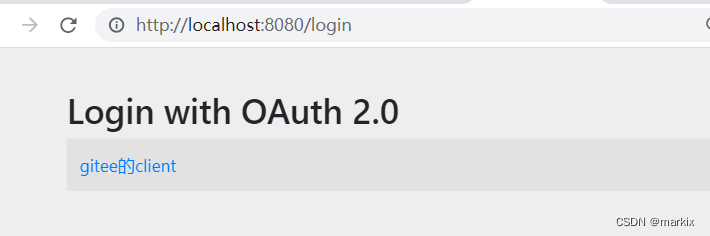
16 OAuth2登录流程分析

上文已经简单说过，OAuth2登录的基本实现原理是：Client获取用户授权，得到令牌，通过令牌，获取用户信息（资源）。再在本地构建用户登录认证信息，维持用户会话状态，以此达到登录的目的。

下文便从源码层面进行分析

OAuth2登录从这里开始



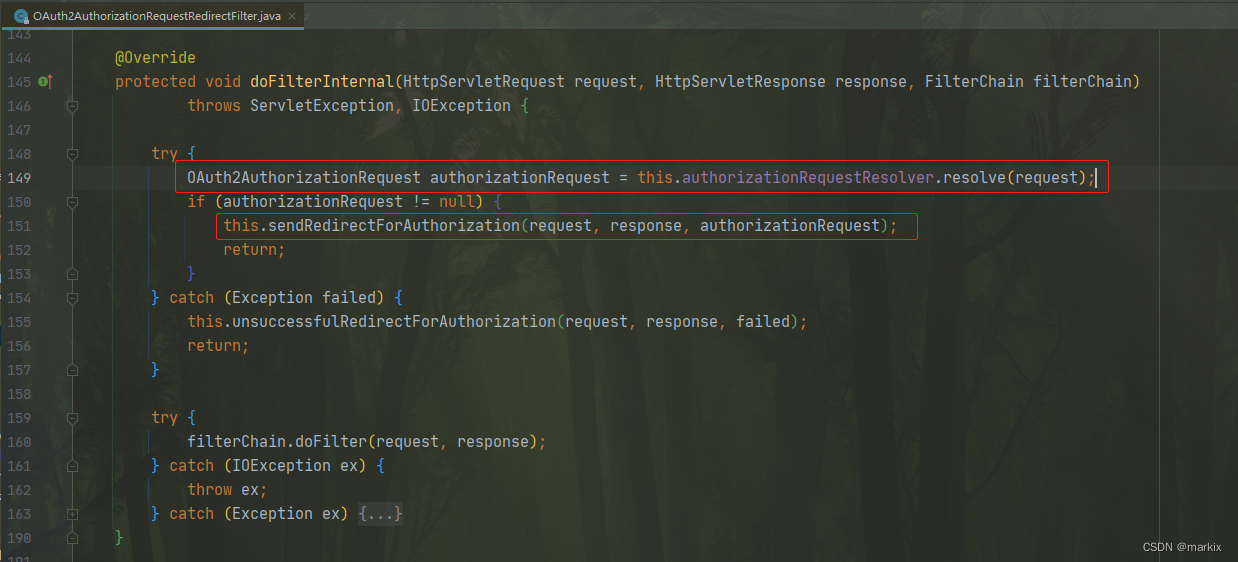
点击“gitee的client”时，会发出 /oauth2/authorization/gitee-app 请求。后台会由 OAuth2AuthorizationRequestRedirectFilter 处理。

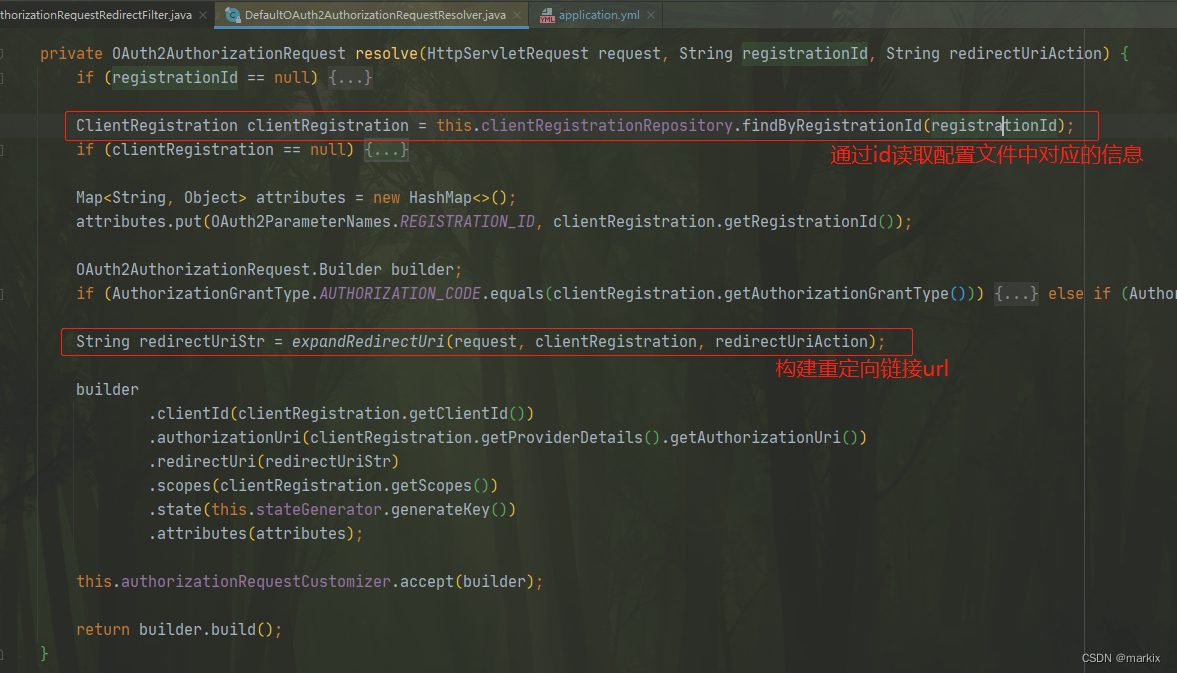
OAuth2AuthorizationRequestRedirectFilter 的核心处理逻辑

解析url中的client id

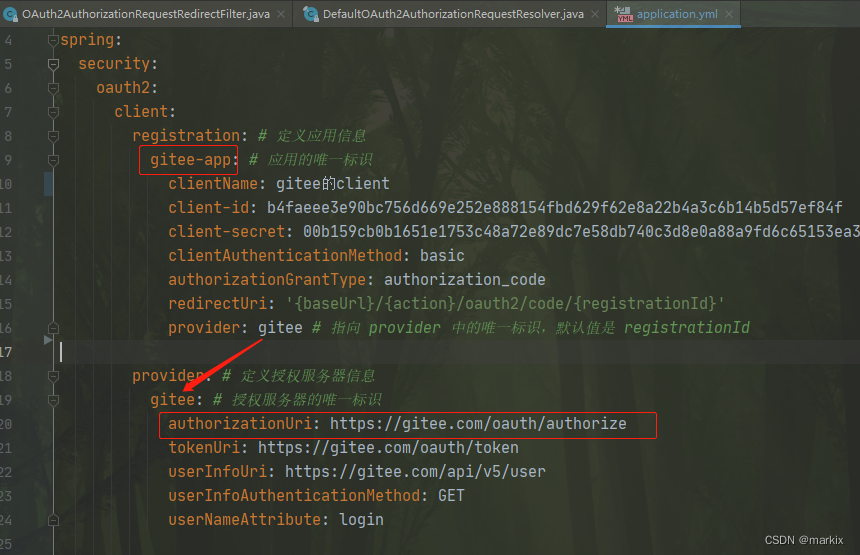
通过id读取配置文件中对应的信息

构建重定向链接





配置信息也就是在application.yml 之中



重定向链接如下：

https://gitee.com/oauth/authorize?response\_type=code&client\_id=b4faeee3e90bc756d669e252e888154fbd629f62e8a22b4a3c6b14b5d57ef84f&state=PToZKXTpmH7MlxqdC1FbEyYnKQ7kYeUavcSZ3-3-WAI%3D&redirect\_uri=http://localhost:8080/login/oauth2/code/gitee-app

浏览器会重定向上述链接，也就是gitee的授权页面

gitee用户授权后，会重新重定向到我们应用，链接如下：后台会由 OAuth2LoginAuthenticationFilter 处理

http://localhost:8080/login/oauth2/code/gitee-app?code=2885e6579426ae449169d4339a1f21c73a3aae3fb84e4232fde7cf2668387bf8&state=PToZKXTpmH7MlxqdC1FbEyYnKQ7kYeUavcSZ3-3-WAI%3D

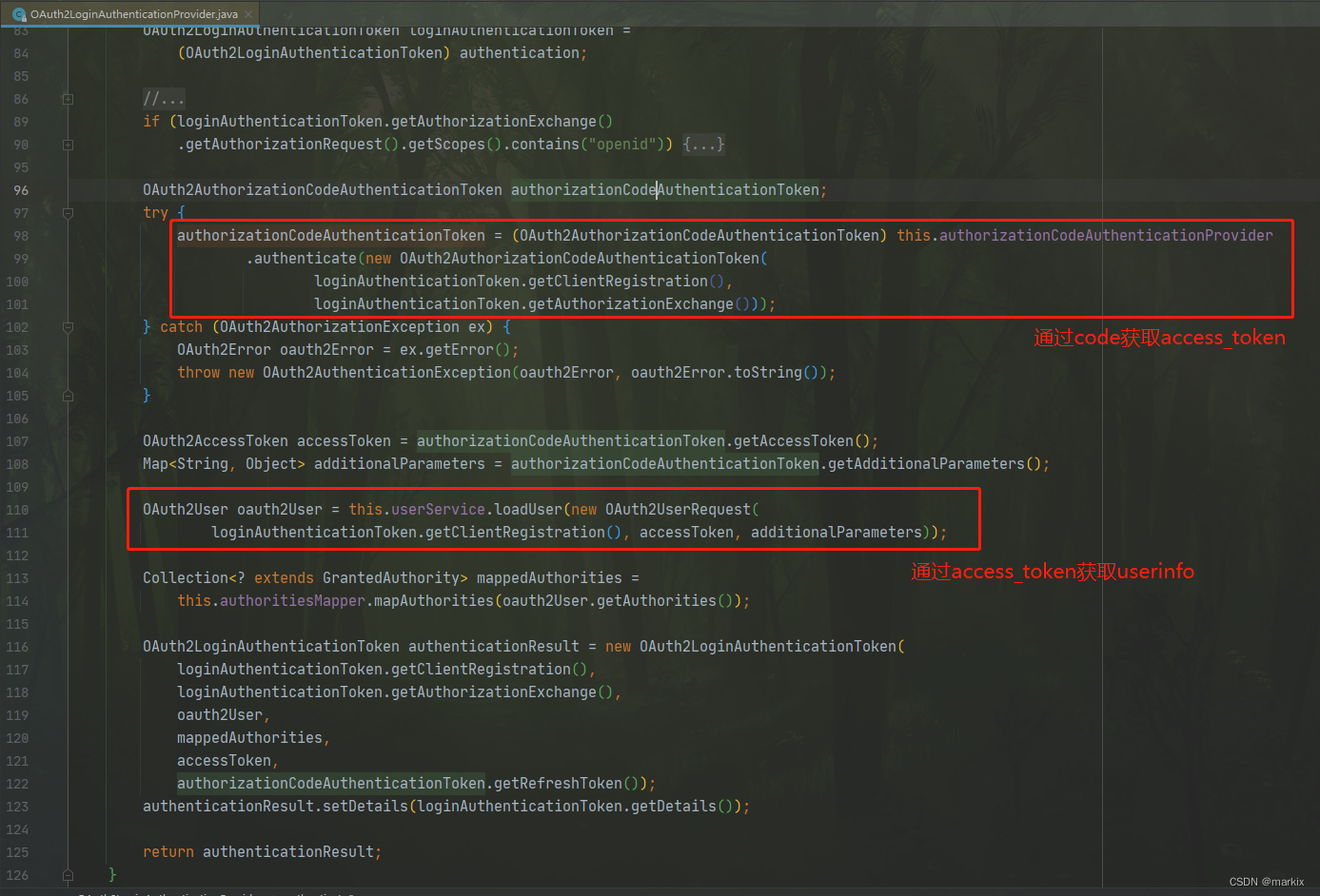
OAuth2LoginAuthenticationFilter 处理逻辑

解析请求参数

构建 OAuth2LoginAuthenticationToken，后续由Provider处理

OAuth2AuthorizationCodeAuthenticationProvider 负责通过 code 获取 access\_token。

OAuth2LoginAuthenticationProvider 负责通过 access\_token 获取 gitee用户信息，再构建认证信息。



最终是由SpringSecurity统一的机制，将认证信息保存在会话（默认是session）中。表明用户已经登录。

核心组件

OAuth2AuthorizationRequestRedirectFilter

OAuth2LoginAuthenticationFilter

OAuth2AuthorizationCodeAuthenticationProvider

OAuth2LoginAuthenticationProvider