丰富案例讲解Web应用测试的“4W1H”
充分覆盖S-SDLC的应用安全测试战略方法
助你开发和维护安全的应用程序

CWASP安全培训指定用书

# TESTING GUIDE V4.0

# 安全测试指南（第4版）

[美] 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

# 安全测试指南

## （第4版）

［美］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

软件安全问题也许是这个时代面临的最为重要的技术挑战。Web 应用程序让业务、社交等网络活动飞速发展，这同时也加剧了它们对软件安全的要求。我们急需建立一个强大的方法来编写和保护我们的互联网、Web 应用程序和数据，并基于工程和科学的原则，用一致的、可重复的和定义的方法来测试软件安全问题。本书正是实现这个目标的重要一步，作为一本安全测试指南，详细讲解了 Web 应用测试的“4W1H”，即“什么是测试”、“为什么要测试”、“什么时间测试”、“测试哪里”以及“如何测试”。

本书适合高等院校计算机相关专业师生阅读，也适合广大软件开发人员、测试人员以及所有对软件安全问题感兴趣的读者阅读。



**图书在版编目（CIP）数据**

安全测试指南 / 美国 OWASP 基金会著；OWASP 中国 / SECZONE 译. —4 版. —北京：电子工业出版社，2016.7

ISBN 978-7-121-29208-8

Ⅰ. ① 安… Ⅱ. ① 美… ② O… Ⅲ. ① 软件可靠性—测试—指南 Ⅳ. ①TP311.5-62

中国版本图书馆 CIP 数据核字（2016）第 145474 号

责任编辑：李 冰 文字编辑：朱雨萌
印 刷：三河市华成印务有限公司
装 订：三河市华成印务有限公司
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：787×1 092 1/16 印张：30.25 字数：739.2 千字
版 次：2016 年 7 月第 1 版
印 次：2016 年 7 月第 1 次印刷
定 价：89.00 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）88264750。

# 序 1

软件安全问题也许是我们这个时代最为重要的技术挑战。Web 应用程序实现了业务、社交网络等网络活动的飞速发展，同时也加剧了对软件安全的要求。我们急需建立一个强大的方案来编写和保护我们的互联网、Web 应用程序和数据。

OWASP 团队努力使安全的软件成为这个世界上正常、规范的产品，而这份 OWASP 测试指南正是实现这个目标的重要一步。重要的是，我们用来测试软件安全问题的方法是基于工程和科学的原则。我们需要一个一致的、可重复的和定义的方法来测试 Web 应用程序。而一个没有工程和技术的最低标准的世界将是一个混乱的世界。

毫无疑问，没有进行安全测试就无法建立一个安全的应用程序。测试是建立一个安全的系统使用的广泛措施的一部分。然而，许多软件开发组织的标准软件开发流程中却并不包含安全测试这一步骤。更糟的是，许多安全厂商提供了不同程度的质量和要求的测试。

由于攻击者能够利用无数种方法来攻破应用程序，而安全测试不可能测试全部的攻击方法，所以安全测试其自身并非是衡量应用安全最有效的方法。我们只有有限的时间来测试和捍卫软件安全，而攻击者却没有这样的限制，所以我们不能自己降低对安全的要求。

结合使用其他 OWASP 项目文档，如《代码审查指南》《开发指南》和类似 OWASP ZAP 的工具，是建立和维护安全的应用程序的一个好的开始。《开发指南》将告诉你如何设计和构建安全的应用程序，《代码审查指南》将告诉你如何验证应用程序源代码的安全性，而《安全测试指南》将告诉你如何验证正在运行的应用程序的安全性。我强烈推荐使用这些指南作为应用程序安全性验证的一部分。

## 为什么选择 OWASP

创建一本这样的指南是一份艰巨的工作，因为它汇集了数百位世界各地的专家的专业技能才得以完成。测试安全漏洞有许多不同的方式，但是这本指南却在怎样快捷、准确、

有效地测试方面获得了权威人士的一致认可。志同道合的安全专家们在 OWASP 团队中一起工作，构建了安全问题的领先实践方法。

安全不应该躲在暗处，只有少数人可以操作。它应该是向所有人开放，例如 QA 人员、开发人员和技术管理人员，而不只是专用于安全从业人员。建立这个指南的目的是让需要它的人——你、我和参与构建软件的任何人能掌握这些专业知识。

这本指南必须要在开发者和软件测试者中推广。因为世界上没有足够的应用安全专家来对所有问题做出重要建议。而应用安全最开始的责任肯定是落在软件开发者的肩上，因为他们负责代码的编写。如果开发者没有对软件进行测试，或者在编写时没有考虑可能导致漏洞的 Bug，那么他是不能编写出安全的代码的。

保证信息及时更新对这本指南至关重要。通过采用 Wiki 方式，OWASP 团队能逐渐发展和扩大这本指南中的信息，以跟上快速发展的应用安全威胁的步伐。

本指南很好地证明了 OWASP 成员和项目志愿者的激情和能量，而这也必将小小地改变世界。

## 裁剪和优先级

这本指南可以通过裁剪来适用于组织的技术、流程及组织架构。一般在组织中有几个不同的角色会使用到本指南。

- 开发人员：使用本指南以确保编写出安全的代码。这些测试应该是正常的编码和单元测试计划的一部分。
- 软件测试和 QA 人员：使用本指南以扩充应用程序的测试组，尽早发现这些漏洞，将为以后节省大量的时间和精力。
- 安全专家：结合使用本指南与其他技术指南，作为一种确认方式，以确保应用程序中没有被忽略的安全漏洞。
- 项目经理：思考本指南存在的原因，以及发现在代码和设计缺陷中显现的安全问题。

切记执行安全测试时，要不断调整优先级。因为有无数种可能都会导致应用程序失败，而组织的测试时间和资源是有限的。所以用有限的时间和资源来关注真正的安全漏洞风险业务，以及研究应用风险和其产生的条件是非常明智的做法。

本指南可以看作一组技术，我们可以用它们来寻找不同类型的安全漏洞。但并不是所有的技术同样重要。请尽量避免将本指南作为核对清单来使用，因为新的漏洞总会出现，没有任何指南可以穷尽测试的方法。但是，使用这本指南将是一个好的开始。

## 自动化工具的作用

有许多公司销售自动化安全分析工具和测试工具，但是这些工具是有局限性的，需要将它们用在恰当的地方。正如迈克尔·霍华德在 2006 年 OWASP 西雅图 AppSec 峰会上所

说："工具不会让软件安全！它们只是去规范过程和加强政策。"

重点是这些工具是通用的。也就是说，它们不是专门为自定义代码，而是为了一般的应用程序而开发设计的。这意味着它们可以找到一些通用的问题，但是它们没有足够的应用程序知识来检测大多数缺陷。根据经验，最严重的安全问题是那些非通用的、深深交织在一起的业务逻辑和定制应用程序设计。

但是这些工具也是有用处的，它们确实发现了很多潜在的问题。运行这些工具并不需要太多时间，但是每一个潜在的问题都需要时间调查和验证。如果我们的目标是尽快找到并消除最严重的缺陷，就最好考虑是否使用自动化工具或采用本指南中所述的技术来检测。另外，这些工具也是一个平衡的应用程序安全计划的一部分，如果使用得当，它们可以支持整个流程，以产生更安全的代码。

## 行动呼吁

如果你正在构建、设计或测试软件，我强烈建议你熟悉本书中的安全性测试指导。这是一个很好的关于今天面临的最常见应用程序问题的测试汇总，但它并不详尽。如果发现错误，请联系我们修改。这将帮助成千上万使用本指南的人。

欢迎任何一个个人或公司加入我们，这样我们才能继续创建像《安全测试指南》和其他 OWASP 项目的一样的成果。

感谢所有的在过去和未来为这份指南做出贡献的人们。你们的努力将推进并加强全球应用程序的安全性的发展。

Eoin Keary
OWASP 董事会成员
2013 年 4 月 19 日

# 序2

## 1）OWASP的宗旨：开放、协同的知识管理

在第4版OWASP测试指南中，我们创建了一个新的测试指南，它将成为指导大家执行Web应用渗透测试的事实标准。

——Matteo Meucci

OWASP感谢每一位作者、审稿者和编辑的努力，正是他们的辛勤工作才让测试指南成为今天这个样子。如果你有任何关于本测试指南的意见或建议，请发电子邮件到以下邮箱：

http://lists.owasp.org/mailman/listinfo/owasp-testing

或者直接发邮件给本指南的负责人Andrew Muller 和Matteo Meucci。

## 2）第4版OWASP测试指南

相比第3版，第4版OWASP测试指南在以下3个方面进行了改进：

①本版测试指南集成了OWASP的其他两个重要文档交付件《开发者指南》和《代码审查指南》。为了做到这一点，我们重新编排了测试类别和测试编号，以便与其他OWASP文档交付件保持一致。《测试指南》和《代码审查指南》的目的是评估《开发者指南》中所描述的安全控件是否达到了要求。

②对所有章节都进行了改进，并将测试用例数量扩展到87个（第3版只有64个），新增以下4个章节的介绍：

- 身份管理测试
- 错误处理
- 密码
- 客户端测试

③在这个版本的测试指南中，我们不仅鼓励有关机构和团体简单地接受本指南所列的测试用例，还鼓励安全测试人员与其他软件测试人员一起设计用于具体测试目标的有针对性的测试用例。如果发现了具有更广泛适用性的测试用例，我们鼓励安全机构和团体将它们分享出来，以完善本测试指南。这将有助于持续构建应用安全知识体系，使本测试指南

的开发成为不断迭代的而不是单向的过程。

### 3）历史修订

第 4 版《测试指南》发布于 2014 年。OWASP 的测试指南于 2003 年首次发布，Dan Cuthbert 作为最初的编辑之一参与其中。于 2005 年移交给 Eoin Keary 并转变成 Wiki 超文本系统。之后，Matteo Meucci 接管了本测试指南，现在是 OWASP 测试指南项目负责人。从 2012 年起 Andrew Muller 协助 Matteo Meucci 领导这个项目。

- 2014 年 OWASP 测试指南第 4 版
- 2008 年 9 月 15 日 OWASP 测试指南第 3 版
- 2006 年 12 月 25 日 OWASP 测试指南第 2 版
- 2004 年 12 月 OWASP 测试指南第 1 版
- 2004 年 7 月 14 日 OWASP Web 应用安全渗透检查表第 1.1 版

Andrew Muller

Matteo Meucci

## 项目领导

- Andrew Muller：从 2013 年开始领导 OWASP 测试指南项目
- Matteo Meucci：从 2007 年开始领导 OWASP 测试指南项目
- Eoin Keary：2005—2007 年领导 OWASP 测试指南项目
- Daniel Cuthbert：2003—2005 年领导 OWASP 测试指南项目

## 4）原版作者和校验

### 第 4 版作者

- Matteo Meucci
- Pavol Luptak
- Marco Morana
- Giorgio Fedon
- Stefano Di Paola
- Gianrico Ingrosso
- Giuseppe Bonfà
- Andrew Muller
- Robert Winkel
- Roberto Suggi Liverani
- Robert Smith
- Tripurari Rai
- Thomas Ryan
- Tim Bertels
- Cecil Su

- Aung KhAnt
- Norbert Szetei
- Michael Boman
- Wagner Elias
- Kevin Horvat
- Tom Brennan
- Tomas Zatko
- Juan Galiana Lara
- Sumit Siddharth
- Mike Hryekewicz
- Simon Bennetts
- Ray Schippers
- Raul Siles
- Jayanta Karmakar
- Brad Causey

- Vicente Aguilera
- Ismael Gonçalves
- David Fern
- Tom Eston
- Kevin Horvath
- Rick Mitchell
- Eduardo Castellanos
- Simone Onofri
- Harword Sheen
- Amro Alolaqi
- Suhas Desai
- Ryan Dewhurst
- Zaki Akhmad
- Davide Danelon
- Alexander Antukh

- Thomas Kalamaris
- Alexander Vavousis
- Christian Heinrich
- Babu Arokiadas
- Rob Barnes
- Ben Walther
- Anant Shrivastava
- Colin Watson
- Luca Carettoni
- Eoin Keary
- Jeff Williams
- Juan Manuel Bahamonde
- Thomas Skora
- Irene Abezgauz
- Hugo Costa

### 第 4 版校验

- Davide Danelon
- Andrea Rosignoli
- Irene Abezgauz
- Lode Vanstechelman
- Sebastien Gioria
- Yiannis Pavlosoglou
- Aditya Balapure

### 第 3 版作者

- Anurag Agarwwal
- Daniele Bellucci
- Ariel Coronel
- Stefano Di Paola
- Giorgio Fedon
- Adam Goodman
- Christian Heinrich
- Kevin Horvath
- Gianrico Ingrosso
- Roberto Suggi Liverani
- Kuza55

- Pavol Luptak
- Ferruh Mavituna
- Marco Mella
- Matteo Meucci
- Marco Morana
- Antonio Parata
- Cecil Su
- Harish Skanda Sureddy
- Mark Roxberry
- Andrew Van der Stock

### 第 3 版校验

- Marco Cova
- Kevin Fuller
- Matteo Meucci
- Nam Nguyen
- Rick Mitchell

## 第 2 版作者

- Vicente Aguilera
- Mauro Bregolin
- Tom Brennan
- Gary Burns
- Luca Carettoni
- Dan Cornell
- Mark Curphey
- Daniel Cuthbert
- Sebastien Deleersnyder
- Stephen DeVries
- Stefano Di Paola
- David Endler
- Giorgio Fedon
- Javier Fernández-Sanguino
- Glyn Geoghegan
- Stan Guzik
- Madhura Halasgikar
- Eoin Keary
- David Litchfield
- Andrea Lombardini
- Ralph M. Los
- Claudio Merloni
- Matteo Meucci
- Marco Morana
- Laura Nunez
- Gunter Ollmann
- Antonio Parata
- Yiannis Pavlosoglou
- Carlo Pelliccioni
- Harinath Pudipeddi
- Alberto Revelli
- Mark Roxberry
- Tom Ryan
- Anush Shetty
- Larry Shields
- Dafydd Studdard
- Andrew van der Stock
- Ariel Waissbein
- Jeff Williams
- Tushar Vartak

## 第 2 版校验

- Vicente Aguilera
- Marco Belotti
- Mauro Bregolin
- Marco Cova
- Daniel Cuthbert
- Paul Davies
- Stefano Di Paola
- Matteo G.P. Flora
- Simona Forti
- Darrell Groundy
- Eoin Keary
- James Kist
- Katie McDowell
- Marco Mella
- Matteo Meucci
- Syed Mohamed
- Antonio Parata
- Alberto Revelli
- Mark Roxberry
- Dave Wichers

# 中文版说明

本书为“OWASP Testing Guide V4.0”的中文版。该版本尽量提供原英文版本中的图片，并与原版本保持相同的风格。存在的差异，敬请谅解。

感谢 OWASP 中国及 SecZone 自 2008 年 OWASP Testing Guide V3.0 发布以来，对该项目持续的跟进、翻译研究分享。同时，也对该项目的参与人员表示感谢。

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：

电话：4000-983-183

邮箱：cwasp@seczone.org

TESTING GUIDE 项目支持单位：

OWASP 中国 The Open Web Application Security Project

SECZONE

**译者（按姓氏笔画排名）：**

| | | | |
|---|---|---|---|
| 王 玢 | 王 颉 | 王永霞 | 孙 军 |
| 刘北水 | 何伊圣 | 邹荣新 | 郑 凯 |
| 顾凌志 | 徐瑞祝 | 樊 山 | 魏建星 |

**校验（按姓氏笔画排名）：**

| | | | |
|---|---|---|---|
| RIP | 王 阳 | 包悦忠 | 许 飞 |
| 孙 军 | 刘北水 | 何伊圣 | 林怡旭 |
| 林坤潮 | 范 懿 | 袁晓峰 | 曾张帆 |

译者简介

| | |
|---|---|
| 王　玢 | 英国纽卡斯尔大学计算机安全专业硕士。现在中国太平洋保险公司信息安全部任职，从事安全运维工作 |
| 王　颉 | 英国拉夫堡大学博士，Citrix、ITIL 认证专家，近年来致力于企业信息化体系建设和软件开发全生命周期安全研究，并担任 OWASP 中国成都区负责人，先后牵头和负责了“OWASP Top 10”、“OpenSAMM”、“OWASP 安全编码规范快速参考指南”等系列项目，并参与了“CWASP 认证体系”项目 |
| 王永霞 | 现任著名云服务企业高级合规专家，CSA 云安全联盟大中华区个人会员和志愿者；曾担任英国标准协会（BSI）中国区 ICT 产品经理多年；致力于 ICT 管理领域研究和推动良好实践，近年来专注于云计算安全及云计算服务管理领域的研究与实践 |
| 孙　军 | 现任深圳云塔信息技术有限公司副总经理，云安全联盟 CSA 深圳分会秘书长，CISP、系统分析师。曾在中国电信、UT 斯达康、华为等公司从事电信行业及软件研发、市场等工作 10 余年，近年来专注于信息安全咨询、培训和服务，参与了云安全、信息技术服务 ITSS 等相关标准的制定 |
| 刘北水 | 信息安全工程师，西安电子科技大学硕士，CISSP、FreeBuf 资深作者，主要研究方向为渗透测试、逆向分析、智能硬件安全等 |
| 何伊圣 | 山石网科安全服务总监，9 年信息安全从业经历，OWASP 高级会员，SAINTSEC（原白细胞）安全团队创始人，魔方渗透测试系统作者，CNVD、CNNVD 多份原创通用高危漏洞提交者，多所华南高校的外聘信息安全教师，发表过多篇信息安全技术相关论文 |
| 邹荣新 | 有十几年的信息安全从业经验，先后在国内几家大型公司从事安全工作。参与研发多个知名的安全产品，发明过 10 多项技术专利，主导建设过大型企业的安全监控防御体系及信息安全管理体系，致力于计算机攻防对抗、云安全体系、企业安全管理实践等方向的研究 |
| 郑凯 | 北京诸元数据科技有限公司总经理，CISSP、CWASP 认证 Web 应用安全专家，北京大学硕士，2015 年创办北京诸元数据科技有限公司，通过核心技术将互联网数据、传统征信数据、案情线索整合，通过大数据关联匹配、行为建模、科学计算等技术手段，将数据结构化可视化，为公安、检察院等国家机构提供互联网信息（情报）检索产品和服务 |

| | |
|---|---|
| 顾凌志 | 华为资深安全专家，华为 SDL 应用创始人之一，擅长安全架构设计、威胁建模；长期从事移动、虚拟化及通信领域业务安全的分析和研究 |
| 徐瑞祝 | SecZone 安全开发部总监，具有 10 年安全行业从业经验。参与实施了清华大学、移动、国开行、农业银行、电科院、顺丰、携程等多家企业与机构的代码安全审核以及 S-SDLC 项目实施。目前专注于 S-SDLC 安全软件开发生命周期的推广与应用 |
| 樊　山 | 自由职业者、CISP、CISI，主要从事信息安全培训、咨询与规划设计工作。专心于信息安全培训体系的设计和教学工作，致力于信息安全体系框架设计研究和探索，需求第三只眼睛看安全的出路 |
| 魏建星 | 现就职于国内一家知名电商企业，曾服务过金融、电信、游戏等行业，2010 年在 IBM 任职时开始接触安全方向，主要兴趣为安全加密算法、SDLC 安全等，是开源项目的积极拥护者 |

# 目 录

## 第一部分 项目概述及测试框架

## 第二部分 测试方法