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

本文链接：https://blog.csdn.net/qq_45837896/article/details/108024329

等了这么久这道题终于能注册了！赶紧做一波

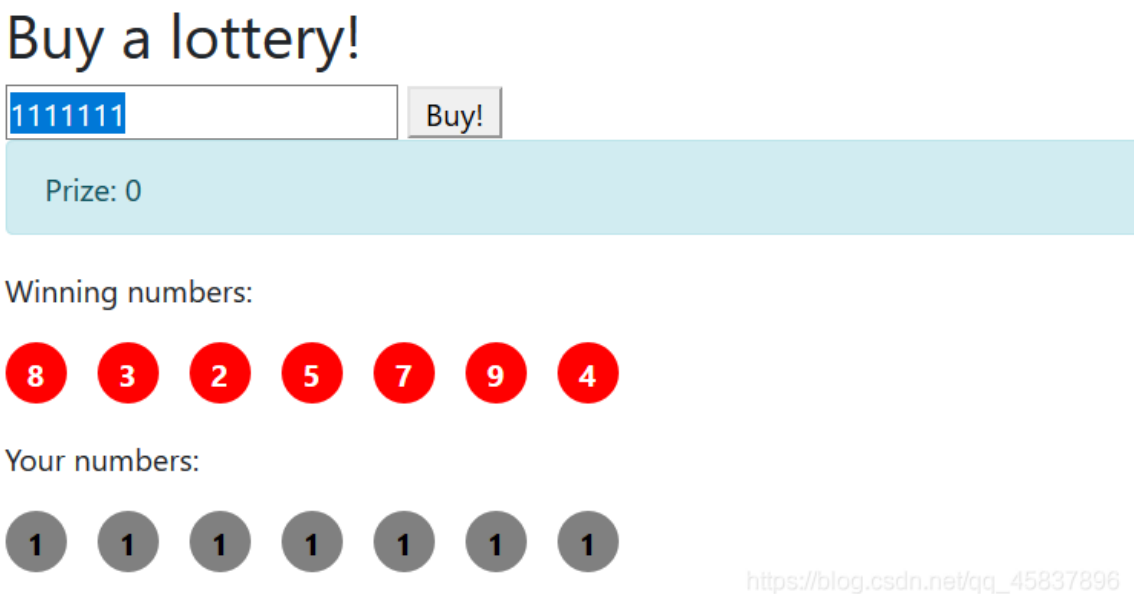
这是一道长得比较新奇的题

打开是一个博彩网站

根据提示注册之后

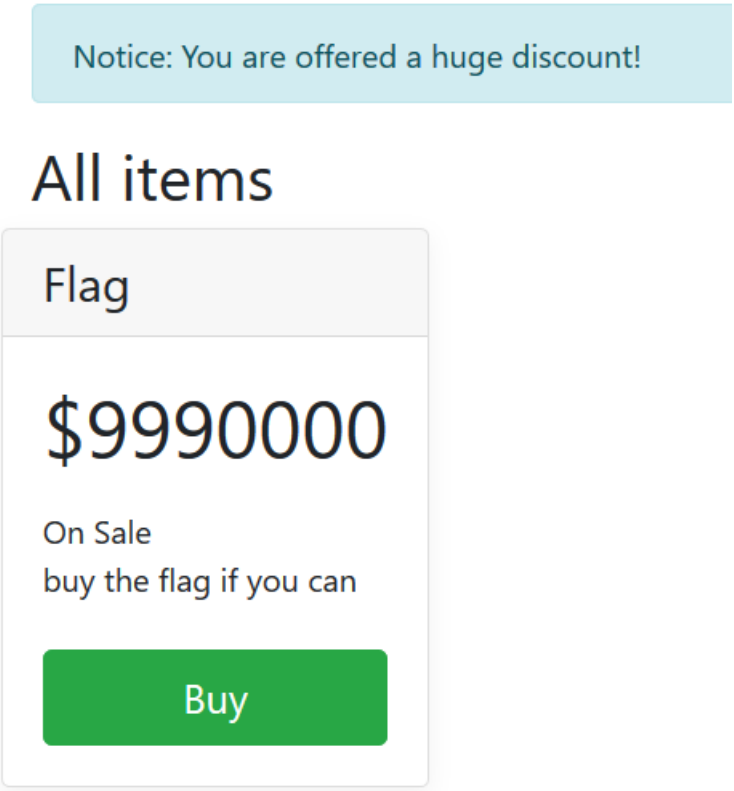
> 如果不能注册，没关系不只是你一个人遇到了这个问题，多大开几次再不济多开几次环境，我试了n次...

首先尝试一下



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



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

```php
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

```php
$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

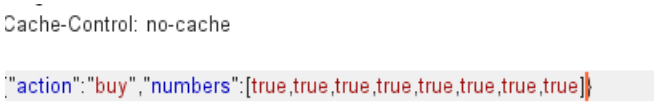
PHP类型比较表

松散比较 ==

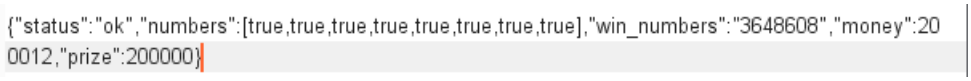
	TRUE	FALSE	1	0	-1	"1"	"0"	"-1"	NULL	array()	"php"	""
TRUE	TRUE	FALSE	TRUE	FALSE	TRUE	TRUE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE
FALSE	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	TRUE	TRUE	FALSE	TRUE
1	TRUE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
0	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE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

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

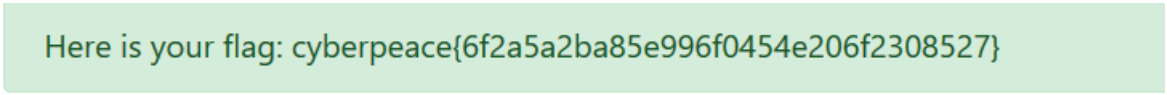
但是网站上传只能是一串数字，我们可以考虑一下bp抓包改一下数据



将上传的一串数字改成数组，然后放过



多来几次多搞点，去买一下flag



很有趣