

摘要

第一次参加CTF，小白视角参赛体验，从零开始学CTF

WEB

第一题Hitchhiking_in_the_Galaxy

题解

第二题 Watermelon

第三题 宝藏走私者

第四题 智商检测鸡

第五题 走私者的愤怒

MISC

第一题 Base全家福

WEB

第一题Hitchhiking_in_the_Galaxy

Level - Week1

Hitchhiking_in_the_Galaxy[已完成]

描述

第一次在银河系里搭顺风车，要准备啥，在线等，挺急的

题目地址 <http://hitchhiker42.0727.site:42420>

基准分数 100

当前分数 100

完成人数 412

这一题其实我看了蛮久的，好几题那没看出啥来，不过后来想到这题只有100分，那应该不是很难。果然是自己想太多！

题解

打开网页 <http://hitchhiker42.0727.site:42420/>，看到如下页面

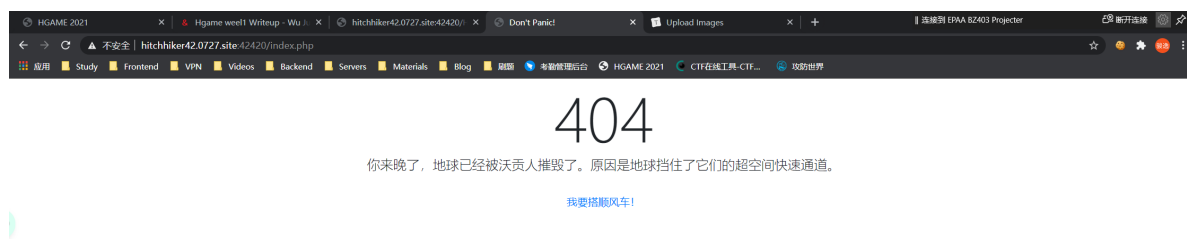


直接一个404，没啥信息，于是 F12 打开控制台看看有没有什么线索。header 里没看见什么奇怪的信息，只有页面源代码给出了一个 link 连接 `HitchhikerGuide.php`

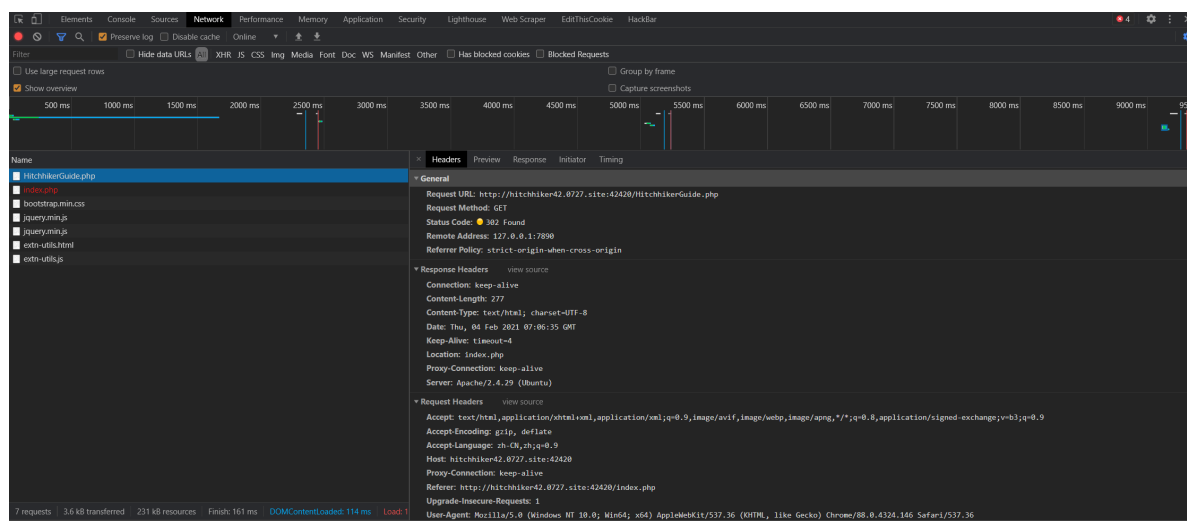
```
Q 搜索 HTML
<html>
  <head>
  </head>
  <body>
    <div class="page-wrap d-flex flex-row align-items-center">
      <div class="container">
        <div class="row justify-content-center">
          <div class="col-md-12 text-center">
            <span class="display-1 d-block">404</span>
            <div class="mb-4 lead">你太晚了，地球已经被沃贡人摧毁了。原因是地球挡住了它们的超空间快速通道。</div>
            <a class="btn btn-link" href="HitchhikerGuide.php">我要搭顺风车！</a>
          </div>
        </div>
      </div>
    </body>
  </html>
```

那就去看看那里有啥。

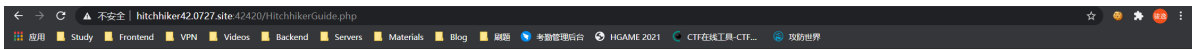
直接访问 <http://hitchhiker42.0727.site:42420/HitchhikerGuide.php>



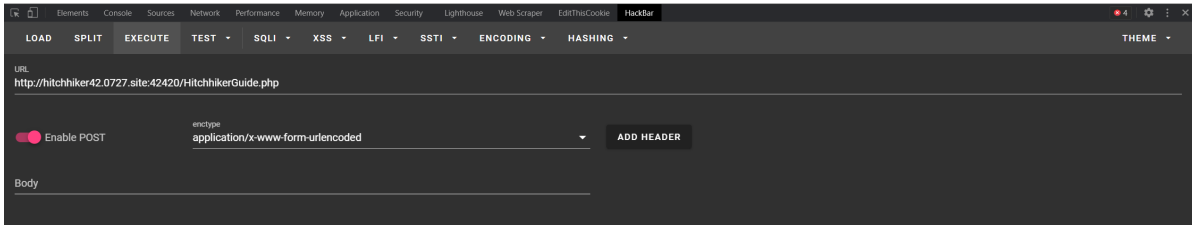
好家伙又来到404页面，但是注意到这次来到的是 `index.php`。打开控制台，发现是302转向到了 `index.php` 页面。



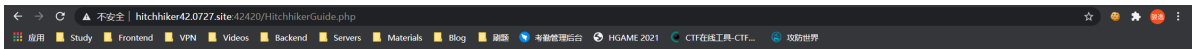
大胆猜测 maybe 访问方式不对，那把 GET 方式换成 POST方式试试。打开 Hackbar 插件，启用 POST 请求，发送！有信息了！



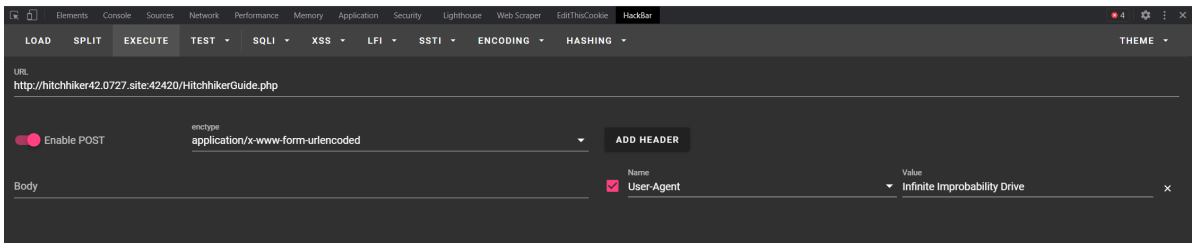
只有使用“无限非概率引擎”(Infinite Improbability Drive)才能访问这里~



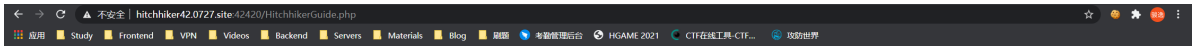
使用 Infinite Improbability Drive 方式? 可能再说 User-Agent? 那 header 里加上 User-Agent 看看。



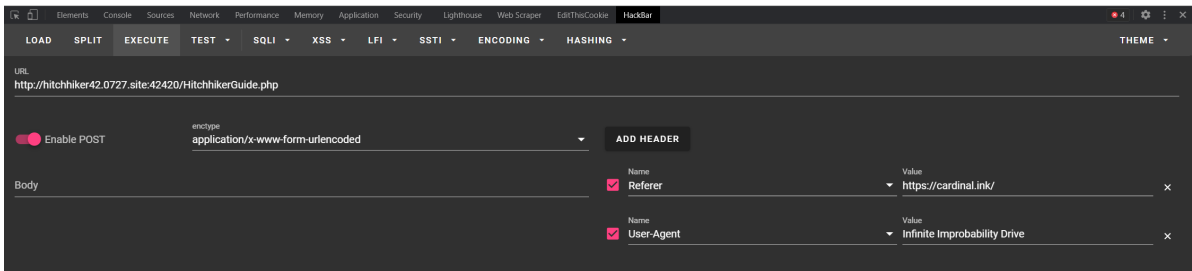
你知道吗? 茄子特别要求: 你得从他的Cardinal过来



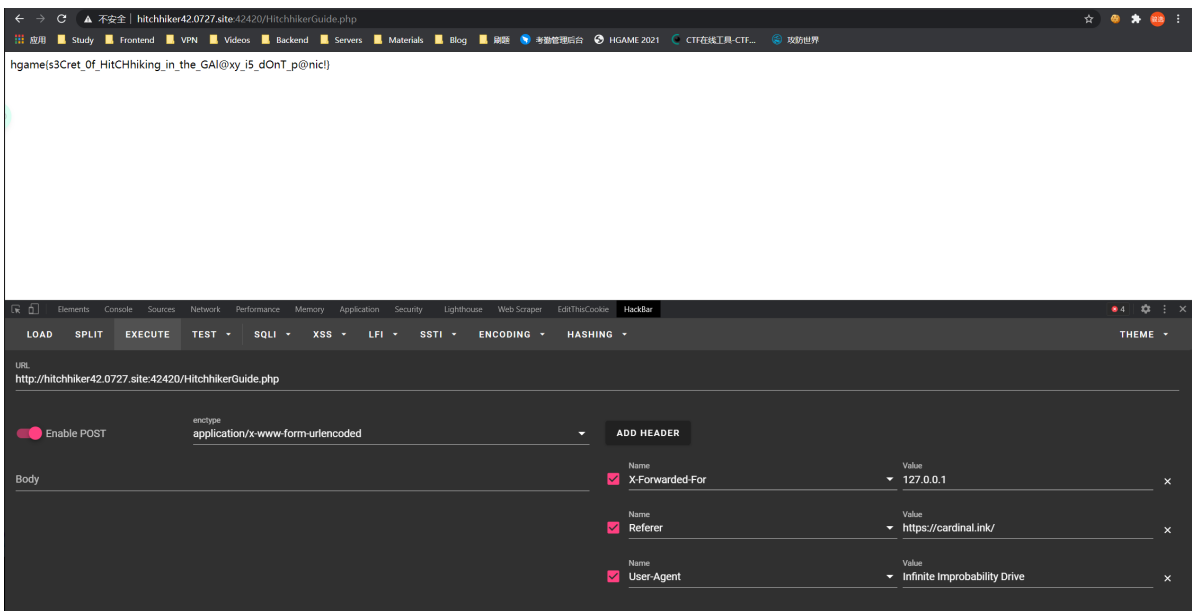
好家伙, 成功了。不过又说要从 [Cardinal](#) 过来, 那么很 easy, header 里再加上 Referer 参数。



flag仅能通过本地访问获得



没毛病, 成功了。又说要本地访问, 那就在 header 里加个 x-Forwarded-For 参数, 值为 127.0.0.1。



GET! `hgame{s3Cret_0f_HitChHiking_in_the_GAl@xy_i5_dOnT_p@nic!}`

第二题 Watermelon

简单上头的小游戏——真的上头，完了好久好久！

watermelon[已完成]

描述

简单且上头的游戏

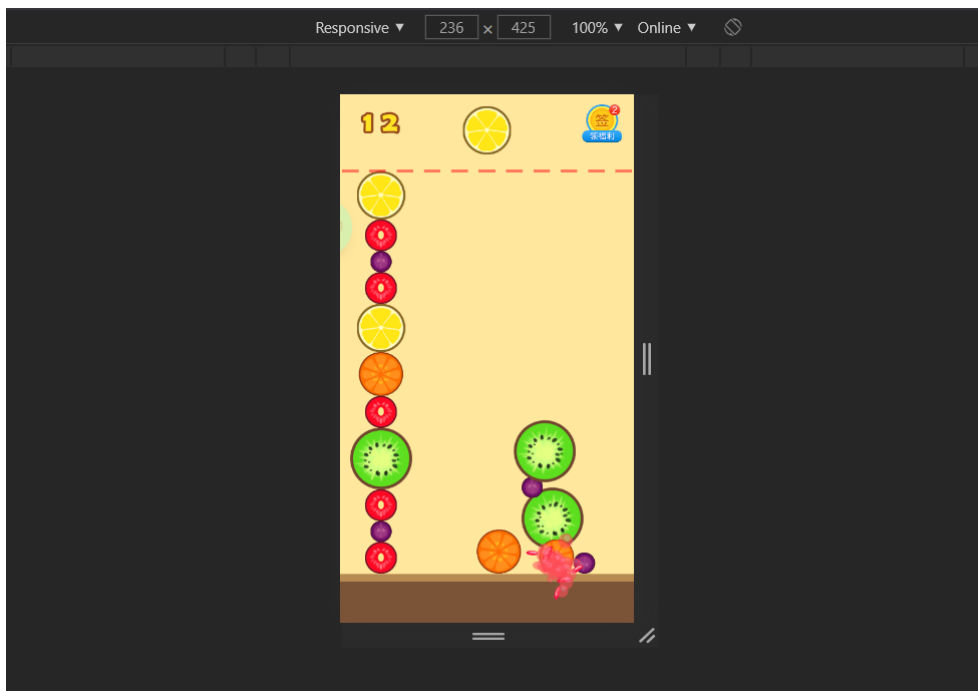
题目地址 <http://watermelon.yeyz800/>

基准分数 100

当前分数 100

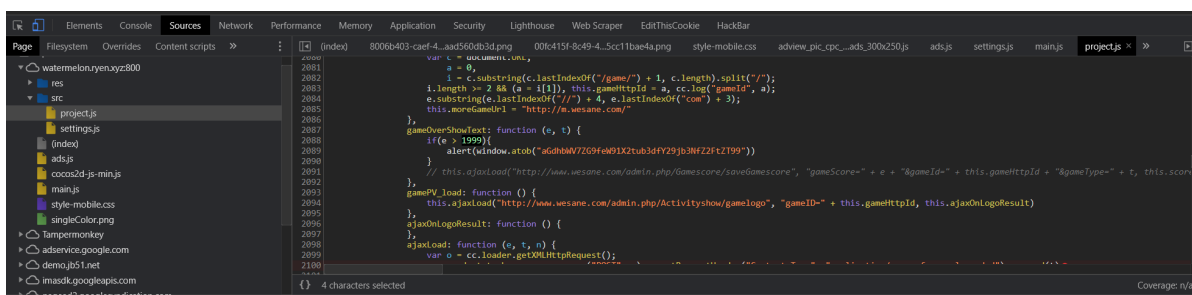
完成人数 403

不难发现，得到了 2000 分才能拿到 flag。



也许能通过操作 js 来获得 flag。

通过审计页面源代码，很快定位到了一个叫 `project.js` 的文件，里面的变量 `e` 应该就是分数。



发现里面有这样一段代码：

```
gameOverShowText: function (e, t) {  
    if(e > 1999){  
        alert(window.atob("aGdhbwV7ZG9few91X2tub3dfY29jb3NfZ2FtZT99"))  
    }  
},
```

`atob()` 方法用于解码使用 base-64 编码的字符串，那么

`aGdhbwV7ZG9few91X2tub3dfY29jb3NfZ2FtZT99` 应该就是 base-64 编码的字符串。解码一下

— **base编码**

base16、base32、base64

aGdhbwV7ZG9few91X2tub3dfY29jb3NfZ2FtZT99

编码

base64

字符集

utf8(unicode编码)

编 码

解 码

hgame{do_you_know_cocos_game?}

GET! `hgame{do_you_know_cocos_game?}`

第三题 宝藏走私者

宝藏走私者(已完成)

描述

hint: 注意留意服务器信息

资料: <https://paper.seebug.org/1048/>

宝藏走私者 Switch 喜欢偷盗并将奇特的宝藏走私到一些黑市商家手中。

为了阻止其继续作恶，警探 Liki 奉命将 Switch 抓捕归案。

调查过程中，Liki 发现 Switch 将一个秘密藏在了一个私人服务器中。

这或许会成为后续追查 Switch 的重大线索。你能找到这个秘密吗？

题目地址 <http://thief.0727.site:80>

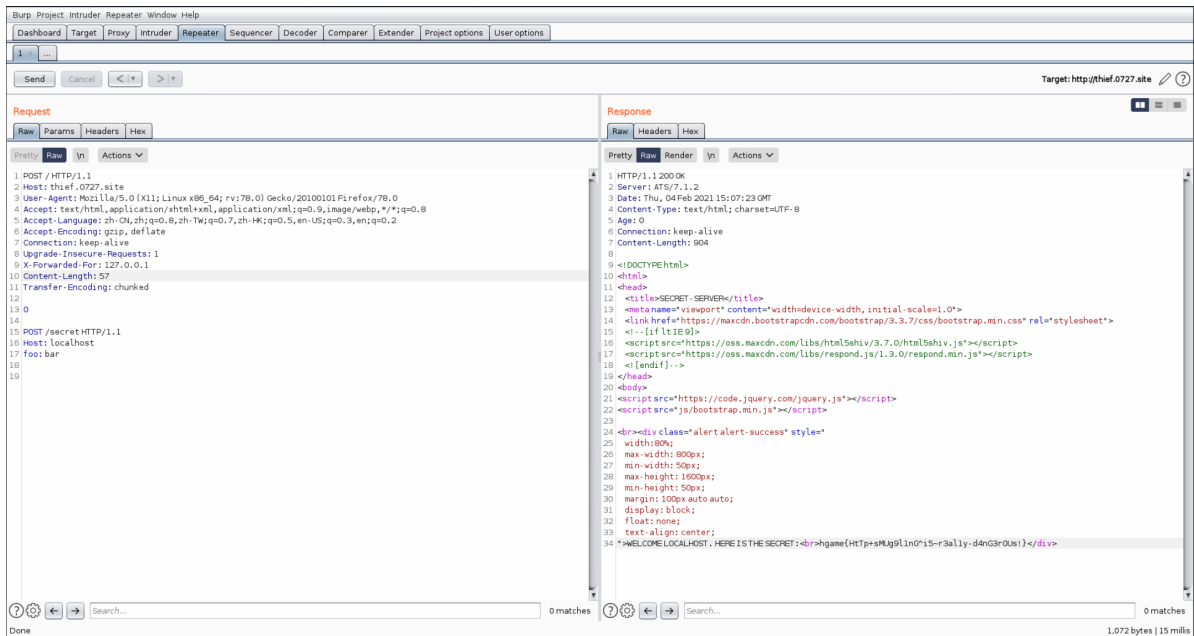
基准分数 50

当前分数 50

完成人数 230

这应该是一道关于HTTP走私的题目，目前知识学明白了，但操作上不知道哪出了问题一直没成功。

BUT！我好像多次搭上了顺风车



flag如上图，具体搞明白了再补充吧。

第四题 智商检测鸡

智商检测鸡(已完成)

描述

又有谁不爱奥数呢？反正我不爱（请使用firefox浏览器打开题目）

题目地址

<http://4u.top:5000/>

基准分数

150

当前分数

150

完成人数

309

100道定积分计算，做完给flag。服务器通过临时session来识别用户，因此手算必然不可能。那么试试自动计算？

瞬间想到Python，打算试试 selenium 自动化。但是对于分析了页面源码后，我发现以我现有水平读取积分上下限的值和程式有难度（负号在单独的标签里）。所以打算先收算几道看看有没有啥规律。

然后在微软数学手机软件的帮助下，做了十几道题，发现规律——**积分下限都是负整数，上限都是正整数，积分式子都是 $AX+B$ 的形式，其中 A 和 B 都为正整数**

那就很 ez 了，编写Python代码：

```
from time import sleep
from selenium import webdriver
from sympy import *
积分计算

wd = webdriver.Chrome(r'chromedriver.exe')
//定位chrome浏览器自动化的驱动程序（因为我使用chrome）
wd.get('http://r4u.top:5000/')
//打开网页窗口，自动访问该网页
sleep(1)
//我怕网页没加载好就开始寻找元素，那必报错，所以让程序sleep一会

for i in range(100):
    try:
        inPutBox = wd.find_element_by_id('answer') //定位答案输入框
        clickBtn = wd.find_element_by_css_selector('.btn.btn-primary') //定位验证答案框
        //100道题，循环100次
        //导入sleep包来使用sleep函数
        //导入webdriver自动化组件
        //sympy里的integrate函数用于定
        //定位答案输入框
        //定位验证
```

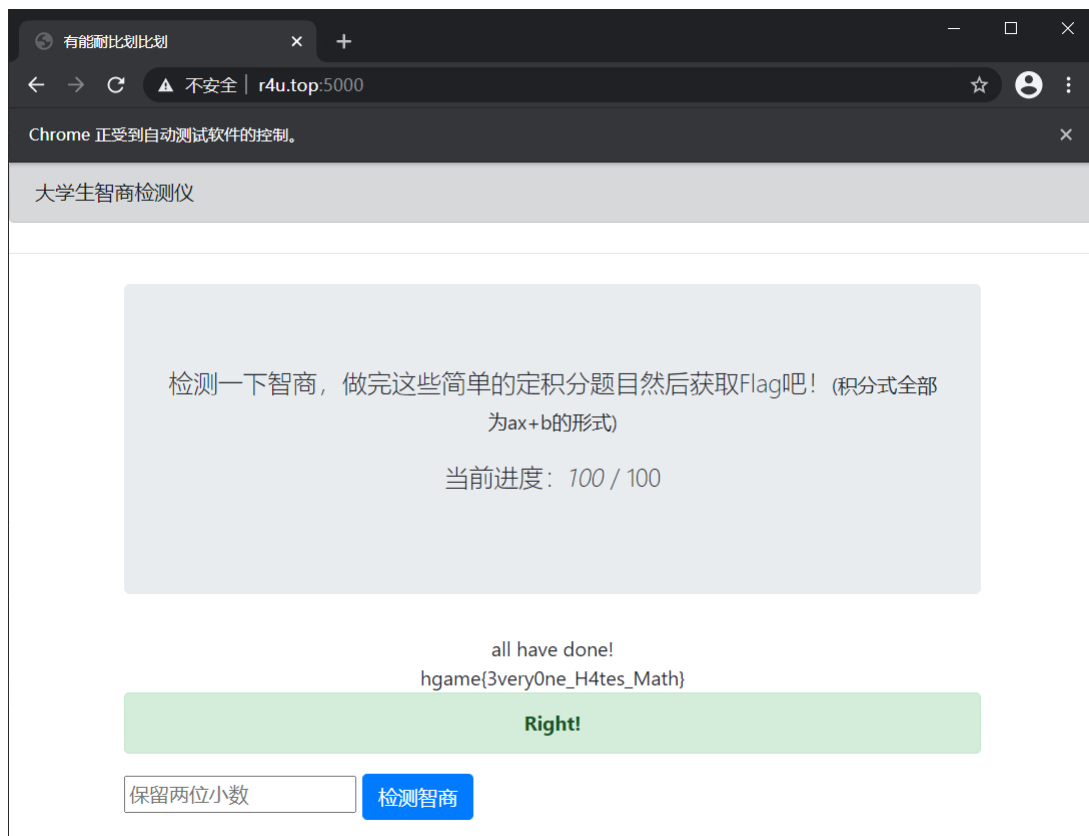
```

a = "-" + wd.find_element_by_css_selector('#integral > math > mrow >
msubsup > mrow:nth-child(2) > mn').text //积分下限
b = wd.find_element_by_css_selector('#integral > math > mrow > msubsup >
mrow:nth-child(3) > mn').text //积分上限
c = wd.find_element_by_css_selector('#integral > math > mrow > mn:nth-
child(3)').text //积分式 Ax+B 中的 A
d = wd.find_element_by_css_selector('#integral > math > mrow > mn:nth-
child(6)').text //积分式 Ax+B 中的 B
a = int(a) //字符串转数字
b = int(b) //字符串转数字
c = int(c) //字符串转数字
d = int(d) //字符串转数字
x = symbols('x') //x为积分变量
result = str(integrate(c * x + d, (x, a, b))) //计算答案，同时转换为字符串
格式

if '/' in result: //这里很重要，定积分计算结果不是用
小数表示的，比如 1.5 是用 3/2 表示的，所以要处理一下
    eq = result.split('/')
    result = float(eq[0]) / float(eq[1])
    result = str(result) //用split函数把分子分母取出来，转
换成浮点数除一下，就得到小数了，最后转换成字符串
    inPutBox.send_keys(result) //向输入框中输入答案
    clickBtn.click() //自动点击验证答案切换到下一题
    //没学过python的，本来想试一下
finally:
try, 然后就出现了没啥用的try-finally结构
    sleep(1) //等下一题加载出来
    inPutBox.clear() //清空输入框

```

Ctrl + Shift + F10，稍等片刻：



得到Flag `hgame{3very0ne_H4tes_Math}`

第五题 走私者的愤怒

我还没整明白

MISC

第一题 Base全家福

Base全家福(已完成)

描述

新年即将来临之际，Base家族也团聚了，他们用他们特有的打招呼方式向你问了个好，你知道他们在说什么吗？

R1k0RE1OWldHRTNFSU5SVkc1QkRLTpXR1VaVENOUIRHTVIETVJCv0dVMIVNTlpVR01ZREISUIVlQJTET01aVudsQQRHTVpWSVlaVEVNWlFHTVpER01KWEIRPT09PT09

本次比赛为招新赛，请各位选手不要在当周比赛进行期间至结束后24小时内发布当周比赛题目的writeup

题目地址 <https://www.baidu.com>

基准分数 50

当前分数 50

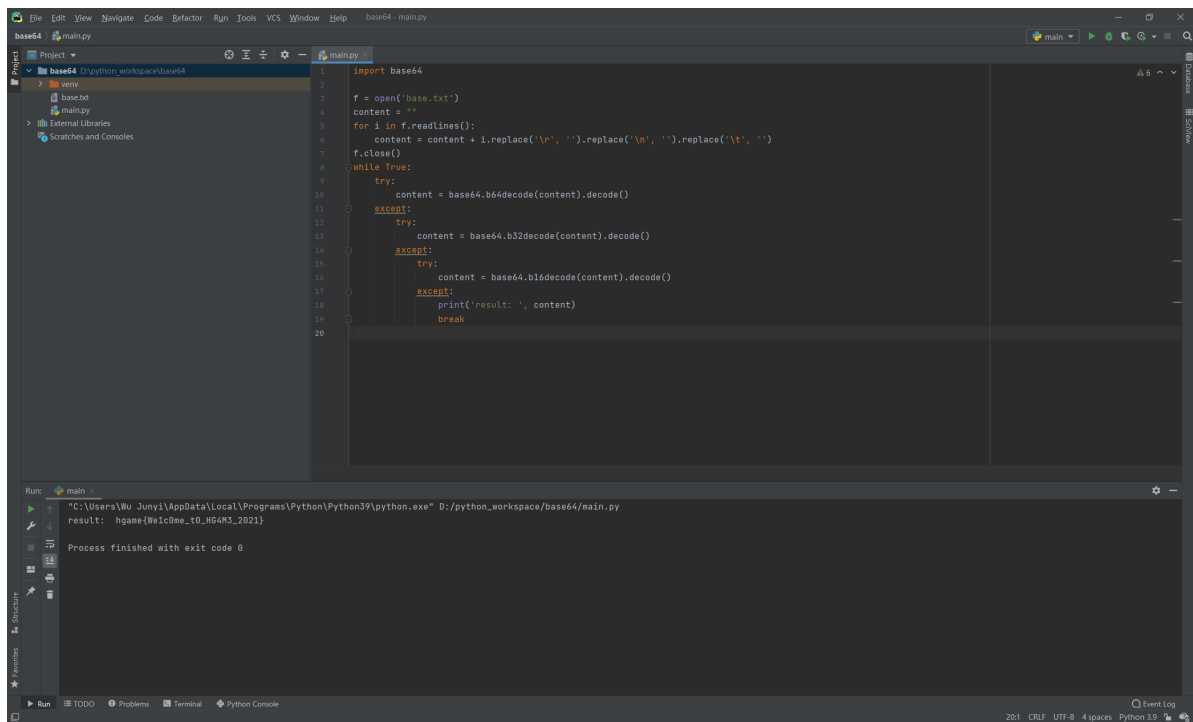
完成人数 664

这题蛮easy的，都说了 Base全家福 那应该就是 Base混合编码的解码，直接用 python 解决

```
import base64

f = open('base.txt')
content = ""
for i in f.readlines():
    content = content + i.replace('\r', '').replace('\n', '').replace('\t', '')
f.close()
while True:
    try:
        content = base64.b64decode(content).decode()
    except:
        try:
            content = base64.b32decode(content).decode()
        except:
            try:
                content = base64.b16decode(content).decode()
            except:
                print('result: ', content)
                break
```

运行！



```
1 import base64
2
3 f = open('base.txt')
4 content = ''
5 for i in f.readlines():
6     content = content + i.replace('\n', '').replace('\r', '').replace('\t', '')
7 f.close()
8 while True:
9     try:
10         content = base64.b64decode(content).decode()
11     except:
12         try:
13             content = base64.b32decode(content).decode()
14         except:
15             try:
16                 content = base64.b16decode(content).decode()
17             except:
18                 print('result: ', content)
19                 break
20
```

Run: main

"C:\Users\Wu Junyi\AppData\Local\Programs\Python\Python39\python.exe" D:/python_workspace/base64/main.py
result: hgame{we1c0me_t0_HG4M3_2021}

Process finished with exit code 0

得到Flag `result: hgame{we1c0me_t0_HG4M3_2021}` 啊哈原来是签到题

参考文章:

[X-Forwarded-For 伪造Localhost](#)