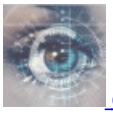
攻防世界web之Lottery

原创

n0vic3 于 2019-05-23 16:55:45 发布

分类专栏： ctf 文章标签： 攻防世界 web git泄露

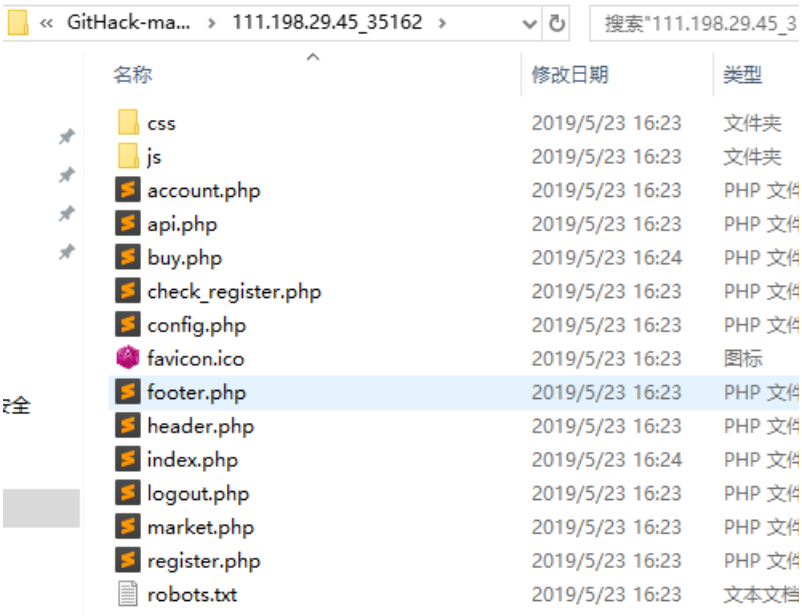


Lottery

上来先测试了一下，注册用户，购买彩票，拿到足够的钱，购买flag。大概就这样，发现buy.php页面，买完之后还是buy.php，没有页面的跳转，这让我有点搞不懂。

所以扫了一下网站，发现有robots.txt，访问发现

似乎也是Git泄露问题，下载一下试试，拿到很多文件



发现关键代码在api.php里面

```php
<?php
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'])){
  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']);
  buy($data);
  break;

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

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

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

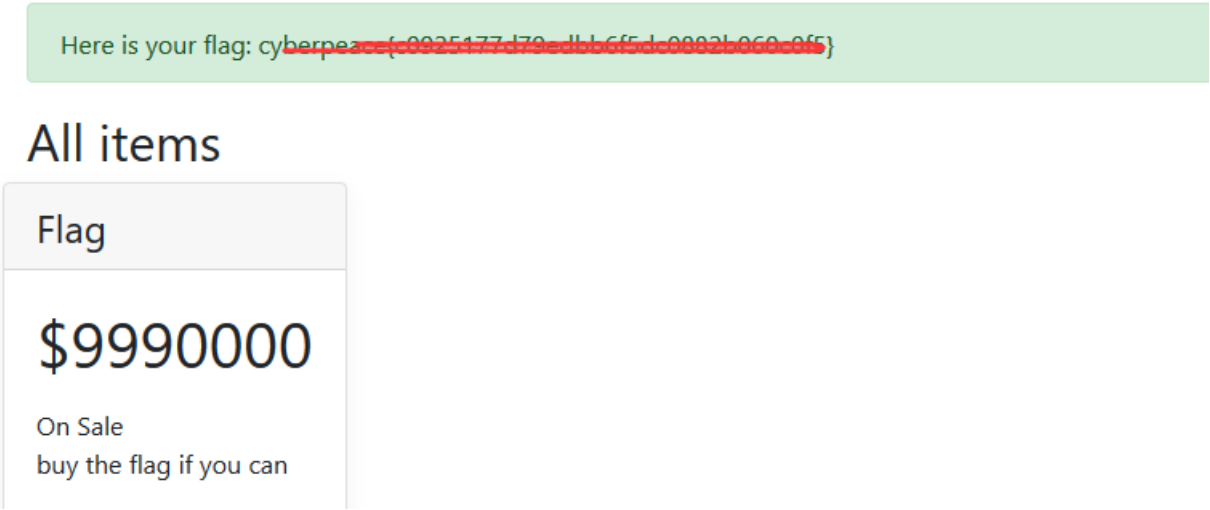
阅读源码我们发现，

> 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较的

通过以上三点，我们就可以操作一下了，

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，

bp抓包，然后构造数组，即可得到5000000，再来一次就是10000000，可以购买flag了



参考文章