ctf 选择题 题库_CTF 试题初体验

原创

weixin_39576066 于 2020-12-19 21:44:32 发布 1063 收藏 2
文章标签： ctf选择题 题库

被逗哥(@Hustcw)安利了一波 CTF 赛，作为萌新我决定找点题目练练手。

什么是 CTF？

CTF(Capture The Flag)中文一般译作夺旗赛，在网络安全领域中指的是网络安全技术人员之间进行技术竞技的一种比赛形式。其大致流程是，参赛团队之间通过进行攻防对抗、程序分析等形式，率先从主办方给出的比赛环境中得到一串具有一定格式的字符串或其他内容，并将其提交给主办方，从而夺得分数。

CTF 主要分为3类比赛模式：

一、解题模式(Jeopardy)

在解题模式CTF赛制中，参赛队伍可以通过互联网或者现场网络参与，这种模式的CTF竞赛与ACM编程竞赛、信息学奥赛比较类似，以解决网络安全技术挑战题目的分值和时间来排名，通常用于在线选拔赛。题目主要包含逆向、漏洞挖掘与利用、Web渗透、密码、取证、隐写、安全编程等类别。

二、攻防模式(Attack-Defense)

在攻防模式CTF赛制中，参赛队伍在网络空间互相进行攻击和防守，挖掘网络服务漏洞并攻击对手服务来得分，修补自身服务漏洞进行防御来避免丢分。攻防模式CTF赛制可以实时通过得分反映出比赛情况，最终也以得分直接分出胜负，是一种竞争激烈，具有很强观赏性和高度透明性的网络安全赛制。在这种赛制中，不仅仅是比参赛队员的智力和技术，也比体力(因为比赛一般都会持续48小时及以上)，同时也比团队之间的分工配合与合作。

三、混合模式(Mix)

结合了解题模式与攻防模式的CTF赛制，比如参赛队伍通过解题可以获取一些初始分数，然后通过攻防对抗进行得分增减的零和游戏，最终以得分高低分出胜负。采用混合模式CTF赛制的典型代表如iCTF国际CTF竞赛。

上手题

萌新当然选择解题模式上手啦。找到了一个入门网站 ctflearn.com，特意 随便选了几道 Easy 的题目试试。

Problem A - Basic Injection

检查 html 文件，发现 input 栏上有注释：

于是我随便试了几个名字，发现查询 Luke 时，会展示 data：

因为这是一道简单题，我猜测很可能通过很简单的 SQL注入 的方式就能拖库，于是键入 ' or '1'='1。(后台很可能就是一条 SQL:

SELECT * FROM users WHERE name = 'SOMENAME_KEYIN'

果然，注入成功。Flag 为 th4t_is_why_you_n33d_to_sanitiz3_inputs

Problem B - FORENSICS 101

题目给了一个图像文件：

要从二进制文件里取到 Flag，我立马用 python 将图片文件以二进制读入，然后查询其中是不是夹带了 Flag。

果然夹带了 flag！

Problem C - Taking Ls

题目给了一个 zip 包 The Flag.zip，使用 unzip 解压时发现里面有个隐藏文件夹 .ThePassword，内含 ThePassword.txt，查看此文件发现一份密码 Im The Flag.

The Flag/ 下还有一个 pdf 文件，需要密码打开，输入上一步中得到的密码就行啦。

Problem D - WIKIPEDIA

题目没有给定任何文件，只给了两个关键字 WIKIPEDIA 和 128.125.52.138。

于是上 WIKIPEDIA 搜索这个 ip，得到以下结果：

发现在词条 Flag 下有一个 diff 来源于 128.125.52.138，查看这个 diff 的详情：

得到 FLAG{cNi76bV2lVERlh97hP}！