攻防世界lottery

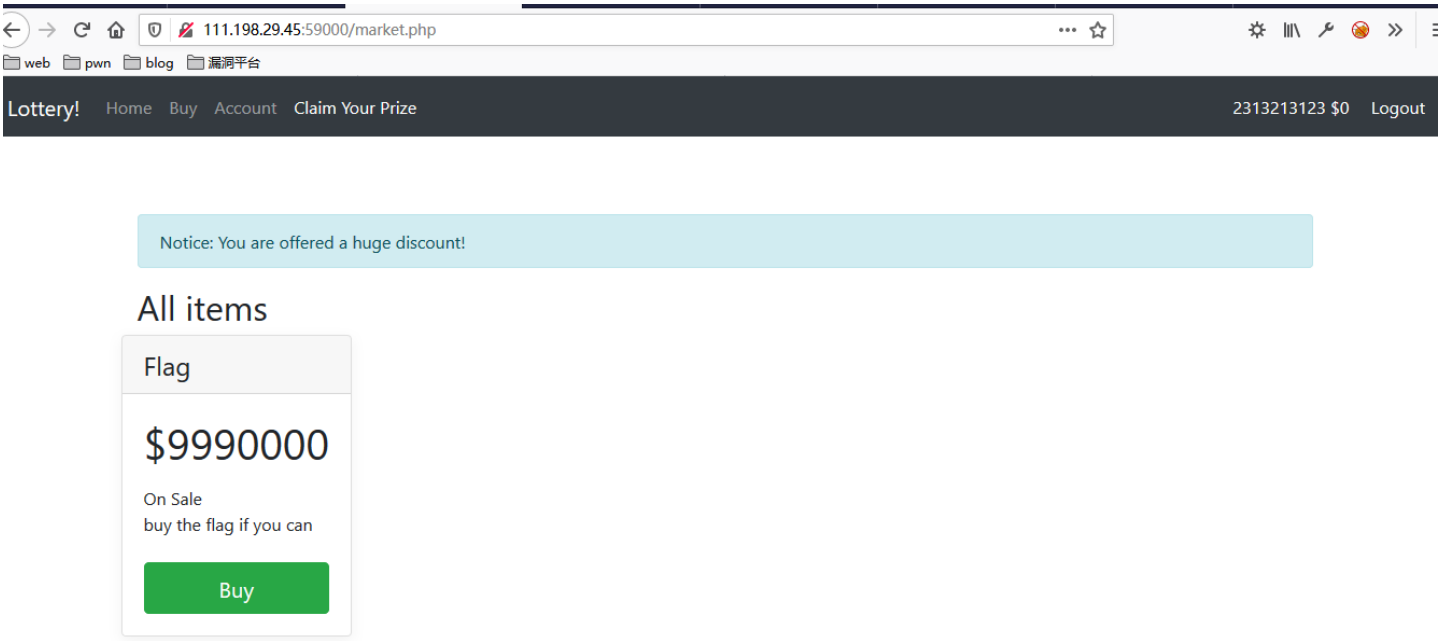
原创

expyoyo 于 2020-07-18 23:25:19 发布 527 收藏

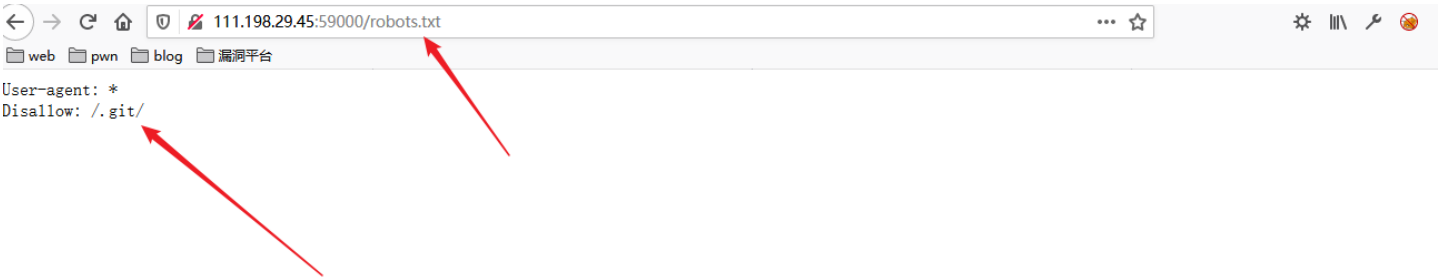
昨天第一次写博客被自己水到了，因此在这里推荐几位大师傅，A_dmin.这位pwn师傅doudoudedi.现在每天从师傅哪学一招都很开心。好了现在我们来愉快的刷题。

攻防世界lottery

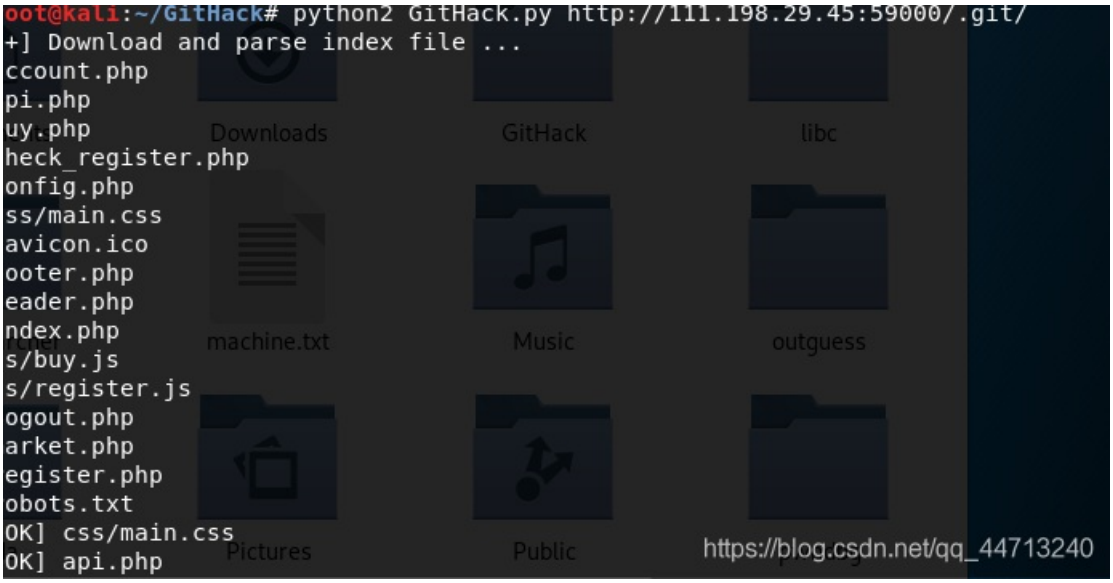
先访问一下题目，通过网页的浏览发现只有输入7个数字来跟玩彩票一样猜对几个数字对于多少钱，可以通过钱购买flag。可是我们有什么办法修改钱数，有点迷茫，常规操作先爆破一下目录。



发现robots.txt发现



/.git/常见的网站备份后缀常见的网站备份后缀,希望有帮助，看了大佬的博客知道了lijiejie的git信息泄露利用工具：
https://github.com/lijiejie/GitHack好像需要python2环境，想了想只能搭载到自己的kali里面
apt-get install https://github.com/lijiejie/GitHack
git clone https://github.com/lijiejie/GitHack
使用很简单python GitHack.py https://mp.csdn.net/mdeditor/103022286



被小姐姐get下来了，接下来进行代码审计，这个对于小白来说有点难，今天尽力看看吧，

```
require_once('config.php');
header('Content-Type: application/json');

function response($resp){
 die(json_encode($resp));
}

function response_error($msg){
 $result = ['status'=>'error'];
 $result['msg'] = $msg;
 response($result);
}

function require_keys($req, $keys){
 foreach ($keys as $key) {
  if(!array_key_exists($key, $req)){
   response_error('invalid request');
  }
 }
}

function require_registered(){
 if(!isset($_SESSION['name']) || !isset($_SESSION['money'])){
  response_error('register first');
 }
}

function require_min_money($min_money){
 if(!isset($_SESSION['money'])){
```

```
 if(!isset($_SESSION['money'])){
  response_error('register first');
 }
 $money = $_SESSION['money'];
 if($money < 0){
  $_SESSION = array();
  session_destroy();
  response_error('invalid negative money');
 }
 if($money < $min_money){
  response_error('you don\' have enough money');
 }
}


if($_SERVER["REQUEST_METHOD"] != 'POST' || !isset($_SERVER["CONTENT_TYPE"]) || $_SERVER["CONTENT_TYPE"] != 'appl
ication/json'){
 response_error('please post json data');
}

$data = json_decode(file_get_contents('php://input'), true);
if(json_last_error() != JSON_ERROR_NONE){
 response_error('invalid json');
}

require_keys($data, ['action']);

// my boss told me to use cryptographically secure algorithm
function random_num(){
 do {
  $byte = openssl_random_pseudo_bytes(10, $cstrong);
  $num = ord($byte);
 } while ($num >= 250);

 if(!$cstrong){
  response_error('server need be checked, tell admin');
 }

 $num /= 25;
 return strval(floor($num));
}

function random_win_nums(){
 $result = '';
 for($i=0; $i<7; $i++){
  $result .= random_num();
 }
 return $result;
}


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]);
}

function flag($req){
 global $flag;
 global $flag_price;

 require_registered();
 $money = $_SESSION['money'];
 if($money < $flag_price){
  response_error('you don\' have enough money');
 } else {
  $money -= $flag_price;
  $_SESSION['money'] = $money;
  $msg = 'Here is your flag: ' . $flag;
  response(['status'=>'ok','msg'=>$msg, 'money'=>$money]);
 }
}

function register($req){
 $name = $req['name'];
 $_SESSION['name'] = $name;
 $_SESSION['money'] = 20;

 response(['status'=>'ok']);
}


switch ($data['action']) {
 case 'buy':
  require_keys($data, ['numbers']);
```

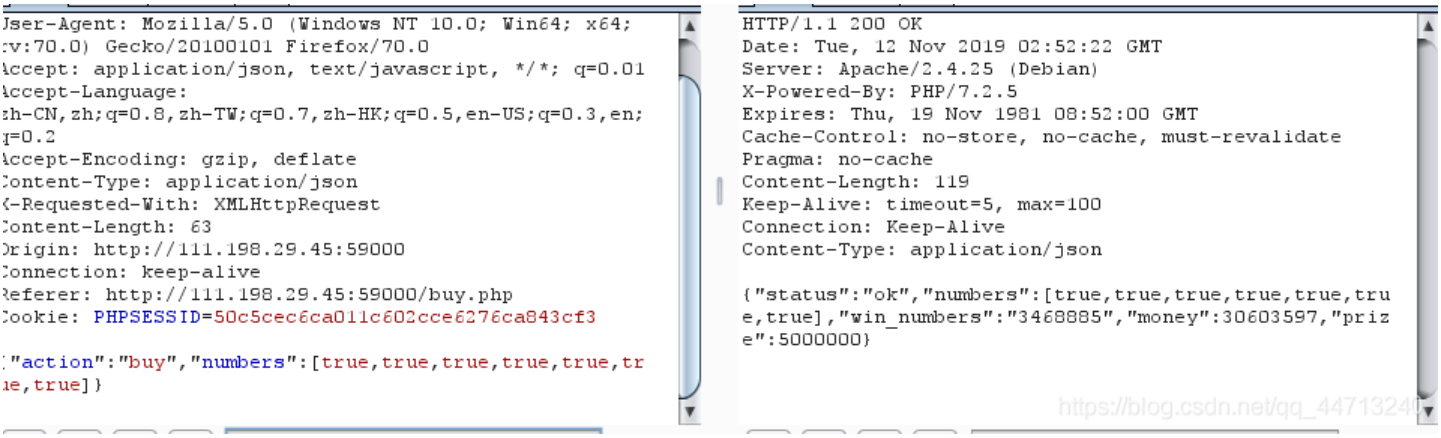
```
  require_keys($data, ['numbers']);
  buy($data);
  break;

 case 'flag':
  flag($data);
  break;

 case 'register':
  require_keys($data, ['name']);
  register($data);
  break;

 default:
  response_error('invalid request');
  break;
}
```

于是在先前下载下来的网站源文件中打开api.php
注意到这串代码，意思是将传入的数字和随机的数字进行比较，最后对比两者相等的个数来增加相应的钱。这里没有对输入的数据进行任何的过滤，而且对比相等处用的" == “来比较，所以可以用传入” true "来绕过判断



接下来就可以购买flag愉快的解题就结束了，嘻嘻嘻嘻嘻嘻嘻