数据库存储

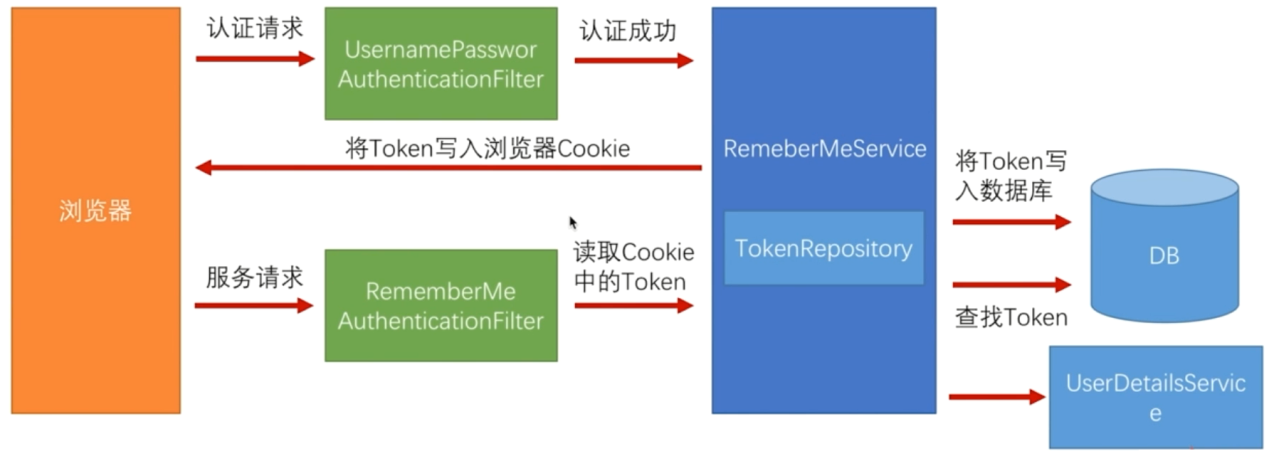
使用 Cookie 存储虽然很方便，但是大家都知道 Cookie 毕竟是保存在客户端的，而且 Cookie 的值还与用户名、密码这些敏感数据相关，虽然加密了，但是将敏感信息存在客户端，毕竟不太安全。

Spring security 还提供了另一种相对更安全的实现机制：在客户端的 Cookie 中，仅保存一个无意义的加密串（与用户名、密码等敏感数据无关），然后在数据库中保存该加密串-用户信息的对应关系，自动登录时，用 Cookie 中的加密串，到数据库中验证，如果通过，自动登录才算通过。

2.2.1 基本原理

当浏览器发起表单登录请求时，当通过 UsernamePasswordAuthenticationFilter 认证成功后，会经过 RememberMeService，在其中有个 TokenRepository，它会生成一个 token，首先将 token 写入到浏览器的 Cookie 中，然后将 token、认证成功的用户名写入到数据库中。

当浏览器下次请求时，会经过 RememberMeAuthenticationFilter，它会读取 Cookie 中的 token，交给 RememberMeService 从数据库中查询记录。如果存在记录，会读取用户名并去调用 UserDetailsService，获取用户信息，并将用户信息放入Spring Security 中，实现自动登陆。



RememberMeAuthenticationFilter 在整个过滤器链中是比较靠后的位置，也就是说在传统登录方式都无法登录的情况下才会使用自动登陆。

