攻防世界题目练习--MISC新手关(7~12)



<u>-日三省小白</u> 于 2019-10-26 00:02:14 发布



小白 专栏收录该内容
9 篇文章 0 订阅
订阅专栏

题目地址: 攻防世界MISC

题目7: 坚持60s

题目描述: 菜狗发现最近菜猫不爱理他, 反而迷上了菜鸡

解决:

一个jar包,利用java的反编译工具jd-gui打开jar包,可在PlaneGameFrame类中找到flag

🍵 Java Decompiler - PlaneGam	eFrame.class	– 🗆 🗙											
File Edit Navigate Search I	Help												
40013830022a4fdbaa4f9f36	89b13f18.jar $ imes$												
🕀 🖶 META-INF	GameObject.class Plane.class PlaneGameFrame.class ×												
🚔 🕀 🖶 cn.bjsxt	case 3:												
🖃 🖶 plane	67 printInfo(g, "哟, 炊事班长呀兄弟", 50, 150, 300);												
🕀 🕖 Bullet	68 break;												
🗄 🕖 Explode	case 4: 70 mmintTafa/a "加速你龄县天一会老王" 50 150 200)。												
🕀 🚺 GameObject	70 printinio(g, 加油你就是下一个老主, 50, 150, 500); 71 break:												
	case 5:												
∎ D PlaneGameFrame	73 printInfo(g, "如果撑过一分钟我岂不是很没面子", 40, 3	30, 300);											
🖻 🖶 util	74 break;												
🗄 🗐 Constant	76 printInfo(g, "flag{RGFgaURhbGlfSmlud2FuO2hpamk=}", 5	50, 150, 300);											
🗄 🗐 GameUtil	77 break;	.,,,.											
🗄 🗐 MyFrame	}												
🗄 🖶 images	}												
	3												
	public void printInfo(Graphics g, String str, int size, in	nt x, int y)											
	{												
	90 Color c = g.getColor(); 01 g getColor(Color PED);												
	92 Font f = new Font("宋体", 1, size);												
	93 g.setFont(f);												
	< niips://biog.esan.	nevqq_49499988											

题目8: gif

题目描述:菜狗截获了一张菜鸡发给菜猫的动态图,却发现另有玄机

解决:

下载后发现是一个压缩包,解压后,有104张图,都是黑白图组成的,非此即彼,类似于二进制,视白色图为 0,黑色图为1,得到一长串二进制编码,通过工具转换为字符串,得到flag

e	字符信息与二进制
ſΞ	进制串转换成字符 字符转换成N进制数 汉字转换 软件说明
	请依次输入二进制数: 01100110011011000110000101100111011101
	0101111101100111010010100011001111101
	长度: 104
-	十六进制数:66 6C 61 67 7B 46 75 4E 5F 67 69 46 7D
	十进制数: 102 108 97 103 123 70 117 78 95 103 105 70 125
	字符: flag{FuN_giF}
	hitps://blog.esclaurei/gg_4049088

题目9: 掀桌子

题目描述: 菜狗截获了一份报文如下

c8e9aca0c6f2e5f3e8c4efe7a1a0d4e8e5a0e6ece1e7a0e9f3baa0e8eafae3f9e4eafae2eae4e3eaebfaebe3f5e7e 生气地掀翻了桌子(╯°□°) ╯ ⌒ ┶━━┶

解决:

•

一串十六进制编码,两两一位,转换成十进制,再根据ASCII码转换为字符

写一段js脚本,运行一下



是乱码..因为每个转换后的ASCII码值都大于127,不是有效字符

é	ò óè	è	ìá	éó	èêú	- ù	êú	ê	ê	ú	éó	èêùêó	ò
~	0 00	•	1 4	00	000	~	00	· ·	<u> </u>	~		00000	<u> </u>

试着将每个转换后的十进制先减去128,再转为字符



再运行一遍

FreshDog! The flag is: hjzcydjzbjdcjkzkcugisdchjyjsbdfr

可看到flag值

题目10: 如来十三掌

题目描述: 菜狗为了打败菜猫, 学了一套如来十三掌。

解决:

下载后发现为一串看不懂的文字,网上搜索发现有一个"与佛论禅"的网站,应该可以解密

网站地址: 与佛论禅

开始直接粘贴进去,好像解不了..

太深輿了,参悟不出佛经的真意										
听佛说宇宙的真谛	参悟佛所言的真意		渡众生							
	人大善	謎, <u>善悲存乎</u> 尔心								
态 略来:普多苦奢欣客:译更	油咯虑稳修三位三即諸音	別更泇軍魏數萌耶泇麥芳吉住陀語怖麥恕係諸芳麥數	芭荟生造							
俱老竟寫明奢若梵等盧皤	豆蒙密離怯婆皤磯他哆提	略多缽以南哆心曰姪罰蒙呐神。舍切真怯勝呐得俱沙	周娑是怯!							
遠得吶數罰輸哆遠薩得槃	漫夢盧皤亦醯呐娑皤瑟輸	譜尼摩罰薩冥大倒參夢侄阿心罰等奢大度地冥殿皤沙	囌輸奢恐							
豆住得前提哆伽諸沙楞缽	三化怯摩大廝者数一處									

_ _ . .

之后尝试白话转"佛说"

发现格式要在前面加上佛曰:

MzkuM3gvMUAwnzuvn3cgozMLMTuvqzAenJchMUAeqzWenzEmLJW9
听佛说宇宙的真谛 参悟佛所言的真意 普度众生
不可说,不可说,一说即是错
佛曰: 夜哆悉諸多苦奢陀奢諾具神哆盧穆皤三任三即結語即冥迦冥隸數顛耶迦春若吉怯陀語怖春智侄諸若春數善 奢集遠俱老寬寫明春若梵等虛皤豆蒙密雜怯婆皤礙他哆提哆多缽以南哆心曰姪罰蒙呐神。舍切真怯勝呐得俱沙罰 娑是怯遠得呐數罰輔修遠薩得氣漫夢虛皤亦藝呐娑皤瑟輔語尼摩罰薩冥大倒參夢任阿心罰等希大度地冥殿瞻沙難 輔春恐豆侄得罰提哆伽語沙楞缽三死怯摩大蘇者數一遍

第一反应将其进行BASE64解密,但是解码失败,据题意,十三...ROT13编码。

将其先ROT13再加密一次即解密,之后再进行BASE64解码

得到flag值

flag{bdscjhbkzmnfrdhbvckijndskvbkjdsab}

BASE64解码网址: http://tool.oschina.net/encrypt?type=3

ROT13解码网址: https://www.jisuan.mobi/puzzm6z1B1HH6yXW.html

题目11: base64stego

题目描述:菜狗经过几天的学习,终于发现了如来十三掌最后一步的精髓

解决:

如来十三掌的最后一步,即BASE64解密,在压缩软件里打开这个文件

↑ 名称	文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
(上层目录)	U3R Z2Fub2dyYXBoeSBpcyB0aGUgYXJ0 GFuZCBzY2 bmN G9m 🧭
stego.txt	HdyaXRpbmcgaGlkZGVulG1lc3NhZ2VzlGlulHN1Y2ggYSB3YXkgd
	GhhdCBubyBvbmV= LCBhcGFydCBmcm9t1HRoZSBzZW5kZX1gYW5k1G1udGVuZGVk1HJ1Y 21waWVudCwgc3VzcGU= Y3Rz1HRoZSB1eG1zdGVuY2Ugb2YgdGh11G11c3M= YWd1LCBh1GZvcm0gb2Ygc2VjdXJpdHkgdGhyb3VnaCBvYnNjdXJpd Hku1FS= aGUgd29yZCBzdGVnYW5vZ3JhcGh51G1z1G9m1EdyZWVr1G9yaWdpb iBhbmQgbWVhbnMg1mNvbmN1YW== bGVk1HdyaXRpbmci1GZyb20gdGh11EdyZWVr1HdvcmRz1HN0ZWdhb m9z1G11YW5pbmcg1mNv dmVyZWQgb31gcHJvdGVjdGVk1iwgYW5k1GdyYXBoZW1u1G11YW5pb mcg1nRv1Hc= cm10ZS1u1FRoZSBmaXJzdCByZWNvcmR1ZCB1c2Ugb2YgdGh11HR1c m0gd2Fz1G1u1DE00TkgYnkgSm9o
<	GFødH.IIYV==

发现有很长的BASE64编码。

...查看writeup后,涉及到BASE64隐写

原理与题解参照一位大神博客: https://www.tr0y.wang/2017/06/14/Base64steg/

题目12: 功夫再高也怕菜刀

题目描述: 菜狗决定用菜刀和菜鸡决一死战

(查看了别人的writeup...)

将该文件拖到foremost应用程序上,用foremost分离文件中的隐藏文件,输出结果为一个压缩文件

打开发现解压需要密码

🕌 輸入密码 - 万能压缩 🛛 🗙 🗙
为加密的文件输入密码
flag.txt
🗌 显示密码 (勾选可支持中文密码输入)
── 將当前密码应用到所有加密文件
确定 跳过 86 跳过所有加密文件 0088

用wireshark打开该pcapng数据包,通过表达式搜索流量包中是否有flag

	🦲 Wireshark · 显示过滤器表达式				×			
ſ	字段名称		关系					
•	> HPEXT · HP Extended Local-Link Control	^	is present		^			
•	> HPFEEDS · HPFEEDS HoneyPot Feeds Protocol		==					
•	> HPSW · HP Switch Protocol		!=					
-	> HPTEAM · HP NIC Teaming Heartbeat		>					
•	> HSMS · High-speed SECS Message Service Protocol		<					
•	> HSR · High-availability Seamless Redundancy (IEC62439 Part 3 Ch		>=					
-	> HSR_PRP_SUPERVISION · HSR/PRP Supervision (IEC62439 Part 3)		<=					
	> HSRP · Cisco Hot Standby Router Protocol		contains					
	> HTTP · Hypertext Transfer Protocol		matches		~			
	> HTTP2 · HyperText Transfer Protocol 2		[. (P					
	> HyperSCSI · HyperSCSI							
	> I2C · Inter-Integrated Circuit		fiag					
	> IAP · Information Access Protocol		预定义的值					
	> IAPP · Inter-Access-Point Protocol							
	> IAX2 · Inter-Asterisk eXchange v2							
	> IB · InfiniBand							
	> iBeacon · Apple iBeacon							
	> iCall · iCall Communication Protocol	~	范围(偏移:长度)					
	搜索:							
	http contains flag							
	点击确定插入此过滤器							
			OK Cancel	Hel				
L			niip s://bto g.osdmnei/d.c	_40219	10083			

	htt	p contains flag					
ī	ło.	Time	Source	Destination	Protocol	Length	Info
		189 8.491449977	192.168.43.83	192.168.25.128	HTTP	474	HTTP/1.1 200 OK (text/html)
		195 8.586889274	192.168.43.83	192.168.25.128	HTTP	474	HTTP/1.1 200 OK (text/html)
		639 26.245426915	192.168.43.83	192.168.25.128	HTTP	475	HTTP/1.1 200 OK (text/html)
-	-	641 26.245821034	192.168.43.83	192.168.25.128	HTTP	475	HTTP/1.1 200 OK (text/html)
	1	1150 50.147576455	192.168.43.83	192.168.25.128	HTTP	515	HTTP/1.1 200 OK (text/html)
	1	1314 65.547155778	192.168.43.83	192.168.25.128	HTTP	515	HTTP/1.1 200 OK (text/html)
	1	1320 65.582424279	192.168.43.83	192.168.25.128	HTTP	515	HTTP/1.1 200 OK (text/html)
	1	1367 70.304861262	192.168.43.83	192.168.25.128	HTTP	524	HTTP/1.1 200 OK (text/html)

筛选出这些流量包,逐个右击选择跟踪TCP流,查看完整的数据流中数据包的信息 在第1150个包中发现巨长串十六进制编码,观察到结尾为FFD9,为jpg格式的文件结束标志 所以在前面的编码中寻找FFD8(jpg文件头标识)

aa=@eval.
(base64_decode(\$_POST[action]));&action=QGluaV9zZXQoImRpc3BsYX1fZXJyb3JzIiwiMCIpO0BzZXRfdGltZV9saW1pdCgwKTt
Ac2V0X21hZ21jX3F1b3R1c19ydW50aW11KDAp02VjaG8oIi0%2BfCIp0zskZj1iYXN1NjRfZGVjb2R1KCRfUE9TVFsiejEiXSk7JGM9JF9Q
T1NUWyJ6MiJd0yRjPXN0c19yZXBsYWN1KCJcciIsIiIsJGMp0yRjPXN0c19yZXBsYWN1KCJcbiIsIiIsJGMp0yRidWY9IiI7Zm9yKCRpPTA
7JGk8c3RybGVuKCRjKTskaSs9MikkYnVmLj11cmxkZWNvZGUoIiUiLnN1YnN0cigkYywkaSwyKSk7ZWNobyhAZndyaXR1KGZvcGVuKCRmLC
J3IiksJGJ1Zik%2FIjEi0iIwIik702VjaG8oInw8LSIp02RpZSgpOw%3D%3D&z1=RDpcd2FtcDY0XHd3d1x1cGxvYWRcNjY2Ni5qcGc%3D&
z2=FFD3FFE000104A46494600010101007800780000FFDB0043000101010101010101010101010101010101
01010101010101010101010101010101010101
10101010101010101010101010101010101010
C0001108013901E203012200021101031101FFC4001F00000105010101010101000000000000000
0B5100002010303020403050504040000017D01020300041105122131410613516107227114328191A1082342B1C11552D1F0243362
7282099011617181910252627282920334353637383930435464748494053545556575859566364656667686964737475767778797

将FFD8,FFD9之间的内容复制下来,保存在文本文件(txt)中

打开010Editor,选择导入十六进制文件

¥	编辑方		十六	进制(行脚	本 ~		行模	板~							
																		0123456789ABCDEF
0000		FF		FF				4A	46	49	46		01	01	01			ÿØÿàJFIFx
0010						FF			43			01						.xÿÛ.C
0020		01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
0030																		
0040		01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
0050											FF			43				ÿû.c
0060		01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
0070												01						
0080		01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	01	
0090		01										01	01	01	01	FF		ÿÀ
00A(11		01	39	01	E2	03	01	22			11	01	03	11	9.â"
00B(01	FF			1F						01	01	01	01	01		.ÿÄ
0000											03	04		06	07			
00D(FF									03		04			ÿÄ.μ
00E(04	04			01		01		03		04	11		12	21	
00F(31	41		13	51	61	07	22	71	14		81	91	A1		23	1AQa."q.2.`;.#
0100		42	в1	C1	15	52		FO	24	33	62	72	82			16	17	B±Á.RÑð\$3br,
011(18	19	1A			27		29	2A	34			37				%&'()*456789:
0120		43	44	45	46	47	48	49	4A	53	54		56	57			5A	CDEFGHIJSTUVWXYZ
0130		63	64			67			6A	73								cdefghijstuvwxyz
014(83	84	85	86	87		89	8A		93	94		96	97	98	99	f,†‡^‰Š′ ``″•~™
0150			A2	A3	A4	Α5	A6	A7	A 8	Α9	AA		в3	В4		в6	в7	𢣤¥¦S"©ª²³′µ¶∙
016(в8	в9	BA		C3	C4			C7			CA	D2		D4		, ¹ °ÂÃÄÅÆÇÈÉÊÒÓÔÕ
017(E1	E2	E3	E4	E.5		E7	E8	E9	EA	F1	ÖרÙÚáâãäåæçèéêñ
0180		F2	F3	F4	F5	F6	F7	F8	F9	FA	FF	C4		1F	01		03	j ∂óôõö httpsj/plog.csdn.net/qq_40490088

导入后,选择保存为jpg格式的文件。

查看该图片,看到图片中间有一串字符(理解为...This is password)



猜测为解压密码,尝试后,解压成功,得到一个flag.txt文件

☐ flag.txt - 记事本 文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H) f l ag {30pWdJ−JP6FzK−koCMAK−VkfWBq−75Un2z}