BugkuCTF web18_秋名山车神 writeup

原创

Mitch311 于 2021-01-11 00:23:29 发布 1875 收藏 1
分类专栏： CTF 文章标签： unctf python

本文链接：https://blog.csdn.net/Mitchell_Donovan/article/details/112453206

web18_秋名山车神

原题链接

key:python脚本

①题目环境里的网页长这样式的

亲请在2s内计算老司机的车速是多少
2126861233*69635979+151515944*1853677350+902603206+1603221138-124923431-1177182821+1731395739+505426748+758578515=?;

意思是2s内让我们算一个变态表达式，疯了吧

刷新多次，发现数字是变化的，问题更严重了.....

不过刷新过程中发现了要提交的参数value

Give me value post about 1419445093*1120069432-504921096-1606936615*1730027932*2022849225*342868091-1401592907+766410450+1231039412*1640398461 ?

②不妨写个(白嫖)python脚本吧

> **本题采用正则表达式，如果不熟悉这个可以先看看教程：正则教程**

```
import requests #引入request库
import re   #引入re库

url = '''http://123.206.87.240:8002/qiumingshan/'''
s = requests.session()  #用session会话保持表达式
retuen = s.get(url)

equation = re.search(r'(\d+[+\-*])+(\d+)',retuen.text).group()
result = eval(equation) #eval()函数用来执行一个字符串表达式,并返回表达式的值。

key = {'value':result}#创建一个字典类型用于传参
flag = s.post(url,data=key)#用post方法传上去

print(flag.text)
```

> **这个脚本重点还是第7行的正则，解释下**
>
> - **re.search()表示从文本的第一个字符匹配到最后一个，其第一个参数为正则表达式，第二个参数是要匹配的文本**
> - **r''表示内容为原生字符串，防止被转义**
> - **(\d+[+\-*])+(\d+)：\d+表示匹配一个或多个数字；[+-*]表示匹配一个加号或一个减号或一个乘号（注：减号在中括号内是特殊字符，要用反斜杠转义）；所以(\d+[+-*])+表示匹配多个数字和运算符组成的“表达式”；最后再加上一组数字(\d+)即可**
> - **group()返回字符串**

③执行脚本后一定概率可能获得flag，所以需要多跑几遍才行

为什么呢？猜测可能是脚本计算错误或者服务器端的PHP脚本计算大数值有误差

> 最后注明一下参考网址