




misc高阶 攻防世界_攻防世界MISC高手进阶区MISCall

原创

石头跑跑  于 2021-01-27 08:51:03 发布  94  收藏

文章标签: [misc高阶 攻防世界](#)

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/weixin_29256771/article/details/113416404

版权

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。

```
binwalk -e 附件
```

发现是一个bzip2格式的压缩包, 于是用命令解压一下。

```
tar -xjf 附件
```

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。

```
cat 附件/ctf/flag
```

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。

```
git stash show
```

发现一个flag文本和一个python脚本, 于是提取出来。

```
tar -xjf 附件
```

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。

```
rm 附件/ctf/flag
```

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。

```
python 附件/ctf/flag.py
```

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。

```
python 附件/ctf/flag.py
```

得到flag: NCN48d76c96f6f9cebc0e8fc014078b9fd4ce483fb6。

点赞

1

收藏

分享

文章举报

MarcusRYZ

发布了23 篇原创文章 · 获赞 22 · 访问量 6801

私信

关注