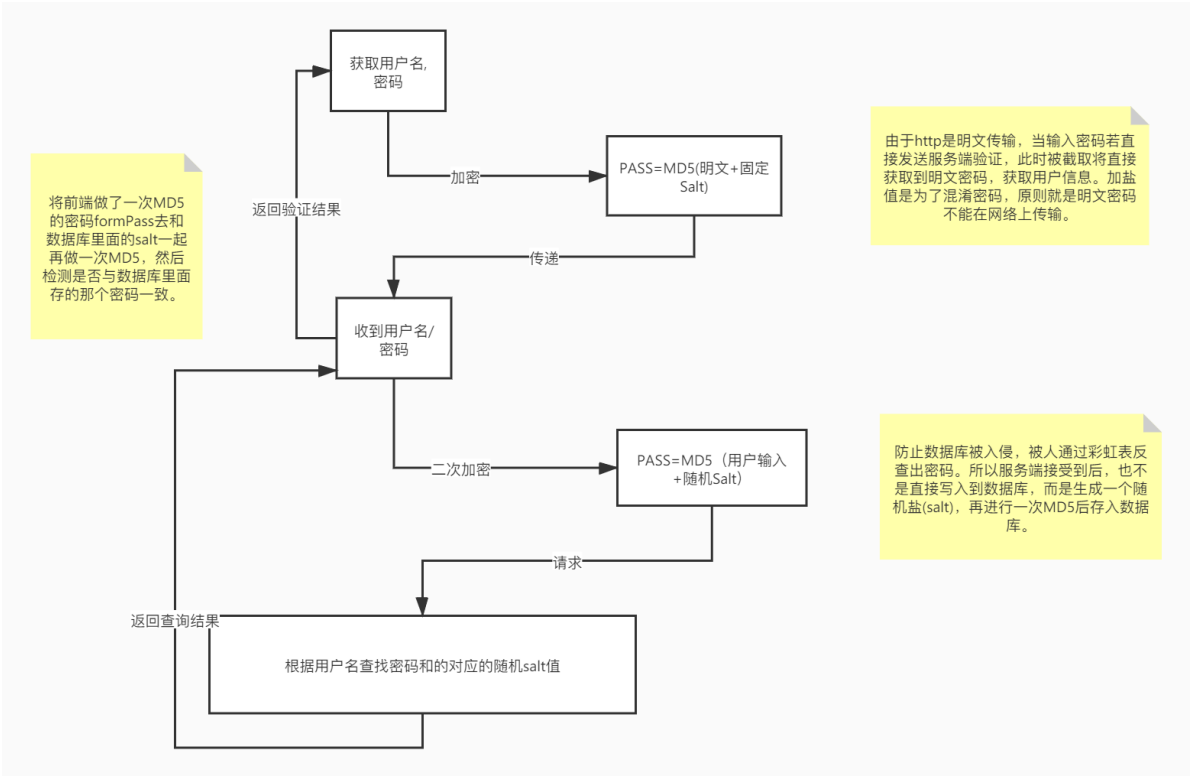

为什么做MD5？
如果不做任何处理：那么明文密码就会在网络上进行传输，假如说恶意用户取得这个数据包，那么就可以得到这个密码，所有不安全。

为什么做两次MD5？

1. 用户端：PASS=MD5(明文+固定Salt)
2. 服务端：PASS=MD5（用户输入+随机Salt）

第一次 （在前端加密，客户端）：密码加密是（明文密码+固定盐值）生成md5用于传输，目的由于http是明文传输，当输入密码若直接发送服务端验证，此时被截取将直接获取到明文密码，获取用户信息。加盐值是为了混淆密码，原则就是明文密码不能在网络上传输。
第二次：服务端接收到已经计算过依次MD5的密码后，我们并不是直接存至数据库里面，而是生成一个随机的salt，跟用户输入的密码一起拼装，再做一次MD5，然后再把最终密码存在数据库里面。
第二次的目的：
防止数据库被入侵，被人通过彩虹表反查出密码。所以服务端接受到后，也不是直接写入到数据库，而是生成一个随机盐(salt)，再进行一次MD5后存入数据库。