新型网络安全
人才培养丛书

协助企业开发和维护安全的应用程序

OWASP CODE REVIEW GUIDE 2.0

应用软件安全代码审查指南

软件安全开发生命周期（S-SDLC）落地实践系列参考书

美国 OWASP 基金会 ◎ 著
OWASP中国/SecZone ◎ 译

中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

新型网络安全人才培养丛书

应用软件安全代码审查指南

美国 OWASP 基金会　著
OWASP 中国/SecZone　译

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

内 容 简 介

本书分为两大部分，共 15 章。第一部分包含第 1～4 章，介绍了安全代码审查的作用和方法，以及在软件安全开发生命周期（S-SDLC）代码审查过程中查找安全漏洞的方法。第二部分包含第 5～15 章，介绍 2013 年版《OWASP Top 10》中提出的安全风险的处理方法和技术，以及其他漏洞处理的方法和技术。

本书适合软件研发组织机构的高层管理人员、专业技术负责人、开发人员、测试人员和软件安全人员，以及高等院校软件工程、网络安全专业的师生等阅读学习。

图书在版编目（CIP）数据

应用软件安全代码审查指南/美国 OWASP 基金会著；OWASP 中国，SecZone 译. —北京：电子工业出版社，2018.11
（新型网络安全人才培养丛书）
ISBN 978-7-121-35220-1

Ⅰ. ①应… Ⅱ. ①美… ②O… ③S… Ⅲ. ①软件开发－安全技术 Ⅳ. ①TP311.522

中国版本图书馆 CIP 数据核字（2018）第 239567 号

策划编辑：朱雨萌
责任编辑：朱雨萌
特约编辑：刘广钦 刘红涛
印　　刷：天津千鹤文化传播有限公司
装　　订：天津千鹤文化传播有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编：100036
开　　本：720×1000　1/16　印张：16.5　字数：314 千字
版　　次：2018 年 11 月第 1 版
印　　次：2018 年 11 月第 1 次印刷
定　　价：59.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：（010）88254750。

关于指南

《应用软件安全代码审查指南》是为应用程序研发组织机构的高层管理人员、专业技术负责人、开发人员、测试人员、软件安全人员及其他负责代码审查人员等编写的技术书籍，由《OWASP 代码审查指南（第 2.0 版）》翻译而来。

版权和许可证

发布历史

《OWASP 代码审查指南（第 2.0 版）》发布于 2017 年，该 OWASP 项目由 Larry Conklin 和 Gary Robinson 领导。

《OWASP 代码审查指南（第 2.0 版）》已成功引入当前主流的安全威胁和对策。此版本还包括了能反映 OWASP 组织有关安全代码审查最佳实践经验的新内容。

内容说明

本指南旨在向软件开发人员和管理人员建议有关安全代码审查的最佳实践，以及如何在软件安全开发生命周期（S-SDLC）中使用它。本指南的开头部分向读者介绍了安全代码审查，以及如何将其引入公司的 S-SDLC 中。随后，本指南集中在特定的技术主题，并提供了审查人员应该在审查技术代码时查找的样例。要特别指出的是，本指南包括如下几部分。

1. 概述

本部分向读者介绍了安全代码审查，以及安全代码审查可以为开发组织带来的好处。另外，还对安全代码审查技术进行了概述，并介绍了安全代码审查与其他安全代码分析技术的对比。

2. 方法论

本部分详细介绍了如何将安全代码审查技术集成到开发组织的 S-SDLC 中，

以及安全代码审查人员如何确保他们执行有效的安全代码审查。另外，本部分还包含了在安全代码审查中应用基于风险的信息，使用威胁模型了解正在审查的应用程序，以及了解由外部业务所驱动的应用程序是如何影响安全代码审查需要的。

3. 基于控制技术的审查

本部分深入常见的安全控制技术，包括身份验证、授权、日志记录和信息防泄露，并使用多种语言的安全代码示例指导审查人员。本部分可用于学习各种控件的重要方面，并在执行安全代码审查时作为直接参考。

4. 基于安全漏洞的审查

本部分深入分析了常见的应用程序安全漏洞，包括 XSS、SQL 注入和会话跟踪问题。与前面的内容一样，读者可以了解各种安全漏洞的信息，并将本指南作为直接参考。

背景

近年来，我国对网络安全高度重视。2016 年年底至 2017 年，国家先后发布并实施了《网络空间安全战略》《网络安全法》《关于加强网络安全学科建设和人才培养的意见》等法律法规和国家指导意见，并对全国各行各业提出了保护网络运行安全和网络数据安全的要求。与此同时，诸如“Equifax 企业数据泄露”这样由应用软件程序漏洞所引起的全球性网络安全事件仍不时刺痛着人们的神经。随着行业与技术的快速发展，越来越多的安全研究机构、软件研发团队、专家学者认识到：“做好软件安全开发、做好软件安全开发生命周期（S-SDLC）管理，才是从技术上解决网络安全的根本之道。”国内大量企业也已开始关注、规划和实践 S-SDLC。我国有关部门也逐渐针对软件安全开发领域，陆续推出了有关软件安全开发的人员能力认证、企业安全开发成熟度认定及软件产品安全检验等全方位的工作。

那么，软件研发团队应该如何开展软件安全开发工作或 S-SDLC 实践工作呢？软件研发团队应该如何快速着手软件安全开发呢？软件开发人员和安全人员如何建立一致的交流语言呢？软件安全开发如何与 DevOps 相融合呢？本书就是基于这样的背景译制的。

项目简介

《OWASP 代码审查指南（第 2.0 版）》最初是从《OWASP 测试指南》中诞生的，其内容涵盖在《OWASP 测试指南》中，因为在那时候是恰当的。但是，随着安全代码审查涉及的主题越来越多，其逐步发展成为一个独立的指南。

OWASP 在 2006 年启动了“审查人员项目”。而本版本则是在 2013 年 4 月“OWASP 重启项目（OWASP Project Reboot）”的指导下开始的，并获得了美国国土安全部的项目资金赞助。

OWASP 代码审查项目团队由一批少量但颇有才华的志愿者组成。这些志愿者具有丰富的经验，并在各类企业组织（从小型的初创公司到世界上最大的软件开发企业）中推动安全代码审查的最佳实践。

在软件开发生命周期的早期检测软件中的 Bug，可以以较低的成本投入更加有效地生产和开发更安全的软件，这已是一个常识。将适当的安全代码审查功能集成到软件安全开发生命周期（S-SDLC）中的企业组织，可以开发出安全性明显较好的代码。简单来说，“我们不能攻击自己的安全性。”相对于为安全运营人员分配的时间，攻击者有更多的时间去探寻应用系统中的漏洞。攻击者对软件系统的入侵和攻击，是一个人数不均、力量不对等的战争和一场极有可能失败的战斗。

本指南没有包含所有的编程语言，主要侧重于 C#、.NET 和 Java，但在有些部分包含了 C、C++、PHP 和其他语言。本书提倡的技术可以很容易地适应几乎任何代码环境。幸运的是（或不幸运的是），Web 应用程序中的安全漏洞在不同的编程语言中是非常相似的。

读者对象

本书的主要读者对象包括：

- 软件研发组织机构的高层管理人员。
- 软件研发组织机构的专业技术负责人。

- 软件研发人员、软件测试人员和软件安全人员。
- 软件安全开发服务咨询与培训相关人员，网络安全前沿领域的专家学者。
- 高等院校软件工程专业和网络安全专业的教育工作者。
- 高等院校软件工程专业和网络安全专业的在校学生。
- 对软件安全开发感兴趣的个人。

内容结构

本书分为两大部分，共 15 章。第一部分包含第 1～4 章，介绍了安全代码审查的作用和方法，以及在软件安全开发生命周期（S-SDLC）审查人员过程中查找安全漏洞的方法。第二部分包含第 5～15 章，介绍了 2013 年版《OWASP Top 10》中提出的安全风险的处理方法和技术，以及其他漏洞处理的方法和技术。

全书由王颉负责总体架构设计，由 Rip、李绪勤、郭锡泉担任翻译顾问，由夏天泽、余瞰、陈香锡进行技术指导。前言、第 1、2 章由王颉翻译，第 3 章由杨盛明翻译，第 4 章由陈中举翻译，第 5、6 章由何伊圣翻译，第 7、8 章由徐瑞祝和何伊圣共同翻译，第 9～15 章由何伊圣翻译，附录由陈中举翻译。全书由赵学文统稿与编排。

致谢

特别感谢 OWASP 总部对 OWASP 中国组织开展中文版《应用软件安全代码审查指南》相关工作予以的支持。

感谢 OWASP 中国和 SecZone 自 *OWASP Code Review Guide（V 2.0）* 发布以来对该项目持续的跟进、翻译、研究与分享。同时，也对该项目的参与人员表示感谢。

OWASP 中国将对“OWASP 安全代码审查指南”项目保持跟进，持续完善和深化本书。

中文版说明

（1）本书为 *OWASP Code Review Guide（V 2.0）* 的中文版。该版本尽量提供英文版本中的图片，并与原版本保持相同的风格。对于存在的差异，敬请谅解。

（2）为方便读者阅读和理解本书中的内容，本书对英文版中的部分章节进行了顺序调整。

（3）由于译者团队水平有限，若存在错误敬请指正。

（4）如果您有关于本书的任何意见或建议，可以通过以下方式联系我们：

邮箱：project@owasp.org.cn

微信公众号：

“OWASP 安全代码审查指南”项目支持单位：

OWASP 中国 The Open Web Application Security Project

开源网安 SECZONE GROUP

中文版工作团队成员简介：（按姓氏拼音顺序排序）

Rip

OWASP 中国主席

OWASP S-SDLC 项目、OWASP 中文项目、OWASP 中国各项目发起人。超过 15 年的安全领域从业经验，资深安全专家。

陈香锡

OWASP 中国会员

安全检测与渗透测试专家，原 SAINTSEC 安全团队联合创始人，清远职业技术学院特聘安全专家和讲师。具有多年软件安全开发、乙方安全攻防实战经验，熟悉 OWASP Top 10 软件安全威胁体系。对软件安全开发、Web 安全渗透有深入的分析和研究；先后为中国移动、金蝶软件、平安银行、招商银行、广州银行、新疆银行、华南理工大学等近 50 家企业级客户提供渗透测试、安全咨询、安全培训等服务项目。

陈中举

OWASP 中国会员

长江大学网络工程系主任、副教授、硕士研究生导师

近 5 年主持湖北省教育厅项目 1 项，参与湖北省自然科学基金项目 2 项，主持和参与油田及地方横向项目 10 余项，获软件著作权 4 项。公开发表论文 10 余篇，其中核心和 EI 检索 7 篇，主编行业规划教材 1 部，参编“十二五”国家规划教材 2 部。主要研究方向为计算机网络及安全、智能信息系统等。

郭锡泉

OWASP 中国会员

清远职业技术学院信息技术与创意设计学院副院长、副教授

暨南大学博士，研究方向为信息安全技术、信息安全管理。曾参与广东省科技计划项目“基于专用协议栈的流过滤网络防火墙研制”、广东省教育部产学研结合项目“基于新一代网络的入侵检测系统产业化研究”等，发表相关论文 25 篇。带领清远职业技术学院信息安全技术与应用研究所团队，获 CNNVD、CNVD、CVE 等原创漏洞证书数百项、信息安全相关的专利和软件著作权多项；获国家级教学成果二等奖，指导学生参加广东省高职院校职业技能竞赛计算机网络应用赛项获一等奖多项；主编项目化教材《网络互连设备配置》（人民邮电出版社出版）。

何伊圣

OWASP 中国会员

山石网科安全服务部负责人

SAINTSEC 信息安全团队创始人。红帽杯、网安中国行等比赛冠军；GeekPwn 澳门站选手；获得众多 CNVD、CNNVD 原创漏洞证书；广东省多所高校的外聘信息安全讲师。

李绪勤

OWASP 中国会员

英国华威大学博士，长期关注金融业务风险、金融风险等领域，拥有超过 10 年 IT 工作经验和信息安全实践经验。

王颉

OWASP 中国副主席兼 OWASP 中国成都区域负责人

深圳开源互联网安全技术有限公司副总经理

英国拉夫堡大学网络安全博士。长期从事企业信息体系建设落地和软件安全开发生命周期研究工作，具有丰富的信息安全学术研究和资深的企业信息化建设实践经验，Citrix、ITIL、PMP、CWASP CSSP 认证专家。自 2009 年加入 OWASP 组织和 OWASP 中国分部以来，曾参与了“OWASP 中文项目”和“OWASP S-SDLC 项目”两个 OWASP 全球项目，并先后主持、参与和独立开展了“OWASP Top 10”“OWASP OpenSAMM”“OWASP 安全编码规范快速参考指南”“OWASP 安全测试指南”等多个 OWASP 中国分部项目，为在国内提高 OWASP 安全组织的影响力、提升 OWASP 研究成果的实用性和适用性做出了重要贡献。

杨盛明

OWASP 中国会员

工业和信息化部电子第五研究所信息安全研究中心工作人员

在校期间研究方向为网络与信息安全，2013 年参加工作至今从事信息系统安全测评及风险评估相关工作，牵头实施的项目涉及政府、电力、医疗、金融、教育等行业，测评对象主要涵盖 Web 应用、移动 App、电力系统、工控系统等不同应用系统。工作职责主要包括渗透测试、安全评估、等保测评、测评工具开发等项目的具体技术实施及管理工作，擅长的编程语言包括 C、C++、Java、Python 等；工作之余喜欢在 Freebuf 上发表文章，翻译国外安全资讯、技术博文等。

徐瑞祝

OWASP 中国会员

CWASP L2 认证专家、Checkmarx 认证专家、CISP 讲师、CWASP 讲师、资深 SDLC 咨询师。具有超过 10 年的安全开发从业经验，对安全编码、代码安全审查、代码安全审查工具有丰富的实践经验，对 SDL 落地实施与深化应用具有高度的认识水平，并擅长对软件安全开发生命周期的各个阶段的质量控制。主导或参与了华为、中兴通讯、国家开发银行、农业银行、顺丰速运等近 40 家企业与组织的安全开发与 SDLC 落地工作；并主导了行业内《源码工具审查基准》的研制，参与了《OWASP 安全测试指南（第 4 版）》的译制。

夏天泽

OWASP 中国安徽区域负责人兼 OWASP S-SDLC 项目核心负责人之一

深圳开源互联网安全技术有限公司首席战略官（CSO）

中国科学技术大学信息安全专业硕士，CWASP L2 CISP 认证专家，CWASP 讲师，CWASP CSSP 讲师，从事信息安全工作近 10 年。曾任惠普公司高级安全顾问、思科系统中国研发中心高级安全架构师、思科安全团队核心成员，曾获思科最高级别安全工程师认证（Cisco Security Ninja Black Belt）。涉及领域包括 Web 安全、Client 安全、Mobile 安全、SecDevOps 等方面。对软件安全开发流程、安全架构、渗透测试、安全事件处理、第三方软件安全管理及安全运维有深入研究和丰富经验。先后参与了 OWASP 中国分部组织的“OWASP CheatSheet”项目和“OWASP Top 10 2017”项目。

余瞰

OWASP 中国会员

南京大学硕士，具有 10 年软件开发和信息安全经验，曾任职于思科研发和安全团队，参与了全球最大的云会议系统的设计、开发及安全开发流程的建立，曾获思科最高级别安全工程师认证。先后负责国内领先的安全开发云平台的设计与开发、国内领先的交互式安全测试工具的设计与开发及 S-SDLC 项目咨询。

赵学文

OWASP 中国会员

“注册软件安全开发人员（CWASP CSSD）”认证持有者。自 2017 年加入 OWASP 中国分部以来，积极参与 OWASP 中国组织的“OWASP Top 10 2017”“OWASP ASVS”“OWASP Code Review”等中文项目，为应用软件安全技术的研究与推广做出了积极贡献。