13 令牌颁发方式 之 刷新令牌

Refresh Token（刷新令牌）

上一篇 授权码模式 就说了，在授权码模式颁发令牌时，当发现该客户端支持 REFRESH\_TOKEN 模式时，还会返回刷新令牌。

客户端可以使用刷新令牌(refresh token)重新获取访问令牌(access token)。（一般来说访问令牌时效会比较短，刷新令牌时效比较长，通过刷新令牌获取访问令牌可以避免多次授权）

示例

同样的，我们用一个示例来讲解。

环境准备

授权服务器

基于 快速搭建一个授权服务器 文章中的示例，修改 SecurityConfiguration 中 registeredClientRepository() 方法，如下：

@Bean

public RegisteredClientRepository registeredClientRepository() {

RegisteredClient registeredClient3 = RegisteredClient.withId(UUID.randomUUID().toString())

.clientId("client3")

.clientSecret("{noop}secret3")

.clientAuthenticationMethod(ClientAuthenticationMethod.CLIENT\_SECRET\_POST)

.authorizationGrantType(AuthorizationGrantType.AUTHORIZATION\_CODE)

// 支持 刷新令牌！

.authorizationGrantType(AuthorizationGrantType.REFRESH\_TOKEN)

.redirectUri("https://cn.bing.com")

.scope("test")

.clientSettings(ClientSettings.builder().requireAuthorizationConsent(true).build())

.build();

return new InMemoryRegisteredClientRepository(registeredClient3 );

}

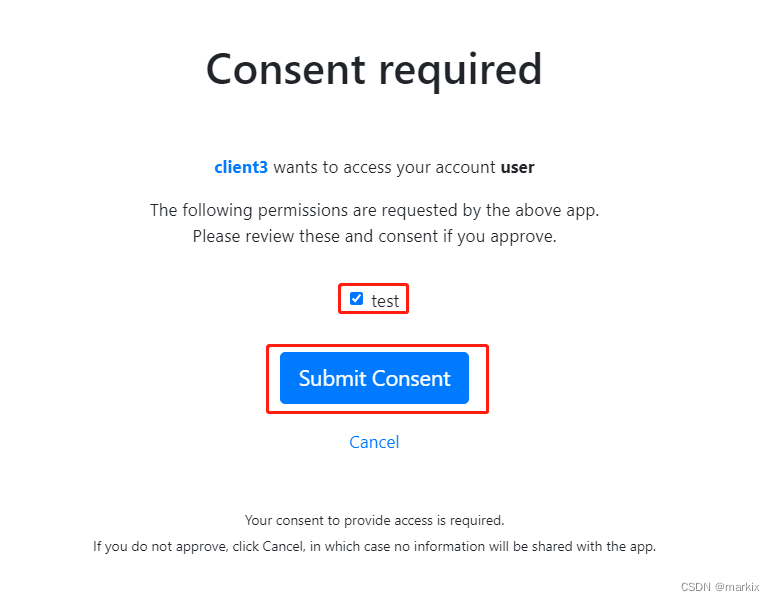
测试

实际上流程和上一篇 授权码模式 一样，下面为了文章完整性，这里也完整列出来。

客户端发起授权请求（浏览器访问）

http://localhost:9000/oauth2/authorize?response\_type=code&client\_id=client3&redirect\_uri=https://cn.bing.com&scope=test

用户授权：勾选 test，点击 Submit Consent



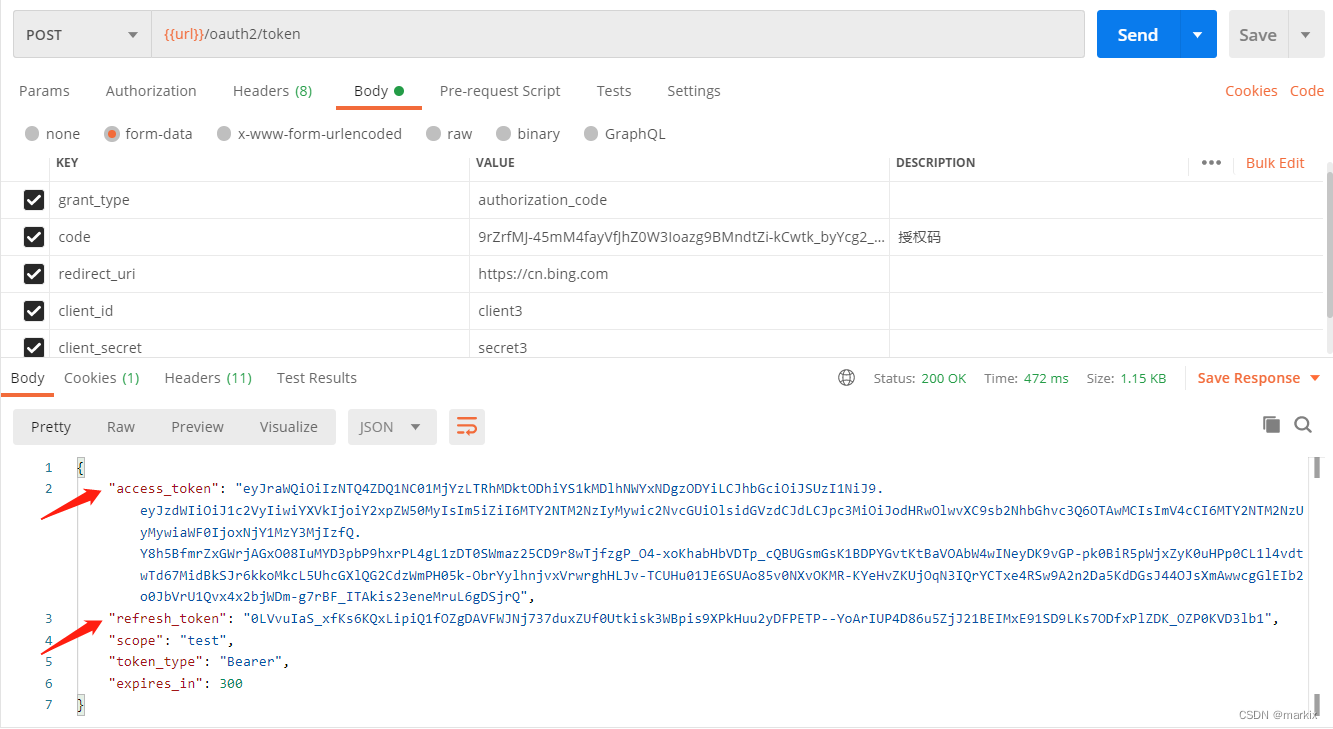
客户端拿到授权码code

用户授权后，会重定向到我们传的redirect\_uri，在url上可以得到授权码code。

https://cn.bing.com/?code=6aEHTI6cAoHjZbt9qKEW7LwsyIFx9PH43YRBsWZCMrbi3JlrD215dtQXID2vqZ8lR97ABGH0tU9JY7OdV7ZG1CPlf1WdbBHL1tVe8gpPQ5NI7XhWvlKYQVpDI-s-72ze

通过 授权码 获取 访问令牌

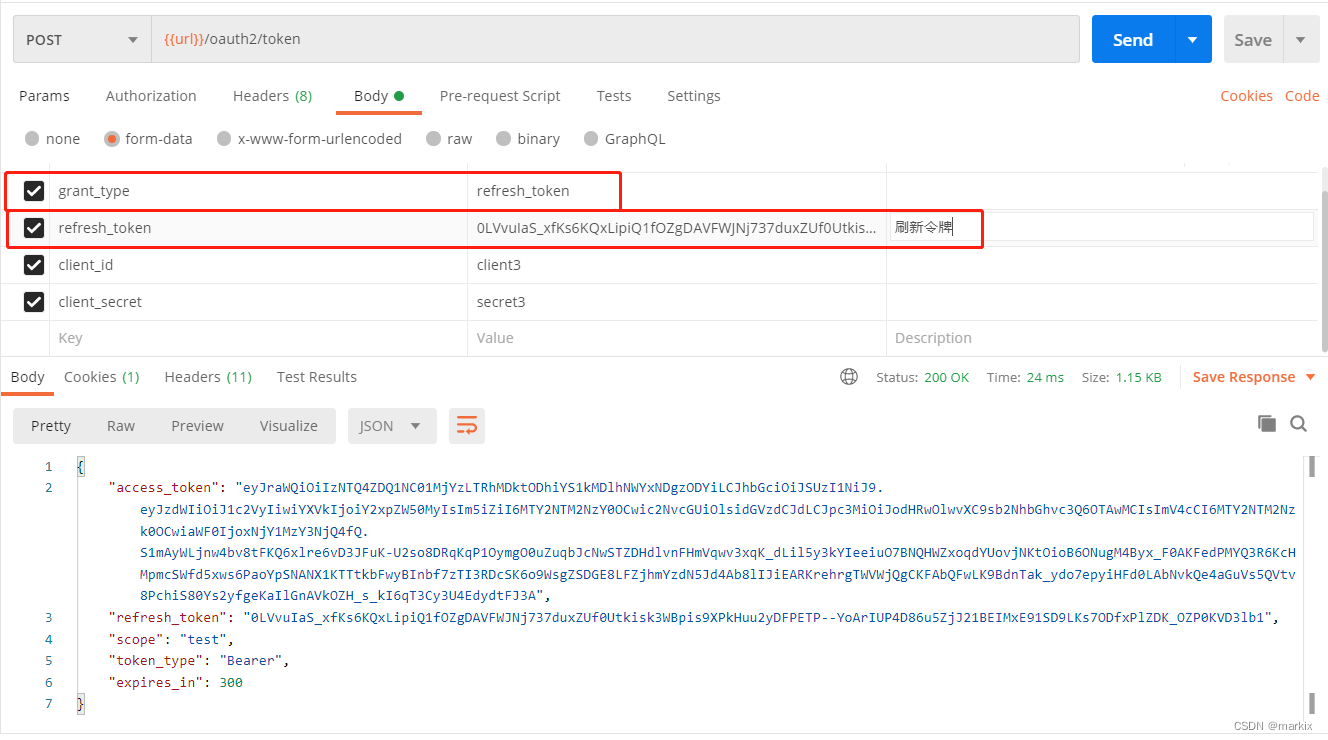
便于测试，直接用postman。在Body栏，填入’grant\_type=authorization\_code’、code、client\_id、client\_secret，发送请求。



可以看到，同时返回了 access\_token（访问令牌）和 refresh\_token（刷新令牌）。这就是支持刷新令牌的授权码流程。

通过 刷新令牌 获取 访问令牌

便于测试，直接用postman。在Body栏，填入’grant\_type=refresh\_token’、refresh\_token、client\_id、client\_secret，发送请求。



如上，有了刷新令牌，我们就能在有效期内重新获取访问令牌了。

源码分析

关于授权码流程的逻辑我们上一篇已经分析过了，这里就来单独分析 “通过 刷新令牌 获取 访问令牌” 这一步骤的相关逻辑。

涉及到两个核心类：OAuth2RefreshTokenAuthenticationConverter 和 OAuth2RefreshTokenAuthenticationProvider

OAuth2RefreshTokenAuthenticationConverter

判断请求参数 grant\_type 的值是否为 refresh\_token，若是，则构建 OAuth2RefreshTokenAuthenticationToken。

OAuth2RefreshTokenAuthenticationProvider

核心逻辑就是先验证 refresh token 的有效期，最后生成 access token（访问令牌）和 refresh token（刷新令牌）。基本和授权码流程的实现差不多，读者可自行阅读。

end