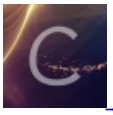
i春秋网鼎杯网络安全大赛blend题目writeup

原创

iqiqiya 于 2018-10-24 10:56:35 发布 1846 收藏
分类专栏： 我的逆向之路 ------2018i春秋网鼎杯 我的CTF进阶之路 文章标签： blend题目writeup i春秋网鼎杯

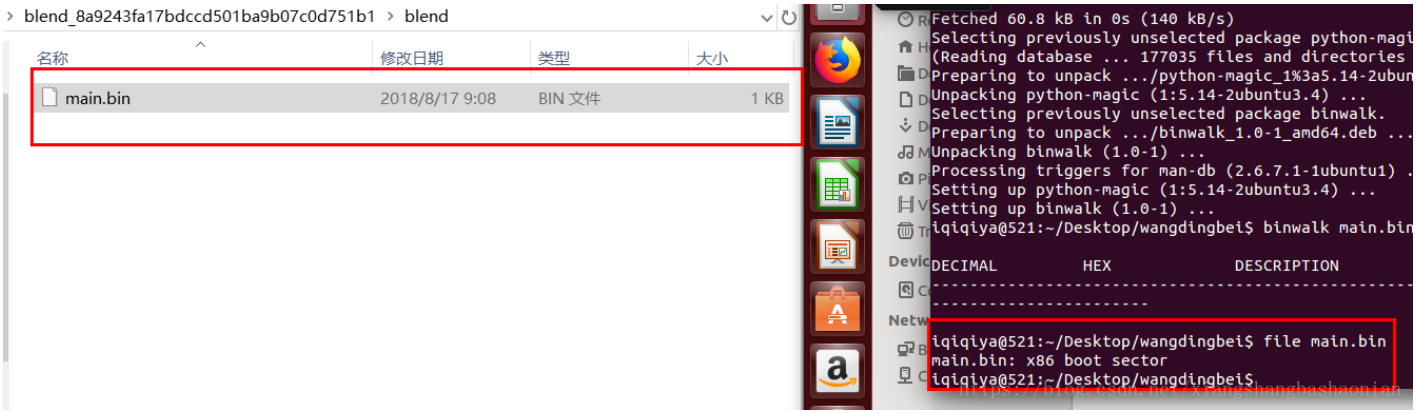

我的逆向之路 同时被 3 个专栏收录
108 篇文章 10 订阅
订阅专栏


------2018i春秋网鼎杯
6 篇文章 0 订阅
订阅专栏

我的CTF进阶之路
108 篇文章 18 订阅
订阅专栏

下载后解压 发现只有1KB what？？？

file 一下 说是main.bin: **x86 boot sector**



百度了一下下

说这个东西是linux的引导扇区

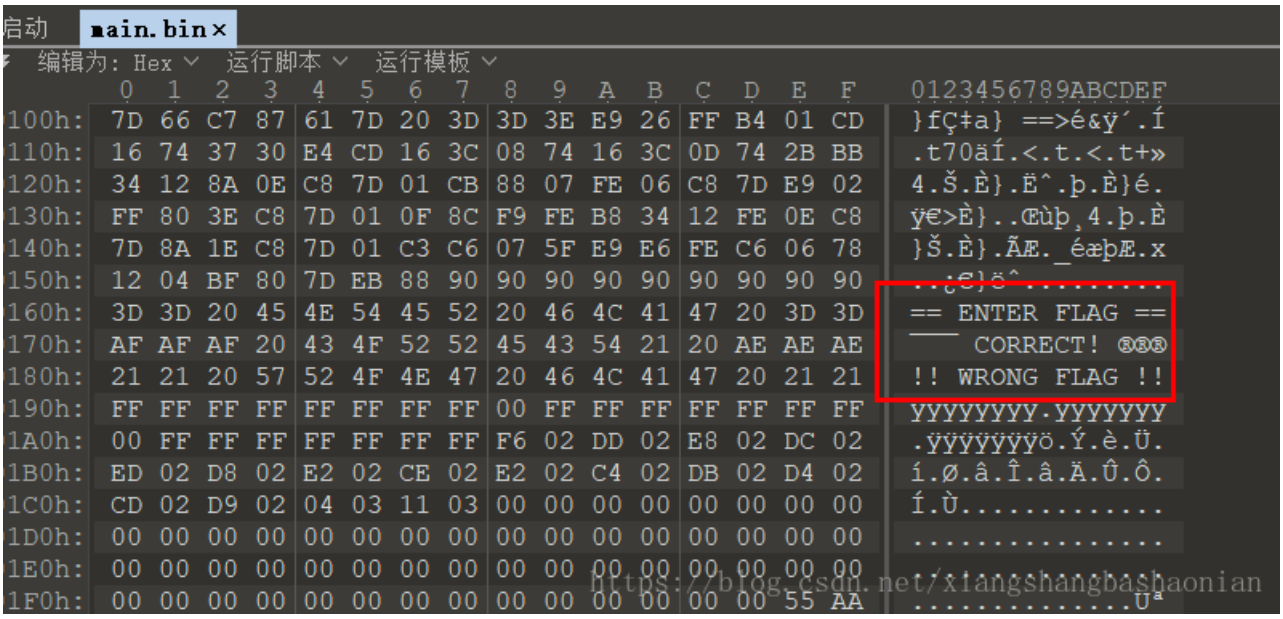
Boot sector是硬盘(严格来说是所有可引导的存储介质)上的第一个扇区，大小为512字节，这个扇区对于计算机启动来说至关重要。
主要分为三个部分，分别是：

MBR(master boot record,主引导记录)446字节

DPT(disk partition table,磁盘分区表)64字节

BRID(boot record ID引导记录标识)2字节

然后直接010 Editer打开 发现



这道题目与其他的题目不一样　文件既不是Linux也不是Windows下的可执行文件，而是需要在QEMU全系统仿真器下才能运行的MBR(主引导记录)

QEMU就是一个通用的开源机器模拟器和虚拟器

运行的命令为：**qemu-system-i386 -drive format=raw,file=文件名**

等补坑

参考链接：

https://github.com/TechSecCTF/writeups/blob/master/CSAWQuals2017/realism/README.md

https://xz.aliyun.com/t/2608#toc-11

https://www.jianshu.com/p/005bda1f8535

https://blog.csdn.net/ww1473345713/article/details/51602825?locationNum=5&fps=1