一种微信开放平台 OAuth 认证授权代理的实现

赵庆明

（成都理工大学图书馆，四川 成都 610059）

摘 要 基于微信开放平台的 OAuth 认证授权已成为一种可以替代传统的账号密码登录网站应用的用户认证方式。腾讯公司为了防止其被滥用而设置了种种限制。本文讨论构建一种“认证授权代理”的方案，突破了当前微信开放平台中的限制，转而将这些限制交由自己控制，而且在新的网站应用程序接入时更为便捷，很好地满足了自己当下多样的业务需求。

关键词 微信开放平台 微信公众号 OAuth 认证授权 网页授权

中图分类号：TP317 **文献标识码**：A **文章编号**：1007-0745(2022)12-0007-03

微信是腾讯公司在 2011 年 1 月发布的一款为智能终端提供即时通讯服务的免费软件 [1]。当前，微信已经渗入了人们生活的方方面面，基于微信又衍生出了可以让第三方应用系统接入微信的微信开放平台 [2]。无论是浏览微信公众号推文，还是通过微信公众号菜单来浏览指定的网站链接，还是直接使用微信扫码来登录某个网站，都将直接或间接地涉及微信开放平台 OAuth 认证授权的功能。

基于 OAuth 协议，单位可自建统一身份认证系统，也可以接入微信、QQ、支付宝、微博等社交软件提供的第三方认证授权系统。OAuth 协议相比于传统的采用账号密码对认证的模式便捷很多，大大减少了用户在“认证”过程中的额外负担。微信在我国的广泛使用，逐步演化成网站应用接入第三方 OAuth 认证的首选平台。

腾讯公司为避免微信 OAuth 被滥用设置了限制：（1）网站应用程序需用域名访问。（2）每个公众号最多支持绑定 2 个域名。（3）一个开发者账号最多允许创建 10 个网站应用。对于类似于高校图书馆有大量网站应用系统的情况，这些限制往往难以满足接入需求。基于此原因，我们采用目前流行的 ASP.NET Core 6 Web Api[3] 构建了一个“微信 OAuth 认证授权代理服务器”，在满足微信开放平台的要求下，实现了通过 1 个公众号、1 个域名和 1 个开发者账号，突破了当前的限制，满足了大量网站应用系统接入微信 OAuth 认证授权的需求。

1 OAuth 协议规范

OAuth 协议最初设计的目的是用于解决一个普遍的“如何通过代理访问受保护的资源”的问题，2007 年 10 月开始建立标准，直至 2010 年 1 月发布了 OAuth1.0 正式版协议 RFC5489[4]。在 2012 年 10 月发布了 OAuth 2.0 正式版协议 RFC6749[5] 后，该协议开始被广泛地应用于各类认证授权服务。

在 OAuth 协议中，当应用程序需要访问服务器上的资源的时候，服务器通过使用“第三方”为该用户授权颁发的“令牌”对每次访问进行身份鉴别和权限识别，然后再对资源进行访问。全程无需用户提供自己的账号密码对等敏感信息，因此避免了用户机密信息泄漏的可能，同时又能保证应用可以通过服务器访问到指定的用户资源。即使用户突然更改了账号密码，也不会影响已经完成的认证授权和接下来即将进行的认证和授权。

当网站应用被接入到当前流行的社交软件所提供的 OAuth 认证授权系统后，用户在登录网站应用时只需简单的几步点击就可完成认证和授权，从而让“认证”变得非常简单。

2 基于微信的认证授权

微信作为一款重量级的社交软件，已在人们的日常生活中扮演起了重要的角色。腾讯公司以微信为依托建立了“微信开放平台”，并开放了大量的、实用的功能，其中与 OAuth 认证授权相关的包括微信公众号网页授权、移动应用微信登录、网站应用微信登录、智能家居小程序用户授权等。

对于网站应用来说，“微信公众号网页授权”与“网站用微信登录”是两个类似但不同的用户认证授权方式。“微信公众号网页授权”用于在微信中访问网站应用，而“网站用微信登录”则用于在 PC 端访问网站应用。

微信认证授权流程分为三步：（1）引导用户进入授权页面，获取微信开放平台返回的 code 参数。（2）应用程序后台通过 code 换取网页授权 access_token 与

openid。（3）如果请求授权时 scope 参数为 snsapi_userinfo，那么还可以再通过 access_token 和 openid 来获取微信用户基本信息。通常情况下，到达第 2 步获取 openid 后就可完成用户身份识别。

2.1 “微信公众号网页授权”的交互逻辑

用户在微信客户端中授权访问第三方网站应用时，需要使用“微信公众号网页授权”模式[6]。网站应用程序可以通过微信公众号网页授权机制实现用户登录逻辑，进而实现自身的业务逻辑。微信用户的微信 ID 与该微信公众号的微信 ID 会通过一种计算得到一个被称为 openid 的字符串。此 openid 就标志着该微信用户基于该微信公众号的身份。在获取 openid 之后，就意味着与微信相关的认证授权已经完成。

对于“微信公众号网页授权”，微信开放平台提供了两种权限不同的 scope 参数。当 scope 为 snsapi_base 时，发起的网页授权属于静默授权，用来获取进入页面的微信用户的 openid。当 scope 为 snsapi_userinfo 时，还可以获取微信用户的个人基本信息。

用户在微信中打开该网站应用中的网页授权页面时，微信开放平台会将被访问的地址重定向到该网站应用指定的回调页面网址，并在网址后添加一个名为 code 的参数。接下来，网站应用后台通过 code 参数从微信开放平台获取一个接口调用凭证 access_token 和 openid，然后在网站后台实现对应的业务逻辑。当 scope 为字符串 snsapi_base 时，属于静默授权，微信用户的感知就是直接进入了回调页面（业务页面），并不会感知到登录过程。当 scope 为字符串 snsapi_userinfo 时，如果用户之前关注过该公众号，则效果同 snsapi_base 一样，用户也不会感知到登录过程。倘若用户并未曾关注过该公众号，则在微信中会增加一个要求用户同意授权的操作，用户同意授权后方可继续执行。

2.2 “网站用微信登录”的交互逻辑

当用户在 PC 端网站应用上选择使用微信登录后，网站应用会显示一个微信登录的二维码。接下来，用户使用微信扫描该二维码，然后在微信中点击“允许”进行授权，该 PC 端网站就可以完成登录，然后再去实现相应的业务逻辑。此功能为被称为“使用微信登录网页”，该功能可以让微信用户使用微信身份安全地登录第三方网站应用。

“使用微信登录网页”同样是一个基于 OAuth2.0 协议标准构建的微信认证授权系统，在网站上的接入方法与“微信公众号网页授权”的形式上保持一致，仅有请求的 url 与参数上的差别。

用户使用移动端微信扫描 PC 机上的登录二维码，然后授权登录接入了“使用微信登录网页”的网站应用后，同“微信公众号网页授权”一样，微信开放平台会将 PC 机上被访问的 url 地址重定向到该网站应用指定的回调页面网址，同样在网址后添加一个名为 code 的参数。接下来，网站就可以通过参数 code 获取到用户的接口调用凭证 access_token 和该微信用户对应于该网站应用的 openid。

2.3 两种交互逻辑的异同

“网站用微信登录”与“微信公众号网页授权”的交互逻辑类似。在“微信公众号网页授权”中，网页认证和授权以及访问网站数据均在微信中进行。在“网站用微信登录”中，网页认证和授权在移动端微信中进行，而访问网站却在 PC 端的进行。在网站应用的后台，除了提供的参数稍有差别外，这两种认证和授权在形式上保持一致。

3 微信开放平台 OAuth 认证的限制

目前，在使用微信公众号进行“微信公众号网页授权”时，并不支持 IP 地址回调，仅支持最多 2 个完全域名的回调，从而一个公众号仅能支持最多 2 网站应用的认证和授权。但一个企业或单位往往为用户提供的网站应用程序不止 2 个，因此这种限制导致往往无法满足网站应用比较多的情况。

在“网站用微信登录”中，微信开放平台中每个开发者账号中最多可创建 10 个网站应用，每个应用中要求绑定一个完全域名。同样，如果网站应用数量超过 10 个，这种也会限制也会带来不能满足实际需求的问题。

无论是额外再申请微信公众号，还是额外再申请开发者账户，除了必要的费用外，还需要通过一系列资质认证。尤其是在日后的维护时，还需要配合腾讯公司完成一系列审核工作，对于网站应用接入微信开放平台带来了诸多不便。

4 扩展的 OAuth 认证授权

我们创建了一个“代理”认证授权的服务器，并将其接入微信开放平台。通过该“服务器”对微信开放平台中的 OAuth2 授权认证进行了扩展，满足了接入网站应用的各种个性化的需求。对于微信开放平台来说，“认证授权代理”服务器是一个完整的、合规的应用程序网站，而该网站真正的用途是用来进行“模拟”和“代理”微信开放平台的认证和授权。

在整个数据交互过程中，微信开放平台仅仅可以感知到作为“合法网站”的“认证授权代理服务器”在申请认证授权，并不会感知到真正的“网站应用”，

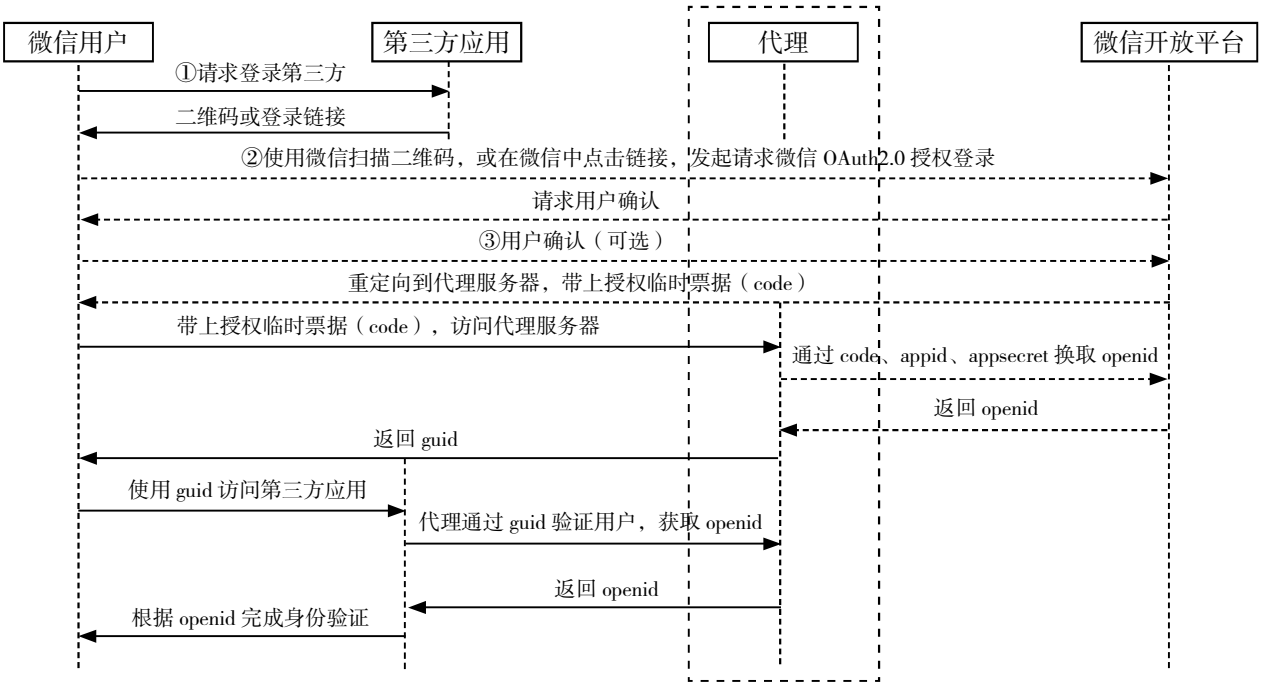

图 1 基于“代理”模式的微信网页 OAuth2 授权认证方式

从而突破了微信开放平台的限制。因此，接入的网站应用不再有任何限制。但由于突破了此限制，原本由微信开放平台所控制的“应该被授权的”网站应用程序，转由“认证授权代理服务器”通过配置相应的参数进行控制和管理。

5 网站应用程序的接入

在标准模式下，网站应用与微信开放平台直接进行数据交互。在“代理”模式下，该功能则由“认证授权代理服务器”代为实现。从而，“认证授权代理服务器”是认证授权过程中的一个中间环节，不但要完成与微信用户之间的数据交互，而且要完成与网站应用程序、微信开放平台之间的数据交互，也是整个实现过程中逻辑最复杂的部分。

我们采用了 ASP.NET Core 6 Web Api，将其业务逻辑进行了封装，并且提供了与微信开放平台中完全相同的接口（源码地址：https://github.com/zmrbak/WxOAuthManager）。相比于标准的 OAuth 认证授权模式，在网站应用程序接入时，除了需更换请求 url 中的主机地址外，与标准的模式保持一致。用户的前端的操作上与仍然与标准的模式下保持一致，仅仅在整个授权期间会增加一次用户难以觉察的“url 重定向”操作。

6 结语

本文讨论了一种扩展微信开放平台的标准的 OAuth 认证授权的模式，让“认证授权代理服务器”代为其进行微信认证和授权，有效地突破了微信开放平台的种种限制，只需一个微信公众号、一个域名、一个开发者账号，就可以满足任意数量、任意网站“合法”“合规”地使用微信开放平台中的 OAuth 认证授权服务，在用户的体验上与标准模式保持一致。

参考文献：

[1] 腾讯公司 .2011 年 1 月 21 日微信诞生 [DB/OL].(2022-01-21)[2022-01-21].https://new.qq.com/rain/a/20220121A0CRHM00.
[2] 腾讯公司 . 微信官方文档 · 开放平台 [DB/OL].(2022-09-30)[2022-09-30].https://developers.weixin.qq.com/doc/oplatform/Mobile_App/Resource_Center_Homepage.html.
[3] 微软公司 .ASP.NET Web API[DB/OL].(2022-09-30)[2022-09-30]. https://dotnet.microsoft.com/zh-cn/apps/aspnet/apis
[4] Hammer-Lahav Ed.RFC 5849The OAuth 1.0Protocol[S].Fremont,CA:IETF,2010.
[5] Hardt Ed.RFC 6749 The OAuth 2.0 Authorization Framework[S].Fremont,CA:IETF,2012.
[6] 同 [2].