

Web安全

一本书不用看完，实践第一

白帽子讲web安全(各种漏洞的综述，很多都是需要自己再去找资料研究的)
web前端黑客技术揭秘(前端漏洞的更详细说明)
web之困:现代Web应用安全指南(web浏览器安全解析)

黑客攻防技术宝典:Web实战篇(第2版)
xss跨站脚本攻击剖析与防御
SQL注入攻击与防御

基本技能

会查官方文档/Google
编程语言速览
正则表达式
c/c++/STL
python:python cookbook(第三版/第二版)/python核心编程(第三版/第二版)
VPS/Linux/WinServer
Git
Linux Shell

工具

神器:中国菜刀/mimikittenz/mimikatz
http(s)截取:BrupSuite/Fiddler
抓包:Wireshark/Tcpdump
sql注入:Sqlmap(with tamper)
整体扫描/利用:AWVS/Nmap/Nessus/Metasploit
爆破:Hydra
完整性检查:Binwalk
chrome/firefox 插件:hackbar/postman/live http header/firebug/Modify Headers/EditThisCookies/...

基础

从前端到上线至少来一遍

HTML(5)/JavaScript/ECMAScript/CSS
PHP/MySQL/MSSQL
Java/Spring/Struct
Python3/Python2/Sqlite:爬虫/数据处理/EXP
Apace/Nginx/IIS/Tomcat
SSH/RDP

可以再去研究研究的:Mongodb/Redis/Django/Flask/Go/Ruby/...

<http://navisec.it/>
wooyun挂掉了，但是你还是能看到内容
题库wechall，其他题库找各种安全训练网站和CTF平台