CTF题目难度等级划分

原创

vper123 于 2021-11-18 18:24:50 发布 359 收藏

分类专栏： CTF 文章标签： 安全

本文链接：https://blog.csdn.net/m0_51193993/article/details/121407056

CTF题目难度等级(1-10)：

难度等级	描述	用途	例子	最大分值
1	赛题的考点是非常常见的，选手们对于此类赛题可以直接进行解题步骤，并且在较短的时间内得到正确答案。该难度下通常不需要利用额外的工具，依靠通常电脑上有的程序便能够解题。	1. 通常用于ctf线上比赛的签到题； 2. 对安全方向感兴趣但是没有去学习、或者刚刚接触安全方向的人员，此类主要是为了培养做题人的兴趣。	web: get/post请求、修改head头信息、cookie修改 reverse:程序中直接明文包含flag，记事本打开时能直接发现flag的 misc:常规编码格式，例如base64、莫斯密码 crypto:古典密码，例如凯撒密码	50
2	赛题需要有一定基础知识培训的人才能够做出来，选手需要有较短时间的考虑分析，然后才会进行解题步骤的。该难度下有时候需要选手学会使用额外的特殊工具来进行做题。	1. 有时候会用于ctf线上赛签到； 2. 适用于新手，让他们能学到更多的知识； 3. 常规赛题中的送分题类型。	web: 简单的无保护措施sql注入、git信息泄露 reverse: flag被异或加密之后的可执行程序、upx加壳之类 misc: 简单隐写，如图片文件中隐藏有一个压缩包；简单数据包分析，如数据包中直接存在flag明文字符串 crypto: 简单的加密，例如异或加密 pwn: 用户输入超过一定范围(溢出)便能获得flag的	100

难度等级	描述	用途	例子	最大分值
3	赛题可能由多个1、2等级的考点结合起来，或者是需要对安全知识具有一定的掌握才能能够解答出来的。该难度下，选手可能需要对赛题中的代码进行分析，需要有一定的代码基础。	1. 通常情况下用于一般比赛的简单赛题； 2. 不太适用于新手，可作为对入门选手的难题或者拔高之类。	web: sql存在waf的注入、xss、文件上传 reverse: 代码逻辑稍微复杂、可能存在简单的混淆、花指令、反调试之类 misc: 稍微复杂的隐写或者文件格式被破坏，需要重新构建文件格式 crypto: 给出密钥的加密算法 pwn: 能通过栈溢出直接在栈中执行代码获得shell的	200
4	赛题考察的知识点较偏但实际掌握之后并不算难的，或者是题目出的会有新意，能让选手掌握到一定的知识技能，题目中可能会存在上面几种难度的知识点作为铺垫。该难度下，选手需要有一定的编程能力，能独立编写脚本，具有快速学习能力。	1. 比赛时这种题目的数量较多，需求量较大； 2. 中等难度的题目，对于不同的比赛都有可能出现此类题。	web: CSRF、爬虫脚本、一定难度的逻辑漏洞 reverse: 算法问题、小众语言分析、代码混淆 misc:文件格式分析、不常见隐写方法、 crypto:简单的针对加密算法加密特性攻击 pwn: 栈不可执行的栈溢出，且程序中不存在system等关键函数、简单的格式化字符串	300
5	赛题开始出现了类型分化，对于不同类型的题，对于大部分选手来说不一定能全部掌握知识点，将会存在解答不出来的情况。在该难度下，选手通常需要几个人一起去进行比赛；需要选手对安全方面的研究要更加深入，分析代码问题。	1. 中等偏难题，适用于学习一年左右相关知识点的选手； 2. 对于偏类型选手来说不能够轻松解答。	web: 反序列化、常用项目漏洞的考察 reverse: 算法问题、代码逻辑复杂、迷宫求解问题 misc: 磁盘内存分析、难度较高的隐写方法 crypto:针对加密算法加密特性攻击，rsa特性攻击 pwn:堆利用，例如一般的uaf、fastbin attack	400
6	针对不同类型的考点专一性更强，需要专门为此方向学习了解很长时间。该难度下，对于选手知识掌握有着较高的考验，学习好不好，扎不扎实，都能够得到很好的检验。	1. 解题较为困难，国内高校一般队伍难以解答； 2. 适用于通常比赛中的亮点题； 3. 作为难题出现。	web: 区块链智能合约漏洞 reverse:不同架构方面的逆向，难度也更高 misc: crypto: pwn:IO_FILE结构体的利用，例如FSOP	500
7	该难度等级中的每一题的知识点都需要选手长期不断的学习，跟着知识点技术的进步去一步一步的达到高难度的水平。	通常比赛很少出现，作为国内顶尖赛事的难题，适用于国内顶尖战队的队伍去解答	defcon 3bit构架攻防	-
8	对于给定的考题，从基本框架层次上进行攻击。	适用于国际顶尖强队	针对于php语言本身存在的漏洞进行攻击利用	-
9	对于操作系统的攻击，需要选手掌握一个甚至好几个0day	适用于众测项目	针对最新版windows、linux、mac os的攻击	-

难度等级	描述	用途	例子	最大分值
10	对于架构的攻防，Inter/AMD/Arm，CPU内核漏洞	-	针对cpu、主板的漏洞进行攻击	-