《黑客攻防技术宝典：浏览器实战篇》阅读计划

——图灵黑客与安全群阅读计划（第1期）

领读人：zusheng（第1—5章），土八路（第6—11章）

本书特色

- 细致讲解了IE、Firefox、Chrome 等主流浏览器及其扩展和应用上的安全问题和漏洞，介绍了大量的攻击和防御技术。
- 基本按攻击方法划分，具体内容主要包括初始控制、持续控制、绕过同源策略、攻击用户、攻击浏览器、攻击扩展、攻击插件、攻击Web 应用、攻击网络等。

适合读者：计算机安全技术人员及浏览器开发人员

总阅读时长（预估）：45—60天

每天阅读用时：2小时以上

答疑时间安排：每周六晚图灵黑客与安全群 20:00—22:00

图灵社区本书网址：http://www.ituring.com.cn/book/1379

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

阅读规划

第 1 章　浏览器安全概述

阅读时长：4—6小时

重点 & 难点

1. 浏览器基础概念
   熟悉浏览器基础概念，对后续学习浏览器安全有重要意义。
2. 沙箱

浏览器和其他应用程序中保护安全的一种组件关系设计模式

3. 同源策略
   浏览器最核心也最基本的安全功能

补充

- 一定要理解各个概念的**核心思想**，技术细节太难的部分可以根据自身能力适当跳过。
- **其他参考书籍**：《HTTP权威指南》

第 2 章　初始控制

阅读时长：6~8小时

重点 & 难点

- 主要介绍了控制初始化的概念以及如何去实现初始控制

补充

- 对于浏览器了解较少的读者，建议**第一遍阅读时只掌握思想和实现方式**，之后再针对原理做深入学习。
- **其他参考书籍**：《JavaScript编程精粹》

第 3 章　持续控制

阅读时长：8~10小时

重点 & 难点

- 控制持久化

  持续控制目标可以大致分为两个方面，一方面是持久通信，另一方面就是持久存续。
- 通信技术
  理解各种通信渠道的工作原理，如 XMLHttpRequest 轮询、WebSocket 通信。
- 持久化技术
  一些持久化通信渠道的方法，如使用内嵌框架、浏览器事件等。

补充

- 跟着书上的实例实现案列后建议**自己再做一些修改**，多多实践理解其中的概念
- **其他参考书籍**:《Web性能权威指南》

第 4 章 绕过同源策略 & 第 5 章 攻击用户

阅读时长：14—16 小时

重点 & 难点

1. 同源策略概念以及一些绕过方法
   SOP即同源策略，SOP是浏览器安全的关键，研究绕过SOP技术非常重要。
2. 浏览器事件
   在捕获用户输入上，浏览器事件能帮我们干很多事情，所以需要了解一些基本的事件及功能。

补充

- 可以开始参考各领域的相关书籍、博客、论文等资料进行深入学习。
- **其他参考书籍**
  - 《黑客攻防技术宝典：Web实战篇（第2版）》

> *我是土八路，本书从第6章到最后由我跟大家共读、探讨与交流。*

第6章 攻击浏览器

阅读时长：6—8小时

重点内容

1. 利用DOM属性、浏览器可能触发的 Bug 及浏览器的特有行为采集浏览器的指纹
2. 了解 Cookie 的原理及它们的特点，介绍如何在复杂的浏览器攻击中利用 Cookie
3. 探讨HTTP降级攻击、证书攻击和 SSL/TLS 攻击
4. 针对 JavaScript 的一些攻击方法
5. 通过Metasploit渗透框架获取系统上的shell

难点内容

1. 灵活运用采集浏览器指纹的各种方法
2. 掌握JavaScript的攻击方法

补充

需要掌握HTTP请求和响应中的HTTP首部

第7章 攻击浏览器扩展

阅读时长：8—10小时

重点内容

1. 介绍什么是扩展，以及不同浏览器中的扩展有什么不同
2. 介绍了几种采集扩展指纹的方法
3. 介绍了几种攻击扩展的方法

难点内容

1. 掌握主流浏览器中扩展的区别
2. 掌握几种扩展的攻击方法

补充

这一章探讨如何利用浏览器扩展的隐患，LastPass、Firebug、AdBlock和NoScript都是常见的扩展。

第8章 攻击浏览器插件

阅读时长：8—10小时

重点内容

1. 介绍什么是插件以及它与扩展的区别
2. 介绍了几种采集插件指纹的方法
3. 介绍了几种攻击插件的方法

难点内容

- 如何举一反三的使用插件攻击技术

补充内容

流行的插件包括Acrobat Reader、Flash Player、Java、QuickTime、RealPlayer、Shockwave和Windows Media Player。

第9章 攻击Web应用

阅读时长：10—15小时

重点内容

1. 如何发现跨域Web应用
2. 如何发现内部设备IP地址和内部域名
3. 跨域 Web 应用指纹的采集方法
4. 如何实现跨域认证检测
5. 如何利用跨站点请求伪造
6. 如何实现跨域资源检测
7. 如何实现跨域 Web 应用漏洞检测
8. 如何启动拒绝服务攻击
9. 如何发动 Web 应用利用

难点内容

1. 如何进一步伪装隐蔽自己，并访问那些位于内部网中不能路由到的Web应用
2. 如何识别和利用跨域漏洞

第10章 攻击网络

阅读时长：10—12小时

1. 如何对目标开展侦察包括确定内网、检测活动主机、扫描主机端口
2. 采集非 HTTP 服务的指纹
3. 如何攻击非 HTTP 服务
4. 获取shell

难点内容

- 对网络实施攻击的流程

第11章 思考与总结