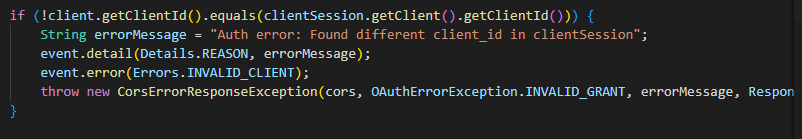
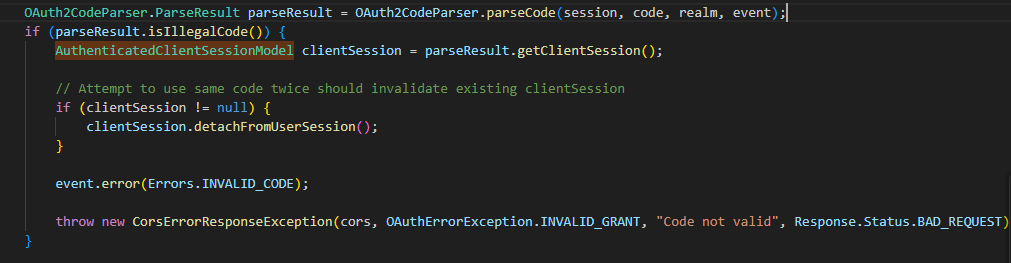
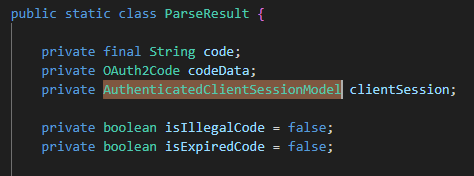
调研  
keycloak  
疑似实现了，code和client\_id存储在服务器端的session里，考虑下一步测试session跟id强是绑定吗，能否尝试绕过

services/src/main/java/org/keycloak/protocol/oidc/grants/AuthorizationCodeGrantType.java  


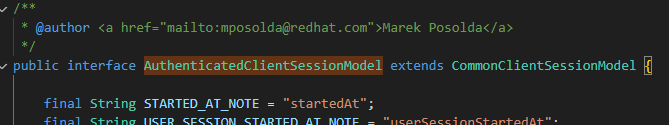
services/src/main/java/org/keycloak/protocol/oidc/grants/AuthorizationCodeGrantType.java



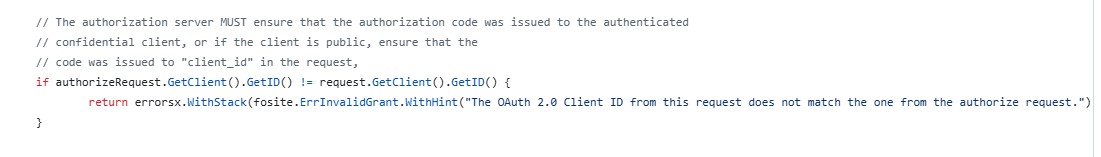
services/src/main/java/org/keycloak/models/AuthenticatedClientSessionModel.java



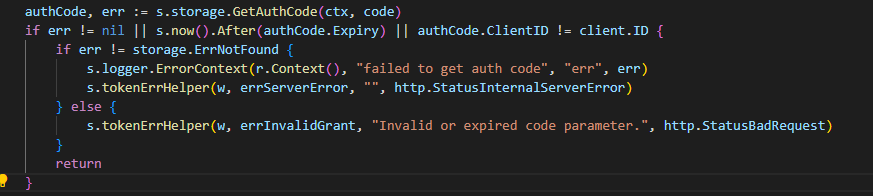
Server-spi/src/main/java/org/keycloak/sessions/CommonClientSessionModel

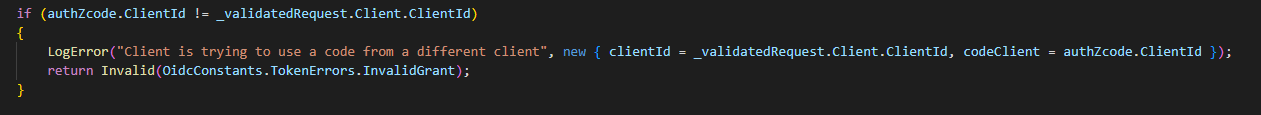


services/src/main/java/org/keycloak/protocol/oidc/ytils/OAuth2CodeParser.java

hydra oauth使用fosite服务器框架  
把授权请求以结构体形式存储在内存，以授权请求和token请求的id比对，下一步考虑如何从请求造假的角度尝试绕过，用假请求欺骗服务器存储一个可被复用提取到的敌手id

dex  
从storage中拿code信息，顺便做id比对，跟hydra类似，放在内存里



identityServer4  
授权请求和token请求的id比对  
跟hydra存储方式类似，但代码逻辑稍有区别，暂时没想到怎么测试攻击

mitreid-connectOpenID-Connect-Java-Spring-Server  
只有通过授权码查找实体后，提取认证信息，建立token时，没有发现认证信息中的id被提取验证，需要进一步查看代码，并考虑搭建测试框架。



