多因素平台开发者操作手册

目录

[1. 开发者注册登录 1](#_Toc16269)

[1.1. 开发者注册 1](#_Toc19988)

[1.2. 开发者登录 2](#_Toc11535)

[1.3. 忘记密码 3](#_Toc8409)

[1.4. 登录失败 4](#_Toc16887)

[2. 首页模块 6](#_Toc7449)

[2.1. 查看应用 6](#_Toc29810)

[2.2. 查看账户 7](#_Toc1947)

[2.3. 查看日志 8](#_Toc18480)

[3. 应用模块 10](#_Toc1845)

[3.1. 添加web应用 10](#_Toc15114)

[3.2. 添加移动端应用 11](#_Toc13127)

[3.3. 查看移动应用详情 13](#_Toc7183)

[3.4. 添加Facets 13](#_Toc1837)

[3.4.1. web端添加Facets 13](#_Toc18336)

[3.4.2. 移动端获取facetsid 15](#_Toc27219)

[3.5. 查看web应用 15](#_Toc22979)

[3.6. 检索应用 16](#_Toc14794)

[3.6.1. 通过应用名称检索应用 16](#_Toc12256)

[3.6.2. 通过时间检索应用 17](#_Toc26506)

[3.6.3. 通过应用类型检索应用 19](#_Toc7548)

[3.7. 应用接入说明 21](#_Toc9415)

[3.8. 查看应用秘钥 22](#_Toc5039)

[3.9. 添加账户 23](#_Toc30732)

[3.10. 查看应用账户 27](#_Toc14696)

[3.11. 查看应用日志 29](#_Toc25838)

[4. 多因素认证 30](#_Toc8895)

[4.1. 动态令牌认证 30](#_Toc14998)

[4.2. 微信认证 30](#_Toc2017)

[4.3. 硬件令牌认证 30](#_Toc1917)

[5. 日志模块 31](#_Toc8288)

[5.1. 查看日志 31](#_Toc25603)

[5.2. 检索日志 31](#_Toc11749)

[6. 设置模块 33](#_Toc4814)

[6.1. 动态令牌设置 33](#_Toc22937)

[6.1.1. web端动态令牌设置 33](#_Toc11539)

[6.1.2. 移动端动态令牌获取 35](#_Toc25030)

[6.2. 硬件令牌设置 36](#_Toc567)

[7. 账户模块 39](#_Toc16759)

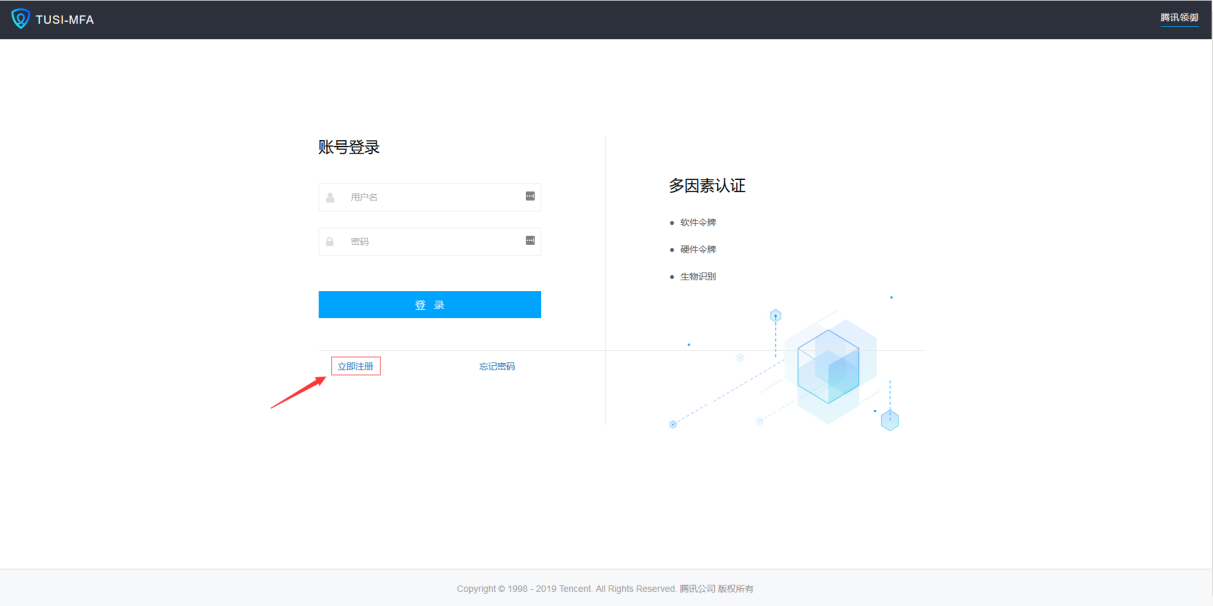
[7.1. 修改密码 39](#_Toc19820)

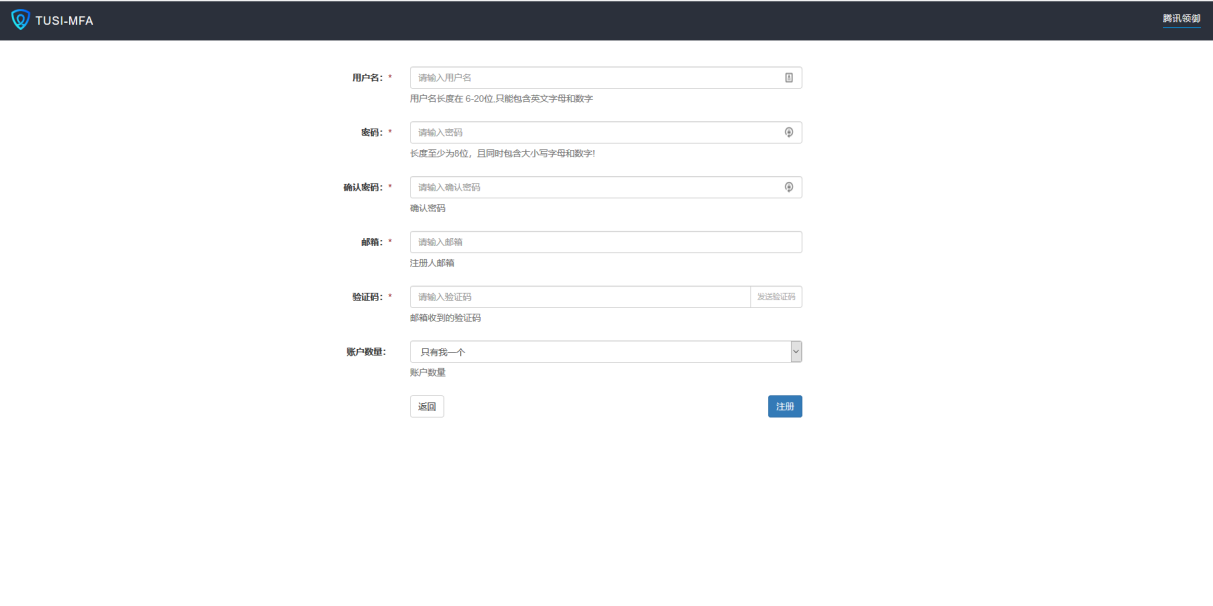
[7.2. 退出登录 40](#_Toc2594)

# 

# 开发者注册登录

## 开发者注册

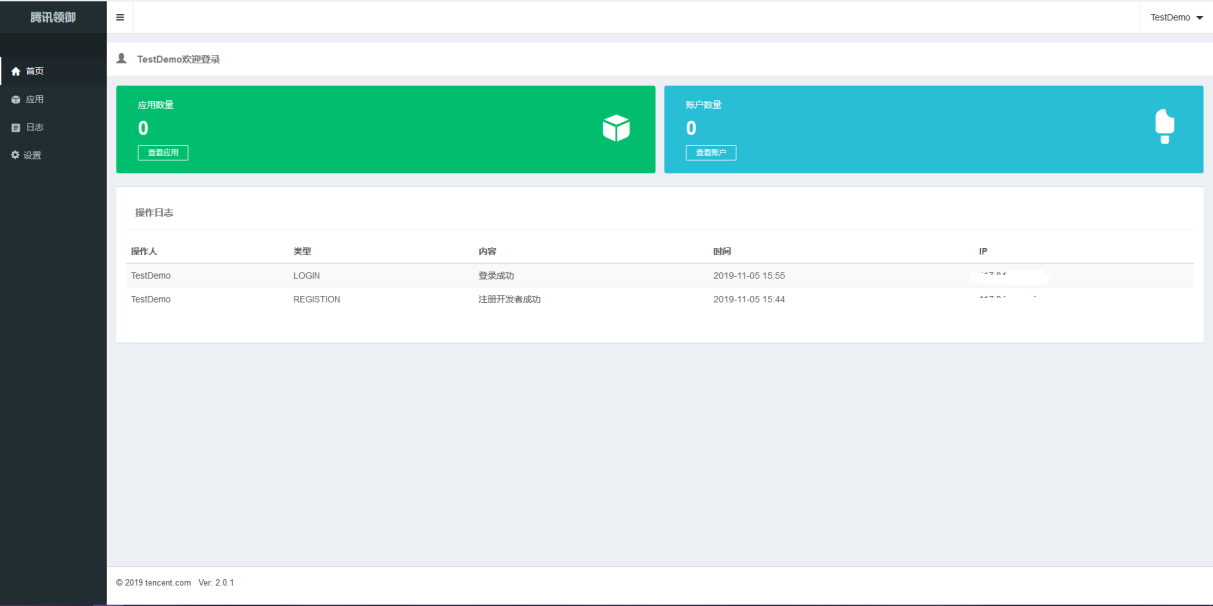
进入官网https://www.bebeman.com/MFA，点击左下角标注的“立即注册”进行注册。

点击后进入开发者注册界面，分别填入用户名（注意用户名格式用户名长度在 6-20位,只能包含英文字母和数字）、密码（注意密码格式：长度至少为8位，且同时包含大小写字母和数字）、确认密码、注册邮箱、验证码。在账户数量中选择使用该注册账户的开发者数量。

注册成功界面：点击登录进入账号登录界面进行对该账户的登录操作。

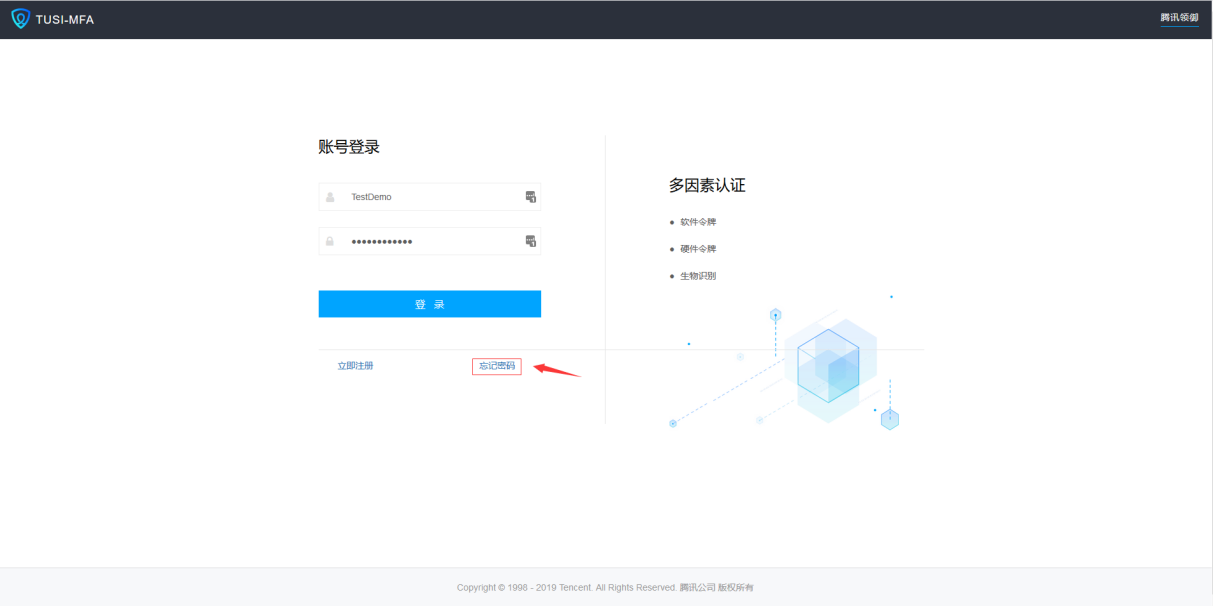
## 开发者登录

注册成功后进入账号登录界面，登录成功进入主界面：

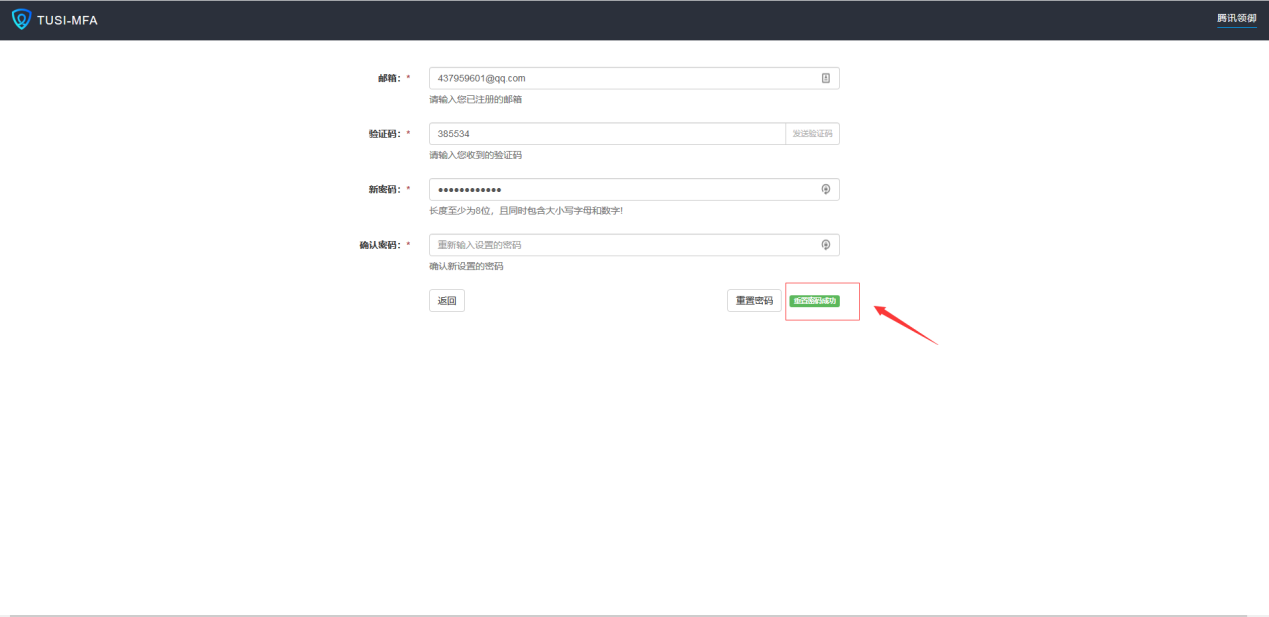


## 忘记密码

如果忘记设置的密码，点击账号登录界面的右下方的忘记密码进行重置密码的操作。

在重置密码界面输入该账号的注册邮箱，输入正确的验证码。然后输入新密码以及确认密码，密码的格式依然要符合要求的密码格式。重置成功后会有提示（“密码重置成功”），密码重置成功后返回到登录界面进行登录验证。





## 登录失败

该系统提供了5次登录机会，5次登录都失败后会锁定账户，锁定时间为30分钟。每次登录失败都会提示还剩余多少次登录机会，用以提醒开发者。如下图提示“认证失败，您还有4次登录次数”。在5次可登录机会内可以使用忘记密码功能重置密码。

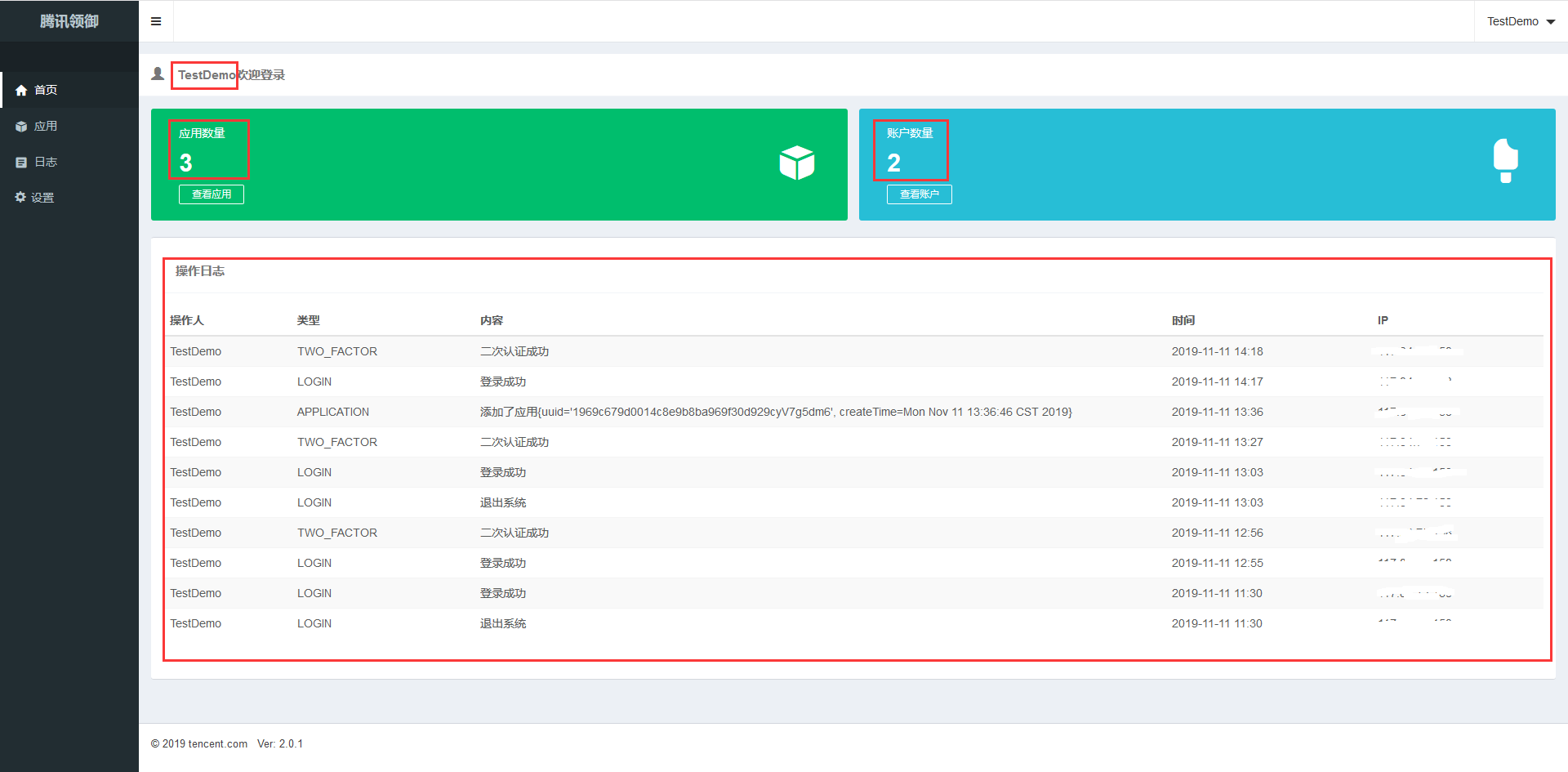


若5登录全部失败，则会提示“您的账户已被锁定，请30分钟后重试”。如下图所示



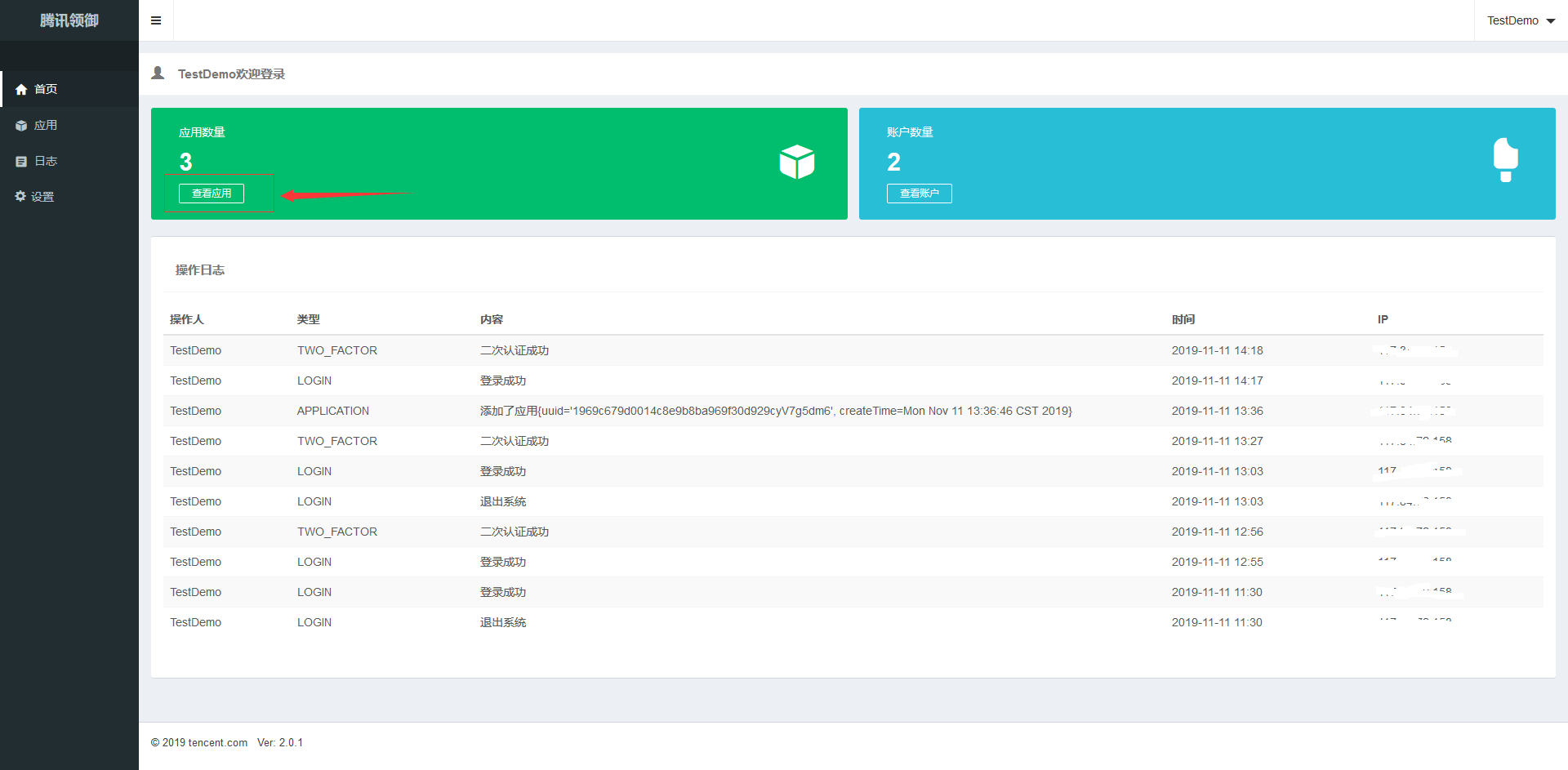
# 首页模块

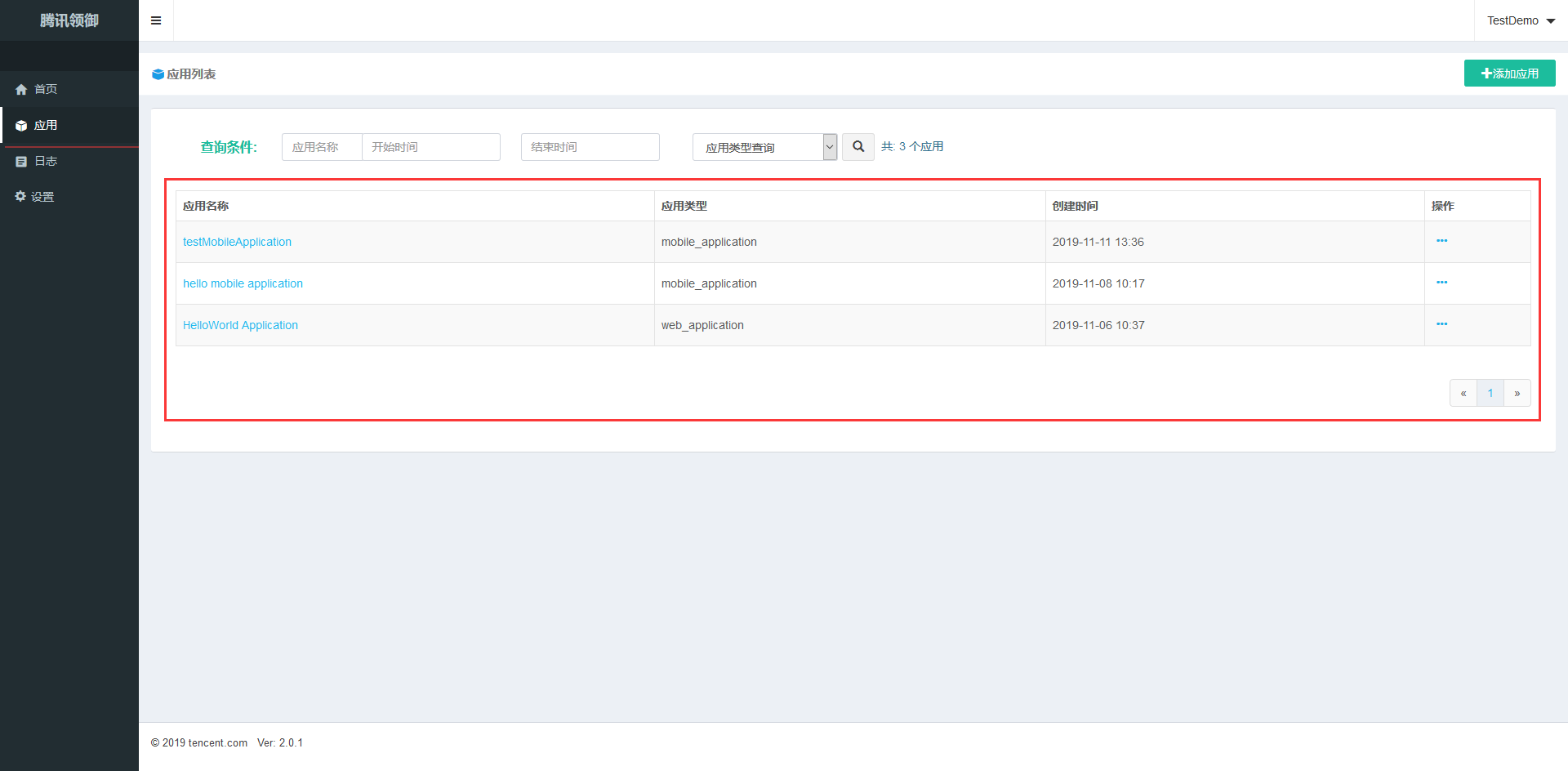
成功登录后或者手动点首页时会进入到首页界面，该界面展示了登录者名称、应用数量、账户数量、最新的日志信息。



## 查看应用

在首页界面中的应用数量下，点击查看应用，会进入到应用列表界面，展示所有已经添加的应用，效果如下：

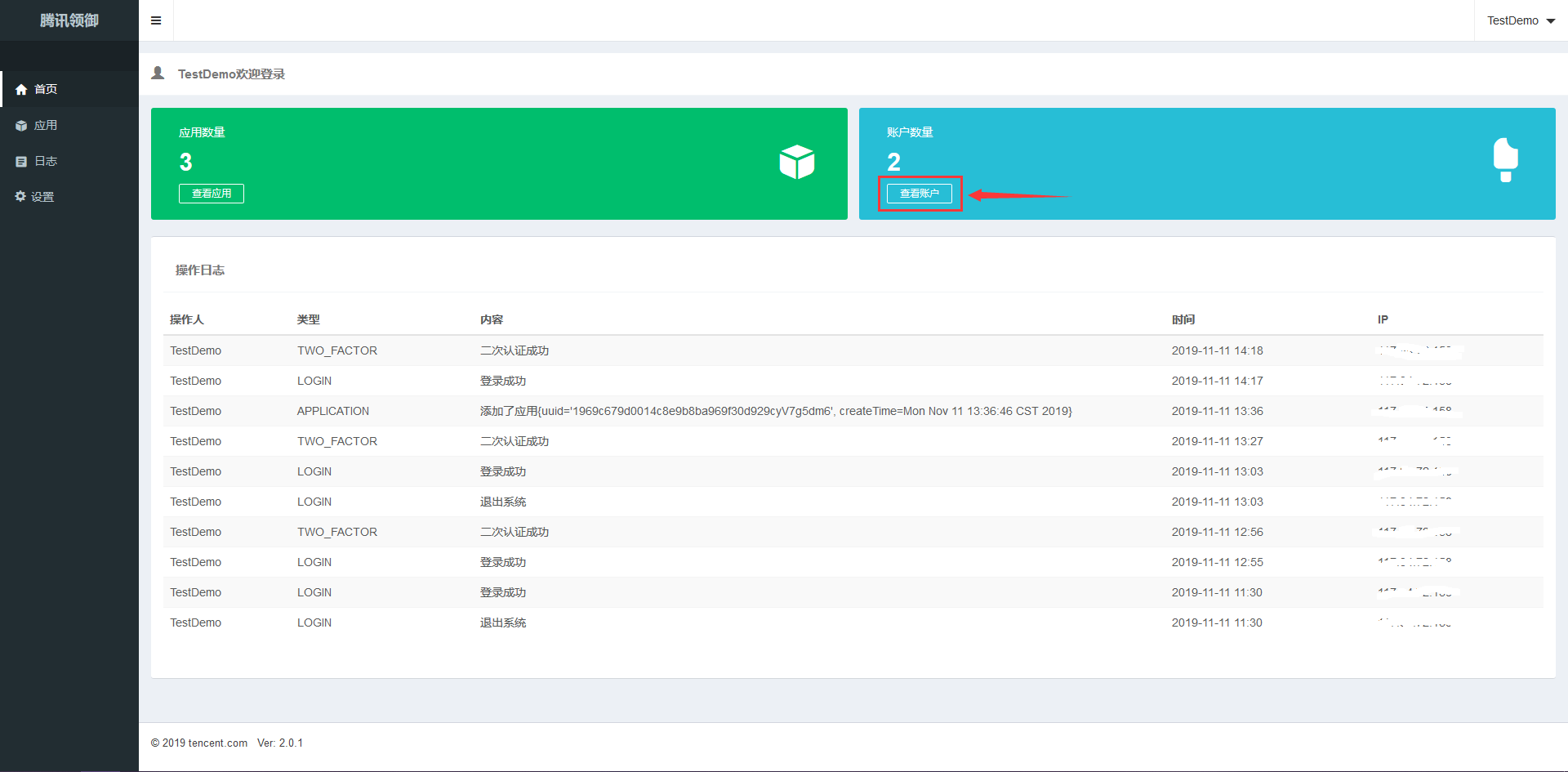


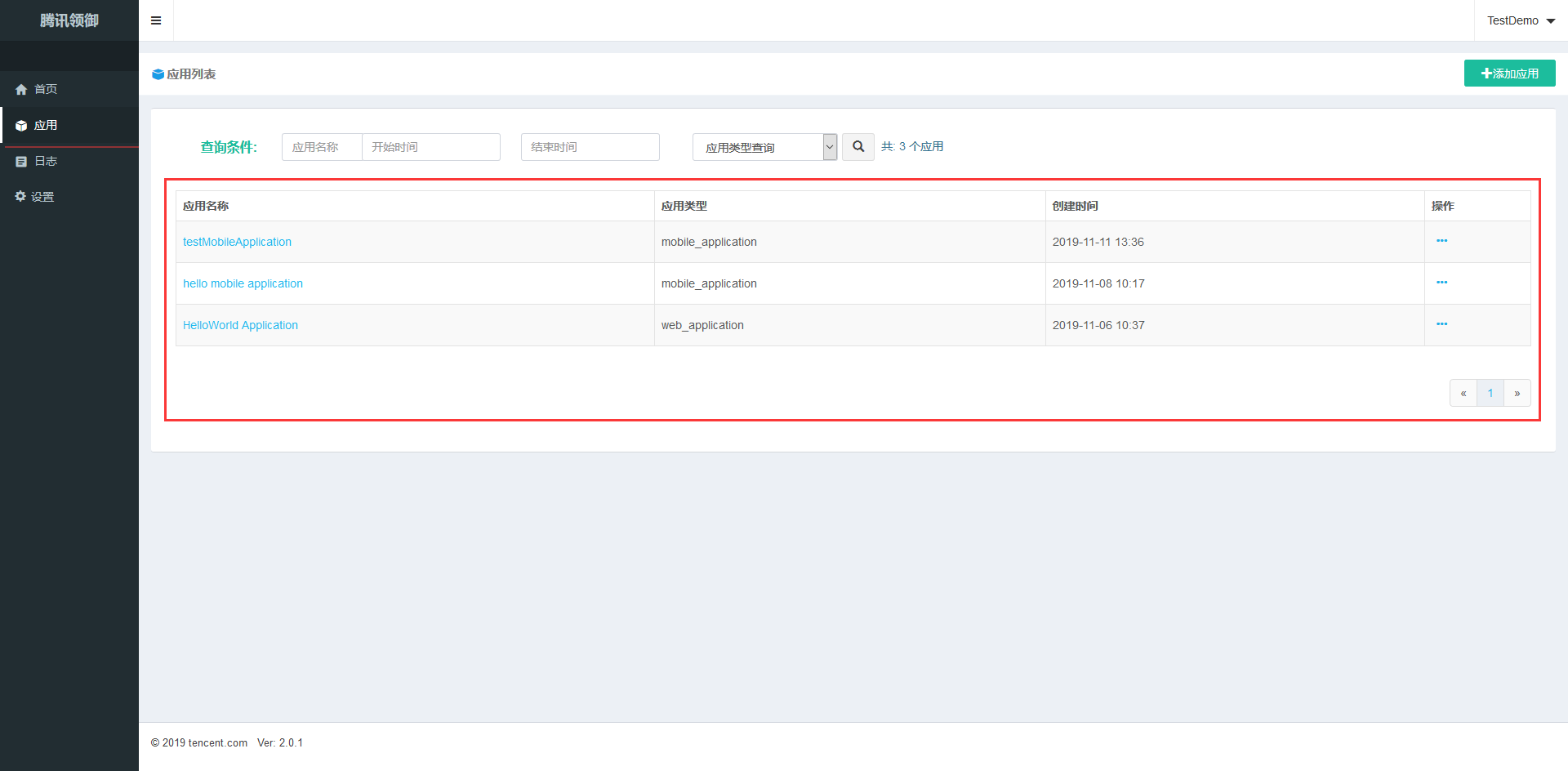


查看应用的具体操作请参照3.3查看移动应用详情和3.5查看web应用、检索应用章节内容。

## 查看账户

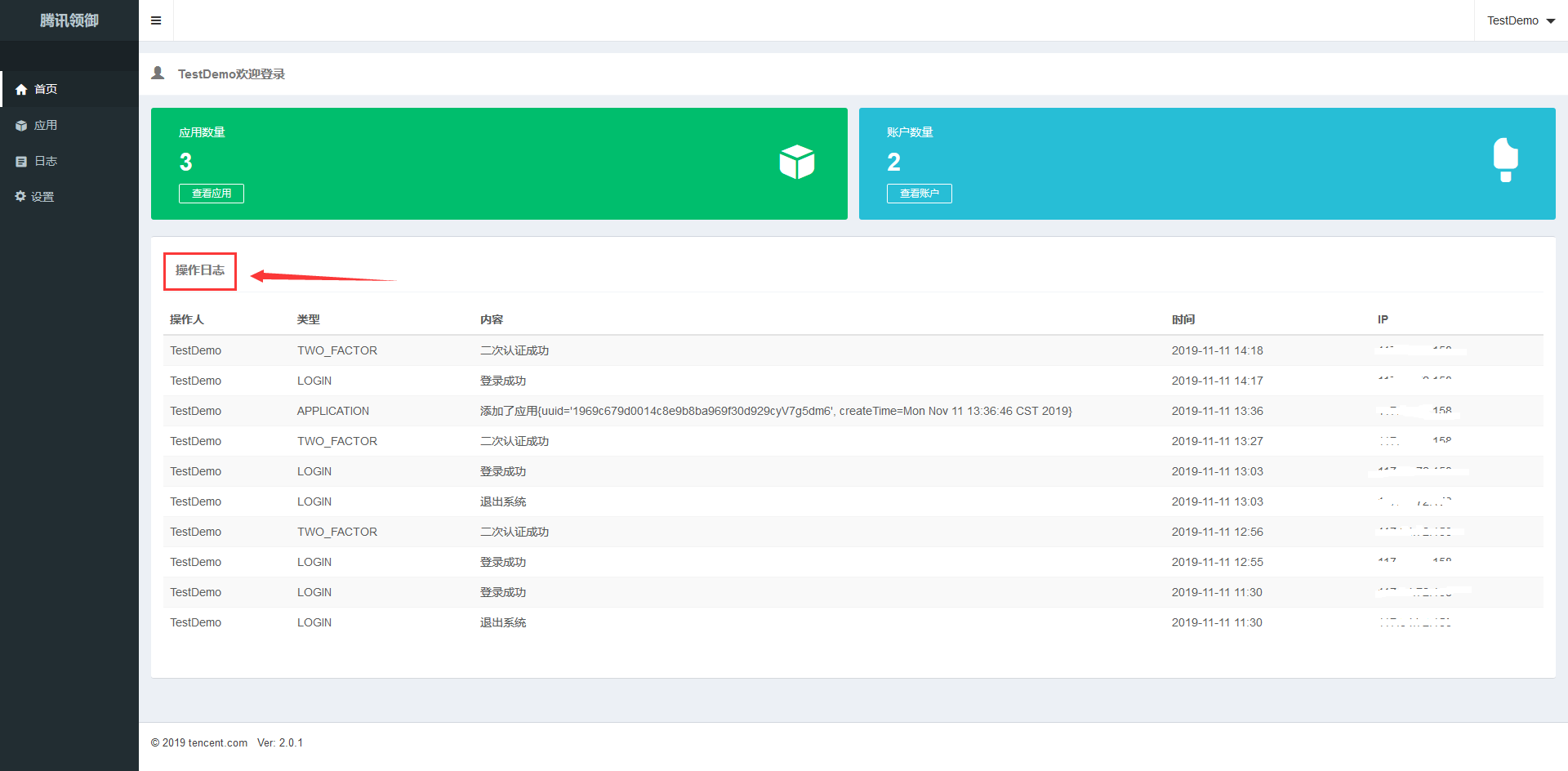
首页中，在账户数量下，点击查看账户，此时会跳转到应用列表界面，查看账户的具体操作请参考3.9查看应用账户章节内容。

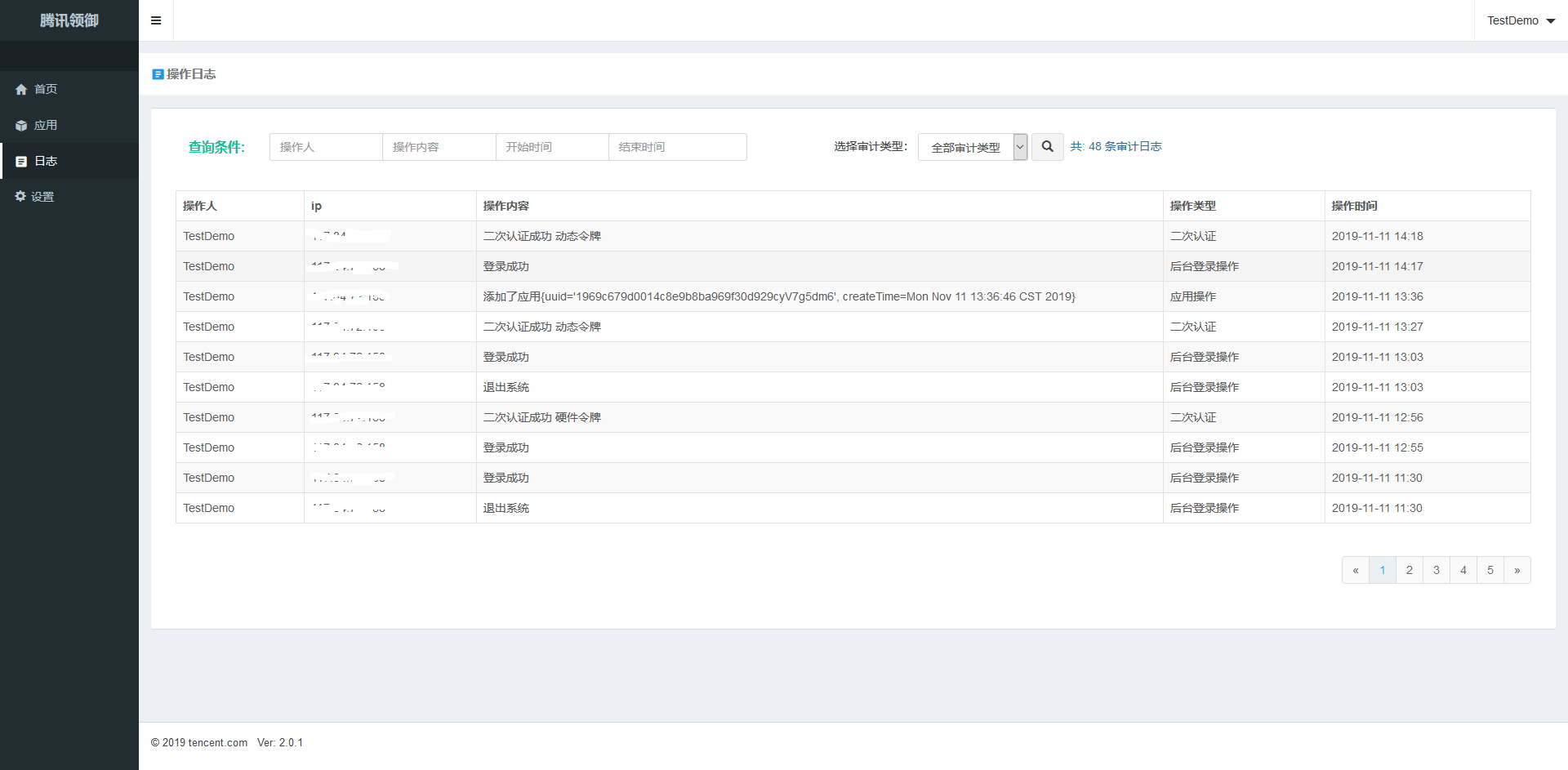




## 查看日志

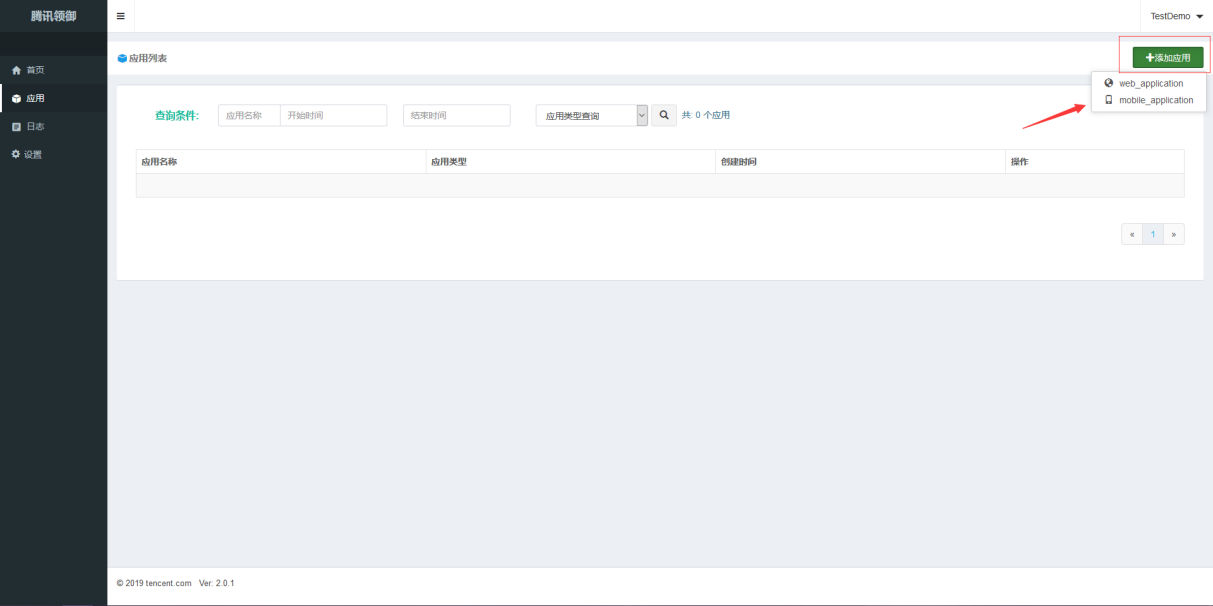
在首页中展示的日志信息是每10秒钟更新信息，以保证首页中展示的日志是最新的信息，但是首页的日志信息只展示最新的10条信息，如果需要查看其它日志信息，就要点击“操作日志”，进入到日志列表界面，查看与检索日志的操作请参照第5章的章节内容。效果如下：

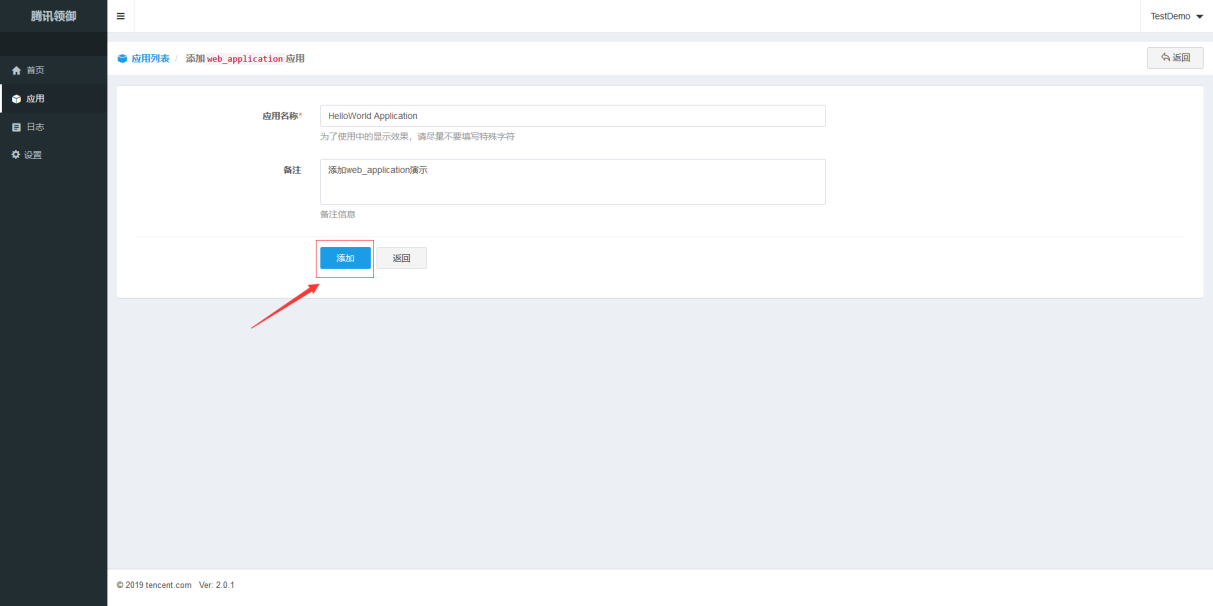


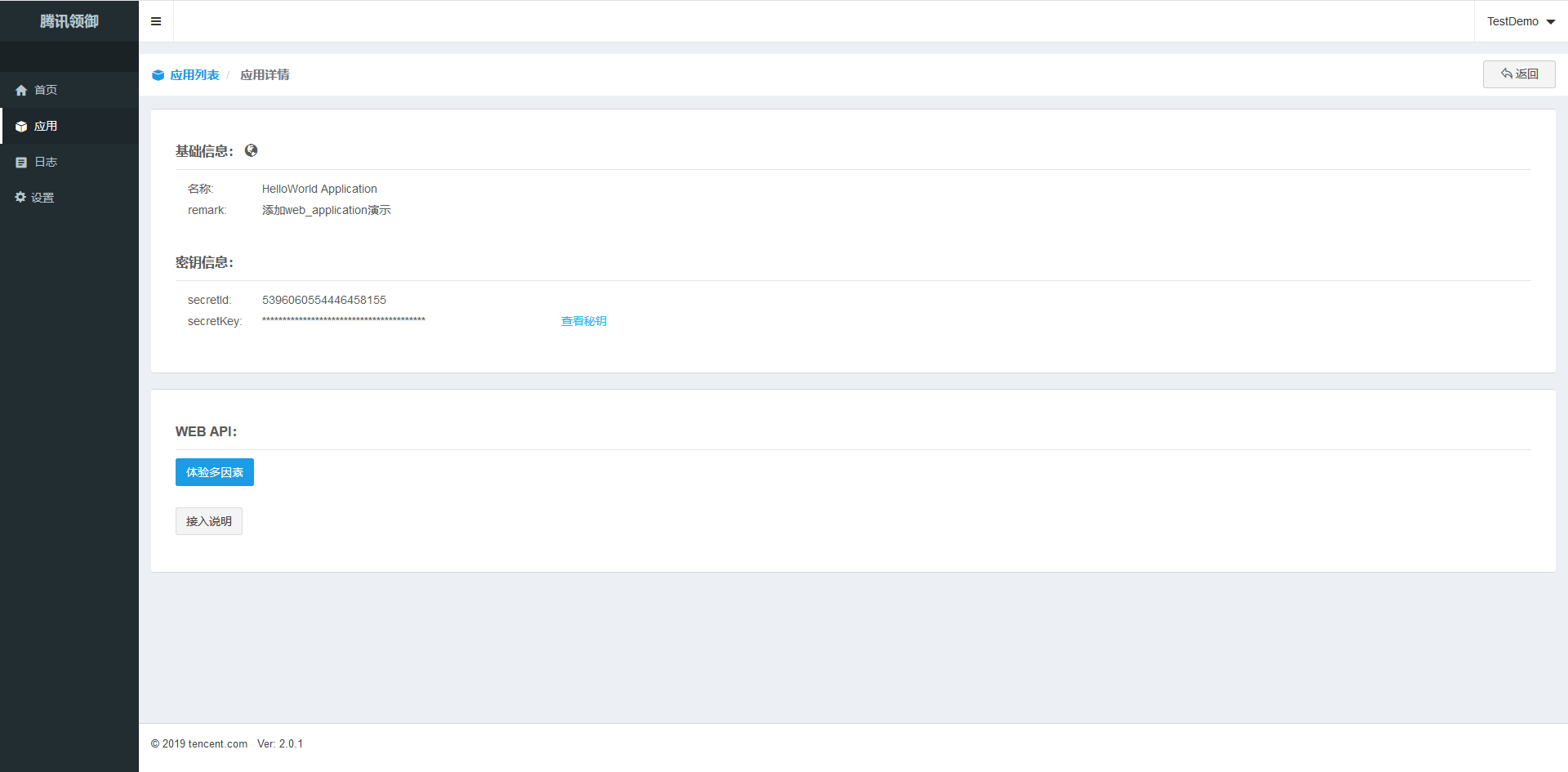


# 应用模块

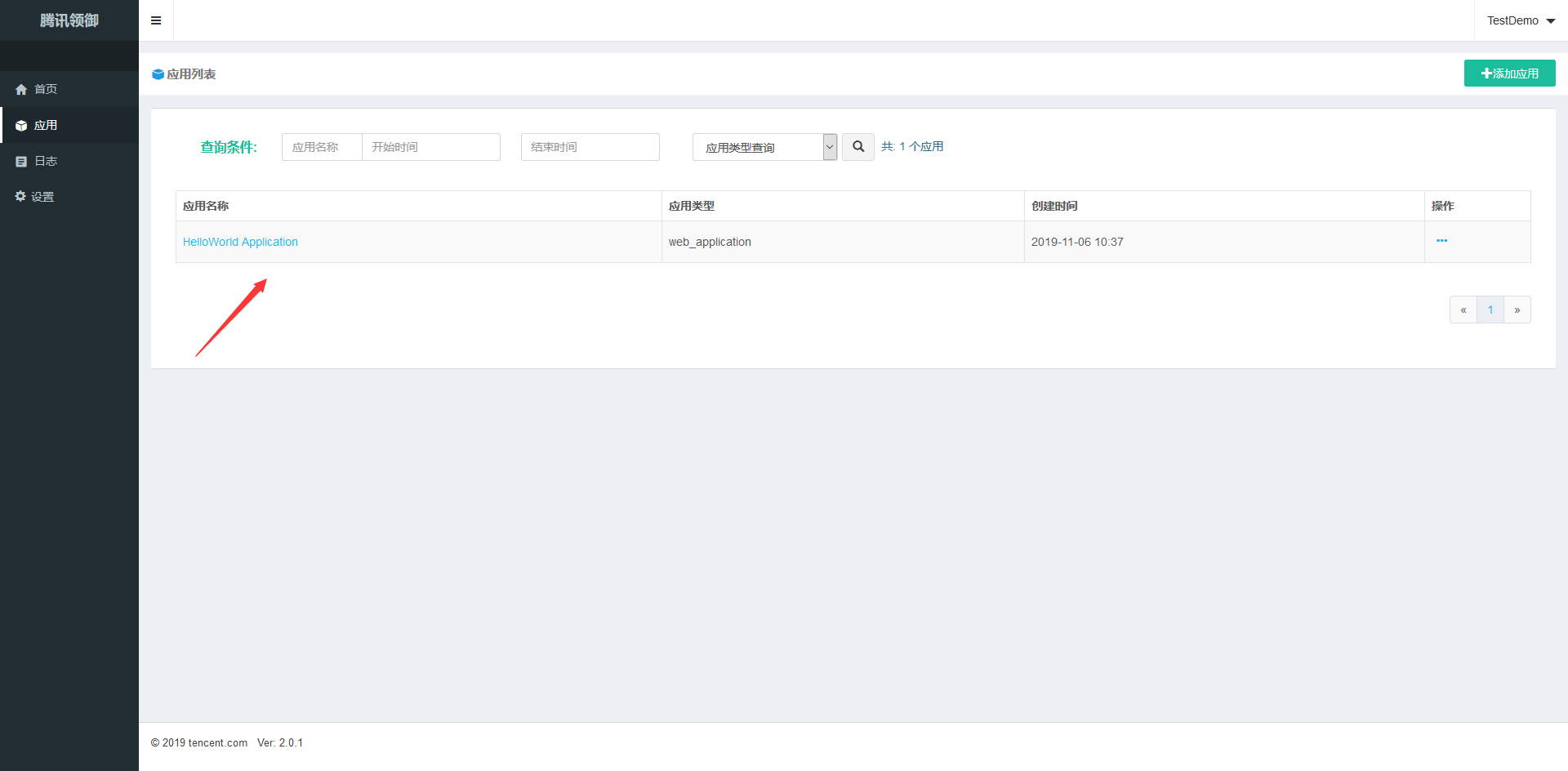
## 添加web应用

添加web应用是添加开发者开发的web应用。进入应用界面并点击右上角的添加应用，选择web\_application进入到添加web应用的界面。添加完成后会进入到该应用的详情界面，展示该应用的名称、备注、秘钥等信息。





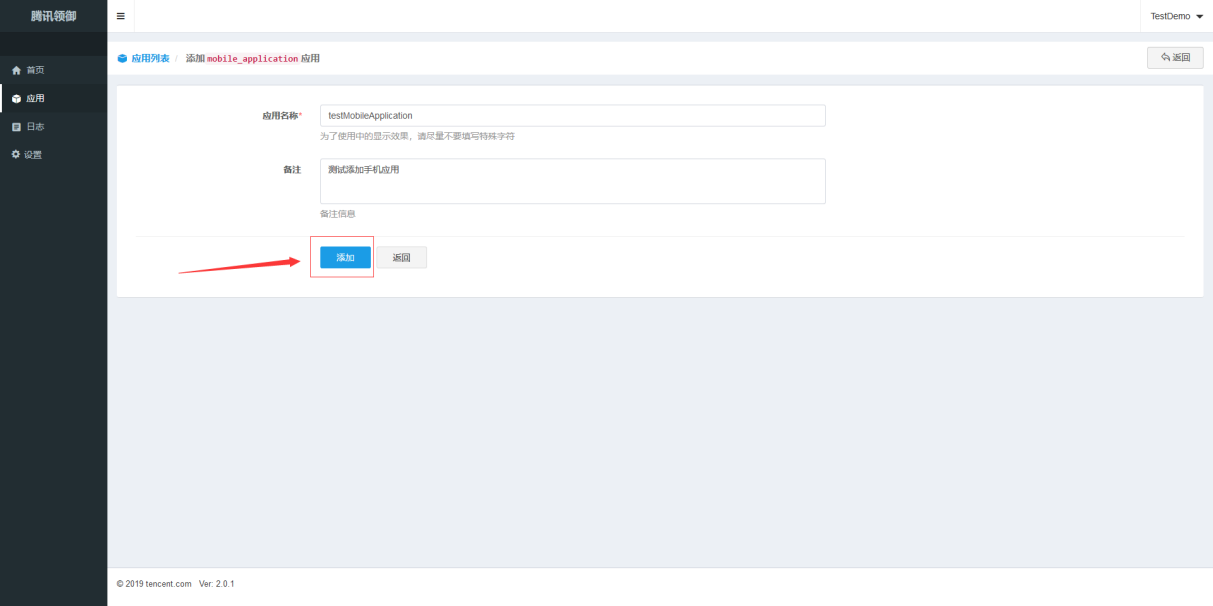
再返回到应用列表界面，查看已经添加的应用，如下图所示。

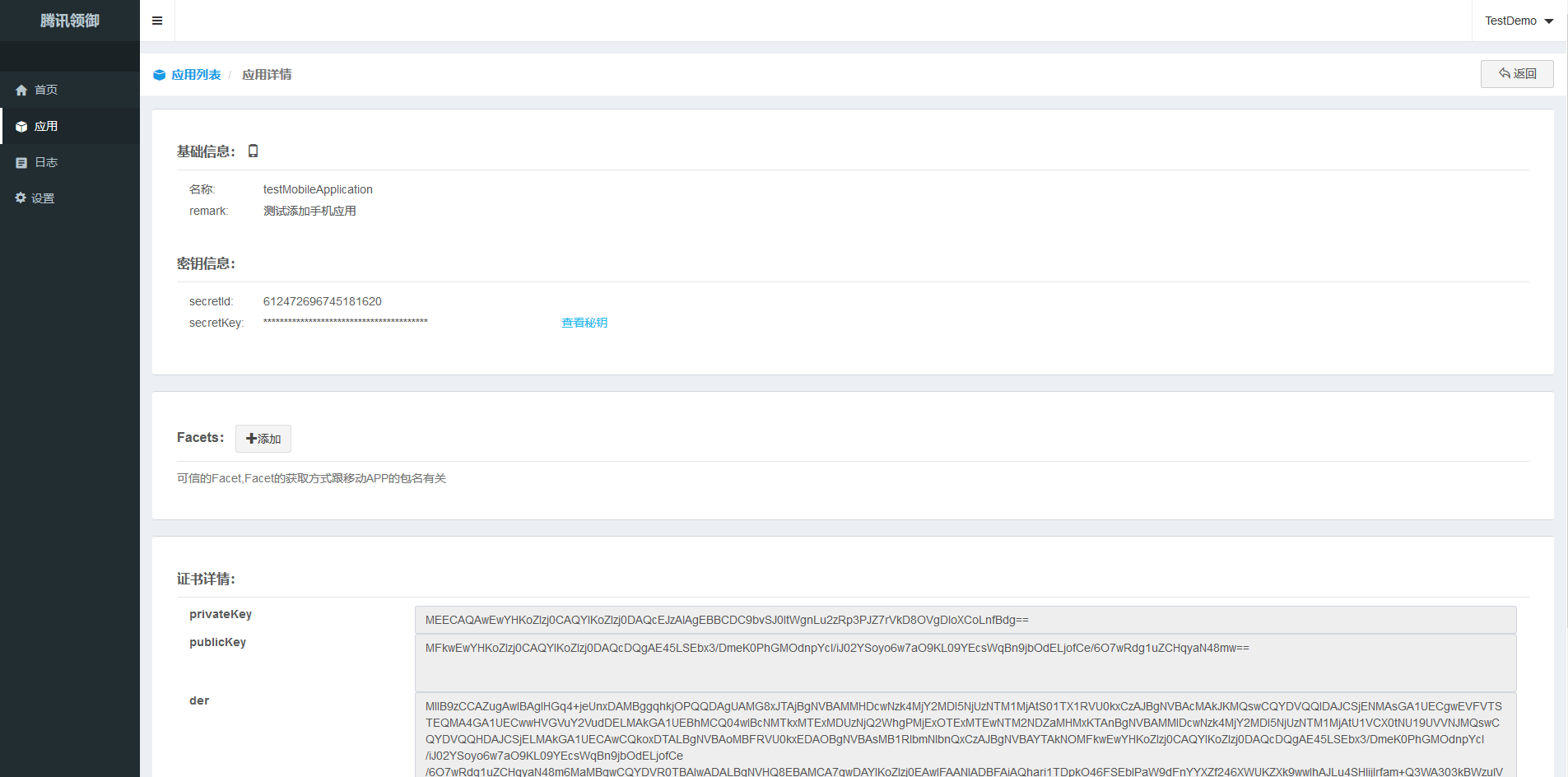


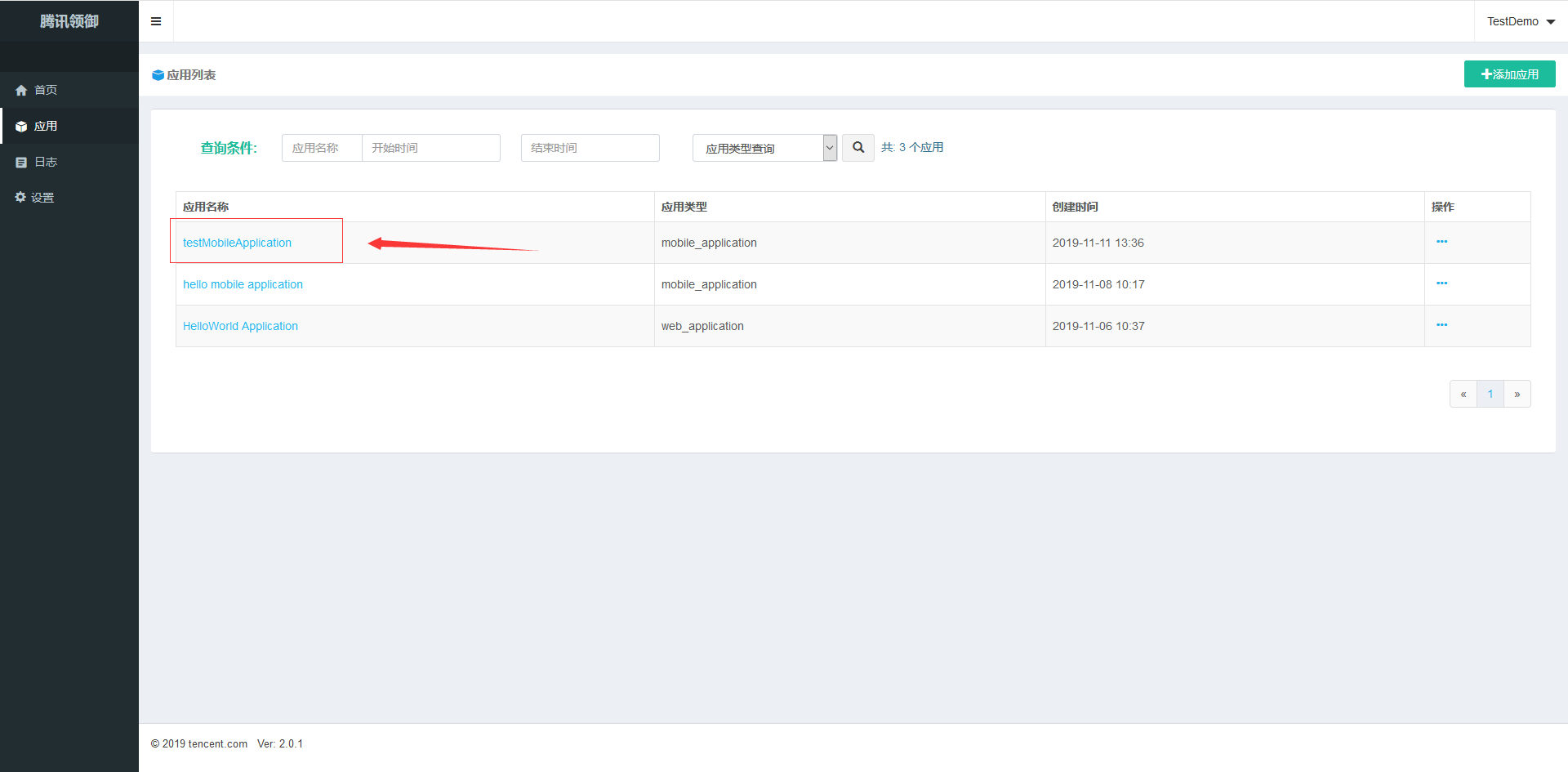
## 添加移动端应用

该功能主要为了开发者添加开发的移动应用而服务的，添加移动端应用与添加web应用步骤大致一样，但细节不同。

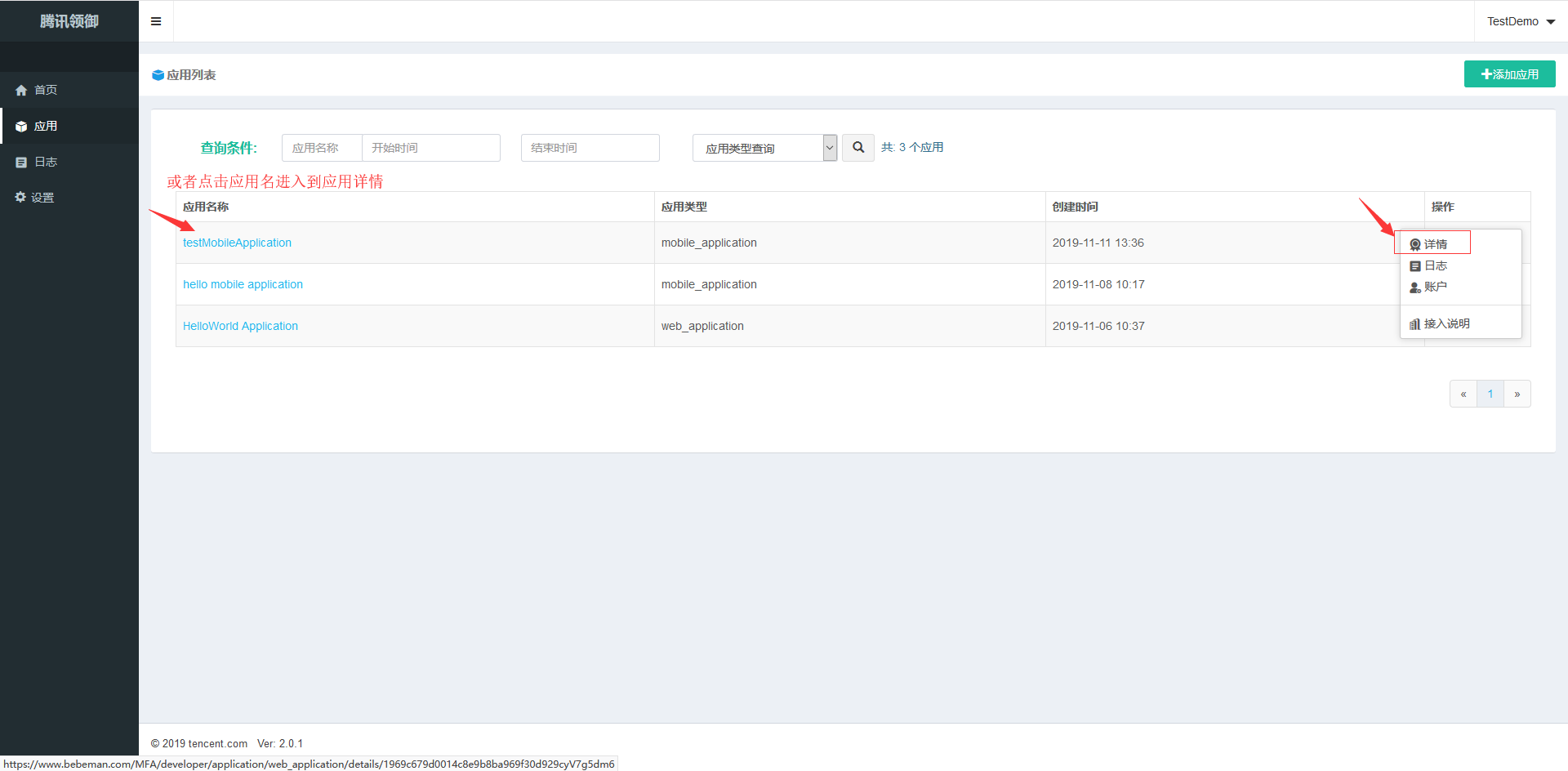
同样的进入到应用列表界面，点击添加应用，选择mobile\_application，进入到添加移动应用的界面，输入应用名称与备注信息，其中应用名称为必填项，备注信息为选填项，点击添加按钮添加移动端应用。添加完成后会跳转到应用详情界面，展示添加的该应用的具体信息。点击菜单栏的应用，进入应用列表界面，查看刚刚添加的移动端应用。

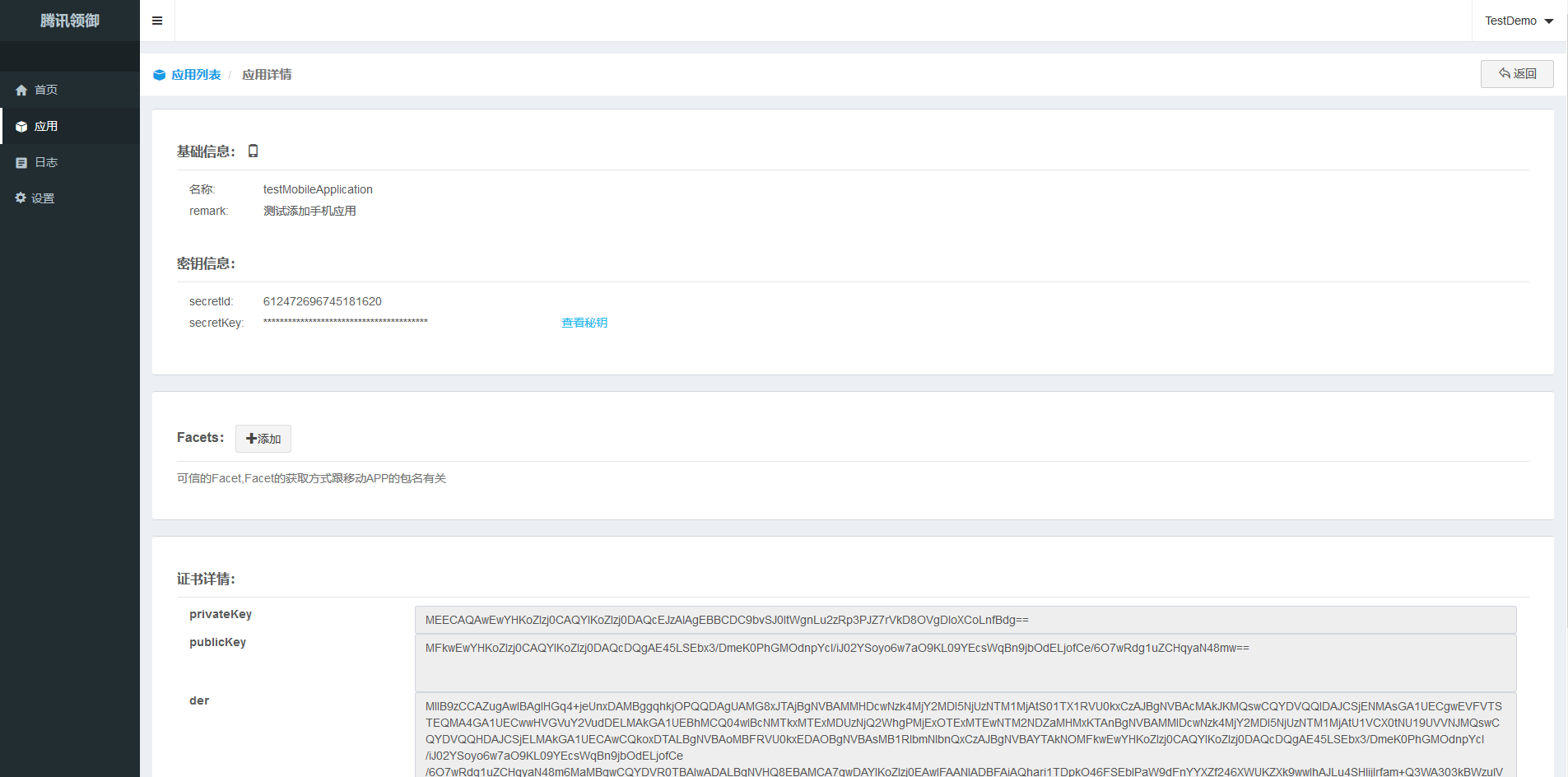






## 查看移动应用详情

移动应用添加完成后，查看该应用的详细信息，请点击应用名或者点击操作选项中的详情，点击后展示的是该移动应用的详情界面。

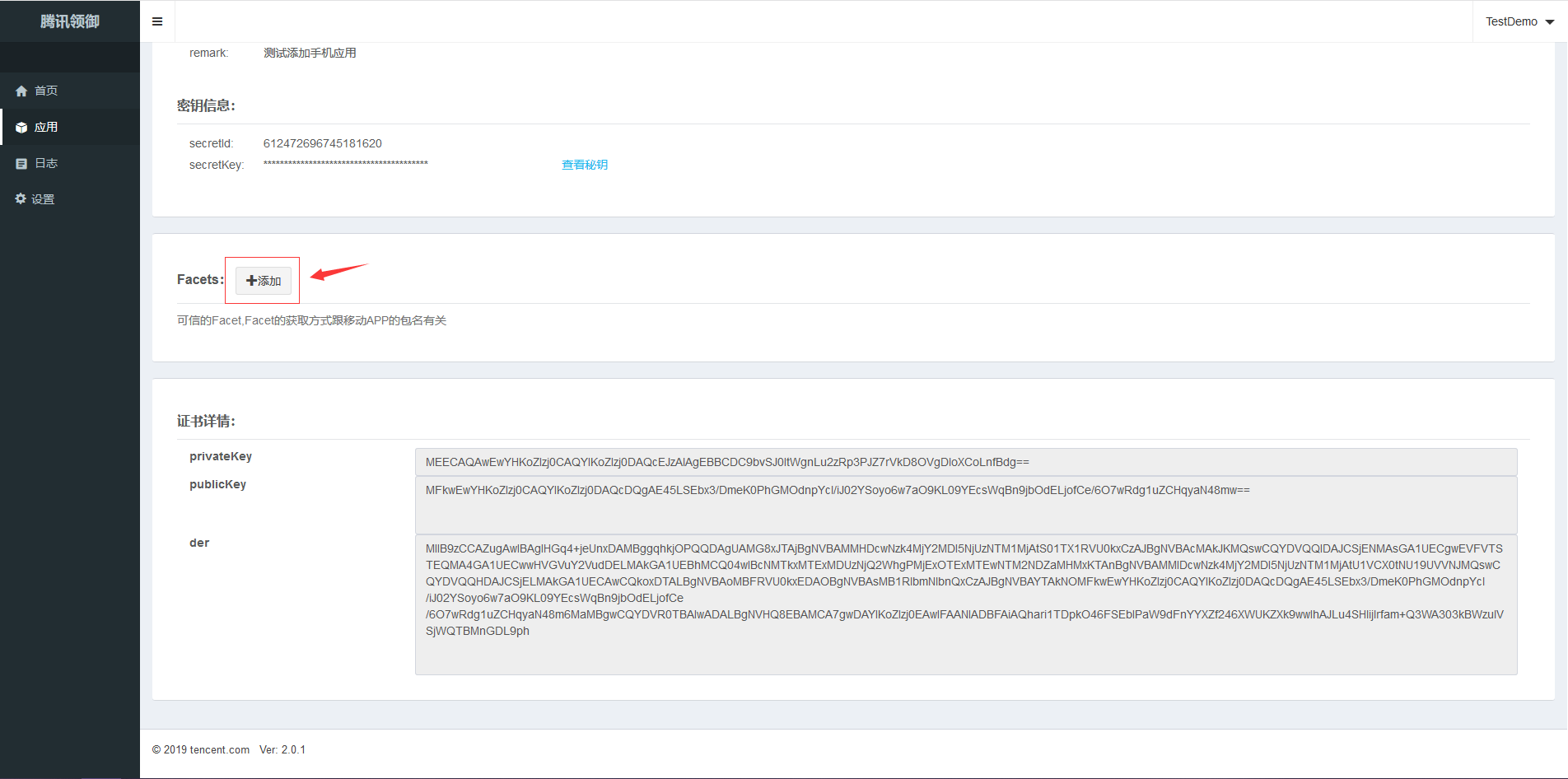
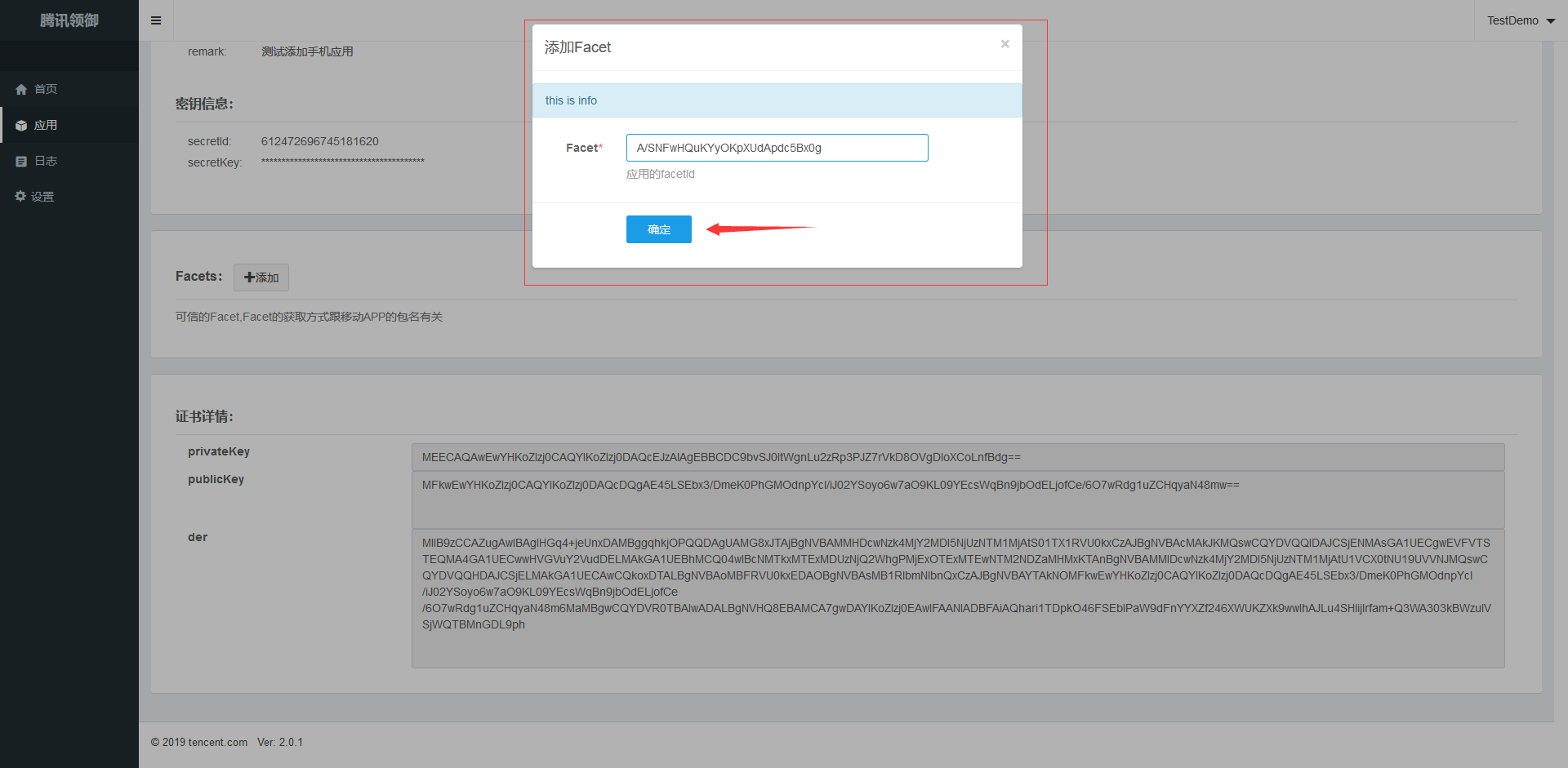
在该界面中，基本信息包括了应用名称和备注信息，秘钥信息中包括了秘钥ID跟秘钥，查看秘钥请参照3.7查看应用秘钥章节的相关内容。秘钥信息是移动应用用来接入到二次认证所使用的。Facets与移动端APP有关，请参照3.4添加Facets章节内容。证书详情包括了KMS发给我们的公钥、私钥、证书秘钥。

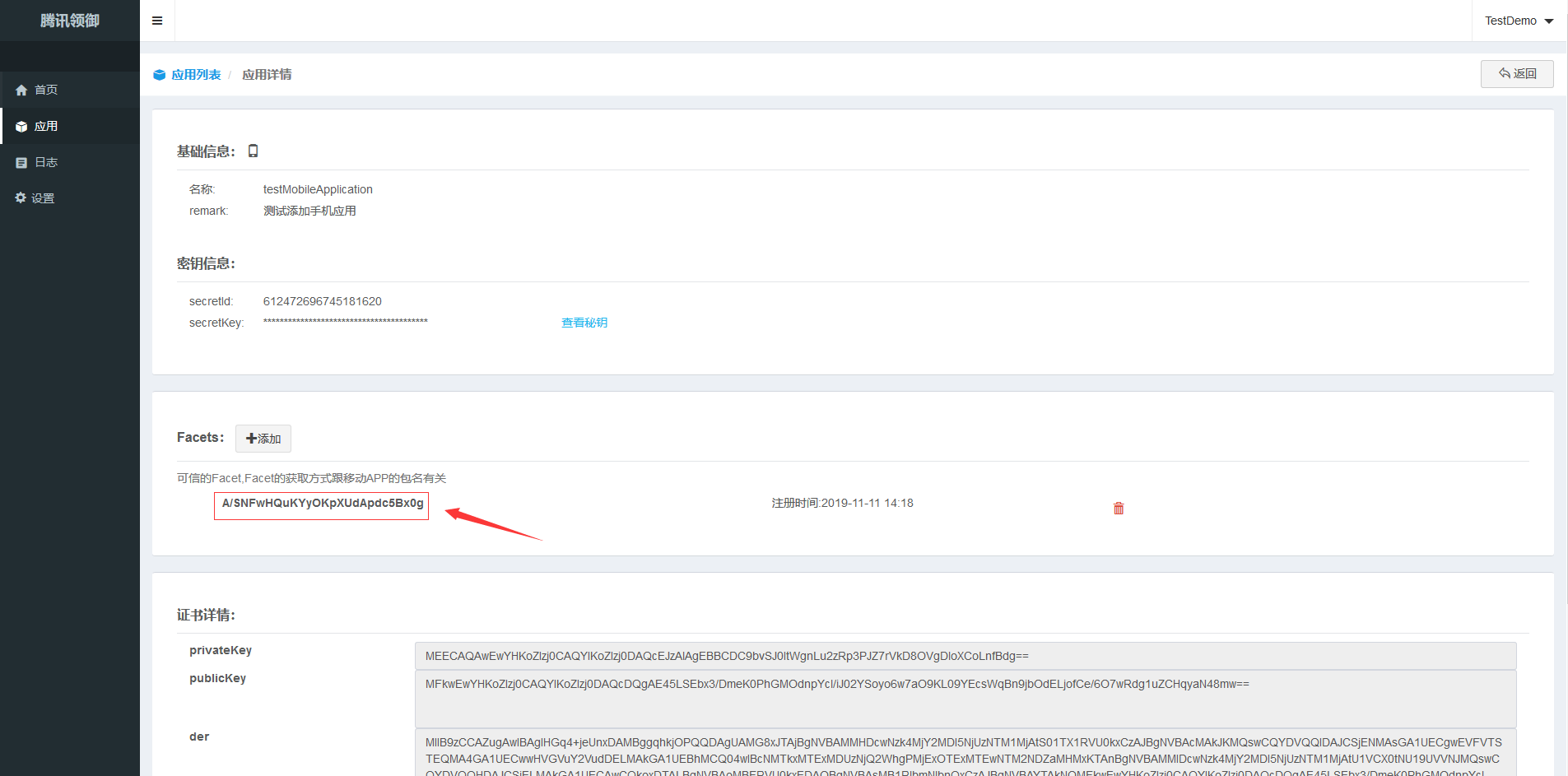
## 添加Facets

测试用到的APP仍然在开发中，测试界面不代表最终产品。该APP中会先对手机硬件条件进行检查，如果有指纹识别硬件，在注册和认证中会有指纹识别这一项，因测试手机无指纹识别硬件，在注册和认证中只有数字认证这一项，该数字是锁屏密码，因安全起见，移动端程序设计中该界面无法截屏，请谅解。

### web端添加Facets

首先在web端进入到移动应用详情界面，详细步骤请参考3.3 查看移动应用详情章节内容，点击“Facets”文本右边的“+添加”按钮，在facet文本输入框中输入移动端获取到的facetsid，此项为必填项，添加完成后会在详情界面看到添加成功的facetsid和注册时间。效果如下：





### 移动端获取facetsid

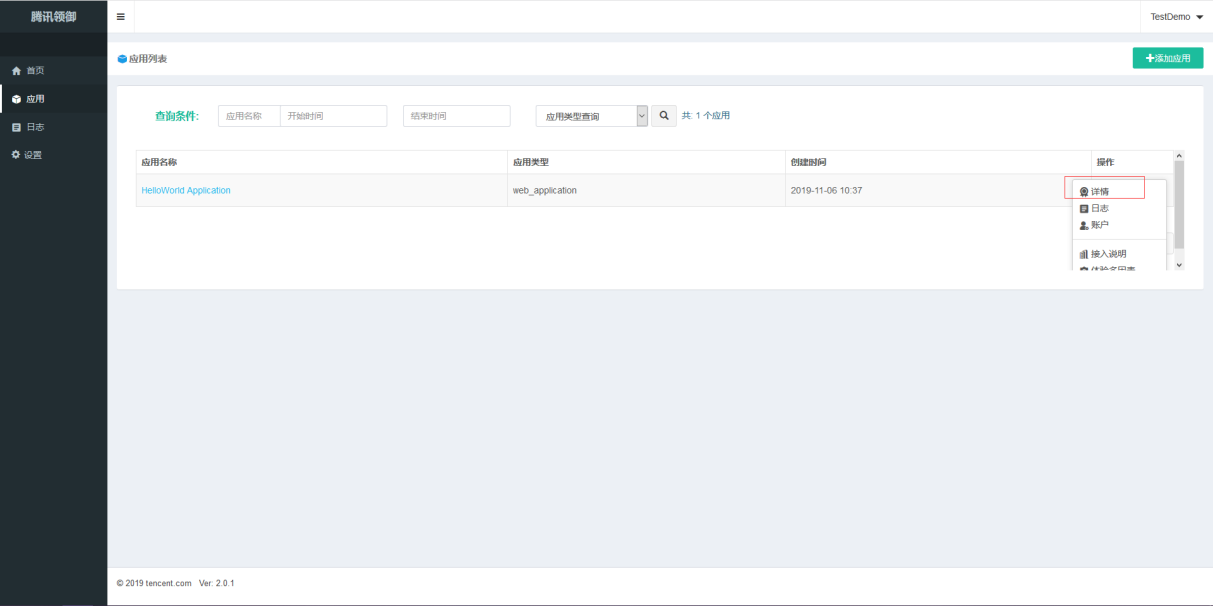
移动端应先输入用户名，再点击注册，进入注册界面后根据需求使用锁屏密码或者使用指纹密码。随后进入app点击“获取FACEID”，获取faceid，需要注意的是，一部移动设备只会产生一个faceid，卸载移动端APP后重新安装，上述结果不成立。接着点击认证，对该账户进行认证操作，同样的，锁屏密码输入行输入锁屏密码，指纹识别用注册时的指纹“输入”。

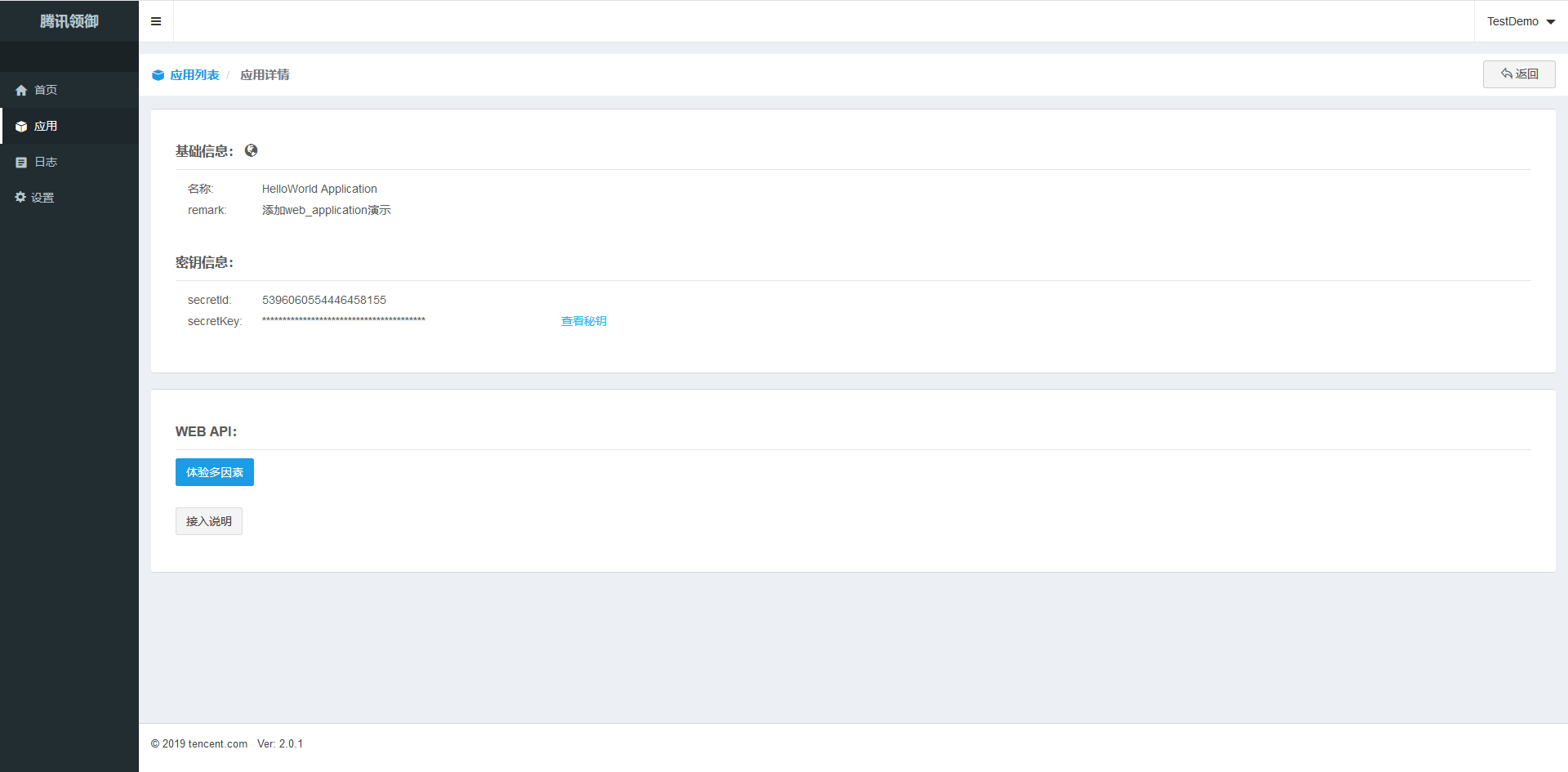


移动端通过认证后，web端添加的的mobile\_application下没有账户

## 查看web应用

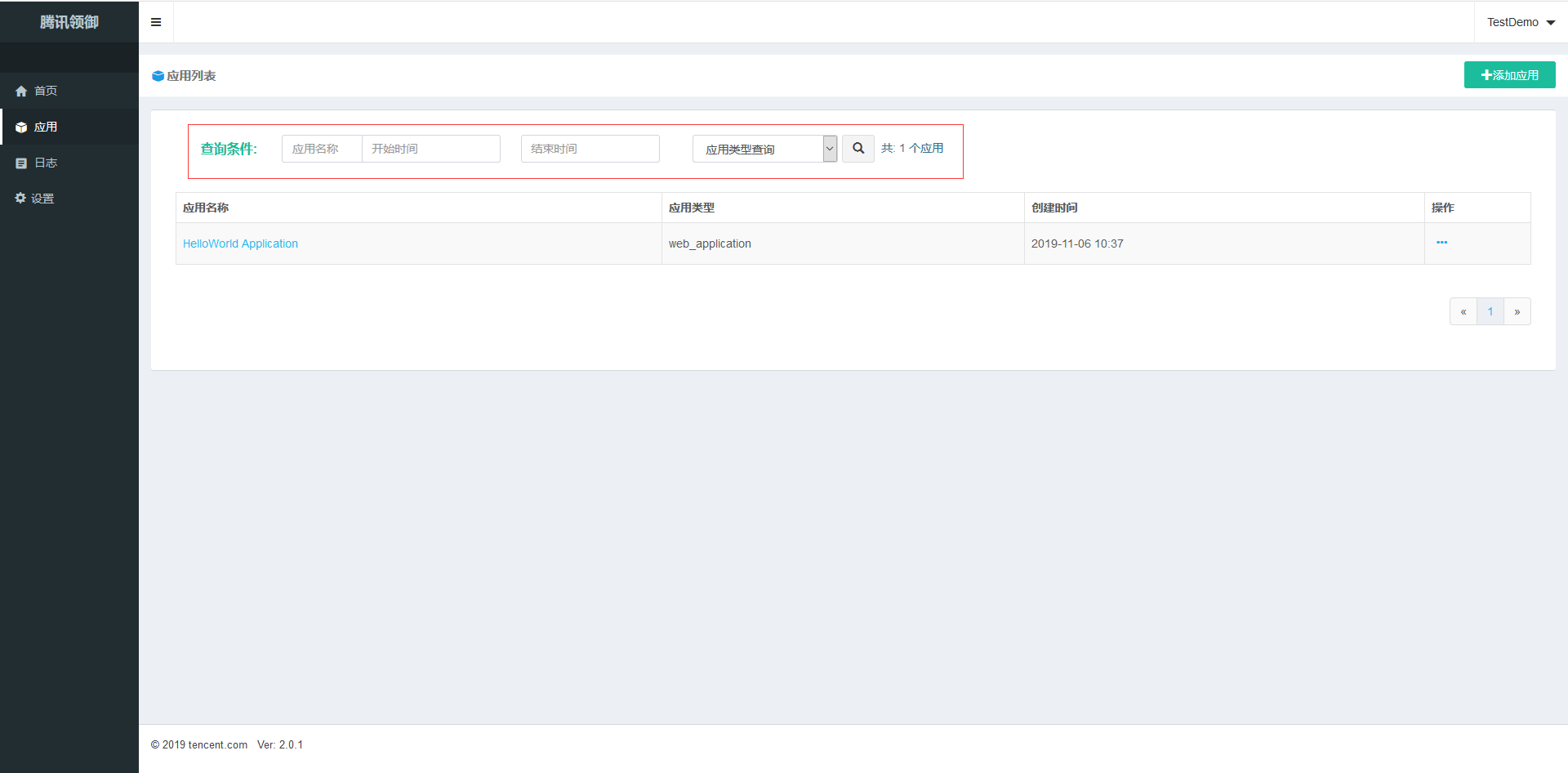
在应用列表界面，需要查看一个应用的详细信息，可以点击应用名或者点击该行应用最后一列的操作按钮，选择点击详情按钮查看该应用的详细信息。





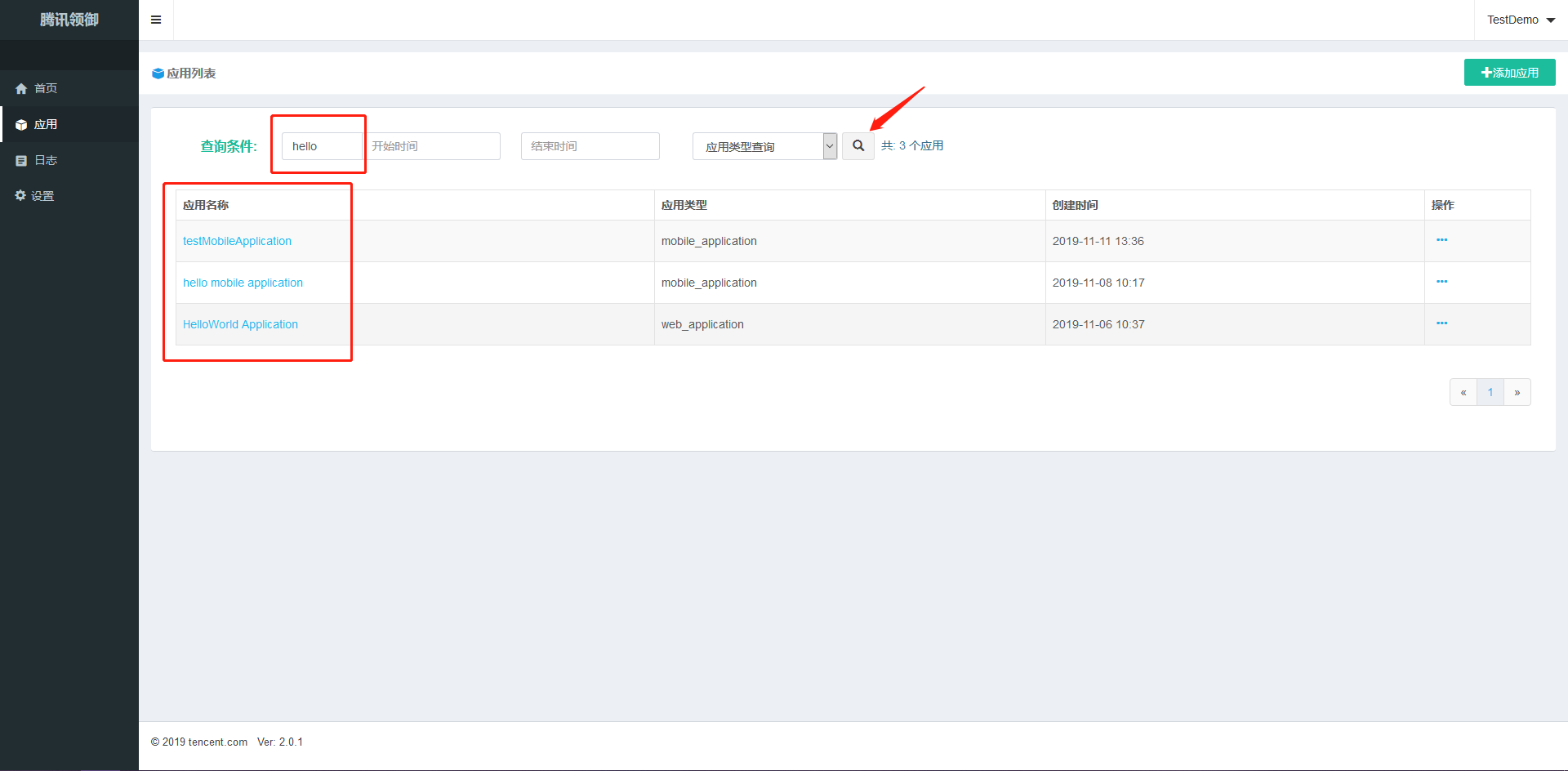
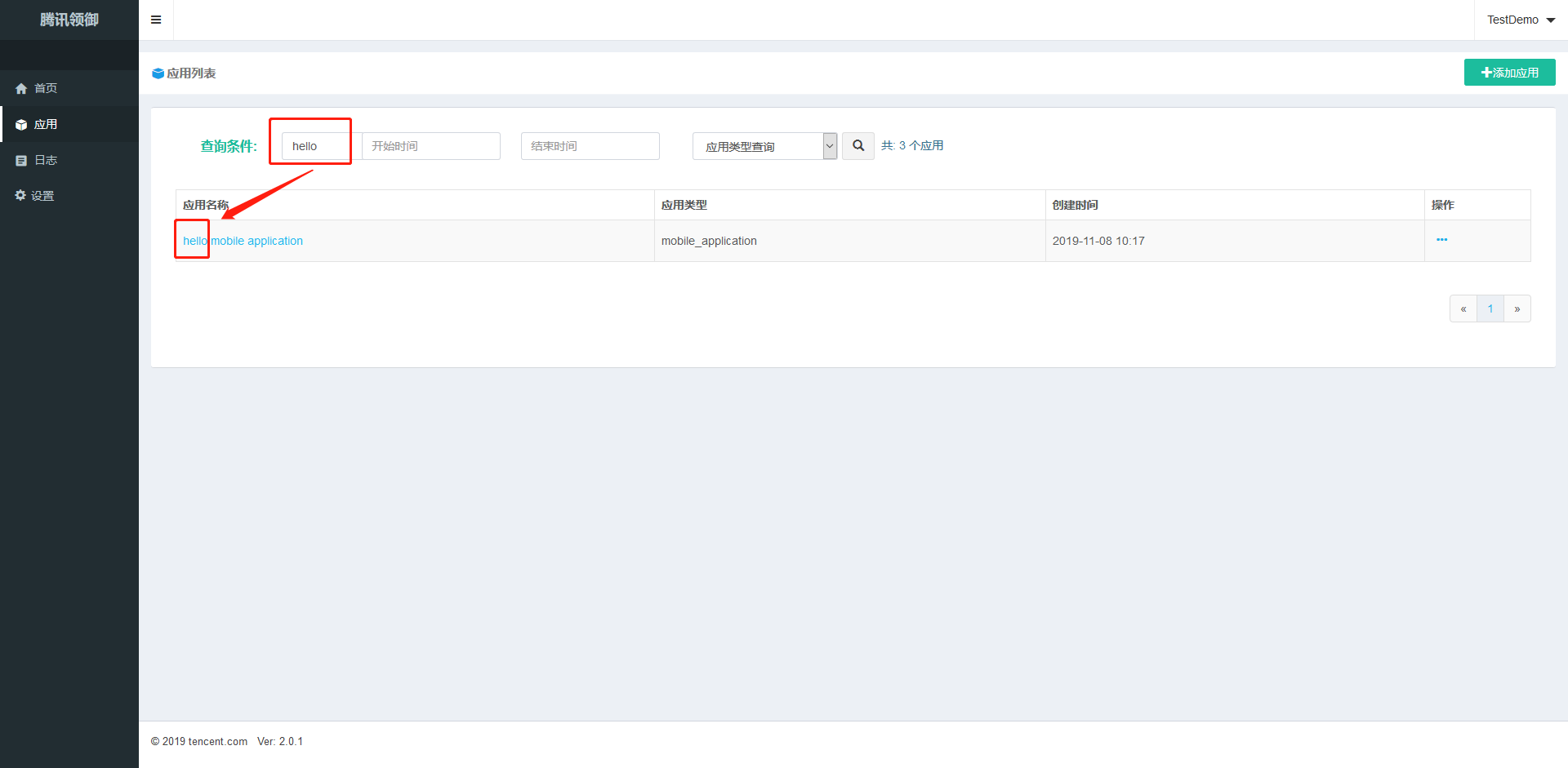
## 检索应用

在一般的场景下需要快速的查找需要的应用信息，可以使用应用的检索功能。该功能有通过应用名称、创建应用的开始时间、创建应用的结束时间、应用类型（包括web\_application和mobile\_application）来进行检索。



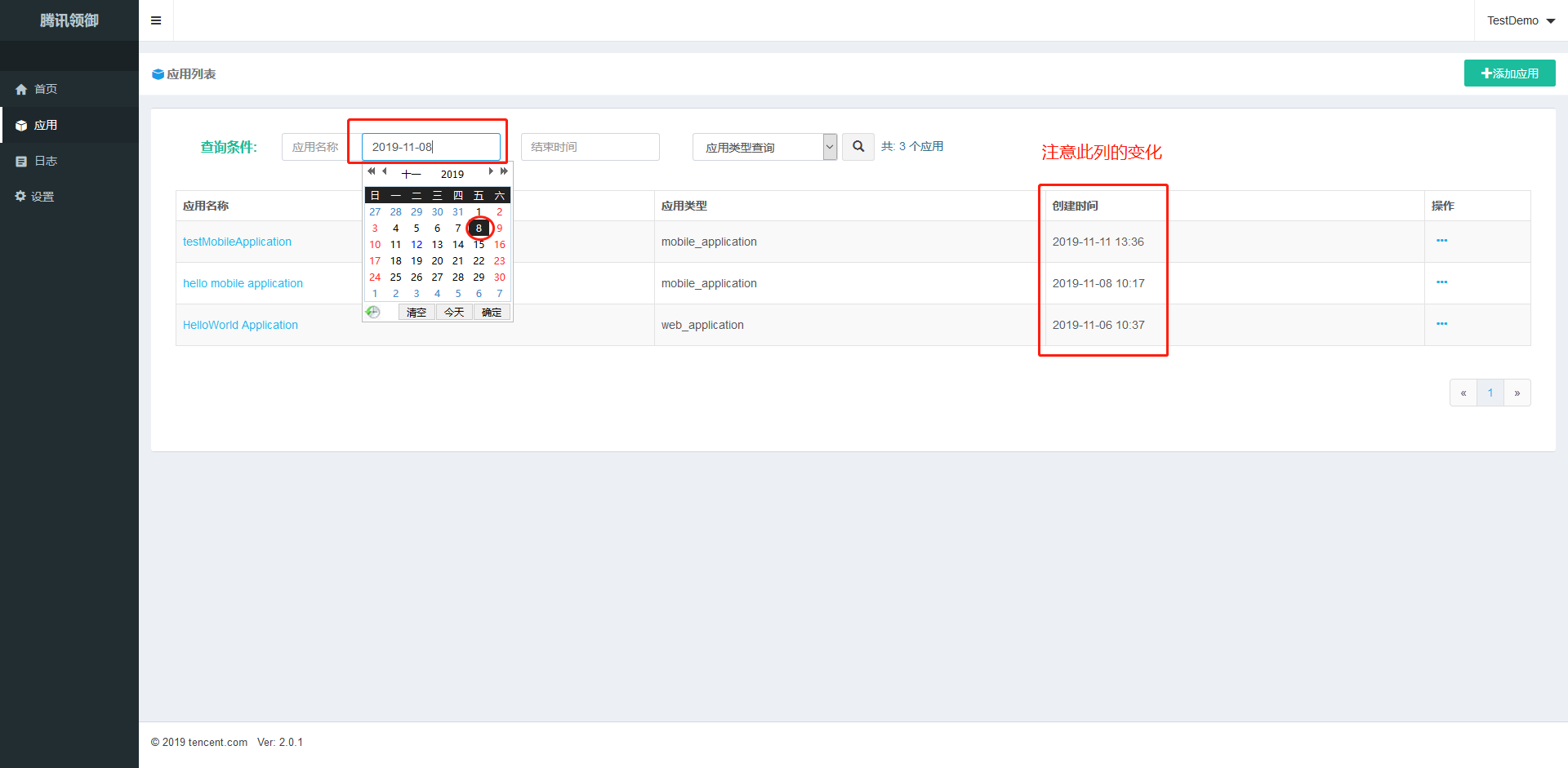
### 通过应用名称检索应用

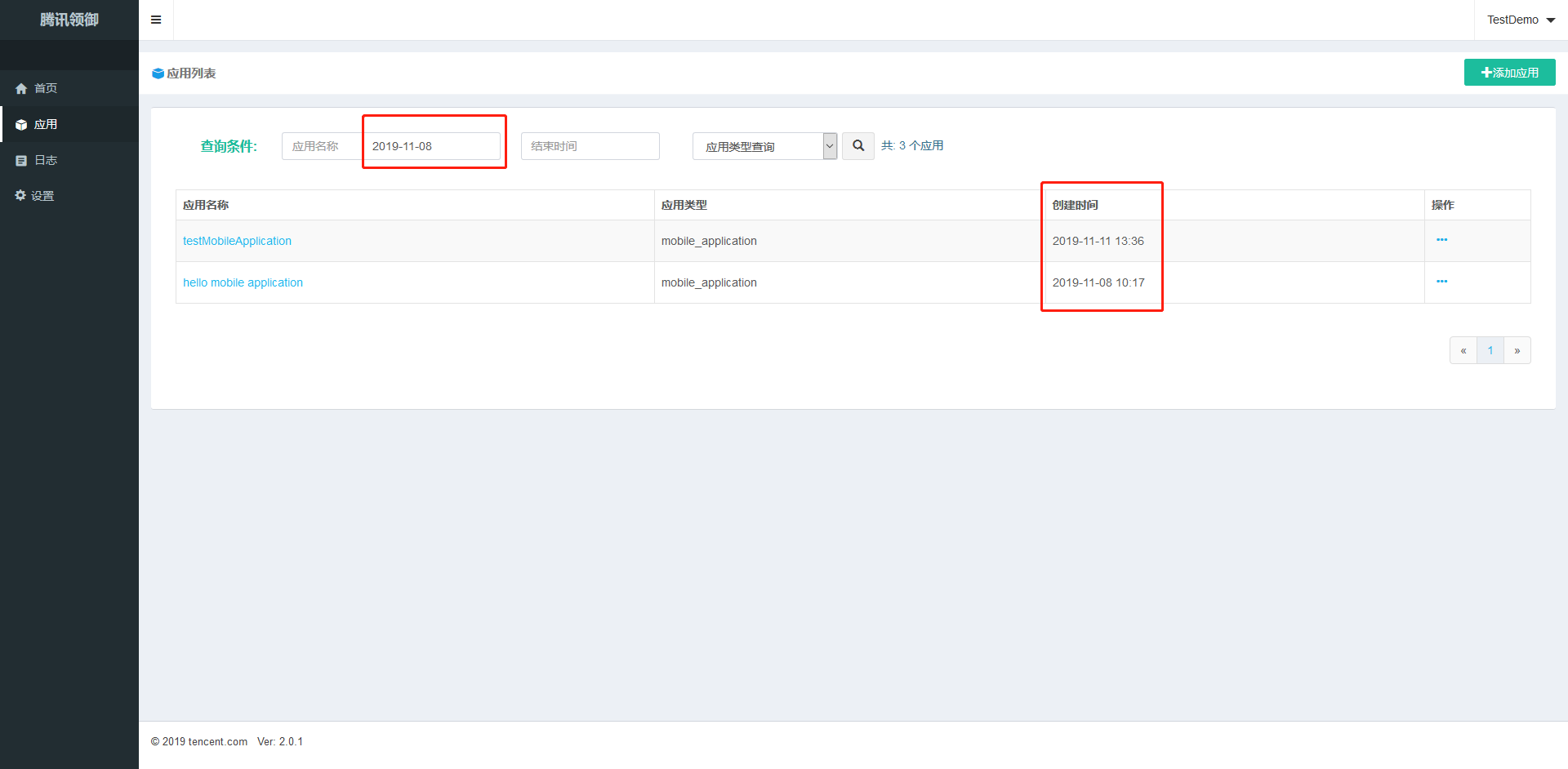
该功能使用的是根据应用名称进行模糊检索，例如在应用名称输入框输入“Test”，在应用列表中会展示所有包含“Test”应用名称的应用，需要注意的是该功能区分英文大小写。操作步骤如下：在应用名称输入框输入“hello”，点击该行最右测的检索按钮，查看应用列表。



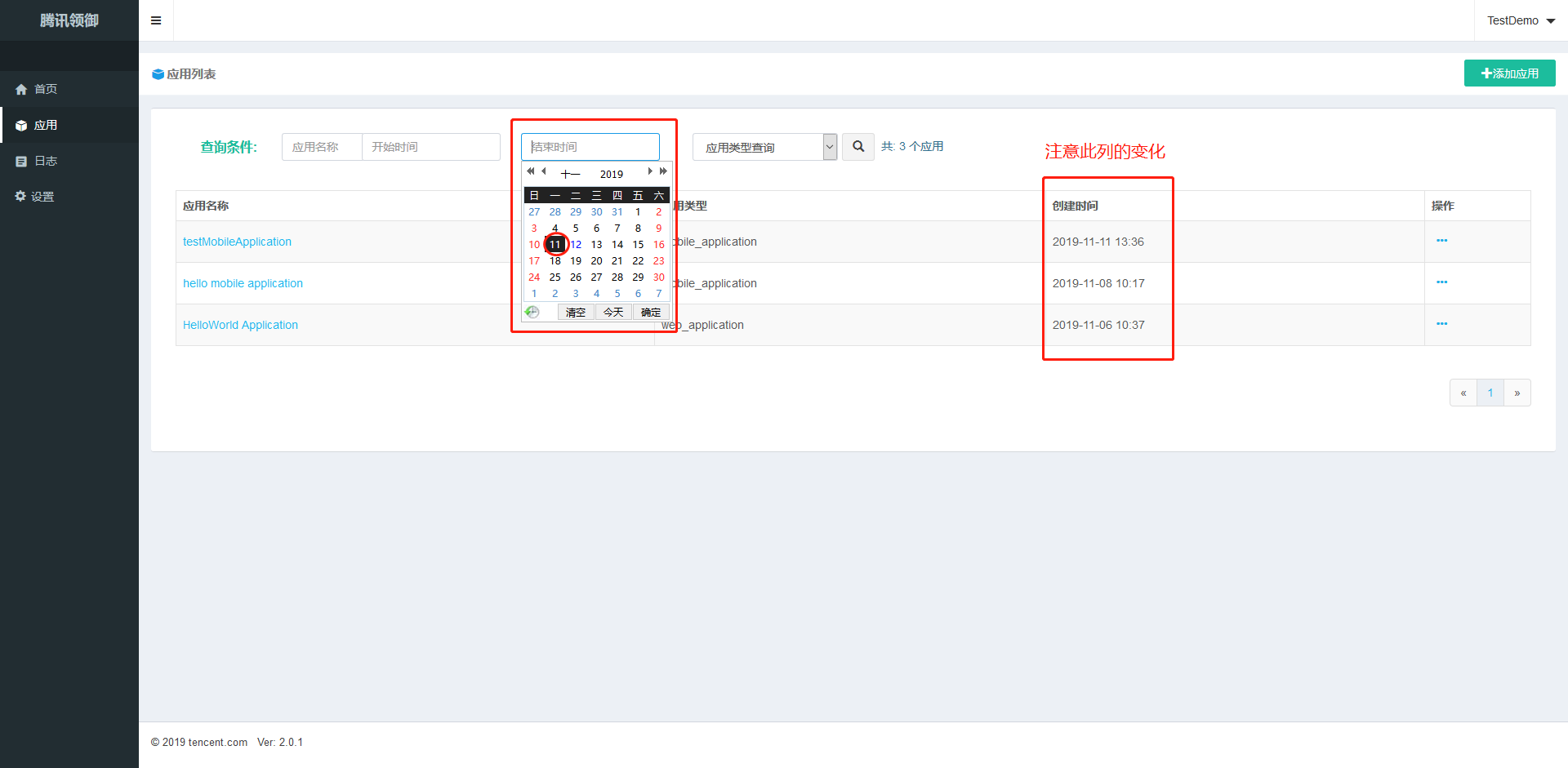
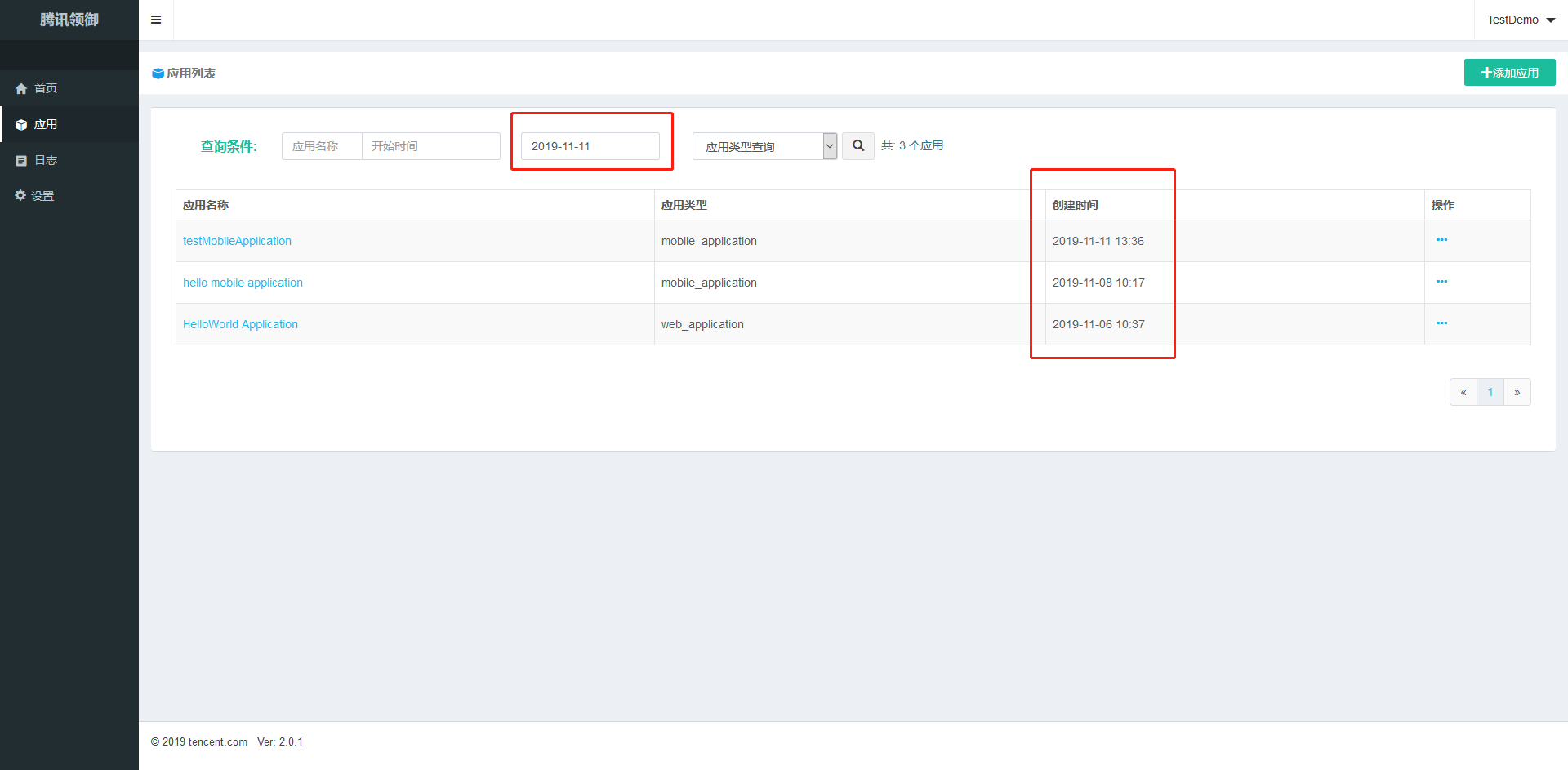
### 通过时间检索应用

通过时间检索应用包括通过开始时间检索应用、通过结束时间检索应用、通过开始时间与结束时间检索应用。

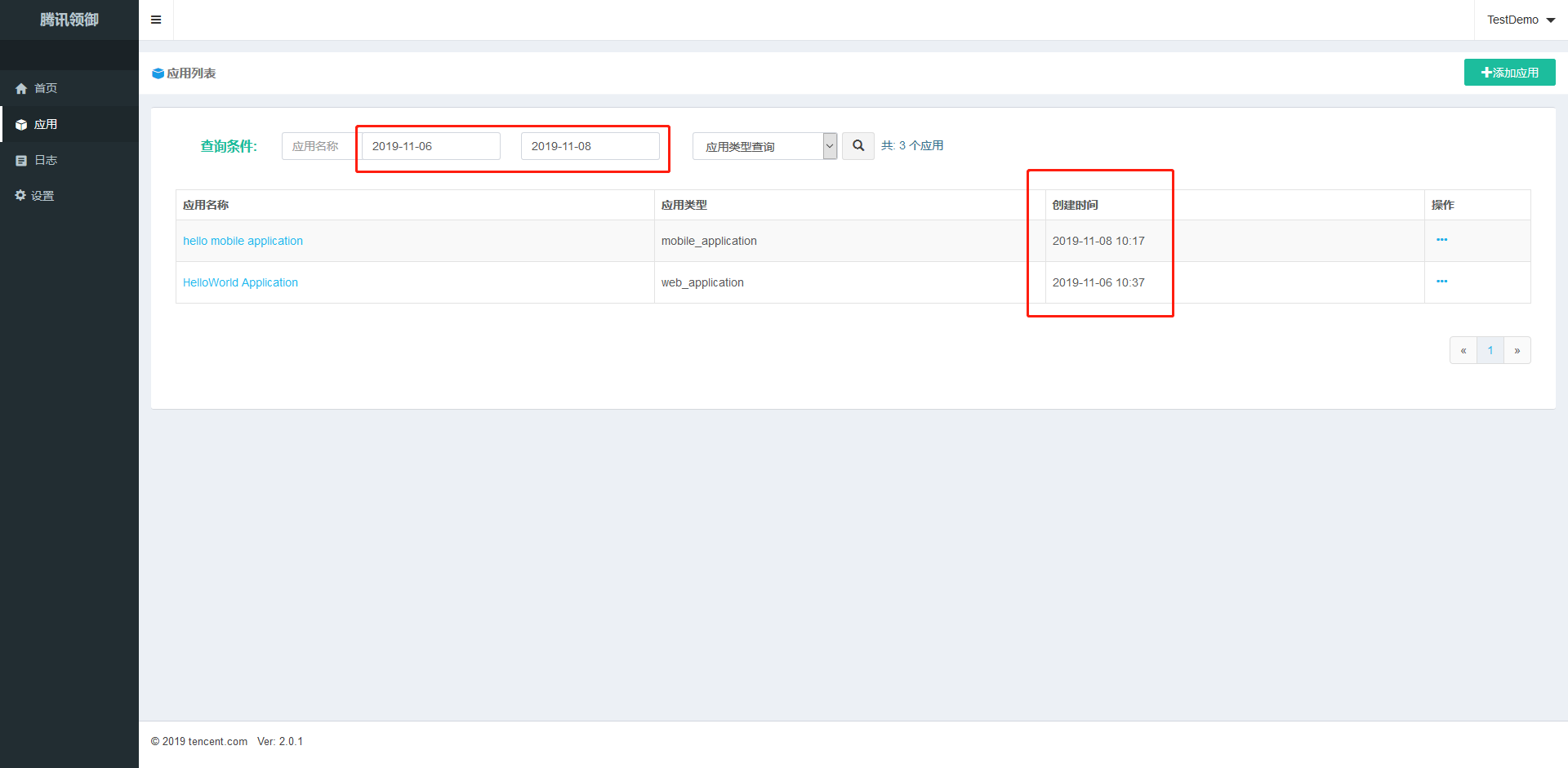
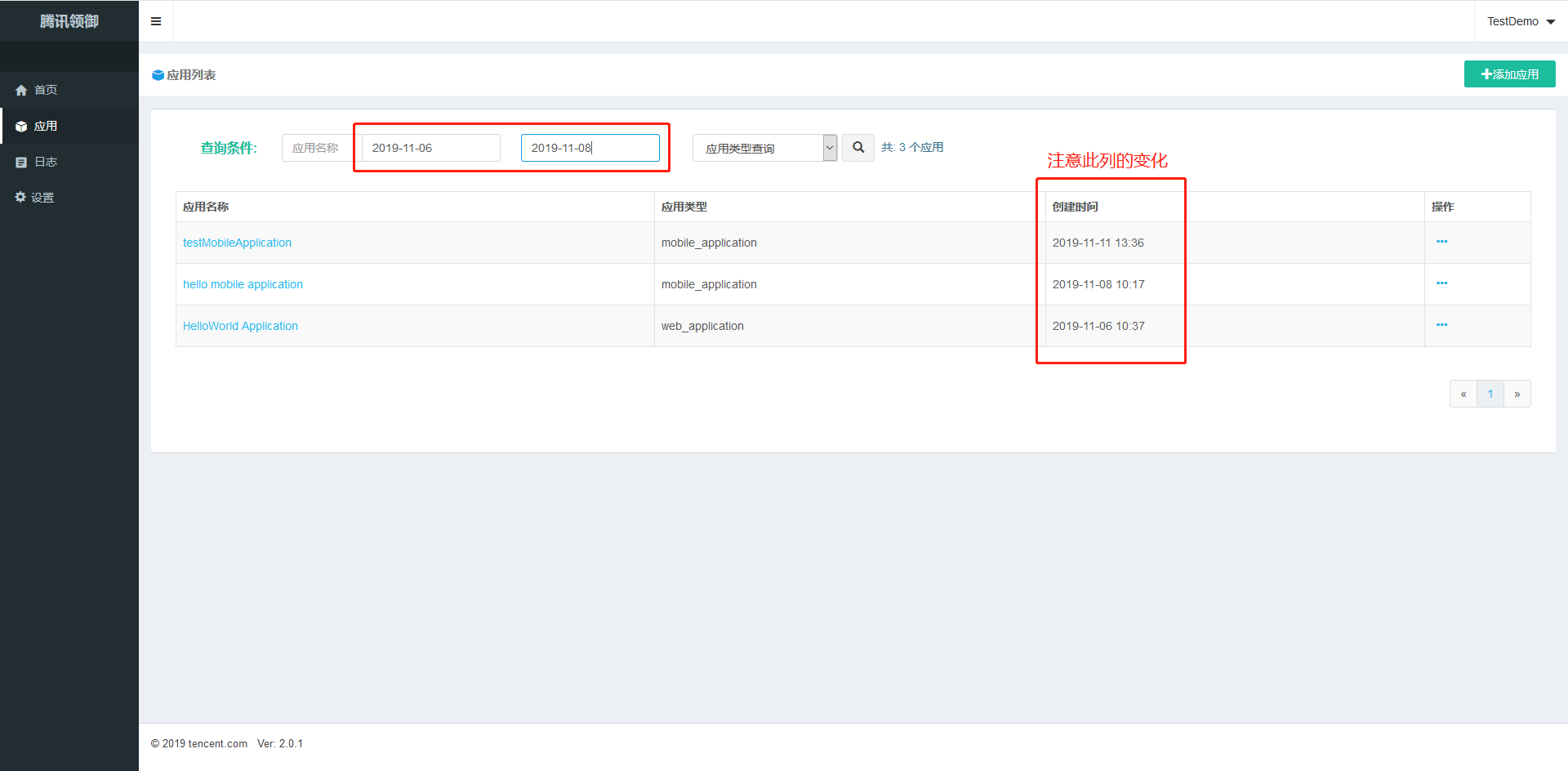
通过开始时间检索应用，该功能根据选择的日期时间的00:00检索以后的所有创建的应用。如下图，选择2019-11-08，然后点击搜索按钮，该界面会展示搜索后的应用列表。



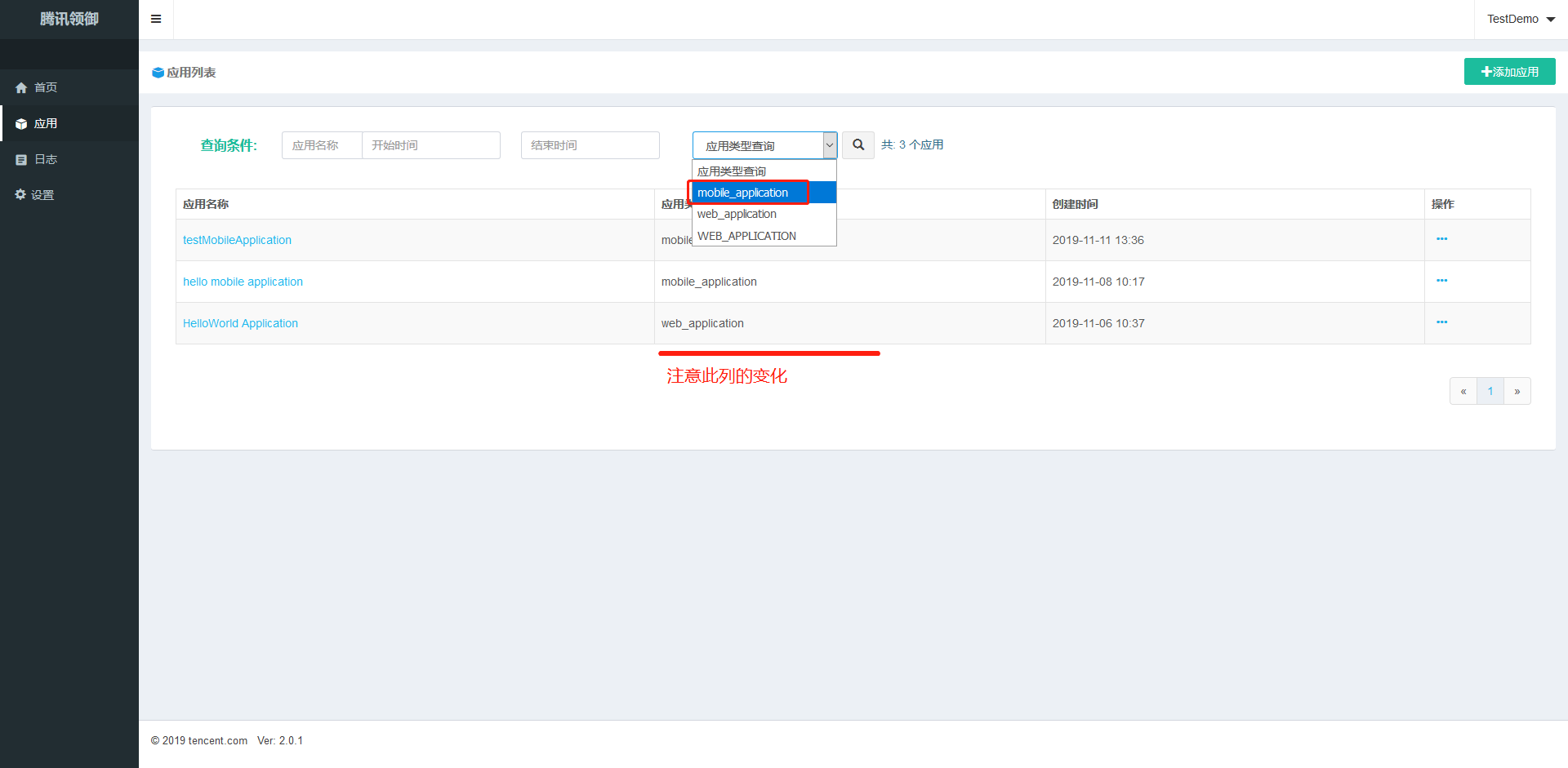
通过结束时间检索应用，该功能根据选择输入的结束日期的23:59检索之前的所有创建的应用。如下图，选择填入2019-11-11，然后点击搜索按钮，该界面会展示搜索后的应用列表。

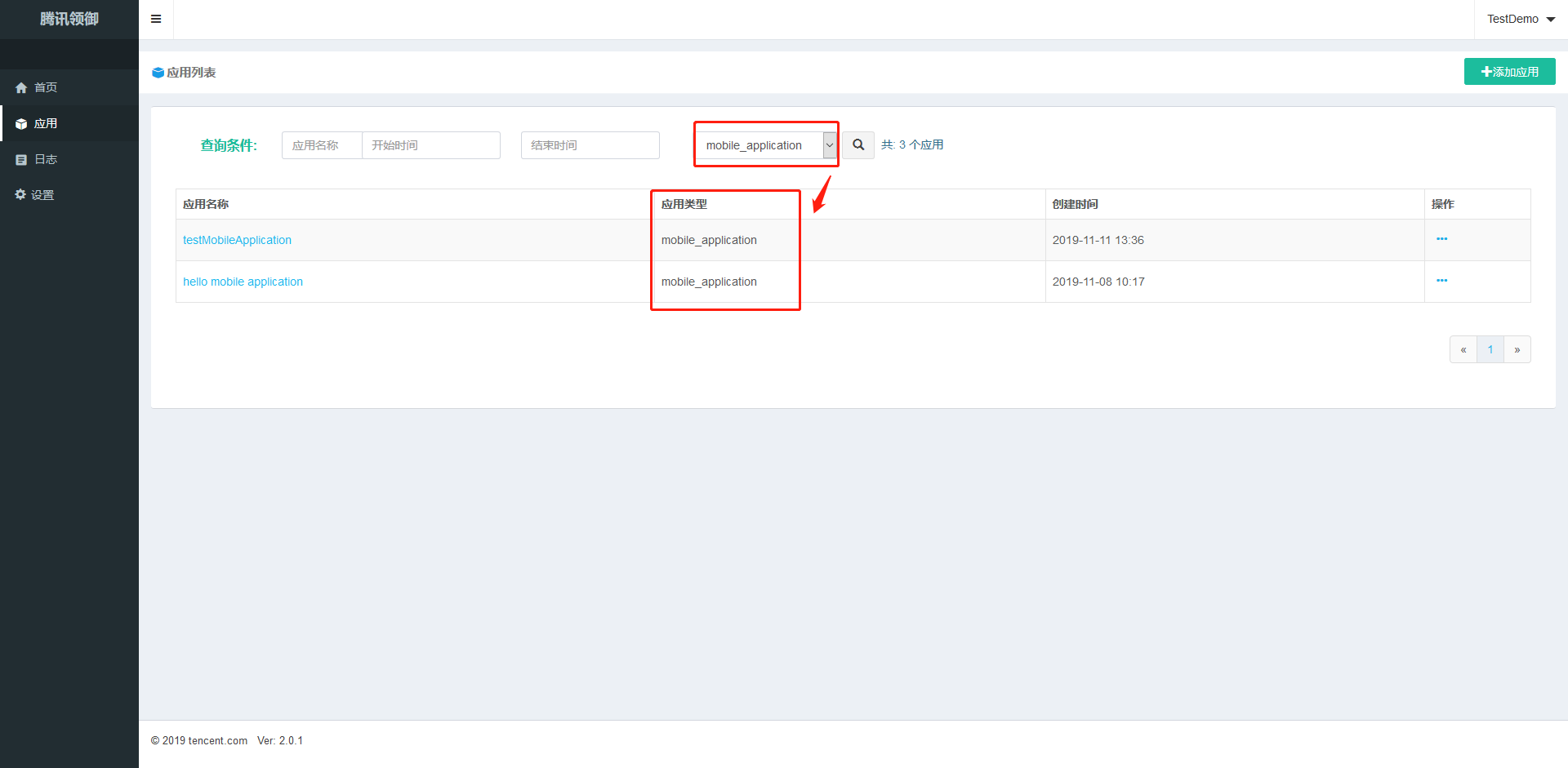


通过开始时间跟结束时间索引，同时包含了上述内容的功能，该功能根据选择输入的开始时间的00:00到选择输入的结束时间的23:59检索在此期间所有创建的应用。如下图，选择输入开始时间为2019-11-06，选择输入结束时间为2019-11-08，点击搜索，查看本界面的应用列表。

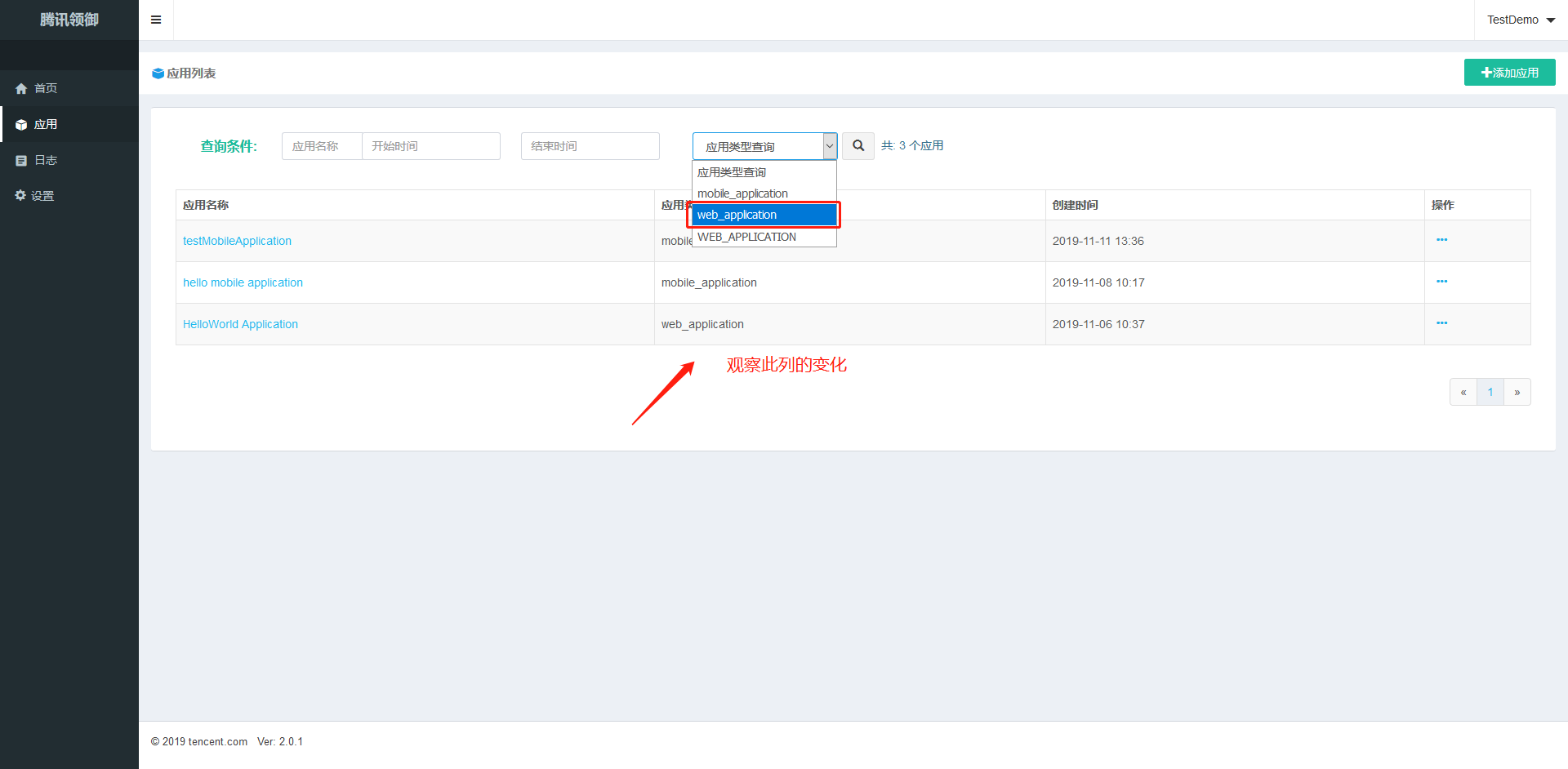
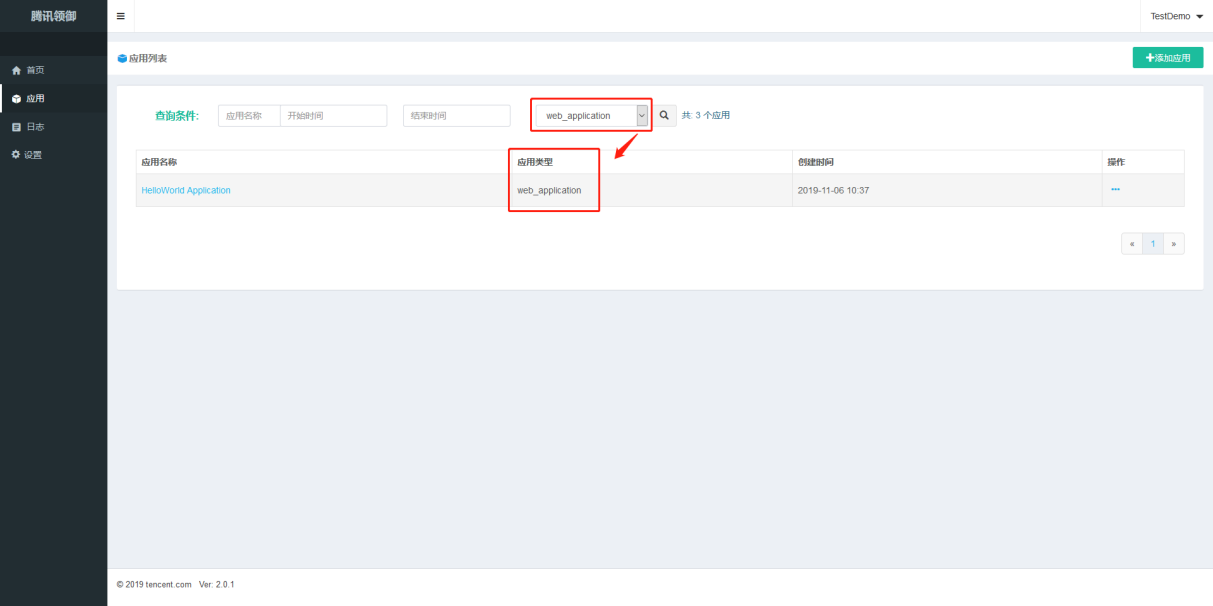


### 通过应用类型检索应用

在应用类型查询下拉框，根据需要选择mobile\_application或者选择web\_application，点击搜索按钮，查看该界面的查询结果。

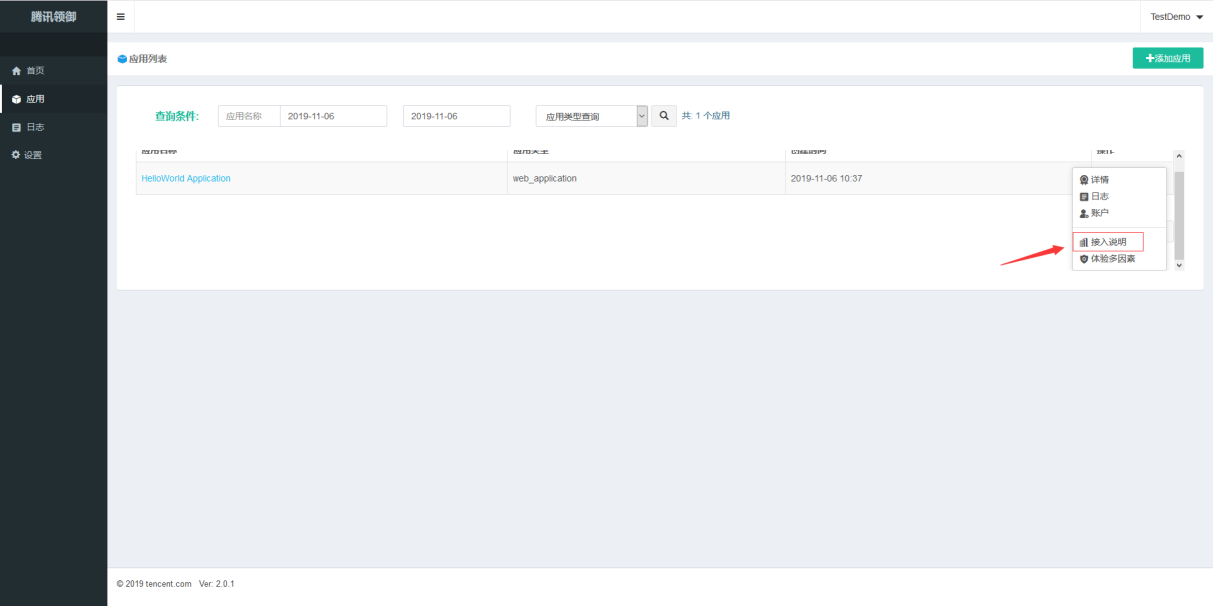
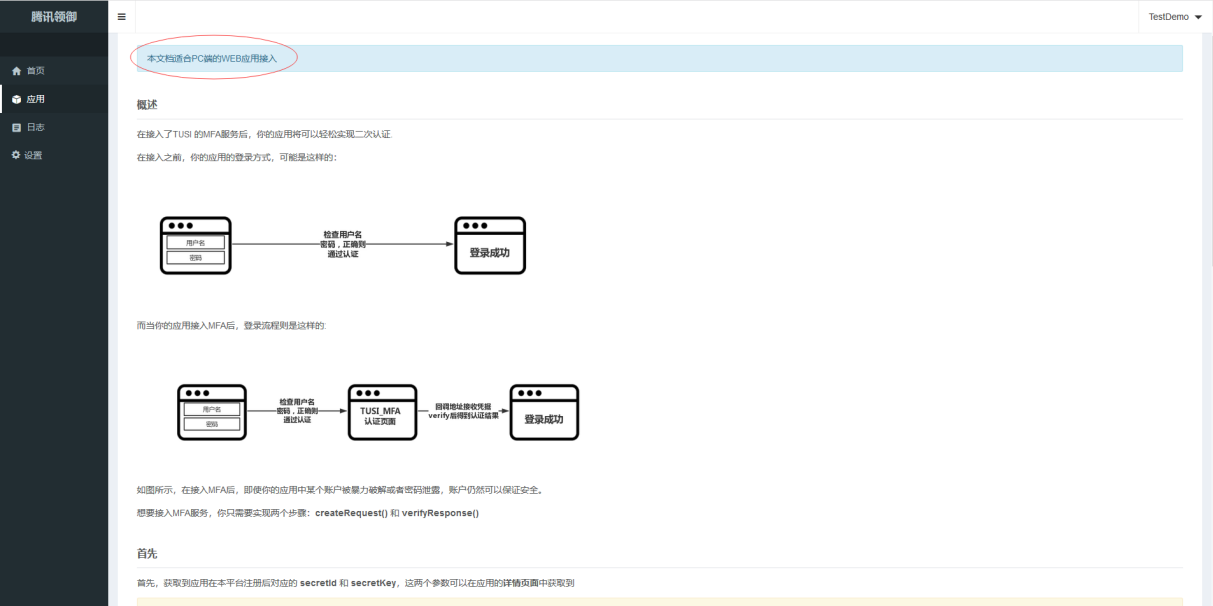
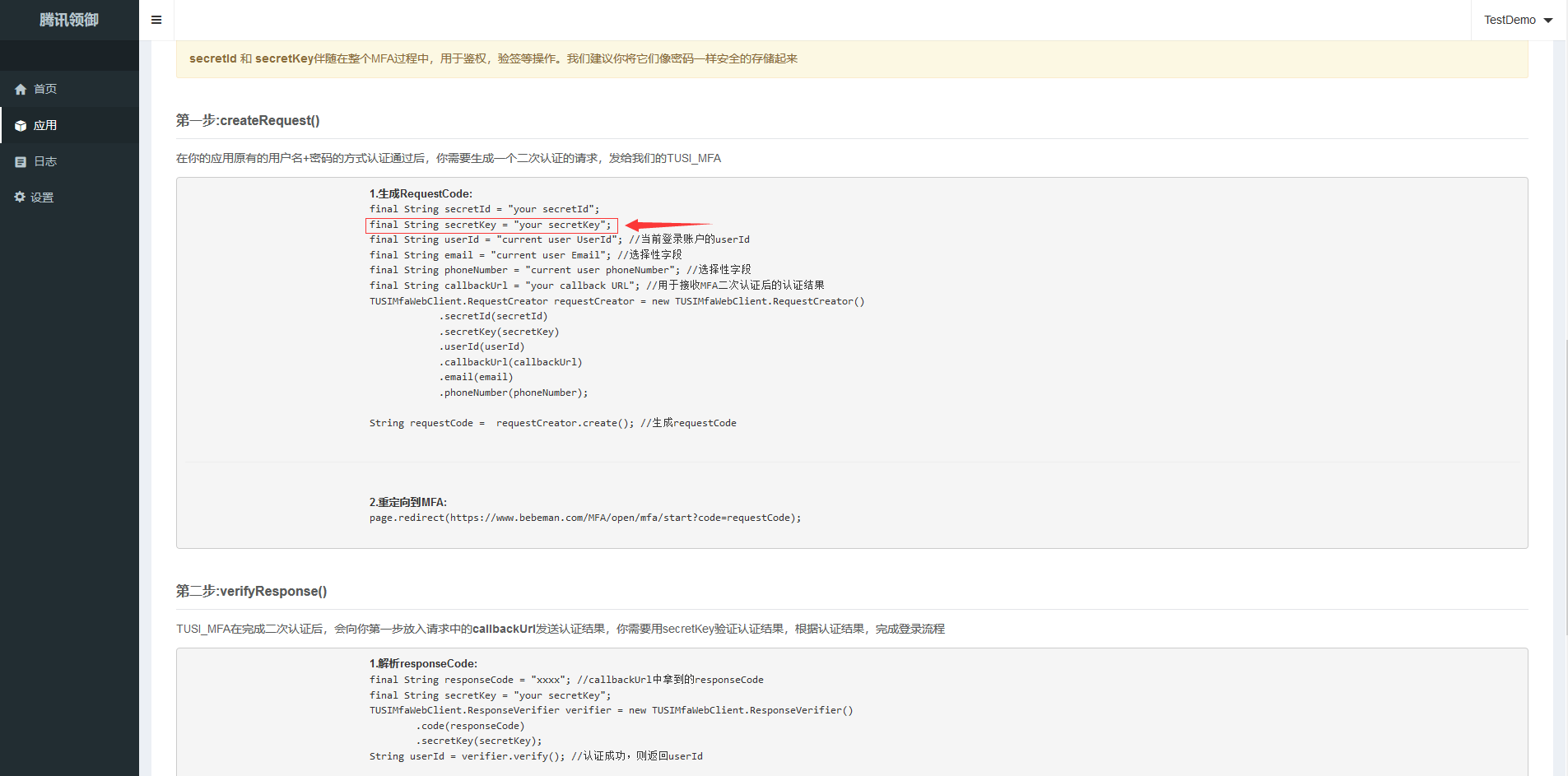


根据需求选择应用类型为web\_application时，先点击下拉框选择web\_application，点击搜索按钮，查看所有应用类型为web\_application的应用列表。如下图所示。



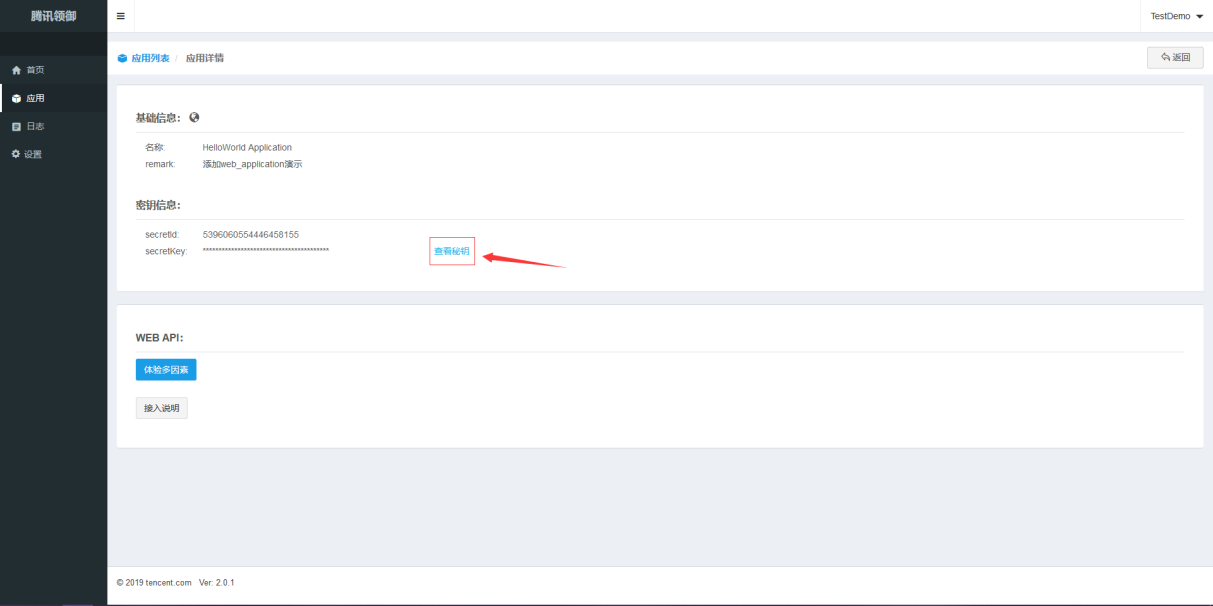
## 应用接入说明

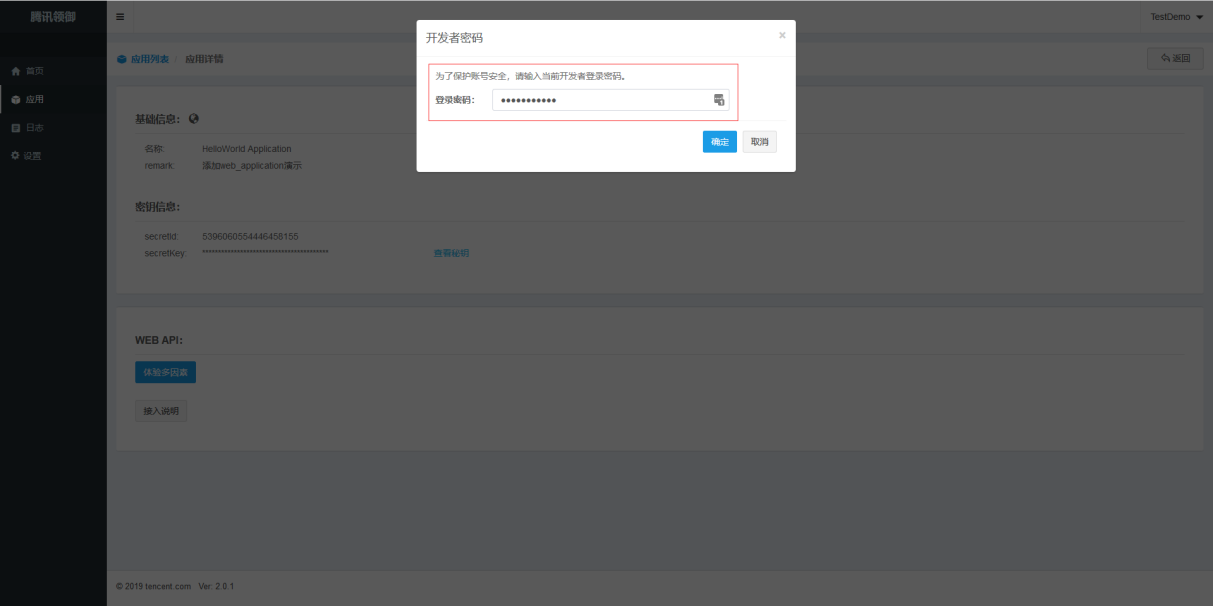
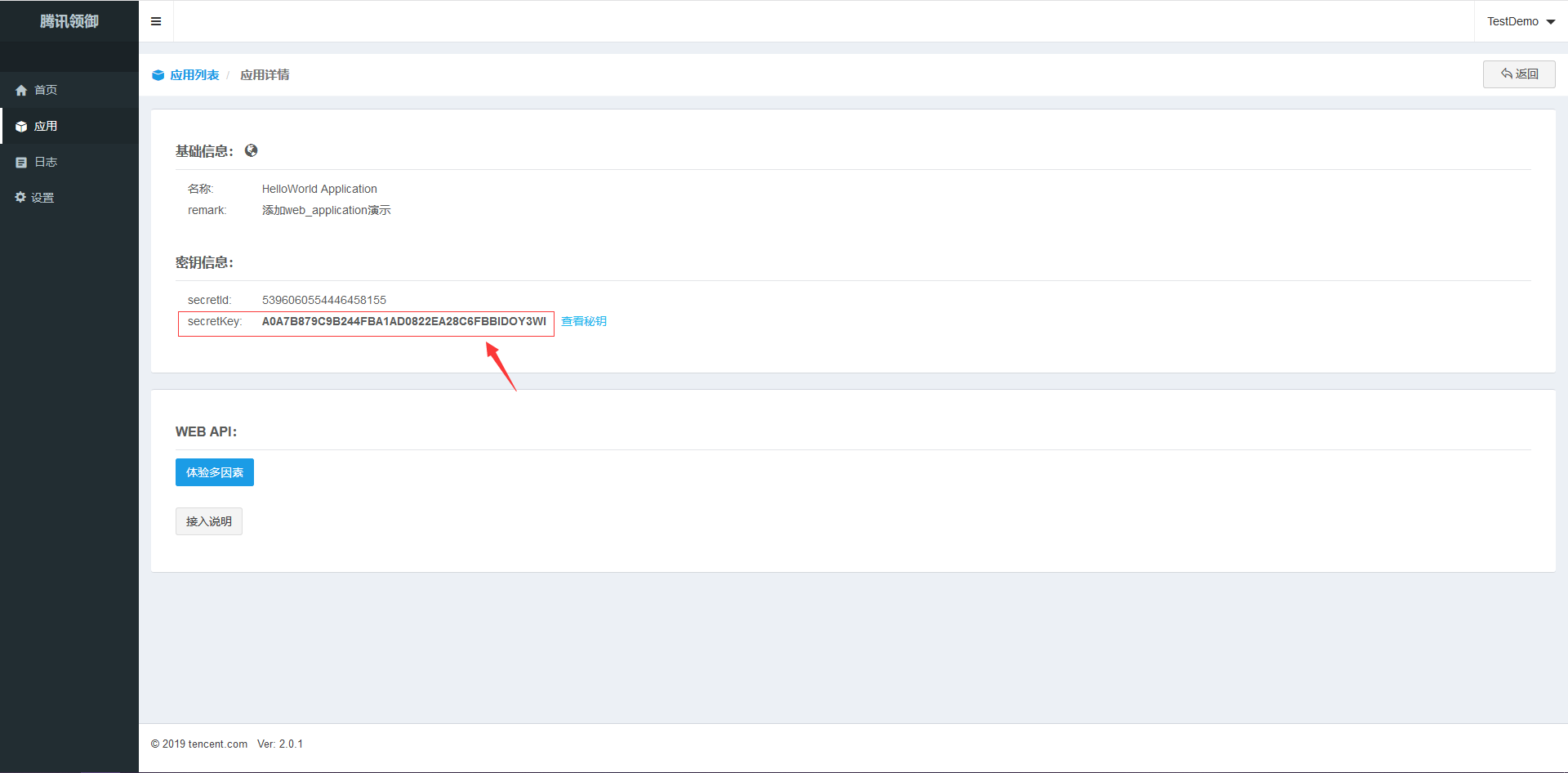
应用接入说明本质上是一个接入文档，该文档介绍了第三方应用使用多因素认证的具体操作步骤，根据接入说明文档中的信息进行操作。在操作菜单栏，会有“接入说明”按钮，点击后进入接入说明界面。



## 查看应用秘钥

在接入文档中需要使用到秘钥信息，为了安全考虑，默认秘钥是不可见的，需要开发者输入登录密码才能获取应用秘钥。

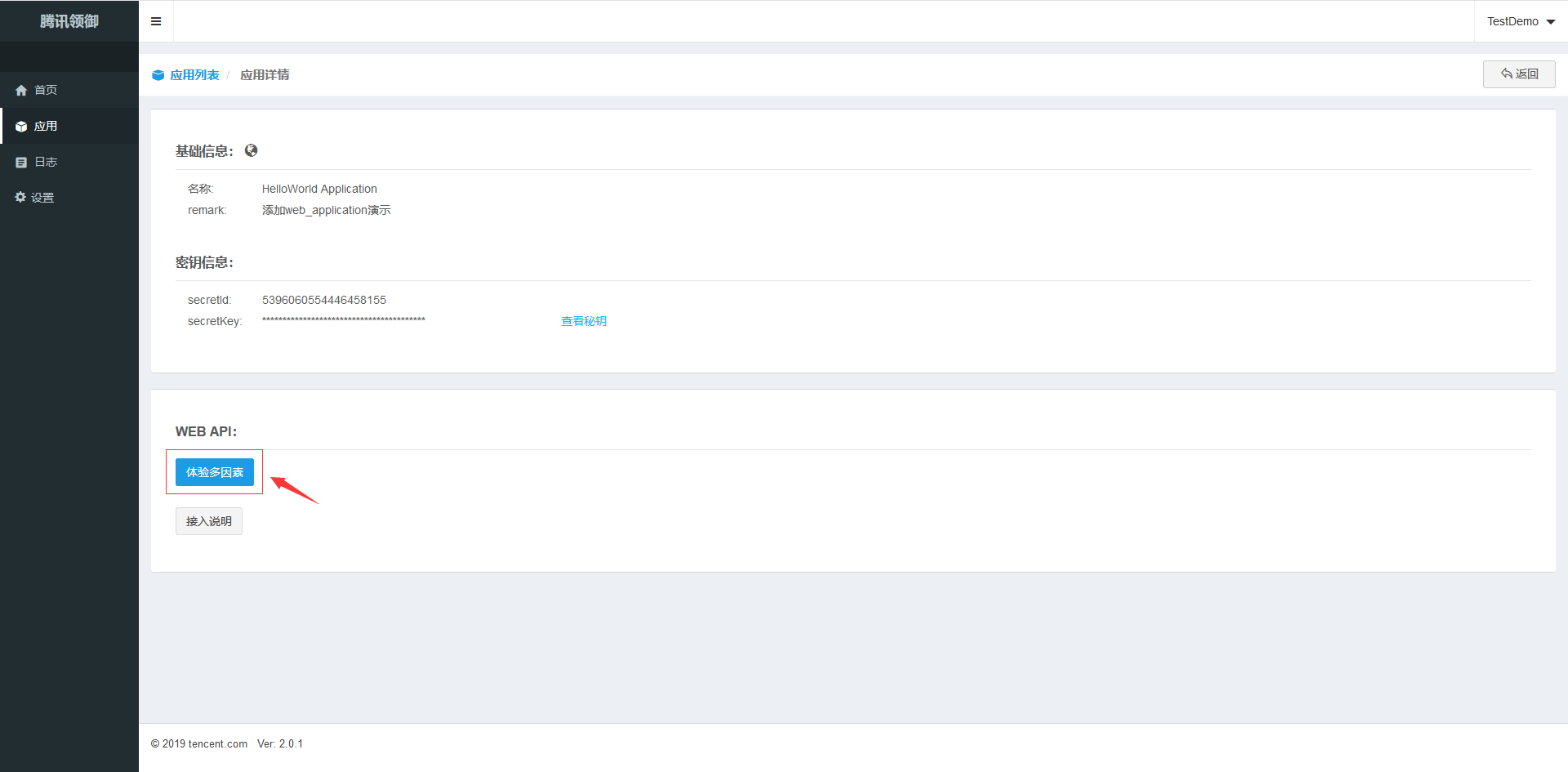
首先进入到应用详情界面，点击查看秘钥，输入开发者登录密码。输入正确后展示秘钥，具体操作如下：

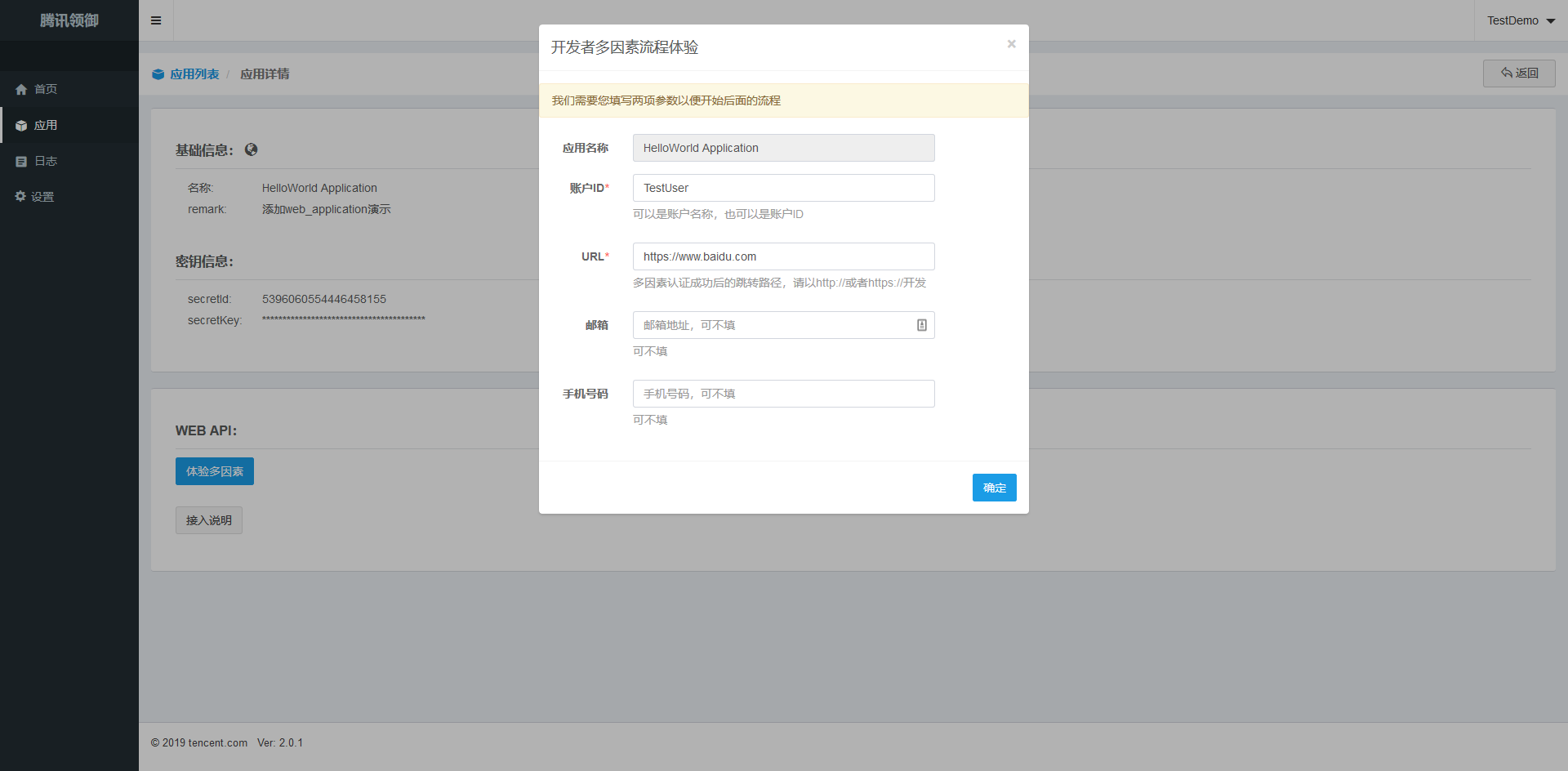


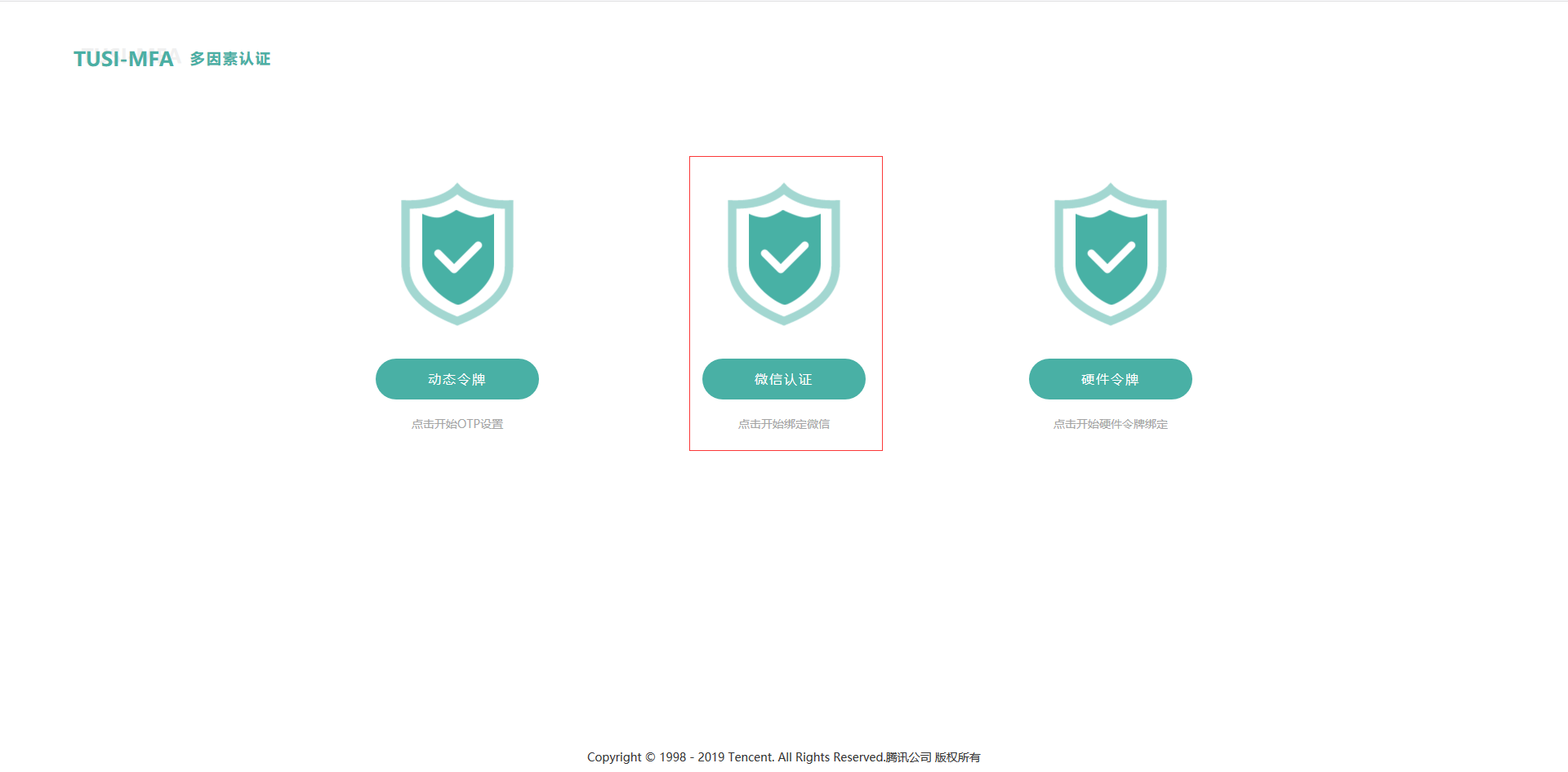
## 添加账户

在接入说明的文档中的secretKey的下一行需要userId属性，该userId就是添加账户后生成的账户名。

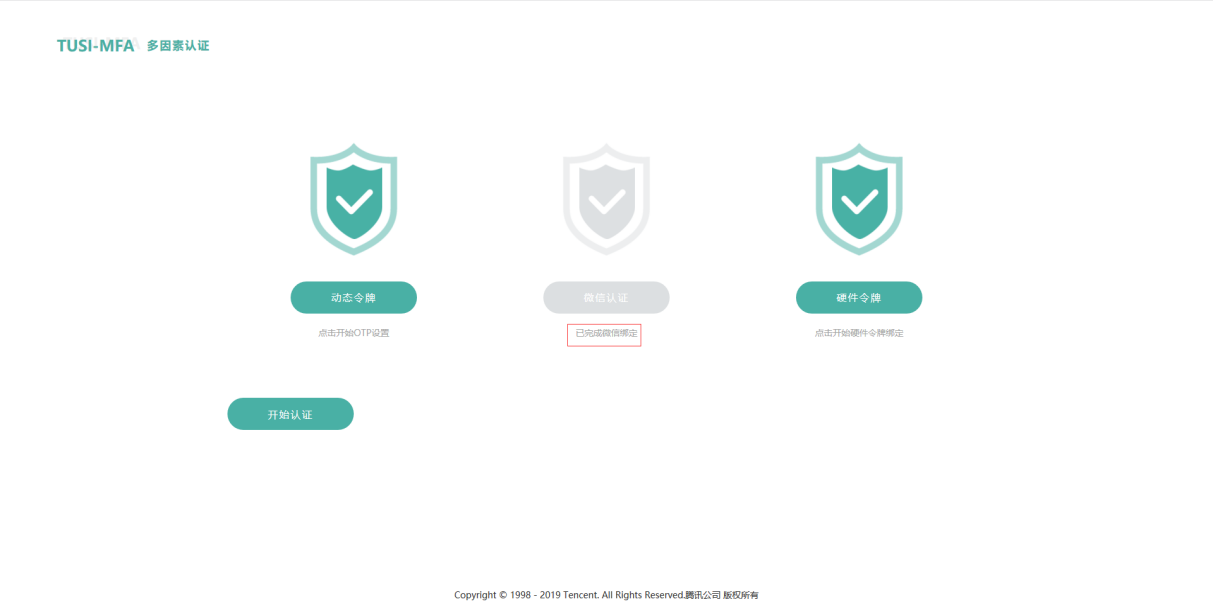
在该应用的详情界面点击体验多因素按钮，在弹出框中输入具体信息，其中账户ID和URL是必填项。点击确认后会进入到多因素认证界面，其中包括了动态令牌认证、微信认证、硬件令牌认证，动态令牌认证跟硬件令牌认证操作请参考第6章设置模块。

在开发者多因素流程体验界面，账户ID文字框中可以填写账户ID或者是账户名，下面的URL文字框中填写通过认证后跳转的网址，这里以百度为例子，所以填写的是百度的网址，开发者可以根据自己的需求填写对应的URL。邮箱跟手机号码是可选项。

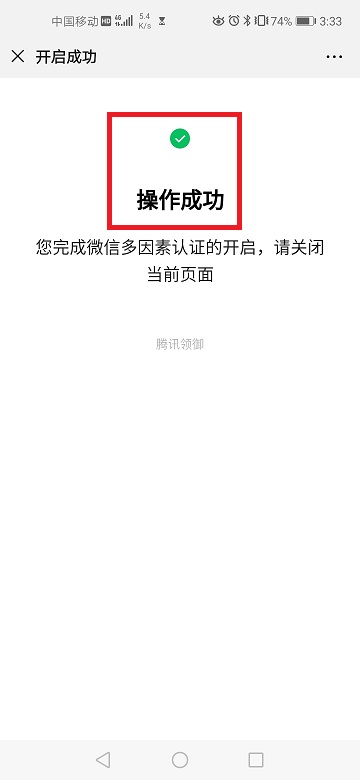




用微信扫描二维码，关注公众号【腾讯领御】，若扫描二维码后微信号未关注该公众号，请手动搜索“腾讯领御”公众号，点击关注。扫描后点击“确认开启”，开启后web端会展示已完成微信绑定。



移动端扫码后的操作如下：



接下来点击开始认证，实验该认证方式是否成功。

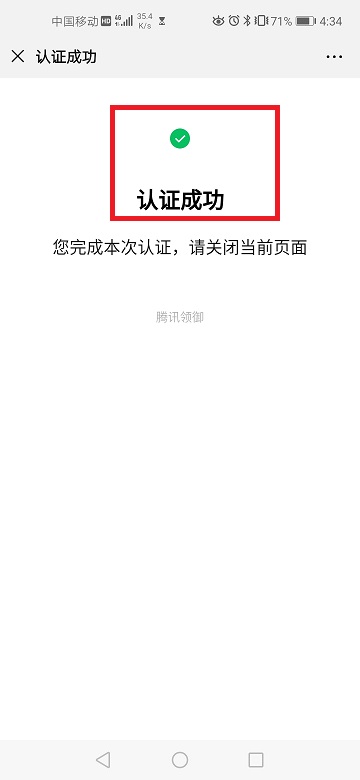
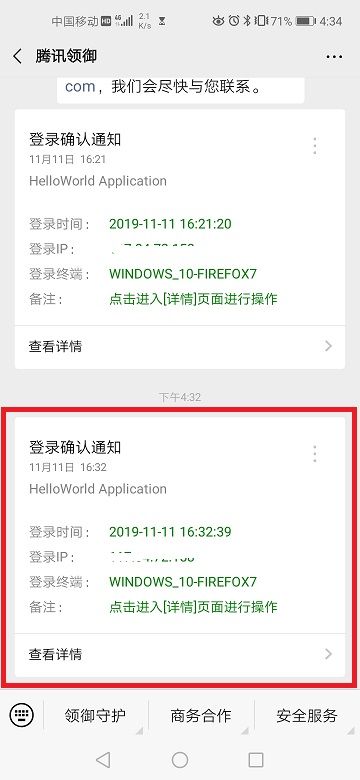
具体步骤如下：第一步点击开始认证，进入到微信认证界面。

点击开始，开始向微信推送请求，由用户决定是否通过验证。

该界面表示正在推送，需要微信端操作。

下面展示微信端是如何操作的。

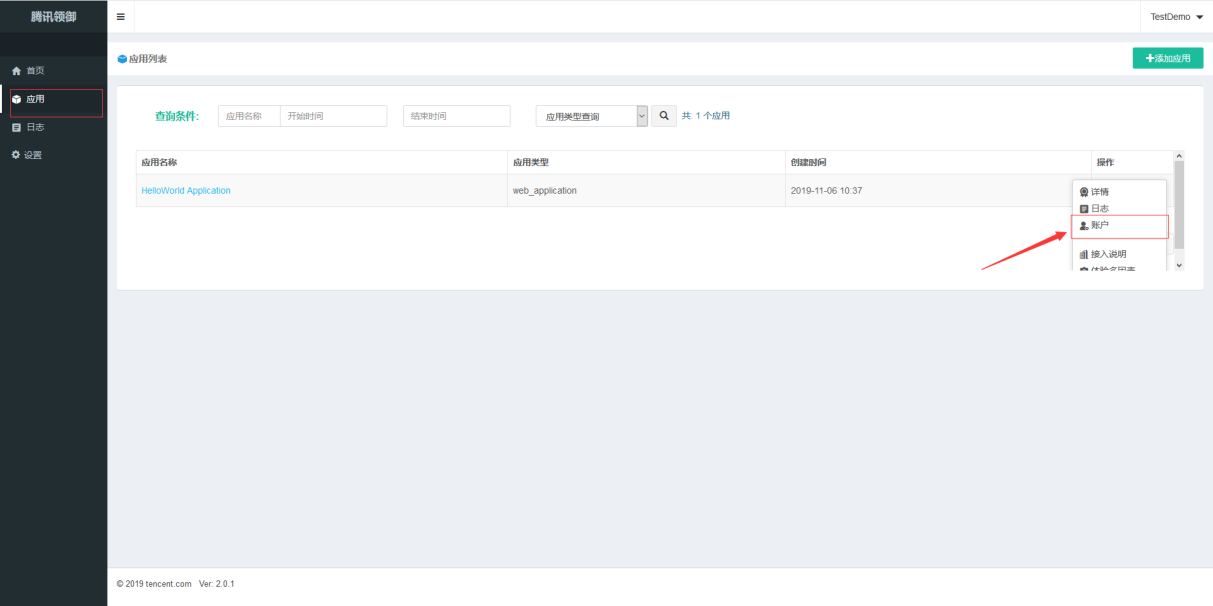
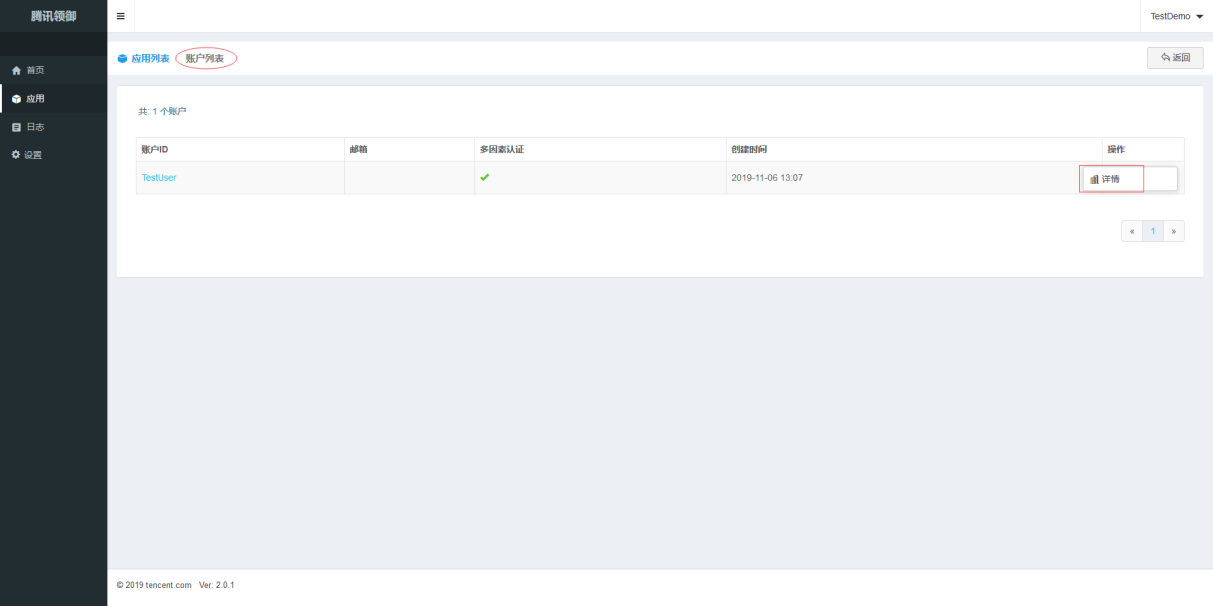
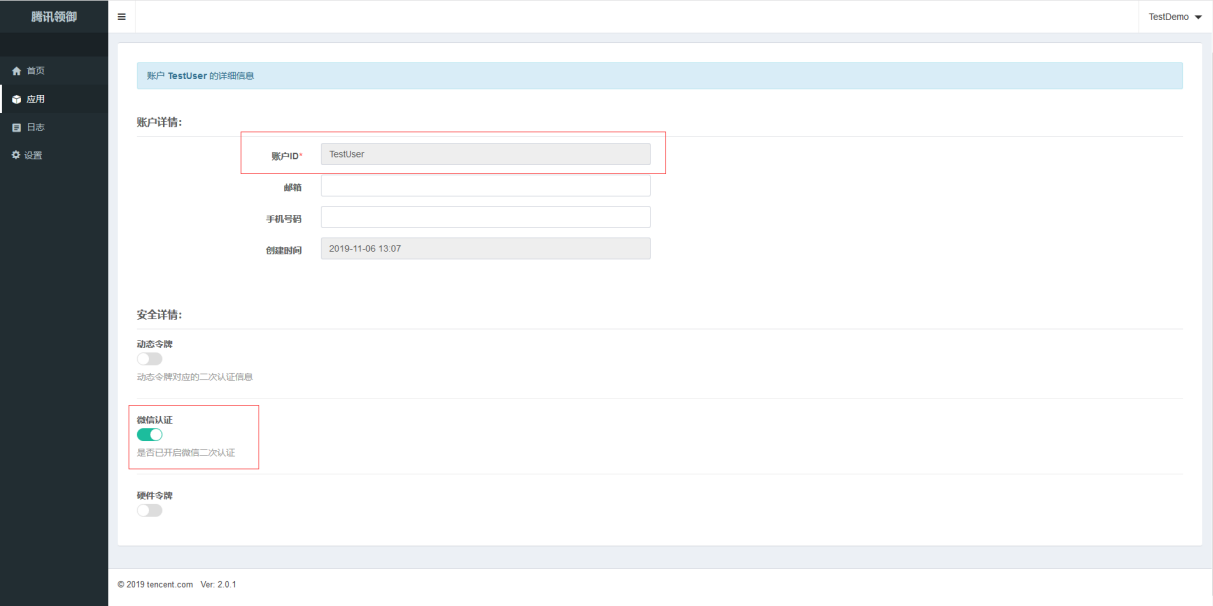
认证成功后，查看web端的响应，成功跳转到了百度主页。





## 查看应用账户

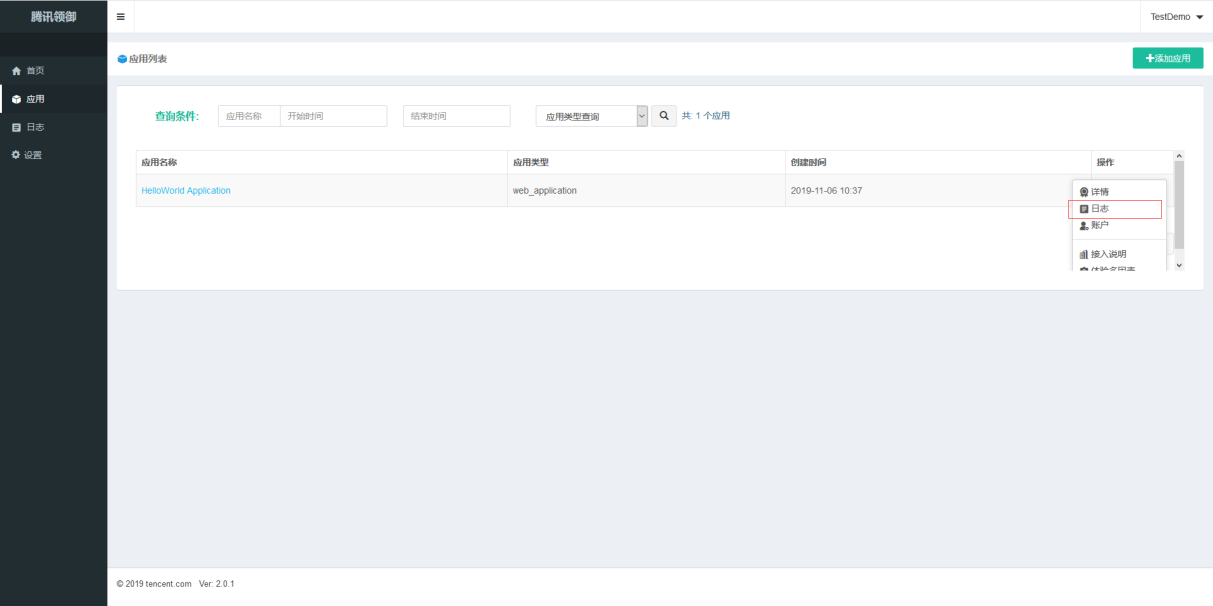
在成功创建一个账户的基础上，需要查看刚刚创建的账户，操作如下：首先进入到应用列表界面，点击该应用的操作按钮，点击账户，会展示该应用添加的账户列表，在账户列表界面，直接点账户名或者点击操作按钮中的详情，来展示该账户的详细信息。

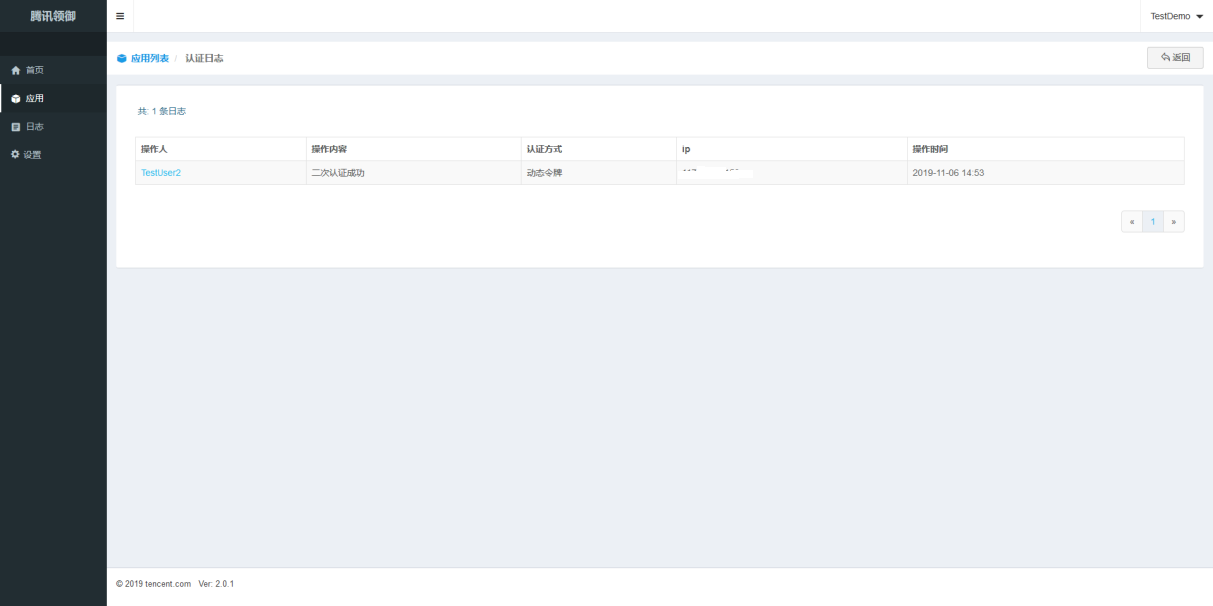


## 查看应用日志

在应用日志中主要展示该应用下的所有账户的相关信息，展示的操作人就是应用下的账户名，操作内容是账户的操作日志，认证方式是指该账户是以何种方式认证的，ip跟操作时间不做赘述。

首先点击应用列表中的操作按钮，选择点击日志，接下来会进入到应用列表中的认证日志界面，在这里可以看到该应用的所有账户的认证日志信息。





# 多因素认证

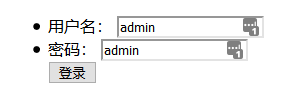
目前，多因素平台提供了动态令牌认证、微信认证、硬件令牌认证三种二次认证方式，开发者根据需求选择开启何种二次认证。该模块的功能主要为了开发者接入多因素认证而服务的。

开发者开发的web应用接入多因素认证请参考3.7应用接入说明操作，或者参考https://github.com/Shan589/mfademo.git。该项目使用的多因素平台是本地项目，所以参数需要按接入说明文档修改。

## 动态令牌认证

### 动态令牌认证web端操作

首先在第三方项目中正确输入用户名与密码，点击登录。



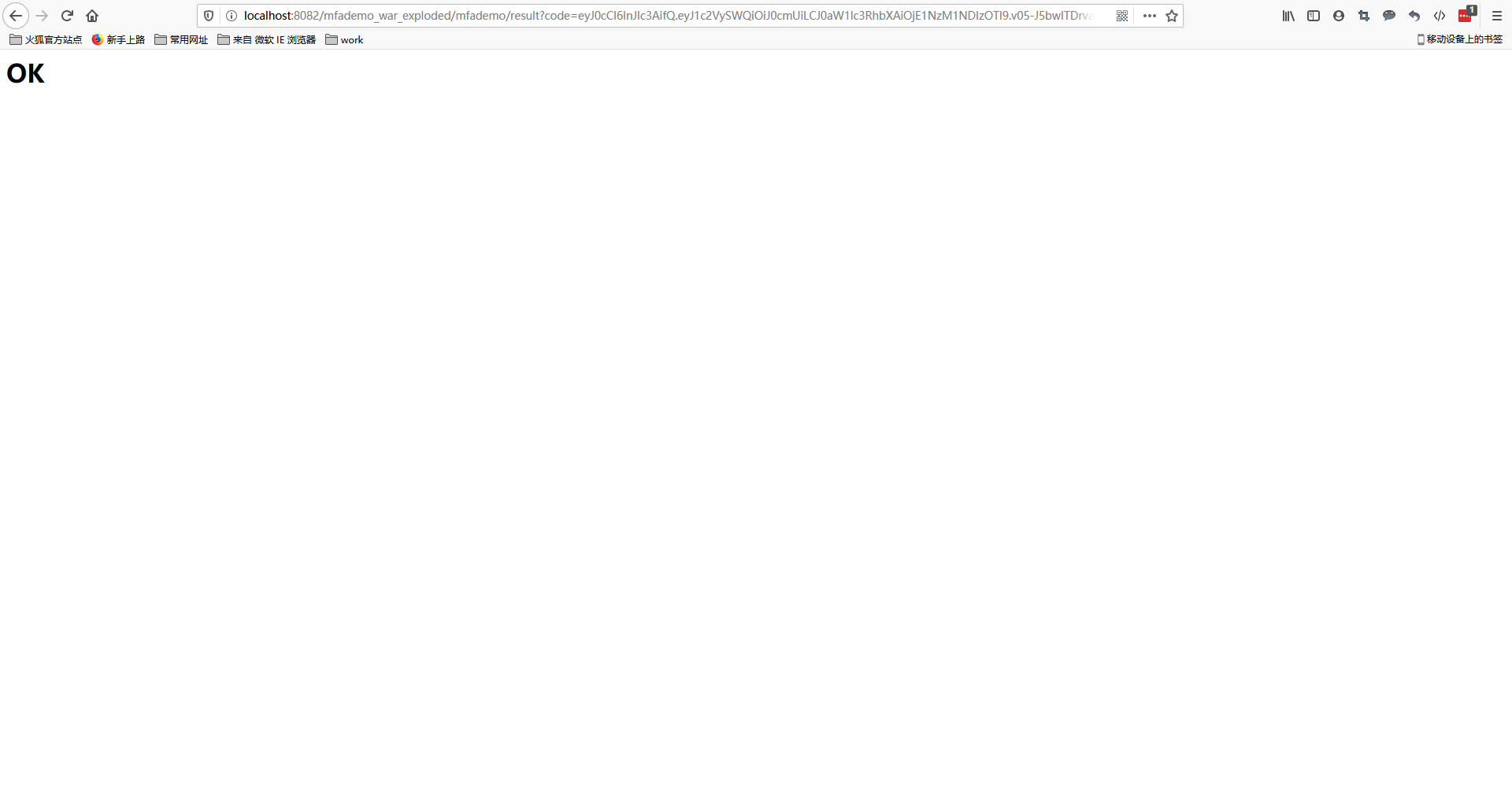
成功登录后进入二次认证界面，选择点击“动态令牌”

然后按操作扫描界面中的二维码，并输入移动端获取的动态6位数一次性密码

完成动态令牌绑定后，开始认证此操作是否有效。

在认证界面输入6位数动态令牌。

认证成功后，返回userid。后续操作按开发者开发需求进行。测试项目中展示“OK”界面，如下图：



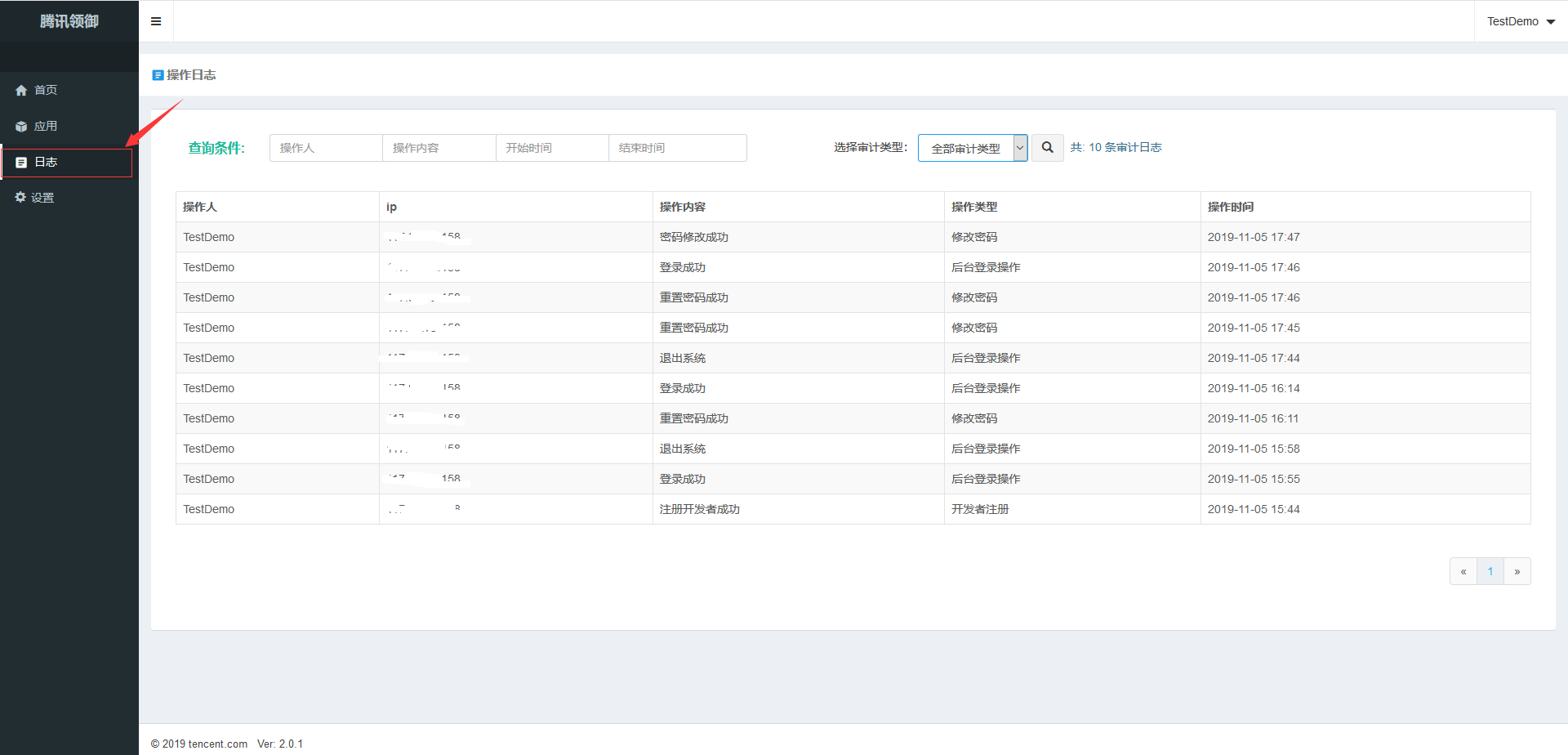
## 微信认证

## 硬件令牌认证

# 日志模块

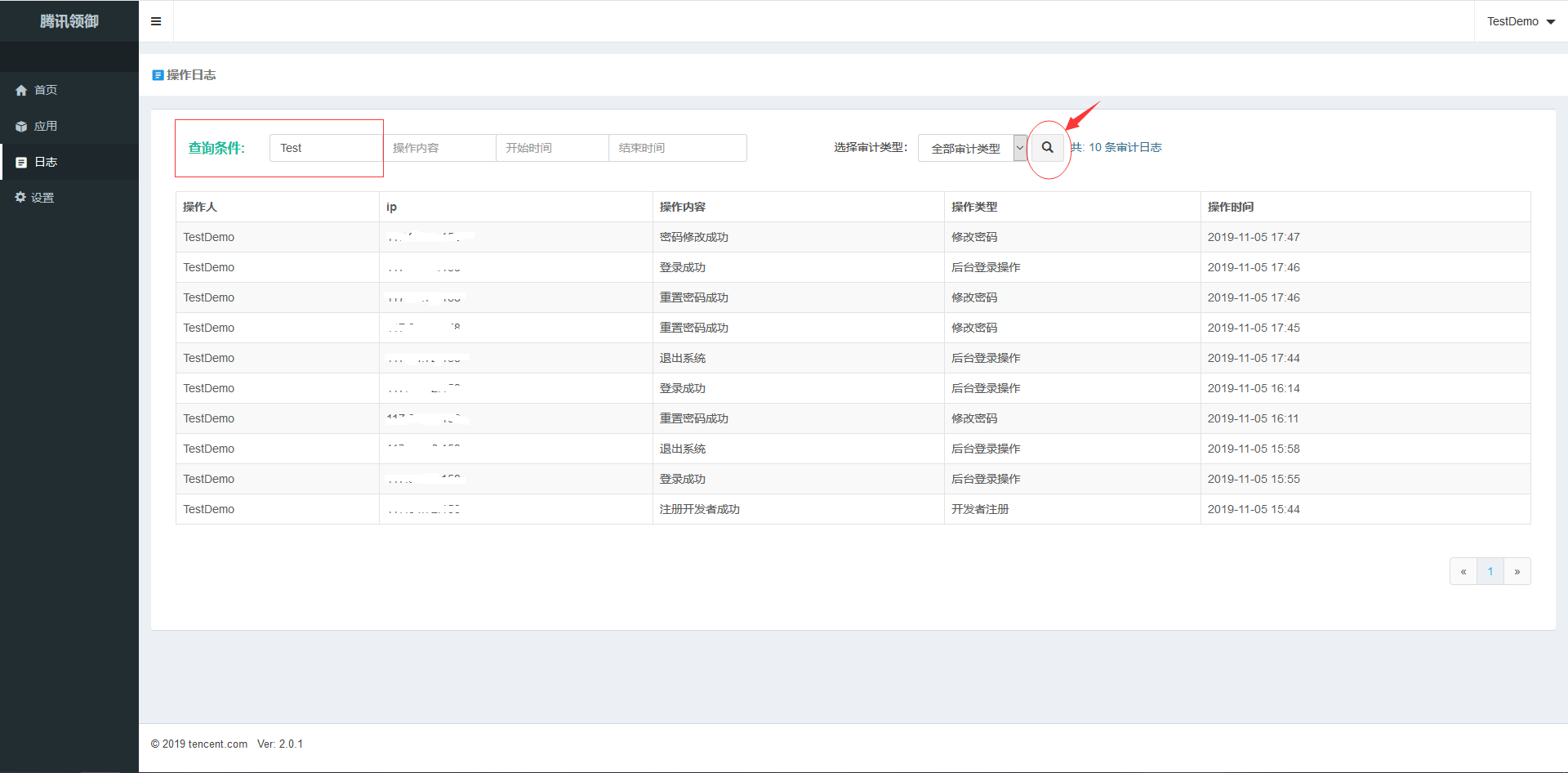
## 查看日志

点击主界面左侧列表中的日志，进行日志查看。该界面中展示了操作人（开发者）、操作地IP、操作内容、操作类型、操作时间以及日志信息的计数。

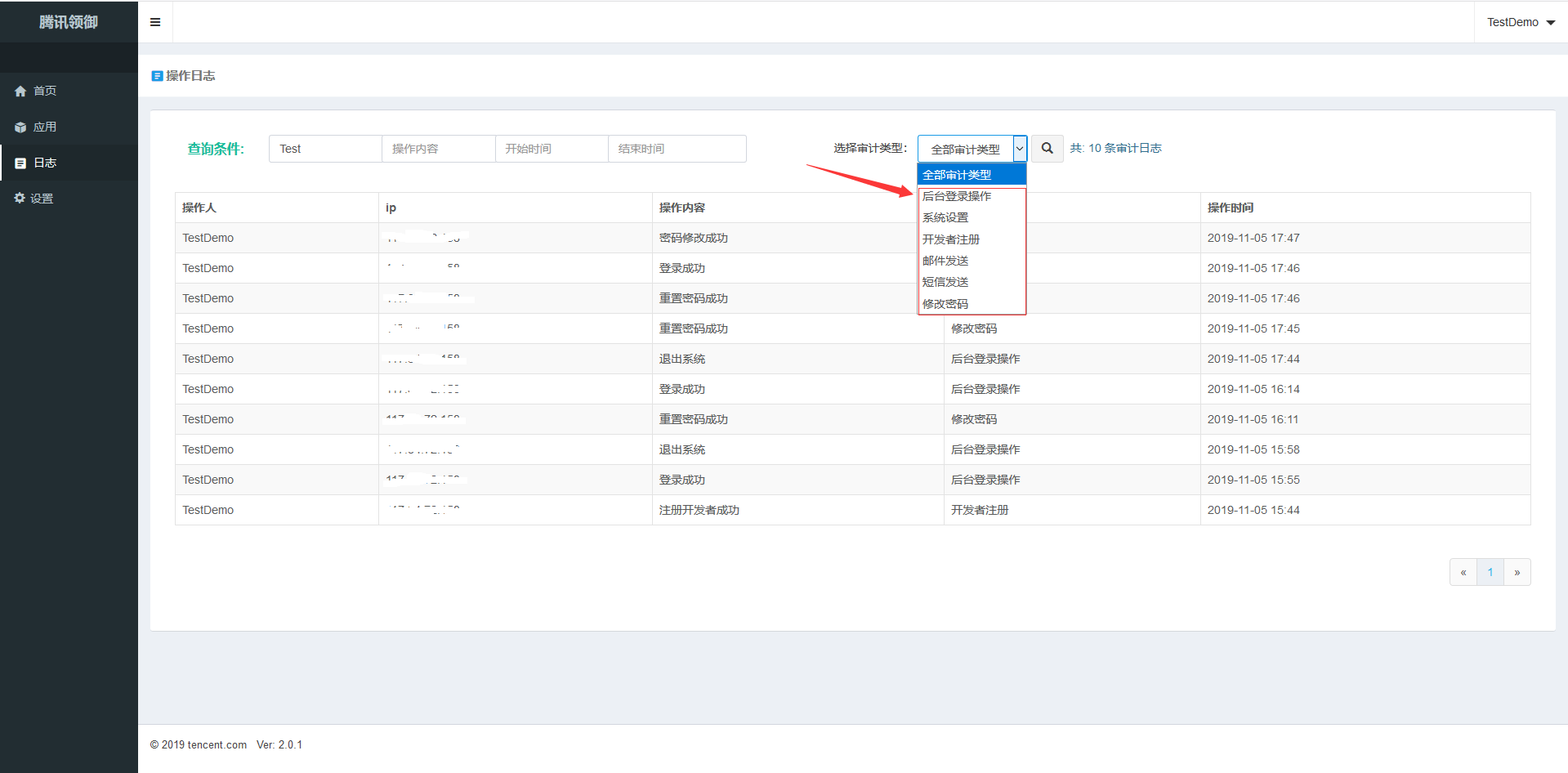


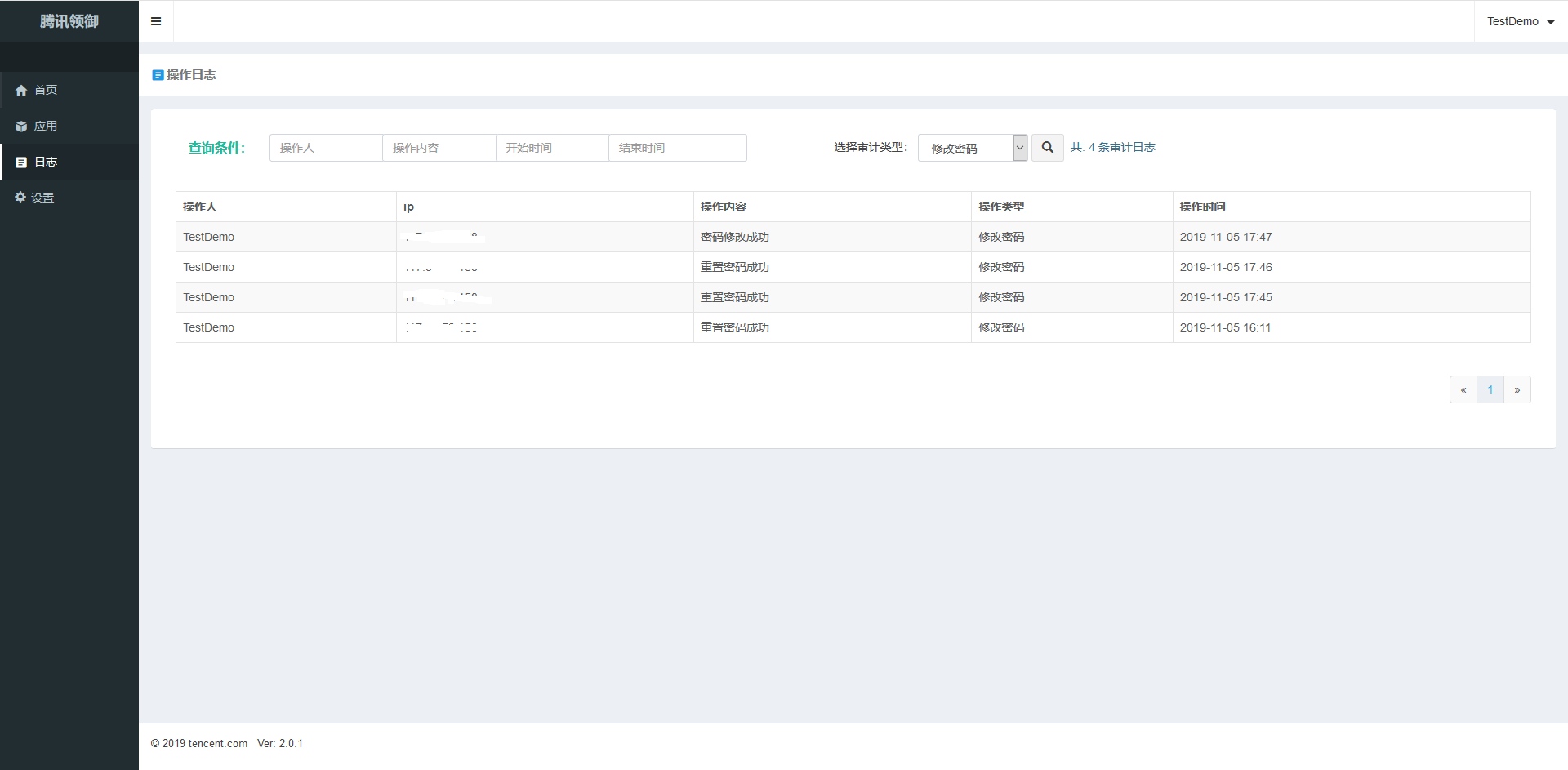
## 检索日志

为了更加方便的查找日志信息，日志模块中的检索功能提供了根据操作人、操作内容模糊检索，根据开始时间、结束时间、审计类型检索。输入查询条件后，点击右侧的“检索”按钮进行检索并根据查询条件展示所有的日志。



其中审计类型包括了后台登录操作类型（指登录成功、失败、二次认证、账户锁定、账户禁用等）、系统设置类型（指在设置模块中的动态令牌与硬件令牌的日志信息）、开发者注册类型（开发者注册的相关日志信息）、邮件发送类型、短信发送类型（手机短信认证的日志信息）、修改密码类型（修改密码的所有日志信息）。点击搜索按钮，展示该类型的所有日志信息。





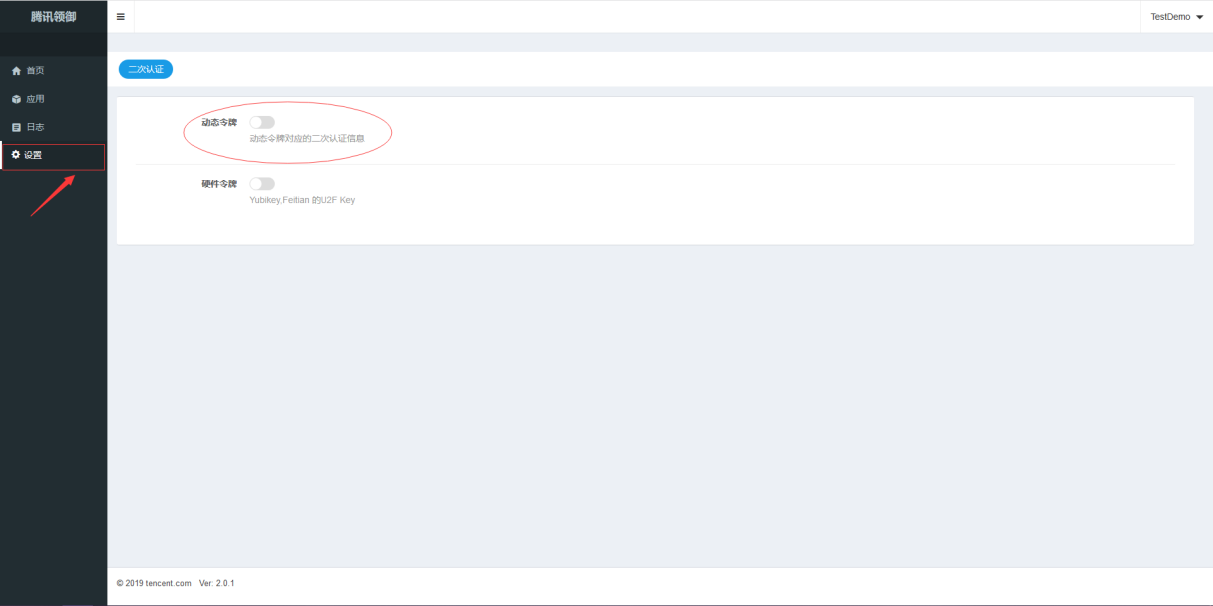
# 设置模块

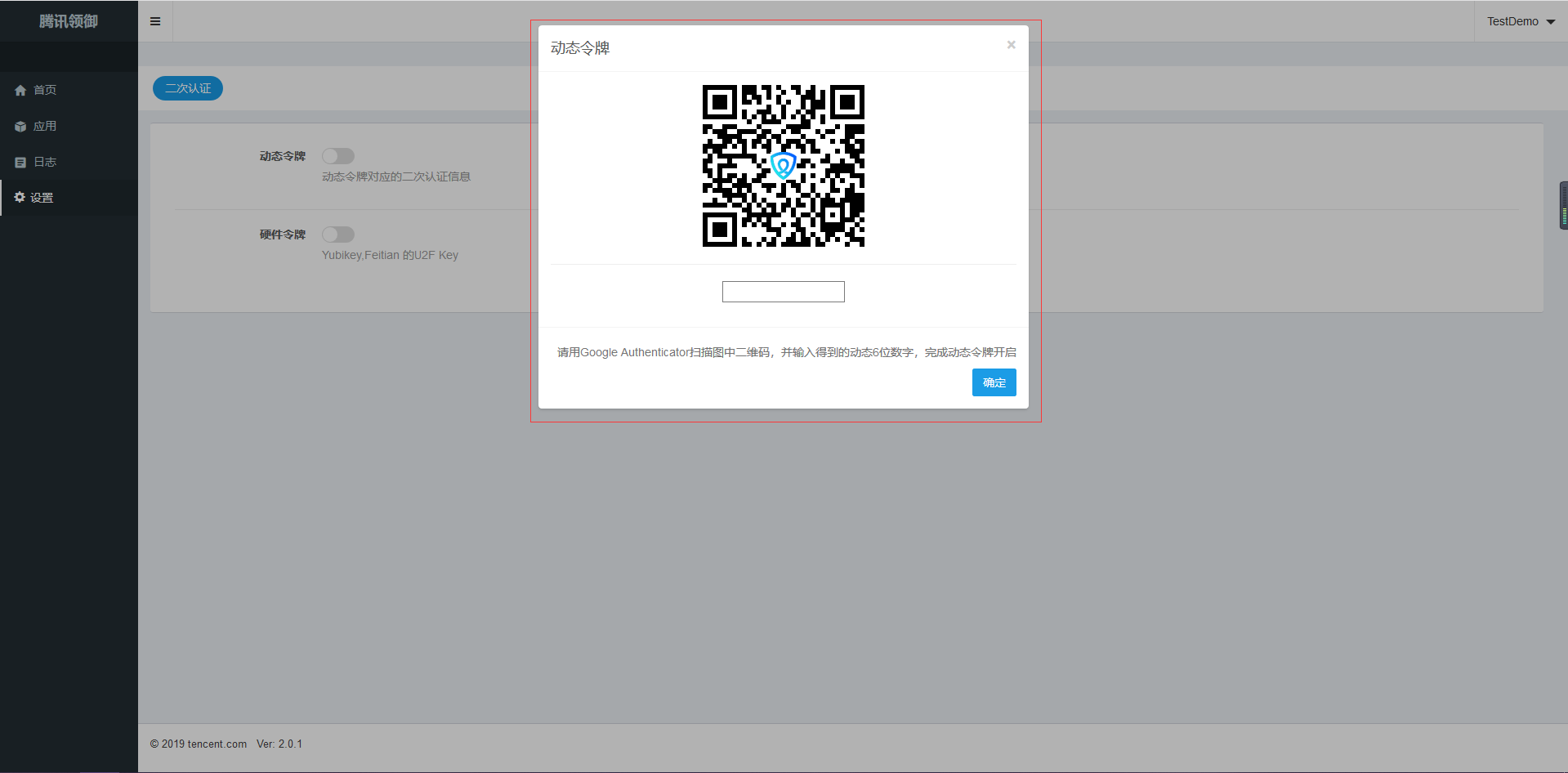
该模块为该账户二次认证服务，包括了动态令牌设置和硬件令牌设置，硬件令牌设置需要硬件设备。

## 动态令牌设置

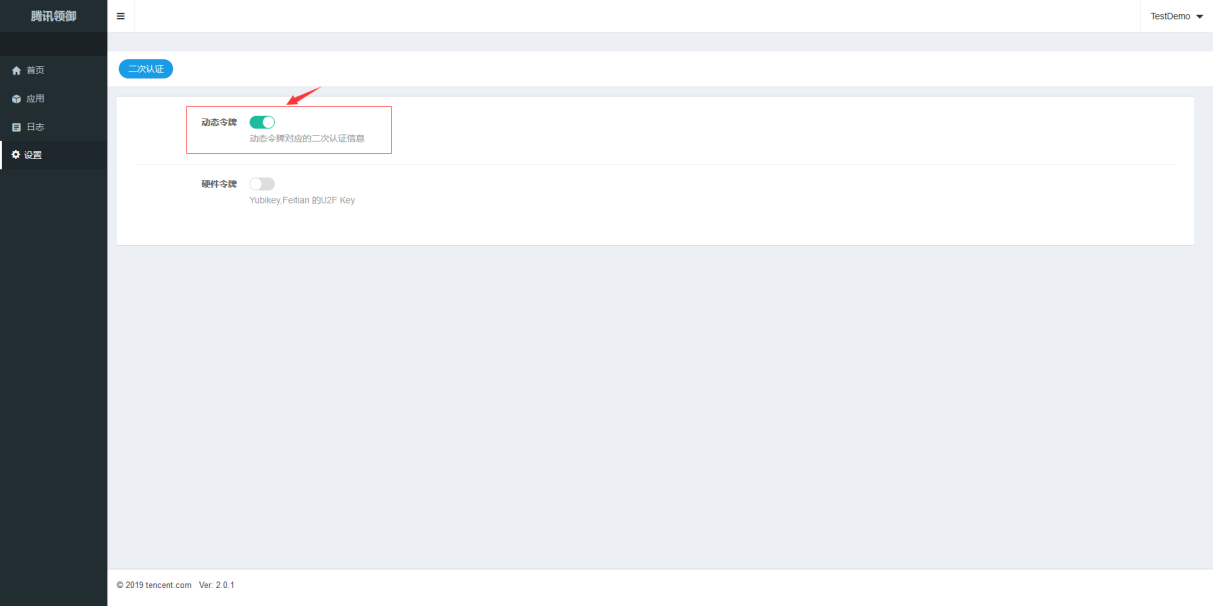
### web端动态令牌设置

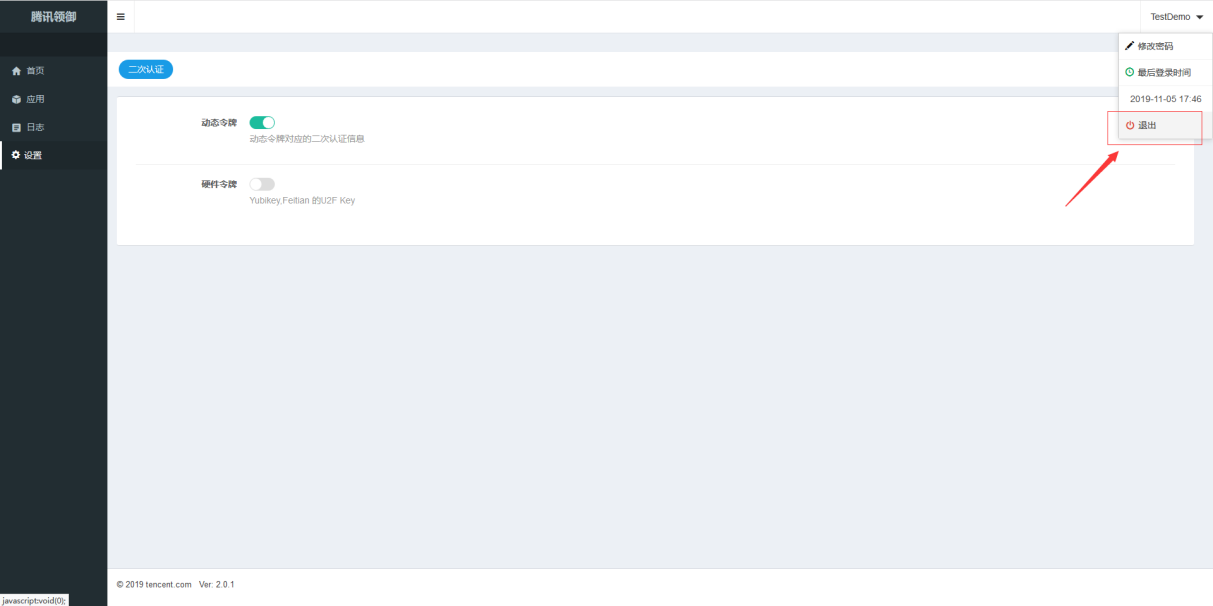
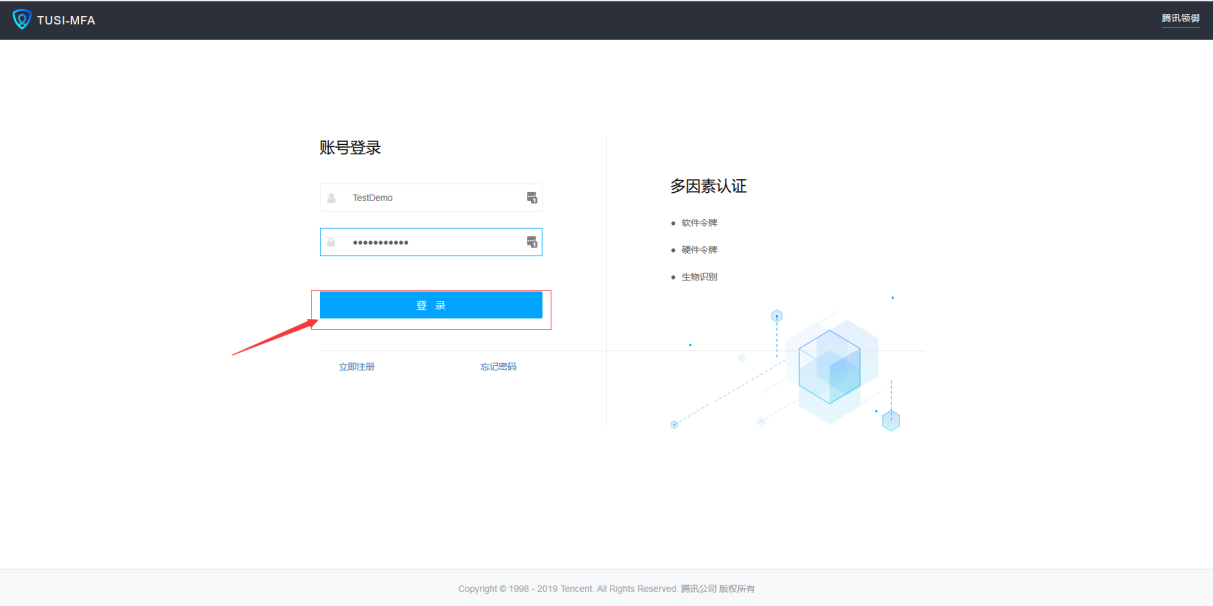
点击设置，进入到二次认证设置界面，如下图。

点击动态令牌会展示一个二维码，在移动端用Google Authenticator或者是Microsoft Authenticator扫描该二维码，扫码后会得到动态刷新的6位数一次性令牌。



在界面中的输入框中输入移动端获得的6位数动态数字，点击确认，查看web界面。

动态令牌开启后，需要重新登录，验证此操作是否有效。输入正确的用户名与密码，点击登录后会进入到多因素认证的界面，输入移动端得到的动态令牌，验证通过后进入首页。



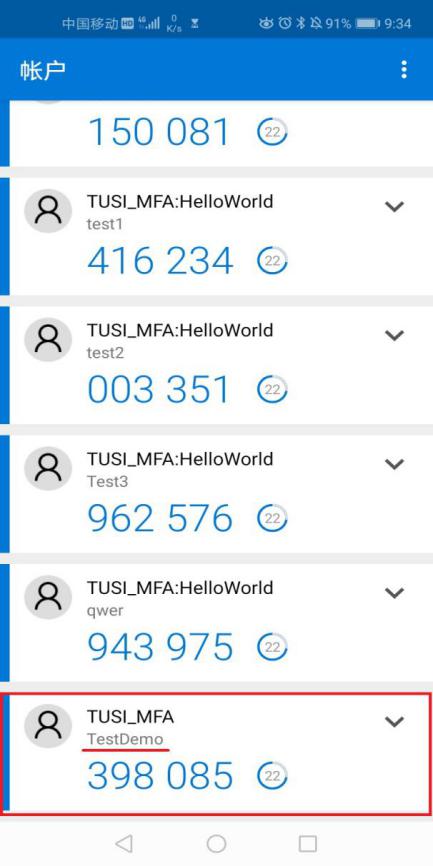


### 移动端动态令牌获取

首先移动端可以网上自行下载Microsoft Authenticator,或者进入微软官网查看帮助文档进行下载安装。

https://docs.microsoft.com/zh-cn/azure/active-directory/user-help/user-help-auth-app-download-install

安装完成后进入应用，点击添加账户，选择工作或学校账户，接着进行扫码操作。具体操作可以看下图。

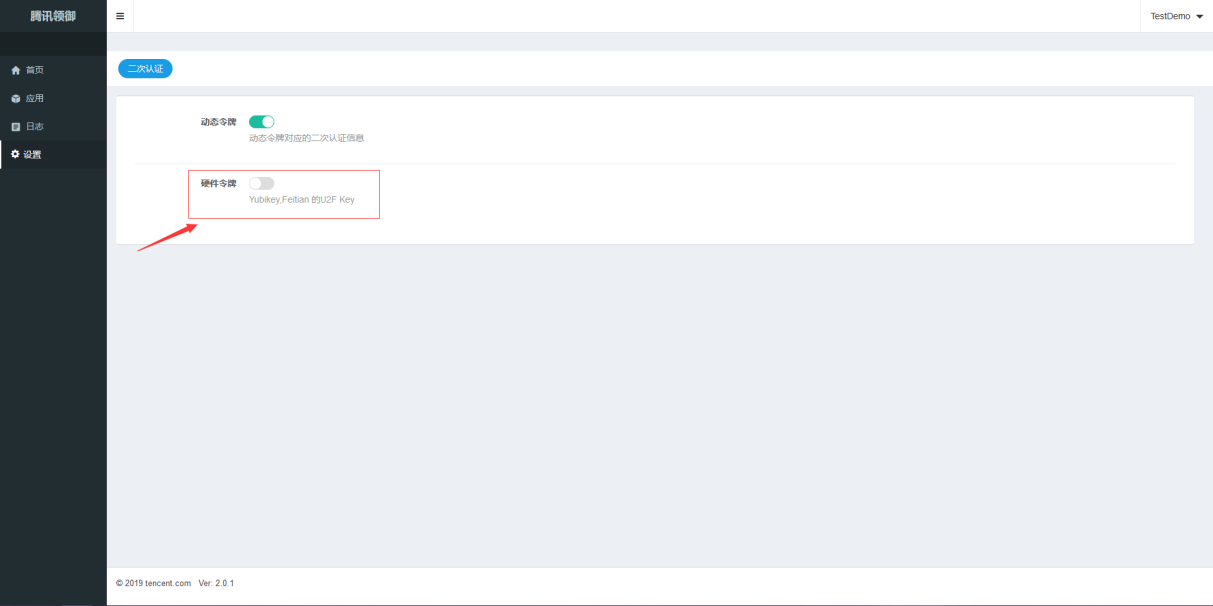
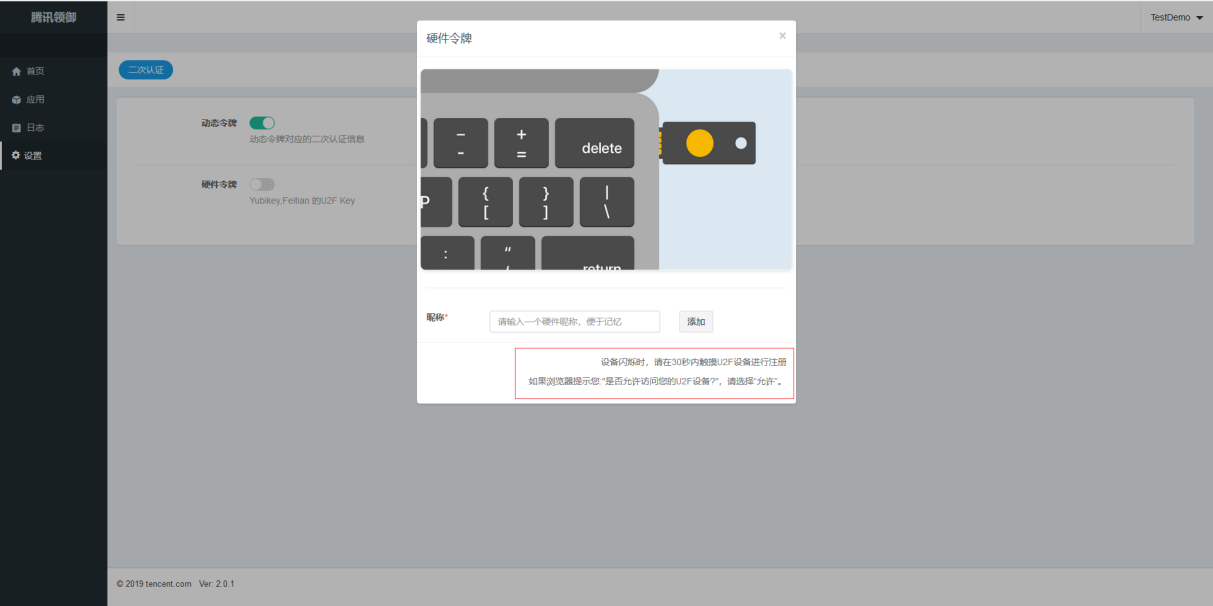


## 硬件令牌设置

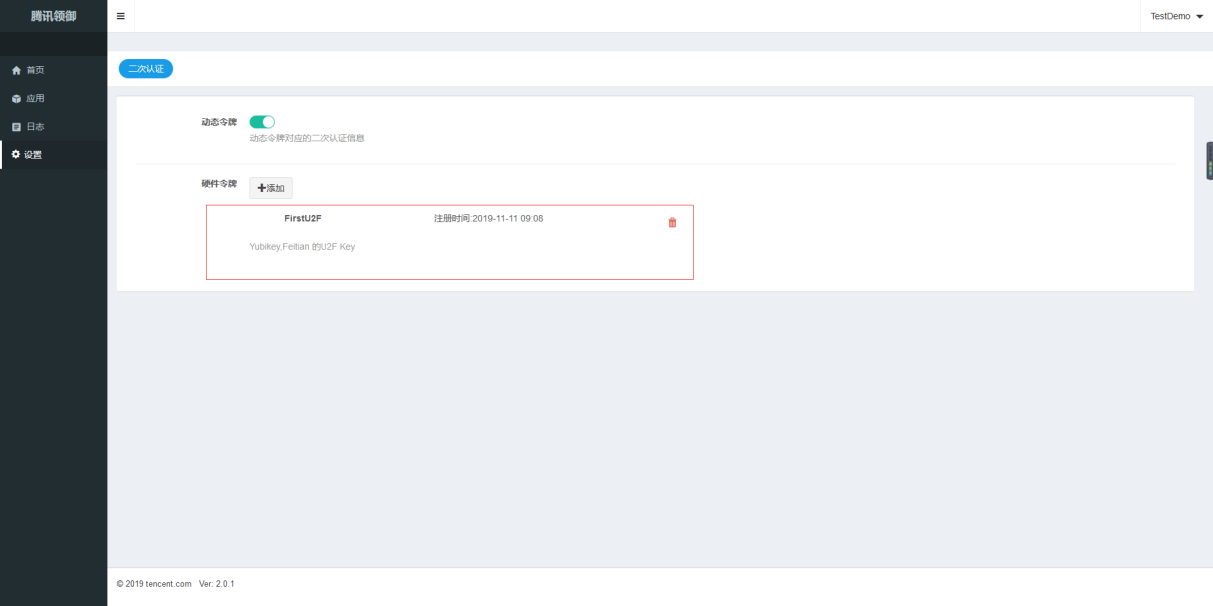
在有硬件令牌的基础上使用该功能。使用硬件令牌进行二次认证省去了动态令牌二次认证的输入过程，使二次认证更加方便快捷。

首先要注意的是该硬件令牌使用的是USB接口，如果使用的电脑无USB接口需要使用USB接口转换器，USB接口转换器提供USB接口后方可正常使用。该硬件令牌使用的是指纹识别技术，所以务必保证添加开启硬件令牌时添加硬件令牌的操作中使用的指纹和登录时用的是同一个指纹。

硬件条件满足后，具体的步骤如下：首先将硬件令牌插入USB接口中，让电脑检测到该设备，然后进入到设置界面点击硬件令牌，进入到硬件令牌的绑定界面后，先输入昵称，再点添加，此时可以注意到硬件令牌的绿灯在闪烁，请30秒内用手指触碰闪烁的部分完成硬件令牌的添加。如果浏览器提示“是否允许访问您的U2F设备？”，请选择“允许”。操作如下图：



添加完成后会展示下图界面，显示硬件令牌昵称和注册时间。



硬件令牌添加完成后，校验此次操作是否有效。首先退出到登录界面，正确输入用户名和密码，点击登录。然后会进入到二次认证界面，点击硬件令牌下的开始按钮，进入到硬件令牌认证界面，根据提示，用添加硬件令牌时的触碰硬件令牌时的手指触碰该硬件令牌就会成功登录。



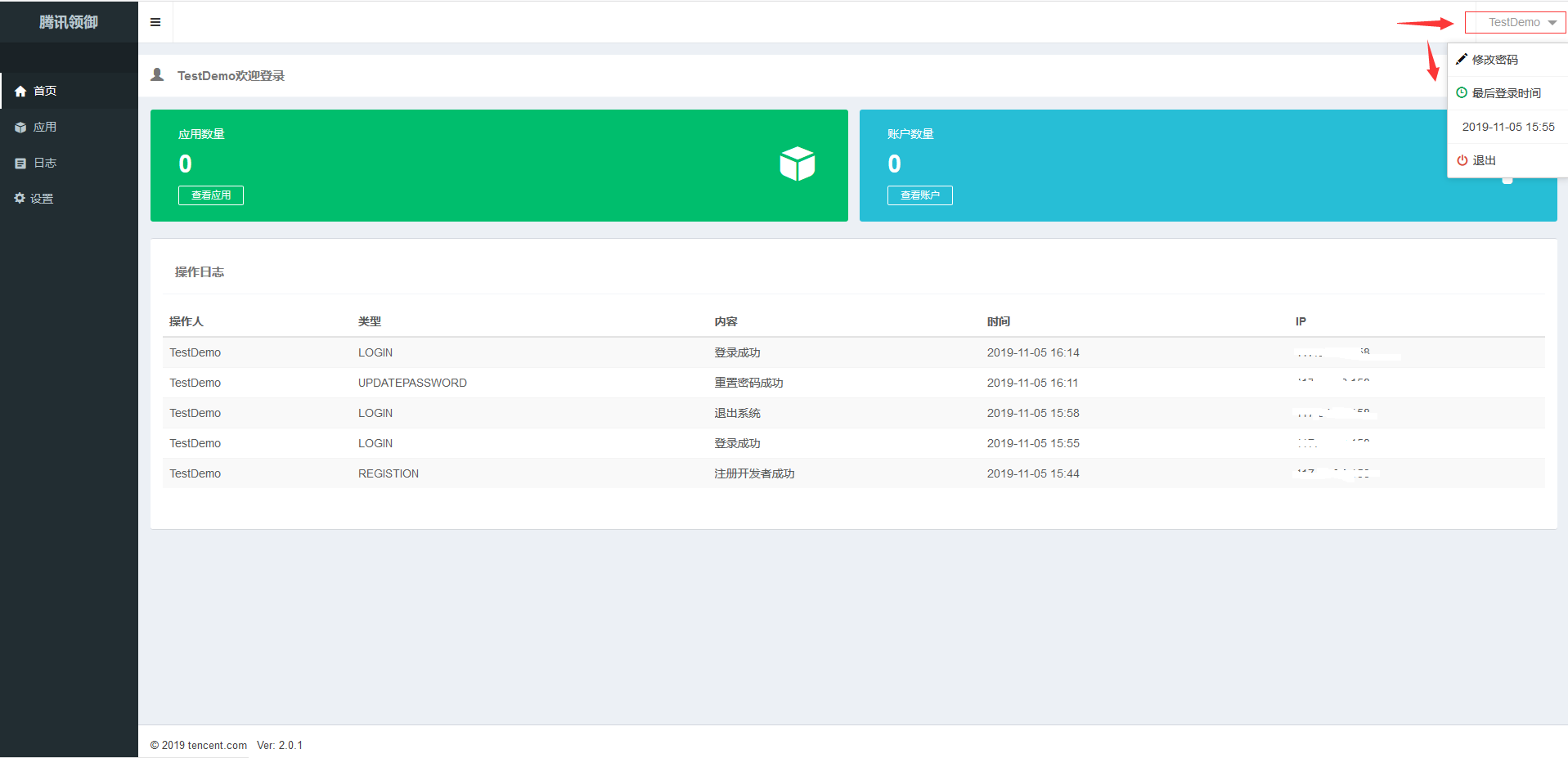
若30秒内未触摸U2F设备进行认证就会出现下图界面。按上图重新操作。



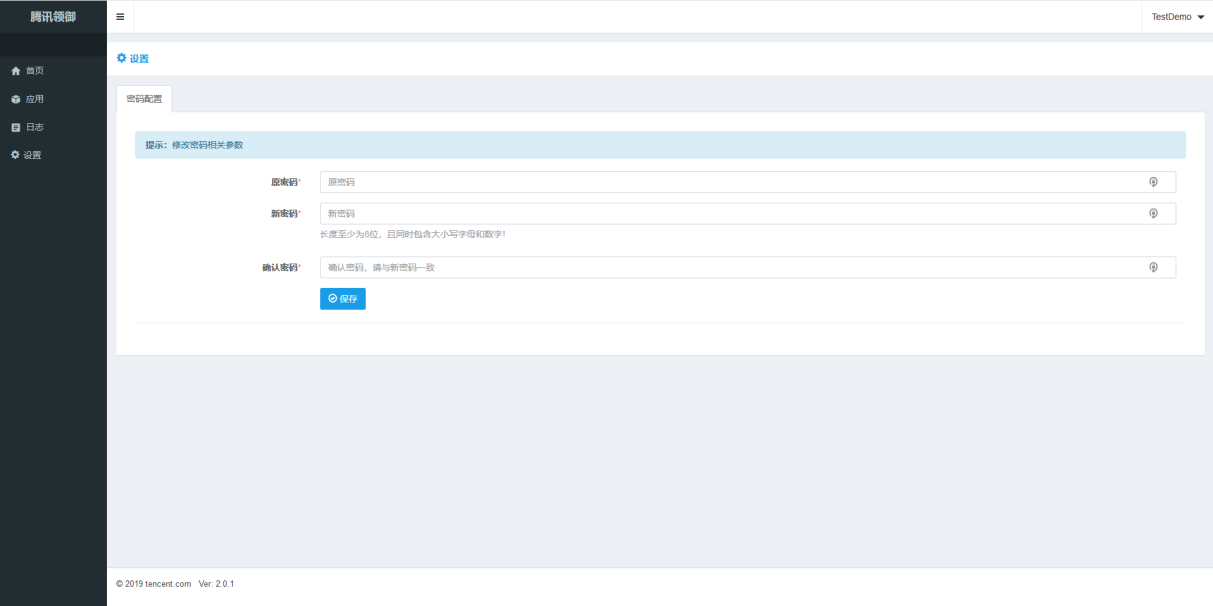
# 账户模块

## 修改密码

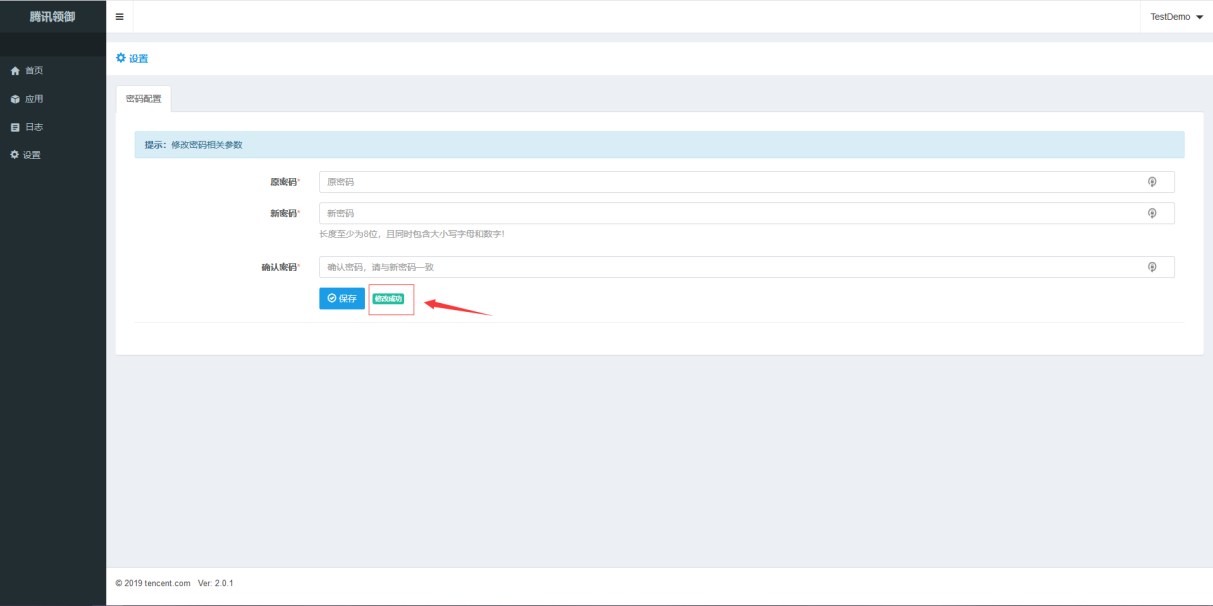
在首页中鼠标放在右上角的账户名称上，展示的是账户模块。在账户模块中，开发者登录后可以进行修改密码、查看上一次登录时间以及退出登录。



以防开发者未开启二次认证的情况下密码别盗等情况，可以在账户模块的修改密码功能下修改密码。修改密码界面如下：

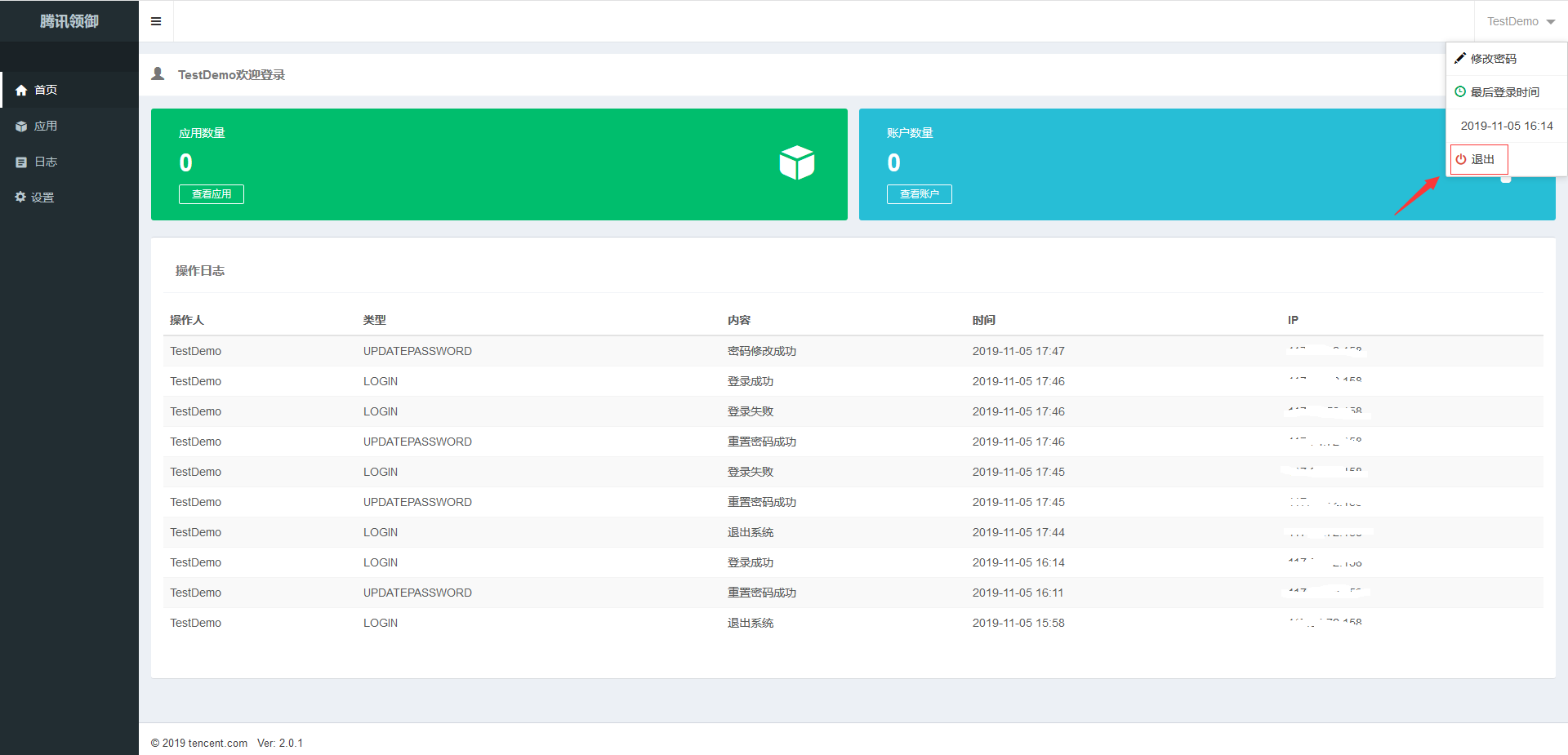


密码修改后，查看提示。



## 退出登录

点击退出按钮后，退出该账户。



未完待续......