# 安全书单

原创

pumpkin.zhu 于 2021-04-10 19:43:55 发布 63 收藏

分类专栏： 追随大师



本文链接：https://blog.csdn.net/soldi_er/article/details/115582830





## 文章目录



---

## MS08067实验室

MS08067实验室在不断地编写安全书籍，目前已出版的书籍如下，从目录看很不戳：

| 书名 | 出版时间 | 作者 |
| --- | --- | --- |
| 《Web安全攻防:渗透测试实战指南》 | 2018-07 | 徐焱，李文轩，王东亚 |
| 《内网安全攻防:渗透测试实战指南》 | 2019-12 | 徐焱，贾晓璐 |
| 《Python安全攻防:渗透测试实战指南》 | 2020-09 | 吴涛，方嘉明，吴荣德，徐焱 |

值得肯定的是，该实验室做了一份安全书单，Web方面有本《Web前端黑客技术揭秘》看起来有点意思，安全编程方面有C++编程和Python编程书籍等。

网站地址https://www.ms08067.com/

## 反思

### 安全从业人员欠缺什么？

个人觉得，最欠缺的就是系统化的学习。

大学环境：在校期间很讨厌理论知识，觉得最重要的是实战。因为学校的课程一般都是讲解某方面的入门知识，基本缺乏进阶的知识，导致产生一种看书也就那样的“经验”。

行业特殊性：安全漏洞立足于程序的非预期执行情况，这意味着安全只是编程世界的一角，历史上的知识多半是零零散散的。但是显而易见的，系统化的训练对专业能力而言是必不可少的，东一榔头西一棒槌的学习方式只会让你流于技术表面并导致平庸。

自学跟上课是完全不同的两个概念，这意味着学习终于不再是填鸭和浅尝辄止，我们有了深入了解某方面知识、甚至研究某个领域的可能性。

目前的实战经验仍然不足，书籍和实战的比例3:7比较合适。

### 发展阶段

入门靶场阶段，初次接触学习漏洞知识，只会看Writeup打靶。长则一个学期。

熟练打靶阶段，可以自己做一些简单的靶场，具有靶场通关的经验，某方面知识串联起来，对某方面知识有一定的理解，但还没有深入到原理层面。初步审计代码，勉强分析pop链。偶尔部署环境，耗时一天复现某个CVE漏洞。长则一个学期。

实战打点入门阶段，熟练部署环境，复现漏洞不再是问题。对不同的实战场景有了些许概念，开始审计代码查看某方面知识的原理。开始有意识地学习和模仿一些技术文章，接触的不再都是入门知识。开始实战，初步使用和对比安全工具，擅长通过网络空间绘测工具、扫描器等查找、探测和利用某个特定漏洞。开始有意识地进行系统化学习。长未知

开始有意识地关注安全圈子，关注安全团队和安全大佬，与安全人才多交流探讨。

实战打点熟练/内网入门阶段。审计并深刻理解常规漏洞原理，擅长漏洞的扫描探测和利用，能够比较全面地测试指定网站。熟练掌握各种安全工具，开发自己的工具小有所成。。开始尝试投稿，在安全平台发布一些技术文章。开始近距离接触安全大佬，有了稍微的地位，不再是一个小透明。

内网熟练阶段。或渗透测试编程阶段。

---

## 数据库书籍

《MySQL注入天书》-连载文章，发布平台是先知社区。

《网络攻防实战研究：MySQL数据库安全》-陈小兵，2020年10月出版。

消息来源：Ms08067安全实验室公众号