BugkuCTF-web-秋名山车神 writeup

原创

会下雪的晴天 于 2019-09-29 17:37:17 发布 3325 收藏 8

分类专栏： CTF做题记录

会下雪的晴天

本文链接：https://blog.csdn.net/weixin_43578492/article/details/101701339

CTF做题记录 专栏收录该内容

33 篇文章 1 订阅

订阅专栏

脚本能力+0.001

快速反弹POST请求

另：bugku 速度要快

题目描述

题目链接

解题思路

本题考验脚本能力，手动提交？哼，不存在的

题目多次刷新，出现要提交的参数：`value`

Give me value post about 1405699375+1861944687*2006341432-1639404255+520566677-1929920056-489222166*1219327956*309089425*1762693366+1111570279=?

这么长的数字计算器算都可能溢出，所以上脚本，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会话保持表达式是同一个
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}
print(s.post(url, data = key).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

FLAG?

执行脚本后一定概率可能获得flag，why?
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

```python
import requests
import re

url = '''http://123.206.87.240:8002/qiumingshan/'''
s = requests.session()
retuen = s.get(url)
equation = re.search(r'(\d+[+\-*])+(\d+)', retuen.text).group()

result = eval(equation)
key = {'value':result}
print(s.post(url, data = key).text)
```

```
å<0x8e><0x9f>æ<0x9d>¥ä¼ ä¹<0x9f>æ<0x98>¯è<0x80><0x81>å<0x8f>¸æ<0x9c>º Bugku{YOU_DID_IT_BY_SECOND}
[Finished in 0.5s]
```