河北师范大学软件学院
Software College of Hebei Normal University

——微信与移动Web开发之

第11讲 Oauth授权与第三方登录

本次课程目录

河北师范大学软件学院
Software College of Hebei Normal University

一．Oauth协议基础

二．微信网页授权

三．实现第三方登录

课程概要

河北师范大学软件学院
Software College of Hebei Normal University

- Oauth入门，简单了解Oauth。
- 微信网页授权是Oauth2.0协议的具体实现，实现微信网页授权获取用户基本信息。

第一节

河北师范大学软件学院
Software College of Hebei Normal University

一．Oauth协议基础

二．微信网页授权

三．实现第三方登录

什么是Oauth协议

- OAuth（Open Authorization，开放授权）是为用户资源的授权定义了一个安全、开放及简单的标准，第三方无需知道用户的账号及密码，就可获取到用户的授权信息，并且这是安全的。
- 目前的版本是2.0。

应用场景

- OAuth的出现是为了解决这样一个问题：

  场景：

  1，你有一个Flickr帐号，在上面有很多照片；

  2，你需要使用某照片打印网站打印Flickr上面的照片，你可以：

  2.1，从Flickr下载照片到本地，然后从电脑里上传照片到打印网站；

  2.2，在照片打印网站输入Flickr的帐号密码，直接让网站去Flickr读照片；

  问题：把Flickr帐号密码透露给了第三方。

- 解决方案：

  OAuth是让第三方应用不需要用户名密码读取用户数据的一个认证过程。

  上面的场景中，Flickr有API支持OAuth，那么打印网站需要根据API注册应用，打印网站可以要求用户授权访问Flickr照片，而不是提供Flickr的帐号密码。这个授权过程就是OAuth的作用。

Oauth的思路

- OAuth在"客户端"与"服务提供商"之间，设置了一个授权层（authorization layer）。"客户端"不能直接登录"服务提供商"，只能登录授权层，以此将用户与客户端区分开来。"客户端"登录授权层所用的令牌（token），与用户的密码不同。用户可以在登录的时候，指定授权层令牌的权限范围和有效期。
- "客户端"登录授权层以后，"服务提供商"根据令牌的权限范围和有效期，向"客户端"开放用户储存的资料。

Oauth优点

- 安全性更高，用户仅需对需要的操作授权，同时不用提供账号密码。
- 不需要针对不同的网站注册多个账号，使用授权就可以实现一个账号通过授权的方式登录不同的网站。

基本处理流程

（A）用户打开客户端以后，客户端要求用户给予授权。

（B）用户同意给予客户端授权。

（C）客户端使用上一步获得的授权，向认证服务器申请令牌。

（D）认证服务器对客户端进行认证以后，确认无误，同意发放令牌。

（E）客户端使用令牌，向资源服务器申请获取资源。

（F）资源服务器确认令牌无误，同意向客户端开放资源。

第二讲

河北师范大学软件学院
Software College of Hebei Normal University

一．Oauth协议基础

二．微信网页授权

三．实现第三方登录

如何配置

- 1、在微信公众号请求用户网页授权之前，开发者需要先到公众平台官网中的“开发 - 接口权限 - 网页服务 - 网页帐号 - 网页授权获取用户基本信息”的配置选项中，修改授权回调域名。请注意，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 。

微信授权类型说明

- 1、以snsapi_base为scope发起的网页授权，是用来获取进入页面的用户的openid的，并且是静默授权并自动跳转到回调页的。用户感知的就是直接进入了回调页（往往是业务页面）
- 2、以snsapi_userinfo为scope发起的网页授权，是用来获取用户的基本信息的。但这种授权需要用户手动同意，并且由于用户同意过，所以无须关注，就可在授权后获取该用户的基本信息。
- 3、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。

微信授权处理流程1

河北师范大学软件学院
Software College of Hebei Normal University

第一步：用户同意授权，获取**code**

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

参数	是否必须	说明
appid	是	公众号的唯一标识
redirect_uri	是	授权后重定向的回调链接地址，请使用urlEncode对链接进行处理
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
#wechat_redirect	是	无论直接打开还是做页面302重定向时候，必须带此参数

微信授权处理流程2

河北师范大学软件学院
Software College of Hebei Normal University

第二步：通过code换取网页授权access_token

https://api.weixin.qq.com/sns/oauth2/access_token?appid=APPID&secret=SECRET&code=CODE&grant_type=authorization_code

注意：这里通过code换取的是一个特殊的网页授权access_token,与基础支持中的access_token（该access_token用于调用其他接口）不同。公众号可通过下述接口来获取网页授权access_token。如果网页授权的作用域为snsapi_base，则本步骤中获取到网页授权access_token的同时，也获取到了openid，snsapi_base式的网页授权流程即到此为止。

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

获取网页access_token返回值

- 正确：

```
{
 "access_token":"ACCESS_TOKEN",
 "expires_in":7200,
 "refresh_token":"REFRESH_TOKEN",
 "openid":"OPENID",
 "scope":"SCOPE"
}
```

- 错误：

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

微信授权处理流程3

河北师范大学软件学院
Software College of Hebei Normal University

第三步：刷新**access_token**（如果需要）

https://api.weixin.qq.com/sns/oauth2/refresh_token?appid=APPID&grant_type=refresh_token&refresh_token=REFRESH_TOKEN

由于access_token拥有较短的有效期，当access_token超时后，可以使用refresh_token进行刷新，refresh_token有效期为30天，当refresh_token失效之后，需要用户重新授权。

参数	是否必须	说明
appid	是	公众号的唯一标识
grant_type	是	填写为refresh_token
refresh_token	是	填写通过access_token获取到的refresh_token参数

微信授权处理流程4

河北师范大学软件学院
Software College of Hebei Normal University

第四步：拉取用户信息(需scope为 snsapi_userinfo)

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

- 正确时返回的JSON数据包如下：

{ "openid":" OPENID",
" nickname": NICKNAME,
"sex":"1",
"province":"PROVINCE"
"city":"CITY",
"country":"COUNTRY",
"headimgurl": "http://wx.qlogo.cn/mmopen/g3MonUZt
NHkdmzicIlibx6iaFqAc56vxLSUfpb6n5WKSYVY0ChQKkiaJSg
Q1dZuTOgvLLrhJbERQQ
4eMsv84eavHiaiceqxibJxCfHe/46",
"privilege":["PRIVILEGE1" "PRIVILEGE2"],
"unionid": "o6_bmasdasdsad6_2sgVt7hMZOPfL"
}

- 错误：{"errcode":40003,"errmsg":" invalid openid "}

返回信息参数说明

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。

第三讲

河北师范大学软件学院
Software College of Hebei Normal University

一．Oauth协议基础

二．微信网页授权

三．实现第三方登录

如何实现第三方登录

- 这里的实现方式采用oauth_code.php获取code授权码。
- 之后跳转到oauth_return.php根据codes授权码获取Oauth授权的access_token。
- 然后按照接口要求构造api参数调用授权接口获取用户信息。
- 使用数据库记录用户信息，检查是有已经记录过，如果没有记录则创建一条数据记录。

河北师范大学软件学院
Software College of Hebei Normal University

感谢聆听！

THANK YOU FOR YOUR ATTENTION