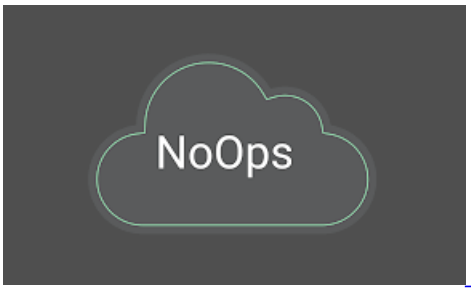
Web 方向学习路线

原创

OceanSec 于 2022-01-10 18:39:16 发布 359 收藏 11

分类专栏： ELSE 文章标签： 前端

本文链接：https://blog.csdn.net/q20010619/article/details/122416664



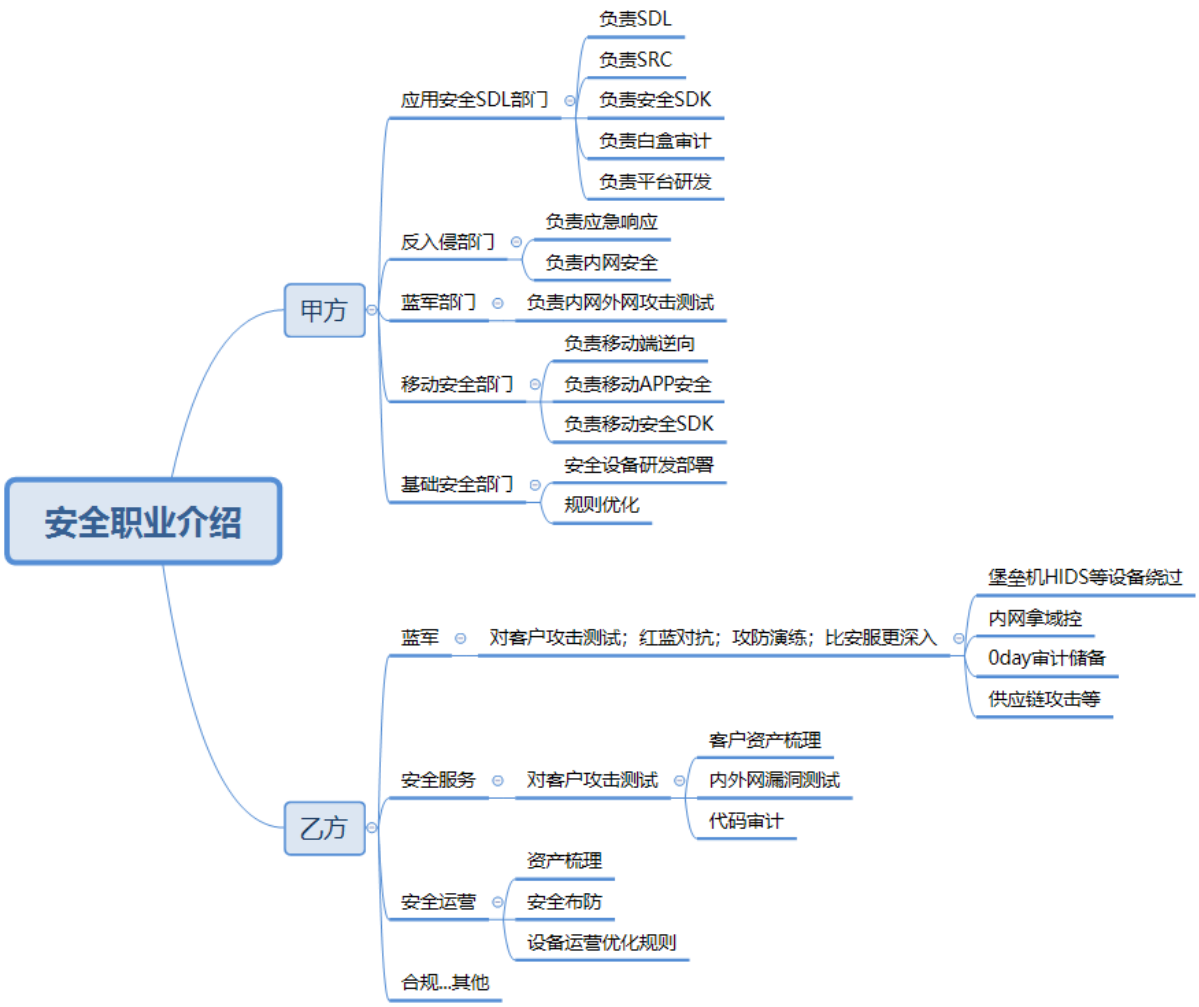
ELSE 专栏收录该内容

7 篇文章 1 订阅

订阅专栏

入门

安全职业介绍



以下几项没有先后顺序，不是说要把编程语言精通之后再去学习后边的，而是可以一边学语言一边学漏洞，自己不知道咋规划建议看学习资料-综合教程部分，入门还是以CTF为主

前导

> 提问的智慧
> https://github.com/ryanhanwu/How-To-Ask-Questions-The-Smart-Way/blob/main/README-zh_CN.md
> 以下根据自己的学习方法来，如果觉得看字太慢的话，可以看视频，不管咋学都要记笔记

1.编程语言

学编程语言一定要跟着教程练习，步骤都跟着做一遍，记笔记

- PHP：https://www.runoob.com/php/php-tutorial.html
- Python：https://www.liaoxuefeng.com/wiki/1016959663602400
  入门阶段不需要精通，代码可以读懂，可以写简单的代码就可以

2.Linux环境

1. 熟悉Linux基本命令（https://shimo.im/docs/vrTgvx8c8kWwx998） Debian、Ubuntu、Centos这些系统尽管命令不是全部相同，但是大体一致
2. 能够使用LNMP或者LAMP搭建环境(Windows下PHPstudy必会，lnmp在kali里边有)

3.漏洞学习

视频教程：

https://www.zhaoj.in/read-6321.html

熟悉漏洞原理，熟悉利用方法

https://vulwiki.readthedocs.io/

SQL注入

命令\代码执行漏洞

文件上传漏洞

文件包含漏洞（做CTF web题目常见）

SSRF漏洞

反序列化漏洞

XXE漏洞

SSTI

等

CTF是入门好方法，之后的比赛也是CTF

4.CTF练习

攻防世界 https://adworld.xctf.org.cn/task

MISC

WEB

CRYPTO
2.BUUCTF：https://buuoj.cn/login?next=%2Fchallenges%3F

MISC

WEB

CRYPTO
buu分类练习文档：https://shimo.im/docs/B9PKtXo2lUMmzlJv/

靶场

```
ctfshow
https://ctf.show/收费的，但是题目质量不错，很多大佬都是刷题刷出来的
重生信息安全在线靶场：
https://bc.csxa.cn
网络信息安全攻防学习平台：
http://hackinglab.cn
墨者学院在线靶场：
https://www.mozhe.cn/bug
封神台在线演练靶场：
https://hack.zkaq.cn/battle
安鸾渗透实战平台：
http://www.whalwl.cn/home
XSS Challenges：
http://xss-quiz.int21h.jp
漏洞靶场
DVWA：
http://www.dvwa.co.uk
BWVS：
https://github.com/bugku/BWVS
Sqli-Labs：
https://github.com/Audi-1/sqli-labs
Webug 3.0：
https://pan.baidu.com/s/1eRIB3Se
Upload-labs：
https://github.com/c0ny1/upload-labs
DVWA-WooYun：
https://sourceforge.net/projects/dvwa-wooyun
```

4.社区论坛:

```
先知社区:https://xz.aliyun.com
安全客：https://www.anquanke.com
freebuf：https://www.freebuf.com
看雪：https://www.kanxue.com
吾爱破解：https://www.52pojie.cn
404paper:https://paper.seebug.org
补天社区：https://forum.butian.net
SEC-IN:https://www.sec-in.com
```

5.学习资料：

视频教程

综合教程：

根据自己的学习方法选一套就行

https://www.bilibili.com/video/BV1Lf4y1t7Mc P123开始

https://www.bugbank.cn/live/xiaobai

https://pan.baidu.com/s/1g0yR8WJZl1LEeaMyxlfYaA?pwd=zw82

单项教程：

Python3：链接：https://pan.baidu.com/s/1c460DSyyhOurdHZBEh8FEQ 提取码：bSB6
或者 https://www.icourse163.org/learn/BIT-268001?tid=1207014257#/learn/content （图形不用学）

https://www.icourse163.org/course/BIT-1001870001

百度网盘和MOOC二选一，最后作业以实际做出的项目上交

- PHP：https://www.w3school.com.cn/php/index.asp
  链接: https://pan.baidu.com/s/1qSK9ewPDrFhfEJxlQs0uLg 提取码: ohee

https://ke.qq.com/course/471769?taid=4018470186857177

要求：能够读懂别人的PHP代码(可以查阅资料)

最好是能够使用PHP开发简单的网站

- Golang https://www.bilibili.com/video/BV1Uq4y1Q7Jn
  新兴语言，学完基础后就去看看golang怎么写爬虫，剩下的多搜索学习吧

文字教程

> CTF推荐仔细看看CTFwiki：https://wiki.x10sec.org/ 里面一些例题自己做做也挺好
> CTF练习题目 以提交的WriteUp为准（以上不要求都做完 尽最大可能做，主要在于总结题型，熟悉套路）
>
> CTF入门手册：链接：https://pan.baidu.com/s/14zuYUZfYzmoW2ervMXhDwQ
> 提取码：1e2x

请根据自己情况制定自己详细学习计划

不懈努力，你可以收获一个更好的自己，可以养成一个坚持学习的习惯，可以提高自己的学习能力。

每天进步一点点，让优秀逐渐成为一种习惯！！！

进阶

在入门阶段基本完成后，可以开始进阶部分，进阶部分最要分为以下几个方向（其实环环相扣）

以下内容安全客 freebuf 先知以及一些师傅博客有大量文章

- CTF深入学习
- 代码审计
- 漏洞复现

CTF深度学习

CTF比赛越来越卷，难度在逐年提升，从PHP永远第一逐渐变成ctf边缘人，时代在进步，也就对Ctfer提出了更高的要求，对ctf比赛的出现的新的考察方法简单罗列

1. PHP 其他深层次利用点（框架漏洞、pop反序列化、冷门知识）
2. Python SSTI、Python反序列化
3. Java 反序列化漏洞，各种gadget
4. nodejs 原型链污染
5. go 反序列化（偶尔出）
6. CVE 漏洞利用 (主流CVE https://vulhub.org)
7. AWD
8. 题可以buu上找
   可以发现其他语言也逐渐成为了CTF的考点，在学习漏洞的过程中，不要想着先把语言基础搞得扎实在学漏洞，时间成本太高，而且很容易脱离网安领域转向开发。正确的打开方式是：简单学习基础（看几篇文章），然后去看漏洞原理，遇到不会的再百度基础，不要脱离初衷

CTF方向大佬博客链接汇总：链接

代码审计

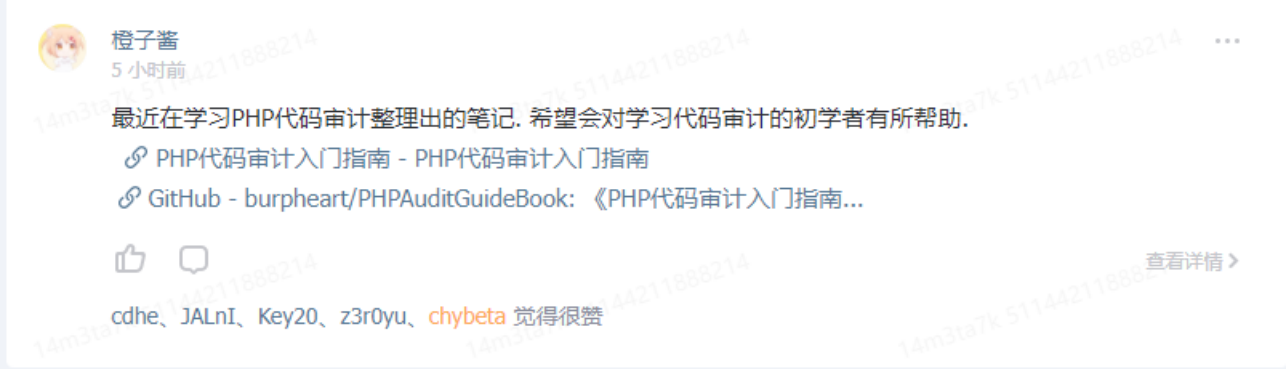
安全客 freebuf 先知也有大量文章

代码审计也是CTF中经常遇到的题目，相比CTF中的审计最多就几十行，真实的代码审计以项目为主

因为代码审计对于语言基础（语言可以选择 PHP 或者 Java）要求比较高，看不懂就读不懂，这时候就可以去补一补语言，建议找一个中型web项目学习，跟着搞一遍代码，而不是从变量定义开始重新来过

学习完毕后去实际审计代码，先从有已知漏洞小型cms开始，然后审计框架

PHP和Java有很大不同，但在漏洞的原理上都是相通的，可以先看php的主流框架和CMS去复现和挖掘，后面慢慢转Java，多找一些大师傅的博客去看，跟着大师傅的博客学习，下面列出一些知识较为系统的博客



https://github.com/burpheart/PHPAuditGuideBook

https://cz0.gitbook.io/phpauditguidebook/

推荐博客：

1. https://www.cnblogs.com/nice0e3/
2. https://www.cnblogs.com/tr1ple/
3. https://www.cnblogs.com/bmjoker/
4. https://landgrey.me/
5. https://p0rz9.github.io/
6. https://www.cnblogs.com/afanti/p/13156152.html
7. https://www.o2oxy.cn
8. https://su18.org
9. github.com

漏洞复现

ocean：漏洞复现很 简单的，脚本一跑拿shell不就完了

谁不想做个快乐的脚本小子呢，可是这样复现了有啥用呢，啥也没学会

复现的过程中应该考虑，复现的漏洞是什么，影响到的web服务有哪些以及服务的作用、漏洞原理、漏洞利用方法最后是漏洞修复方法

关于漏洞复现如果是小型cms环境搭建比较简单，可以自己搭建学习，也可以用别人写好的docker环境（推荐：https://vulhub.org）

实战

注：主力战队可以享受学长学姐留下来的漏洞报告、亲自指导，在你原有基础上帮助你快速提升实战水平。

实战主要分为外网、内网、代码审计

https://github.com/MrWQ/vulnerability-paper

```
tools:https://www.t00ls.cc  (需要投稿获取邀请码)
90sec:https://forum.90sec.com
火线：https://zone.huoxian.cn
```

外网

如果你把上面的学的差不多了，外网基本没问题，不过需要注意的是外网的打点主要是能获取权限的漏洞，其次是能获取数据的漏洞

- java内存马
- shiro、weblogic、OA漏洞等等
  全部的CVE

https://github.com/nomi-sec/PoC-in-GitHub#

一些常见漏洞

https://github.com/EdgeSecurityTeam/Vulnerability

https://github.com/projectdiscovery/nuclei

https://github.com/woodpecker-framework

代码审计

同上

内网

靶场http://vulnstack.qiyuanxuetang.net/vuln/

根据靶场去学习具体的知识点，社团内部课堂也有课程

安全客 freebuf 先知也有大量文章

大致分为以下几点

工具

- Cobalt Strike
- MSF
- 内网常见的扫描工具与脚本比如 fscan、kcsan等多关注github

钓鱼&免杀

内网信息收集

主机漏洞&服务漏洞利用

MS系列漏洞、redis漏洞以及内网常见存在RCE的服务等

代理转发

隧道隐蔽

权限维持

横向渗透

域漏洞利用

基础知识：https://daiker.gitbook.io/windows-protocol

博客：https://www.cnblogs.com/nice0e3/category/1686860.html

面试

多看看别人的面经，不同岗位的侧重点不太一样

优先推荐 牛客网

一些公开的面经

https://github.com/d1nfinite/sec-interview

https://github.com/tiaotiaolong/sec_interview_know_list

https://github.com/Leezj9671/Pentest_Interview

https://github.com/Leezj9671/Pentest_Interview/

https://github.com/Leezj9671/offensiveinterview

https://4o4notfound.org/index.php/archives/183/

http://yulige.top/?p=685

https://mp.weixin.qq.com

https://mp.weixin.qq.com

https://www.yuque.com/feei/sig