

我的第一个wp

零基础菜鸡的痛苦答题

第一题 misc签到题

用16, 32, 64都来一遍直接拿到flag

第二题 web1

1. 先正常发个包看看
2. 405错误--改成post试试
3. 只有“Infinite Improbability Drive”能到达---更改User-Agent
4. 从奇怪的地方过来-----Referer: <https://cardinal.ink/> (ps.ink我多打了个l, 错了好久都没发现)
5. 本地访问----X-Forwarded-For:127.0.0.1
6. 取得flag

第三题 大西瓜

1. 经典f12
2. 搜索score----找到“(a.default.score += this.fruitNumber + 1)”
3. 在这行设置断点
4. 控制台输入“a.default.score += this.fruitNumber + 10000”
5. 拿到flag
6. ps: 第一次直接玩到2000分, 拉着边框一直来回, 直接卡掉水果

第四题 智商检测机

1.先用的request, 但math部分加载不出来, 只能用selenium了
爬虫脚本

```
```python
import requests
import sympy
import lxml
import re
from lxml import etree
from bs4 import BeautifulSoup
from selenium import webdriver
import time
m=0
```

```
driver = webdriver.Chrome()
mycookie = {'name':
'session', 'value': 'eyJzbnIjowfQ.YB1nIQ.oxstyrJHABebWC2JGmF100PWH8I'}
driver.get('http://r4u.top:5000/')
while (m<200):
 content = driver.page_source.encode('utf-8')
 s=requests.session()
 soup=BeautifulSoup(content,"html.parser")
 a=(soup.find_all("mn"))
 y=-float(a[0].next)
 x=float(a[1].next)
 p=float(a[2].next)
 q=float(a[3].next)
 t=(p/2)*x*x+q*x-p/2*y*y-q*y
 t=round(t,2)
 driver.find_element_by_xpath("/html/body/div[2]/input").click()
 driver.find_element_by_xpath("/html/body/div[2]/input").clear()
 driver.find_element_by_xpath("/html/body/div[2]/input").send_keys(str(t))
 driver.find_element_by_xpath("/html/body/div[2]/button").click()
 m=m+1

time.sleep(100)
...
```