# 最详细攻防世界MISC新手区(已完结)小白解法



<u>开着拖拉机卖茄子</u> ● 于 2020-04-05 22:47:25 发布 ● 7404 ☆ 收藏 47 分类专栏: <u>攻防世界解题集合</u> 文章标签: <u>信息安全 经验分享 安全</u> 版权声明:本文为博主原创文章,遵循 <u>CC 4.0 BY-SA</u> 版权协议,转载请附上原文出处链接和本声明。 本文链接: <u>https://blog.csdn.net/qq\_42906381/article/details/105335021</u> 版权



攻防世界解题集合 专栏收录该内容

1篇文章1订阅 订阅专栏

#### 攻防世界MISC! 安排

新手区已完结

001 this\_is\_flag

002 pdf

003 如来十三掌

004 give\_you\_flag

005 坚持60s

006 gif

007 掀桌子

008 ext3

009 stegano

010 SimpleRAR

011 base64stego

012 功夫再高也怕菜刀

## 新手区已完结

001 this\_is\_flag



## 002 pdf

根据题意,只需要把图片**移开**,就能发现flag



003 如来十三掌

原本以为这是一个隐藏文件,结果什么都没解出来 于是看着这段话,尝试读取佛文,果不其然,参悟了其中奥秘 猜这是一段密码,百度发现,需要进入一个名叫与佛论禅的网址解密

与佛论禅

听佛说宇宙的真谛	参悟佛所言的真意	普度众生
	心不变,万物皆不变	
浸信國時代數會構成是 讀者恐己在得點提呼伽語	」擁有来沒要這個小規則發展這些解決的容量的 19 例幕三死住職大歸書數一選	参任时心前守著大度地 <b>共振</b> 電沙擊

加上佛曰之后,解了一段base64编码,解密发现乱码

39.3x/1@0 <b>0;00</b> ;# <b>0</b> 3%1; <b>00</b> 00;0011@00050018;00	MzkuM3gvMUAwnzuvn3cgozMIMTuvqzAenJchMUAeqzWenzEmLJW9
然后又发现这是一种 <b>rot-13</b> 加密方式	
	C   ★ 4000   m 78   C 4
② 本陽奈曲 料着中国 科学百科博奈编写与应用工作项目 审核。 ROT13 (回時13位, rotate by 13 places, 有时中间加了个连字符称作ROT-13 文团性论论: 田氏的理(14, croster), 加速型、通知规范(10 和助能);这些现在的工具、目的思。	3)是一种阔易的普挽式密码。它是一种在英 3)过程主动架相局的性格一颗 POT130#数
文件的LinearCount Figure Coll College 2015年1月19日1日1日1日1日1日1日1日1日1日1日1日1日1日1日1日1日1日1	18921971年時間至20日759分 1999 1999 1999 1999 1999 1999 1999 1
書用ROT13到一時文字上仅仅只需要检查字元字母顺序并取代它在13位之月 字母母4月可可。48点时间、48点时间、46点半接到44点时了、然后自然同样。48点点	后的对应字母,有需要超过时见重新绕回26英文
文字母里头的字元受影响,数字、符号、空白字元以及所有其他字元都不变。因 26=2×13, ROTI3函数是它自己的道反: <sup>[1]</sup>	入 GBORG 新月上房的加加 入日之三山改正吴 协只有在英文字母表里头只有26个,并且
对任何字元x: ROT13(ROT13(x))=ROT26(x)=x。	
换句话说,两个连续的ROT13应用函式会回复原始文字(在数学上,这有时 像对等加密(reciprocalcipher))。	f称之为对合(involution);在亚码学上,这叫

转化之后,再次解码

flag{bdscjhbkzmnfrdhbvckijndskvbkjdsab}

ZmxhZ3tiZHNjamhia3ptbmZyZGhidmNraWpuZHNrdmJramRzYWJ9

即得到flag

004 give\_you\_flag

下载下来之后,发现真的是个表情包,里面还闪现了一个二维码! 利用**Stegsolve.jar**打开之后,**Analyse-Frame Browser**一帧一帧的看 在50个发现了残缺的二维码



少了三个块块,想办法补上。PS可以补,但是涉及到我的知识盲区了,只好找朋友帮忙。 机缘就这么来了!

准备给同学截图的时候,忽然想起来qq截图还有**画笔**的功能!



试了试,成功了哈哈哈 微信扫描就出结果了! 一点都看不出来哈哈哈

005 坚持60s

#### 下载之后发现可以进行反编译

## 下载个**java反编译器,**打开文件之后

英文应该不难懂,查找输入flag,全选上

Search For	Limit To
Type Constructor String Constant	Declarations
matching item:	
□-□ E:\春秋培训\攻防世界\MISC\0006\9dc125b □-⊕ cn.bjsxt.plane ① PlaneGameFrame	f1b84478cb14813d

#### 得到位置,双击进入



看到flag,复制过去 提交不对,看见等号,想是不是base64,解码还真是!

DajiDali\_JinwanChiji

RGFqaURhbGlfSmlud2FuQ2hpamk=

#### 得到flag

006 gif

下载前以为是一个gif动态图 下载后发现事情没那么简单 居然是一个一个的黑白图片,看似有规律



难带代表什么东西?看了一眼手机上电信公司10001发来的短信想到二进制!表示完之后,二进制转字符串得结果

110011001101100011	0000101100111011101101000110	01110101010011100101	111101100111011010010100011001111	101
		9	客场局的文本:	

## 007 掀桌子

这个题让我聪明的大脑无处安放

还是百度方法多

通过观察,试着将16进制字符转为字符串,发现不能直接转化,试着将ascii码值减去128再转化,得到flag. 两个一位,16进制转10进制,然后减去128再转成字符即可

🖨 Elle Edit View Navigate Code Belactor Run Io	ols VCS Window Help Billion (CDBEORIA) - State print	openhore/hello.py - PyCham (Administrator) -	D X
🖿 MEXIKA ) 🖿 Helo pri4 ) 🖬 openhome ) 🐔 helo py			
1 Project + O + O -			
* W HERENA - Statistics     * W Hele of the state of	<pre>1 # B@ 7365. +/~285829768 1 Import re 4 * - 'Statement'/Particle(state)/assette/statement' 5 * - 'res(state)/('S(2)'_e) 7 import 7 import in %: 6 * In %: 8 * * * * * * * * * * * * * * * * * * *</pre>		Coness Solve
Ran: 🐨 hello x			
C.Vineen.19893.VepOHrational homogeneous mi, Freshegi The flag is: hjovdjihjd * # # * # * # * # * #	python(Python37)python, ees fr/##29498/imilia 		
ul 188 terminal — ⊕ Python Coesale — ▶ ≴ Run — № 3; Debug 10		https://blog.csdn.net/qq_4290	6381

这样一整就出来结果了The flag is: hjzcydjzbjdcjkzkcugisdchjyjsbdfr 改格式就行了

## 008 ext3

这么明显的提示一定有问题!

倒不如直接用上次说到的foremost

一下子就整出了哈哈哈

名称	1
📙 outfile	4
f1fc23f5c743425d9e0073887c846d23	1

打开图片之后把flag输进去就发现事情没这么简单 居然是错的!

又想起来这种东西都能够解压,于是改后缀,解压,然后搜索flag



#### 发现了一个.txt打开,=结尾用base64解码

flag(sajbcibzskjjcnbhsbvcjbjszcszbkzj)

ZmxhZ3tzYWpiY2lienNrampjbmJoc2J2Y2pianN6Y3N6Ymt6an0=

得到flag

009 stegano

用火狐浏览器打开刚才下载的pdf文件

#### 按下**F12**进入控制台,输入**document.documentElement.textContent** 回车查看



发现一大段AABABA样式的东西,猜测是01但是这些有分割,能想到的只有摩斯密码有分割的,于是尝试改成摩斯密码(卑微的我只能一个一个改)

#### 摩斯密码在线加密解密工具

······································			 
Space:	Short-	Long:	 
加密 解密	SHORE.	Long.	
CONGRATULATIONS, FLAG:	1NV151BL3N3554G3		

发现flag

## 010 SimpleRAR

下载文件之后,解压只有一个.Txt文件,但是用Notepad++打开,发现了不一样的.png





猜测应该是丢失了。寻找方法。 顺便整了一波大佬的学习笔记 大佬笔记



## 尽管还是不太懂 但依旧掌握了精髓! 把箭头处的7A改为74再次保存解压





改后缀之后打开是一张单纯的白纸 然后用上我毕生所学的PS技能 打开之后发现里面有两个白底图层,分离出来 再用**StegSolve.Jar**打开直接点下面的左右符号,进行调色曝光 得到下面两张图片

٩	StegSo	ol	_		$\times$
File	Analyse	Help			
Red p	lane O				
			المتلع ا	in - in	8a **
		▝			
					- 1
· · · ·				وتلجي "	

这一张是下半部分

🛃 StegSol	_		$\times$
File Analyse Help			
Red plane 0			
	2	să	



右边那张是经过我细心处理又加上角块后的图片 然后再次打开PS继续使出毕生所学,把两张图片合成在了一起



再次打开曾经用过的QR-Research,直接得出了flag

QR Research	- 🗆 X
文件(F) 工具(T) 帮助(H)	
🚞 😰 🔝 🔹	📧 🌒 🖊
	纠错等级 掩码
and the second s	
	^
	~
已解码数据 1:	^
位 置:(654.3,454.1)-(909.9,451.6)-(650.8,713.9)-(907.6	5,711.7)
颜芭止常, 止像   版本: 3	
纠错等级:H, 掩码:4	
內谷: flag{vani4n_bu_we1shi}	

		New Nooncool
解码完成	IIID2000000000000000000000000000000	ny i i i i i i i i i i i i i i i i i i i

## 011 base64stego

这个题再一次证明了Python的重要性!吹爆Python 不多说,下载完文件直接解压就能发现一个.txt文件 然后百度知道这个题是一种base64位的加密版 然后顺便研究了研究: 原文链接 还是好迷糊啊

找到python代码之后运行



#### 得到flag 我要是会python能卑微的去看别人的代码?????

## 012 功夫再高也怕菜刀

下载之后利用foremost获得一个压缩包,解压发现需要密码 于是追踪数据流 CTRL+F搜索flag,发现了一个文本文档 对他进行追踪TCP流 点击下面的Save as...保存到本地 然后从 FFD8FF 开始到 FFD9 复制出来



#### 再利用Winhex

## 把那些粘贴进去,并选择到ASCII HEX

进行写入



### 按照.jpg保存下之后,就可以得到一张图片 这个图片中的字符就是解压密码 输入即可得到flag

MH - Habits jog												
in an	+ 183028	1			Q	谢	$^{\circ}$	0	tự	⊙ mean	34	100109
	这种	38.19	IA	4018.b		014						
						~	-					
(10)(10) (20)(10)(10)	well, yo	u need	pannwd									
								_				
									-			
attaciat	102.04						_	<b>p4</b> ss	wd_			
									1			
-	>						_					
										a (1790)	ER	
											1	100