# 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

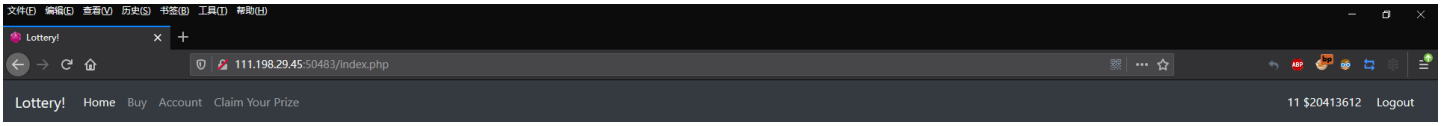


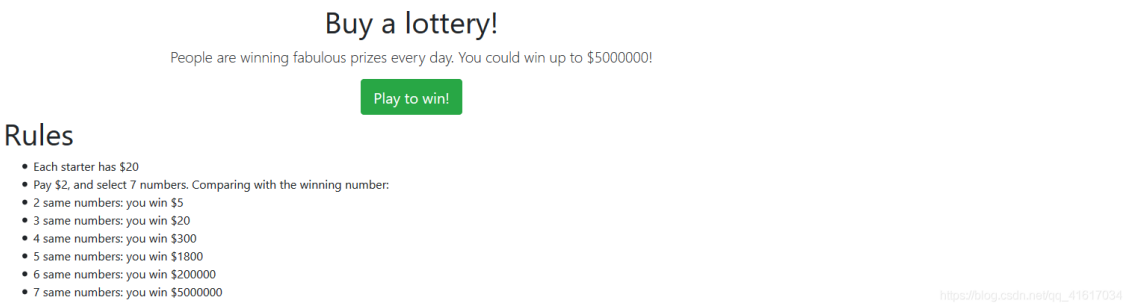
本文链接：https://blog.csdn.net/qq_41617034/article/details/104609105



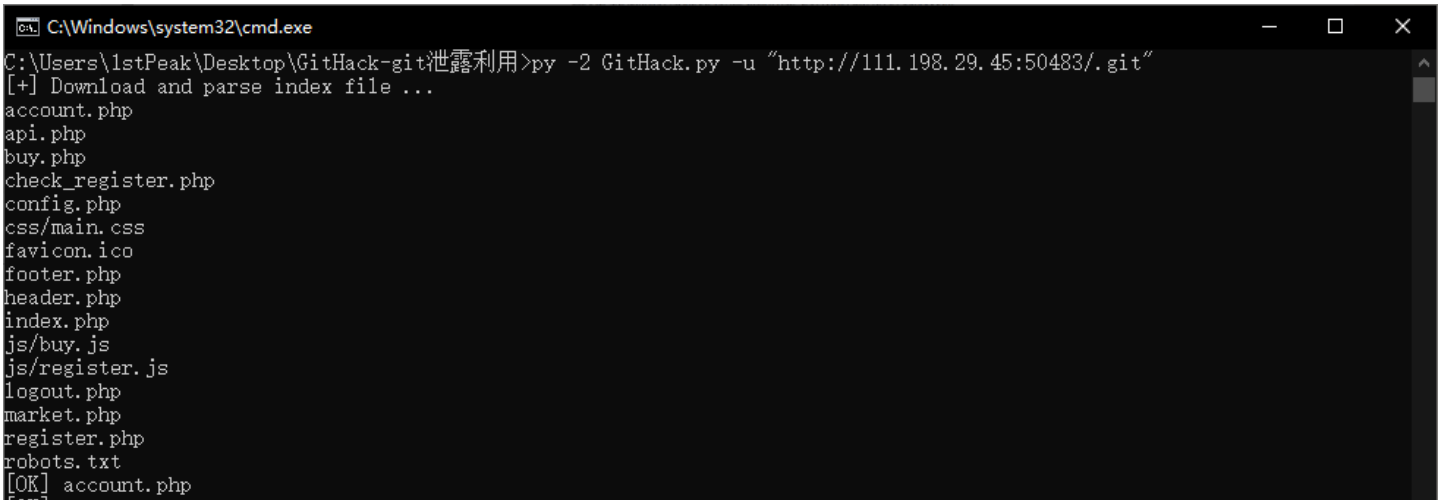


题目：




该题存在git泄露，使用GitHack.py进行扫描



```
[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
```



| 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 |

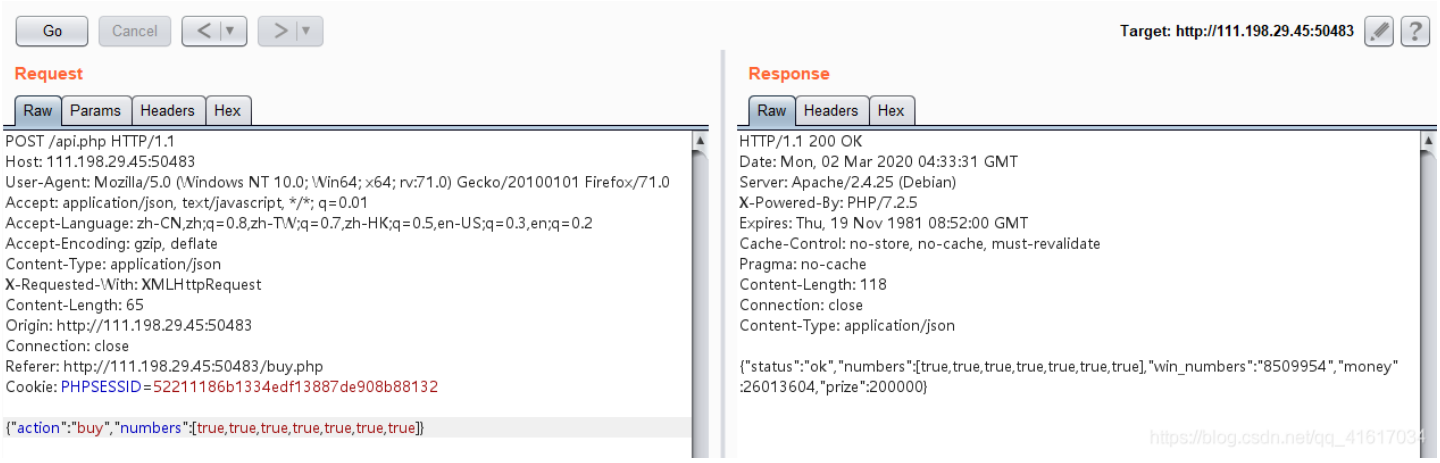


最后定位在api.php中的buy函数存在漏洞
源码：

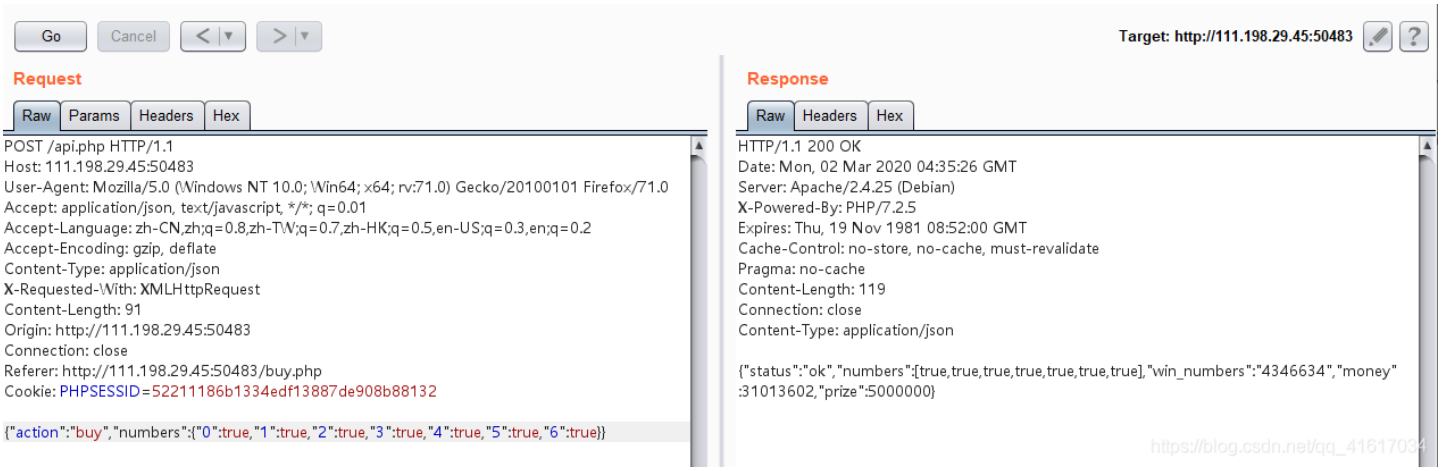
```php
function buy($req){
 require_registered();
 require_min_money(2);

 $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




或




多Go几次，之后就去购买flag吧