CTF MISC和WEB练习记录

原创

极客闪烁 于 2021-11-08 23:46:13 发布 2169 收藏

分类专栏： 服务器 文章标签： 安全

版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/qq_40249515/article/details/121218492

版权

服务器 专栏收录该内容

3 篇文章 0 订阅

订阅专栏

CTF MISC和WEB练习记录

一、CTF是什么？

CTF是一种流行的信息安全竞赛形式，其英文名可直译为“夺得Flag”，也可意译为“夺旗赛”。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。为了方便称呼，我们把这样的内容称之为“Flag”。

二、MISC练习记录

1.如果通过word或者pdf的手段打开某张图片，获取信息可以考虑下flag是不是被隐藏，想办法找出所有信息来。
2.多熟悉加密类型，比方说这次遇到的佛曰加密，乍一看人都傻了。这是个啥？注意多层加密

> ROT13（回转13位，rotate by 13 places，有时中间加了个连字符称作ROT-13）是一种简易的替换式密码。它是一种在英文网络论坛用作隐藏八卦（spoiler）、妙句、谜题解答以及某些脏话的工具，目的是逃过版主或管理员的匆匆一瞥。ROT13被描述成“杂志字谜上下颠倒解答的Usenet点对点体”。ROT13也是过去在古罗马开发的凯撒加密的一种变体。

3.多注意文件类型，当文件缺失部分内容的时候，知道缺失部分的大体内容，类型。
4.注意反编译，多使用反编译工具。
5.多熟悉进制类型之间的转换和进制类型的形态。
6.对于未知文件（这次是ext3），建议善用Winhex进行分析。建议了解文件头尾总结和常见文件头
7.Stegsolve可以分析图片Stegsolve教程
如果是gif可以考虑他是不是有多张
8.注意进行数据恢复、报文分析
9.rar伪加密 看 50 4B 03 04 其第八位应该是08 ， 分析时应当注意
10.wireshark分析pcapng文件（流量包），也需要配合Hex分析文件。

三、WEB练习记录

1.多f12，说不定就能从源码中找到逻辑BUG或者留下的FLAG，同时多注意导航栏，拼接字符串。
2.Robots协议

> robots协议也叫robots.txt（统一小写）是一种存放于网站根目录下的ASCII编码的文本文件，它通常告诉网络搜索引擎的漫游器（又称网络蜘蛛），此网站中的哪些内容是不应被搜索引擎的漫游器获取的，哪些是可以被漫游器获取的。因为一些系统中的URL是大小写敏感的，所以robots.txt的文件名应统一为小写。robots.txt应放置于网站的根目录下。如果想单独定义搜索引擎的漫游器访问子目录时的行为，那么可以将自定的设置合并到根目录下的robots.txt，或者使用robots元数据（Metadata，又称元数据）。

3.php中备份的文件一般为.bak、
4.数据传输多注意cookie
5.熟连掌握h5
6.账号密码表单可以尝试弱密码或者字典爆破。
7.xff和referer是可以伪造的，实现途径可通过抓包进行。（burpsuite）
8.php一句话可以用webshell直接登录；
9.waf,同时要非常熟悉linux操作才行；

> Web应用防护系统（也称为：网站应用级入侵防御系统。英文：Web Application Firewall，简称：WAF）。利用国际上公认的一种说法：Web应用防火墙是通过执行一系列针对HTTP/HTTPS的安全策略来专门为Web应用提供保护的一款产品。

10.多熟悉进制类型之间的转换和进制类型的形态，进行分析。还有ASCii

总结

发散思维，打好基础！！，创新，大胆，尝试！

创作打卡挑战赛
赢取流量/现金/CSDN周边激励大奖