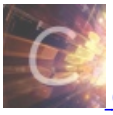
【CTF】基础常识

转载

你们这样一点都不可耐 于 2020-05-06 16:03:13 发布 925 收藏 23

分类专栏： CTF 文章标签： 信息安全 安全 经验分享 恰饭 程序人生

原文链接：https://blog.wujiaxing.cn/2019/10/28/2eb41b8f/



入门必读，少走弯路，少查百度

常见词释义

简称	全称	说明
CTF	Capture The Flag	夺旗赛，从题目信息中获取flag并提交
CTE	Capture the Ether	区块链智能合约，一般是漏洞利用
MISC	miscellaneous	杂项，CTF题目常见题目类型之一
RE	Reverse	逆向，CTF题目常见题目类型之一
Crypto	Cryptography	密码学，CTF题目常见题目类型之一
PWN	发音类似“砰”，是指攻破设备或者系统	系统/硬件破解，CTF题目常见题目类型之一
WEB	website	网站破解，CTF题目常见题目类型之一
Mobile	-	安卓破解，CTF题目常见题目类型之一
区块链	-	以太坊智能合约，CTF题目常见题目类型之一
Steg/Stego	steganography	隐写术，隐藏术
wp	writeup	解题思路，题目解题过程的记录
pl	playload	（有效攻击负载）是包含在你用于一次漏洞利用（exploit）中的ShellCode中的主要功能代码
shellcode	-	可提权代码
exp	exploit	漏洞利用，一般是个demo程序
poc	proof of concept	漏洞证明，一般就是个样本
vul	vulnerable	泛指漏洞
cve	-	漏洞编号，漏洞字典，国际上的
cnvd	-	漏洞编号，漏洞字典，中国的
0day	-	没打补丁，没公开的漏洞

简称	全称	说明
ak	all kill	某一类型题目或者全部题目都被解出
tql	taiqiangle	“太强了”的拼音首字母，常用于复读
ddddhm	daidaididihaoma	“带带弟弟好吗”的拼音首字母，常用于复读
一血	first blood	通常指比赛中最先得分/解出某题
套娃	-	题目有很多层，解完一层还有一层，类似俄罗斯套娃
容器		某类或某些题目解题需要创建出的在线环境，由于需要消耗服务器资源，一般有时间、并行数、操作频率等限制
动态积分	-	比赛中用来衡量成绩的得分，解出人数越多该题目的分数值就越低
非预期	-	在出题人预期的解题方法之外的可行解法
签到题	-	一般指比赛中送分的题目，可用于统计实际参赛人数或团队数
py	-	常用工具类编程语言python。有时也指比赛中通过非解题手段，从其他渠道或选手处违规获得flag或解题提示
出题人	-	题目（问题）的制造者，经常因为题目难度或脑洞过大被做题者口头威胁，是大家喜闻乐见的迫害对象
萌新/萌旧	-	一些很厉害的人自谦的称呼
大佬	-	恭维一些厉害的人的称呼
师傅	-	有问题请教一些不认识的人时的称呼，可用“大佬”替换。或前面加姓/id称呼德高望重的前辈
xxx爷爷	-	公认的对某一类型题目精通的大佬的称呼
菜鸟/菜狗/菜鸡	-	新入门或想入门的人的自称，有时也是一些大佬的自嘲
小白	-	从没接触过ctf出于好奇想入门的人
弟弟	-	在想要得到别人帮助时的自称
妹子/小姐姐	-	一类是比赛的客服。另一类是参赛选手，常被团队用来招新或大佬婉拒带人
菜	-	与“大佬”对应，是水群的常用语

题目类型细分

MISC

- 文件隐写
  - 图片隐写
  - 音频隐写
  - 视频隐写
- 进制转换
  - 不同进制间转换
  - 2/16进制转字符串
  - hex/base64与文件互转

- 编码解码
  - 二维码/条形码
  - base16/32/36/58/62/64/85/91/92
  - aes/des/rc4/rabbit/3des
  - 摩尔斯电码(Morse Code)
  - 凯撒密码
  - rot5/13/18/47
  - 栅栏密码
  - Unicode/UTF-8/URL/Hex/Html
  - Quoted-printable编码
  - XXencode
  - UUencode
  - 键盘编码
  - 敲击码(Tap code)
  - 培根密码
  - 当铺密码
  - 猪圈密码
  - 核心价值观编码
  - 图形编码
    - 圣堂武士密码
    - 盲文
    - 跳舞的小人
    - 国际信号旗
    - kobe code
- 流量分析
- 内存取证
- 代码混淆
  - brainfuck
  - Ook!
  - rockstar
  - deadfish
  - JSfuck
  - jother
  - JJEncoder/AAEncoder
  - PPEncoder
  - RREncoder
- 游戏题
- 各种杂学

WEB

- 信息泄露
- 弱口令
- SQL注入
- 文件上传
  - 存储型
  - 反射型
- 远程命令/代码执行漏洞(RCE)
- 跨站脚本漏洞(XSS-Cross Site Scripting)
- 跨站请求伪造漏洞(CSRF-Cross Site Request Forgery)

SAO姿势

一、根据上下文盲猜flag

1. XCTF-2020-高校战疫，签到题flag是‘flag{shijiejiayou}’，另一道叫“武汉加油”的题目的flag是flag{zhong_guo_jia_you}
2. 校内赛/萌新赛，题目一般备注出题人的昵称，这些昵称有时也会出现在flag中
3. 非容器题目的flag一般是“可读的”，可以 微调/补全 字词

二、Reverse/Pwn

这两类题有时flag以明文存储在附件文件中，直接搜索关键词即可

三、身体强壮的可以手动解题

1. 游戏类题目手动通关
2. 手动解300层有密码压缩包
3. 人工爆破flag

原文：https://blog.wujiaxing.cn/2019/10/28/2eb41b8f/
作者：河东小伍