# 会话标识符

## 前置知识

对于移动应用程序，为了在服务端认证用户后还能识别已被认证用户的后续访问，这就需要通过会话标识符来控制，即用户在访问服务端系统时增加会话标识符来让服务端能够识别是那个用户的访问。

**威胁描述：**

如果系统的会话标识符没有足够长度、随机性和唯一性，那么就可能导致会话标识符被攻击者破解并预测到其它合法用户的会话标识符，这将导致用户身份被欺骗的威胁。

**涉及功能点：**

登录

## 修复方案

1. 在服务端生成会话标识符和实施会话控制，在用户认证通过后，服务端使用getSession方法创建session，并在http头字段中设置sessionid值，客户端每次访问服务端的时候提供此sessionid值来保持会话。
2. 也可以使用JSON Web Token (JWT)机制来生成会话标识符，在用户认证通过后，服务端生成JWT令牌并发送給客户端，客户端后续每次请求时提供此JWT令牌即可来保持会话。