

# 《代码审计》

## 图书基本信息

书名：《代码审计》

13位ISBN编号：9787111520068

出版时间：2015-11-24

作者：尹毅

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：[www.tushu000.com](http://www.tushu000.com)

# 《代码审计》

## 内容概要

代码审计是企业安全运营以及安全从业者必备的基本技能。本书详细介绍代码审计的设计思路以及所需要的工具和方法，不仅用大量案例介绍了漏洞挖掘方法，而且在代码层和功能设计层剖析了各种安全漏洞的成因与预防策略。对应用开发人员和安全技术人员都有参考价值。

### 主要内容

- 代码审计前的准备，包括代码审计前需要了解的PHP核心配置文件以及PHP环境搭建的方法。
- 代码审计需要的工具，以及这些工具的详细使用方法。
- PHP代码审计中漏洞挖掘的思路与防范方法。
- 常见漏洞的审计方法，涵盖SQL注入、XSS、CSRF、文件操作、代码/命令执行、变量覆盖、会话认证以及逻辑处理等等漏洞。
- 二次漏洞的挖掘方法，以及代码审计过程中的一些常用技巧。
- 介绍如何写出更安全的代码，包括参数的安全过滤、常用的加密算法、功能的安全设计、应用安全体系构建等。

## 书籍目录

代码审计：企业级web代码安全架构

I

前言

IV

导读

VI

致谢和感言

IX

目录

XI

第1章

代码审计环境搭建

1.1

wamp/wnmp环境搭建

1.2

lamp/lmp环境搭建

1.3

PHP核心配置详解

第2章

审计辅助与漏洞验证工具

2.1

代码编辑器

2.1.1

notepad++

2.1.2

UltraEdit

2.1.3

Zend Studio

2.2

代码审计工具

2.2.1

Seay源码审计系统

2.2.2

Fortify SCA

2.2.3

RIPS

2.3

漏洞验证辅助

2.3.1

burp suite

2.3.2

浏览器扩展

2.3.3

编码转换及加解密工具

2.3.4

正则调试工具

2.3.5

SQL执行监控工具

第3章

通用代码审计思路

3.1

敏感函数回溯参数过程

3.1.1

espcms注入挖掘案例

3.2

通读全文代码

3.2.1

骑士cms通读审计案例

3.2.1.1

查看应用文件结构

3.2.1.2

查看关键文件代码

3.2.1.3

查看配置文件

3.2.1.4

跟读首页文件

3.3

根据功能点定向审计

3.3.1

Bugfree重装漏洞案例

第4章

漏洞挖掘与防范（基础篇）

4.1

SQL注入漏洞

4.1.1

挖掘经验

4.1.1.1

普通注入

4.1.1.2

编码注入

4.1.1.2.1

宽字节注入

4.1.1.2.2

二次urldecode注入

4.1.1.3

espcms搜索注入分析

4.1.2

漏洞防范

4.1.2.1

gpc/runtime魔术引号

4.1.2.2

过滤函数和类

4.1.2.2.1

addslashes函数

4.1.2.2.2

mysql\_[real\_]escape\_string函数

4.1.2.2.3

intval等字符转换

4.1.2.3

PDO prepare预编译

4.2

XSS漏洞

4.2.1

挖掘经验

4.2.1.1

反射型XSS

4.2.1.2

存储型XSS

4.2.1.3

骑士CMS 存储型XSS分析

4.2.2

漏洞防范

4.2.2.1

特殊字符HTML实体转码

4.2.2.2

标签事件属性黑白名单

4.3

CSRF漏洞

4.3.1

挖掘经验

4.3.1.1

Discuz csrf备份拖库分析

4.3.2

漏洞防范

4.3.2.1

Token验证

4.3.2.2

验证码验证

第5章

漏洞挖掘与防范（进阶篇）

5.1

文件操作漏洞

5.1.1

文件包含漏洞

5.1.1.1

挖掘经验

5.1.1.2

本地文件包含

5.1.1.2.1

远程文件包含

5.1.1.2.2

文件包含截断

5.1.1.2.3

Metinfo文件包含漏洞分析

5.1.2

## 文件读取(下载)漏洞

### 5.1.2.1

#### 挖掘经验

#### 5.1.2.1.1

#### phpcms任意文件读取分析

### 5.1.3

## 文件上传漏洞

### 5.1.3.1

#### 挖掘经验

#### 5.1.3.1.1

#### 未过滤或本地过滤

#### 5.1.3.1.2

#### 黑名单扩展名过滤

#### 5.1.3.1.3

#### 文件头、content-type验证绕过

#### 5.1.3.1.4

#### phpcms任意文件上传分析

### 5.1.4

## 文件删除漏洞

### 5.1.4.1

#### 挖掘经验

#### 5.1.4.1.1

#### Metinfo任意文件删除分析

### 5.1.5

## 文件操作漏洞防范

### 5.1.5.1

#### 通用文件操作防御

### 5.1.5.2

#### 文件上传漏洞防范

## 5.2

## 代码执行漏洞

### 5.2.1

#### 挖掘经验

#### 5.2.1.1

#### 代码执行函数

#### 5.2.1.1.1

#### eval和assert函数

#### 5.2.1.1.2

#### preg\_replace函数

#### 5.2.1.1.3

#### 调用函数过滤不严

### 5.2.1.2

#### 动态函数执行

### 5.2.1.3

#### Thinkphp代码执行漏洞分析

### 5.2.2

#### 漏洞防范

## 5.3

## 命令执行漏洞

- 5.3.1 挖掘经验
  - 5.3.1.1 命令执行函数
  - 5.3.1.2 反引号命令执行
  - 5.3.1.3 亿邮命令执行漏洞分析
- 5.3.2 漏洞防范
  - 5.3.2.1 命令防注入函数
  - 5.3.2.2 参数白名单
- 第6章 漏洞挖掘与防范（深入篇）
  - 6.1 变量覆盖漏洞
    - 6.1.1 挖掘经验
      - 6.1.1.1 函数使用不当
        - 6.1.1.1.1 extract函数
        - 6.1.1.1.2 parse\_str函数
        - 6.1.1.1.3 import\_request\_variables函数
      - 6.1.1.2 \$\$变量覆盖
      - 6.1.1.3 Metinfo变量覆盖漏洞分析
    - 6.1.2 漏洞防范
      - 6.1.2.1 使用原始变量
      - 6.1.2.2 验证变量存在
  - 6.2 逻辑处理漏洞
    - 6.2.1 挖掘经验
      - 6.2.1.1 等于与存在判断绕过
        - 6.2.1.1.1 in\_array函数
        - 6.2.1.1.2 is\_numeric函数
        - 6.2.1.1.3

双等于和三等于

6.2.1.2

账户体系中的越权漏洞

6.2.1.3

未exit或return引发的安全问题

6.2.1.4

常见支付漏洞

6.2.1.5

Ecshop逻辑错误注入分析

6.2.2

漏洞防范

6.3

会话认证漏洞

6.3.1

挖掘经验

6.3.1.1

Cookie认证安全

6.3.1.2

Espcms任意用户登录分析

6.3.2

漏洞防范

第7章

二次漏洞审计

7.1

什么是二次漏洞

7.2

二次漏洞审计技巧

7.3

dedecms二次注入漏洞分析

第8章

代码审计小技巧

8.1

钻GPC等转义的空子

8.1.1

不受GPC保护的全局变量

8.1.2

编码转换问题

8.2

神奇的字符串

8.2.1

字符处理函数报错信息泄露

8.2.2

字符串截断

8.2.2.1

%00空字符截断

8.2.2.2

iconv函数字符编码转换截断

8.3

php:// 输入输出流

- 8.4
- PHP代码解析标签
- 8.5
- FUZZ漏洞发现
- 8.6
- 不严谨的正则表达式
- 8.7
- 十余种MySQL报错注入
- 8.8
- Windows FindFirstFile利用
- 8.9
- PHP可变变量
- 第9章
- 参数的安全过滤
- 9.1
- 第三方过滤函数与类
- 9.1.1
- discuz SQL安全过滤类分析
- 9.1.2
- discuz xss标签过滤函数分析
- 9.2
- 内置过滤函数
- 第10章
- 使用安全的加密算法
- 10.1
- 对称加密
- 10.1.1
- 3DES加密
- 10.1.2
- AES加密
- 10.2
- 非对称加密
- 10.2.1
- RSA加密
- 10.3
- 单向加密
- 10.3.1
- md5/sha1加密
- 第11章
- 业务功能安全设计
- 11.1
- 验证码
- 11.1.1
- 验证码绕过
- 11.1.2
- 验证码资源滥用
- 11.2
- 用户登录
- 11.2.1

撞库漏洞

11.2.2

API登录

11.3

用户注册

11.4

密码找回

11.5

资料查看与修改

11.6

投票/积分/抽奖

11.7

充值支付

11.8

私信及反馈

11.9

远程地址访问

11.10

文件管理

11.11

数据库管理

11.12

命令/代码执行

11.13

文件/数据库备份

11.14

API接口

第12章

应用安全体系建设

12.1

用户密码安全策略

12.2

前后台用户分表

12.3

后台地址隐藏

12.4

密码加密存储方式

12.5

登入限制

12.6

API站库分离

12.7

慎用第三方服务

12.8

严格的权限控制

12.9

敏感操作多因素验证

12.10

应用自身的安全中心

附录  
网站推荐

# 《代码审计》

## 精彩短评

- 1、整理挺全的，不过不够深入。
- 2、php安全防御指南
- 3、内容不错，但为啥是php的？
- 4、web安全，代码审计。至今没挖到一个洞
- 5、比较入门,适合有点PHP基础
- 6、国内少有的专注代码审计的书籍，只是太简单了一些，而且基本都是针对php安全的，企业级web里的java和c#去哪了。不过作者写的php代码审计工具还是蛮好用的，功能集成比较好，但挖洞还是得靠自己积累。
- 7、一个正常的作者会告诉你有漏洞的软件是什么版本，可以到哪下载，漏洞怎么复现，但是本书的作者并没有这样做。
- 8、php代码审计、漏洞挖掘与编码安全入门书。

# 《代码审计》

## 版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:[www.tushu000.com](http://www.tushu000.com)