

ctf入门

原创

[鲨鱼饿死了](#) 于 2021-06-03 15:50:04 发布 66 收藏 1

版权声明：本文为博主原创文章，遵循 [CC 4.0 BY-SA](#) 版权协议，转载请附上原文出处链接和本声明。

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

版权

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

CTF===奥数

能力提升

思维能力

快速学习能力

技术能力

学校荣誉

这个就不多说了

发展前景

信息安全稀缺资源===DOTA选手 (说不定就成网红了呢o(∩∪∩)o)

可能会用到一个小众语言，一天内学习

如何入门-所需技能

如何入门—需要哪些基础

- 1、编程语言基础 (C语言、汇编语言、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 (各种通宵熬夜不睡觉)

有了这些基础能入门不？

不能！

如果没有这些基础怎么办？

且听我继续分 (che) 析 (dan)

https://blog.csdn.net/weixin_43123409

重要元素：逆向，算法——》数学
思想跳跃，推理

如何入门—如何学？

- 1、恶补基础知识 (**有基础的跳过此步**)
- 2、尝试从脑洞开始 (hackgame)
- 3、从基础题目出发
- 4、学习信息安全专业知识
- 5、锻炼体力耐力
(**泡妞？LOL？当然不是它们了，而是学习技术到通宵**)

后面陆续展开

https://blog.csdn.net/weixin_43123409

ctf比赛的分是很难的

如何入门—学之前的思考

前面其实都是扯淡，一个人如果不是特别的天资卓越，是无法一人撬动整个CTF比赛的，美国只有一个神奇小子 Geohot、韩国只有一个神童Lokihardt。

那么问题来了，**我们到底要如何学习呢？**

- 1、分析赛题情况
- 2、分析自身能力
- 3、选择更合适的入手

https://blog.csdn.net/weixin_43123409

赛题种类

如何入门—学之前的思考：分析赛题情况

PWN、Reverse偏重对**汇编、逆向**的理解

Crypto偏重对**数学、算法**的深入学习

Web偏重对**技巧沉淀、快速搜索能力**的挑战

Misc则更为复杂，所有**与计算机安全挑战有关**的都算在其中

https://blog.csdn.net/weixin_43123409

web偏向发散思维，对底层能力要求不高

如何入门—学之前的思考：分析自身能力（兴趣）

常规做法：

A方向：PWN+Reverse+Crypto随机搭配

B方向：Web+ Misc 组合

其实这里Misc所有人都能做

如何做你说的算！

精力有限先从一两个方向做起。

https://blog.csdn.net/weixin_43123409

如何入门—恶补基础知识&信息安全专业知识

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

https://blog.csdn.net/weixin_43123409

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

https://blog.csdn.net/weixin_43123409

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）

B方向:

Web应用安全权威指南

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

代码审计：企业级Web代码安全架构 https://blog.csdn.net/weixin_43123409

适合小白，最推荐《web应用安全权威指南》

怎么学ctf

如何入门—从基础题目出发

从基础题目出发（推荐资源）

<http://ctf.idf.cn/> Idf实验室：题目非常基础



我们不发起CTF
我们只做CTF题目编写



刷题动态



牛刀小试



刷题分享

https://blog.csdn.net/weixin_43123409

如何入门—从基础题目出发

从基础题目出发（推荐资源）

www.ichunqiu.com 有线下决赛题目复现，未来还会有更多精选比赛复现。

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



https://blog.csdn.net/weixin_43123409

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>



Leviathan

Bandit

Natas

Leviathan

Natas

Krypton

Behemoth

Ummio

Maze

Vortex

Sentinel

Marpige

Differ

REK3R3X3

HESPER

Abraxas

Wargames

The wargames offered by the OverTheWire community can help you to learn. To find out more about a certain wargame, just visit its page linked from the

If you have a problem, a question or a suggestion, you can join us on IRC.

Suggested order to play the games in

1. Bandit
2. Leviathan or Natas or Krypton
3. Natas
4. Behemoth
5. Ummio
6. Maze
7. ...

https://blog.csdn.net/weixin_43123409

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。

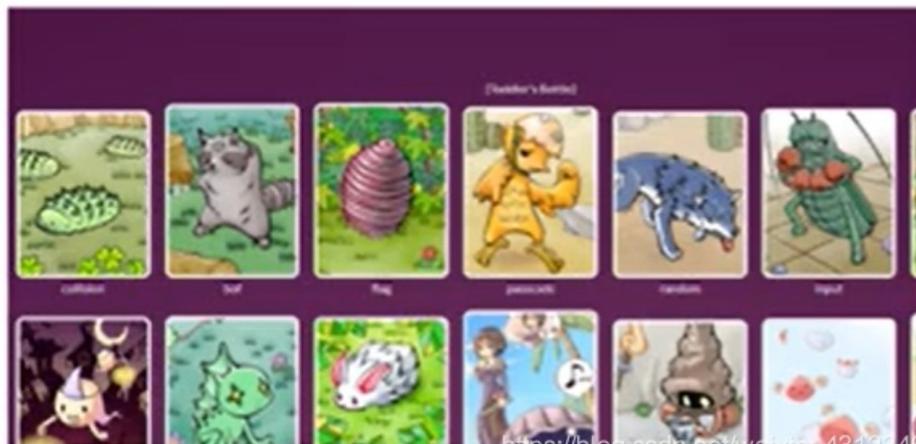


从基础题目出发（推荐资源）

<http://pwnable.kr/play.php> PWN类题目的游乐场

PLAY GAME

Early hacker catches the bug



https://blog.csdn.net/weixin_43123409

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)~

在线试玩



https://blog.csdn.net/weixin_43123409

从基础题目出发（推荐资源）

<http://prompt.ml/0> 国外的xss测试

prompt(1) to win

```
function escape(input) {  
  // warm up  
  // script should be executed without user interaction  
  return "<input type='text' value='" + input + "'>";  
}
```

https://blog.csdn.net/weixin_43123409

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

I know that my anti-blind-checks are not very consistent. So find the right way to exploit the levels. Anyway, have fun!

Start here -->	Level 1	Simple SQL-Injection	solved by 5249 hackers
	Level 2	Simple login-bypass	solved by 3895 hackers
	Level 3	Get an error	solved by 1348 hackers
	Level 4	Blind Injection	solved by 934 hackers
	Level 5	Advanced login-bypass	solved by 781 hackers
	Level 6	SQL-Injection	solved by 559 hackers
	Level 7	SQL-Injection	solved by 449 hackers
	Level 8	SQL-Injection	solved by 434 hackers
	Level 9	SQL-Injection	solved by 401 hackers
	Level 10		solved by 348 hackers

Hackers who solved the hackit

https://blog.csdn.net/weixin_43123409

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> https://blog.csdn.net/weixin_43123409

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

https://blog.csdn.net/weixin_43123409

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！

https://blog.csdn.net/weixin_43123409

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