《Web应用安全权威指南》阅读计划

——黑客与安全群阅读计划（第1期）

领读人：Herry

本书特色

- Web安全入门书，涉及Web安全的大部分方面
- 随书有虚拟机环境，可以边看边练，形成直观印象，激发学习兴趣

适合读者

Web安全初学者，对安全感兴趣的任何人

总阅读时长：3周

每天阅读用时：3小时

答疑时间安排

每周三晚 21:00—23:00，每日阅读有问题也可以在群内 @herry 交流。

图灵社区本书网址：http://www.ituring.com.cn/book/1249

图灵阅读计划网址：https://github.com/BetterTuring/turingWeChatGroups

阅读建议

按照书的内容，多练，想明白这个安全问题形成的原因，利用的方法，防御的方法，绕过的方法。

阅读规划

第一部分（第1—3章）

阅读时长：1周

重点内容

1. Web安全的基本概念
2. 实验环境的搭建

难点内容

1. 理解Web安全基础知识
2. 会话管理的机制
3. 理解同源机制是下一步理解XSS、CSRF等攻击的基础

补充

Web是很灵活的，概念和标准可以参考《HTTP权威指南》。

第二部分（第4—6章）

阅读时长：1周

重点内容

1. 分类介绍各种Web安全问题
2. 针对Web攻击的防御措施

难点内容

1. Web攻防的基本技巧
2. Web应用中繁杂的编码问题
3. SQL注入的基本技巧，从最明显、最简单的方法到一系列高级的攻击机巧（如带外通道、推断和时间延迟）
4. 其他注入攻击方式：命令执行注入、脚本注入、路径遍历、文件包含、注入XML
5. 针对电子邮件的攻击方式
6. 反射型XSS、存储型XSS和DOM XSS的攻击技巧与防御方法
7. CSRF与XSS的异同

补充

关于Web攻防可以延伸阅读《黑客攻防技术宝典：Web实战篇》。

第三部分（第7—8章）

阅读时长：1周

重点内容

1. 在HTTP外的领域讨论Web安全
2. Web安全生命周期的管理

难点内容

1. Web安全外延知识面的扩充
2. Web安全防御方法论
3. 在Web应用中探查本地漏洞，包括：缓冲区溢出、整数漏洞、格式化字符串漏洞
4. 在共享环境情境下的Web安全防护技术

补充

Web安全是个很泛的概念，不只在HTTP协议下讨论，它的范围甚至延展到Web构件的二进制领域，以及各种相关协议的逆向分析等。