链滴

# OAuth 2.0 授权流程

作者：akstianye
原文链接：https://ld246.com/article/1493996803551
来源网站：链滴
许可协议：署名-相同方式共享 4.0 国际 (CC BY-SA 4.0)

客户端必须得到用户的授权（authorization grant），才能获得令牌（access token）。OAuth 2.0义了四种授权方式。

- 授权码模式（authorization code）
- 简化模式（implicit）//不常用
- 密码模式（resource owner password credentials）
- 客户端模式（client credentials）// 不常用

---

一、授权码模式

1.用户访问客户端，后者将前者导向认证服务器。

2.用户选择是否给予客户端授权。

3.假设用户给予授权，认证服务器将用户导向客户端事先指定的"重定向URI"（redirection URI），时附上一个授权码。

4.客户端收到授权码，附上早先的"重定向URI"，向认证服务器申请令牌。这一步是在客户端的后台服务器上完成的，对用户不可见。

5.认证服务器核对了授权码和重定向URI，确认无误后，向客户端发送访问令牌（access token）和新令牌（refresh token）。

---

二、密码模式

1.用户向客户端提供用户名和密码。

2.客户端将用户名和密码发给认证服务器，向后者请求令牌。

3.认证服务器确认无误后，向客户端提供访问令牌。

---

三、简化模式

1.客户端将用户导向认证服务器。

2.用户决定是否给于客户端授权。

3.假设用户给予授权，认证服务器将用户导向客户端指定的"重定向URI"，并在URI的Hash部分包含访问令牌。

4.浏览器向资源服务器发出请求，其中不包括上一步收到的Hash值。

5.资源服务器返回一个网页，其中包含的代码可以获取Hash值中的令牌。

6.浏览器执行上一步获得的脚本，提取出令牌。

7.浏览器将令牌发给客户端。