Bugku CTF梳理

原创

AquilaEAG 于 2021-04-10 10:49:55 发布 109 收藏

本文链接：https://blog.csdn.net/weixin_43202635/article/details/115564581

大佬的刷题记录：https://blog.csdn.net/mcmuyanga

1.CTF常见题型

CTF比赛通常包含的题目类型有七种，包括MISC、PPC、CRYPTO、PWN、REVERSE、WEB、STEGA。

> **MISC(Miscellaneous)类型**，即安全杂项，题目或涉及流量分析、电子取证、人肉搜索、数据分析等等。
>
> **PPC(Professionally Program Coder)类型**，即编程类题目，题目涉及到编程算法，相比ACM较为容易。
>
> **CRYPTO(Cryptography)类型**，即密码学，题目考察各种加解密技术，包括古典加密技术、现代加密技术甚至出题者自创加密技术。
>
> **PWN类型**，PWN在黑客俚语中代表着攻破、取得权限，多为溢出类题目。
>
> **REVERSE类型**，即逆向工程，题目涉及到软件逆向、破解技术。
>
> **STEGA(Steganography)类型**，即隐写术，题目的Flag会隐藏到图片、音频、视频等各类数据载体中供参赛者获取。
>
> **WEB类型**，即题目会涉及到常见的Web漏洞，诸如注入、XSS、文件包含、代码执行等漏洞。

2.CTF常见解题姿势

2.1 MISC类型

Miscellaneous简称MISC，意思是杂项，混杂的意思。

杂项大致有几种类型：

1. 隐写
2. 压缩包处理
3. 流量分析
4. 攻击取证
5. 其它

CTF-MISC总结

CTF MISC常用工具

CTF解题技能之MISC基础

CTF培训-杂项的基本解题思路上半部分

CTF-Misc之隐写术

ctf-misc总结(一)

ctf-misc总结（二）

2.2 CRYPTO类型

1. 摩斯密码
2. 栅栏密码
3. Ook 密码
4. Brainfuck 密码
5. 凯撒密码：
6. Base64 编码 及其混合
7. 类栅栏密码
8. 由0和1组成的摩斯密码
9. Base64 等等各种编码来回转（不知道是谁想得出这么傻b的题型，很无聊）
10. 键盘格子密码
11. 托马斯杰斐逊 转轮密码
12. Base91 编码
13. 核心价值观编码
14. Linux系统的 shadow 文件格式
15. ZIP 伪加密
16. RSA 加解密
17. 标准银河字母
18. 仿射密码 affine cipher

CTF crypto 密码类 题型积累

CTF-Crypto-各种密码原理及解密方法

CTF密码学部分知识总结（一）

CTF密码学部分知识总结（二）

2.3 PWN类型

Pwn是一个骇客语法的俚语词，自”own”这个字引申出来的，这个词的含意在于，玩家在整个游戏对战中处在胜利的优势，或是说明竞争对手处在完全惨败的情形下，这个词习惯上在网络游戏文化主要用于嘲笑竞争对手在整个游戏对战中已经完全被击败（例如：”You just got pwned!”）。

在骇客行话里，尤其在另外一种电脑技术方面，包括电脑（服务器或个人电脑）、网站、闸道装置、或是应用程序，”pwn”在这一方面的意思是攻破（”to compromise”，危及、损害）或是控制（”to control”）。在这一方面的意义上，它与骇客入侵与破解是相同意思的。例如某一个外部团体已经取得未经公家许可的系统管理员控制权限，并利用这个权限骇入并入侵（”owned” 或是“pwned”）这个系统。

CTF中pwn的入门指南

[新手向]Pwn学习笔记：CTF pwn题解题套路实战

Pwn学习历程（1）–基本工具、交互、调试

CTF必备技能丨Linux Pwn入门教程——环境配置

CTF必备技能丨Linux Pwn入门教程——栈溢出基础

CTF必备技能丨Linux Pwn入门教程——ShellCode

ctf中pwn题目总结

2.4 REVERSE类型

Reverse | 逆向入门学习（一）

攻防世界-CTF小白-reverse（新手）

攻防世界reverse新手题wp（通俗易懂）

2.5 WEB类型

1. 基础知识类题目
2. 查看网页源代码
3. 发送HTTP请求
4. 不常见类型的请求发送
5. HTTP头相关的题目
6. 查看相应头
7. 修改请求头、伪造Cookie
8. Git源码泄露
9. python爬虫信息处理
10. PHP代码审计
11. PHP弱类型hash比较缺陷
12. 数组返回NULL绕过
13. 正则表达式相关
14. 命令执行漏洞
15. XSS题目
16. 绕过waf
17. 长度限制
18. 双写
19. 等价替代
20. URL编码绕过
21. Linux命令使用反斜杠绕过
22. URL二次解码绕过
23. 数组绕过
24. SQL注入
25. 使用sqlmap

CTF中Web题目的常见题型及解题姿势

CTF-WEB总结（三）

CTF-WEB总结（四-题目来源i春秋）