

本文为CSDN博主「lady_killer9」的原创文章，遵循CC 4.0 BY-SA版权协议，转载请附上原文出处链接及本声明。

原文链接: https://blog.csdn.net/lady_killer9/article/details/106791542

博主b站账号:[lady_killer9](#)

相关网站推荐

博主研究方向为安全领域，以后可能更多的在圈子内发表文章，提高文章质量。

1、[FreeBuf](#)

国内关注度最高的全球互联网安全媒体平台，爱好者们交流与分享安全技术的社区，网络安全行业门户。

个人账户: lady_killer9

2、[看雪](#)

看雪论坛是个软件安全技术交流场所，为安全技术爱好者提供一个技术交流平台 and 资源。

个人主页: [lady_killer9](#)

3、[吾爱破解](#)

吾爱破解论坛是致力于软件安全与病毒分析的非营利性技术论坛。

4、[阿里云先知社区](#)

一个开放型技术平台。

个人主页:[ladykiller9](#)

5、[腾讯玄武安全实验室](#)

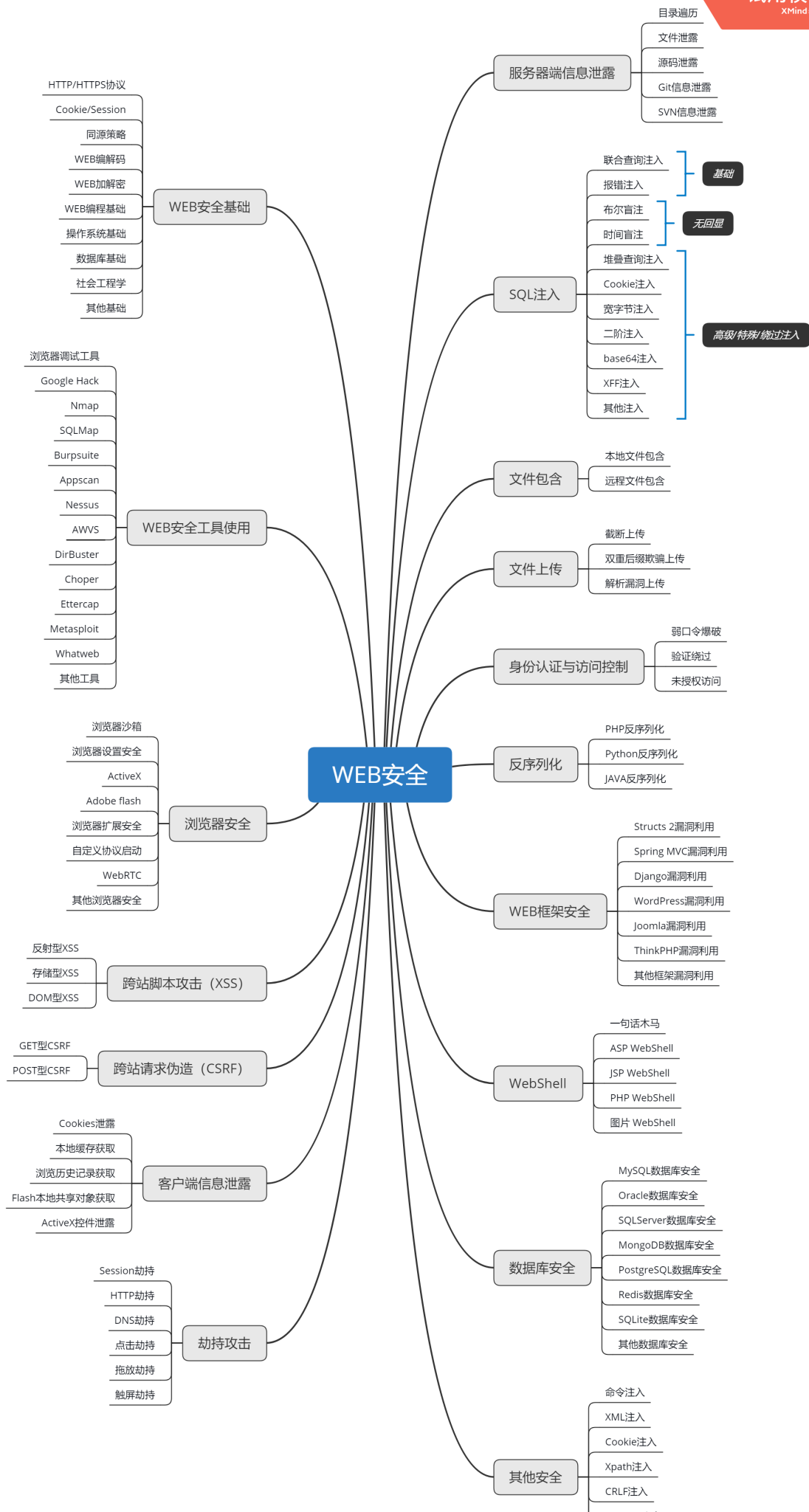
各种CVE，漏洞。

6、<https://www.sec-wiki.com/index.php>

安全维基，各种安全资讯。

WEB（应用）安全

学习路线



想法：分别学习各个模块，搭建靶机进行练习，做CTF中的WEB安全题，然后再看懂后台代码，为什么会有漏洞，接下来复现一些CVE制作成镜像给看雪等CTF比赛官方，最后学习metasploit等软件，以宏观的角度，从情报搜集开始到漏洞利用做整个渗透报告，最后将靶机的漏洞危险程度由low->impossible（感觉并没有那么多时间...慢慢来吧）。和我一起来学习WEB安全吧！！！！

推荐

书籍

入门

1. 《白帽子讲Web安全》 2012
2. 《Web安全深度剖析》 2015
3. 《Web安全攻防 渗透测试实战指南》 2018

进阶

1. 《WEB之困-现代WEB应用安全指南》 2013
2. 《内网安全攻防渗透测试安全指南》 2020
3. 《Metasploit渗透测试魔鬼训练营》 2013
4. 《SQL注入攻击与防御》 2010
5. 《黑客攻防技术宝典-Web实战篇（第2版）》

网站

- [web学习笔记](#)
- [安全词汇 RFC-4949](#)

接下来开始学习，理论并非纯理论，也有靶机攻击举例，实战一般使用离线或线上靶机。

在线靶场

- [国钧CTF](#)
- [BUUCTF](#)
- [bugku](#)
- [网络信息安全攻防平台](#)

基础

web安全必备：

[网络安全-php安全知识点](#)

[网络安全-WEB中的常见编码](#)

[跨域请求-jsonp和cors](#)

学xss注入时再看也可:

[网络安全-js安全知识点与XSS常用payloads](#)

学sql注入时再看也可:

[网络安全-Mysql注入知识点](#)

漏洞排行:

[OWASP TOP 10](#)

XSS攻击

-----理论-----

[网络安全-跨站脚本攻击\(XSS\)自学笔记](#)

[网络安全-XSSStrike中文手册（自学笔记）](#)

-----实战-----

靶机: dvwa

[网络安全-靶机dvwa之XSS注入Low到High详解（含代码分析）](#)

靶机: pikachu

[网络安全-靶机pikachu之xss注入与代码分析（XSSStrike实战）](#)

靶机:[xssplatform](#)

CSRF漏洞

-----理论与实战-----

[网络安全-跨站请求伪造（CSRF）的原理、攻击及防御](#)

劫持攻击

点击劫持

-----理论-----

[网络安全-点击劫持（ClickJacking）的原理、攻击及防御](#)

SSRF漏洞

-----理论及实战-----

[网络安全-SSRF漏洞原理、攻击与防御](#)

文件包含漏洞

-----理论及实战-----

[网络安全-文件包含漏洞原理、攻击及防御](#)

文件上传漏洞

-----理论及实战-----

[网络安全-文件上传漏洞的原理、攻击与防御](#)

XXE漏洞

-----理论及实战-----

[网络安全-XXE（XML外部实体注入）原理、攻击及防御](#)

WebShell

[网络安全-webshell详解（原理、攻击、检测与防御）](#)

解析安全

RCE漏洞

-----理论-----

[网络安全-RCE（远程命令执行）漏洞原理、攻击与防御](#)

SQL注入漏洞

-----理论-----

[网络安全-SQL注入原理及防御SQL注入](#)

[网络安全-sqlmap学习笔记](#)

[网络安全-sqlmap注意项及高级使用](#)

-----实战-----

靶机:dvwa

[网络安全-靶机dvwa之sql注入Low到High详解（含代码分析）](#)

靶机: [sqlilabs](#)

[网络安全-sqlmap实战之sqlilabs-Less1](#)

```
#Less2差不多，整型参数错误，sql语句为
SELECT * FROM users WHERE id=$id LIMIT 0,1
```

[网络安全-sqlmap实战之sqlilabs-Less3](#)

[网络安全-sqlmap实战之sqlilabs-Less4](#)

[网络安全-sqlmap实战之sqlilabs-Less5](#)

[网络安全-sqlmap实战之sqlilabs-Less6](#)

[网络安全-sqlmap实战之sqlilabs-Less8](#)

[网络安全-sqlmap实战之sqlilabs-Less9](#)

[网络安全-sqlmap实战之sqlilabs-Less11](#)

[网络安全-sqlmap实战之sqlilabs-Less12](#)

[网络安全-sqlmap实战之sqlilabs-Less13](#)

反序列化漏洞

-----理论与实战-----

[网络安全-反序列化漏洞简介、攻击与防御](#)

条件竞争

[网络安全-条件竞争（《CTF特训营》第7章复现）](#)

[CTF-【NSCTF 2015】WEB11 条件竞争](#)

通信安全

-----理论与实战-----

应用层

[网络-http协议学习笔记（消息结构、请求方法、状态码等）](#)

[网络-https协议学习笔记（SSL、TLS、CA、抓包与修改）](#)

[网络-Telnet协议与SSH协议（命令、免密登录）及其安全性](#)

[网络-DNS域名系统详解与DNS攻击](#)

传输层

[网络-UDP协议详解（代码、实战）](#)

[网络-TCP协议详解自学笔记（例题、代码、实战）](#)

网络层

[网络-IP协议详解（报文格式、分类、NAT、子网、CIDR、抓包分析）](#)

[网络-ICMP协议、Ping命令实现与ICMP攻击](#)

[网络-ARP协议详解与ARP欺骗（中毒）攻击实战](#)

-----实战-----

[网络安全-scapy学习笔记](#)

[网络安全-python脚本资源整理](#)

身份认证与访问控制

弱口令爆破

-----理论-----

<https://github.com/insightglacier/Dictionary-Of-Pentesting>

渗透测试

学习路线



时间关系，仅关注渗透测试基础与WEB渗透相关的内容。

基础知识

kali

[渗透测试-Kali Linux学习（Linux基础、Shell编程、渗透测试软件）](#)

推荐

书籍

《Metasploit渗透测试魔鬼训练营》

《Metasploit渗透测试指南》

《KALI渗透测试技术实战》

练习靶场

[hackthebox](#)

[vulnhub](#)

信息收集

[网络安全-信息收集](#)

[《MetaSploit渗透测试魔鬼训练营》之环境搭建](#)

[《MetaSploit渗透测试魔鬼训练营》之信息搜集](#)

漏洞扫描

[OpenVAS的安装、使用及实战\(GVM, Metasploit使用\)](#)

渗透攻击

[《MetaSploit渗透测试魔鬼训练营》之WEB应用渗透技术](#)

现代密码学

基本知识

1. [现代密码学-密码学概论与基本知识](#)
2. 传统密码
3. 对称密码
4. 非对称密码
5. 哈希函数与消息认证
6. 数字签名
7. 公钥管理
8. 数字信封

CTF

项目推荐

[CTF入门](#)

[CTF工具](#)

[CTF工具2](#)

比赛推荐

全国大学生信息安全竞赛

[DDCTF](#)

["强网杯"全国网络安全挑战赛](#)

[网鼎杯网络安全大赛](#)

[XCTF](#)

[WCTF](#)

[ICTF](#)

[NSCTF](#)

KCTF

模糊测试

[Fuzzing大合集](#)

-包含fuzz书籍、课程、开源软件等

AFL

[模糊测试-AFL学习笔记之C/C++](#)

[模糊测试-AFL学习笔记之Java](#)

文件模糊测试

[模糊测试-radamsa学习笔记](#)

插桩

java插桩

[java插桩-javaassist](#)

[java插桩-Jacoco java代码覆盖率可视化](#)