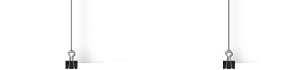
# 金融科技SDL安全设计checklist

沈发挺 [美的金融科技](https://mp.weixin.qq.com/s/javascript:void(0);)

**安全设计checklist**

SDL安全设计checklist，属于金融科技SDL安全开发生命周期系列里面很重要的一个篇章。金融科技的产品线广，业务复杂，既有2B的业务，也有2C的业务，既有传统的资金业务，也有新技术广泛应用的消费金融业务、产业链金融业务，第三方支付业务。

！很多的网络安全事件告诉我们，代码层面的安全多数是由于代码业务逻辑判断不严谨、输入校验不完善、身份校验缺失、异常处理不合理、访问控制不严谨，以及配置不善等因素引起的。其实，主要是缺乏将安全设计融入到软件开发生命周期中，以及未做好严格的项目流程安全控制。



正是因为我们的业务涉及资金，正是因为我们的业务涉及客户数据，正是因为我们的业务涉及合规，正是因为我们的业务广泛运用新技术，所以，迫切需要一个安全设计最佳实践来指导软件项目的安全落地，SDL安全设计checklist应运而生了。

**1 前言**

   2017年12月5日，金融科技SDL安全设计Checklist正式对外发布，版本为1.0。将采用持续迭代开发的方式发布SDL安全设计CheckList。

   金融科技SDL安全设计checklist是一本关于开发人员、运维人员针对软件项目安全设计、安全编码、安全运维的行动指南。行动指南将贯穿软件开发生命周期各个阶段，包含需求、设计、编码实现、测试和上线发布各阶段，针对编码设计中的输入验证、输出编码、身份认证、异常处理、会话管理、访问控制、权限控制、敏感信息、运行环境、以及常见web安全防护等内容做了详细的安全设计约束。

   SDL安全设计checklist将是安全设计的最佳实践，愿伴随开发、运维人员一起做好安全设计和安全实现！确保安全是金融科技发展的生命线！

——中国互联网金融协会会长李东荣

**2 SDL安全设计checklist目的**

1安全设计和安全编码

指导开发人员安全设计和安全编码实现，提高安全质量

2安全测试

指导测试人员安全测试：提供测试案例参照与测试结果校验

3**安全配置**

指导运维人员安全配置：面向操作系统、中间件、数据库等进行安全配置

**3 SDL安全设计checklist的意义**

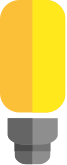
**在软件开发生命周期各个阶段，均执行相应阶段的安全控制任务，不将安全隐患带入下一阶段，以减少后期不可预见的安全问题和安全事件。**

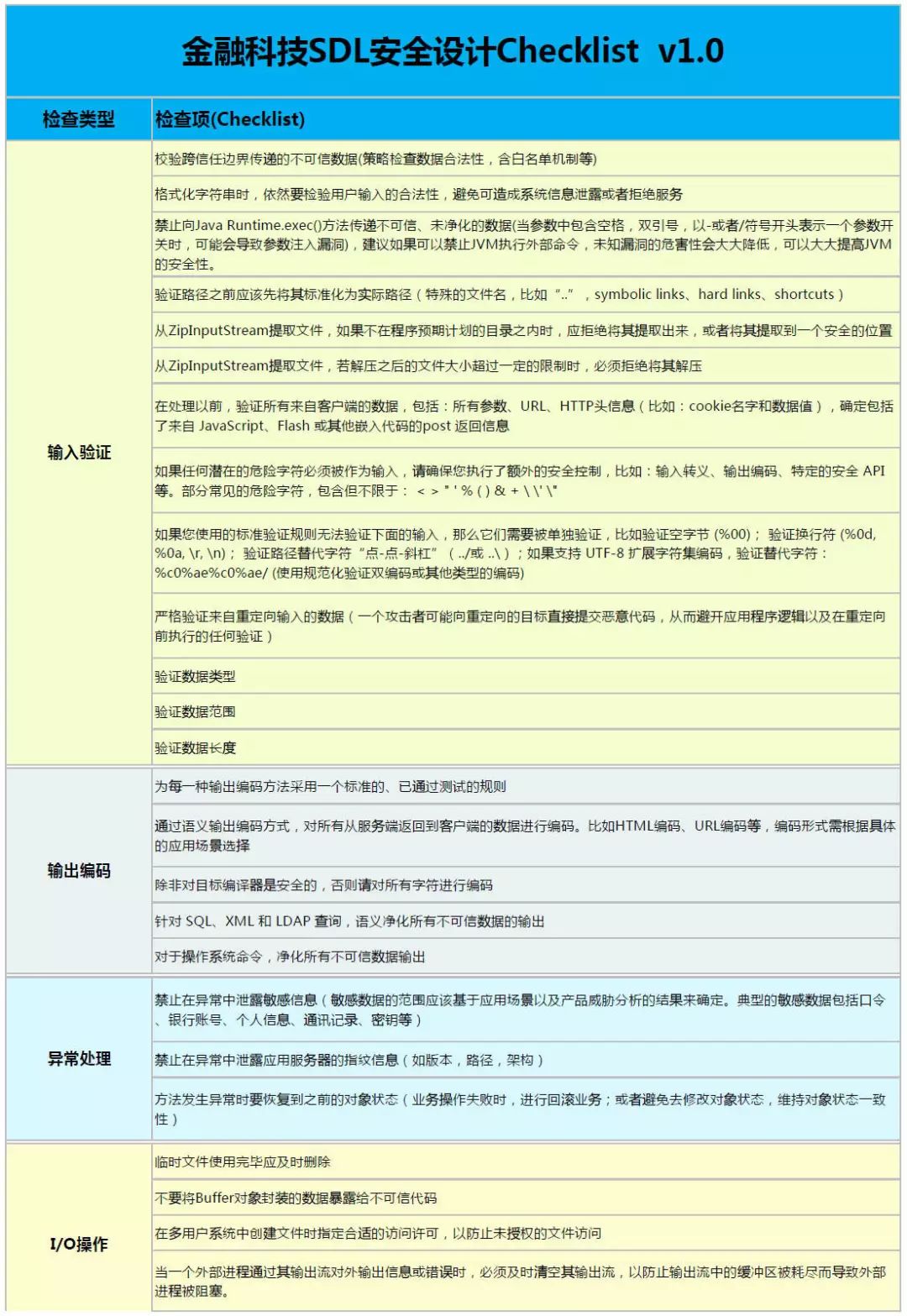
**在软件开发期间的安全建设成本远远小于后期的安全维护成本！**

**4 SDL安全设计checklist的内容**



内容涵盖输入验证、输出编码、身份认证、异常处理、会话管理、访问控制、接口调用、权限控制、敏感信息、运行环境、以及常见web安全防护等。

**内容有些多，请耐心阅读完哦，很重要滴~**











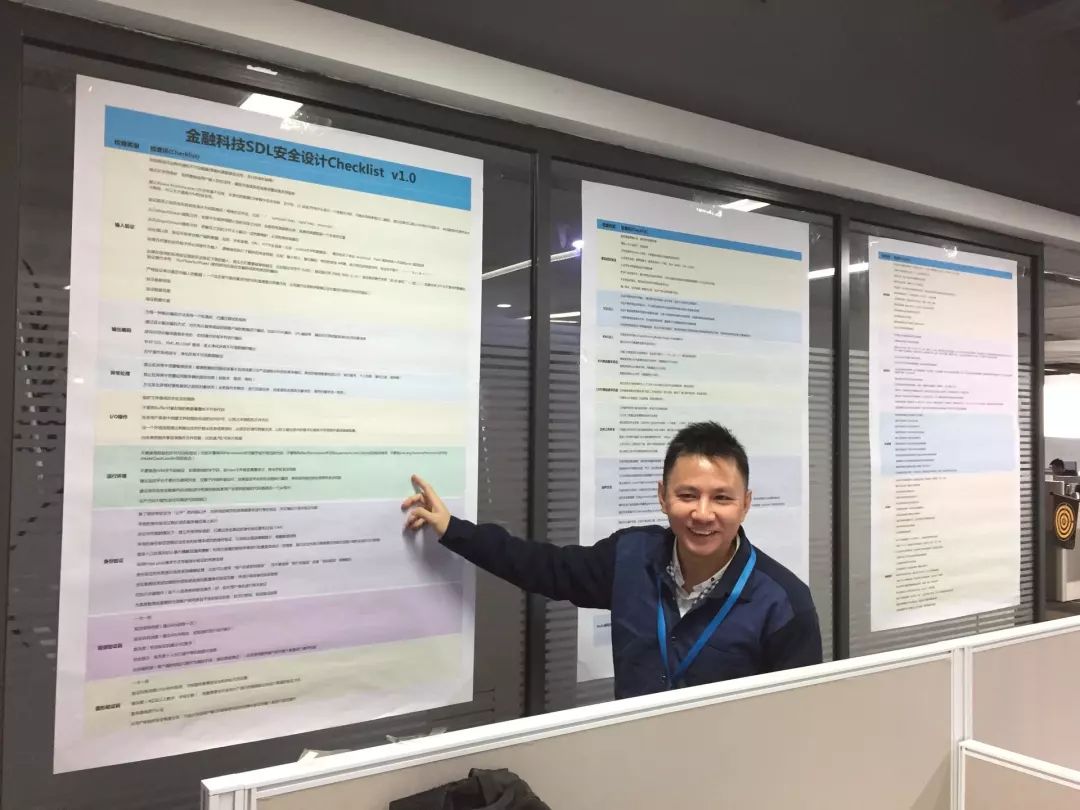
**5 SDL安全设计checklist推广学习方式**

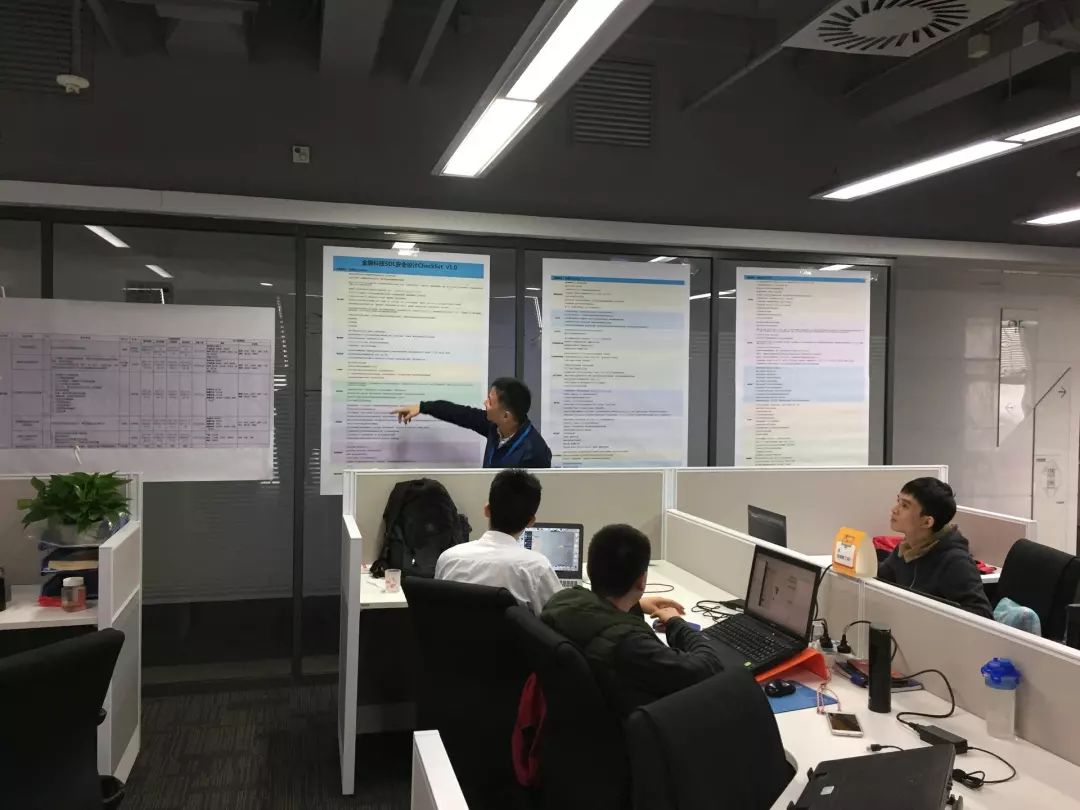
目前，采用线上和线下方式推广学习，线上采用邮件、工作微信群，以及美课方式进行推广。

 通过访问美课平台mk.midea.com，模糊搜索"SDL"或"安全设计"关键字即可搜索到SDL安全设计checklist。



线下，采用印刷粘贴和宣讲方式推广，目前已在金融科技各楼层开发区域粘贴宣传，并推广学习。

热情的黎老师正微笑地给大家解读首次发布的SDL安全设计Checklist，技术同事们好认真地在学习~哈^\_^



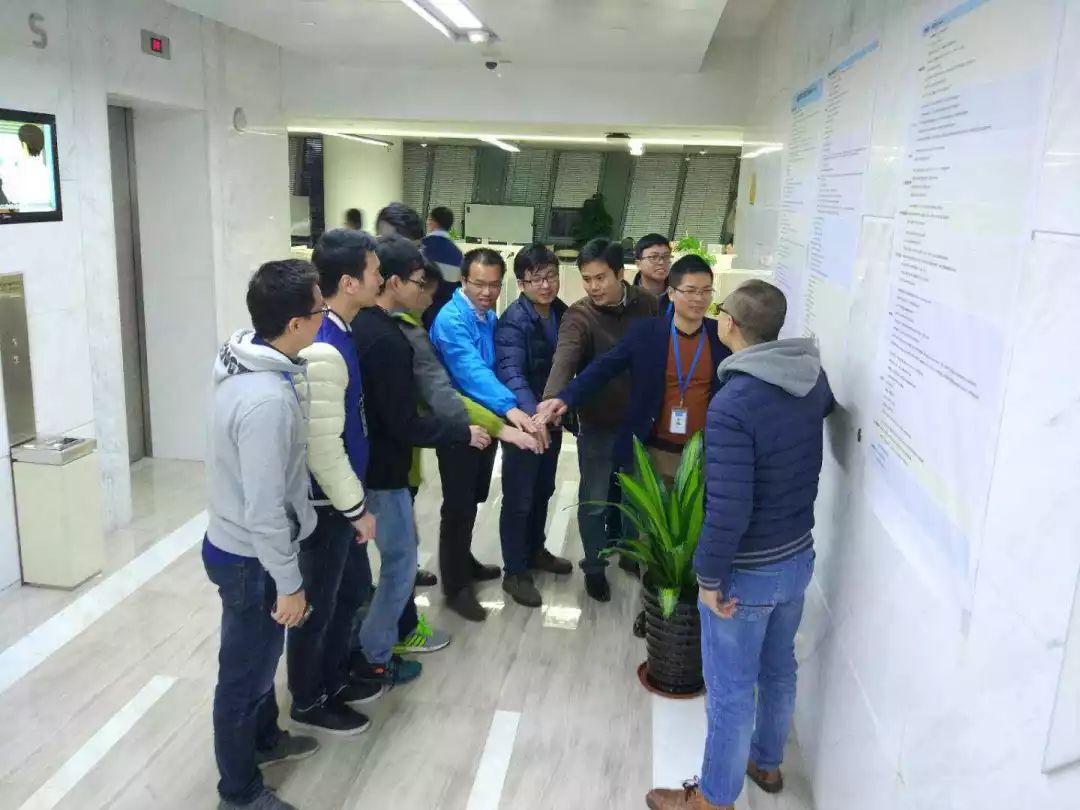
SDL安全设计checklist在全球资金推广也得到了大家热情地支持。微笑，是最坚定的支持！

幽默风趣的王老师利用午饭时间热情地为大家解读SDL安全设计checklist，赢得资金技术大咖们阵阵掌声。



还有很多很多线下推广SDL安全设计checklist学习的场景靓图，基于篇幅就不一一展示了。深深地感受到大家对安全的高度重视和支持！

安全开发不仅能体现个人能力，还能带来涨工资的可能哈^\_^

安全建设一直在路上，让我们一起，携手共同守护金融安全！

原文链接：https://mp.weixin.qq.com/s/MR3SmOLj834LK4RBMcZ2pg