

# xctf攻防世界 MISC高手进阶区 MISCall

原创

18947943 于 2022-01-17 14:53:13 发布 3664 收藏

分类专栏: [攻防世界misc之路](#) 文章标签: [misc](#)

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/18947943/article/details/122539125>

版权



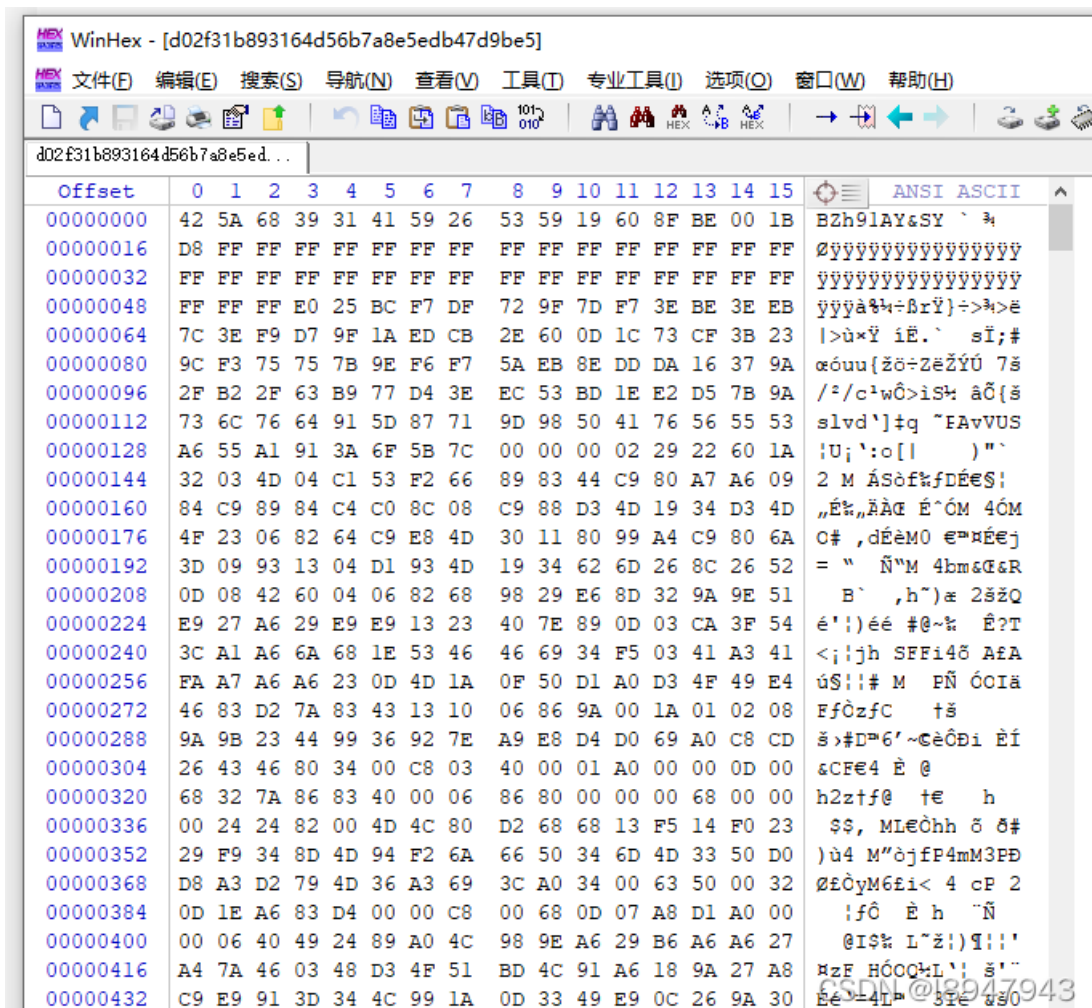
[攻防世界misc之路](#) 专栏收录该内容

68 篇文章 2 订阅

订阅专栏

## 1. 进入环境, 下载附件

给的是一个磁盘文件, 不知道怎么打开, 果断扔进winhex, 如图:



## 2. 问题分析

### 1. 判断文件类型

做了这么多题，总结起来就是搜关键词，其次看文件头和尾部是否有包含的文件，最后就是看文件的头进行判断，修改尾缀。

这个题文件开始为 425A68，对照：各类文件的文件头标志，得知该文件是个Bzip文件或者我们把文件扔进kali中查看文件的类型，如图：

```
(zhangfa@kali)-[~/下载]
└─$ file d02f31b893164d56b7a8e5edb47d9be5
d02f31b893164d56b7a8e5edb47d9be5: bzip2 compressed data, block size = 900k

(zhangfa@kali)-[~/下载]
└─$
```

### 2. 修改类型解压

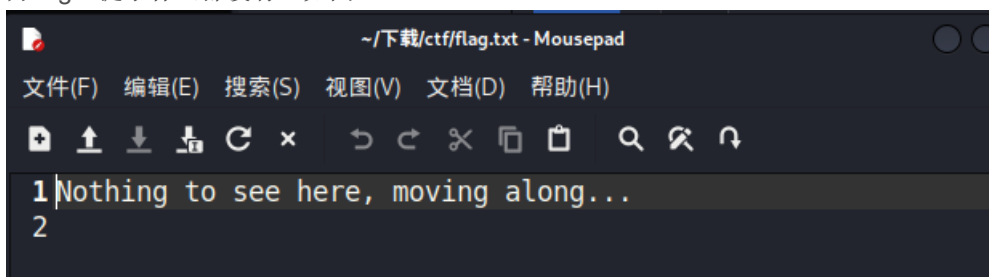
将其修改为bzip2后缀文件然后解压：

```
mv d02f31b893164d56b7a8e5edb47d9be5 d02f31b893164d56b7a8e5edb47d9be5.bzip2
tar jxvf d02f31b893164d56b7a8e5edb47d9be5.bzip
```

解压后如图：



有一个git和flag，打开flag，提示什么都没有，如图：



### 3. git中恢复

去git目录下，查看一下git日志，如图：

```
git log
```

```
(zhangfa@kali)-[~/下载/ctf]
└─$ git log
commit bea99b953bef6cc2f98ab59b10822bc42afe5abc (HEAD -> master)
Author: Linus Torvalds <torvalds@klaava.Helsinki.Fi>
Date: Thu Jul 24 21:16:59 2014 +0200

Initial commit

(zhangfa@kali)-[~/下载/ctf]
```

有文件上传，但是文件夹中没有，我们瞅瞅是否是在本地缓冲区，如图：

```
git stash show
```

```
(zhangfa@kali)-[~/下载/ctf]
└─$ git stash show
flag.txt | 25 ++++++-----
s.py     | 4 ++++
2 files changed, 28 insertions(+), 1 deletion(-)

(zhangfa@kali)-[~/下载/ctf]
└─$
```

好家伙，有个python文件，我们将其复原：

```
git stash apply
```

```
(zhangfa@kali)-[~/下载/ctf]
└─$ git stash apply
位于分支 master
要提交的变更：
  (使用 "git restore --staged <文件> ..." 以取消暂存)
    新文件：   s.py

尚未暂存以备提交的变更：
  (使用 "git add <文件> ..." 更新要提交的内容)
  (使用 "git restore <文件> ..." 丢弃工作区的改动)
    修改：    flag.txt

(zhangfa@kali)-[~/下载/ctf]
└─$
```

CSDN @I8947943

#### 4. 跑一下python代码

得到一个python文件，运行结果如图：

```
(zhangfa@kali)-[~/下载/ctf]
└─$ python2 s.py
NCN4dd992213ae6b76f27d7340f0dde122288df4d3

(zhangfa@kali)-[~/下载/ctf]
└─$
```

得到最终的答案：`NCN4dd992213ae6b76f27d7340f0dde122288df4d3`