Python 灰帽子：黑客与逆向工程师的 Python 编程之道

中文名: Python 灰帽子：黑客与逆向工程师的 Python 编程之道
原名: Gray Hat Python: Python Programming for Hackers and Reverse Engineers
作者: Justin Seitz
图书分类: 软件
资源格式: PDF
版本: 英文文字版/更新源代码
出版社: O'Reilly
书号: 978-1593271923
发行时间: 2009年04月01日
地区: 美国
语言: 英文
下载地址：http://python.ttlearn.net/tushu/python_huimaozi.html

内容介绍：

本书是由知名安全机构 ImmunityInc 的资深黑帽 JustinSeitz 先生主笔撰写的一本关于编程语言 Python 如何被广泛应用于黑客与逆向工程领域的书籍.老牌黑客,同时也是 Immunity Inc 的创始人兼首席技术执行官(CT0)Dave Aitel 为本书担任了技术编辑一职。本书的绝大部分篇幅着眼于黑客技术领域中的两大经久不衰的话题：逆向工程与漏洞挖掘，并向读者呈现了几乎每个逆向工程师或安全研究人员在日常工作中所面临的各种场景，其中包括：如何设计?构建自己的调试工具，如何自动化实现烦琐的逆向分析任务，如何设计与构建自己的 fuzzing 工具，如何利用 fuzzing 测试来找出存在于软件产品中的安全漏洞，一些小技巧诸如钩子与注入技术的应用，以及对一些主流 Python 安全工具如 PyDbg、Immunity Debugger、Sulley、IDAPython、PyEmu 等的深入介绍。作者借助于如今黑客社区中备受青睐的编程语言 Python 引领读者构建出精悍的脚本程序来——应对上述这些问题。出现在本书中的相当一部分 Python 代码实例借鉴或直接来源于一些优秀的开源安全项目，诸如 Pedram Amini 的 Paimei，由此读者可以领略到安全研究者?是如何将黑客艺术与工程技术优雅融合来解决那些棘手问题的。

本书适合热衷于黑客技术，特别是与逆向工程与漏洞挖掘领域相关的读者，以及所有对 Python 编程感兴趣的读者阅读与参考。

目录:

6: Hooking
7: DLL and Code Injection
8: Fuzzing
9: Sulley
10: Fuzzing Windows Drivers
11: IDAPython -- Scripting IDA Pro
12: PyEmu -- The Scriptable Emulator