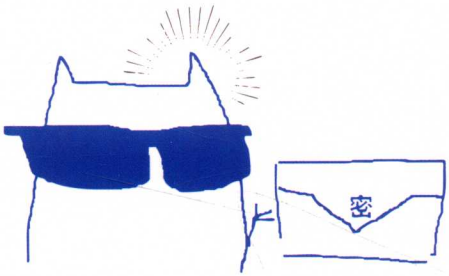
从常见的网络攻击入手，介绍代码安全、前端脚本安全、后端应用安全、账户安全、加解密及认证技术、SQL注入以及服务器配置防护等安全知识，以案例揭示安全漏洞并提供解决方案。

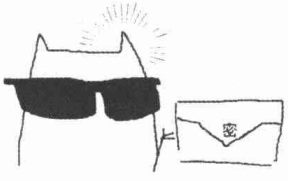


揭示安全漏洞，提供解决方案

PHP Web 安全开发实战

汤青松 / 编著

清華大學出版社



PHP Web 安全开发实战

汤青松 / 编著

清华大学出版社
北京

内 容 简 介

本书结合在安全方面的开发经验，站在开发者的角度，循序渐进地介绍了大量实际发生的漏洞案例，并给出了技术解决方案，包括：常见的网络攻击、代码安全、前端脚本安全、后端应用安全、账户安全、加解密认证、SQL 注入以及服务器配置等内容。通过阅读本书，读者能够对整个网络安全有一个全新的认识和深入的理解，从而成为一位懂安全、会防护的工程师，避免在工作中成为黑客攻击的对象。

本书适合 PHP 开发人员、网络维护人员以及对网络安全攻防技术感兴趣的读者阅读。

图书在版编目（CIP）数据

PHP Web 安全开发实战/汤青松编著. —北京：清华大学出版社，2018
ISBN 978-7-302-51127-4

Ⅰ. ①P… Ⅱ. ①汤… Ⅲ. ①网页制作工具—PHP 语言—程序设计 Ⅳ. ①TP393.092②TP312

中国版本图书馆 CIP 数据核字（2018）第 202142 号

责任编辑： 王金柱
封面设计： 王　翔
责任校对： 闫秀华
责任印制： 丛怀宇

出版发行： 清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn

印 装 者： 北京密云胶印厂
经　　销： 全国新华书店
开　　本： 180mm×230mm　　**印　　张：** 14　　**字　　数：** 314 千字
版　　次： 2018 年 10 月第 1 版　　**印　　次：** 2018 年 10 月第 1 次印刷
定　　价： 59.00 元

产品编号：077352-01

推荐序 1

随着互联网的快速发展以及大量中小型互联网公司的出现，网络用户数也在不断增长，用户安全意识不断提升，人们越来越注重个人隐私及数据安全的防护，出现用户密码泄露、隐私外泄、财产损失等都是不能忍受的。

目前大多数中小型公司都在用 PHP 开发 Web 端，但这些公司往往缺乏安全相关的技术团队来为网络安全方面提供技术保障。尤其在开发过程中，工程师忽略安全方面的考虑，导致线上网站服务器出现各种安全漏洞，留下安全隐患，对用户和公司都会造成不同程度的损失。

加上近些年各大互联网公司陆续曝出被攻击的安全问题，大量账户和密码泄露。例如有些用户在很多网站都使用同一账户和密码，使得黑客更容易破解他在其他网站的账户信息。类似问题让企业在安全性方面面临严峻挑战，可以说一个网站没有安全，就像没有穿衣服一样，它是裸露透明的，一丝不挂，毫无隐私和保障可言。

纵观市场，很少有类似结合实际案例著作的 Web 安全方面的图书，本书正是基于此，总结作者在安全方面的经验，循序渐进地讲述大量实际发生的案例以及处理方案，来应对各种新奇的攻击技术。从常见的网络攻击、代码安全、前端脚本安全、后端应用安全、账户安全、加解密及认证、SQL 注入以及服务器配置防护等方面提供了比较成熟的技术解决方案。

通过阅读本书能够帮助读者对整个网络安全有一个全新的认识和质的提升，从而成为一位懂安全、会防护的工程师，避免在工作中成为黑客的攻击对象。

总之，这是开发工程师在安全方面不可多得的一本网络安全图书，值得一读。

爱卡汽车高级工程师 张锋

推荐序 2

安全是一个系统工程，涉及项目管理、架构设计、代码编写等方面。一位合格的开发人员除了要有安全意识外，还要掌握一些安全编程的知识点。这本书为开发人员介绍了一些 Web 安全的基础知识，分别以原理、实践两个方面进行了阐述，Web 安全入门简单，重要的是实践和积累。

看雪学院（kanxue.com）创始人　段钢

前　言

在准备写这本书的时候参考了很多 Web 安全方面的资料和书籍，我发现很多书籍和资料都是从攻击者的角度来讲述 Web 安全的。为了防止本书和其他的书籍以及相关资料同质化，在规划本书的时候，特意从 PHP 开发者的角度出发，目的是让开发者提升安全开发的能力，书中会讲到目前 Web 安全中的常见漏洞、相关的漏洞案例、最佳的安全防范方法，以及我自己的观点，希望能帮到需要提升安全知识的 PHP 从业者。

本书内容

第 1 章　信息泄露

此书面向安全意识薄弱的开发者，因此在第 1 章中带领读者入门，主要介绍攻击者在攻击服务器时在前期如何探查服务器信息，攻击者有哪些手段来挖掘漏洞，让读者能够快速了解漏洞是如何被发现的。

第 2 章　常规漏洞

讲解开发者在编码过程中，因缺乏安全意识或遗漏而导致的安全问题；同时通过生动的案例分析来说明攻击者是如何发现此类安全问题的；最后在章节末尾会提到开发者如何规避这些编码导致的安全问题。

第 3 章　业务逻辑安全

在设计一些业务的时候，不仅编码会产生安全漏洞，业务同样会产生大问题，比如常见的越权漏洞、支付漏洞、验证码问题，这些问题其实在设计功能之初就应该考虑到项目计划中去。

第 4 章　LANMP 安全配置

对于 PHP 开发者来说，一定离不开 Nginx、Apache、MySQL、PHP、Redis 等配置，不过这些配置并不会经常用到，通常是配置一次，后面就不用再理会。这也导致了开发者因为对配置的陌生而出现不少安全问题，本章会总结出因为配置不当而带来的安全问题，同时也会给出正确的安全配置建议。

第 5 章　认证与加密

在进行业务开发的过程中，我们很频繁地使用加密与解密，但对其底层原理却了解得甚少，甚至部分开发者无法分清认证与加密的区别，本章主要介绍加密和认证的相关技术，以帮助开发人员了解其技术特点，从而开发出安全的应用。

第 6 章　其他 Web 安全主题

攻击者的攻击方式是多样的，我们在防范安全问题的同时，一定要有重点目标，所以本章会提到漏洞的危险等级划分、CMS 引起的漏洞如何防御、对自身的业务如何安全测试、在测试的同时如何提升效率，本章还会介绍两款经典的安全检测工具：Burp Suite 和 SQLMap，让读者能够对自己开发的产品进行安全检测。

本书读者对象

这本书面向懂 PHP 开发但不擅长安全方面的开发者，可以通过此书让你在 Web 安全方面快速成长，在书中列出了很多互联网的漏洞案例，目的是让读者看了之后更加了解攻击者是如何发现漏洞的，从而让开发者在开发时能够对症下药。

由于编者水平有限，虽已尽力，但书中肯定还会存在许多不妥甚至谬误，敬请广大读者和专家不吝指教，非常感谢。

联系邮箱地址：booksaga@126.com。

汤青松

2018 年 4 月于北京

目　录

第1章

信息泄露

安全是一个整体，不在于强大的地方有多强大，而在于弱小的地方有多弱。一个系统被攻击的原因有很多，比如有信息泄露、编码问题、业务逻辑问题、配置不当等方面，而其中信息泄露是一个不小的原因。攻击者要入侵一个网站，首要就是收集目标的更多信息，其中有些信息对于开发者来说或许并不在意，但攻击者获取这些信息之后却可以以更低成本攻击系统，比如当攻击者得到该站点的端口信息之后，就可以分析出目标网站提供了哪种服务，再对这些服务的弱点进行定向攻击。

本章将从一个攻击者的角度来分析攻击者收集信息的意义以及利用的方法，包括主机信息泄露、源码信息、弱口令信息，希望可以通过本章的内容让读者了解攻击者是如何收集服务器信息的，从而把一些以往容易忽视的地方重视起来。

1.1 主机信息

一个网站被攻击，通常情况是指服务器主机受到了攻击，而要攻击服务器主机，首要的操作就是收集服务器的弱点信息，这些信息包括子域名收集、端口信息、域名注册信息、网站管理地址，本节将介绍攻击者收集主机信息的方法。

1.1.1 子域名信息

子域名是指顶级域名、一级域名或父域名的下一级，域名整体包括两个“.”或包括一个“.”和一个“/”。在攻击者收集信息时，首先就是发现目标，而通过子域名收集的方式可以迅速发现更多目标主机，找到更多目标则能挖掘出更多弱点信息，比如当发现某域名存在一个admin.xxx.com子域名后，就大致可以推测此域名是网站后台，这样攻击者就可能围绕着后台来进行攻击，所以对于攻击者来说，子域名收集可以很大程度地降低攻击成本。

现在假设要查询bing.com域名还有多少子域名，攻击者会怎么做呢？下面来看一下常见的域名收集方式。

1. 浏览器访问

浏览器访问是判断一个子域名是否存在的最简单的方法，例如通过浏览器尝试子域名api.bing.com 是否可以访问，如果服务器返回的状态码为200，就说明目标地址是存在的，表示子域名可以访问。如果是其他状态码，那么可以对应HTTP状态码来判断。有关HTTP状态码可参考百度百科“HTTP状态码”的内容。如图1-1所示，表示子域名api.bing.com不可以访问，如图1-2所示表示子域名可以访问。

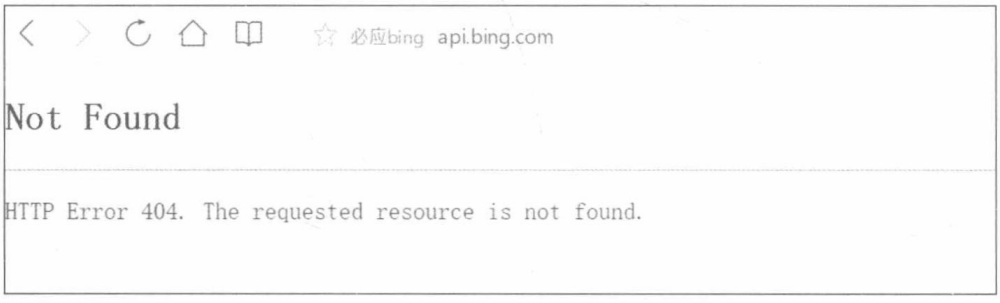


图 1-1 子域名 api.bing.com 不可以访问

图 1-2 子域名可以访问

2. 搜索引擎查找

如果不知道域名有多少个子域名，想寻找域名下有多少子域名，可以借助搜索引擎的查询指令来帮且寻找，比如site:songboy.net。在如图1-3所示中，我们可以看到根域名site:songboy.net下百度记录了5个子域名。

图 1-3　site:songboy.net 域名下的子域名

3. Layer

攻击者在对目标有强烈的渗透欲望时，就会更加愿意花费时间，因此会用一些工具来辅助，虽然下载工具麻烦一些，不过挖掘效果确实更加好。

工具“Layer子域名挖掘机”是一款使用.NET开发的Windows平台软件，Layer可以用来快速查找子域名信息。如果没有安装.NET环境，在Windows 10环境打开会自动安装，网速比较好的情况下安装时间在5分钟左右。

安装好之后打开界面，如图1-4所示，需要输入目标网址，单击“开始”按钮就可以在下面的列表中看到挖掘到的子域名结果，在Windows系统中操作起来非常方便。

图 1-4 Layer 子域名挖掘机操作界面

4. wydomain

工具“wydomain”是白帽子“猪猪侠”开发的一款子域名挖掘工具（如图1-4所示），该工具可以通过命令行交互来获取子域名信息，目前在GitHub开源，项目地址为：https://github.com/ring04h/wydomain。wydomain的帮助文档如图1-5所示。

```
$ python dnsburte.py –h
usage: dnsburte.py [-h] [-t] [-d] [-f] [-o]
wydomian v 1.2.0 to bruteforce subdomains of your target domain.
optional arguments:
-h, --help          show this help message and exit
-t , --thread       thread count
-d , --domain       domain name
-f , --file         subdomains dict file name
-o , --out          result out file
```

图 1-5 wydomain 的帮助文档

wydomain是基于Python开发的，在运行的时候需要先安装Python环境，挖掘的原理是基于常见的子域名字典探测，工具中默认提供一些字典表，如果使用者想自己添加也非常方便，把需要挖掘的子域名放到CSV文件中即可。wydomain的帮助文档如图1-5所示。

字典是指一个包含很多密码的文本文件，攻击者常用相关软件将数字、字母、符号等按照特定组合方式生成字典文件，然后通过特定软件使用字典中的密码不断尝试，直到成功。该过程被称为暴力破解，也叫穷举或跑字典。

扫描域名的过程及扫描结果如图1-6和图1-7所示。

```
$ python dnsburte.py -d songboy.net -f dnspod.csv -o songboy.log
2018-01-05 22:24:29,845 [INFO] starting bruteforce threading(16) : songboy.net
2018-01-05 22:26:16,186 [INFO] dns bruteforce subdomains(134) successfully...
2018-01-05 22:26:16,186 [INFO] result save in : C:\Users\Administrator\
Desktop\wydomain-wydomain2\songboy.log (11001u.songboy.net', 'A', '<timeout>')
```

图 1-6　扫描域名的过程

```
[
    "11001u.songboy.net",
    "16.songboy.net",
    "13.songboy.net",
    "13.songboy.net",
    "176.songboy.net",
    "178896.songboy.net",
    "18.songboy.net",
    "2.songboy.net",
    "2.songboy.net",
```

图 1-7　扫描后的结果

1.1.2　端口信息

攻击者欲找到目标，最常用的方法就是端口扫描。顾名思义，端口扫描就是逐个对一段端口或指定的端口进行扫描。攻击者可以通过扫描结果知道一台计算机上都提供了哪些服务，之后可以通过所提供服务的已知漏洞进行攻击，比如当攻击者发现服务器开放了80端口，就知道服务器提供了Web服务；再比如当发现开放了3306端口，则可以判断服务器安装了MySQL服务，此时攻击者就会从Web服务和MySQL服务的弱点进行攻击。

1. 端口扫描原理

当一个攻击者向服务器的一个端口发起建立连接的请求时，如果服务器提供此项服务就会应答，如果服务器未提供此项服务，即使攻击者向相应的端口发出请求，服务器也是不会应答的。

利用这个原理，攻击者对所有熟知的端口分别建立连接，并记录下远端服务器所返回的内容，最后查看一下记录就能知道目标服务器上都安装了哪些服务，这就是端口扫描，通过端口扫描，攻击者就可以搜集到关于服务器的各种很有参考价值的信息。