MISCall的writeup

原创

MarcusRYZ 于 2020-02-14 21:53:26 发布 405 收藏

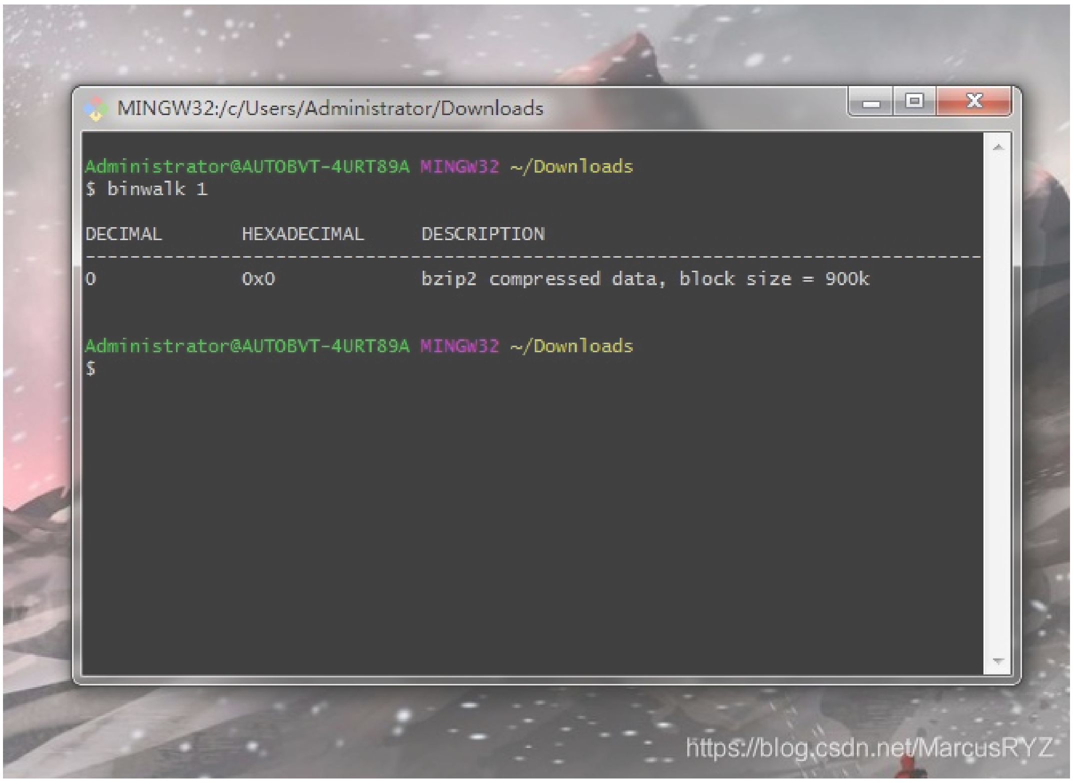
分类专栏： 攻防世界MISC高手进阶区 文章标签： 安全

本文链接：https://blog.csdn.net/MarcusRYZ/article/details/104315686

大家好，这次我为大家带来攻防世界misc部分MISCall的writeup。

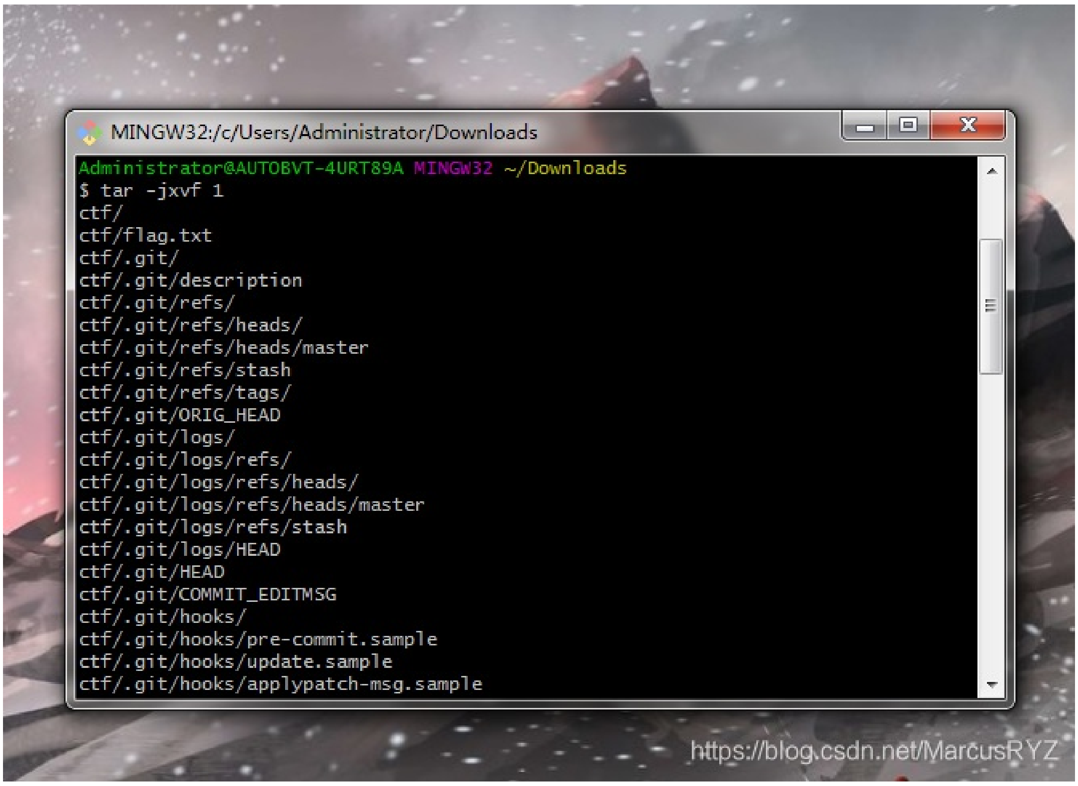
在开始解题前我先讲几句，这道题解题全靠一些Linux指令，所以，建议再看writeup前先了解一下。

好，言归正传，先下载附件，发现是一个未知文件，于是binwalk一下。



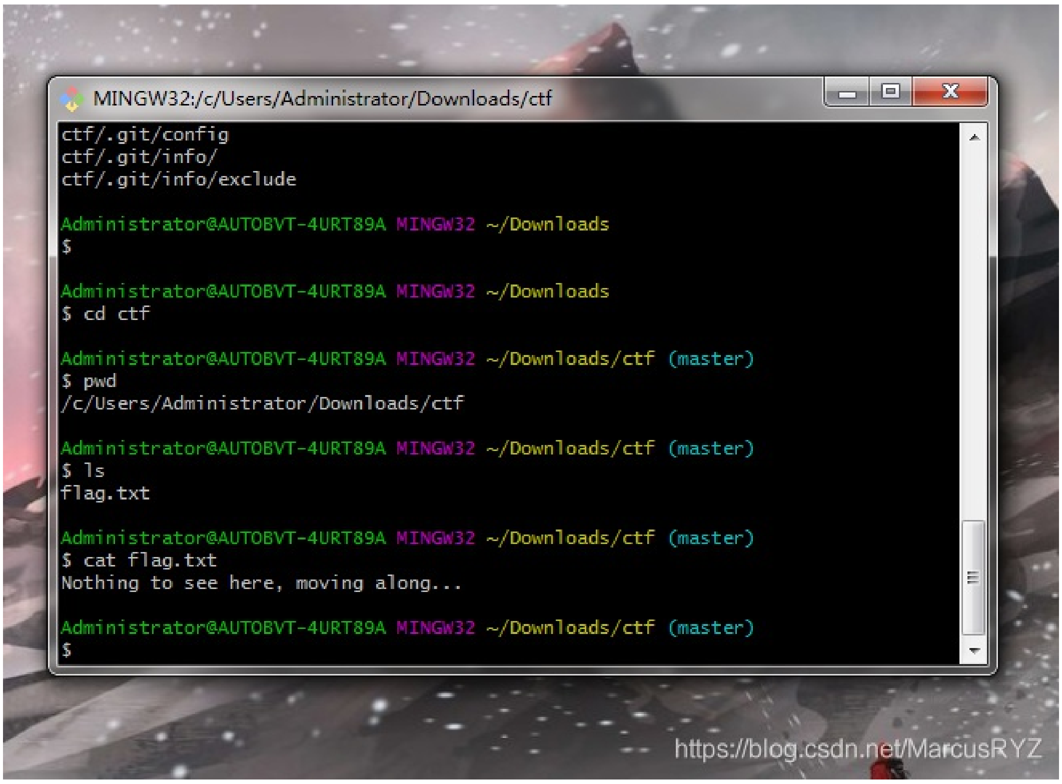
```
Administrator@AUTOBVT-4URT89A MINGW32 ~/Downloads
$ binwalk 1

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             bzip2 compressed data, block size = 900k


Administrator@AUTOBVT-4URT89A MINGW32 ~/Downloads
$
```

发现是一个bzip2格式的压缩包，于是用命令解压一下。



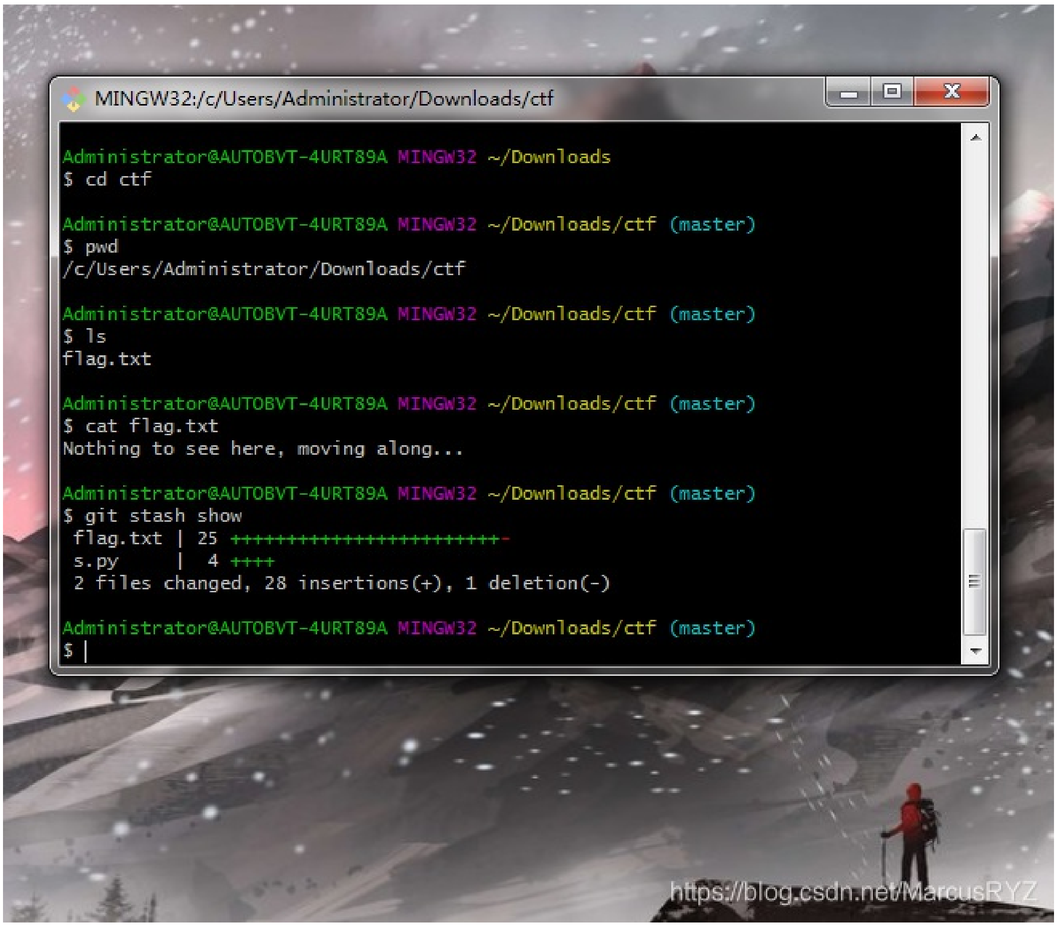
```
Administrator@AUTOBVT-4URT89A MINGW32 ~/Downloads
$ tar -jxvf 1
ctf/
ctf/flag.txt
ctf/.git/
ctf/.git/description
ctf/.git/refs/
ctf/.git/refs/heads/
ctf/.git/refs/heads/master
ctf/.git/refs/stash
ctf/.git/refs/tags/
ctf/.git/ORIG_HEAD
ctf/.git/logs/
ctf/.git/logs/refs/
ctf/.git/logs/refs/heads/
ctf/.git/logs/refs/heads/master
ctf/.git/logs/refs/stash
ctf/.git/logs/HEAD
ctf/.git/HEAD
ctf/.git/COMMIT_EDITMSG
ctf/.git/hooks/
ctf/.git/hooks/pre-commit.sample
ctf/.git/hooks/update.sample
ctf/.git/hooks/applypatch-msg.sample
```

发现有一个是一个ctf文件夹，进入后看到一个flag。打开看看，然而里面并没有flag。



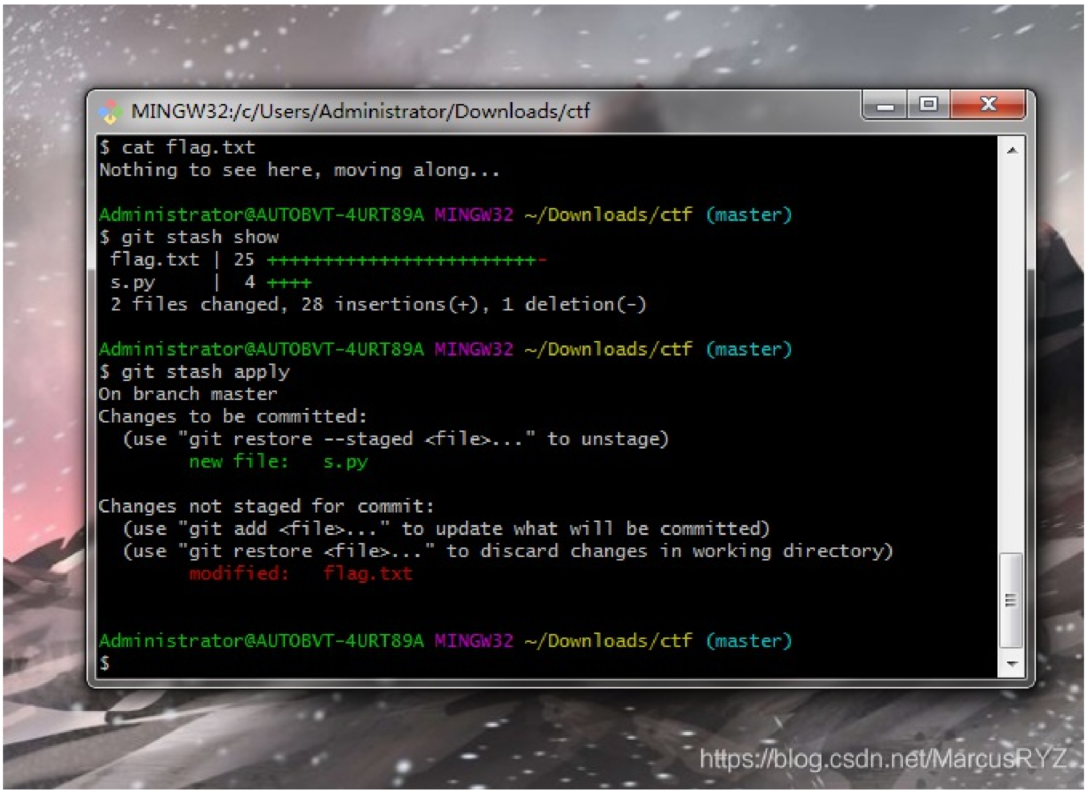
```
ctf/.git/config
ctf/.git/info/
ctf/.git/info/exclude

Administrator@AUTOBVT-4URT89A MINGW32 ~/Downloads
$

Administrator@AUTOBVT-4URT89A MINGW32 ~/Downloads
$ cd ctf

Administrator@AUTOBVT-4URT89A MINGW32 ~/Downloads/ctf (master)
$ pwd
/c/Users/Administrator/Downloads/ctf

Administrator@AUTOBVT-4URT89A MINGW32 ~/Downloads/ctf (master)
$ ls
flag.txt

Administrator@AUTOBVT-4URT89A MINGW32 ~/Downloads/ctf (master)
$ cat flag.txt
Nothing to see here, moving along...

Administrator@AUTOBVT-4URT89A MINGW32 ~/Downloads/ctf (master)
$
```

这时我们注意到还有一个.git文件夹，于是我们考虑到可能是Git泄露，于是我们用git stash show来查看一下文件被做了什么改动。



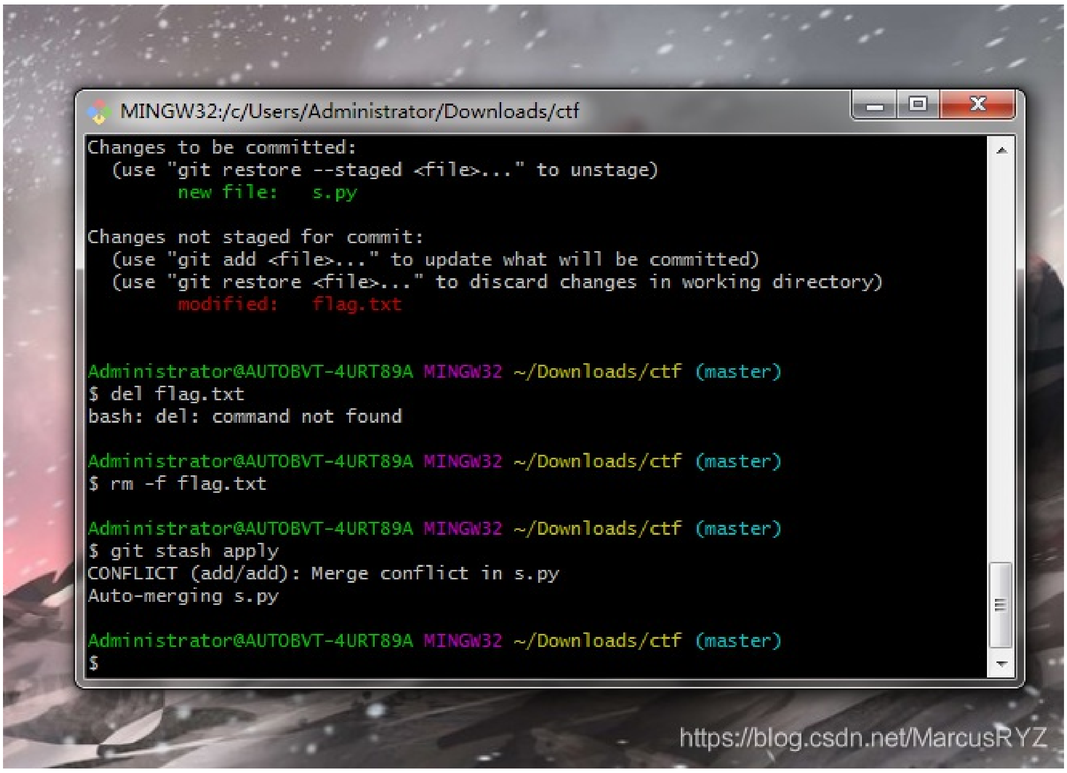
```
Administrator@AUTOBVT-4URT89A MINGW32 ~/Downloads
$ cd ctf

Administrator@AUTOBVT-4URT89A MINGW32 ~/Downloads/ctf (master)
$ pwd
/c/Users/Administrator/Downloads/ctf

Administrator@AUTOBVT-4URT89A MINGW32 ~/Downloads/ctf (master)
$ ls
flag.txt

Administrator@AUTOBVT-4URT89A MINGW32 ~/Downloads/ctf (master)
$ cat flag.txt
Nothing to see here, moving along...

Administrator@AUTOBVT-4URT89A MINGW32 ~/Downloads/ctf (master)
$ git stash show
 flag.txt | 25 ++++++++++++++++++++++++-
 s.py     |  4 ++++
 2 files changed, 28 insertions(+), 1 deletion(-)

Administrator@AUTOBVT-4URT89A MINGW32 ~/Downloads/ctf (master)
$ |
```

发现一个flag文本和一个python脚本，于是提取出来。



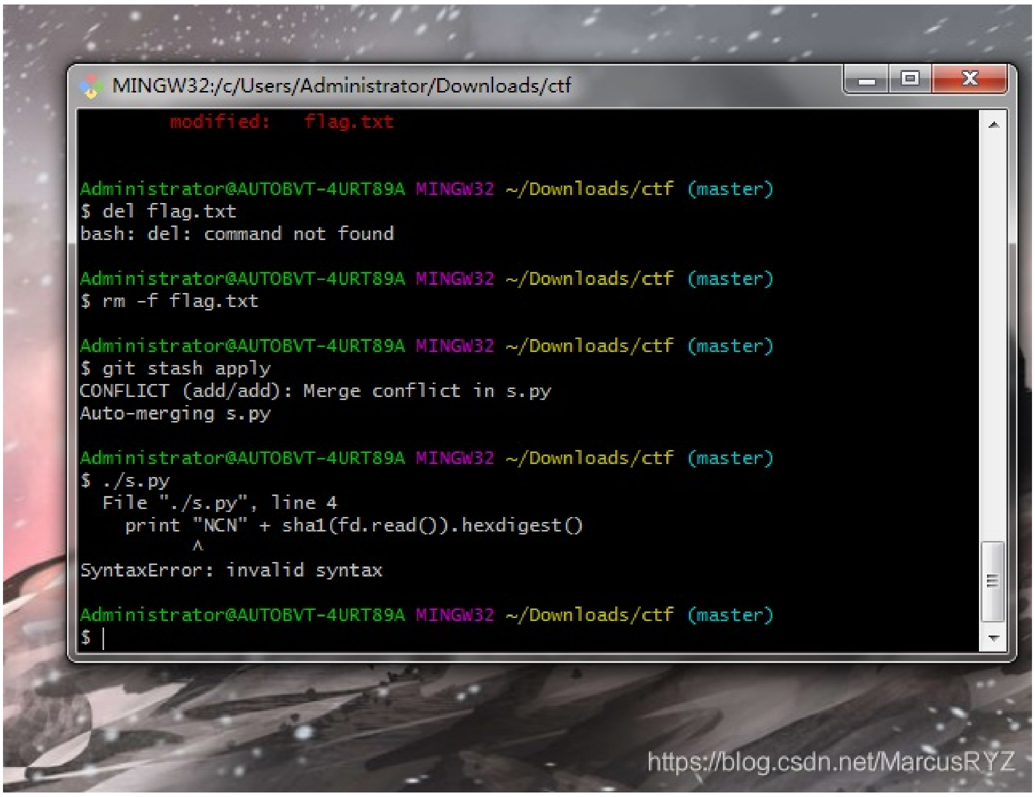
```
$ cat flag.txt
Nothing to see here, moving along...

Administrator@AUTOBVT-4URT89A MINGW32 ~/Downloads/ctf (master)
$ git stash show
 flag.txt | 25 ++++++++++++++++++++++++-
 s.py     |  4 ++++
 2 files changed, 28 insertions(+), 1 deletion(-)

Administrator@AUTOBVT-4URT89A MINGW32 ~/Downloads/ctf (master)
$ git stash apply
On branch master
Changes to be committed:
  (use "git restore --staged <file>..." to unstage)
        new file:   s.py

Changes not staged for commit:
  (use "git add <file>..." to update what will be committed)
  (use "git restore <file>..." to discard changes in working directory)
        modified:   flag.txt


Administrator@AUTOBVT-4URT89A MINGW32 ~/Downloads/ctf (master)
$
```

但是这里提醒我们，要先将已存在的flag文本删除后，才能提取文件。于是我们先将flag文本删了再提取。



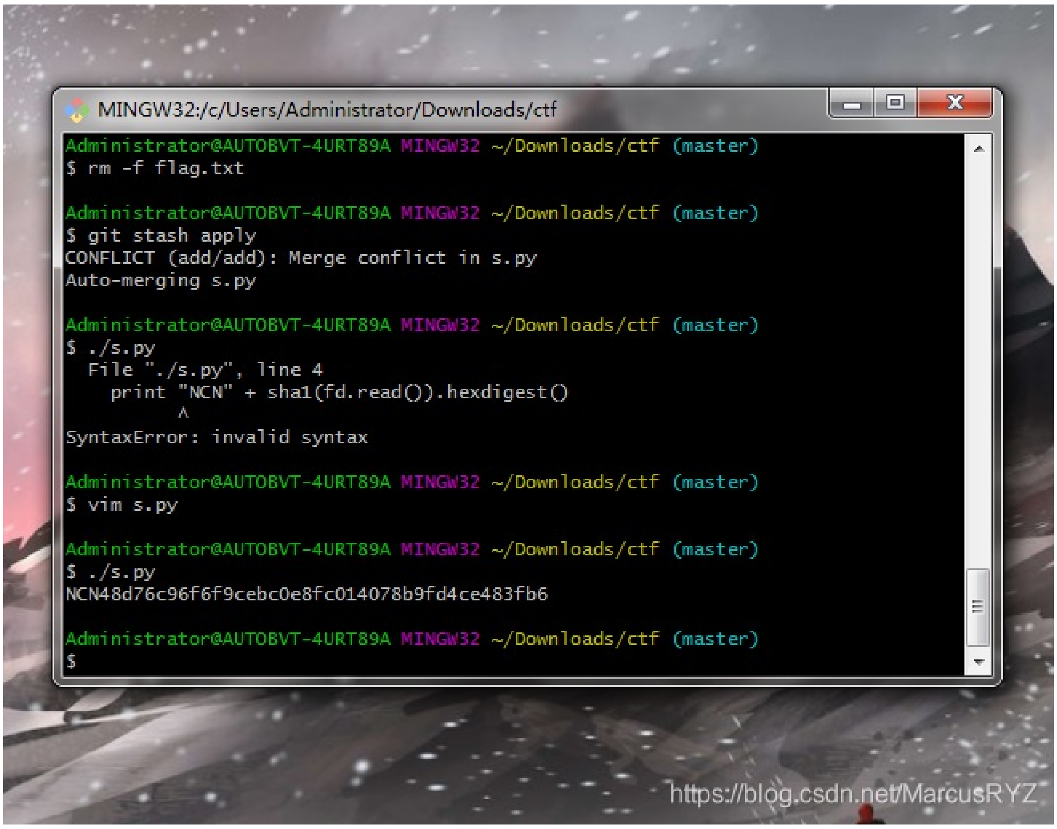
```
Changes to be committed:
  (use "git restore --staged <file>..." to unstage)
        new file:   s.py

Changes not staged for commit:
  (use "git add <file>..." to update what will be committed)
  (use "git restore <file>..." to discard changes in working directory)
        modified:   flag.txt


Administrator@AUTOBVT-4URT89A MINGW32 ~/Downloads/ctf (master)
$ del flag.txt
bash: del: command not found

Administrator@AUTOBVT-4URT89A MINGW32 ~/Downloads/ctf (master)
$ rm -f flag.txt

Administrator@AUTOBVT-4URT89A MINGW32 ~/Downloads/ctf (master)
$ git stash apply
CONFLICT (add/add): Merge conflict in s.py
Auto-merging s.py

Administrator@AUTOBVT-4URT89A MINGW32 ~/Downloads/ctf (master)
$
```

直接查看flag文本，发现一堆英文，肯定不是flag，这时我们想到还有一个python脚本，于是运行一下。



```
        modified:   flag.txt


Administrator@AUTOBVT-4URT89A MINGW32 ~/Downloads/ctf (master)
$ del flag.txt
bash: del: command not found

Administrator@AUTOBVT-4URT89A MINGW32 ~/Downloads/ctf (master)
$ rm -f flag.txt

Administrator@AUTOBVT-4URT89A MINGW32 ~/Downloads/ctf (master)
$ git stash apply
CONFLICT (add/add): Merge conflict in s.py
Auto-merging s.py

Administrator@AUTOBVT-4URT89A MINGW32 ~/Downloads/ctf (master)
$ ./s.py
  File "./s.py", line 4
    print "NCN" + sha1(fd.read()).hexdigest()
              ^
SyntaxError: invalid syntax

Administrator@AUTOBVT-4URT89A MINGW32 ~/Downloads/ctf (master)
$ |
```

有语法错误，print后缺少括号，于是输入vim（空格后跟文件名）进入文本编辑器，按住i进入编辑状态，编辑完后按Esc退出编辑状态，然后按住Shift加：进入可查询状态，输入wq!保存修改并退出，更正错误后再次运行脚本。



```
Administrator@AUTOBVT-4URT89A MINGW32 ~/Downloads/ctf (master)
$ rm -f flag.txt

Administrator@AUTOBVT-4URT89A MINGW32 ~/Downloads/ctf (master)
$ git stash apply
CONFLICT (add/add): Merge conflict in s.py
Auto-merging s.py

Administrator@AUTOBVT-4URT89A MINGW32 ~/Downloads/ctf (master)
$ ./s.py
  File "./s.py", line 4
    print "NCN" + sha1(fd.read()).hexdigest()
              ^
SyntaxError: invalid syntax

Administrator@AUTOBVT-4URT89A MINGW32 ~/Downloads/ctf (master)
$ vim s.py

Administrator@AUTOBVT-4URT89A MINGW32 ~/Downloads/ctf (master)
$ ./s.py
NCN48d76c96f6f9cebc0e8fc014078b9fd4ce483fb6

Administrator@AUTOBVT-4URT89A MINGW32 ~/Downloads/ctf (master)
$
```

得到flag：NCN48d76c96f6f9cebc0e8fc014078b9fd4ce483fb6。