

CTF入门指南(0基础)

转载

[weixin_33874713](#) 于 2017-04-11 06:41:00 发布 2640 收藏 56
文章标签: [php](#) [web安全](#) [密码学](#)
ctf入门指南

如何入门? 如何组队?

capture the flag 夺旗比赛

类型:

Web

密码学

pwn 程序的逻辑分析, 漏洞利用windows、linux、小型机等

misc 杂项, 隐写, 数据还原, 脑洞、社会工程、与信息安全相关的大数据

reverse 逆向windows、linux类

ppc 编程类的

国内外著名比赛

国外:

国内: xctf联赛 Ocf上海国内外都有, 很强

入门需要哪些基础：

- 1.编程语言基础（c、汇编、脚本语言）
- 2.数学基础（算法、密码学）
- 3.脑洞大开（天马行空的想象、推理解密）
- 4.体力耐力（通宵熬夜）

如何入门学

- 1.恶补基础知识
- 2.尝试从脑洞开始 如黑客game
- 3.从基础题出发 一般都是100，200，最高分在500，600 先把100分的学好，可从实践，高中的ctf学起，比较简单，只涉及1，2个点
- 4.学信息安全专业知识
- 5.锻炼体力耐力 周六日都有比赛

到底如何学？

- 1.分析赛题情况
- 2.分析自身能力 自己最适合哪个方向
- 3.选择更适合的入手

分析赛题

PWN、Reverse偏重对汇编、逆向的理解 对底层理解

Crypto偏重对数学、算法的深入学习 密码课要深入学

Web偏重对技巧沉淀、快速搜索能力的挑战 发散思维，对底层只需要了解，代码原理，关于漏洞点的积累

Misc则更复杂，所有与计算机安全挑战有关的都在其中 隐写，图片数据分析还原，流量，大数据，对游戏分析
逆向

常规做法：

A方向：PWN+Reverse+Crypto随机搭配

B方向：Web+Misc组合

Misc所有人都可以做

入门知识：

都要学的内容：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（fs插件）、逆向工程、密码学、缓冲区溢出等

B方向：Web安全、网络安全、内网渗透、数据库安全等 前10的安全漏洞

推荐书：

A方向：

RE for Beginners

IDA Pro权威指南

揭秘家庭路由器0day漏洞挖掘技术

自己定操作系统

黑客攻防技术宝典：系统实战篇 有各种系统的逆向讲解

B方向：

Web应用安全权威指南 最推荐小白，宏观web安全

Web前端黑客技术揭秘

黑客秘籍——渗透测试实用指南

黑客攻防技术宝典 web实战篇 web安全的所有核心基础点，有挑战性，最常规，最全，学好会直线上升

代码审计：企业级web代码安全架构

入门----从基础题目出发（推荐资源）：

<http://ctf.idf.cn> !!!首推 idf实验室：题目非常基础，只1个点

www.ichunqiu.com 有线下决赛题目复现

<http://oj.xctf.org.cn/xctf> 题库网站，历年题，练习场，比较难

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

<http://canyouhack.it/> 国外，入门，有移动安全

<https://microcorruption.com/login> A方向 密码，逆向酷炫游戏代

<http://smashthestack.org> A方向，简洁，国外，wargames，过关

<http://overthewire.org/wargames/> ! ! ! ! 推荐A方向 国内资料多，老牌wargame

<https://exploit-exercises.com> A方向 老牌wargame，国内资料多

<http://pawnable.kr/play.php> pwn类游乐场，不到100题

<http://ctf.moonsoscom/pentest/index.php> B方向 米安的Web漏洞靶场，基础，核心知识点

<http://prompt.ml/0> B方向 国外的xss测试

<http://redtiger.labs.overthewire.org/> B方向 国外sql注入挑战网站，10关，过关的形式 不同的注入，循序渐近地练习

工具：

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

<https://github.com/Plkachu/v0It>

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

<https://github.com/TUCTF/Tools>

入门--以练促赛，以赛养练

选择一场已经存在writeup的比赛

总结解题过程，分析出题人想法

参加一场最新的ctf比赛

<https://ctftime.org/> 国际比赛，有很多基础的

<http://www.xctf.org.cn/> 国内比赛，比较难

组建团队---强力成员画像CTF入门指南CTF入门指南

- 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：连续一天研究技术
- 4.团队精神：责任、凝聚、分享

有3条为强力成员，有4条会成为强力队长！

组队问题：

新人招募、队员培养、梯队有序、纪律严格

学习的地方很多，不能一一列举，一些优秀的网址和博客可能也没有提到，大家补充吧:P
就简单总结一些常用的吧，本人是十足的彩笔，还望大家多多指点，表哥们带我飞Orz

<http://www.sec-wiki.com/skill/> 安全技能(里面渗透逆向编程都有介绍)

http://blog.knownsec.com/Knownsec_RD_Checklist/ 知道创宇研发技能表v3.0

安全编程方面的不太清楚，问问安全编程的表哥吧QAQ

综合学习平台：

<http://edu.gooann.com/> 谷安网校

<http://www.jikexueyuan.com/> 极客学院

<http://www.hetianlab.com/> 合天

<http://www.moonsos.com/> 米安网

<http://www.ichunqiu.com/> i春秋

<http://www.honyaedu.com/> -红亚

<http://www.baimaoxueyuan.com/> 白帽学院

<http://www.simplexue.com/ctf/index> 西普学院

<http://www.imooc.com/course/list> 慕课

<http://www.secbox.cn/> 安全盒子

<http://www.freebuf.com/> freebuf

<http://bobao.360.cn/> 360安全播报

<http://www.wooyun.org/> 乌云

<http://drops.wooyun.org/> 乌云知识库

<http://wiki.wooyun.org/> WooYun Wiki

<https://www.91ri.org/> 91ri

<https://www.t00ls.NET/tools>

<http://www.ijiandao.com/> 爱尖刀

<http://www.secwk.com/article/index.html> 威客众测

<http://bluereader.org/> 深蓝阅读

<http://www.shentou.org/> 黑客安全军火库

<http://netsecurity.51cto.com/> 51cto

<http://security.csdn.net/> csdn

<http://www.80sec.com/> 80sec team

<https://security.alibaba.com/blog.htm?spm=0.0.0.0.knOqal> 阿里巴巴安全响应中心

<http://security.tencent.com/index.PHP/blog> 腾讯安全应急响应中心 博客

<http://security.360.cn/blog> 360安全应急响应中心 博客

<http://sec.baidu.com/index.php?research/list> 百度安全应急响应中心 博客

博客推荐

<http://security.tencent.com/index.php/blog>

<http://217.logdown.com/> 217

<http://www.blue-lotus.net> blue-lotus 蓝莲花

<http://blog.0ops.net/> 0ops

<http://le4f.net/> e4f

<http://www.programlife.net/> 代码疯子

<http://www.hackdog.me/> redrain'blog

<http://www.syjzwj.com/> 俊杰

<http://syclover.sinaapp.com/> 三叶草安全小组

<http://appleu0.sinaapp.com/> appleU0大大

<http://bl4ck.in/> tomato表哥

<http://www.sco4x0.com/> 4叔叔

<http://laterain.sinaapp.com/> 白神

<http://0nly3nd.sinaapp.com/> 0nly3nd

<http://hijacks.in/> LateRain'blog

<http://www.waitalone.cn/> 独自等待

<http://evilcos.me/> 余弦

<http://www.moonsec.com/> 暗月

<http://www.cnblogs.com/xuanhun/> 玄魂

<https://www.leavesongs.com/> 离别歌

<http://huaidan.org/> 鬼仔

<http://www.03sec.com/> sky的自留地

<http://joychou.org/> jc老师

<http://www.unhonker.com/> 90's blog

<http://www1.taosay.net/> 道哥的黑板报

<http://blog.knownsec.com/> 知道创于

<http://www.sadk.org/> 焯安

<http://www.cnseay.com/> seay'blog

<http://blog.aptsec.net/> AptSec Team

<http://lcx.cc/> 网络安全研究中心

<http://www.kali.org.cn/> kali中文网

<http://xiao106347.blog.163.com/> xiao106347 kali折腾

更多大家推荐

渗透:

<http://www.wooyun.org/> 乌云

<http://bbs.blackbap.org/> 习科

<http://www.1937cn.net/> 1937

<http://forum.cnsec.org/> 暗组

<http://www.k33nteam.org/> keen team

<http://forum.eviloctal.com/> 邪恶八进制

<http://www.evil0x.com/> 邪恶十六进制

<http://www.myhack58.com/> 黑吧安全吧

<http://www.cnhonkerarmy.com/> 中国红客 红盟

<http://www.chinahacker.com/> 中国黑客联盟

<http://www.hxhack.com/> 华夏黑客联盟

<http://www.heikexiehui.com/> 中国黑客协会官网

<http://www.hackbase.com/> 黑基

<http://www.2cto.com/> 红黑联盟

<http://bbs.2cto.com/> 红黑联盟论坛

<http://www.hackwd.com/>

<http://www.heishou.com.cn/> 黑手安全网

<https://www.sitedirsec.com/> 非安全中国网

<http://www.zatokaszuki.com/> 学生技术联盟

逆向

<http://www.52pojie.cn/> 吾爱破解

<http://bbs.pediy.com/> 看雪论坛

一蓑烟雨貌似被关了，逆向方面了解不多，问问表哥们吧(?? ω ??)y

编程

<http://www.he11oworld.com/> hello word

<http://www.w3school.com.cn/> w3school

<http://www.runoob.com/> 菜鸟

<https://github.com/>

<http://navisec-Git.qiniudn.com/>

<http://c.biancheng.net/cpp/>

<http://www.liaoxuefeng.com/>

<http://www.php100.com/>

<https://ruby-china.org/wiki>

<http://bbs.csdn.net/forums/Java/>

<http://outofmemory.cn/tutorial/>

书籍

<http://zhuanlan.zhihu.com/Evi1m0/19706178> Evi1m0: 书籍推荐

<http://www.douban.com/doulist/3339701/> 信息安全必读书单

<http://www.douban.com/doulist/1363865/> 信息安全经典书籍

<http://www.zhihu.com/question/21390646>

http://my.oschina.net/bluefly/blog/335409?utm_source=tuicool&utm_medium=referral Web安全核心书单
连载

《安全参考》<http://www.douban.com/group/topic/72383272/> (2013年第一期--2015年第一期)全集

《书安》(更新中)

<http://www.secbox.cn/hacker/8205.html> 书安SecBook 第一期《icloud iOS安全大揭秘》

<http://www.secbox.cn/hacker/7366.html> 书安SecBook 第二期《信息安全攻防赛》

渗透实战文章可以看看里的杨凡(http://blog.sina.com.cn/s/articlelist_1758675673_4_1.html)

和法克文章 (<http://pan.baidu.com/share/link?shareid=249629&uk=2198816663>)

工具(黑软有分风险, 最好在虚拟机里搞)

<ftp://222.18.158.199/>(校园网内网可以访问, 不仅仅只有工具哦, 有许多总结, 各方面的)

<http://forum.cnsec.org/thread-94330-1-1.html> 2015暗组工具包(渗透)

<http://bbs.secbox.cn/thread-196-1-1.html> 2015_安全盒子工具包

<http://www.secbox.cn/hacker/tools/3552.html> 法客论坛2015工具包-第三版

<http://www.52pojie.cn/forum.php?mod=viewthread&tid=388015> 吾爱破解工具包 2015/7/22(逆向)

<http://down.52pojie.cn/> 爱盘 -- 在线破解工具包, 教程,

<http://www.52pojie.cn/thread-341238-1-1.html> 吾爱破解论坛专用破解虚拟机

ctf常用工具包请看<http://tieba.baidu.com/p/3933947157>里面群文件

其他

<http://www.zhihu.com/topic/19558642> 黑客知乎话题

<http://www.zhihu.com/topic/20011446> ctf知乎话题

<http://www.zhihu.com/topic/19561983> 信息安全知乎话题

<http://zhuanlan.zhihu.com/evilcos/19961466> 余弦知乎专栏

CTF方面

<http://blog.idf.cn/2015/02/ctf-field-guide/>

<http://tieba.baidu.com/p/3933947157> ctf大全

<https://ctftime.org/event/list/upcoming> 各种CTF赛事预告

(ps:国内各个高校或企业举办的比赛请进<http://tieba.baidu.com/p/3933947157>里面的群)

平时ctf练习

ctf逆向:

<http://reversing.kr/>

<http://pwnable.kr/>

<http://exploit-exercises.com/>

<http://overthewire.org>

<http://security.cs.rpi.edu/courses/binexp-spring2015/> bin 干货区

<http://www.52pojie.cn/forum-67-1.html> 【2014CrackMe大赛】

SQL:

<https://github.com/Audi-1/sqli-labs>

<http://redtiger.labs.overthewire.org/>

ctf XSS:

<http://prompt.ml/>

<http://xss.pkav.net/xss/>

<http://www.doscn.org/xss/>

<http://xss-quiz.int21h.jp/>

<http://escape.alf.nu/>

ctf综合练习:

<http://hackinglab.cn/> 网络信息安全攻防学习平台

<http://captf.com/> ctf题目

<http://cafebabe.cc/nazo/> 脑洞开发, 与ctf只有那么一点关系, 有85关了(?? ω ??)y

<http://1111.segmentfault.com/> 光棍节程序员闯关秀

<http://www.helloisa.com/test/>

<http://www.fj543.com/hack/> 黑客丛林之旅

<http://monyer.com/game/game1/> 梦之光芒的小游戏

<http://oj.xctf.org.cn/> XCTF_OJ练习平台

<http://hackgame.blackbap.org/> 习科黑客游戏

<http://ctf.3sec.cn/> Jlu.CTF

<http://www.baimaoxueyuan.com/ctf/> 白帽学院ctf挑战赛

<http://www.ichunqiu.com/tiaozhans/> i春秋ctf挑战

<http://ctf.idf.cn/> idf 实验室

<http://ctf.moonsos.com/pentest/index.php> 米安网ctf

<http://www.hetianlab.com/CTFace.html> 合天ctf

<http://www.shiyanbar.com/ctf/index> 实验吧(前名西普学院)

<http://hkyx.myhack58.com/> 黑吧安全网-红客闯关游戏

<http://202.108.211.5/> 实训竞赛系统

国外比较好的几个综合练习平台

<http://www.wechall.net>

<http://insight-labs.org/>

<http://wargame.kr/>

<http://canyouhack.it/>

<http://hackit.sinaapp.com/>

<http://webhacking.kr/>

<http://fun.coolshell.cn/>

<http://ringzer0team.com/challenge>

<https://backdoor.sdslabs.co/>

<http://smashthestack.org/> 漏洞利用练习网站

ctf writeup(WP):

直接百度:writeup(一边看一边总结,有道笔记,印象笔记什么的,最好能复现)

另外乌云和360安全播报上有些WP

<http://drops.wooyun.org/?s=writeup&submit=%E6%90%9C%E7%B4%A2>

<http://bobao.360.cn/ctf/>

<https://github.com/ctfs/> 各种 writeup

<http://sec.yka.me/> CTF Writeup Summary

<https://ctf-team.vulnhub.com/> Write Ups

更多请看<http://tieba.baidu.com/p/3933947157>