PHP Security

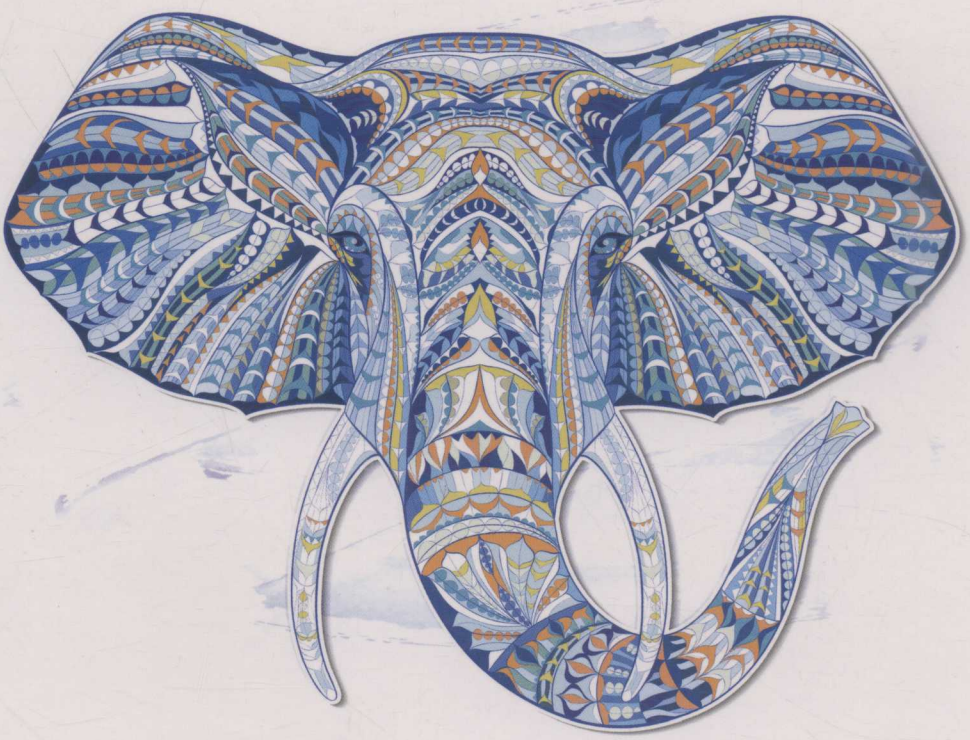
针对 PHP 研发人员的项目安全高级指南，涵盖百余种安全问题解决方案

多位 PHP 安全领域大咖联合力荐，全面引导读者探索项目更深层次的安全问题

PHP 安全之道

项目安全的架构、技术与实践

◎栾涛 著



中国工信出版集团

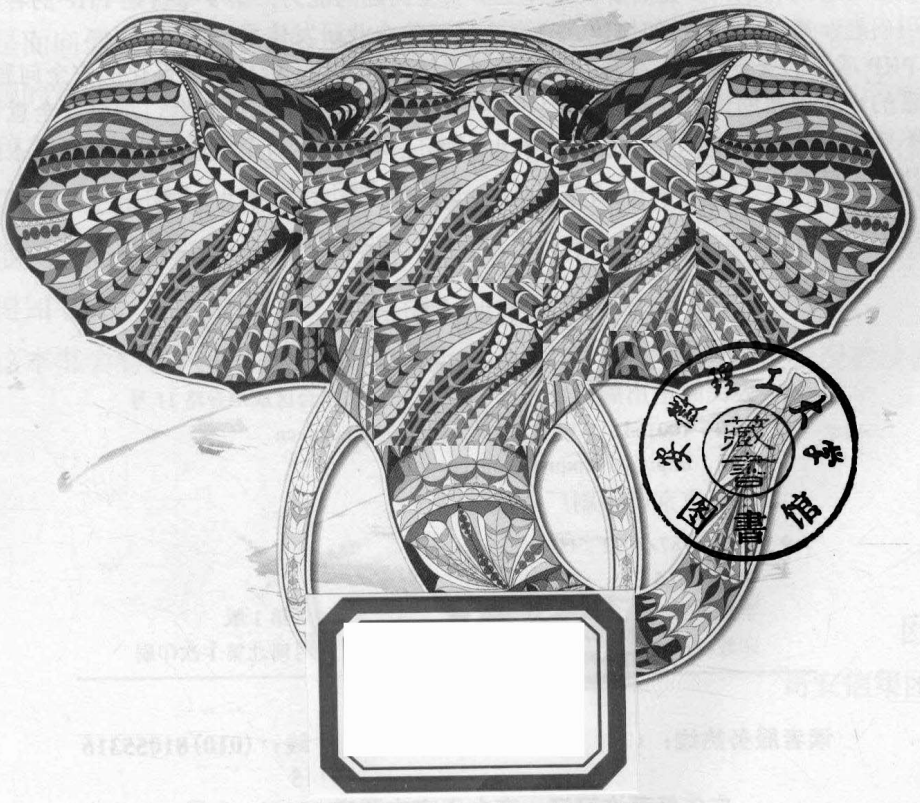
人民邮电出版社
POSTS & TELECOM PRESS

PHP Security

PHP 安全之道

项目安全的架构、技术与实践

◎栾涛 著



人民邮电出版社
北京

图书在版编目（CIP）数据

PHP安全之道 ：项目安全的架构、技术与实践 / 栾涛著. -- 北京 ：人民邮电出版社，2019.11
ISBN 978-7-115-51527-8

Ⅰ. ①P… Ⅱ. ①栾… Ⅲ. ①PHP语言－程序设计
Ⅳ. ①TP312.8

中国版本图书馆CIP数据核字(2019)第220534号

内 容 提 要

本书主要面向 PHP 研发人员，详细讲解 PHP 项目漏洞的产生原理及防范措施，帮助研发人员在项目研发过程中规避风险。

全书共有 10 章。第 1 章讲述 PHP 项目安全问题的主要形成原因以及解决 PHP 项目安全问题的原则；第 2 章讲述 PHP 项目安全的基础，以使研发人员了解 PHP 语言自身的安全机制；第 3 章通过讲解 PHP 编码过程中需要注意的安全问题，帮助研发人员正确运用 PHP 函数及变量转换；第 4 章阐述常见的漏洞并给出了相应的处理方式，涉及 SQL 注入漏洞、XML 注入漏洞、邮件安全、PHP 组件安全、文件包含安全、系统命令注入等方面，帮助研发人员在项目初期即能有效防范漏洞问题；第 5 章讲述 PHP 与客户端交互过程中存在的安全隐患及解决方案，包括浏览器安全边界、客户端脚本攻击、伪造劫持等一系列和客户端相关的安全防护；第 6 章讲述在 PHP 项目中常用的加密方式及其应用场景；第 7 章讲述 PHP 项目安全的进阶知识，帮助研发人员在更高的角度防范风险；第 8 章从 PHP 业务逻辑安全的角度讲述每个业务场景的安全防范路径，以进一步提升研发人员在 PHP 项目实战中对安全问题的认识，并提高解决具体业务安全问题的能力；第 9 章讲述 PHP 的各种支撑软件的安全应用问题；第 10 章讲述如何建立有安全保障的企业研发体系。

对于 PHP 项目的安全问题，本书不仅进行了系统性的阐释，给出了体系化的安全问题解决之道，还通过丰富的小示例帮助读者在平常工作中得以见微知著，并能防微杜渐，增强安全意识，提高安全警惕，不放过任何威胁到项目安全的“细枝末节”。因而，本书不仅适合 PHP 研发人员，也适合网络安全技术人员参阅。

◆ 著　　栾　涛
责任编辑　李　莎
责任印制　马振武

◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路 11 号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
涿州市京南印刷厂印刷

◆ 开本：787×1092　1/16
印张：19.5
字数：345 千字　　2019 年 11 月第 1 版
印数：1－2 500 册　　2019 年 11 月河北第 1 次印刷

定价：79.00 元

读者服务热线：(010)81055410　印装质量热线：(010)81055316
反盗版热线：(010)81055315
广告经营许可证：京东工商广登字 20170147 号

序 Preface

在第六届中国互联网安全大会（Internet Security Conference，ISC）前夕，从栾涛这里得知本书已完成编写，欣喜之余我认真翻阅，认为此书对改善网络安全状况具有积极意义。

IT 系统的漏洞是网络安全问题的根源，而漏洞的产生往往是 IT 系统研发人员“不知不觉”导致的，如安全意识不强、工作疏忽以及安全防范技能有所欠缺等。近几年，随着全球信息化程度及互联网化程度的提高，越来越多的系统承载在 Web 之上，所以，如果能在 Web 系统的设计、研发之初即避免漏洞，就能有效地减少网络安全问题的产生，从而在一定程度上改善整个网络的安全状况。

栾涛所著的这本书，依托他多年来在实际研发过程中所积累的宝贵经验，讲述了 PHP 项目安全研发的方方面面，深度剖析了安全问题的各种场景，能让 PHP 研发人员了解安全原理与安全风险，从而引导研发人员对 PHP 项目安全问题进行思考，提高安全意识和技能。据万维网技术调查（W3Techs）统计，全球 80% 的 Web 系统是使用 PHP 语言研发的，可见，从代码安全的角度做好 PHP 项目的意义重大。此外，目前市场上专业的安全技术类图书大多是面向信息安全人员的，面向研发人员的非常少，研发教程类图书基本上缺乏关于安全问题的章节，可以说本书将帮助 PHP 从业人员提高对 PHP 项目安全的认知。

栾涛与我在 360 企业安全集团共事期间，全程参与了漏洞扫描、安全防护、系统监控等产品研发项目，正是因为他在这些项目上的深厚积累，使得他具备了良好的安全意识与技能。客观地说，他主导研发的系统几乎很难找到安全漏洞。我曾鼓励他将安全经验整理成书，今日得知书成，特为之作序，颇感荣幸与欣慰。

我相信这本书会给广大研发人员带来很多帮助，从而为互联网安全状况的改善发挥积极作用。

欧怀谷

奇安信集团 副总裁

推荐语录
Recommend

潘剑锋 | 奇虎 360 首席安全架构师

PHP 是最流行的 Web 开发语言之一，但要找到一本关于 PHP 研发安全的优秀图书却并不容易。本书作者总结其在该领域的丰富经验，深入浅出地介绍了相关安全问题及解决之道。本书适合 PHP 研发人员、安全从业人员以及对安全攻防技术感兴趣的人员阅读。

韩天峰 | Swoole 开源项目创始人、学而思网校首席架构师

随着互联网技术的大规模应用，企业用户和个人用户的大量信息存在于网络服务中，安全问题变得越来越重要。据万维网技术调查（W3Techs）统计，全球有 80% 的网站是使用 PHP 语言编写的，而这些网站程序中或多或少会存在一些安全隐患。本书是专门为 PHP 编写的安全指南，内容详尽、细节严谨，非常值得 PHP 研发人员阅读。

刘焱 (兜哥) | 百度安全实验室 AI 安全负责人

我一直认为 PHP 是世界上最棒的开发语言之一，不仅仅是因为它使用广泛，更是因为它简洁且功能强大的语法，寥寥几行就可以完成其他语言几十行才能完成的功能。但从安全角度看，PHP 的确算不上一门让人省心的语言，各类安全漏洞让人“应接不暇”。栾涛的这本书详细介绍了 PHP 应用常见的安全问题及其防护手段，无论是对于研发人员还是对于安全工作者，都将是一本很好的工具书。

陈雷 |《PHP 7 底层设计与源码实现》图书作者

很多 PHP 研发人员在开发 PHP 应用程序时，更多的是关注业务实现，对 PHP 开发中的安全问题并没有太多关注，但安全隐患往往不少，一旦出现安全问题，则会带来非常严重的后果。目前虽然有很多安全技术方面的图书，但专注于 PHP 安全的图书和资料较为匮乏，而本书的出版可谓是及时雨，我相信它能给 PHP 研发人员提供很好的帮助，使其在安全问题方面少走很多弯路。

刘健皓 | 奇虎 360 智能网联汽车安全事业部负责人

随着科技发展和产业升级，软件开发正在重新定义整个世界，互联网、大数据、人工智能等技术改变了人们的生活方式。但是软件是由人编写的，是人就有可能犯错误，不可

避免地会出现安全漏洞。与此同时，由于安全漏洞造成的安全风险也将威胁到世界、威胁到国家、威胁到人们的人身及财产安全。这本书由栾涛这位曾服务于奇虎 360 企业的资深安全技术人员，根据自己丰富的实战经历总结著作而成，其内容实用，结构清晰，言简意赅，可读性强。通过阅读此书，研发人员可以在 PHP 程序开发过程中提高信息安全意识，并能主动地全面考虑安全问题，以避免漏洞的产生，让编写出来的代码更为安全、可靠。总之，这是一本值得 PHP 研发人员学习参考的图书。

王枭卿 | 奇安信网站安全事业部负责人

很高兴可以读到这样一本从研发角度出发，分享在实际工作中所积淀的安全编程心得的图书。本书涉及 PHP 项目中多种应当重视的安全问题，因而它作为 PHP 研发人员提升安全认识、实现安全编程的参考用书，再合适不过了。

白健 | 补天平台（全国最大的漏洞响应平台之一）负责人

作为一名资深的 Web 安全产品开发者，栾涛结合自己多年的工作经验，对 PHP 语言的安全问题进行了深入浅出的分析和总结。这本书系统地介绍了研发人员如何有效规避 PHP 项目的安全问题，是广大 PHP 研发人员的案头宝典！

马勇（znsoft） | 网络空间安全博士

PHP 犹如网站开发语言中的瑞士军刀，灵活方便却充满危险性。本书从安全角度描述了 PHP 开发中所需要规避的风险，让 PHP 新手和高级研发人员都能开发出成熟稳健的后台程序，从而能更好地使用这把锋利的瑞士军刀。

王晶（半桶水） | 滴滴出行高级架构师

随着互联网的发展，信息越来越透明，但随之而来的巨大挑战却是安全问题，涉及信息、数据、隐私等方面。作为在奇虎 360 企业奋战于信息安全一线的“先锋战士”，栾涛敏锐地洞察到：与其出了问题再“亡羊补牢”，不如在应用软件开发之初防患于未然。因而他便以“PHP 项目如何安全地研发”为切入点，将自己多年在项目研发和安全防范工作中积累的知识与经验记录下来，并进行全面的归类整理，编写成此书。该书详细介绍了各类 PHP 项目安全问题到底是如何产生的，又该如何解决，其知识点讲解透彻，实战性强，我认为不只 PHP 项目研发人员需要仔细研读，几乎所有基于 Web 的项目研发人员都能从中获益。

李强 | 中国科学技术大学计算机学院博士

我从 1999 年开始使用 Linux 操作系统进行研发工作，在这过程中自然而然地接触到 LAMP 架构中的 PHP、Perl 和 Python 等语言，其中 PHP 以灵活性好、开发速度快、适用场景广令我印象深刻，而我也使用 PHP 成功开发了嵌入式的打印机管理系统及普通 Web 系统等多个产品。栾涛多年来一直从事 Web 安全研发工作，技术功底深厚，我非常欣喜地看到他能将自己在 PHP 项目安全方面所积累的弥足珍贵的经验编写成此书，我相信该书在信息安全方面会给 PHP 研发人员带来一种崭新的工作视角。

吉跃奇 | 滴滴企业级事业部总经理

在企业业务系统设计上，我始终坚持安全第一，持续优化体验，不断提升效率的工作准则。PHP 简单易学，开发效率高，为企业业务系统的实现提供了强大的支撑，但随着业务体量的不断增长，安全则成为重中之重。该书集中梳理 PHP 项目中可能存在的安全风险，帮助 PHP 研发人员提高安全意识，使其有意识亦有能力守住安全红线，避免所开发的项目因安全问题造成严重损失，从而为企业的系统安全更好地保驾护航。

石东海 | 滴滴高级技术总监

PHP 因简单易学和研发效率高而备受程序员关注，越来越多的大型平台使用 PHP 作为主要研发语言，但 PHP 历来被大家诟病的安全问题，给平台的信息安全和交易安全带来了巨大的风险。栾涛在多年的业务系统研发过程中，累积了大量实战经验，经过体系化的思考和梳理，编写了此书。本书言简意赅，深入浅出，不仅完整介绍了 PHP 安全问题的全貌和漏洞原理，而且结合实际应用场景，详细介绍了各类问题的解决方案，是一本难得的既有理论高度，又能指导实际工作的 PHP 安全研发宝典，非常值得推荐。

高磊（安恺） | 阿里巴巴安全运营专家

“安全编码”是企业应用安全软件生命周期中非常重要的一环，因而让研发人员更好地理解和实现安全开发，一直是安全从业者努力的方向。栾涛从研发视角出发，结合多年关于信息安全的学习和实践经验编写了这本书。该书对于 PHP 项目安全问题的条分缕析，能很好地帮助研发人员深刻认识到“风起于青萍之末”，并拥有一定的防微杜渐之能，这对企业的安全建设无疑具有非常重要的作用。

前言 Foreword

作为资深的 PHP“码农”，多年来无论面对多么复杂的项目，我总是能带领研发团队顺利攻破难关，满足各种需求，甚至超出预期。但是无论多么努力，总是会出现各种安全问题，我自己也一直被安全问题所困扰。因此，我一直在寻觅面向研发人员的项目安全类图书，但是不尽如人意。市场上针对各种漏洞进行挖掘的图书应有尽有，所面向的读者大都是白帽子、信息安全人员，提供给研发人员，帮助其对系统进行加固、防止漏洞产生的安全类图书却很少。

安全无小事，企业系统应根据自己的业务特点，建立安全红线，特别是在涉及人身、资金、敏感信息等方面，需要在效率、增长、系统性能做出取舍的情况下，确保把安全放在第一位。

如果一个企业连基本的人身、资金、敏感信息等方面的安全都不重视，那么一旦出现问题，就会给企业造成致命的伤害。如果漏洞被攻击者发现并利用，造成的人身损害、企业名誉损失、资金损失、信息损失等基本上是无法弥补的。

在网络安全问题日益突出的今天，必须对网站系统的安全加以重视。只要加以重视，大部分安全问题就可以在系统的研发阶段消灭掉。然而，大多数研发人员只注重代码功能的实现，没有考虑到业务的安全问题，也没有考虑到编码的安全问题，这将给企业和互联网带来严重的安全隐患。

因一个很好的机遇，我加入了奇虎 360 企业，非常幸运地和很多安全专家一起共事，这使我对安全有了新的认知，同时也丰富了我的安全知识。在不断学习中，我将研发项目时积累的经验记录下来汇成此书，希望能给 PHP 研发人员提供帮助。

本书的定位

本书面向的读者是 PHP 研发人员。经统计，90% 的安全问题是由于研发人员缺乏安全意识造成的。本书阐述了一些漏洞的产生原理及防范措施，希望可以帮助 PHP 研发人员提高安全意识。本书不是为了让研发人员去做一个白帽子或者攻击者，而是为了更好地帮助研发人员进行系统的安全加固，在项目的研发过程中重视项目安全，合理编码，从根本上解决 PHP 项目的安全问题。

致谢

能认识欧总（欧怀谷）是我的荣幸，感谢欧总在工作上对我的悉心指导，并将多个 Web 安全业务交给我负责，这对我经验的积累以及编写此书起着决定性作用。非常感谢欧总在百忙之中为本书题写序言。

栾　涛

名词解释

漏洞 | 指一个系统存在的弱点或缺陷，可能来自应用软件或操作系统设计时的缺陷或编码时产生的错误，也可能来自业务在交互处理过程中的设计缺陷或逻辑流程上的不合理之处。

漏洞可能被有意或无意地利用，从而对一个组织的资产或运行造成不利影响，如信息系统被攻击或控制、重要资料被窃取、用户数据被篡改、系统被作为入侵其他主机系统的跳板。

白帽子 | 也称为白帽黑客，指能够识别计算机系统或网络系统中安全漏洞的安全技术专家，但他们并不会恶意利用漏洞，而是提交给企业，帮助企业在被其他人恶意利用之前修补漏洞，以维护计算机和互联网安全。

攻击者 | 本书中统一将针对缺陷实施攻击的人称为攻击者。这里的缺陷，包括软件缺陷、硬件缺陷、网络协议缺陷、管理缺陷和人为失误。

目录

Contents