2018鹏程杯 初赛 Writeup

原创

god_speed丶 于 2018-12-14 18:48:43 发布 1657 收藏

分类专栏： CTF

本文链接：https://blog.csdn.net/qq_38677814/article/details/84748650

1.签到

公众号回复

2.Traffic Light

`misc`

stegsolve打开看可以发现1000多帧

网上找了个脚本分离所有帧(python3+PIL）

根据红黄绿信号猜测0 1 空格

可以图像识别 但细心点可以发现**文件大小**并不相同 于是根据图像大小得到一串数字 相应的图片做一个映射即可

3.Quotes

`misc`

脑洞题

`My+mission+in+life+is+not+mer ely+to+survive+but to+thrive+and+to+do+so+w ith+s 空 ome+pass i on+some+compass ion+so me+humor+and+some+style`

有个地方有空格 额外注意一下 上面我用汉字表示了 markdown吃空格

```
#include <bits/stdc++.h>
using namespace std;
int cal(string s){
 int ans = 0;
 for(int i=0;i<s.size();++i){
  if(s[i]=='+') ans++;
 }
 return ans;
}
char emm[]={" abcdefghijklmnopqrstuvwxyz"};
int main(){
 string s;
 string ans;
 while(cin>>s){
  int t = s.size();
  t -= cal(s);
  ans += emm[t];
 }
 cout<<ans<<endl;

 return 0;
}
```

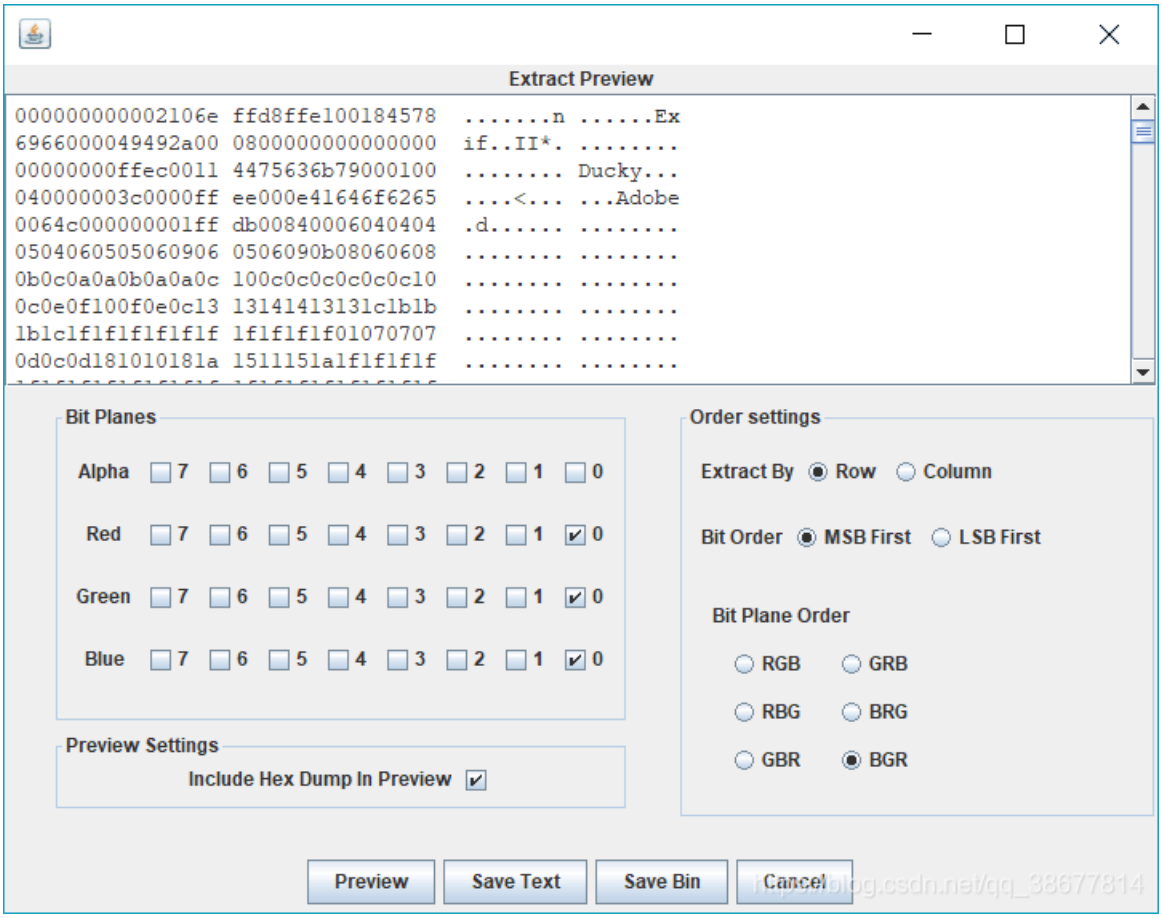
4.GreatWall

`misc`

lsb

stegsolve打开

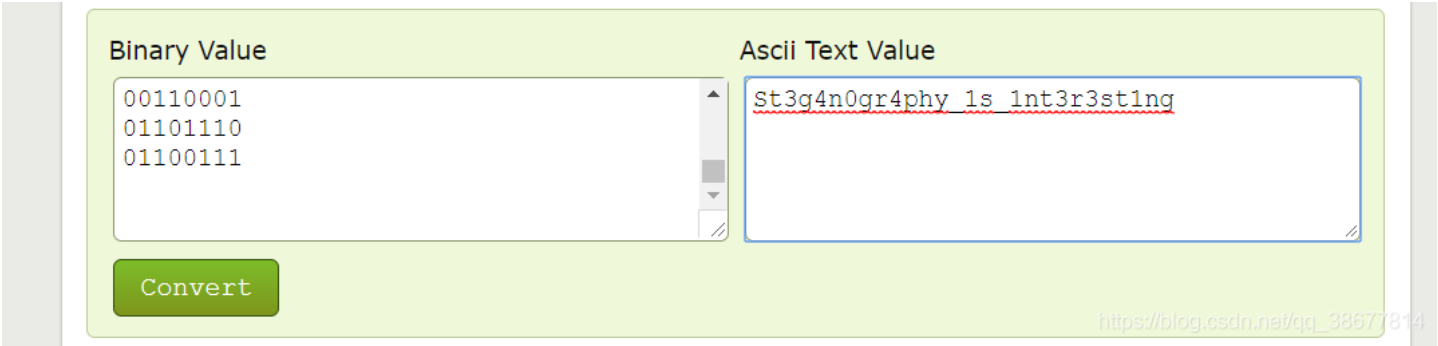
data-extract



导出bin...

删去前面没用的字符 他是个jpg...

jpg里是+ - —— 猜测为分隔符 0 1



5.MyBlog

`web`

1. 扫后台 http://58.20.46.148:26111/index.php
2. response flag: JTNGZmxhZw==
3. 解码得到 '?flag'
4. 根据提示about也有后端？
5. http://58.20.46.148:26111/YWJvdXQ=.php about base64加密后。。
6. 格式：echo "str" | base64
   将字符串str+换行 编码为base64字符串输出。

格式：echo -n "str" | base64
将字符串str编码为base64字符串输出。注意与上面的差别。
7./index.php?flag=php://filter/convert.base64-encode/resource=YWJvdXQ%3D

```php
<?php

$filename = 'flag.txt';
$flag = 'flag.txt';
extract($_GET);

if(isset($sign)){
 $file = trim(file_get_contents($filename));
 if($sign === $file){
  echo 'Congratulation!<br>';
  echo file_get_contents($$falg);
 }
 else{
  echo 'don`t give up';
 }
}

?>
```

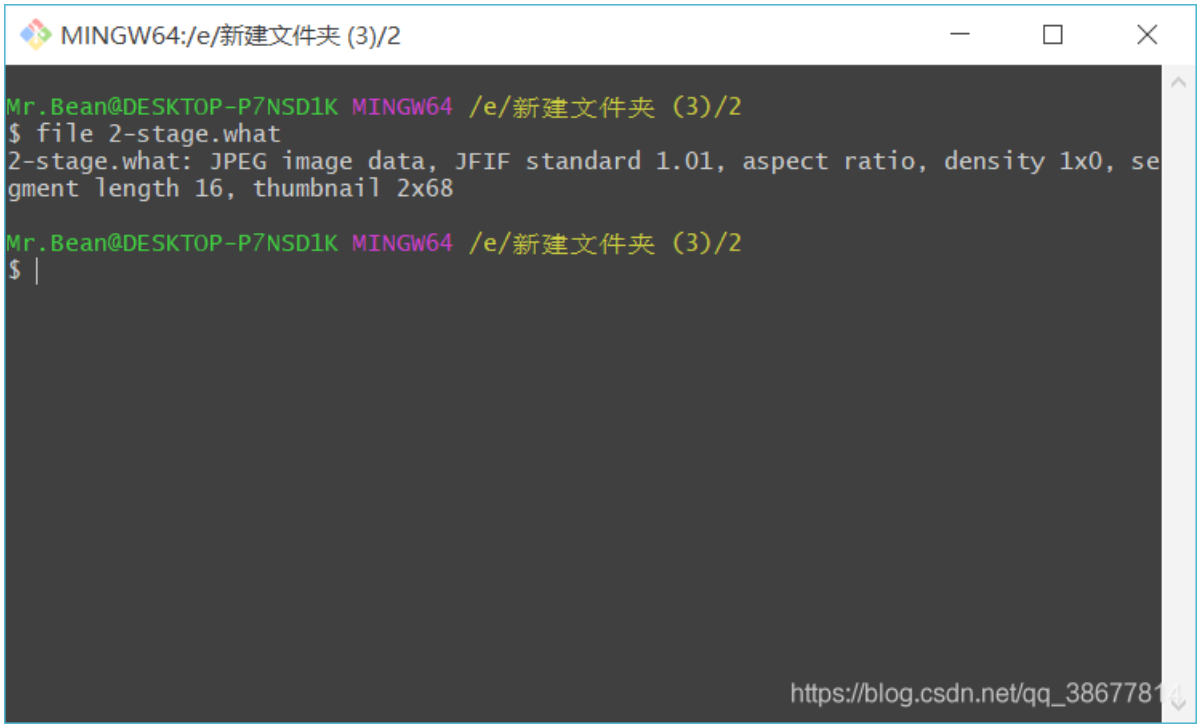
8.审计php代码 如何bypass?
当传进去的参数作为文件名变量去打开文件时，可以将参数php://传进，同时post方式传进去值作为文件内容，供php代码执行时当做文件内容读取
POST传值

6. what's this

1. 得到一张玫瑰图片 改成zip解压
2. word改成zip解压

3.

4. 可以看到word里有一段隐藏文字

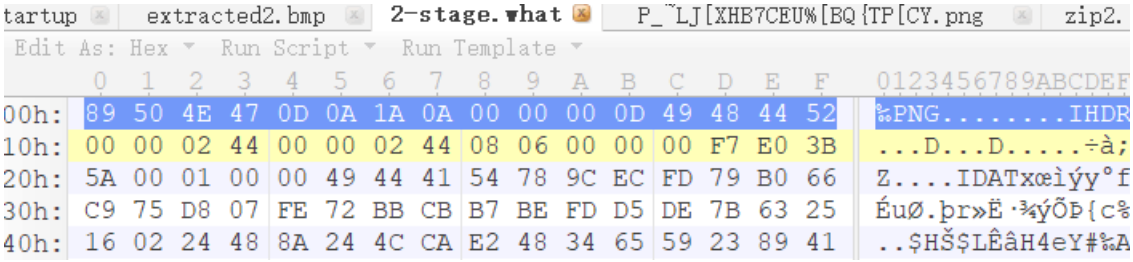


5.

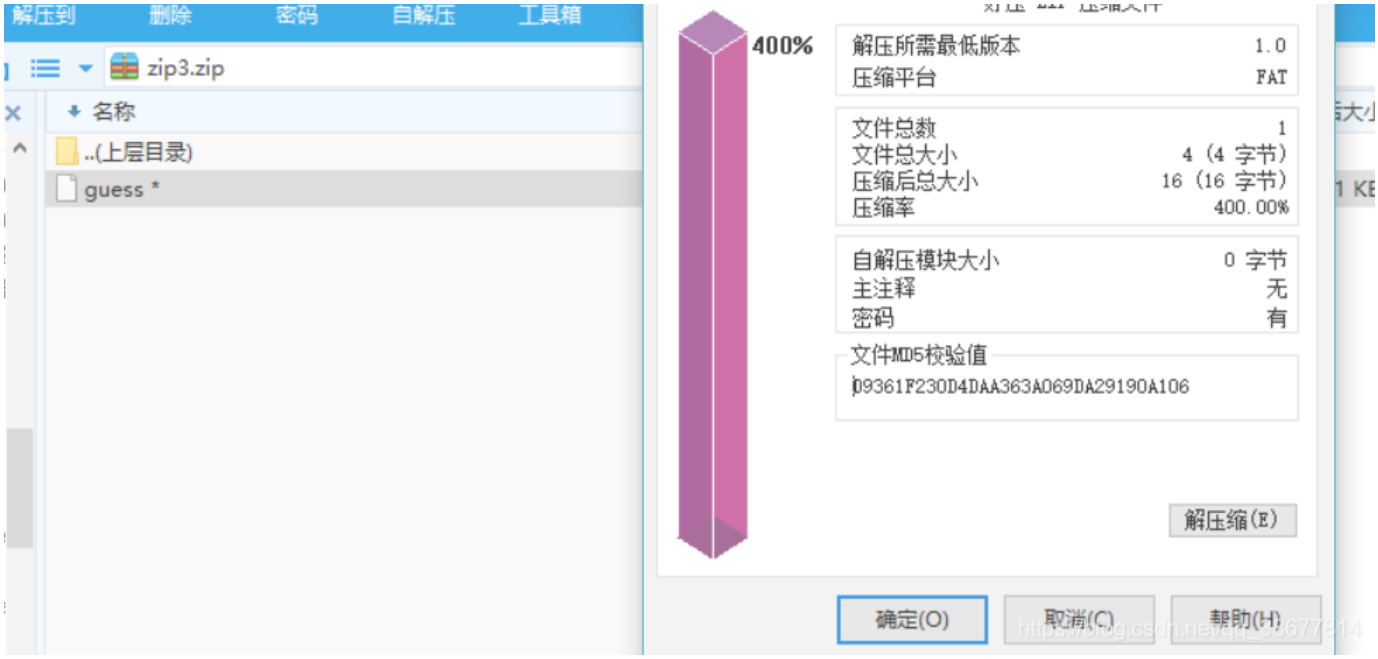
6. 将其改成jpg 发现并不能打开

7. zip2.zip中有一个文件和2-stage似乎一样 所以可以明文攻击

8. 但是我们发现CRC32并不一样 所以010editor打开2-stage.what 再随便打开一个png 修改文件头



9. 然后用神器archpr 明文攻击一下
   得到：Hello_Hi
10. ps:你有没有发现那个txt。。。有同学指出将word里的隐藏文字copy到txt中同样可以实现明文攻击
11. 解压之后修改2-stage为jpg
12. `python lsb.py extract 2-stage out Hello_Hi`
    是个图片 考虑lsb
13. file一下发现是个zip 解压之



14.
15. 发现只有4个字节 暴力跑crc32

```
import datetime
import binascii
def showTime():
 print datetime.datetime.now()

def crack():
 crcs = set([0x99BED60E])
 r = "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789"
 for a in r:
  for b in r:
   for c in r:
    for d in r:
     txt = a+b+c+d
     # print txt
     crc  =binascii.crc32(txt)
     if (crc & 0xFFFFFFFF) in crcs:
      print txt

crack()
```

得到`girl`
解压之后得到fakeflag 很失望了
16. 回到word解压之后的文件中 我们可以发现有个I_Love_You.emf大小刚好702字节和我们的zip4相同。。。
17. 异或？

```
file1 = open("I_Love_You.emf",'rb')
file2 = open("zip4.zip",'rb')
f1 = file1.read()
f2 = file2.read()
print len(f1),len(f2)
out = ''
for i in range(len(f2)):
 out += chr(ord(f1[i])^ord(f2[i]))
with open('flag.zip','wb') as f:
 f.write(out)
```

解压之后发现真的是flag~

出题人nb