TCTF writeup

原创

逃课的小学生 于 2021-08-08 23:00:39 发布 99 收藏 1
分类专栏： ctf crypto

本文链接：https://blog.csdn.net/zhang14916/article/details/118634267


ctf 同时被 2 个专栏收录
30 篇文章 2 订阅
订阅专栏


crypto
20 篇文章 1 订阅
订阅专栏

crypto

checkin

题目如下图所示

```
D:\netcat-1.11>nc 111.186.59.11 16256
Show me your computation:
2^(2^11545483) mod 167858951004072480680556314745152428896746921737890036409502726529742366812455318202878722548913569870720670963113868371617521174796163251325863100478500435514262041974513552794941918624075386518370085024735380404623226418045187952620593888543380073746021037431640956910636458398803274159025300115393615925 81 = ?
You have 10 seconds. gogogo!
Your answer: Timeout!
```

我们发现题目是要求算一个比较复杂的算数，且要求十秒内出结果。这里需要调数学库gmpy2计算，使用python来算会超时。解题过程如下

```
from pwn import *
import hashlib
import math
import gmpy2
io=remote("111.186.59.11",16256)
io.recvuntil("(2^")
tian=int(io.recvuntil(")")[:-1],10)
io.recvuntil("mod ")
#ress=io.recvuntil(" = ?")[:-4]
#print(ress)
res=int(io.recvuntil(" = ?")[:-4],10)
res1=gmpy2.powmod(2,pow(2,tian),res)
io.recvuntil("answer:")
io.sendline(str(res1)+'\n')
io.interactive()
print(res1)
```

2.guthib

从题目中可以看出flag已经被bfg工具替换了，在当前页面中无法找到flag，但是所有github的pushevent和commentevent都会被记录在/repos/{owner}/{repo}/events下，所以我们可以从https://api.github.com/repos/awesome-ctf/TCTF2021-Guthib/events中寻找。但我们会发现有许多事件，从https://api.github.com/repos/awesome-ctf/TCTF2021-Guthib/events?page=1到https://api.github.com/repos/awesome-ctf/TCTF2021-Guthib/events?page=8都是一些操作。由于我们知道try.2.md最开始也是push进去的，所以我们寻找关键词"type": "PushEvent",然后我们可以找到四条记录，一一搜索，在一条记录Try 2: Taking memos · awesome-ctf/TCTF2021-Guthib@da88350中可以找到flag


```
  }
},
{
  "id": "17021153902",
  "type": "PushEvent",
  "actor": {
    "id": 7986667,
    "login": "HenryzhaoH",
    "display_login": "HenryzhaoH",
    "gravatar_id": "",
    "url": "https://api.github.com/users/HenryzhaoH",
    "avatar_url": "https://avatars.githubusercontent.com/u/7986667?"
  },
  "repo": {
    "id": 382436656,
    "name": "awesome-ctf/TCTF2021-Guthib",
    "url": "https://api.github.com/repos/awesome-ctf/TCTF2021-Guthib"
  },
  "payload": {
    "push_id": 7448403574,
    "size": 5,
    "distinct_size": 5,
    "ref": "refs/heads/master",
    "head": "6ae87cd1d9b35cfdca4f56f8d8ac78508a404a8b",
    "before": "932795a9ea18ee35ae0f5339973ef0d2d9dd9bca",
    "commits": [
      {
        "sha": "da883505ed6754f328296cac1ddb203593473967",
        "author": {
          "email": "nobody@no.one",
          "name": "Nobody"
        },
        "message": "Try 2: Taking memos",
        "distinct": true,
        "url": "https://api.github.com/repos/awesome-ctf/TCTF2021-Guthib/commits/da883505ed6754f328296cac1ddb203593473967"
      },
      {
        "sha": "a17ed270522072895e5e2b11b6fdd0e9a210fdfb",
        "author": {
          "email": "nobody@no.one",
          "name": "Nobody"
        },
        "message": "Try 1: Taking memos",
        "distinct": true,
        "url": "https://api.github.com/repos/awesome-ctf/TCTF2021-Guthib/commits/a17ed270522072895e5e2b11b6fdd0e9a210fdfb"
      }
    ]
  }
},
```



```
@@ -6,6 +6,7 @@
- ### Watch Later
+ ### Accounts
- - Attack on Titan
- - DARLING in the FRANXX
- - Wonder Egg Priority
- - The Day I Became a God
- - Kemono Friends
- - Charlotte
+ ID: nobody@no.one
+ Password: flag{ZJaNicLjnDytwqosX8ebwiMdLGcMBL}
```