中睿·领航IT服务

软件安全设计与开发

中睿信息技术有限公司

ZHONGRUI INFO &TECHNOLOGY CO.,LTD

目录

一、课程介绍

课程描述

本课程在主动的安全开发框架指导下，深入剖析软件开发生命周期各阶段的安全细节问题，理解协同构建安全系统的方法。并通过大量的动手实操和相关案例贯穿所有的理论知识，使学员熟练掌握代码安全漏洞分析、编程规范、代码质量问题分析、安全设计与防御常见问题及解决方法。

课程收益

1. 学会分析软件安全脆弱性产生的根源；
2. 展示多种攻击软件的手段、指出软件开发过程中不同人员在设计和开发中常犯的错误；
3. 探讨当前软件安全界关注的热点问题；
4. 总结和提高软件质量和安全性的指导思想、开发策略、技术路线和实施方法；
5. 掌握代码安全典型漏洞；
6. 安全漏洞攻防演练；
7. 掌握通用代码编程规范；
8. 能够对代码进行质量问题分析；
9. 掌握项目的安全设计与防御；
10. 通过一个真实案例贯穿所有的知识点。

培训对象

1）IT 企业中的技术负责人；

2）软件架构师、系统分析师以及资深开发人员；

3）信息技术安全部门的相关人员；

4）大专院校或科研院所相关专业的教师、研究人员；

5）对信息行业安全问题感兴趣的人员。

授课说明

课程形式：课堂讲授、讲义解析、情景模拟、实战互动演练

课程时间：3 天

授课地点：中睿培训室/客户处

培训环境

机器要求：	**计算机**	**1 台**	**1 人**
软件要求：	Windows 2003 Server 及以上版本 Enterprise Architecture Axure RP Pro		
硬件要求：	CPU： 主流即可 RAM：2GB 以上		
教学环境：	局域网、白板、投影仪		

详细培训大纲

课程大纲	
时间安排：	**第一天**
课程内容：	● **攻击、利用、破坏软件的手段以及预防、防御对策** ● **以 Web 应用软件为例，分析不安全现状** ● **Web 应用的十大安全漏洞详解** ■ 非法输入 ■ 失效的访问控制 ■ 失效的帐户和线程管理 ■ 跨站点脚本攻击 ■ 缓冲溢出问题 ■ 注入式攻击 ■ 异常处理错误 ■ 不安全的存储 ■ 程序拒绝服务攻击 ■ 不安全的配置管理

- **攻击行为模式和攻击模型的建立**
  - 攻击行为模式
  - 攻击模型的建立
- **安全性在开发过程中难以实现的原因**
- **主动的安全软件开发模型(基于风险的威胁建模方法)**
  - 安全漏洞的常见类型
  - 传统安全模型的缺陷
  - 创建安全策略的原则
  - 基于风险的建模方法
- **识别、分析、评估、跟踪软件安全风险的可操作办法**
  - 应用开发过程中的安全性
  - STRIDE 威胁模型
  - 如何创建安全模型
  - 威胁及分类
  - 如何使用安全模型
- **安全的体系结构、在软件分析与设计阶段关注安全性**
  - .NET 框架安全特性
  - J2EE 框架的安全特性
  - 设计安全的体系架构
- **密码学基础理论**
- **对称密钥密码体制、非对称密钥密码体制**
  - 对称密钥体系
  - 对称密钥体系的典型使用场景
  - 对称密钥体系的优缺点
  - 非对称密钥体系
  - 非对称密钥的典型使用场景
  - 非对称密钥的优缺点
  - 组合两种密钥体系

	● **消息摘要、数字签名** ■ Hash 算法 ■ Hash 算法的实现 ● **Crypto++和 CryptoAPI 加密算法库的使用**
时间安排：	**第二天**
学习内容：	● **安全漏洞攻防演练** ■ 访问控制缺陷 ➢ 使用访问控制模型 ➢ 绕过基于路径的访问控制方案基于角色的访问控制远程管理访问 ■ Ajax 安全同源策略保护 ➢ 基于 DOM 的跨站点访问 ➢ 小实验:客户端过滤 ➢ DOM 注入 XML 注入 JSON 注入静默交易攻击 ➢ 危险指令使用 ➢ 不安全的客户端存储 ■ 认证缺陷 ➢ 密码强度 ➢ 忘记密码 ➢ 基本认证 ➢ 多级登录 1 ➢ 多级登录 2 ■ 缓冲区溢出 ➢ Off - by - One 缓冲区溢出 ■ 代码质量 ➢ 在 HTML 中找线索 ■ 并发 ➢ 线程安全问题

- 购物车并发缺陷

■ 跨站脚本攻击

- 使用 XSS 钓鱼
- 小实验：跨站脚本攻击
- 存储型 XSS 攻击
- 跨站请求伪造
- 绕过 CSRF 确认
- 绕过 CSRFToken
- HTTPOnly 测试
- 跨站跟踪攻击

■ 不当的错误处理

- 打开认证失败方案

■ 注入缺陷

- 命令注入
- 数字型 SQL 注入
- 日志欺骗
- XPATH 型注入
- 字符串型注入
- 小实验：SQL 注入
- 通过 SQL 注入修改数据
- 通过 SQL 注入添加数据
- 数据库后门
- 数字型盲注入
- 字符串型盲注入

■ 拒绝服务

- 多个登录引起的拒绝服务

■ 不安全的通信

- 不安全的登录

	■ 不安全的配置 ➢ 强制浏览 ■ 不安全的存储 ➢ 强制浏览 ■ 恶意执行 ➢ 恶意文件执行 ■ 参数篡改 ➢ 绕过 HTML 字段限制 ➢ 利用隐藏字段 ➢ 利用未检查的 E - mail ➢ 绕过客户端 JavaScript 校验 ■ 会话管理缺陷 ➢ 会话劫持 ➢ 认证 Cookie 欺骗 ➢ 会话固定 ■ Web 服务 ➢ 创建 SOAP 请求 ➢ WSDL 扫描 ➢ Web Service SAX 注入 ➢ Web Service SQL 注入
时间安排：	**第三天**
学习内容：	● **安全设计与防御** ■ 软件安全性原则 ■ 安全风险评估 ➢ 安全威胁建模及工具应用 ➢ 如何减少攻击面 ■ 安全设计评审

- 信息安全存储设计
- 密码安全管理设计
- 用户注册安全设计
- 安全架构设计评审
- Java 常用 Web 框架安全漏洞检查

■ 应用安全组件 ESAPI

■ 编写安全的代码实现安全系统的技术
- 安全技术分类
- 编写安全代码综述

■ 安全编程规范与漏洞知识库
- CWE
- OWASP

■ 数据在传输、使用和存储状态中安全性的实现
- 数据传输的形式及安全性实现
- XML Web 服务的安全性实现

■ SQL 注入攻击的纵深防御技术
- SQL 注入攻击的防御实现
- 如何书写安全的数据访问代码

■ 企业应用安全监控

■ 构建 Web 应用安全防火墙

■ 构建企业安全开发知识库

■ 持续集成框架与安全测试自动化

■ 利用威胁模型制定测试计划
- 分解应用形成组件.
- 识别组件的接受.
- 根据潜在的威胁确定接口的优先级
- 确定每个接口使用的数据结构。
- 注入变异数据发现安全问题

	■ 面向软件安全性的测试方法 ■ 利用代码审查保证代码安全 ➢ 代码审查的方式分类 ➢ 安全代码审查的重点 ■ 利用输入验证保证功能性安全 ➢ 一般输入验证实现 ➢ 使用正则表达式验证输入 ➢ 实现安全的认证与访问控制 ■ 正确应用密码技术 ■ 理解和防范缓冲区溢出攻击 ■ 安全数据通信信道和安全运行环境的实现
	总结、回顾、答疑

二、公司简介

全面的 IT 服务提供商—中睿信息

公司介绍

全面的 IT 服务提供商—中睿信息是一家专业的 IT 服务提供商，致力于解决企业信息化所遇到的最棘手问题。公司与微软（Microsoft）、甲骨文（Oracle）、思科（Cisco）、Pearson VUE 等全球著名 IT 厂商建立长期的合作伙伴关系，业务涵盖企业 IT 架构与应用服务、软件研发顾问咨询服务、数据库服务、高级 IT 技术培训、软件项目研发、解决方案实施和就业培训。

公司拥有顶尖的技术团队，掌握国际最前沿技术，采用标准化的服务体系，为客户高效、稳定的 IT 运营提供强有力支撑，提升企业核心竞争力。服务客户遍及各种行业，包括金融、通讯、制造业、政府、企事业单位。目前，中睿作为华南区实力最强的 IT 服务商，已成为客户优秀 IT 服务商的首选，并与上百家客户建立了长期、多赢的战略性合作。

中睿资质

- 微软金牌能力认证合作伙伴
- 微软优秀解决方案供应商
- VUE 考证中心
- 软件认定企业
- EXIN 认证合作伙伴
- PMI 注册教育机构
- ORACLE 认证合作伙伴
- 微软 TechNet IT-Pro 最佳合作伙伴
- HP 服务供应商
- Ultimus BPM 解决方案提供商
- DELL 服务供应商
- Arcplan 银牌解决方案提供商

业务范围

IT 培训

课程大类	*课程细类*
开发技术	移动应用开发/Microsoft .NET 平台/ Java 平台/前端开发
软件工程	开发过程/TOGAF 软件架构/软件需求/软件测试/软件设计
系统与网络	系统管理类/企业管理类/网络管理类
数据库	数据库开发/数据库高级管理/数据库优化与设计/数据仓库
IT 管理	项目管理系列/ ITSM 系列/沟通力系列
Office 办公	Microsoft Word/Excel/Powerpoint/Outlook/Visio/Access 实用技巧

IT 服务

服务项目	*服务细项*	
企业 IT 架构与应用服务	IT 基础架构规划与部署	统一的消息与协作
	企业内容管理和门户	企业网络&系统管理
	企业客户端标准化及服务管理智能化	
软件研发顾问咨询服务	iScrum 敏捷开发过程规划咨询	软件需求开发与管理
	软件体系架构的规划与实施	数据仓库开发顾问咨询
	SharePoint 定制与二次开发	软件测试实施与管理

	数据库模型设计与优化 手机/平板电脑应用设计开发 使用 TFS2010 构建企业软件生命周期管理平台	UI/UE 顾问咨询
数据库服务	数据库安装升级 健康检查	性能评估与优化
人才外包	系统网络方向 研发方向	数据库/数据仓库方向

软件研发信息整合者

- 企业信息门户
- 知识管理系统
- 决策支持系统
- 数据挖掘系统
- Ultimus BPM
- 统一沟通系统
- 企业定制应用

部分成功客户

- 广东核电
- 中国银行
- 联想集团
- 南方航空
- 中南空管局
- 广州海关
- 东风柳汽
- 易方达基金
- 索尼中国
- 新世界地产
- 信诚人寿
- 喜之郎
- 中兴通讯
- 王老吉
- 艾默生能源
- 佛山移动
- 安利（中国）
- 汇丰银行

三、讲师简介

鹿传明

中睿创始人，CIO。厦门大学 EMBA、PMP、Scrum Master、TOGAF 认证企业架构师、微软认证讲师（MCT）、微软认证架构师（MCA）。拥有 17+年的团队管理、人员培养、项目管理、研发管理及咨询经验。曾为**联想中国、华为、平安科技、黄埔海关**等世界五百强企、事业做过上门的服务。先后担任项目经理、研发部经理、研发总监、技术部总经理等职务，也曾因工作需要，带领过一支从技术转成管理团

队，多次对不同公司的储备经理给予不同方式的指导和培训。具有大型跨国团队管理和海外工作经验，擅长企业信息化规划、IT 项目管理、企业架构、需求开发与管理等在企业的实战应用。成功主持过多家企业的项目团队的管理、外包人员管理、研发项目管理、软件工程等体系的咨询、培训与实施。现为中睿总经理和首席企业金牌顾问。

行业专家

- 面向对象的分析与设计
- 企业架构与软件架构设计
- 项目管理
- 外包项目管理
- 从技术岗位如何转向管理岗位
- 产品需求分析与管理
- Scrum敏捷开发过程

教学风格

注重因材施教，注重实际应用，在授课引入大量的实际开发经验。授课条理清晰，深入浅出，通过一个或多个实际案例贯穿整个课程，语言表达能力强；善于调动学员学习积极性；思维敏捷，可以根据学生的实际需求随即应变；说明问题耐心细致，受到学员一致好评。

工作经历

17年IT工作经验，13年IT培训经验。

资质证书

- 微软认证讲师（MCT）
- 微软认证架构师（MCA）
- 美国项目管理协会项目管理专家(PMP)
- TOGAF企业架构师
- Scrum Master

部分成功客户

通讯科技

- 金鹏电子
- 深圳联想
- 中兴通讯
- 广东移动
- 深圳电信
- 重庆移动

国企事业机构：

- 南方航空
- 省信息中心
- 深圳国土规划局
- 中南空管局
- 深圳国税
- 广东地税
- 黄埔海关
- 中广核
- 深圳烟草公司

企事业单位：

- 信诚人寿
- 富士康集团
- 东方思维
- 深圳华为
- 龙记集团
- 艾默生网络能源
- 东莞TTI集团
- 深圳联友
- 万海资讯

金融行业：

- 中国银行
- 南方基金
- 广州农村商业银行
- 工商银行
- 平安科技
- 招商银行
- 易方达基金
- 招商信诺
- 中国建设银行