解：首先，以上的这种做法是没有办法抵抗重放攻击的，监听者只需将监听到的url重放一下，即可冒充你的身份登录系统。可以按照以下的方式改进：

1、进入登陆页面时，生成一个随机码，在客户端页面和session中各保存一份。

2、客户端提交登录请求时，将md5之后的密码与该随机码拼接后，再次执行md5，然后提交（提交的密码=md5(md5(密码明文)+随机码)）。

3、后端接收到登录请求后，将从数据库中查询出的密码与session中的随机码拼接后，md5运算，然后与前端传递的结果进行比较。

还可以使用以下的两种方法：

①1、系统设置一个固定的盐值，该盐值最好足够复杂。

2、用户注册、修改密码时，将用户的原始密码与我们的固定盐值拼接，然后做md5运算。

3、传递至后端，保存进数据库（数据库中保存的密码是用户的原始密码拼接固定盐值后，md5运算后的结果）。

4、登录时，将用户的原始密码与我们的固定盐值进行拼接，然后做md5运算，运算后的结果再拼接上我们的随机码，再次md5运算，然后提交。

5、后端接收到登录请求后，将从数据库中查询出的密码与session中的随机码拼接后，md5运算，然后与前端传递的结果进行比较。

②1、加登录验证码，可预防人为地暴力登录破解，为方便合法用户的正常登录，可设置密码输入错误次数达到3次后再出现验证码。

2、账户锁定，如果用户密码输入错误次数达到一定量后（如6次），则可以锁定该账号，为了方便合法用户的正常登录，可以设置成一小时后自动解锁。