微信公众平台开发——微信授权登录（OAuth2.0）

1、OAuth2.0简介

OAuth（开放授权）是一个开放标准，允许用户让第三方应用访问该用户在某一网站上存储的私密的资源（如照片，视频，联系人列表），而无需将用户名和密码提供给第三方应用。

允许用户**提供一个令牌，而不是用户名和密码来访问他们存放在特定服务提供者的数据**。每一个令牌授权一个特定的网站（例如，视频编辑网站)在特定的时段（例如，接下来的2小时内）内访问特定的资源（例如仅仅是某一相册中的视频）。这样，OAuth允许用户授权第三方网站访问他们存储在另外的服务提供者上的信息，而不需要分享他们的访问许可或他们数据的所有内容。

我们这里主要模拟在微信公众号中使用OAuth2.0进行授权，获取用户的基本信息的过程。详细的开发文档可查看微信的官方文档。

微信公众平台开发者文档：

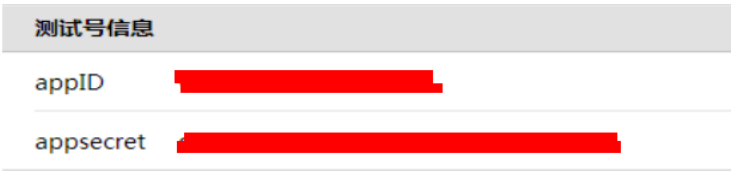
http://mp.weixin.qq.com/wiki/14/89b871b5466b19b3efa4ada8e577d45e.html

2、获取测试公众账号及其相关配置

1）、公众测试账号获取

访问上面的连接，选择“接口测试号申请”获得直接打开http://mp.weixin.qq.com/debug/cgi-bin/sandboxinfo?action=showinfo&t=sandbox/index通过微信客户端扫码登录即可登录。

登录完即可获取到一个测试公众账号的信息。主要有appId和appsecret两个参数，这将唯一标示一个公众号，并且需要将他们作为参数获取用户的信息。



2）、关注公众号

用户只有关注了这个公众号了，才能通过打开有公众号信息的链接去授权第三方登录，并获取用户信息的操作。故我们还需要用我们的微信关注微信号，操作如下：

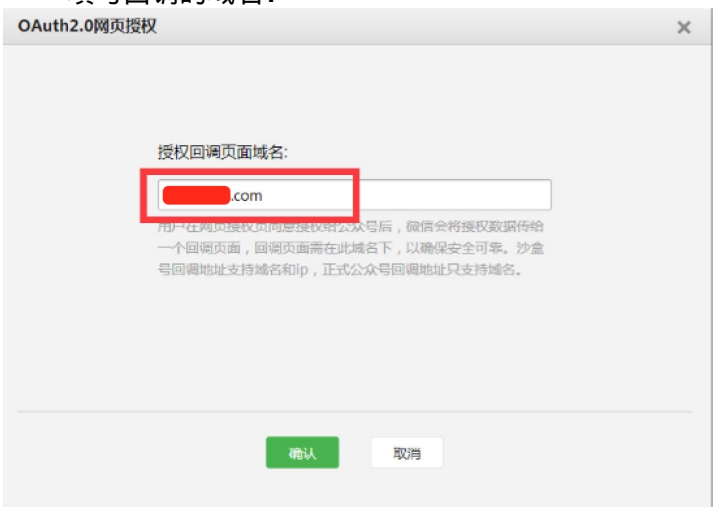
还是刚刚那个登录成功后跳转的页面，我们可以看到，该页面有一个二维码，我们可以通过扫描该二维码进行关注，关注成功在右边的“用户列表”会多一个用户的信息。如下图所示：

3）、配置回调函数

我们在微信客户端访问第三方网页（即我们自己的网页）的时候，我们可以通过微信网页授权机制，我们不仅要有前面获取到的appid和appsecret还需要有当用户授权之后，回调的域名设置，即用户授权后，页面会跳转到哪里。具体的配置如下：

还是在刚刚的页面，有一个“网页授权获取用户基本信息”，点击后面的修改

填写回调的域名：



如果你的网址没有被列入过黑名单，就会在顶部出现

然后，域名配置就成功了！

注意：

```
1、这里填写的是域名（是一个字符串），而不是URL，因此请勿加http://等协议头；
2、授权回调域名配置规范为全域名，比如需要网页授权的域名为：www.qq.com，配置以后此域名下面的页面
http://www.qq.com/music.html 、 http://www.qq.com/login.html 都可以进行OAuth2.0鉴权。但
http://pay.qq.com 、 http://music.qq.com 、 http://qq.com无法进行OAuth2.0鉴权
```

到这里，我们就获取到我们必须用到的测试信息了，包括

- 公众号appID、appsecret的获取；
- 关注我们测试的公众号；
- 配置扫码用户授权后回调的域名。

3、微信授权登录并获取用户基本信息

微信授权使用的是OAuth2.0授权的方式。主要有以下**简略步骤：**

第一步：用户同意授权，获取code

第二步：通过code换取网页授权access_token

第三步：刷新access_token（如果需要）

第四步：拉取用户信息(需scope为 snsapi_userinfo)

详细的步骤如下：

1．用户关注微信公众账号。

2．微信公众账号提供用户请求授权页面URL。

3．用户点击授权页面URL，将向服务器发起请求

4．服务器询问用户是否同意授权给微信公众账号(scope为snsapi_base时无此步骤)

5．用户同意(scope为snsapi_base时无此步骤)

6．服务器将CODE通过回调传给微信公众账号

7．微信公众账号获得CODE

8．微信公众账号通过CODE向服务器请求Access Token

9．服务器返回Access Token和OpenID给微信公众账号

10．微信公众账号通过Access Token向服务器请求用户信息(scope为snsapi_base时无此步骤)

11．服务器将用户信息回送给微信公众账号(scope为snsapi_base时无此步骤)

1）、用户授权并获取code

在域名（前面配置的回调域名）根目录下，新建一个文件，命名为oauth.php(名字随便你取，下面的redirect_uri做相应修改即可）该php实现的功能也很简单，只是将url上的code参数取出来并打印出来而已，方便我们进行接下来的操作。

Oauth.php中的内容如下：

```
<?php
if (isset($_GET['code'])){
    echo $_GET['code'];
}else{
    echo "NO CODE";
}
?>
```

这个php的主要目的是当用户确认授权登录之后，会调转到redirect_uri这个地址上，并带上code参数（微信生成），我们为了方便获取，这里也可以是一个空白的页面，下面有其他方法得到url上面的code参数。

请求授权页面的构造方式：

```
https://open.weixin.qq.com/connect/oauth2/authorize?
appid=APPID&redirect_uri=REDIRECT_URI&response_type=code&scope=SCOPE&state=STATE#wechat_redi
rect
```

参数说明

参数	必须	说明
appid	是	公众号的唯一标识（这个就是我们前面申请的）
redirect_uri	是	授权后重定向的回调链接地址（我们前面申请的）
response_type	是	返回类型，请填写code

scope	是	应用授权作用域，snsapi_base（不弹出授权页面，直接跳转，只能获取用户openid），snsapi_userinfo（弹出授权页面，可通过openid拿到昵称、性别、所在地。并且，即使在未关注的情况下，只要用户授权，也能获取其信息）
state	否	重定向后会带上state参数，开发者可以填写a-zA-Z0-9的参数值，最多128字节，该值会被微信原样返回，我们可以将其进行比对，防止别人的攻击。
#wechat_redirect	否	直接在微信打开链接，可以不填此参数。做页面302重定向时候，必须带此参数

应用授权作用域：由于snsapi_base只能获取到openid，意义不大，所以我们使用snsapi_userinfo。
回调地址：填写为刚才上传后的oauth.php的文件地址，
state参数：随便一个数字，这里填123

尤其注意：由于授权操作安全等级较高，所以在发起授权请求时，微信会对授权链接做正则强匹配校验，**如果链接的参数顺序不对，授权页面将无法正常访问**

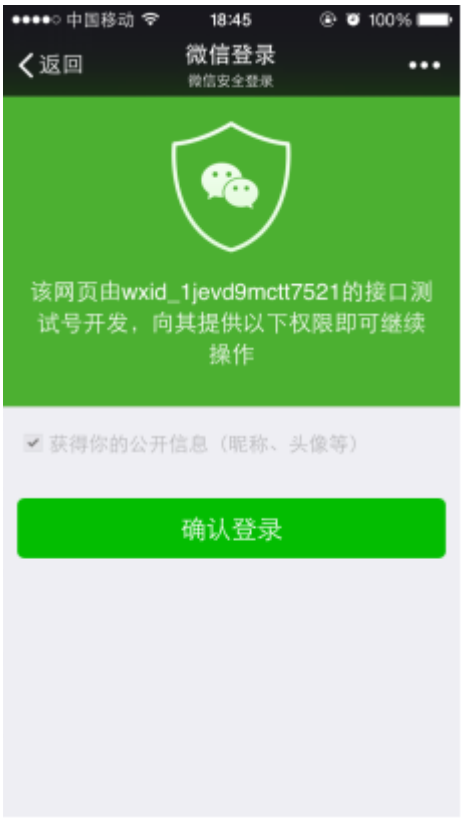
构造请求url如下：

```
https://open.weixin.qq.com/connect/oauth2/authorize?appid=wx4a22b50d7e897f97&redirect_uri=http%3a%2f%2fad.seewo.com%2foauth.php&response_type=code&scope=snsapi_userinfo&state=123#wechat_redirect
```

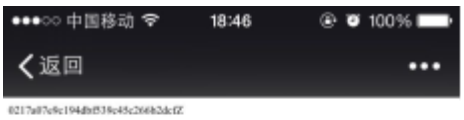
这个需要发到微信中，使用微信浏览器才能打开。

点开上面的链接，点击确认登录即可跳转到刚刚配置的回调页面，并获取了微信传回的code参数，用于下面的操作。

授权页面如下：



授权后跳转的页面（我们前面配置的redirect_uri）：



假如我们没有在php中打印出了code，这个时候我们可以通过右上角按钮中的复制链接，得到链接如下：

```
http://ad.seewo.com/oauth2.php?code=0217a07e9c194dbf539c45c266b2dcfZ&state=123
```

code说明：

```
code作为换取access_token的票据，每次用户授权带上的code将不一样，code只能使用一次，5分钟未被使用自动过期。
```

1）、使用code换取access_token

换取网页授权access_token页面的构造方式：

```
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	公众号的唯一标识
secret	是	公众号的appsecret
code	是	填写第一步获取的code参数
grant_type	是	填写为authorization_code

code：在这里填写为上一步获得的值。
构造的url如下，在网页中打开链接就行：

```
https://api.weixin.qq.com/sns/oauth2/access_token?
appid=wx41cb8dbd827a16e9&secret=d4624c36b6795d1d99dcf0547af5443d&code=00137323023ab55775be09
d6d8e75ffA&grant_type=authorization_code
```

只有获取code的链接必须是在微信客户端中点开的，获取access_token和用户信息可以直接在网页打开即可。

返回说明

正确时返回的JSON数据包如下：

```
{

   "access_token":"ACCESS_TOKEN",

   "expires_in":7200,

   "refresh_token":"REFRESH_TOKEN",

   "openid":"OPENID",

   "scope":"SCOPE"

}
```

参数	描述
access_token	网页授权接口调用凭证,注意：此access_token与基础支持的access_token不同
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	用户唯一标识
scope	用户授权的作用域，使用逗号（,）分隔

错误时微信会返回JSON数据包如下（示例为Code无效错误）:

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

2）、通过access_token、openid获取用户信息

请求方法：

```
https://api.weixin.qq.com/sns/userinfo?access_token=ACCESS_TOKEN&openid=OPENID
```

参数说明

参数	描述
access_token	网页授权接口调用凭证,注意：此access_token与基础支持的access_token不同
openid	用户的唯一标识

构造url如下：

```
https://api.weixin.qq.com/sns/userinfo?
access_token=OezXcEiiBSKSxW0eoylIeABONBTt9gBE6cK3arF_L6aOvwU4ynS5ZxG4r6ZUIJxh7y_ClmPRkYbMeOc
_r30LAGB2IEAlCFsQQvfQMJSwHcU6109-
6vz603Jho4oZhdns6AOXwoxaWcLujT1RWnC_hQ&openid=oF3PcsnsrMiJzEwalZZbAfWQpxCI
```

可以在浏览器中直接执行这个。

得到的json格式数据如下：

```
{

   "openid":" OPENID",

   " nickname": NICKNAME,

   "sex":"1",

   "province":"PROVINCE"

   "city":"CITY",

   "country":"COUNTRY",

    "headimgurl":
"http://wx.qlogo.cn/mmopen/g3MonUZtNHkdmzicIlibx6iaFqAc56vxLSUfpb6n5WKSYVY0ChQKkiaJSgQ1dZuTO
gvLLrhJbERQQ4eMsv84eavHiaiceqxibJxCfHe/46",

"privilege":[

"PRIVILEGE1"

"PRIVILEGE2"

    ],

    "unionid": "o6_bmasdasdsad6_2sgVt7hMZOPfL"

}
```

参数	描述

openid	用户的唯一标识
nickname	用户昵称
sex	用户的性别，值为1时是男性，值为2时是女性，值为0时是未知
province	用户个人资料填写的省份
city	普通用户个人资料填写的城市
country	国家，如中国为CN
headimgurl	用户头像，最后一个数值代表正方形头像大小（有0、46、64、96、132数值可选，0代表640*640正方形头像），用户没有头像时该项为空。若用户更换头像，原有头像URL将失效。
privilege	用户特权信息，json 数组，如微信沃卡用户为（chinaunicom）
unionid	只有在用户将公众号绑定到微信开放平台帐号后，才会出现该字段。详见：获取用户个人信息（UnionID机制）

错误时微信会返回JSON数据包如下（示例为openid无效）：

```
{"errcode":40003,"errmsg":" invalid openid "}
```

值得注意的地方：

用户管理类接口中的“获取用户基本信息接口”，是在用户和公众号产生消息交互或关注后事件推送后，才能根据用户OpenID来获取用户基本信息。这个接口，包括其他微信接口，**都是需要该用户（即openid）关注了公众号后，才能调用成功的。**

网页授权获取用户基本信息也遵循UnionID机制。即如果开发者有在多个公众号，或在公众号、移动应用之间统一用户帐号的需求，需要前往微信开放平台（open.weixin.qq.com）绑定公众号后，才可利用UnionID机制来满足上述需求。

UnionID机制的作用说明：如果开发者拥有多个移动应用、网站应用和公众帐号，可通过获取用户基本信息中的unionid来区分用户的唯一性，因为同一用户，对同一个微信开放平台下的不同应用（移动应用、网站应用和公众帐号），unionid是相同的。

尤其注意：由于公众号的secret和获取到的access_token安全级别都非常高，必须只保存在服务器，不允许传给客户端。后续刷新access_token、通过access_token获取用户信息等步骤，也必须从服务器发起。

微信网页扫码登录：http://www.cnblogs.com/0201zcr/p/5133062.html

微信公众号群发消息：http://www.cnblogs.com/0201zcr/p/5866296.html

致谢：感谢您的阅读！