前后端不分离的状态下我们可以用cookie,session来用于保存用户的登录状态

但在前后端分离的状态下，由于http协议是无状态的，所以当我们通过账号密码的验证后下次请求服务器不知道用户是否处于登录状态，是哪个用户处于登录状态。

我之前的做法是用户登录成功后服务器返回userid,前端把userid存在本地的seesionStorage,以后的接口请求就携带上userid来判断用户的身份，这样做的不好在于后端没有做登录状态的保存也就是说后端的开放接口是无状态的，现在存在这样一个问题，不通过前端访问后端接口而是使用postman这样的接口测试工具，由于后端没有做登录状态认证所以只要知道接口地址和携带的参数就可以轻易的伪造前端数据，所以后端也要做登录状态验证。

具体有这样的做法

问题二：如何验证token的合法性

本地的sessionStorage是什么安全吗

## php前后端项目做登录状态验证

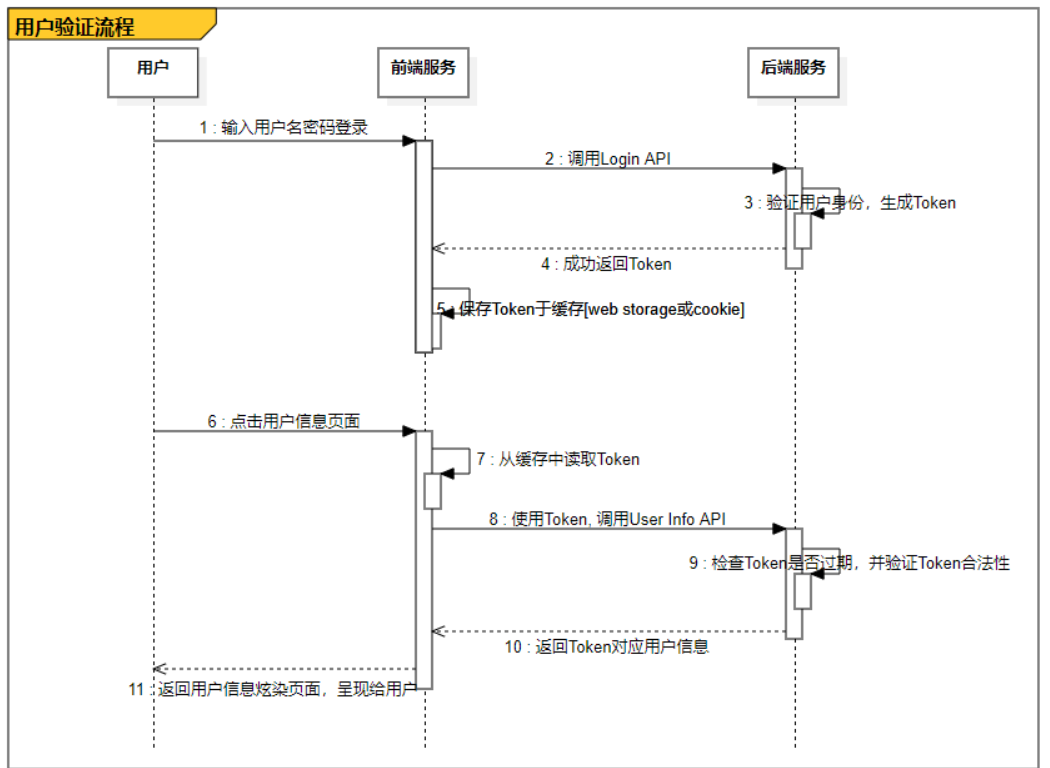
### 使用token纪录用户身份

整体流程

前端访问登录接口，后端验证成功后生成token存在数据库或者redis

后端的返回token给前端，前端保存在sessionStorage中

前端下次访问其他接口就在请求中加上token,后端验证一下token即可



这样有一个问题就是token的生成与验证的问题，因为别人可以伪造你的请求的token