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 APPLICATION SECURITY VERIFICATION STANDARD 3.0.1

软件安全开发指南

应用软件安全级别验证参考标准

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

软件安全开发指南
——应用软件安全级别验证参考标准

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

本书系统性地介绍了 OWASP 安全组织研究总结的应用安全验证标准，为软件开发过程中的安全控制措施开发提供了直接指导与必要参考。全书分为两大部分：第一部分介绍了应用安全验证要求的使用方法和参考案例。第二部分详细介绍了 19 项安全控制措施的验证要求，并针对每种安全验证介绍了不同级别的控制目标和详细要求。本书旨在帮助软件开发企业机构和团队提升有关应用软件安全开发的相关意识；并在应用软件设计、开发和测试过程中，能明确对功能性和非功能性安全控制的要求。

本书适合软件开发企业的管理人员和执行人员，从事软件安全开发相关的专业人员，以及高等院校软件工程、信息安全、信息管理等专业的研究生、本科生学习和参考。

图书在版编目（CIP）数据

软件安全开发指南：应用软件安全级别验证参考标准 / 美国 OWASP 基金会著；OWASP 中国，SecZone 译. —北京：电子工业出版社，2018.4
（新型网络安全人才培养丛书）
ISBN 978-7-121-33849-6

Ⅰ. ①软… 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 048226 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：三河市鑫金马印装有限公司
装　　订：三河市鑫金马印装有限公司
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：9.5　字数：160 千字
版　　次：2018 年 4 月第 1 版
印　　次：2018 年 4 月第 1 次印刷
定　　价：36.00 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。

关于标准

本书是根据《OWASP 应用程序安全验证标准》翻译编写的。《OWASP 应用程序安全验证标准》是架构师、开发人员、测试人员、安全专业人员及用户可以使用的应用程序安全性要求或测试的列表，以定义安全的应用程序。

版权和许可证

发布历史

第 3.0.1 版《OWASP 应用程序安全验证标准》发布于 2016 年，该项目由 Daniel Cuthbert 和 Andrew van der Stock 领导。

- 2014 年 8 月，第 2.0 版《OWASP 应用程序安全验证标准》发布。
- 2015 年 9 月，第 3.0 版《OWASP 应用程序安全验证标准》发布。
- 2016 年 6 月，第 3.0.1 版《OWASP 应用程序安全验证标准》发布。

2015 年第 3.0 版的贡献者

项目负责人	主要作者	贡献者和审稿人
Andrew van der Stock	Jim Manico	Abhinav Sejpal
Daniel Cuthbert		Ari Kesäniemi
		Boy Baukema
		Colin Watson
		Cristinel Dumitru
		David Ryan
		François-Eric Guyomarc'h
		Gary Robinson
		Glenn Ten Cate
		James Holland
		Martin Knobloch
		Raoul Endres
		Ravishankar S
		Riccardo Ten Cate
		Roberto Martelloni
		Ryan Dewhurst
		Stephen de Vries
		Steven van der Baan

2014 年第 2.0 版的贡献者

项目负责人	主要作者	贡献者和审稿人
Daniel Cuthbert	Andrew van der Stock	Antonio Fontes
Sahba Kazerooni	Krishna Raja	Archangel Cuison
		Ari Kesäniemi
		Boy Baukema
		Colin Watson
		Dr Emin Tatli
		Etienne Stalmans
		Evan Gaustad
		Jeff Sergeant
		Jerome Athias
		Jim Manico
		Mait Peekma
		Pekka Sillanpää
		Safuat Hamdy
		Scott Luc
		Sebastien Deleersnyder

2009 年第 1.0 版的贡献者

项目负责人	主要作者	贡献者和审稿人
Mike Boberski	Jim Manico	Andrew van der Stock
Jeff Williams		Barry Boyd
Dave Wichers		Bedirhan Urgun
		Colin Watson
		Dan Cornell
		Dave Hausladen
		Dave van Stein
		Dr. Sarbari Gupta
		Dr. Thomas Braun
		Eoin Keary
		Gaurang Shah
		George Lawless
		Jeff LoSapio
		Jeremiah Grossman
		John Martin
		John Steven

续表

项目负责人	主要作者	贡献者和审稿人
		Ken Huang
		Ketan Dilipkumar Vyas
		Liz Fong　　Shouvik Bardhan
		Mandeep Khera
		Matt Presson
		Nam Nguyen
		Paul Douthit
		Pierre Parrend
		Richard Campbell
		Scott Matsumoto
		Stan Wisseman
		Stephen de Vries
		Steve Coyle
		Terrie Diaz
		Theodore Winograd

欢迎使用《OWASP 应用程序安全验证标准（ASVS）》第 3.0.1 版。ASVS 是通过 OWASP 团队努力建立而成的安全要求和控制框架，其侧重于在应用程序设计、开发和测试时所需的功能和非功能安全控制。

本版本被认为是识别和采用的最佳实践经验。这将有助于新兴标准计划采用 ASVS 中的内容，同时协助现有的企业学习他人的经验。

OWASP ASVS 项目组预计这个标准可能永远不会达到 100%的完善并被认同。风险分析在某种程度上是主观的，这在尝试以适合所有标准的尺度进行泛化时，会产生挑战。但是，OWASP ASVS 项目组希望本版本的最新更新是朝着正确的方向迈出的一步，并期望能为行业引入这一重要的概念。

第 3.0.1 版有什么新功能

（1）在第 3.0.1 版本中，ASVS 增加了几个部分，包括配置、Web 服务等，使本标准更适用于现代应用，如 HTML5 前端或移动客户端、使用 SAML 身份验证来调用一组 RESTful Web 服务。

（2）为确保使用人员不需要多次重复验证相同的项目，第 3.0.1 版 ASVS 删除了重复的标准。

第 3.0.1 版 ASVS 提供了一个映射到 CWE 常见弱点的枚举（CWE）字典。CWE 映射可以用于识别信息利用的可能性，成功地利用这一结果。广义地说，如果不使用或实施安全控制及如何缓解弱点，那么还可以洞悉将来有可能出现的问题。

最后，在 2015 年 OWASP AppSec 欧洲大会期间，OWASP ASVS 项目组与其他项目组、专家进行了评审，并在 2015 年的 OWASP AppSec 美国大会进行了最后的工作会议，纳入大量反馈意见。OWASP ASVS 项目组希望读者能找到对本书有用的更新，并以项目组所能想象的方式使用它。

背景

2016 年和 2017 年是我国网络安全行业飞速发展的两年。自 2016 年年底至 2017 年，国家先后发布并实施《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》等涉及网络安全方面的法律法规和政策文件。同时，“WannCry 勒索病毒”“Structs2 漏洞”“Office 高危漏洞”等这样的全球性网络安全事件也不时刺痛着人们的神经。越来越多的网络安全研究机构、软件研发机构、专家学者逐渐认识到“没有软件安全，就没有网络安全”“安全不仅是网络安全专家的责任，更是每个软件开发从业人员的责任”。

那么，软件研发机构如何开发出安全的应用程序呢？安全的应用程序应该符合哪些标准呢？软件研发机构需要验证应用程序的哪些方面呢？本书是在这样的背景下翻译出版的。

ASVS 简介

“OWASP 应用程序安全验证标准（ASVS）”项目是 OWASP 全球安全组织的成功项目之一。该项目的主旨如下：为执行 Web 应用程序安全验证提供一套可行的标准，以规范应用程序的安全验证覆盖范围和安全级别。该项目的研究成果，即《OWASP 应用程序安全验证标准（ASVS）》，最新版本为第 3.0.1 版。

该成果不仅为 Web 应用程序技术安全控制提供了测试参考标准，还为应用程序开发人员提供了一系列安全开发需求建议。为测试应用程序技术安全控制及依赖于测试环境中的任何技术安全控制提供了参考依据，以消除应用程序受到跨站脚本（XSS）、SQL 注入等软件安全威胁的影响。此外，该成果还可用于标识应用程序的安全信任级别。

该成果可根据读者或使用人员的需要，作为度量标准、安全指导和采购要求。

（1）度量标准：为应用程序开发人员和应用程序所有者提供一个参考标准，以评估应用程序的可信任程度。

（2）安全指导：为应用程序中安全控制的开发人员提供有关构建安全控制的指导建议，以满足应用程序的安全开发需求。

（3）采购要求：为应用程序的采购合同，提供应用程序安全验证需求的参考标准。

读者对象

本书的主要读者对象包括但不限于：

（1）软件研发组织机构的技术专业负责人和项目主管。

（2）软件安全开发服务咨询与验证的相关人员。

（3）网络安全基础核心领域研究的专家学者。

（4）高等院校软件工程专业和网络安全专业的教育工作者。

（5）对软件安全开发感兴趣的个人。

内容结构

本书分为 3 篇，共 19 章。第一篇由第 1、2 章组成，对 ASVS 及其评估软件的使用方式进行了介绍。第二篇由第 3～18 章组成，分别介绍了 16 类验证关键点。第三篇由第 19 章组成，表述了 ASVS 的实践案例。

全书由王颉负责总体架构设计和质量控制，由 Rip、张家银担任翻译顾问，由包悦忠、李旭勤负责技术指导。第 1 章由王颉翻译，第 2 章由王厚奎翻译，第 3～10 章由王厚奎和吴楠共同翻译，第 11～18 章由吴楠翻译，第 19 章及附录由王厚奎翻译。全文由赵学文负责统稿与编排。

致谢

特别感谢 OWASP 总部对 OWASP 中国组织本中文版 ASVS 相关工作予以的支持。

感谢 OWASP 中国和 SecZone 自 *OWASP Application Security Verification Standard*（*V2.0*）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 ASVS 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 Application Security Verification Standard*（*V3.0.1*）的中文版。本书尽量保留原版本的格式与风格，但部分语言风格调整为中文表述。其中存在的差异，敬请谅解。

（2）为方便读者阅读和理解本书中的内容，本书对原英文版中明确内容为空的章节进行了删除，并对原英文版中的部分章节内容进行了顺序调整，致使本书的章节编号与原英文版中的章节编号不同。

（3）本书中的表格包含每条描述项的序号，以及其在原英文版中的原描述项序号，以方便读者进行匹配。

（4）由于译者团队水平有限，存在的错误敬请指正。

（5）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 ASVS 项目支持单位：

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。

包悦忠

OWASP 中国副主席

加拿大滑铁卢大学应用科学硕士。曾任职亚马逊（中国）首席信息安全官、微软可信赖计算部总监。长期在北美和中国高科技软件和互联网公司从事信息安全管理、软件安全开发及相关流程体系建设。微软内部认证 SDL 讲师，曾负责为中国政府、电信和金融等行业大客户提供软件安全评估、SDL 培训及流程实施方面的咨询服务，帮助客户利用 SDL 的方法和实践，通过在软件开发生命周期过程中融入必要的安全活动，整体提高软件和应用的安全性。先后参与“OWASP Top 10”“OWASP 安全测试指南”等多个 OWASP 中国分部项目。

李绪勤

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。

王厚奎

OWASP中国广西区域负责人

南宁职业技术学院信息工程学院 副教授

硕士研究生，持有CISP（CISO）、NISP、网络规划设计师、初级等保测评师、NSACE网络信息安全讲师等资质证书，并取得中国信息安全测评中心颁发的CISI讲师资格。中国计算机学会会员、广西信息安全学会会员。拥有14年IT工作经验，8年信息安全实践经验和培训教学经验，涉及网络管理、信息安全与风险管理、信息产品安全管理、信息安全省级项目调研等多个方面。自2010年加入OWASP组织和OWASP中国分部以来，先后参与了“OWASP Top 10”“OWASP Cheat Sheets”“OWASP Hacking-Lab”等多个应用安全研究项目。

王颉

OWASP中国副主席

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开

发全生命周期研究工作，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。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。

吴楠

OWASP 中国辽宁区域负责人

大连银行 高级信息安全顾问

长期从事信息安全体系建设、银行业安全合规建设、S-SDLC 的研究工作，并深入项目实施安全代码审计。在从事信息安全工作前，曾多年从事全生命周期的软件开发及项目管理工作。获得 CISP、PMP、ISO 27001 IA、ISO 22301、Risk Mangement、CWASP L2 安全专家、国家软件工程师、C-CCSK、ITIL 等认证资质。自 2015 年加入 OWASP 组织和 OWASP 中国分部以来，先后参与了“OWASP Top 10”“OWASP Cheat Sheets”“OWASP Code Review”等应用安全项目，并从中积累了宝贵的经验。

张家银

OWASP S-SDLC 项目主要负责人

安徽开源互联网安全技术有限公司 总经理

拥有 15 年安全领域从业经验，资深 S-SDLC 专家。对软件安全开发流程、安全架构设计、应用安全解决方案、安全测试，以及应用安全扫描工具原理与设计有深入的研究与实践经验，曾主导完成全球最大云安全产品（年用户数 7+ 亿人次）的 S-SDLC 全流程及落地。

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，先后参与了 OWASP 中国组织的“OWASP Top 10 2017”“OWASP SAMM”“OWASP Cheat Sheets”“OWASP Code Review”等中文项目，为应用软件技术的研究与推广做出了积极项献。