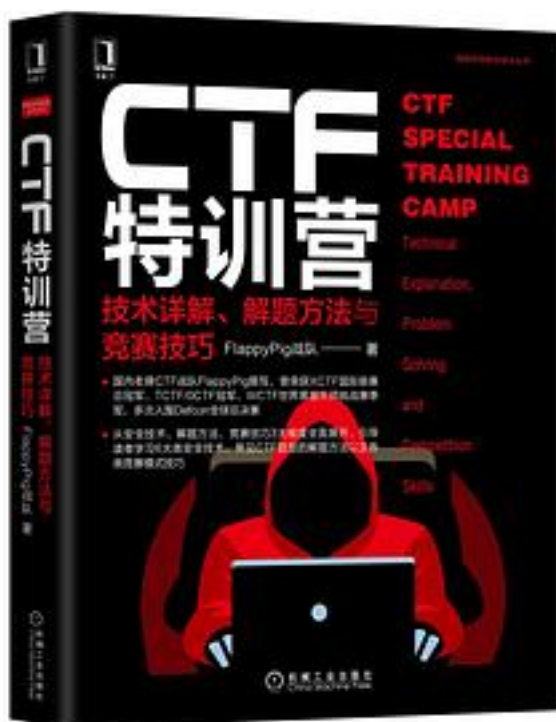


CTF特训营:技术详解、解题方法与竞赛技巧



[CTF特训营:技术详解、解题方法与竞赛技巧 下载链接1](#)

著者:FlappyPig战队

出版者:机械工业出版社

出版时间:2020-6-25

装帧:平装

isbn:9787111657354

本书由国内老牌CTF战队FlappyPig撰写，战队成员曾多次荣获XCTF国际联赛冠军、TCTF/OCTF冠军、WCTF世界黑客大师挑战赛季军，多次入围Defcon全球总决赛，具有丰富的实战经验。

本书围绕CTF竞赛需要的安全技术、解题方法和竞赛技巧3个维度展开，旨在通过作者扎实的技术功底和丰富的竞赛经验，引领对CTF竞赛感兴趣的读者快速入门。书中依据CTF竞赛的特点，分别从Web、Reverse、PWN、Crypto、APK、IoT这6个方面系统地对CTF竞赛的知识点、模式、技巧进行了深入讲解，每一篇都搭配历年真题，帮助读者加深理解。

全书一共分六篇。

Web篇（第1~8章）

主要讲解CTF比赛中Web类型题目的基础知识点与常用的工具和插件，这些知识点和工具也可以用于部分渗透测试的实战中。

Reverse篇（第9~10章）

主要讲解CTF中逆向分析的主要方法、常用分析工具、逆向分析技术和破解方法，帮助读者提高逆向分析能力。

PWN篇（第11~17章）

对PWN二进制漏洞挖掘与利用的详细分析，主要讲解了针对各种漏洞的利用方法和利用技巧，读者可以结合实例题目加深理解。

Crypto篇（第18~22章）

对Crypto类型题目的知识和例题讲解，主要从概述、编码、古典密码、现代密码以及真题解析几个方向阐述。

APK篇（第23~25章）

讲解CTF中APK的相关内容，主要从APK的基础知识点、Dalvik层的逆向分析技术，以及Native层的逆向分析技术3个方面介绍APK题目的基础内容、解题方法和竞赛技巧。

IoT篇（第26~30章）

对IoT类型题目的讲解，内容涉及IoT、无线通信的基础知识和相关题型的解题技巧，帮助读者培养解决IoT相关题目的能力。

作者介绍:

FlappyPig

国内老牌知名CTF战队，曾获数十个各级CTF竞赛冠亚季军，具备国际CTF竞赛水准，具备丰富的CTF参赛经验。先后获得XCTF联赛总冠军、XNUCA总决赛冠军、CISCN冠军、TCTF/0CTF（Defcon外卡赛）冠军、WCTF世界黑客大师挑战赛季军，连续三年闯进Defcon决赛，Defcon最好成绩第10名。战队开发维护了用于CTF赛事评级的CTFRank网站。

现在以r3kapiG联合战队的方式参赛。

战队成员挖掘并披露漏洞获得CVE编号上百枚，向各类SRC报备漏洞数百个。战队成员在Geekpwn、天府杯、PWN2OWN等漏洞挖掘类竞赛中也取得了不错的成绩。

战队主要成员目前就职于阿里巴巴、腾讯、京东等，从事网络安全、漏洞挖掘相关工作。在网络安全竞赛、漏洞挖掘、渗透测试等领域具有非常深厚的经验积累，擅长Web、应用层软件、操作系统、区块链、嵌入式等多领域的漏洞挖掘与利用。

目录: 前言

第一篇 CTF之Web

第1章 常用工具安装及使用 2

1.1 Burp Suite 2

1.2 Sqlmap 8

1.3 浏览器与插件 9

1.4 Nmap 11

第2章 SQL注入攻击 13

2.1 什么是SQL注入 13

2.2 可以联合查询的SQL注入 14

2.3 报错注入 14

2.4 Bool 盲注 16

2.5 时间盲注 17

2.6 二次注入 18

2.7 limit之后的注入 20

2.8 注入点的位置及发现 20

2.9 绕过 21

2.10 SQL读写文件 24

2.11 小结 24

第3章 跨站脚本攻击 25

3.1 概述 25

3.2 常见XSS漏洞分类 25

3.3 防护与绕过 29

3.4 危害与利用技巧 38

3.5 实例 40

第4章 服务端请求伪造 42

4.1 如何形成 42

4.2 防护绕过 43

4.3 危害与利用技巧 43

4.4 实例 46

第5章 利用特性进行攻击 48

5.1 PHP语言特性 48

5.1.1 弱类型 48

5.1.2 反序列化漏洞 49

5.1.3 截断 51

5.1.4 伪协议 51

5.1.5 变量覆盖 52

5.1.6 防护绕过 54

5.2 Windows系统特性 54

第6章 代码审计 56

6.1 源码泄露 56

6.2 代码审计的方法与技巧 61

第7章 条件竞争 67

7.1 概述 67

7.2 条件竞争问题分析及测试 68

第8章 案例解析 73

8.1 NSCTF 2015 Web实例 73

8.2 湖湘杯2016线上选拔赛Web实例 75

8.3 OCTF 2017 Web实例 79

8.4 2019 WCTF 大师赛赛题剖析： P-door 80

本篇小结 87

第二篇 CTF之Reverse

第9章 Reverse概述 90

- 9.1 逆向分析的主要方法 90
- 9.2 汇编指令体系结构 91
 - 9.2.1 x86指令体系91
 - 9.2.2 x64指令体系92
- 9.3 逆向分析工具介绍 93
 - 9.3.1 反汇编和反编译工具93
 - 9.3.2 调试器97
 - 9.3.3 Trace类工具100
- 第10章 Reverse分析 102
 - 10.1 常规逆向分析流程 102
 - 10.1.1 关键代码定位102
 - 10.1.2 常见加密算法识别104
 - 10.1.3 求解flag109
 - 10.2 自动化逆向 113
 - 10.2.1 IDAPython114
 - 10.2.2 PythonGdb114
 - 10.2.3 pydbg115
 - 10.2.4 Angr115
 - 10.3 干扰分析技术及破解方法 116
 - 10.3.1 花指令116
 - 10.3.2 反调试117
 - 10.3.3 加壳119
 - 10.3.4 控制流混淆121
 - 10.3.5 双进程保护124
 - 10.3.6 虚拟机保护127
 - 10.4 脚本语言的逆向 132
 - 10.4.1 .NET程序逆向132
 - 10.4.2 Python程序逆向135
 - 10.4.3 Java程序逆向137
- 本篇小结 139
- 第三篇 CTF之PWN
- 第11章 PWN基础 142
 - 11.1 基本工具 142
 - 11.2 保护机制 143
 - 11.3 PWN类型 143
 - 11.4 常见利用方法 144
 - 11.5 程序内存布局 149
 - 11.6 真题解析 150
- • • • • [\(收起\)](#)

[CTF特训营:技术详解、解题方法与竞赛技巧 下载链接1](#)

标签

ctf

好书，值得一读

信息安全

计算机科学

大神

安全

Security

服务网格

评论

花了五年耕耘出来的书.. 其实还是有很多不足的地方

在CTF这条路上，希望有书籍为伴，一路成长

FlappyPig 永远滴神

国内首本CTF赛事技术解析书籍，我们等了5年，终于，，，

CTF新人，一本入门的好书

CTF赛题出书了，可以系统学习了

又是一本干货满满的书

看了书的目录，满满干货，五百多页厚厚实实的一本。

ctf小白，从第一篇开始学，还是很不错的，但总体仍是类似大纲性的引导。比如最近在看的sql注入，很多东西只有短短一页，但其实内容很多，需要结合网上其他的资料，而且缺乏原理讲解和实例分析。
但总体瑕不掩瑜，毕竟一本书想要包含ctf所以内容是不可能的，还需要自己不断扩充。

读一本好书是在同伟人交流，读一本好的CTF书，胜似在同仰慕的大师傅们交流学习。

第一本

[CTF特训营:技术详解、解题方法与竞赛技巧_下载链接1](#)

书评

CTF是安全从业人员入门和进阶非常好的方式，寓学于练，以练促学，打一场好的CTF竞赛如洗筋易髓。本书以拔尖题目为骨，化知识体系为肉，覆盖了安全攻防技术的方方面面，实战与理论结合，深入浅出，娓娓道来，不仅适合对CTF感兴趣的初学者，更适合想在安全技术上精进的每位技术人...

国内首本CTF赛事技术解析书籍，五年之约，兑现了！
每一个CTF战队的发展其实都面临着一个问题，那就是“如何传承”。作为一个联合战队，随着老成员走向工作岗位，如何用良好的机制实现新老更替，是战队管理者需要认真考虑的问题。我们也尝试过在社会上公开招募成员，但是从他们...

