

CTF总结 (1)

原创

山兔1 于 2021-05-18 19:40:24 发布 165 收藏 3

分类专栏: [CTF](#) 文章标签: [信息安全](#)

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/m0_53008479/article/details/116999265

版权



[CTF 专栏收录该内容](#)

50 篇文章 1 订阅

订阅专栏

CTF: [catch the flag](#), **CTF** 比赛包括以下几个部分:

1. **WEB**: [SQL](#) 注入、文件包含、反序列化 (30%)。
2. **MISC**: 图片隐写、文件、压缩包伪加密、流量分析 (15%)。
3. 逆向: [z23](#) 本地破解 (20%)、软件逆向、安卓逆向。
4. 密码学: [RSA](#)、[MD5](#)、[BASE64](#)、猪圈密码。
5. **PWN**: (10%)
6. 汇编: (内存溢出、寄存器溢出)。

NC: 地址。

CTF 队伍一般是3人一队, 工业杯是四人一队。

初赛一般比的是理论、**CTF**, 决赛是 **AWD**, 通常一般比赛都是通过 **AWD** 来角逐出名次, **flag** 隔一定时间刷新一次。

国内著名的 **CTF** 比赛和举办方:

i春秋、奇安信、安恒、深信服、全国大学生安全竞赛、强网杯、网鼎杯。

CTF 练习平台:

[bunctf](#) [XCTF](#) [i春秋](#) [BUGKU](#)、[CTFHUB](#)、

CTF 比赛比完之后会让我们提交 [writup](#), 就是我们的解题过程,

WP 要加图片和文字。

CTF 学习过程的注意点:

1. **CTF** 会两个方向, 就是大佬了。
2. **PWN** 和逆向可以去学, 但不要去动他
3. 密码学必学
4. **WEB** 必须会的3种语言
5. [php](#) 100%会, [html](#) 要看懂, [python](#) 要会自动化脚本。
6. [php](#) 先学, 学完在学 [python](#), [python](#) 学些基础的就可以了。
7. [SQL](#) 注入、常见 [web](#) 漏洞要懂。
8. 先学 **MISC**。

AWD 代码审计很重要。

CTF 工具: [hackbar](#)、御剑、**BP**、

学 **CTF** 入门的, 主要以掌握工具为主和常见的网络协议和应用层协议、报文。

总结: 一开始去参见比赛, 拿不了奖, 见见世面也好。