Bugku web18 Writeup

原创

5mack 于 2021-04-25 19:13:52 发布 93 收藏

分类专栏： CTF

本文链接：https://blog.csdn.net/Code_Aape/article/details/116136154

Bugku web18 Writeup

题目描述

> 秋名山车神
>
> 亲请在2s内计算老司机的车速是多少
>
> 14180054436*29560789-15192333921*175548399-2093405283-12328199721*369963596+21310695541*983217943*1732954684+1645835278=?;

分析

秋名山车神，2s内

所以就是个**快**字，那我慢慢计算不行嘛？

尝试刷新网页，果然表达式在变...多刷几次，发现偶尔会出现这样的：

Give me value post about 965232173+583109685+1264792480+1590486025-1561369099-2130153687*1035104824-1002206700+947010525-2484529203*04373883=?

果然是把答案POST过去，参数应该是`value`

那要这么快，只有上脚本了呗。

尝试解题

试着写个python脚本

脚本大概思路，requests库获取html内容，在用lxml的etree获取`<div>`标签中的表达式

但是发现他那个表达式吧，有时候结尾是`=?;`有时候又是`=?`，所以表达式还得处理以下。

这个方法挺蠢的，后来看到其他带佬们用的是正则表达式来直接寻找表达式。

正则表达式：`r'(\d+[+\-*])+(\d+)'`

```python
import requests
import re

url = 'http://114.67.246.176:18368/'
session = requests.session()
respone = session.get(url)
htmltext = respone.text

expression = re.search(r'(\d+[+\-*])+(\d+)',htmltext).group()
result = eval(expression)
value = {'value':result}

flag = session.post(url,data=value)

print(flag.text)
```

有时候获取不到flag，应该是因为有时候python和php计算的大数字结果不一样，用PHP来写这个脚本应该更好

考察

脚本编写

正则表达式