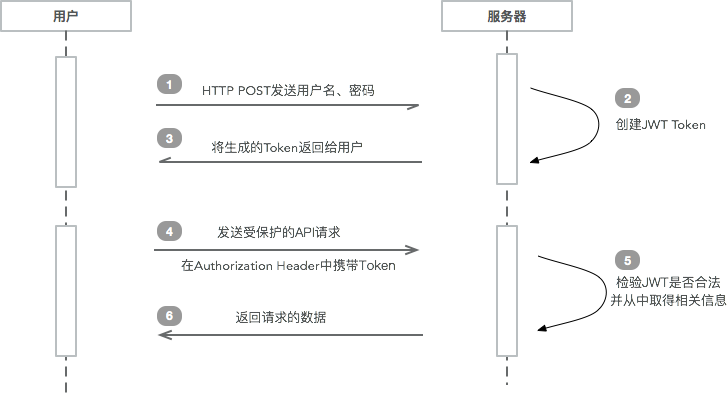
**JWT的工作流程**

下面是一个JWT的工作流程图。模拟一下实际的流程是这样的（假设受保护的API在/protected中）

1. 用户导航到登录页，输入用户名、密码，进行登录
2. 服务器验证登录鉴权，如果改用户合法，根据用户的信息和服务器的规则生成JWT Token
3. 服务器将该token以json形式返回（不一定要json形式，这里说的是一种常见的做法）
4. 用户得到token，存在localStorage、cookie或其它数据存储形式中。
5. 以后用户请求/protected中的API时，在请求的header中加入 Authorization: Bearer xxxx(token)。此处注意token之前有一个7字符长度的 Bearer
6. 服务器端对此token进行检验，如果合法就解析其中内容，根据其拥有的权限和自己的业务逻辑给出对应的响应结果。
7. 用户取得结果



学习博客：

<https://juejin.im/post/58c29e0b1b69e6006bce02f4>

<https://blog.csdn.net/linzhiqiang0316/article/details/78358907>

<https://blog.csdn.net/lhc1105/article/details/78399955>