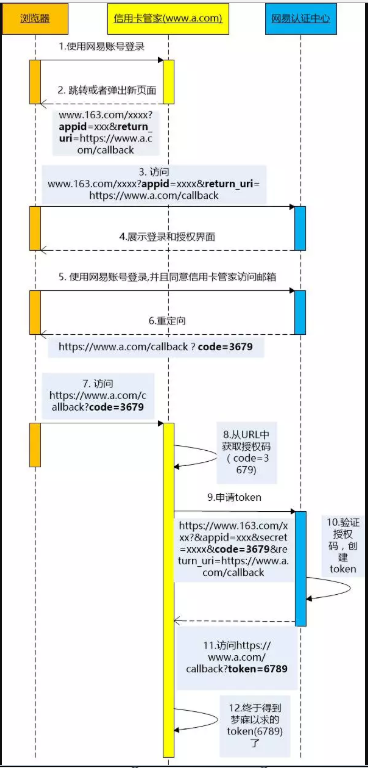
**3. Authorization Code + Token**

又过了一周，小梁成功地把信用卡管家升级为3.0.

他对张大胖说： “这次我成功地把那个非常重要的、表示授权的token 给隐藏起来了， 你要不要看看？”

“你先说说你是怎么隐藏的？”

“其实整体思路和之前的类似，只是我引入了一个叫做Authorization Code 的中间层。 当你用网易账号登录的时候， 网易认证中心这一次不给我直接发token,而是发一个授权码(authorization code) , 我的信用卡管家服务器端取到这个code以后，在后台再次访问网易认证中心， 这一次他才发给我真正的token 。 还是直接上图吧：”



**从第7步开始用户是感知不到的。**

张大胖说： “还比较容易理解， 本质上就是你拿着这个返回的授权码在服务器后台‘偷偷地’完成申请token 的过程， 所以token 浏览器端根本就接触不到，对吧？”

“什么叫偷偷地申请token ？ 这是我信用卡管家服务器和网易之间的正常交流， 只是你看不到而已。”

“开个玩笑了， 你虽然隐藏了token,但是这个授权码确是暴露了啊，你看第7步，我在浏览器中都能明文看到， 要是被谁取到， 不也是照样能取到token吗？”

小梁说： “我们肯定有防御措施， 比如这个授权码和我的信用卡管家申请的app\_id，app\_secret关联， 只有信用卡管家发出的token请求， 网易认证中心才认为合法； 还可以让授权码有时间限制，比如5分钟失效，还有可以让授权码只能换一次token, 第二次就不行了。 ”

“听起来似乎不错， 好吧， 这次我可以放心地使用了！”

**4. 后记**

本文讲的其实就是就是OAuth 中的三种认证方式，依次是：

1. Resource Owner Password Credentials Grant(资源所有者密码凭据许可)

2. Implicit Grant(隐式许可)

3. Authorization Code Grant(授权码许可)

还有一种叫做Client credentials ,用的较少，文章没有涉及。

这些名称有些古怪， 但是本质没那么复杂。 在OAuth中，还有几个术语大家可以理解下：

资源所有者 : 就是我们上文的张大胖

资源服务器 ： 即网易邮箱

客户端: 就是上文的信用卡管家

授权服务器 ： 即上文的网易认证中心