# CTF

原创

ChengKaoAO 于 2017-10-18 15:31:25 发布 5444 收藏 225
分类专栏： CTF CTF 文章标签： ctf



CTF 同时被 2 个专栏收录
5 篇文章 0 订阅
订阅专栏
CTF
11 篇文章 0 订阅
订阅专栏

## 摘要

CTF是一种流行的信息安全竞赛形式，其英文名可直译为“夺得Flag”，也可意译为“夺旗赛”。

- 其大致流程是，参赛团队之间通过进行攻防对抗、程序分析等形式，率先从主办方给出的比赛环境中得到一串具有一定格式的字符串或其他内容，并将其提交给主办方，从而夺得分数。
- 为了方便称呼，我们把这样的内容称之为“Flag”。

---

## CTF对于我们的意义

### 1：CTF类似于奥数

### 2：能力提升

思维能力
快速学习能力
技术能力

### 学校荣誉

## 如何入门

### 基础

1：编程语言[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：体力脑力[熬夜突破某个技术]

### 如何学

1：恶补基础知识[有基础的可以跳过此步]
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[学习某个技术通宵，利用好周六周天]

## 分析赛题情况

pwn、Reverse{汇编、逆向}
Crypto{对数学，算法的深入学习}
Web{对技巧的沉淀，快速搜索能力}
Misc{各类新题型，包含以上，较为复杂}

>>>常规做法：

**A:Pwn+Reverse+Crypto[偏底层]**

**B:Web+Misc[发散思维]**

Suggestion：先从一个方向做起。

## 都需要学习的内容

Linux基础
计算机组成原理
操作系统
网络协议分析

## 推荐书籍

### A方向

IDA工具使用（F5插件） 逆向工程神器
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
黑客技术宝典

### B方向

Web应用安全权威指南(宏观角度让你了解信息安全)
Web前段黑客技术揭秘
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

## 从基础题出发

### CTF练习

idf实验室：http：//ctf.idf.cn {题目非常基础}
移动安全：http：//canyouhack.it{容易入门}
酷炫化：http://microcorruption.com/login{pwn、Crypto}
题库网站：http://oj.xctf.org.cn/xctf
国外ctf题库：http：//www.wechall.net/challs{国内选手成长摇篮}
http：//smashthestack.org
XCTF实训平台

### A方向

Wargame : Http://exploit-exercises.com
Pwn类题目的游乐场： Http：//pwnable.kr/paly.php

### B方向

米安的漏洞靶场：
http://moonsos.com/pentest/index.php
国外的XSS测试：
http：//prompt.ml/o
国外的SQL注入的挑战网站
http://redtiger.labs.overthewire.org

## 选择什么工具

### burp、IDA

### CTF 工具集

https://github.com/thruongkma/ctf-tools
https://github.com/Plakachu/volt
https://github.com/zardus/ctf-tools
https://github.com/TUCTF/Tools

## 利用比赛

以练促赛：选择一场已存在Writeup的比赛
以赛养赛：自己养成写Writeup的习惯

国际比赛：https://ctftime.org
国内比赛：http://www.xctf.org.cn

# 如何组织比赛

## 强力成员

1：思维活跃、灵活性、不会钻墙角
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

## 组建团队需要解决的问题

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[个人能力的成长]
3：梯队有序：如何建立阶层梯队
4：纪律严格：如何拒绝无团队精神的对员{军人的素质，责任感}