网站应用微信登录开发指南

摘录自官方开发文档：
https://open.weixin.qq.com/cgi-bin/showdocument?action=dir_list&t=resource/res_list&verify=1&id=open1419316505&token=&lang=zh_CN

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。如图 1 所示。

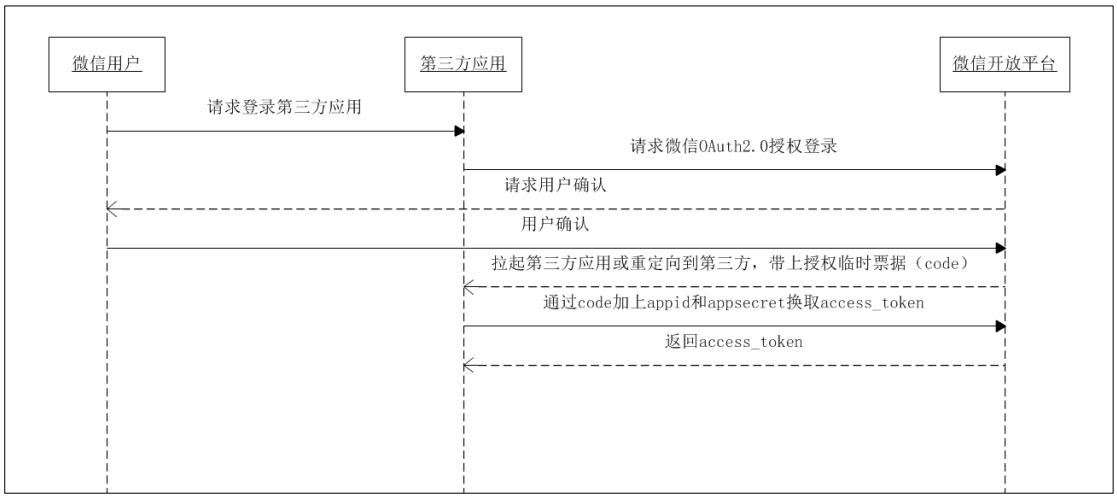
图 1 接入流程

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：



实现步骤

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	重定向地址，需要进行UrlEncode
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即可
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

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）：
  `<script src="http://res.wx.qq.com/connect/zh_CN/htmledition/js/wxLogin.js"></script>`
- 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({
        id:"login_container",
        appid: "",
        scope: "",
        redirect_uri: "",
        state: "",
        style: "",
        href: ""
});
```

其中参数说明：

参数	是否必须	说明
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

一、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
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"}

二、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
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"}

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
	/sns/oauth2/refresh_token	刷新或续期access_token使用
	/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。