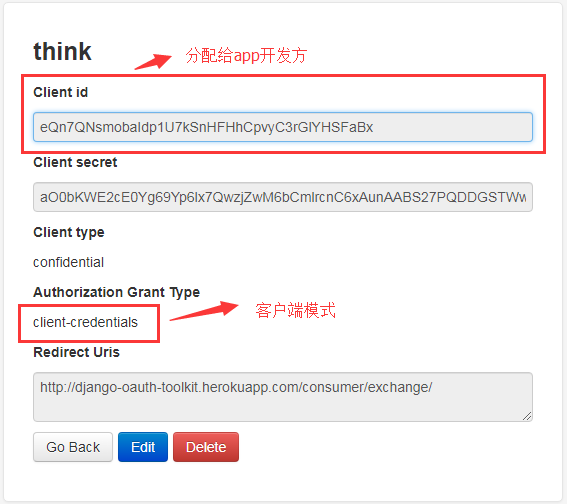
**接口安全设计初步方案**

为保障接口安全和页面只在特定app打开，初步设定安全方案如下：

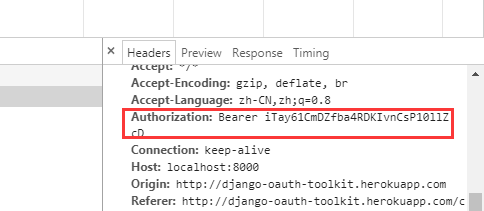
认证鉴权方式：采用OAuth2.0的客户端模式。具体操作办法：

1、创建应用。获取到client id分配给app开发方



2、使用rsa加密解密方案，生成公钥和私钥，并把私钥也给app开发方。我们保留私钥方便做解密。

3、app开发方拿到client id、client secret和公钥后，开发中需要使用iframe打开我们的爬虫页面之前，需要先获取access\_token, 并将access\_token放到请求头进行请求，才能打开我们的爬虫页面。比如：



4、获取access\_token的方法。

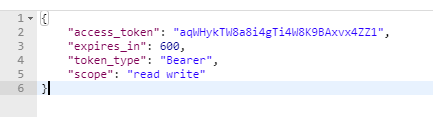
App开发方根据获取到的密钥加密client id、client secret和timestamp（13位）,并将加密后的信息post提交到爬虫服务器：

<http://localhost:8000/get_access_token?info>=密文

爬虫服务器接收到加密的信息之后，根据私钥进行解密，得到client id和client secret的明文, 然后post请求token地址，比如：

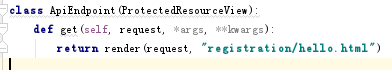
<http://localhost:8000/o/token/?client_id=eQn7QNsmobaIdp1U7kSnHFHhCpvyC3rGlYHSFaBx&grant_type=client_credentials&client_secret=aO0bKWE2cE0Yg69Yp6lx7QwzjZwM6bCmlrcnC6xAunAABS27PQDDGSTWwx34jqwZ1VJ2C90WY0o7VuC413ICnwcHux27P5CzxjjPnwz0n9Hfufkf1NqvPq1jib4Rnqs7>

得到返回带有access\_token和expires\_in等信息：



Access\_token过期时间可以设置，建议10分钟

5、爬虫页面的处理。App中使用access\_token打开页面之后，页面中需要获取access\_token并一直使用带有access\_token的请求头进行访问。同时，爬虫代码也需要做一些修改，凡是需要用access\_token才能访问到的请求代码，需要继承ProtectedResourceView，并实现其对应的get或者post方法，比如：



特别备注：该方案主要问题要防止app被反编译而获取到私钥信息，采用代码混淆和360加固可以从一定程度上改善app被反编译的问题。