# 登录重放攻击

## 前置知识

通常客户端把用户的登录请求发送到服务端进行验证，如果验证通过则登入系统。而如果登录请求被重放发送而没有控制机制的话，将导致用户通过重放攻击登入系统中。

**威胁描述：**

当正常用户的登录请求被攻击者通过某种方式获取到，即使攻击者不知道用户的账号密码，但是只要攻击者将此登录请求重新发送到服务端，那么就可以登入到系统中。

**涉及功能点：**

登录

## 修复方案

1. 用户登录时，服务端生成随机数token，并缓存此token在服务端缓存中，设置5分钟的有效期，此token发送到客户端；
2. 在用户登录请求报文中增加随机数token，登录时将此token随登录请求一起发送到服务端进行认证，检查缓存中是否存在此token来判断是否存在重放攻击。
3. 也可以在登录时增加图形验证码/短信验证验证码，由于每次登录的验证码都不同，并且验证码在验证一次后都将重置，因此可以来防御重放攻击。

参考业务流程图如下：

