# 攻防世界MISCall

原创

一个小南瓜 于 2020-04-02 18:04:09 发布 709 收藏

分类专栏： CTF 文章标签： python git



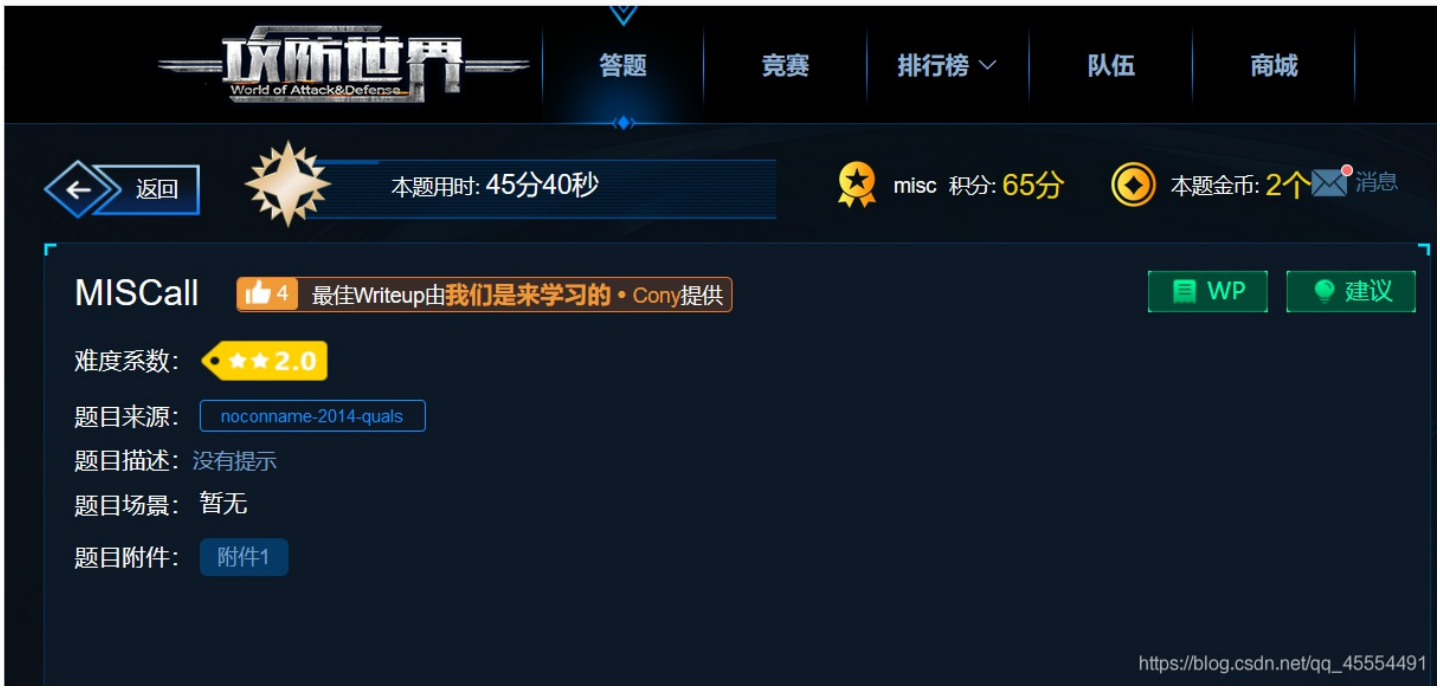
本文链接：https://blog.csdn.net/qq_45554491/article/details/105275670





## 攻防世界MISCall

### 1、题目




网址：攻防世界

### 2、原理及工具

原理：git信息泄露

git官网资料：https://www.git-scm.com/book/zh/v2

工具：kali、python

### 3、解题过程

下载下来的文件名字太长，先改个名字

```
root@kali:~/Desktop/CTF# mv d02f31b893164d56b7a8e5edb47d9be5 miscall
root@kali:~/Desktop/CTF# ls
miscall
```

先来查看文件类型

```
root@kali:~/Desktop/CTF# file miscall
miscall: bzip2 compressed data, block size = 900k
```

发现是个bzip2的压缩包，解压

```
root@kali:~/Desktop/CTF# bzip2 -d miscall
bzip2: Can't guess original name for miscall -- using miscall.out
#无法猜出miscall的原始名称--使用miscall.out
root@kali:~/Desktop/CTF# ls
miscall.out
```

虽然报了错误，但是可以发现文件名发生了改变

```
root@kali:~/Desktop/CTF# bzip2 -d miscall
bzip2: Can't guess original name for miscall -- using miscall.out
root@kali:~/Desktop/CTF# ls
miscall.out
```

二话不说再看看文件类型

```
root@kali:~/Desktop/CTF# file miscall.out
miscall.out: POSIX tar archive (GNU)  #tar文件
```

继续解压

```
root@kali:~/Desktop/CTF# tar -xvf miscall.out
root@kali:~/Desktop/CTF# ls
ctf  miscall.out
```

发现出现了一个新的目录ctf，进去看看，终于看到flag了，可是是个假的

```
root@kali:~/Desktop/CTF# cd ctf/
root@kali:~/Desktop/CTF/ctf# ls
flag.txt
root@kali:~/Desktop/CTF/ctf# cat flag.txt
Nothing to see here, moving along...
```

什么都没有，怎么办？再仔细看看,发现了隐藏文件.git,是个啥，百度一波，找到了可用的命令，试试看

```
root@kali:~/Desktop/CTF/ctf# ls -a
.  ..  flag.txt  .git
```

使用命令查看git记录

```
root@kali:~/Desktop/CTF/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
```

使用git stash show校验列表中存储的文件

```
root@kali:~/Desktop/CTF/ctf# git stash show
 flag.txt | 25 ++++++++++++++++++++++++-
 s.py     |  4 ++++
 2 files changed, 28 insertions(+), 1 deletion(-)
```

使用git stash apply 重新进行存储，复原文件,可以发现出现一个s.py文件

```
root@kali:~/Desktop/CTF/ctf# 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

root@kali:~/Desktop/CTF/ctf# ls
flag.txt  s.py
```

运行s.py文件，得到flag

```
root@kali:~/Desktop/CTF/ctf# python s.py
NCN4dd992213ae6b76f27d7340f0dde1222888df4d3
```