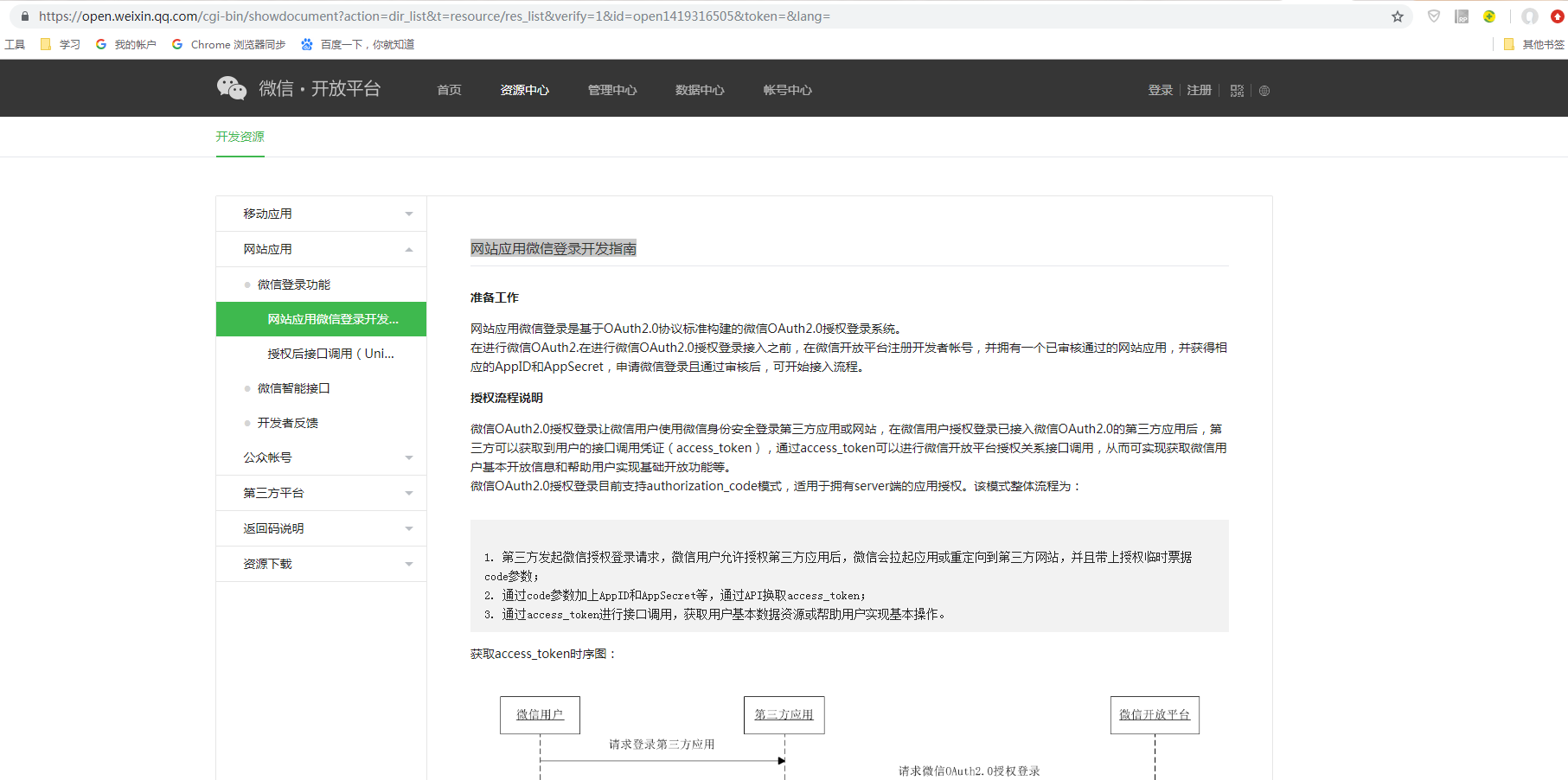
https://open.weixin.qq.com/cgi-bin/showdocument?action=dir\_list&t=resource/res\_list&verify=1&id=open1419316505&token=&lang=

网站应用微信登录开发指南

李孟军：从微笑的角度，客户端就是第三方。这里所说的第三方，都是客户端系统。在第三方账户登录时，从客户端角度看，微信是服务端，微信就是第三方账户端。

名词描述有时候你要明白，站的角度不同，描述的用词可能就不同，要区分清楚这些用词，再以后遇到负责逻辑时才不会混乱。



#### 准备工作

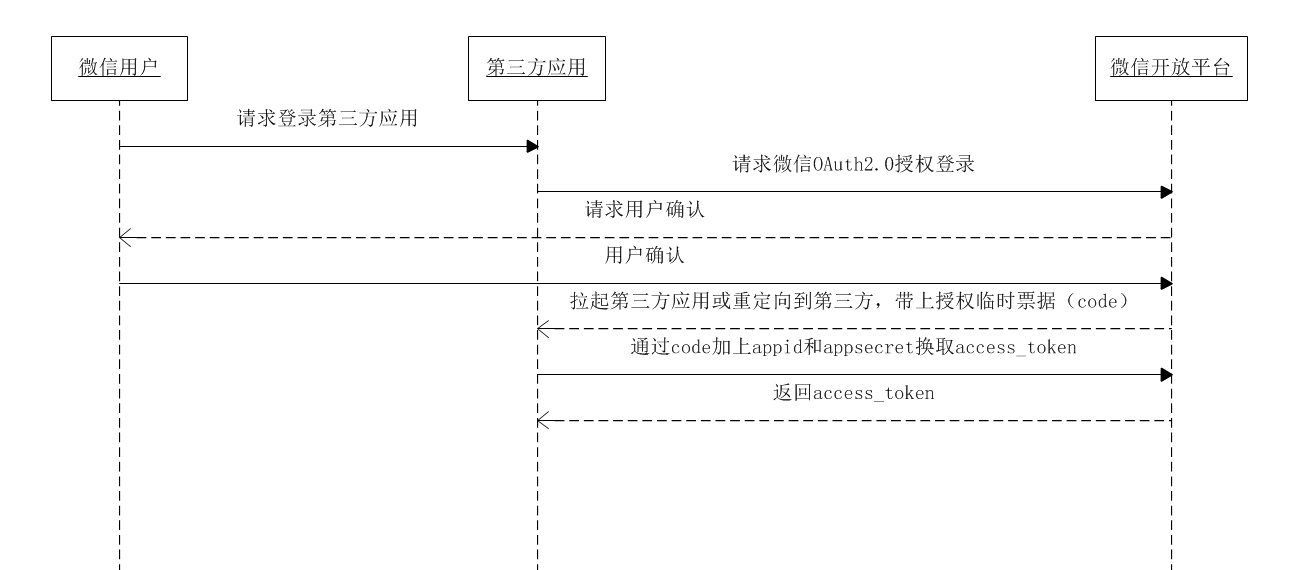
网站应用微信登录是基于OAuth2.0协议标准构建的微信OAuth2.0授权登录系统。  
在进行微信OAuth2.在进行微信OAuth2.0授权登录接入之前，在微信开放平台注册开发者帐号，并拥有一个已审核通过的网站应用，并获得相应的AppID和AppSecret，申请微信登录且通过审核后，可开始接入流程。

#### 授权流程说明

微信OAuth2.0授权登录让微信用户使用微信身份安全登录第三方应用或网站，在微信用户授权登录已接入微信OAuth2.0的第三方应用后，第三方可以获取到用户的接口调用凭证（access\_token），通过access\_token可以进行微信开放平台授权关系接口调用，从而可实现获取微信用户基本开放信息和帮助用户实现基础开放功能等。  
微信OAuth2.0授权登录目前支持authorization\_code模式，适用于拥有server端的应用授权。该模式整体流程为：

1. 第三方发起微信授权登录请求，微信用户允许授权第三方应用后，微信会拉起应用或重定向到第三方网站，并且带上授权临时票据code参数；  
2. 通过code参数加上AppID和AppSecret等，通过API换取access\_token；  
3. 通过access\_token进行接口调用，获取用户基本数据资源或帮助用户实现基本操作。

获取access\_token时序图：



**第一步：请求CODE**

第三方使用网站应用授权登录前请注意已获取相应网页授权作用域（scope=snsapi\_login），则可以通过在PC端打开以下链接：  
<https://open.weixin.qq.com/connect/qrconnect?appid=APPID&redirect_uri=REDIRECT_URI&response_type=code&scope=SCOPE&state=STATE#wechat_redirect>  
若提示“该链接无法访问”，请检查参数是否填写错误，如redirect\_uri的域名与审核时填写的授权域名不一致或scope不为snsapi\_login。

**参数说明**

| 参数 | 是否必须 | 说明 |
| --- | --- | --- |
| appid | 是 | 应用唯一标识 |
| redirect\_uri | 是 | 请使用urlEncode对链接进行处理 |
| response\_type | 是 | 填code |
| scope | 是 | 应用授权作用域，拥有多个作用域用逗号（,）分隔，网页应用目前仅填写snsapi\_login即 |
| state | 否 | 用于保持请求和回调的状态，授权请求后原样带回给第三方。该参数可用于防止csrf攻击（跨站请求伪造攻击），建议第三方带上该参数，可设置为简单的随机数加session进行校验 |

**返回说明**

用户允许授权后，将会重定向到redirect\_uri的网址上，并且带上code和state参数

redirect\_uri?code=CODE&state=STATE

若用户禁止授权，则重定向后不会带上code参数，仅会带上state参数

redirect\_uri?state=STATE

**请求示例**

登录一号店网站应用  
<https://passport.yhd.com/wechat/login.do>  
打开后，一号店会生成state参数，跳转到  
<https://open.weixin.qq.com/connect/qrconnect?appid=wxbdc5610cc59c1631&redirect_uri=https%3A%2F%2Fpassport.yhd.com%2Fwechat%2Fcallback.do&response_type=code&scope=snsapi_login&state=3d6be0a4035d839573b04816624a415e#wechat_redirect>  
微信用户使用微信扫描二维码并且确认登录后，PC端会跳转到  
<https://passport.yhd.com/wechat/callback.do?code=CODE&state=3d6be0a4035d839573b04816624a415e>  
为了满足网站更定制化的需求，我们还提供了第二种获取code的方式，支持网站将微信登录二维码内嵌到自己页面中，用户使用微信扫码授权后通过JS将code返回给网站。  
JS微信登录主要用途：网站希望用户在网站内就能完成登录，无需跳转到微信域下登录后再返回，提升微信登录的流畅性与成功率。 网站内嵌二维码微信登录JS实现办法：

步骤1：在页面中先引入如下JS文件（支持https）：

http://res.wx.qq.com/connect/zh\_CN/htmledition/js/wxLogin.js

步骤2：在需要使用微信登录的地方实例以下JS对象：

var obj = new WxLogin({  
 self\_redirect:true,  
 id:"login\_container",   
 appid: "",   
 scope: "",   
 redirect\_uri: "",  
 state: "",  
 style: "",  
 href: ""  
 });

**参数说明**

| 参数 | 是否必须 | 说明 |
| --- | --- | --- |
| self\_redirect | 否 | true：手机点击确认登录后可以在 iframe 内跳转到 redirect\_uri，false：手机点击确认登录后可以在 top window 跳转到 redirect\_uri。默认为 false。 |
| id | 是 | 第三方页面显示二维码的容器id |
| appid | 是 | 应用唯一标识，在微信开放平台提交应用审核通过后获得 |
| scope | 是 | 应用授权作用域，拥有多个作用域用逗号（,）分隔，网页应用目前仅填写snsapi\_login即可 |
| redirect\_uri | 是 | 重定向地址，需要进行UrlEncode |
| state | 否 | 用于保持请求和回调的状态，授权请求后原样带回给第三方。该参数可用于防止csrf攻击（跨站请求伪造攻击），建议第三方带上该参数，可设置为简单的随机数加session进行校验 |
| style | 否 | 提供"black"、"white"可选，默认为黑色文字描述。详见文档底部FAQ |
| href | 否 | 自定义样式链接，第三方可根据实际需求覆盖默认样式。详见文档底部FAQ |

**第二步：通过code获取access\_token**

通过code获取access\_token

https://api.weixin.qq.com/sns/oauth2/access\_token?appid=APPID&secret=SECRET&code=CODE&grant\_type=authorization\_code

**参数说明**

| 参数 | 是否必须 | 说明 |
| --- | --- | --- |
| appid | 是 | 应用唯一标识，在微信开放平台提交应用审核通过后获得 |
| secret | 是 | 应用密钥AppSecret，在微信开放平台提交应用审核通过后获得 |
| code | 是 | 填写第一步获取的code参数 |
| grant\_type | 是 | 填authorization\_code |

**返回说明**

正确的返回：

{   
"access\_token":"ACCESS\_TOKEN",   
"expires\_in":7200,   
"refresh\_token":"REFRESH\_TOKEN",  
"openid":"OPENID",   
"scope":"SCOPE",  
"unionid": "o6\_bmasdasdsad6\_2sgVt7hMZOPfL"  
}

**参数说明**

| 参数 | 说明 |
| --- | --- |
| access\_token | 接口调用凭证 |
| expires\_in | access\_token接口调用凭证超时时间，单位（秒） |
| refresh\_token | 用户刷新access\_token |
| openid | 授权用户唯一标识 |
| scope | 用户授权的作用域，使用逗号（,）分隔 |
| unionid | 当且仅当该网站应用已获得该用户的userinfo授权时，才会出现该字段。 |

错误返回样例：

{"errcode":40029,"errmsg":"invalid code"}

**刷新access\_token有效期**

access\_token是调用授权关系接口的调用凭证，由于access\_token有效期（目前为2个小时）较短，当access\_token超时后，可以使用refresh\_token进行刷新，access\_token刷新结果有两种：

1. 若access\_token已超时，那么进行refresh\_token会获取一个新的access\_token，新的超时时间；  
2. 若access\_token未超时，那么进行refresh\_token不会改变access\_token，但超时时间会刷新，相当于续期access\_token。

refresh\_token拥有较长的有效期（30天），当refresh\_token失效的后，需要用户重新授权。

**请求方法**

获取第一步的code后，请求以下链接进行refresh\_token：

https://api.weixin.qq.com/sns/oauth2/refresh\_token?appid=APPID&grant\_type=refresh\_token&refresh\_token=REFRESH\_TOKEN

**参数说明**

| 参数 | 是否必须 | 说明 |
| --- | --- | --- |
| appid | 是 | 应用唯一标识 |
| grant\_type | 是 | 填refresh\_token |
| refresh\_token | 是 | 填写通过access\_token获取到的refresh\_token参数 |

**返回说明**

正确的返回：

{   
"access\_token":"ACCESS\_TOKEN",   
"expires\_in":7200,   
"refresh\_token":"REFRESH\_TOKEN",   
"openid":"OPENID",   
"scope":"SCOPE"   
}

**参数说明**

| 参数 | 说明 |
| --- | --- |
| access\_token | 接口调用凭证 |
| expires\_in | access\_token接口调用凭证超时时间，单位（秒） |
| refresh\_token | 用户刷新access\_token |
| openid | 授权用户唯一标识 |
| scope | 用户授权的作用域，使用逗号（,）分隔 |

错误返回样例：

{"errcode":40030,"errmsg":"invalid refresh\_token"}

注意：

1、Appsecret 是应用接口使用密钥，泄漏后将可能导致应用数据泄漏、应用的用户数据泄漏等高风险后果；存储在客户端，极有可能被恶意窃取（如反编译获取Appsecret）；  
2、access\_token 为用户授权第三方应用发起接口调用的凭证（相当于用户登录态），存储在客户端，可能出现恶意获取access\_token 后导致的用户数据泄漏、用户微信相关接口功能被恶意发起等行为；  
3、refresh\_token 为用户授权第三方应用的长效凭证，仅用于刷新access\_token，但泄漏后相当于access\_token 泄漏，风险同上。  
  
建议将secret、用户数据（如access\_token）放在App云端服务器，由云端中转接口调用请求。

**第三步：通过access\_token调用接口**

获取access\_token后，进行接口调用，有以下前提：

1. access\_token有效且未超时；  
2. 微信用户已授权给第三方应用帐号相应接口作用域（scope）。

对于接口作用域（scope），能调用的接口有以下：

| 授权作用域（scope） | 接口 | 接口说明 |
| --- | --- | --- |
| snsapi\_base | /sns/oauth2/access\_token | 通过code换取access\_token、refresh\_token和已授权scope |
| snsapi\_base | /sns/oauth2/refresh\_token | 刷新或续期access\_token使用 |
| snsapi\_base | /sns/auth | 检查access\_token有效性 |
| snsapi\_userinfo | /sns/userinfo | 获取用户个人信息 |

其中snsapi\_base属于基础接口，若应用已拥有其它scope权限，则默认拥有snsapi\_base的权限。使用snsapi\_base可以让移动端网页授权绕过跳转授权登录页请求用户授权的动作，直接跳转第三方网页带上授权临时票据（code），但会使得用户已授权作用域（scope）仅为snsapi\_base，从而导致无法获取到需要用户授权才允许获得的数据和基础功能。  
接口调用方法可查阅[《微信授权关系接口调用指南》](https://open.weixin.qq.com/cgi-bin/showdocument?action=dir_list&t=resource/res_list&verify=1&id=open1419316518&lang=zh_CN)

F.A.Q

1. 什么是授权临时票据（code）？  
   答：第三方通过code进行获取access\_token的时候需要用到，code的超时时间为10分钟，一个code只能成功换取一次access\_token即失效。code的临时性和一次保障了微信授权登录的安全性。第三方可通过使用https和state参数，进一步加强自身授权登录的安全性。
2. 什么是授权作用域（scope）？  
   答：授权作用域（scope）代表用户授权给第三方的接口权限，第三方应用需要向微信开放平台申请使用相应scope的权限后，使用文档所述方式让用户进行授权，经过用户授权，获取到相应access\_token后方可对接口进行调用。
3. 网站内嵌二维码微信登录JS代码中style字段作用？  
   答：第三方页面颜色风格可能为浅色调或者深色调，若第三方页面为浅色背景，style字段应提供"black"值（或者不提供，black为默认值），则对应的微信登录文字样式为黑色。相关效果如下：



若提供"white"值，则对应的文字描述将显示为白色，适合深色背景。相关效果如下：



4.网站内嵌二维码微信登录JS代码中href字段作用？  
答：如果第三方觉得微信团队提供的默认样式与自己的页面样式不匹配，可以自己提供样式文件来覆盖默认样式。举个例子，如第三方觉得默认二维码过大，可以提供相关css样式文件，并把链接地址填入href字段

.impowerBox .qrcode {width: 200px;}  
.impowerBox .title {display: none;}  
.impowerBox .info {width: 200px;}  
.status\_icon {display: none}  
.impowerBox .status {text-align: center;}

相关效果如下：