ctf入门

原创

鲨鱼饿死了 于 2021-06-03 15:50:04 发布 66 收藏 1

本文链接：https://blog.csdn.net/weixin_43123409/article/details/117523384

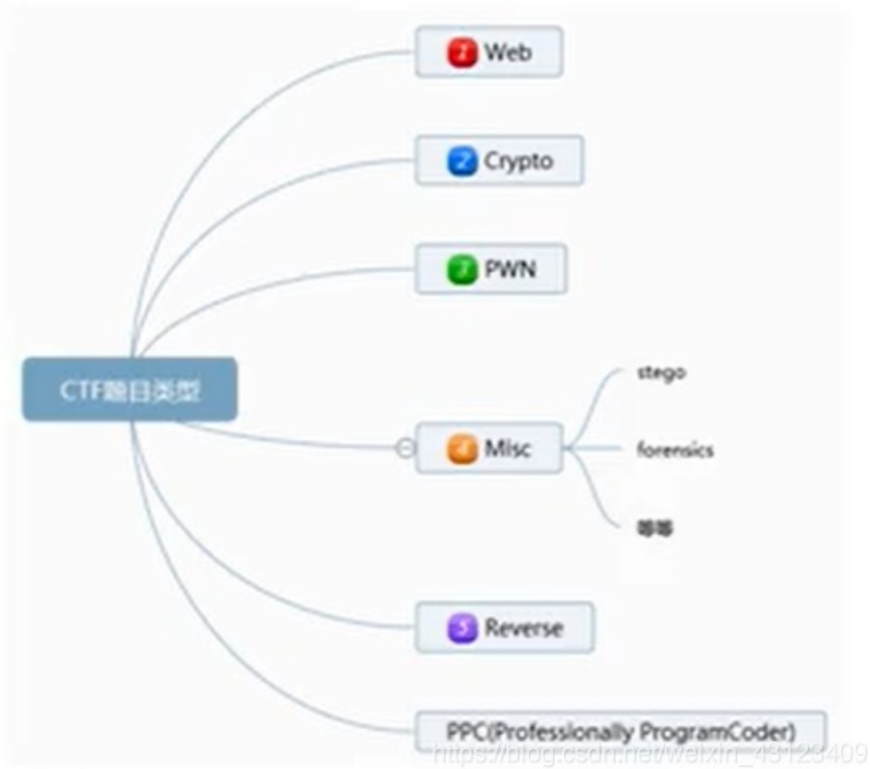
ctf对我们的意义？？

CTF对我们的意义—什么是CTF

Capture The Flag（CTF）夺旗比赛

ctf类型

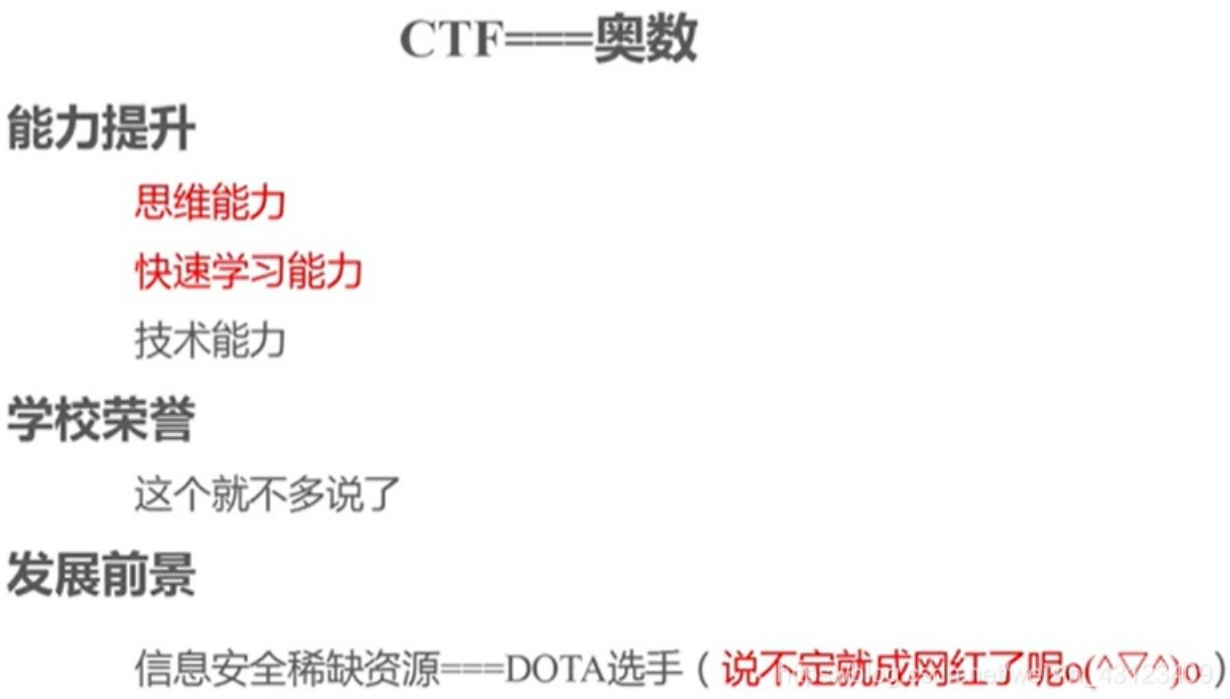
CTF对我们的意义—CTF类型



1. web网络安全
2. 密码学：对算法的理解
3. 程序逻辑分析，利用
4. 杂：数据还原
5. 逆向破解
6. 编程

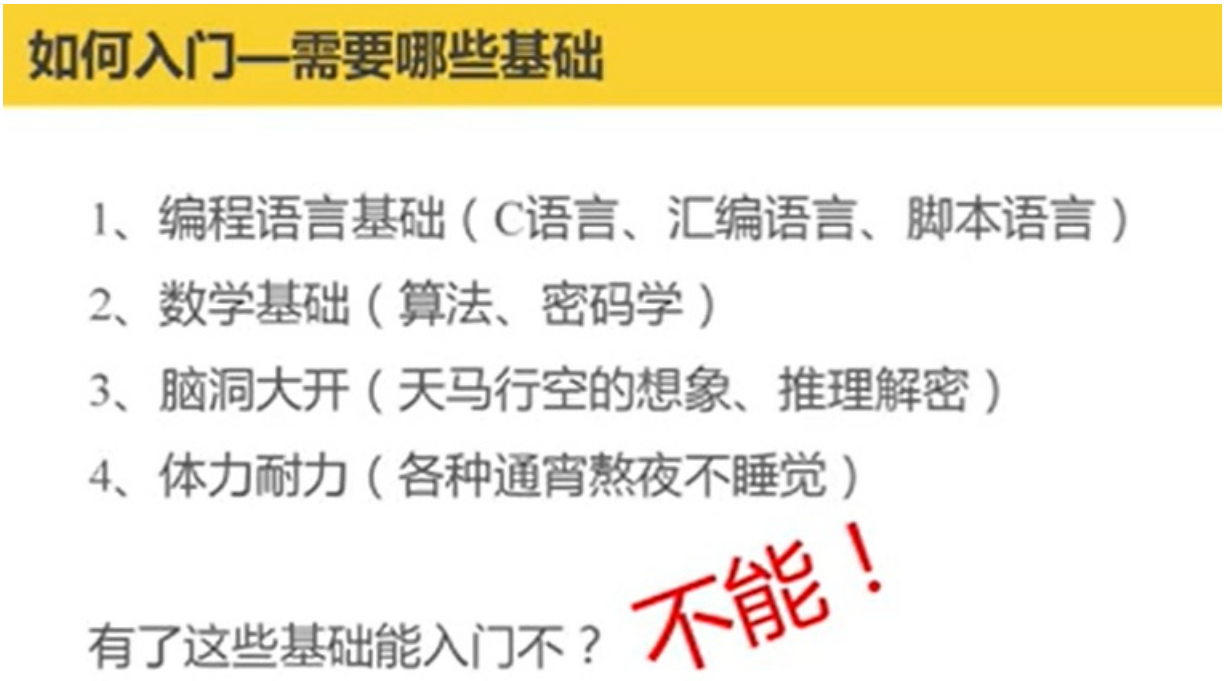
CTF对我们的意义—著名CTF比赛有哪些

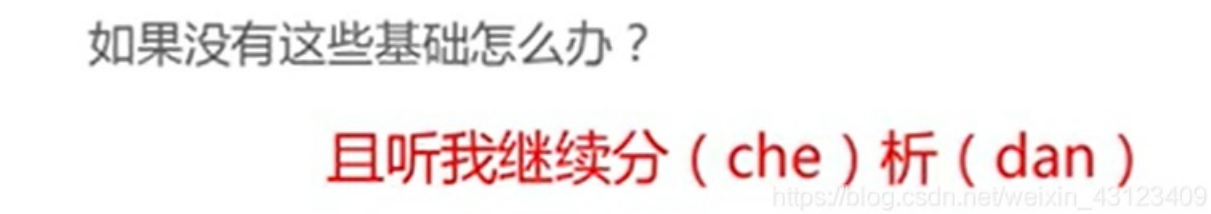
为什么打ctf===奥数
思维能力，快速学习能力，—》技术能力
可能两天内思维快速运转



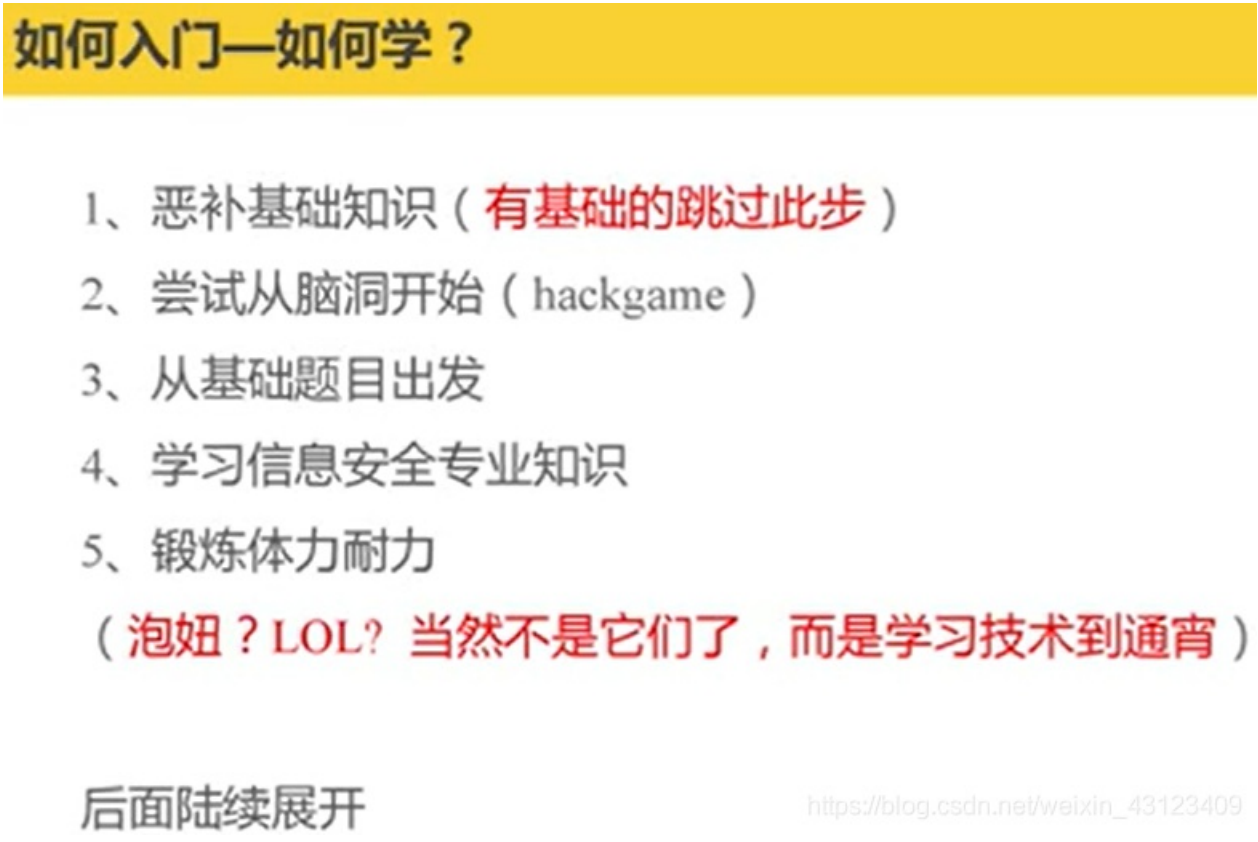
可能会用到一个小众语言，一天内学习

如何入门–所需技能

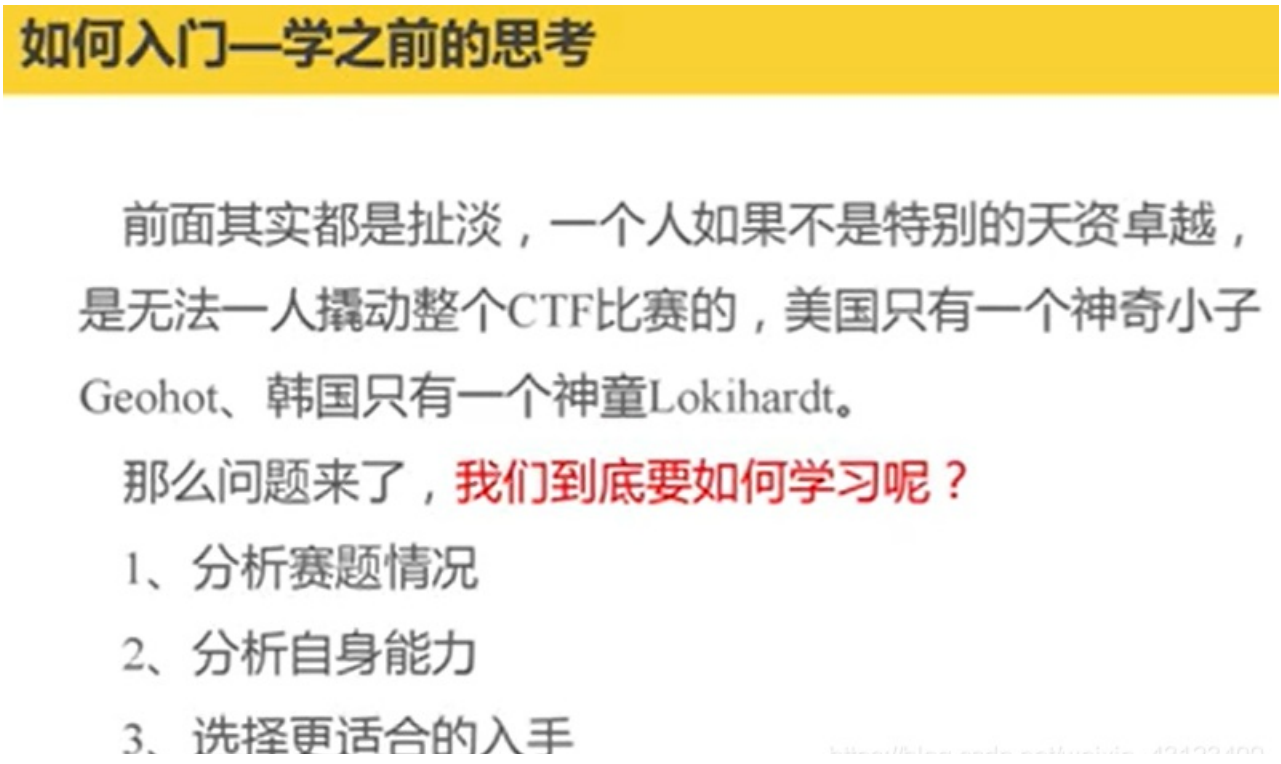




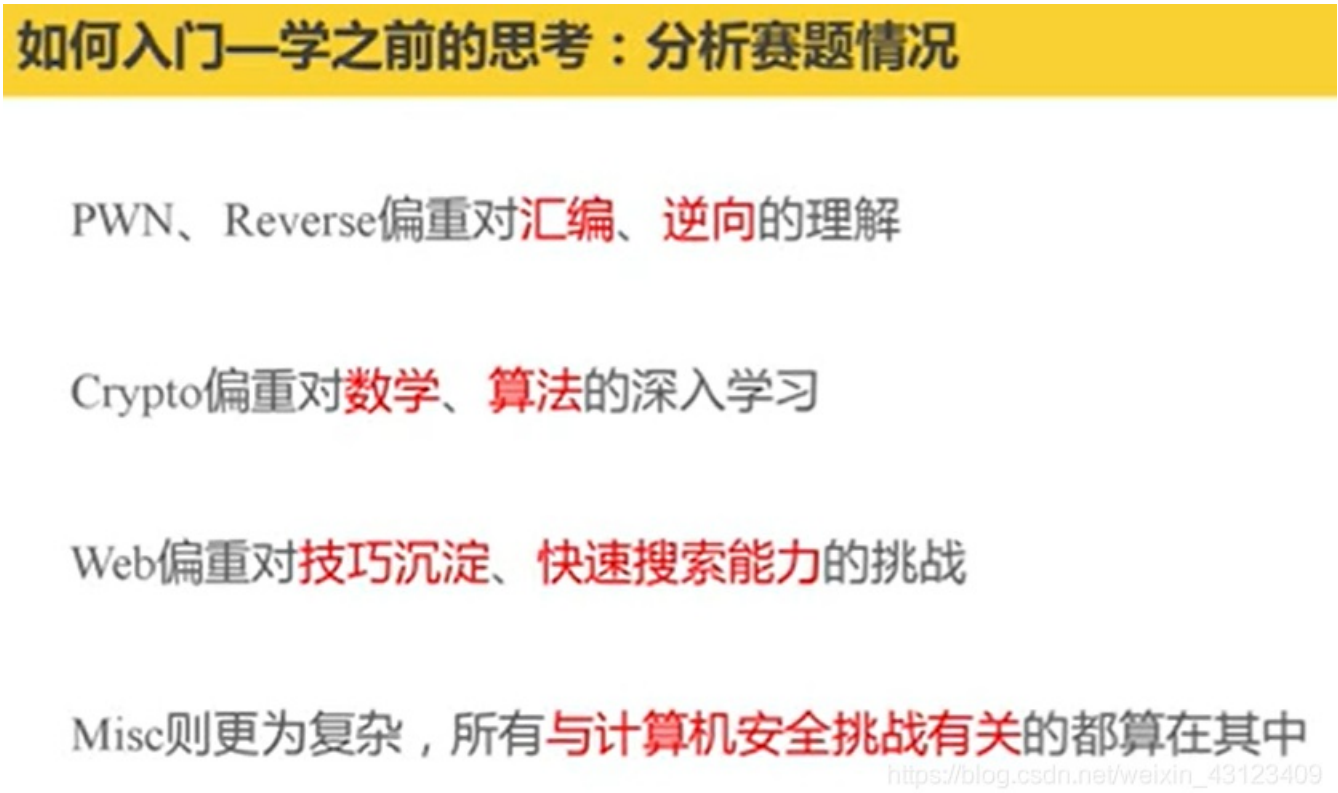
重要元素：逆向，算法-------》数学
思想跳跃，推理



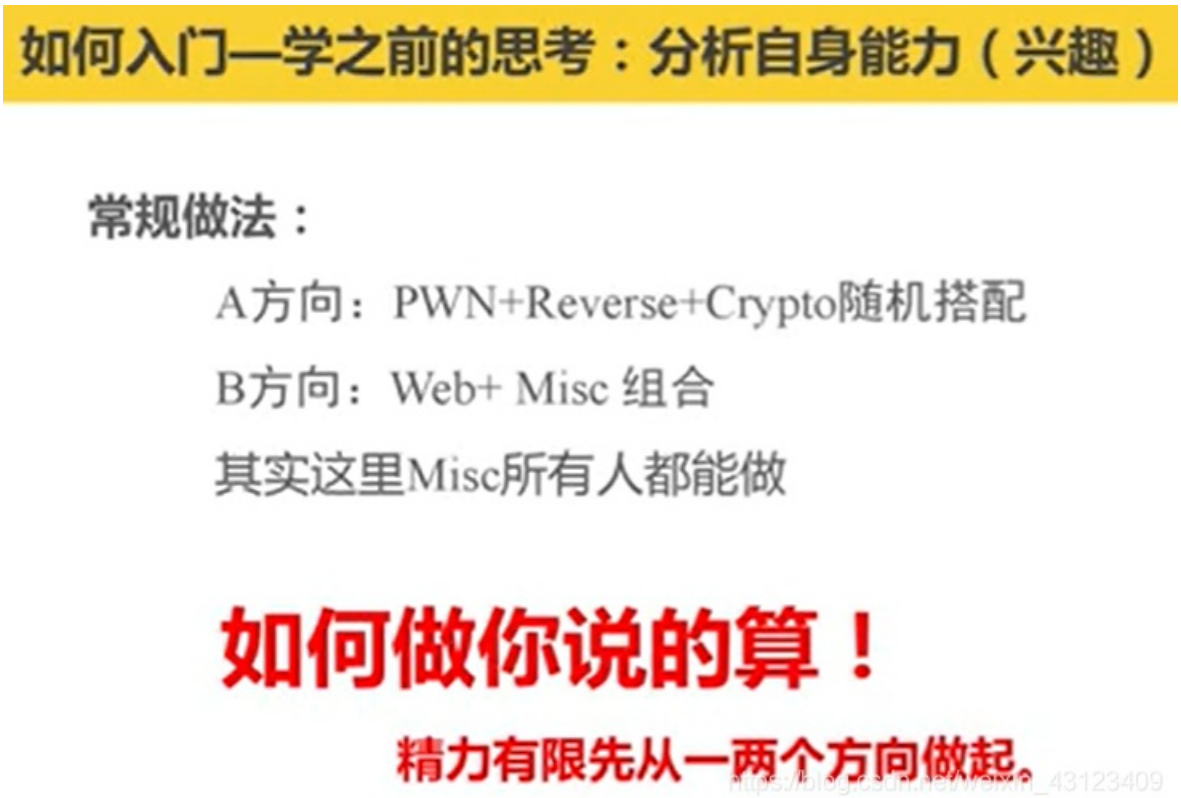
ctf比赛的分是很难的



赛题种类



web偏向发散思维，对底层能力要求不高



都需要学的内容：

Linux基础、计算机组成原理、操作系统原理、网络协议分析

A方向：

IDA工具使用（f5插件）、逆向工程、密码学、缓冲区溢出等

B方向：

网络安全、内网渗透、数据库安全等

ida最重要
od工具

如何入门—恶补基础知识&信息安全专业知识

推荐图书：（基础书籍按照自己喜欢的看）

A方向：

RE for Beginners(逆向工程入门)

IDA Pro权威指南

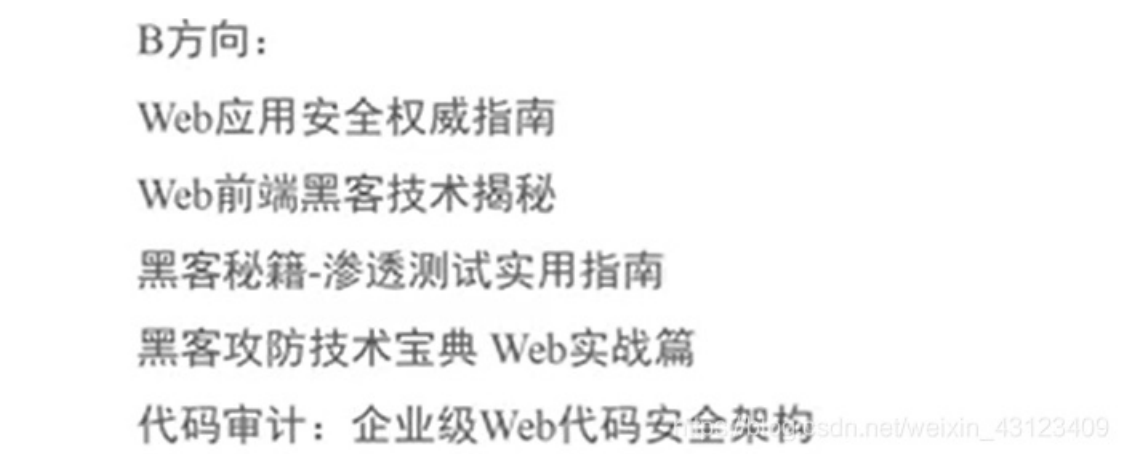
揭秘家庭路由器0day漏洞挖掘技术

自己动手写操作系统

黑客攻防技术宝典：系统实战篇

如何入门—恶补基础知识&信息安全专业知识

推荐图书：（基础书籍按照自己喜欢的看）



适合小白，最推荐《web应用安全权威指南

怎么学ctf

xctf相对较难

http://oj.xctf.org.cn/ xctf题库网站

国外较好的入门

从基础题目出发（推荐资源）

www.wechall.net/challs 非常入门的国外ctf题库，很多国内选手都是从这里刷题成长起来。

涉及移动安全

http://canyouhack.it/ 非常入门的国外ctf题库

https://microcorruption.com/login 很酷炫游戏化

与ctf相关的

http://smashthestack.org 比较简洁的内容，SSH连入即可开始玩

从基础题目出发（推荐资源）

http://overthewire.org/wargames/ 比较老牌的Wargame ，国内资料也比较多。一些writeup http://drops.wooyun.org/author/litao3rd

从基础题目出发（推荐资源）

https://exploit-exercises.com/ 也是一个比较老的Wargame，国内资料也比较多。

从基础题目出发（推荐资源）

http://pwnable.kr/play.php PWN类题目的游乐场

从基础题目出发（推荐资源）

http://ctf.moonsos.com/pentest/index.php 米安的Web漏洞靶场，还挺好玩

VRP 漏洞靶场平台 (内测版)~

从基础题目出发（推荐资源）

http://prompt.ml/0 国外的xss测试

http://redtiger.labs.overthewire.org/ 国外的SQL注入的挑战网站

如何入门—选择什么工具

CTF比赛一般都是使用网络安全常用工具，比如burp、IDA等，但是会有很多大家不常见的工具。

这里我列举一些聚合：

https://github.com/truongkma/ctf-tools

https://github.com/P1kachu/v0lt

https://github.com/zardus/ctf-tools

https://github.com/TUCTF/Tools

参加比赛

如何入门—以练促赛、以赛养练

以练促赛：

选择一场已经存在Writeup的比赛。

以赛养练：

参加一场最新CTF比赛。

https://ctftime.org/ 国际比赛

http://www.xctf.org.cn/ 国内比赛

同一道题的不同解题方式
名次不重要，过程最重要
分析出题人想法

组建团队

如何组建团队—强力成员画像

1、思维跳跃：灵活性、不会钻墙脚
2、专注：遇到问题不放弃直到解决
3、耐力：可以一天一夜不睡觉的研究技术
4、团队精神：责任、凝聚、分享

有以上三条为强力成员；有以上四条会成为强力队长！

国内的xctf可能是36小时比赛
国外可能是48小时甚至更长时间
目标：我们队就是要的第一！

如何组建团队—组建团队要解决的问题

1、新人招募：如何评判新人潜力
2、队员培养：如何快速培养队伍能力
3、梯队有序：如何建立阶梯层级
4、纪律严格：如何拒绝无团队精神的队员

综上所述：~~我目前还是不搞CTF子~~