

# ctf入门——实验吧

原创

搬运代码打工人  于 2017-10-29 21:44:59 发布  3130  收藏 11

分类专栏: [♥♥♥♥♥信息安全♥♥♥♥♥](#) 文章标签: [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/lancecrazy/article/details/78388356>

版权



[♥♥♥♥♥信息安全♥♥♥♥♥](#) 专栏收录该内容

1 篇文章 0 订阅

订阅专栏

###ctf简介

## 1. ctf:capture the flag

解题模式

攻防模式: 互相攻击

混合模式: 结合

## 2. 常见题型

- web: 常见web漏洞: 注入, xss, 文件包含, 代码执行, 上传等漏洞
- 密码学: 各种加解密技术,
- misc安全杂项: 流量分析, 电子取证, 人肉搜索, 数据包分析, 大数据统计,
- 逆向工程: 软件逆向, 破解技术:
- 隐写术: 熟悉隐写工具, 隐写算法
- 编程: 程序编程, 编程算法实现
- 溢出: 栈溢出, 堆溢出

## 3. 赛前准备

## 4. 比赛准备:

- 头脑清醒
- 团队合作
- 作战规划
- 后勤保障
- 大量信息搜集
- 开阔思路
- 抓住考点

## 5. 套路

- web: mysql, php特性, 文件上传绕过, 伪造http请求头
- 密码常见套路: 密码互相融合, 文件异或, hash长度攻击
- 杂项常见套路: 花式分析数据包, 各种隐写, 密码学知识大杂烩,
- 隐写常见套路, 各种因些工具, LSB, 文件开始结束符(图种), exif(图片原信息)  
###ctf工具
- web: firebox (hackbar, firebug)