# wmctf2020-记录-writeup

原创

拾光、 于 2020-08-03 12:34:12 发布 3540 收藏 3
分类专栏： ctf 文章标签： wmctf ctf wmctf2020 writeup



目录



---

周末参加了一下wmctf2020，只做出了三道简单题目。简单记录一下。

## Misc：sign-in

welcome to WMCTF2020,here is your flag: https://t.me/WMCTF

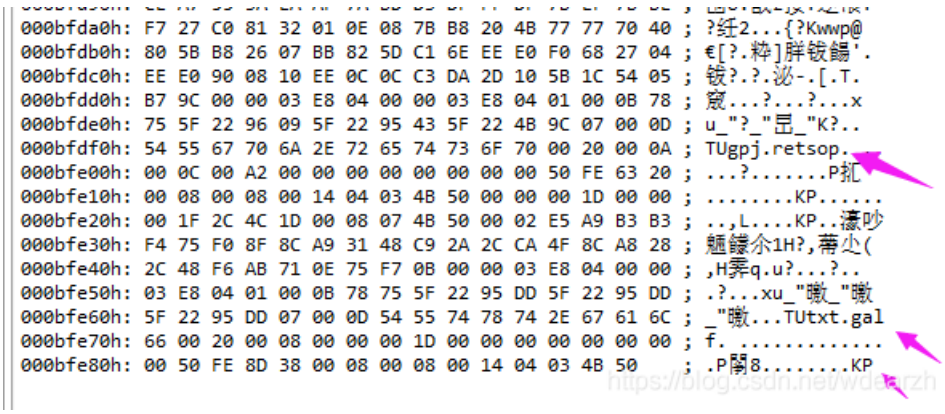
打开网址发现拒绝连接，因为是个短网址，尝试访问短网址地址，同样的错误。搜了下域名发现是国外地址，找了个F墙软件成功打开，里面需要下载的app，下载安装上加入提示的群组，在聊天框上方里即可看到flag。

---

## Misc：XMAN_Happy_birthday!

下载下载是一个zip文件，解压失败，网上找了下zip文件格式，改了下文件头，也不对。

继续往下看看到最后的时候发现是做了逆序的文件，写个脚本把文件内容再做个逆序就可以了。




上图可以看到倒序的 flag.txt和 destop.jpg文件名字符串，还有最后方是个倒序的 zip文件开头。

写个倒序处理文件的脚本：

```
with open("D:\\ctf\\wmctf\\XMAN\\daolnwod.zip","rb") as f:
    tmp = f.read()
with open("D:\\ctf\\wmctf\\XMAN\\daolnwodreverse.zip","wb") as f:
    f.write(tmp[::-1])
```

解压新生成的文件即可。

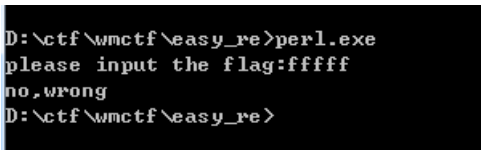
---

## Reverse：easy_re

题目描述：The flag is hidden in the perl code, can you find it?

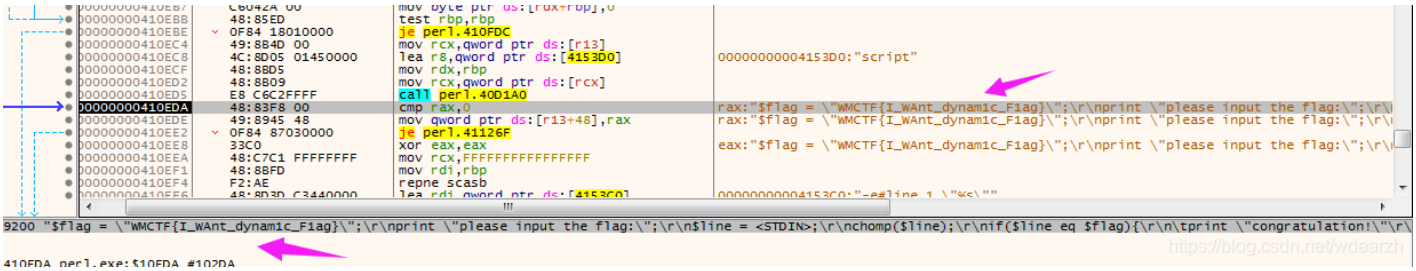
使用ida打开发现是个64位的程序，看题目应该是perl脚本转成的exe程序，网上搜了下perl反编译得工具没有找到。

执行了一下如图：




使用ida查看字符串也没有找到 这俩字符串，点了动态调试，(以前没用过ida的动态调试， olldbg没法调试64位程序) 考虑应该会将perl代码加载到内存中，随便点了一些 提取内存快照后 搜索字符串找到了字符串。不过还是不太会动态调试就先放下了。

第二天下了个x64dbg 单步跟踪，没花多久就找到了perl代码：




获取到的perl脚本：

```
$flag = "WMCTF{I_WAnt_dynam1c_F1ag}";
print "please input the flag:";
$line = <STDIN>;
chomp($line);
if($line eq $flag){
 print "congratulation!"
}else{
 print "no,wrong"
}"
```