

Web入门

作者：中山大学W4terDr0p战队成员 Pazuris

Web安全综述

相对于其他方向，web方向所需要学习的内容偏多，涉及到各类编程语言与开发框架，漏洞的类型也偏多，但是不用担心，web方面的安全研究并不会过于深入开发的底层原理，也并不会涉及太多开发的高级应用。

那么，选择web安全作为安全的学习方向有哪些理由呢？

- 以后好找工作，web应用普及在各个领域，市场需求大
- 个人认为web安全比较有趣味性，基本思想是绕过检测并执行命令，像是Assassin（刺客）
- 学习web安全不用过多考虑计算机的底层原理

如果你经过综合考量，最终决定选择Web方向的学习，那么接下来这份学习路线也许可以帮助你少走一些入门的弯路。

正式学习Web前的准备

首先，千万不要一上来就急着去看web方向的常见漏洞（sql注入，文件上传等等），你需要先进行前置知识的学习（先要有装备才能打怪），否则你很有可能看不懂网上的任何一篇研究这些漏洞的文章。

前置的web技术基础知识包括HTML，CSS，JavaScript，Http，Python，PHP，linux基础操作，下面是详细的学习资料推荐，最好的学习方法就是看一遍敲一遍，并且对不懂的知识点多上网查询，也可以问问chatgpt，最好还可以做做笔记。

做笔记的话推荐使用软件Typora，然后稍微学一点markdown语法就可以。

HTML+CSS+JS

这三样被称为前端三件套，由于网站最直观呈现给我们看的就是前端的代码（F12或者右键查看源代码），所以拥有前端代码基础显得尤为重要。

但是应该注意，我们并不需要对这三种语言进行深入研究，只需要达到能大致看懂网页代码的水平 and 知道基础操作就行，并不需要我们真正去开发前端页面。

三种语言中，又以JavaScript最为重要，宜花较多时间学习，css最为不重要，看看就好。

推荐的学习资料

推荐b站 遇见狂神说 的前端三件套

[【狂神说Java】HTML5完整教学通俗易懂哔哩哔哩bilibili](#)

[【狂神说Java】CSS3最新教程快速入门通俗易懂哔哩哔哩bilibili](#)

[【狂神说Java】JavaScript最新教程通俗易懂哔哩哔哩bilibili](#)

视频讲解废话很少，通俗易懂，而且时长较短，只需要把视频看完，代码跟着敲一遍，就算是已经掌握了这些基本的知识。

HTTP

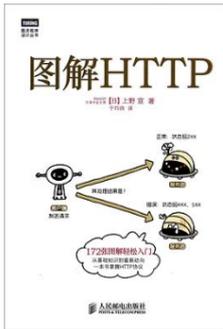
HTTP是web应用程序中最基本的协议之一，它定义了Web浏览器和Web服务器之间的通信方式，学习HTTP可以帮助我们更好地了解web应用程序的基本结构，且很多web基本的漏洞（XSS和CSRF）都是基于HTTP协议的。而且对于计算机类专业的学生来说，计网是必修课，迟早要学。

但是在这个阶段，我们先重点了解http协议即可，毕竟计网本身涉及的知识过多，先学习web安全必需的前置知识就好。

推荐的学习资料

不要一上来就看那种很厚的《计算机网络》之类的书，很有可能看不下去，我推荐看的书是上野宣的图解HTTP，讲的很有趣而且通俗易懂，非常适合新手入门。

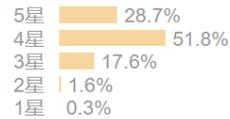
图解HTTP



作者: [日] 上野宣
出版社: 人民邮电出版社
出品方: 图灵教育
原名: HTTPの教科書
译者: 于均良
出版年: 2014-4
页数: 308
定价: 49.00元
装帧: 平装
丛书: 图灵程序设计丛书·图解与入门系列
ISBN: 9787115351531

豆瓣评分

8.1  3342人评价



想读

在读

读过

评价: ☆☆☆☆☆

[写笔记](#) [写书评](#) [加入购书单](#) [分享到](#)

推荐

内容简介 ·····

本书对互联网基石——HTTP协议进行了全面系统的介绍。作者由HTTP协议的发展历史娓娓道来，严谨细致地剖析了HTTP协议的结构，列举诸多常见通信场景及实战案例，最后延伸到Web安全、最新技术动向等方面。本书的特色为在讲解的同时，辅以大量生动形象的通信图例，更好地帮助读者深刻理解HTTP通信过程中客户端与服务器的交互情况。读者可通过本书快速了解并掌握HTTP协议的基础，前端工程师分析抓包数据，后端工程师实现REST API、实现自己的HTTP服务器等过程中所需的HTTP相关知识点本书均有介绍。

这本书在网上很容易找到电子版，稍后群里也会发。

Python与PHP

Python和PHP的代码基础也很重要，因为这两是web方向最常用到的两种语言，在前置知识阶段，只需要了解语法基础，能看懂简单的代码就可，不用真的用python去力扣上刷题，也不需要PHP去写一个网站的后端架构。

推荐的学习资料

[100天精通Python从入门到就业 袁袁袁袁满的博客-CSDN博客](#)

这个看到第28天就行，后面暂时先不用看，100天只要9.9，文章质量还是很过关的，按需开通专栏吧，其他免费的也挺好，但是没那么全和详细

[PHP语言基础知识（超详细） SeaOf0的博客-CSDN博客](#)

这个就一篇文章，看完就行

[Python3 教程 | 菜鸟教程\(runoob.com\)](#)

菜鸟教程这个网站上也有很多基本语法的教学，可以查阅。

linux基础

只需要了解基础的linux命令如ls, cat等等即可，因为网站的服务器多数都是linux系统，在攻击服务器的时候需要我们对linux也有一定的了解。

推荐自己使用vmware workstation装一个虚拟机，然后学习一下基本操作。

[Linux常用操作命令大全linux常用命令星星@点点的博客-CSDN博客](#)

[小白 虚拟机,kali Linux安装 详细教程kali linux安装教程热气, 腾腾的博客-CSDN博客](#)

开始学习Web的基本漏洞类型

常见的：

SQL注入、文件上传、XSS跨站、文件包含、反序列化、代码执行、逻辑安全、未授权访问

稍微少一点的

CSRF、SSRF、目录遍历、文件读取、文件下载、命令执行、XXE漏洞

这些基本漏洞类型是web安全研究的重中之重，需要花较多的时间来学习并进行练习。

推荐的学习资料与练习网站

b站小迪安全系列视频，虽然看起来很多，但是看完真的会很有收获！可以跟着他的讲课内容做笔记，以后自己回顾的时候也比较好。

<https://www.bilibili.com/video/BV1JZ4y1c7ro/>

还可以在[CSDN - 专业开发者社区](#)上面输入对应的漏洞类型，然后选择标题里有全总结字样的，然后仔细慢慢看，做一点笔记。

在学习完一个漏洞后，最好可以加以实践，从而更好地掌握，常见的刷题练习可以通过靶场如

sqlilabs学习sql注入漏洞：[Sqli-labs介绍、下载、安装 - lcamry - 博客园\(cnblogs.com\)](#)

这种靶场需要自己搭建，同时也可以使用在线的刷题网站进行练习，选择你想要学习的漏洞的标签，然后做比较简单的题即可。

[ctf.show](#)：对web入门非常好，提供了大量循序渐进的例题，缺点是要钱，可以几个人合买一个vip

<https://www.nssctf.cn/problem>：不用充钱，收录了很多比赛的题，有难度提示有标签分类

[BUUCTF在线评测\(buuoj.cn\)](#)：不用充钱，题目质量较高，但是没有难度提示且没有标签分类且难的题比较多，新手可以做第一第二面，后面的推荐有点基础再来做

等你把这些基本漏洞类型学的差不多的时候，恭喜你，已经不再需要入门手册的指引，你已经是一位合格的web方向选手了！

总结语

学web安全，其实广度远比深度重要，重在的是多积累。新手入门最容易犯的一个误区就是一说到一个知识点，就一头扎进去，很久都不出来，比如python入门到就业看到了第一百天，然后直接去搞python开发不做安全了（），这样很容易就会让你感到疲乏和厌倦，事实上并不需要研究得这么深，很多知识其实都是了解即可。特别是刚入门的时候，千万不要花费过多的时间和精力去研究前置知识。

另外不要总是盲目相信和使用工具，工具固然好，也需要自己分析，自己理解原理，不然题目稍微变形就无法解决。

多在网上搜索相关资料，可以在google和bing上搜索，baidu就尽量不要使用了（），也可以直接在csdn上搜索，更推荐一些基础的知识点直接问chatgpt，他会解释得非常详细。

多记笔记，记录下自己当时学习的东西和想法，日后再遇到相似的知识点时也许你会庆幸自己做了笔记。

个人小博客，记录所学所思所想，欢迎来访问：<https://pazuris.cn>

如果在web学习上遇到了什么问题也欢迎来问我和tel：[11nyz-tel.cc](tel:11nyz-tel.cc)或者其他学web的人

最后，衷心祝福各位选择了web方向的同学都能走得更远！！