CISAW 认证培训

安全软件开发课程

学员手册

（v1.0）

2011 年 11 月

一、 培训课程目标

本课程参照安全开发最佳实践设计安排，在顺利完成本课程的培训后，学员应能达到以下目标：

1. 了解众多安全开发所涉及的标准和实践，吸收安全编码的经验和积累；
2. 强化对安全开发生命周期管理的理论，形成安全开发管理的框架体系；
3. 针对开发和测试环节进行强化，提升学员在安全开发和测试环节的实际技能。

二、 目标学员

开发人员、测试人员、开发项目管理人员。

三、 课程简介

内容概要：

安全开发相关标准与实践在软件安全生命周期管理中的运用经验分享；
运用开发手段对主流安全威胁进行防范；
安全开发环节的安全流程与安全实践；
安全测试环节的关键原则与安全测试实践。

课程主旨：

以安全编码相关的标准为基础，从实用和借鉴的角度阐述安全开发的实践和经验。

课程特色：

从实践的角度展开，着重于经验分享与实践技能提升；
课程融合并扩展诸多标准与实践，贯穿安全开发的整个生命周期管理；
从互联网主流威胁追溯至安全开发过程的防范措施，形成安全开发的全方位视角。

四、 培训课程安排：

培训课程分为 10 个部分：

1.职业素质讨论
2.安全开发生命周期
3.开发安全合规
4.安全漏洞剖析
5.安全设计规范
6.安全测试实践
7.深入安全开发的核心-密码模块的安全实践
8.源代码检查实验
9.项目管理
10.考试

培训课程共 5 天，每天安排 7 小时授课和讨论，具体安排详见附件一：《安全软件开发课程大纲》。

五、 培训资料

每名参见培训的学员将会获得如下资料：

1. 学员手册及练习册
2. 培训教程

六、 授课方式

本课程的讲师来自 ISCCC 和 atsec 中国。课程以讲述为主，讨论会与测试为辅。授课语言为中文。

七、 学员评价

完成全部课程的学员可以参加最终书面考试。发放的证书包括：

- 完成培训，经考试合格并通过注册审查的学员由 ISCCC 颁发“安全软件”等级证书。
- 所有成功参加课程的学员均颁发“安全软件”培训证书，该证书由 ISCCC 和 atsec 中国统一颁发。

八、 对学员的纪律要求

学员在参见培训课程整个过程中需要遵守以下规定：

1. 学员应按时出勤、签到。
2. 学员应遵守课程纪律，保持安静，有问题请举手示意。课堂上不允许使用移动电话、录音、照相等干扰教师授课的电子设备。
3. 学员应遵守教学的组织和管理。
4. 参见书面考试的学员应遵守考试纪律，独立完成试卷内容，准时交卷，交卷后及时离开考场。对违反考试纪律的学员，书面考试将不予通过。

九、 学员的反馈意见

学员对培训课程和讲师有任何意见，可通过填写附件二：《安全软件开发培训反馈》进行反馈。

附件一：

安全软件开发课程大纲		（共计 5 天）
天	**内容标题**	**时间**
第一天（上午）	职业素养讨论	9：00-12：00
自我介绍	姓名，教育经历，工作经历，软件开发相关经历，学习目的，素质要求理解，最难忘，最喜欢（事、颜色），最讨厌，最好的和最难合作的客户事例，最难的技术问题，最得意的工作成果等	
老师点评	就关键问题进行点评，特别是在软件开发过程中需要注意的问题需要讨论清楚。	
第一天（下午）	安全开发生命周期管理	1：30-4：30
安全开发的业界标准与实践	从最佳实践的角度，引入软件安全开发相关的标准与实践，精确定位各个标准实践对软件安全开发的借鉴意义。	
安全开发生命周期	从生命周期的角度，分析软件开发各个阶段的安全要求与关键控制点。	
第二天（上午）	开发安全合规	9：00-12：00
物理与逻辑环境合规建设	从合规的角度，展开安全开发环境建设所涉及的主要安全标准规范，分享合规建设的实践。	
安全开发的角色分配与流程控制	讲解安全开发与测试环境角色分工的最佳实践，分享通用开发流程控制实践。	
第二天（下午）	安全漏洞剖析	1：30-4：30
重大安全漏洞深入分析	基于最主流的安全漏洞（如 OWASP、CWE 等）展开，从漏洞本身着手，导出软件开发与测试过程中的控制点缺失，导出开发过程中的关键控制要求。通用弱点评价体系（CVSS）讲解，缺陷管理的最佳实践。	
第三天（上午）	安全设计规范	9：00-12：00
安全架构	安全架构模型与安全规范。包括安全需求分析。	
安全设计	高层设计、底层设计，及其接口功能规范等。	
安全功能	讲解业界最佳实践所可能涉及的安全功能要求。	
第三天（下午）	安全编码与测试实践	1：30-4：30
安全编码	详细探讨安全编码。	
安全测试	展开安全测试的讨论，重点探讨渗透测试。	
第四天（上午）	深入安全开发的核心	9：00-12：00
密码模块的安全实践	以安全开发最具挑战的密码模块展开安全设计的控制要求。	
（转下页）		

第四天（下午）	源代码检查实验	1：30-4：30
源代码自动和人工检查	给出代码实例（含常见安全问题），要求制定具体的安全检查规范，并提升代码的安全性。	
第五天（上午）	项目管理	9：00-12：00
通用项目管理	项目管理综述，分类。	
开发管理项目的管理实例化	结合开发类管理实例进一步实例化为软件开发类项目。	
第五天（下午）	考试	1：30-4：30

附件二：

安全软件开发培训反馈

学员信息

公司名称_____

学员姓名:_____联系电话:_____ 职位:_____ 电子邮件:_____

您对本次培训活动的整体评价？

☐非常满意 ☐满意 ☐一般 ☐不满意

您对本次培训讲师的整体评价？

第一天	☐非常满意	☐满意	☐一般	☐不满意
第二天	☐非常满意	☐满意	☐一般	☐不满意
第三天	☐非常满意	☐满意	☐一般	☐不满意
第四天	☐非常满意	☐满意	☐一般	☐不满意
第五天	☐非常满意	☐满意	☐一般	☐不满意

您认为本次培训内容如何？

☐非常实用 ☐实用 ☐一般 ☐不实用

您认为可以在本次培训中受益吗？

☐受益良多 ☐比较受益 ☐一般 ☐完全没有

您希望再次组织类似的培训活动吗？

☐非常希望 ☐希望 ☐一般 ☐不希望

您认为本次培训哪些地方需要改进？

☐培训组织 ☐课程设计 ☐讲师授课方式 ☐培训时间

其 他：_____

您还关注哪些信息安全相关领域？

☐ISO/IEC 27001 ☐FIPS 140-2 ☐Common Criteria ☐NASPO标准

☐支付卡行业数据安全标准(PCI DSS) ☐联邦信息安全管理法案(FISMA)

☐风险管理 ☐隐私保护 ☐渗透测试 ☐出口管制

☐供应链安全 ☐健康保险便利及责任法案(HIPAA)

其 他：_____

信息安全项目实施过程中，您有哪些希望分享的经验？比如安全协议、OWASP Top10防范、脆弱性评估、渗透测试等等？

其他意见和建议？
