

# 信安之路CTF小组招募志同道合的朋友

原创

Harvey丶北极熊 于 2020-11-01 17:10:27 发布 517 收藏 4

分类专栏: [网络安全 CTF 渗透测试](#) 文章标签: [信息安全](#) [网络安全](#) [CTF](#)

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/qq\\_38867330/article/details/109430921](https://blog.csdn.net/qq_38867330/article/details/109430921)

版权



[网络安全](#) 同时被 3 个专栏收录

12 篇文章 0 订阅

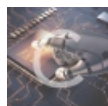
订阅专栏



[CTF](#)

20 篇文章 3 订阅

订阅专栏



[渗透测试](#)

14 篇文章 2 订阅

订阅专栏

## 信安之路CTF小组招募志同道合的朋友

CTF 是 Capture The Flag 的简称, 中文叫夺旗赛, 其本意是西方的一种传统运动。在比赛上两军会互相争夺旗帜, 当有一方的旗帜已被敌军夺取, 就代表了那一方的战败。在信息安全领域的 CTF 是说, 通过各种攻击手法, 获取服务器后寻找指定的字段, 或者文件中某一个固定格式的字段, 这个字段叫做 **flag**, 其形式一般为 `flag{xxxx}`, 提交到裁判机就可以得分。

CTF 题目类型一般分为 Web 渗透、RE 逆向、Misc 杂项、PWN 二进制漏洞利用、Crypto 密码破译, 有志于渗透测试的同学一开始建议从 Web 渗透的题目开始, 辅以 Misc 杂项和 Crypto 密码学。CTF 里面也有一血、二血、三血之说, 前三提交 Flag 能获得分数加成, 所以说手速快也很重要。

CTF 主要分为两种模式, 一是**解题模式**。对于 Web 安全来说, 会要求你入侵网站或者靶机, 攻击成功后系统会显示flag或者在某个目录文件数据库寻找 Flag, 提交到答题系统得分。逆向工程题目一般形式是破解注册机、动态调试、dump 内存等等。这些题目可以百度或谷歌别人的解题报告 (关键字: CTF writeup) 来认识一下。这种模式的缺点是类似于“应试教育”, 当前的趋势是注重出题难、出题偏, 没有考虑实际, 就跟奥数似的。而且这种模式只有攻击, 却没有防守, 而在企业中工作更多的还是考虑如何防护的问题, 这个时候 AWD 攻防赛模式就应运而生了。

二是**攻防赛**, 也叫 AWD(Attack With Defense, 攻防兼备)模式。你需要在一场比赛里要扮演攻击方和防守方, 攻者得分, 失守者会被扣分。也就是说, 攻击别人的靶机可以获取 Flag 分数时, 别人会被扣分, 同时你也要保护自己的主机不被别人得分, 以防扣分。这种模式非常激烈, 准备要非常充分, 手上要有充足的防守方案和 EXP 攻击脚本。我第一次参加这种比赛的时候就被打惨了QWQ, 不过后面参赛越多, 积累的经验就会越多。所以说, 这种比赛不用慌, 多打多学多积累就好了。

基于以上的介绍, 我们想组建一个CTF小组, 作为技术交流与组队参加CTF竞赛的小圈子。互相交流学习、参与各大CTF比赛、刷各大CTF平台, 共同学习。小组介绍如下:



## 组长介绍

常用ID: Harveysn0w-北极熊

职务: 信安之路CTF小组组长

工作: 某专科学校大二在读

个人博客: <https://harvey-blog.com>

内部CTF平台: <http://www.yqsec.club>

## 小组文章作品展

Bugku-WP(持续更新): <https://harvey-blog.com/Safety/2323>

从0到1: CTFer成长之路-WP(持续更新): <https://harvey-blog.com/Safety/1818>

Harveysn0w·北极熊-CTF专辑: <https://harvey-blog.com/ionsafe/ctf>

m0re-CTF专辑: [https://blog.csdn.net/qq\\_45836474/category\\_9717381.html](https://blog.csdn.net/qq_45836474/category_9717381.html)

CTFd平台搭建: <https://harvey-blog.com/Safety/1230>

H1ve-基于CTFd的美化平台搭建笔记: <https://blog.csdn.net/YIGAOYU/article/details/108663285>

AWD线下攻防平台搭建: <https://blog.csdn.net/YIGAOYU/article/details/107048115>

AWD线下攻防环境使用: <https://blog.csdn.net/YIGAOYU/article/details/107048865>

## 小组研究方向

Web、Crypto、MISC、Pwn、Reverse、Mobile、BlockChain

## 加入小组要求

满足以下任意一点即可:

- 1、目前正在参加CTF比赛或在各大CTF平台上有刷题记录并且撰写writeup
- 2、有Web安全&渗透测试经验、熟悉各种常见漏洞环境
- 3、有二进制逆向经验
- 4、掌握PHP、Java、python、C、C++其中任意两项
- 5、熟悉应急响应和数字取证、网络服务配置

编辑简历(自我介绍+CTF方向+加入小组原因以及在哪些平台刷过题目参加过哪些比赛)发送到harveysn0w@163.com。主题《申请加入信安之路CTF小组》