web渗透测试学习路线

原创

爱睡觉的扬扬 已于 2022-03-26 22:26:03 修改 5526 收藏 9
文章标签： 网络安全 web安全
于 2022-03-26 16:05:06 首次发布

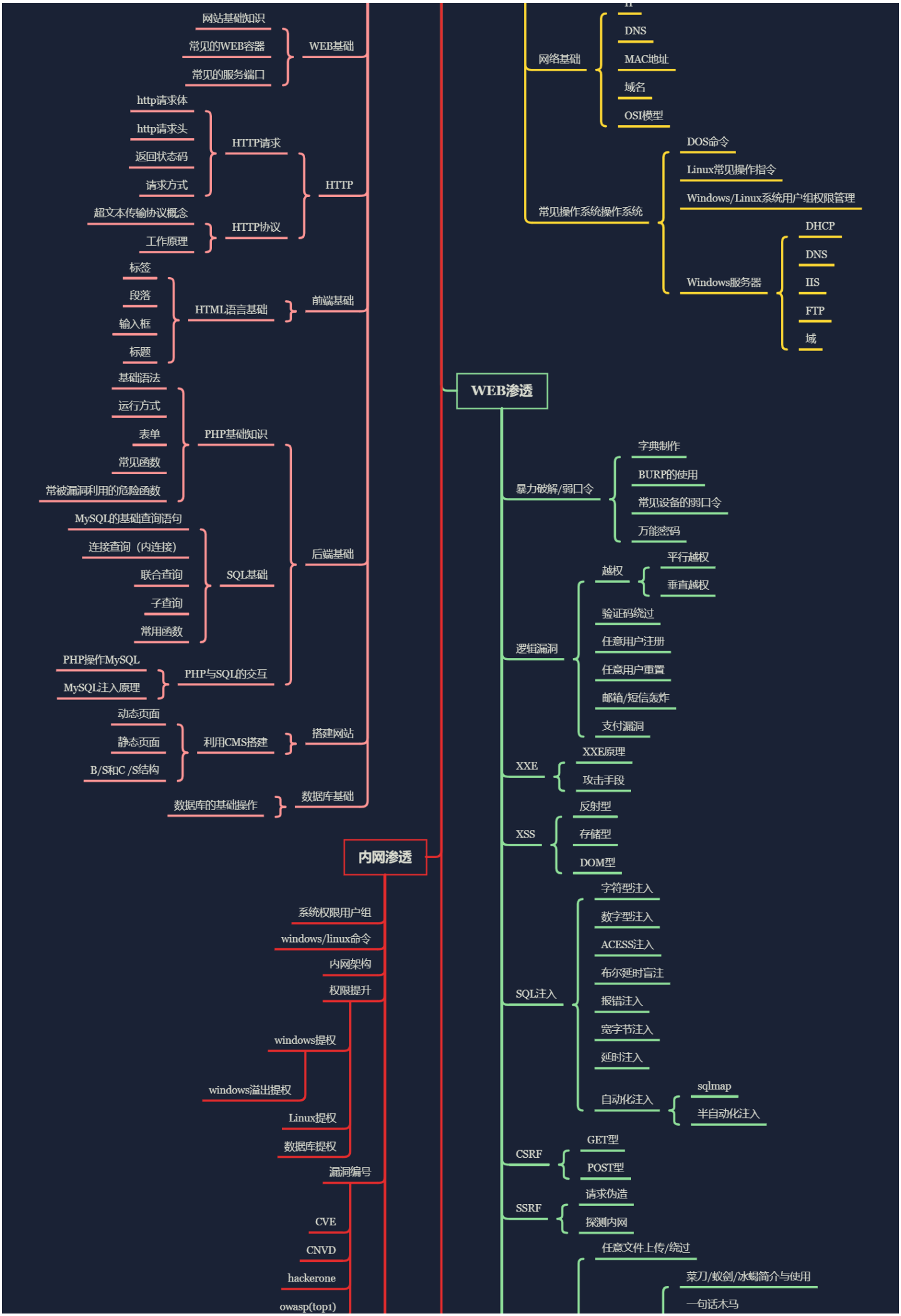
web渗透学习路线

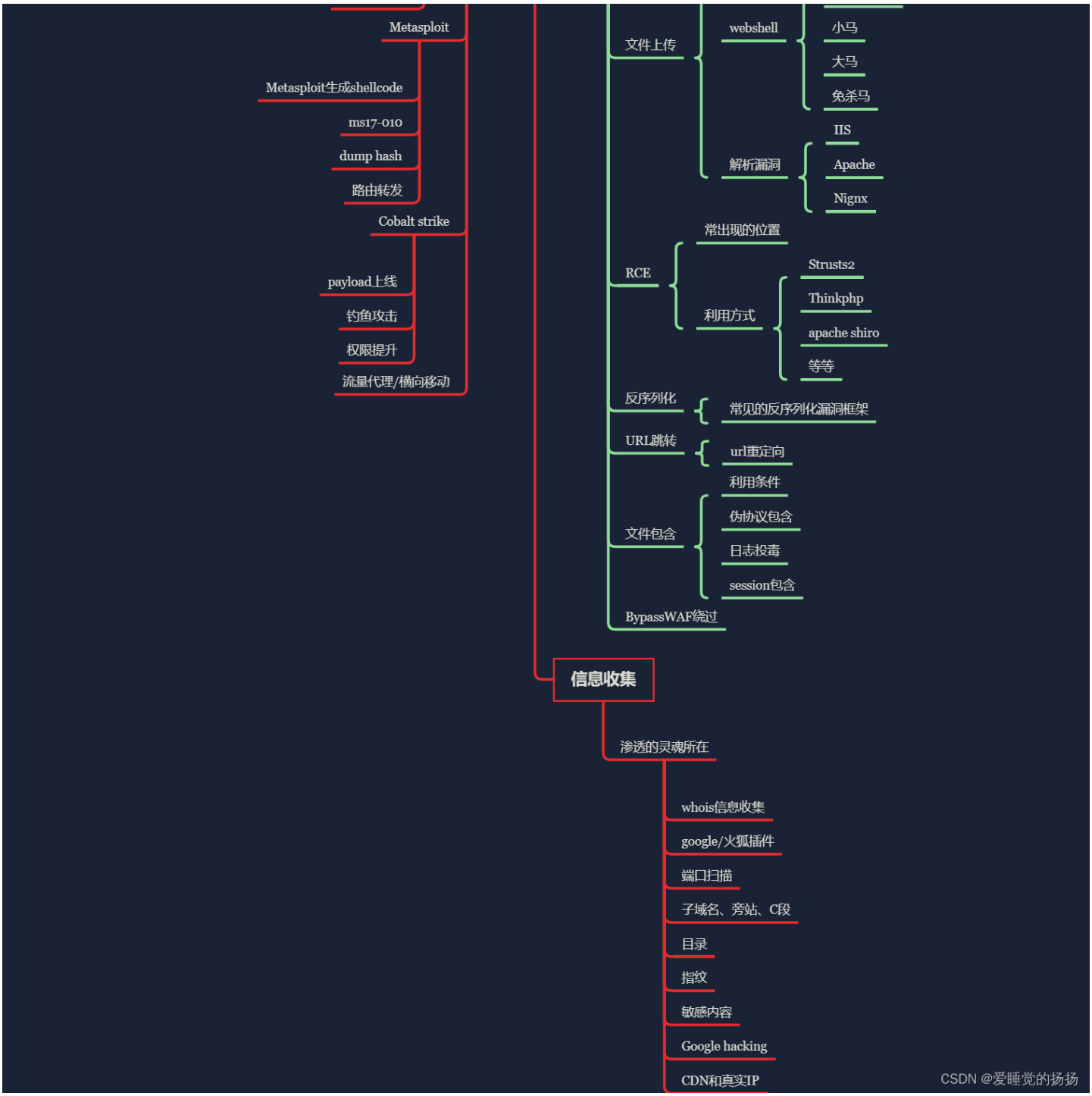
文章目录

web渗透学习路线
前言
一、web渗透测试是什么？
二、web渗透步骤
1.前期工作
2.中期提高
3.后期打牢
总结

前言

本文整理的学习路线，清晰明了，重点分明，能快速上手实践，相信想学的同学们都能轻松学完。都是干货啦，先收藏□再看吧。本文偏基础能让萌新们快速摸到渗透测试的门道，少走弯路，也能让正在学习的小伙伴们查漏补缺，也欢迎大佬们在评论区指正错误~
这里附上我之前学习的路线图


网站基础知识
常见的WEB容器
常见的服务端口
WEB基础
http请求体
http请求头
返回状态码
请求方式
HTTP请求
超文本传输协议概念
工作原理
HTTP协议
HTTP
标签
段落
输入框
标题
HTML语言基础
前端基础
基础语法
运行方式
表单
常见函数
常被漏洞利用的危险函数
PHP基础知识
MySQL的基础查询语句
连接查询（内连接）
联合查询
子查询
常用函数
SQL基础
后端基础
PHP操作MySQL
MySQL注入原理
PHP与SQL的交互
动态页面
静态页面
B/S和C /S结构
利用CMS搭建
搭建网站
数据库的基础操作
数据库基础
内网渗透
系统权限用户组
windows/linux命令
内网架构
权限提升
windows提权
windows溢出提权
Linux提权
数据库提权
漏洞编号
CVE
CNVD
hackerone
owasp(top1)
网络基础
DNS
MAC地址
域名
OSI模型
常见操作系统操作系统
DOS命令
Linux常见操作指令
Windows/Linux系统用户组权限管理
Windows服务器
DHCP
DNS
IIS
FTP
域
WEB渗透
暴力破解/弱口令
字典制作
BURP的使用
常见设备的弱口令
万能密码
逻辑漏洞
越权
平行越权
垂直越权
验证码绕过
任意用户注册
任意用户重置
邮箱/短信轰炸
支付漏洞
XXE
XXE原理
攻击手段
XSS
反射型
存储型
DOM型
SQL注入
字符型注入
数字型注入
ACESS注入
布尔延时盲注
报错注入
宽字节注入
延时注入
自动化注入
sqlmap
半自动化注入
CSRF
GET型
POST型
SSRF
请求伪造
探测内网
任意文件上传/绕过
菜刀/蚁剑/冰蝎简介与使用
一句话木马



一、web渗透测试是什么？

Web渗透测试分为白盒测试和黑盒测试，白盒测试是指目标网站的源码等信息的情况下对其渗透，相当于代码分析审计。而黑盒测试则是在对该网站系统信息不知情的情况下渗透，以下所说的Web渗透就是黑盒渗透。

二、web渗透步骤

Web渗透分为以下几个步骤，信息收集，漏洞扫描，漏洞利用，提权，内网渗透，留后门，清理痕迹。一般的渗透思路就是看是否有注入漏洞，然后注入得到后台管理员账号密码，登录后台，上传小马，再通过小马上传大马，提权，内网转发，进行内网渗透，扫描内网c段存活主机及开放端口，看其主机有无可利用漏洞（nessus）端口（nmap）对应服务及可能存在的漏洞，对其利用（msf）拿下内网，留下后门，清理痕迹。或者看是否有上传文件的地方，上传一句话木马，再用菜刀链接，拿到数据库并可执行cmd命令，可继续上大马…思路很多，很多时候成不成功可能就是一个思路的问题，技术可以不高，思路一定得骚。

1.前期工作

html+css+js

前端三要素 html、css、js是被浏览器解析的代码，是构成静态页面的基础。也是前端漏洞如xss、csrf的基础。

重点了解html和js

能力要求：能够写出简单表单，能够通过js获取DOM元素，控制DOM树即可。

apache+php
推荐使用phpstudy来进行傻瓜式安装，可以少走很多弯路。通过apache+php体会一下网站后端的工作，客户端浏览器通过请求apache服务器上的php脚本，php执行后生成的html页面返回给浏览器进行解析。

重点了解php

能力要求：了解基本网站原理，了解php基本语法，开发简单动态页面
mysql
之前已经安装的phpstudy可以轻易的安装mysql。mysql是一款典型的关系型数据库，一般来说，大部分网站都会带有数据库进行数据存储。

重点了解sql语句

能力要求： 能够用sql语句实现增删改查，并且能用php+mysql开发一个增删改查的管理系统（如学生管理系统）
python
虽然“php是最好的语言”，但它主要还是应用在服务端做网站开发，我们搞安全经常需要写一些脚本或工具来进行诸如密码爆破、目录扫描、攻击自动化等操作，需要一个方便且趁手的编程语言，这里我推荐python

重点学习requests、BeautifulSoup、re这三个库

能力要求： 了解python基础语法，能够用python爬取网站上的信息（requests+BeautifulSoup+re）
burpsuite
web安全的工具很多，但我觉得必备的渗透工具还得是它

重点学习Proxy、Repeater、Intruder三个模块，分别用于抓包放包、重放包、爆破

初步使用即可，在中期的漏洞学习中去逐渐熟练它

能力要求： 能够用burpsuite抓包改包、爆破用户名密码

2.中期提高

此时我们对网站已经不再陌生，能够自己动手完成一个简单站点。但我们写出来的代码真的安全吗？进入中期，我们便要开始着眼经典漏洞的学习。

一个漏洞的学习，要搞明白三点（每学完一个漏洞就问自己这三个问题）：

- 如何利用这个漏洞进行恶意操作？ 为什么会产生这个漏洞？ 如何修复这个漏洞？

SQL注入
(1) 了解产生sql注入的原理
(2) Union注入
(3) POST类型注入
(4) 万能用户
(5) 盲注

能力要求： 能够手工注入出任意表的数据，熟悉三种盲注的手法，能够通过sql注入实现任意文件读取和任意文件写入，能够自己编写一个不含sql注入的查询功能

文件上传

(1) 了解原理
(2) 会编写一句话木马
(3) 会用cmd命令吧一句话木马与图片结合
(4) 利用一句话木马getshell

能力要求： 会写php的webshell，明白webshell的原理，熟悉常见的文件上传绕过方法（如过后缀检测、过文件头检测、过MIME类型检测），能够自己编写一个不含漏洞的上传功能

文件包含

(1) 了解原理
(2) 会利用文件包含与文件上传文件相结合来getshell
(3) 会访问容易文件
(4)file协议、php伪协议的利用

命令执行

(1) 了解原理
(2) 了解一些cmd的基本命令
(3) 知道哪些特殊字符有特殊作用
(4)php常见的代码执行（eval）、命令执行（system）函数

XSS

(1) 了解原理
(2) 学一下javascript的基本语法
(3) 然后会利用xss获取cookie
(4) 编写一个简单的xss蠕虫

CSRF

(1) 了解原理
(2) 可以利用CSRF进行一些小操作(通过csrf让用户点击恶意链接就触发敏感操作)
(3) 结合xss来利用

变量覆盖

(1) 了解原理
(2) 利用变量覆盖来getshell

XEE

(1) 了解一些XML的语法
(2) 了解原理
(3) 会用XEE来getshell之类的

反序列化

(1) 了解序列化
(2) 了解反序列化
(3) 了解POP链

逻辑漏洞

3.后期打牢

多多参与CTF赛事

参与当下举行的ctf赛事是最好的学习方法之一，即使是初学者也能够找到一些适合自己能力的赛事，比如极客大挑战、UNCTF、各个大学的新生赛等等都是不错的选择，在比赛中去发现自己知识的不足，然后去针对的补充这部分知识，是很好的学习循环，无需迷茫的去到处获取知识，而是在需要时去学习。

Tips: 或许有人觉得直接刷题是一样的，但完全不是，当下比赛中的题往往更加前沿和流行，你可以找到当下的ctf题目趋势，紧跟技术热点，而且可以多多融入ctf竞技的氛围中，成长的更快。

ctfhub 可以很方便的查看最近举行的ctf赛事

多多看其他师傅的博客

打完ctf比赛的你肯定是想看writeup（答案）的，一般来说赛后过几天就会有很多师傅发出他的writeup，从比赛群、百度等途径都可以找到。多多看看其他师傅的解题思路，关注几个大牛，看看他们发的技术文章，都是很好的学习方法。

总结

web安全其实是个大坑，进去容易出去难，入门容易提升难，我们这行没有其他专业那么有趣，甚至可以说是枯燥乏味，但是还是希望选择web路线的学弟学妹们坚持web这条路线，不要中途放弃