XCTF MISCall

原创

YQK易乾坤 于 2020-10-27 22:17:08 发布 121 收藏

文章标签： git 安全

本文链接：https://blog.csdn.net/qq_30076719/article/details/109322000

XCTF MISCall做题记录

下载回来是一个txt文件，打开是乱码，放到WinHex，看出是BZ开头，猜测是压缩文件，放到kali里面用file命令查看

```
root@YQK:~# file d02f31b893164d56b7a8e5edb47d9be5.txt
d02f31b893164d56b7a8e5edb47d9be5.txt: bzip2 compressed data, block size = 900k
```

果不其然，是压缩文件，修改之后解压，得到一个flag.txt，打开发现并没有Flag。

同时还有一个.git文件夹（能看到的前提是打开了查看隐藏文件的功能），打开发现也没有找到想要的东西。

网上百度得到一条命令，git stash apply 恢复以前修改/删除的文件,执行一下

```
root@YQK:~/d02f31b893164d56b7a8e5edb47d9be5/ctf# git stash apply
位于分支 master
要提交的变更：
  (use "git restore --staged <file>..." to unstage)
        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）
  (use "git restore <file>..." to discard changes in working directory)
        修改：      flag.txt
```

发现多了一个文件（能执行成功是需要把原来的flag.txt删掉，不然执行不了）

然后运行一下这个s.py即是答案

```
root@YQK:~/d02f31b893164d56b7a8e5edb47d9be5/ctf# python s.py
NCN4dd992213ae6b76f27d7340f0dde1222888df4d3
```

附上答案：

NCN4dd992213ae6b76f27d7340f0dde1222888df4d3