2018鹏程杯 初赛 Writeup



 god_speed、
 于 2018-12-14 18:48:43 发布
 1657 % 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_38677814/article/details/84748650

版权

CTF 专栏收录该内容

22 篇文章 0 订阅

订阅专栏

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+PL) 根据红黄绿信号猜测01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 2 Queters

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;
}
</pre>
```

4.GreatWall

misc

lsb

stegsolve打开

data-extract

\$3)	- 🗆 X								
Extract Preview									
00000000002106e ffd8ffe100184578 n Ex 6966000049492a00 08000000000000 if.II*. 00000000ffec0011 4475636b79000100 Ducky 04000003c0000ff ee000e41646f6265 Adobe 0064c00000001ff db00840006040404 Adobe 0b0c0a0a0b0a0a0c 100c0c0c0c0c010 0c0e0f100f0e0c13 13141413131c1b1b									
Bit Planes	▼ Order settings								
Alpha 7 6 5 4 3 2 1 0	Extract By 🖲 Row 🔾 Column								
Red 7 6 5 4 3 2 1 2 0	Bit Order 💿 MSB First 🔾 LSB First								
Green 7 6 5 4 3 2 1 2 0 Blue 7 6 5 4 3 2 1 2 0	Bit Plane Order								
Preview Settings Include Hex Dump In Preview 🖌	 ○ RBG ○ BRG ○ GBR ● BGR 								
Preview Save Text Save Bin Cancel blog.csdn.net/gg_38677814									

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

St3g4n0gr4phy 1s 1nt3r3st1ng

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。。
- 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

```
$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

Word 选项		?	\times						
常规	□ ■改文档内容在屏幕上的显示方式和在打印时的显示方式。								
显示									
校对	页面显示选项								
保存	✓ 在页面视图中显示页面间空白(W) ^①								
版式	☑ 显示突出显示标记(出) ^①								
语言	☑ 悬停时显示文档工具提示(L)								
高级	始终在屏幕上显示这些格式标记								
自定义功能区	□ 制表符(I) →								
快速访问工具栏	□ 卒格(S) ***								

加载项	✓ 段落标记(M)	
信任中心	✓ 隐藏文字(D) abc	
	□ 可选连字符(Y) ¬	
	✓ 对象位置(C)	
	可选分隔符(<u>O</u>)	
	显示所有格式标记(<u>A</u>)	
	1770%	
	打印选坝	
	✓ 打印在 Word 中创建的图形(<u>R</u>) ^①	
	打印背景色和图像(<u>B</u>)	
	□ 打印文档属性(P)	
	□ 打印隐藏文字(凶)	
	□ 打印前更新域(<u>F</u>)	
	打印前更新链接数据(<u>K</u>)	
		https://blog_确定

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

tartup) 🗵	ex	tra	cted2	2. bmj	p 🗵	2-	sta	ge.	That	: 🗷	P.	_~LJ	[XHE	37CEI	J% [BQ]{TP[CY.png 📧 zip2.
Edit	As:	Hex		Run	Scri	ipt	- R	un 1	Cemp	late	Ψ.						
	Ò	1	2	3	4	5	6	7	8	9	A	B	Ç	D	E	F	0123456789ABCDEF
00h:	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNGIHDR
10h:	00	00	02	44	00	00	02	44	08	06	00	00	00	F7	E0	3B	Dֈ;
20h:	5A	00	01	00	00	49	44	41	54	78	9C	EC	$\mathbf{F}\mathbf{D}$	79	в0	66	ZIDATxœìýy°f
30h:	C9	75	D8	07	FE	72	BB	CB	в7	BE	\mathbf{FD}	D5	DE	7B	63	25	ÉuØ.þr≫Ë ⅓ýÕÞ{c%
40h:	16	02	24	48	8 A	24	4C	CA	E2	48	34	65	59	23	89	41	\$HŠ\$LÊâH4eY#‰A

- 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 b in r:
        for c in r:
        for c in r:
        for c in r:
        for d in r:
        txt = a+b+c+d
        # print txt
        crc =binascii.crc32(txt)
        if (crc & 0xFFFFFFF) 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