LitCTF2023备赛指南 暨 知识点清单

校外赛道QQ群：782400974

前期准备：

如果对CTF不熟悉可以先看 【CTF快速入门手册】https://github.com/ProbiusOfficial/CTF-QuickStart
同样提过视频教程：【CTF快速入门手册——第一讲什么是CTF 以及如何入门】https://www.bilibili.com/video/BV13o4y1x7L2/

关于

- 本次比赛五个方向，分别是：Web、Pwn、Crypto、Misc、Reverse
- 如果在做题过程中没有思路没有头绪 请善用搜索引擎 同时 也我们运行您使用Chat GPT这类Ai产品辅助答题 因为网络安全从来都是开卷的 能寻找工具 利用工具 善用工具本就是我们互联网赋予我们的优势
- MISC中出了常规题目 还有GAME —— Minecraft | OSINT —— 开源情报获取
- Crypto 题目有古典密码学 和 现代密码学 两个部分 | 最后三道题目为算法题目 采用时间+数据样例给分 题目内容和ACM相似 难度为省选+提高

考点

因为是校内第一次CTF赛，为了给刚入门的各位更好的答题体验，所以这里提供每个方向的考点，供大家参考。

Web

- HTML + CSS + JS 基础(会查看源码 能看懂简单的js代码 了解一些特殊的js如JSfuck)
- 会有一些游戏题 你可以自行选择遵守规则还是 绕过 / 打破规则(比如来到规则的后台)
- PHP 基础 (常见的PHP语法 一句话木马形式 一些命令执行函数)
- SQL 注入 (SQL基础 数字型SQL注入 以及 小变形)
- 网络基础请求 GET POST
- 请求包参数 Cookie UA头 Reference ...
- 抓包 前端校验 后端校验 bypass
- Github中一些 git的特性 如 git泄露 commit 查询等等

MISC 杂项

- MISC中有一些带有 **OSINT** 标志的题目 这类题目为开源获取 你需要根据题目附件中的信息来获取题目要求的情报，包括但不限于
    - 图片拍摄信息 拍摄时间 拍摄地点 拍摄经纬度
    - 图片内容特点 标志性建筑物 特征性文字 场景
      你可能需要借助一些搜索引擎(如百度识图 谷歌识图等)去从图片中发掘更多信息
- MISC 题目有涉及到一些古典密码 / 常见编码 的考察 如Base64 当然也有一些根据某些特征写的古典密码加解密
- 图片隐写 图片隐写比较简单的 如直接附加 篡改高度
- 文件修复 涉及到文件结构 头 体 尾 三个部分的其中一个 这次主要是考察图片文件的修复
- 上面提到的 基于文件的 如 部分隐写 文件修复 可能需要在文件的16进制形势下进行 这里推荐 010Editor 或者 WinHEX

Crypto 密码学

- Crypto这次提供四道古典密码题目(虽然按照目前的形式他们应该在MISC 但是严格意义来讲 古典密码属于密码学)
- 古典密码的考点涉及的即是 古典的核心 替换 位移 混淆 ， 这次比赛主要考察目前CTF常见的密码 当然也有创新的古典密码 (比如某些游戏的符号语言 涉及生物知识的密码语言)
- 然后便是现代密码 这也是如今CTF中密码学的核心考点，比如RSA，对于RSA我们考察主要是 基础的RSA过程 在针对因数分解的时候用到的工具 网站
- 然后便是在RSA的基础上 基于一些数学理论(可能是初中 高中的方程 也可能是一些现代的数学定理)进行加工后再RSA
- 当然RSA 核心点有一个欧拉定理 这也能是考点
- 最后 Crypto 提供三道算法题目 题目题目和ACM一样 但是评判规则为时间+数据点维度 支持C Cpp java Python

Reverse 逆向工程

- 逆向工程这次考察不难 主要是会使用IDA进行基础的静态调试 理解简单的程序逻辑(如位运算 XOR AND 之类)即可
- 常用的如：
    - Shift + F12 查看字符串
    - 跟进
    - X 进行跟进
    - F5反编译源码
- 难题会涉及到一些编码算法的逆向 如Base64的 Encode / Decode

PWN 二进制

PWN的入门门槛较高 所以 这里提供的题目都是比较简单的，考点大概就是下面的

- 知道和使用 NC 命令即是 nc ip prot 这样的命令
- 然后是Linux的一些基础命令 如怎么看当前目录有哪些文件 怎么看某些文件的内容 等等
- PWNtool 交互工具的基本使用 能够编写简单的脚本
- 最后是一道基础的栈溢出题目