**同程旅行app存在敏感信息泄露**

漏洞简述

同程旅行app存在敏感信息泄露，攻击者可以通过反编译获得百度token，从而任意调用api付费服务

复现步骤

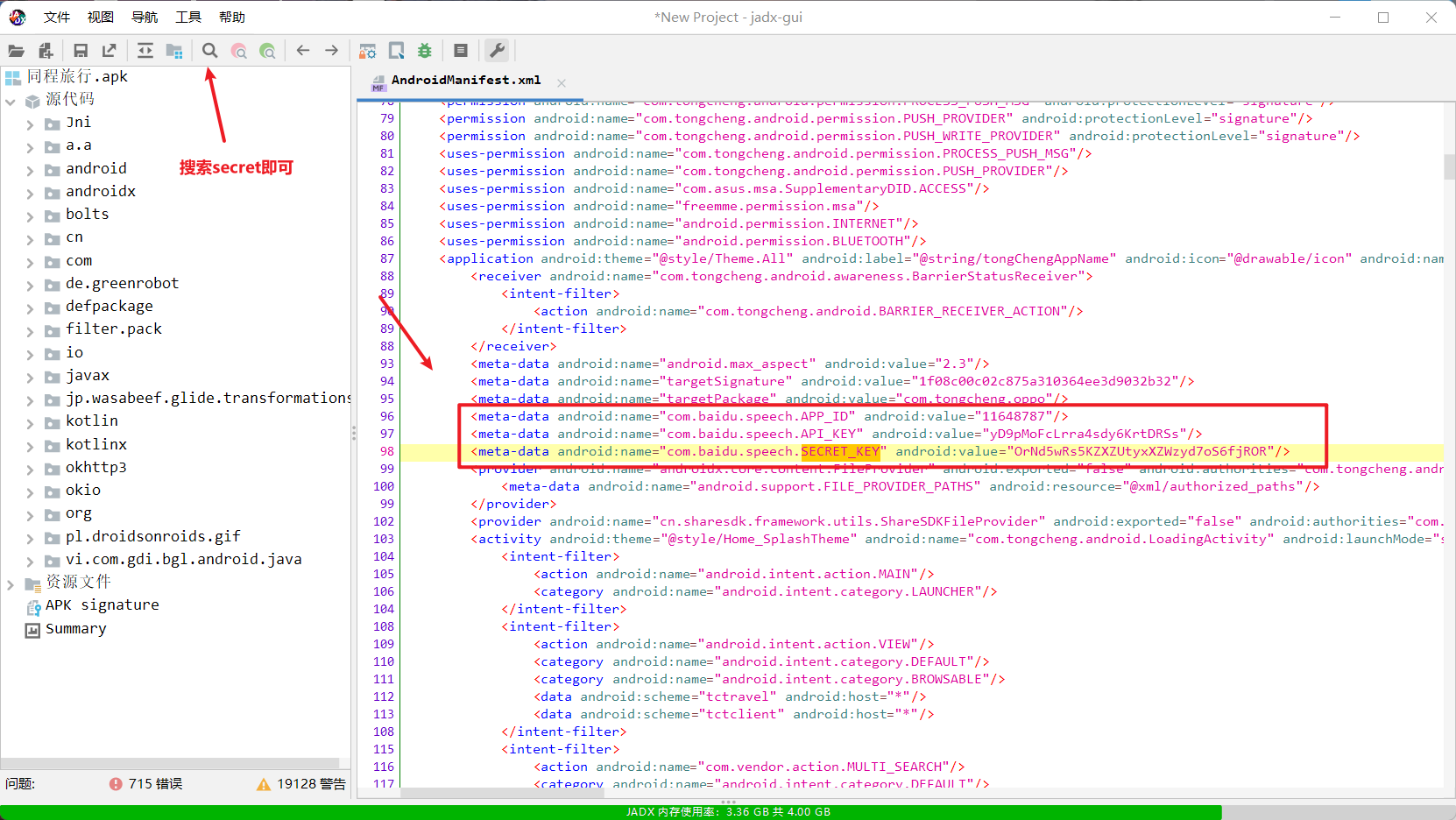
下载app

<https://www.wandoujia.com/apps/39733>



利用工具进行反编译





此处泄露百度api

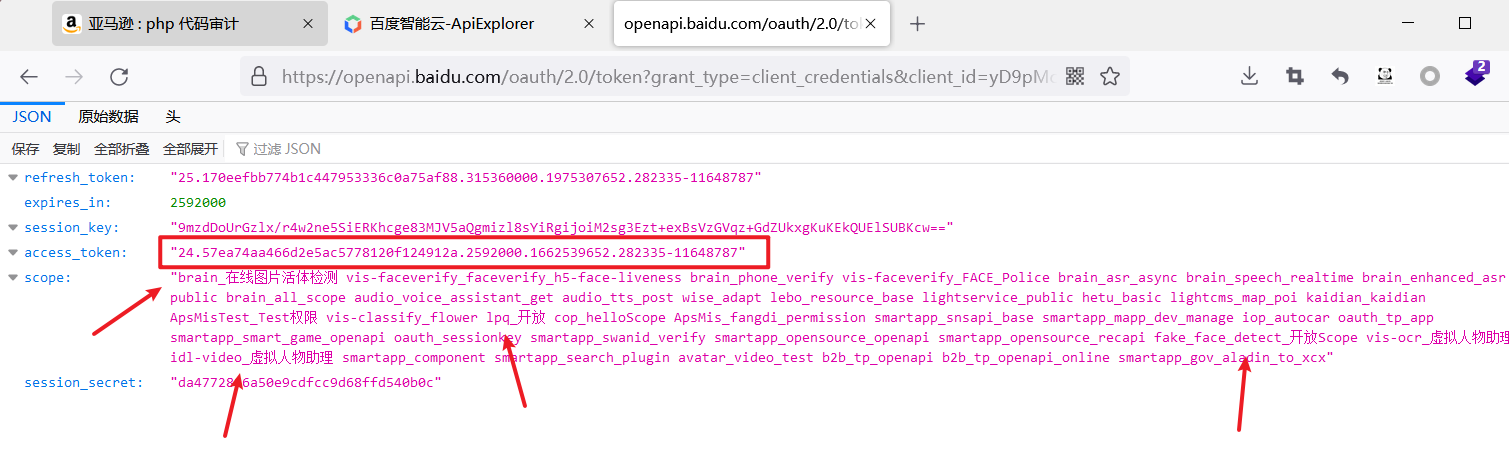
<meta-data android:name="com.baidu.speech.APP\_ID" android:value="11648787"/>

<meta-data android:name="com.baidu.speech.API\_KEY" android:value="yD9pMoFcLrra4sdy6KrtDRSs"/>

<meta-data android:name="com.baidu.speech.SECRET\_KEY" android:value="OrNd5wRs5KZXZUtyxXZWzyd7oS6fjROR"/>

利用官方文档进行调用获取access\_token

https://openapi.baidu.com/oauth/2.0/token?grant\_type=client\_credentials&client\_id=yD9pMoFcLrra4sdy6KrtDRSs&client\_secret=OrNd5wRs5KZXZUtyxXZWzyd7oS6fjROR&scope=smartapp\_snsapi\_base

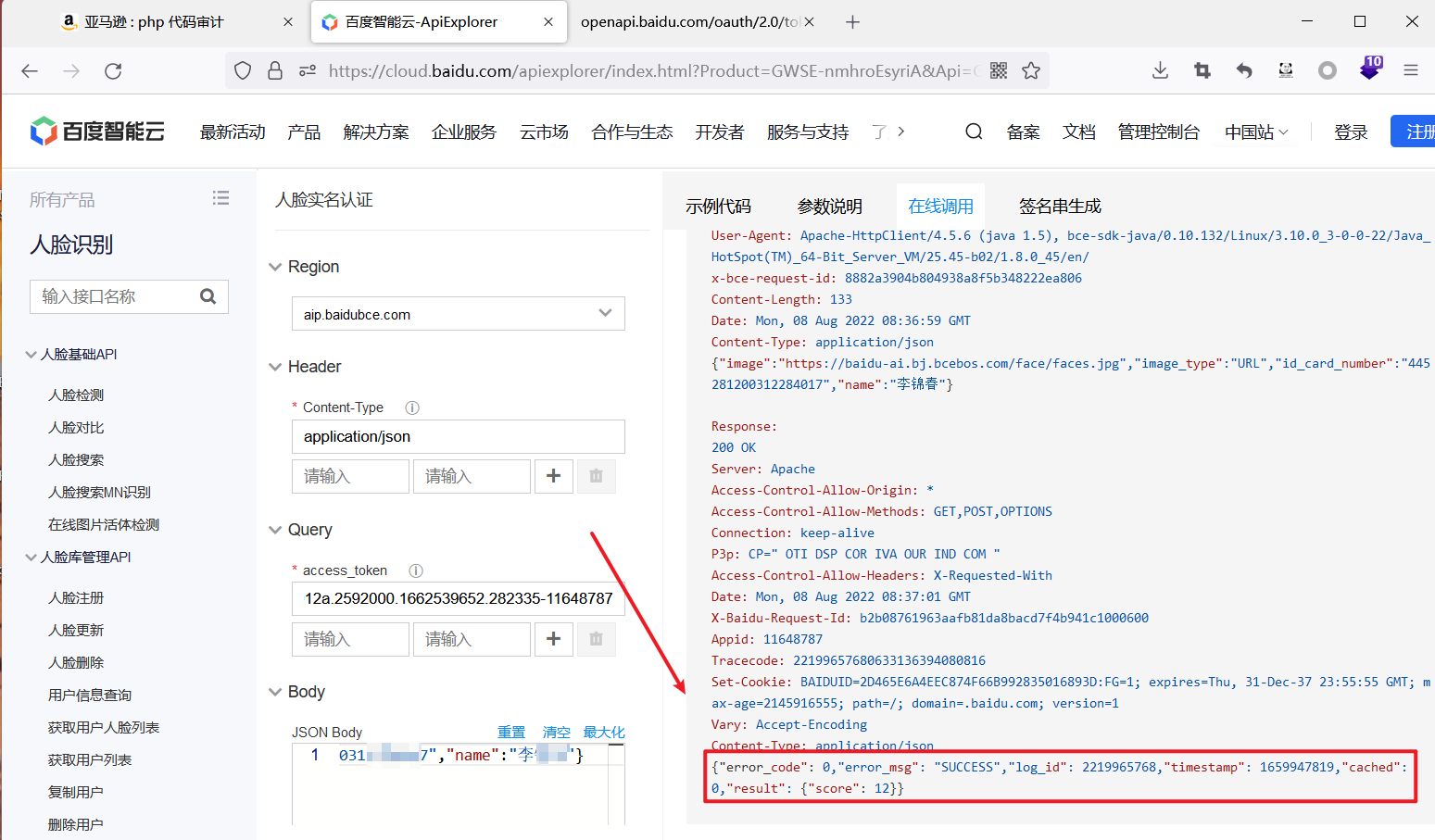


成功获取到accesstoken值，并且看到此处使用了大量的付费接口

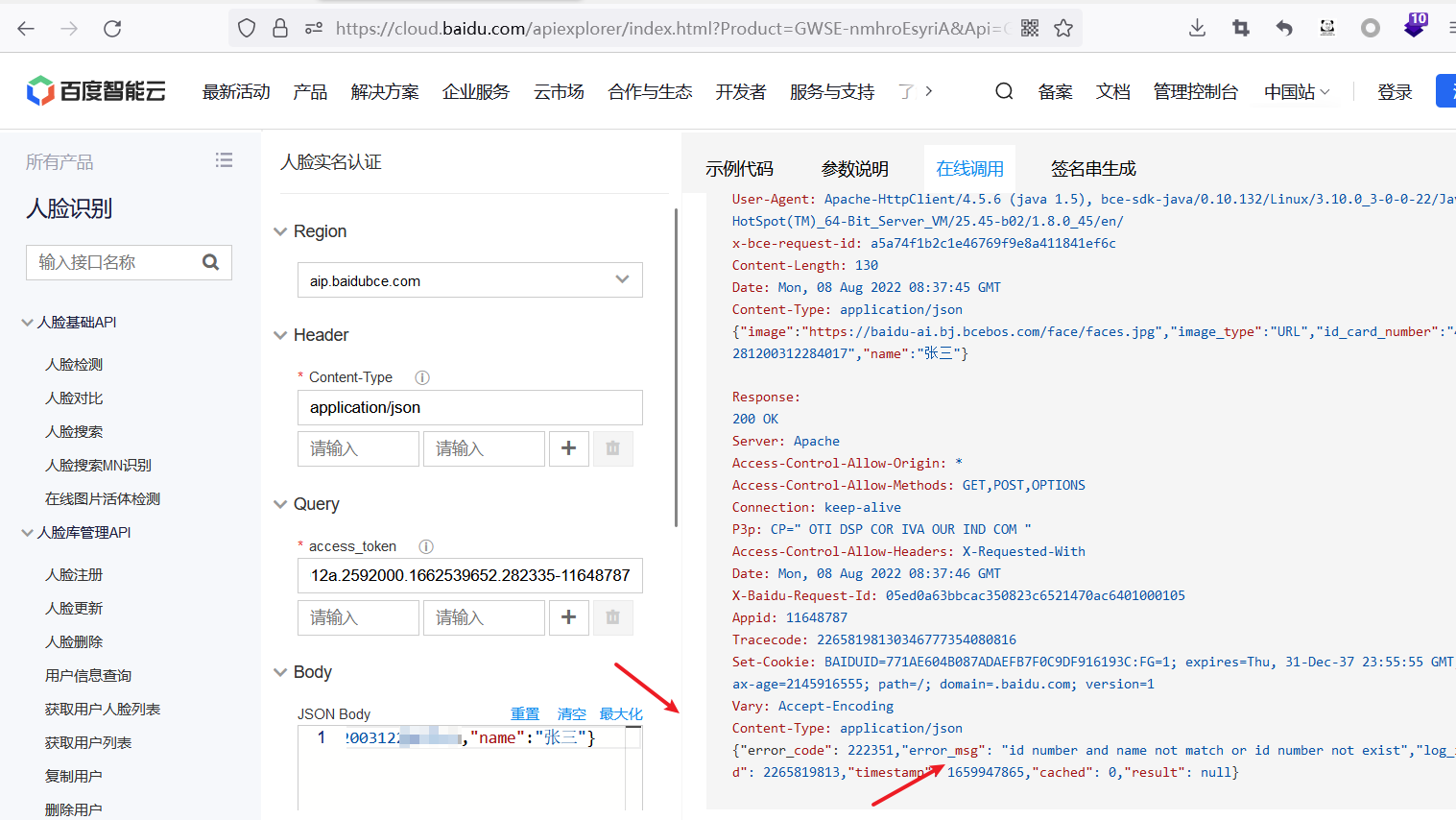
|  |  |
| --- | --- |
| access\_token | ："24.57ea74aa466d2e5ac5778120f124912a.2592000.1662539652.282335-11648787" |

于是尝试调用付费接口，利用百度的在线工具

<https://cloud.baidu.com/apiexplorer/index.html?Product=GWSE-nmhroEsyriA&Api=GWAI-PZVqcHoyUhD>

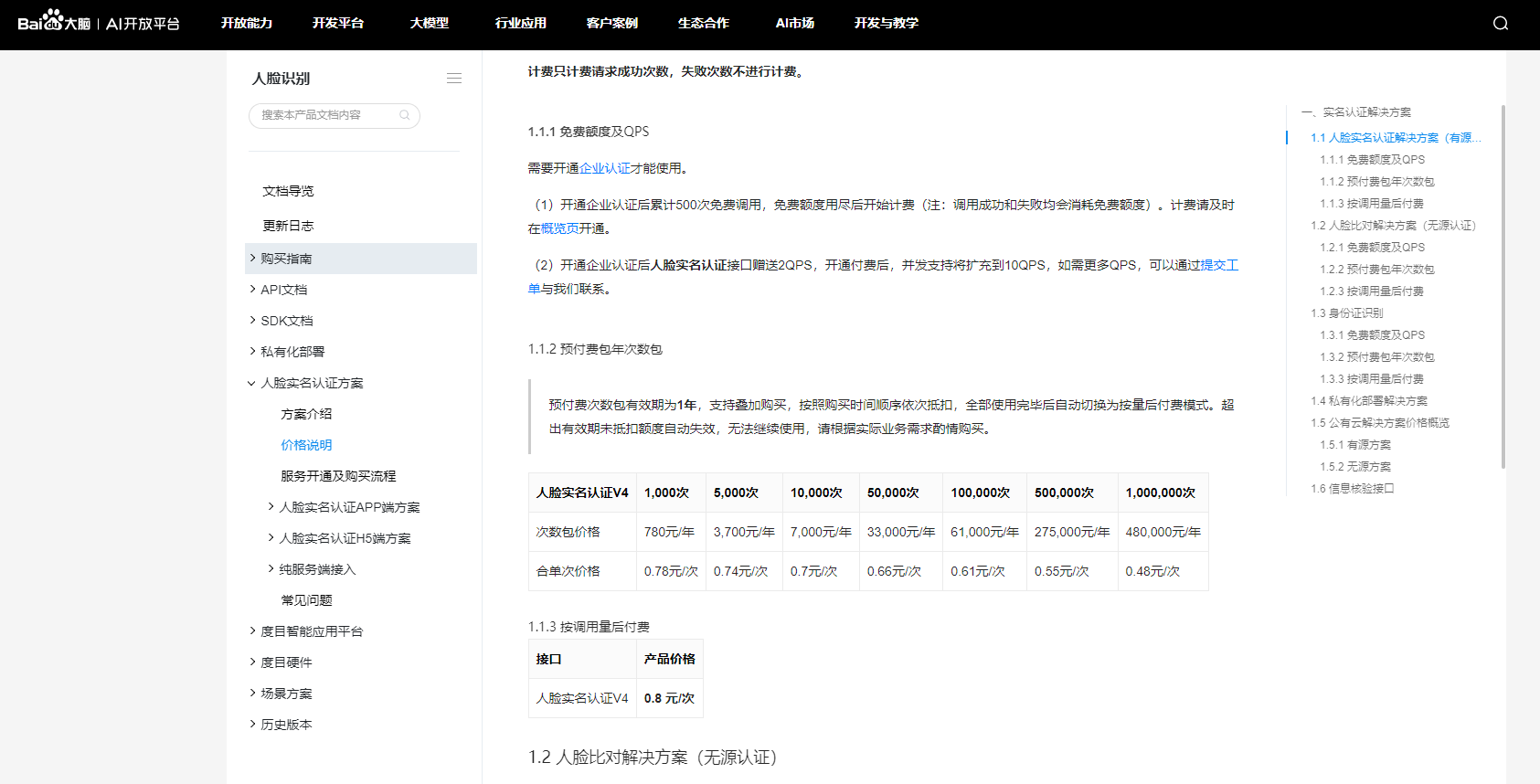


header处填入application/json access\_token处填入上面获得的token，body处填入身份证号和对应的姓名，可以看到返回success，证明匹配成功



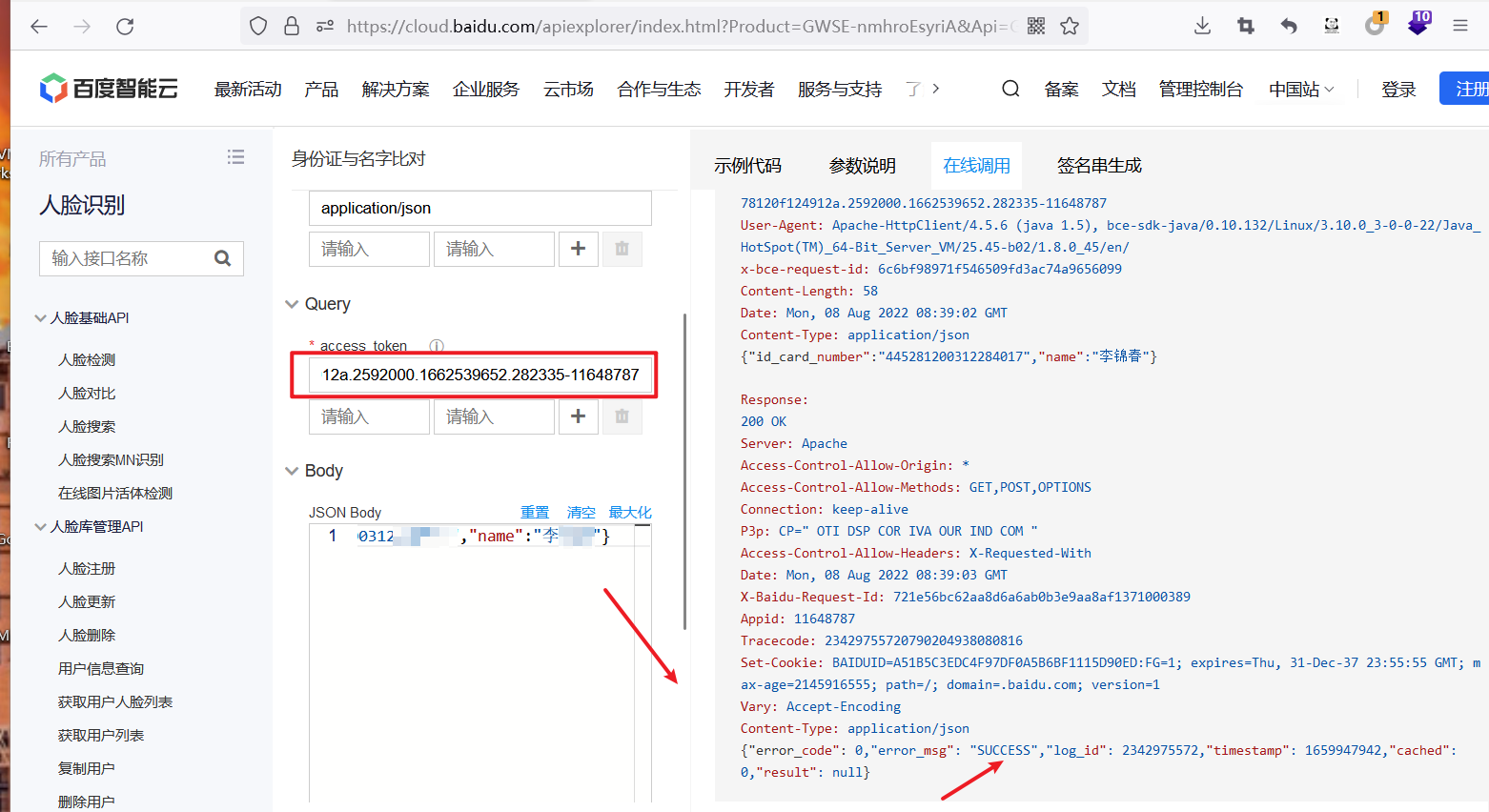
当输入错误的姓名时显示不匹配，并且查询官方文档得知此api接口是付费接口，成功实现接管

<https://ai.baidu.com/ai-doc/FACE/ek8dz0tl6>



同样的 此接口也可调用，这里进行测试调用了自己的

<https://cloud.baidu.com/apiexplorer/index.html?Product=GWSE-nmhroEsyriA&Api=GWAI-ropk3axeb3W>



修复方案

隐藏敏感信息，并将key全部更换，避免存在已经泄露的潜在危害