全网最详细攻防世界MISC新手区题

原创

yatkm ● 于 2020-11-01 21:45:30 发布 ● 733 ☆ 收藏 5 分类专栏: ctf_misc 文章标签: <u>信息安全</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/Yshshsj/article/details/109433565</u> 版权



ctf_misc 专栏收录该内容

1篇文章0订阅 订阅专栏

全网最详细攻防世界MISC新手区题

- this_is_flag
 pdf
 give_you_flag
 坚持60s
 gif
 掀桌子
 如来十三掌
 stegano
 SimpleRAR
 base64stego
 - 11. ext3
 - 12. 功夫再高也怕菜刀

1. this_is_flag



由一眼看出法得到令人心动不已的flag。

2. pdf

根据题目意思flag就在图片的后面,把**文件后缀**改成**doc**(也可以右键图片,在图片层级选项设置为至于底层),就可以获得 flag啦啦啦啦





3. give_you_flag

下载后发现是一张gif图,第50帧是二维码(我是用stegsolve一帧帧看的)。



奈何ps如此高深(我太菜了,还不会ps。。),没有办法只好打开电脑的**画图**工具来把这二维码缺失的三个定位符补上。不禁 感叹学信息安全还得学画画,唉。。。



扫码赢大奖啦~~

4. 坚持60s

jd-gui github下载:https://github.com/java-decompiler/jd-gui/releases/tag/v1.6.6

头顶上的青青草原,哈哈哈。看到这是一个java游戏,用jd-gui打开





查看了一下源代码可以发现flag(当然也可以使用搜索功能搜索flag)



5. gif

刚开始的时候看着这些黑白块,联想到了摩斯密码,但是好像不太可行。于是盲猜黑白块代表的是黑为1、白为0的二进制。



二进制在线转化字符串:http://www.txttool.com/WenBen_BinaryStr.asp

二进制转化字符串的结果就是梦寐以求的flag啦。

6. 掀桌子

掀桌子 Leftwriteup由flag{not_here} · 适适再提供	📘 WP 🚺 🔮 建议
难度系数: ●★★★★ 4.0	
题目来源: DDCTF2018	
题目描述: 菜狗截获了一份报文如下c8e9aca0c6f2e5f3e8c4efe7a1a0d4e8e5a0e6ece1e7a0e9f3baa0e8eafae3f9e 5e7e9f3e4e3e8eaf9eaf3e2e4e6f2, 生气地掀翻了桌子(╯°□°)╯⌒┻┻	4eafae2eae4e3eaebfaebe3f
题目场景:暂无	
题目附件: 暂无	https://blog.csdn.net/Yshshsj





7. 如来十三掌

夜哆悉諳多苦奢陀奢諦冥神哆盧穆皤三侄三即諸諳即冥迦冥隸數顛耶迦奢若吉怯陀 諳怖奢智侄諸若奢數苔奢集遠俱老竟寫明奢若梵等盧皤豆蒙密離怯婆皤礙他哆提哆 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**數罰輸哆遠薩得 槃漫夢盧皤亦醯**呐**娑皤瑟輸諳尼摩罰薩冥大倒參夢侄阿心罰等奢大度地冥殿皤沙蘇 輸奢恐豆侄得罰提哆伽諳沙楞缽三死怯摩大蘇者數一遮

https://blog.csdn.net/Yshshsj

看到这些可以联系到与佛论禅编码

在开头加上'佛曰: '然后'参悟佛所言的真意'

与佛论禅

MzkuM3gvMUAwnzuvn3cgozMlMTuvqzAenJchMUAeqzWenzEmLJW9	
听佛说宇宙的真谛 参悟佛所言的真意 悠然,随心,随性,随缘	普度众生
佛曰:夜哆悉諳多苦奢陀奢諦冥神哆盧穆皤三侄三即諸諳即冥迦冥隸數顛耶迦奢若吉怯陀譡 若奢數菩奢集遠俱老竟寫明奢若梵等盧皤豆蒙密離怯婆皤礙他哆提哆多缽以南哆心曰姪罰蒙 真怯勝呐得俱沙罰娑是怯遠得呐數罰輸哆遠薩得槃漫夢盧皤亦醯呐娑皤瑟輸諳尼摩罰薩冥大 心罰等奢大度地冥殿皤沙蘇輸奢恐豆侄得罰提哆伽諳沙楞缽三死怯摩大蘇者數一遮 musc/blog.c	i怖奢智侄諸 I呐神。舍切 I倒參夢侄阿 sdn.net∕Yshshs

得到一串编码后,突然想起题目是在暗示rot13加密方式(敲着base64的手突然就停了下来)

rot13	
ZmxhZ3tiZHNjamhia3ptbmZyZGhidmNraWpuZHNrdmJramRzYWJ9	
L Rot13 编码 Rot13 解码 接回 前切 ¥kw 清除	

解密完后发现还是一串编码,再次使用rot13解密,发现不行,于是转用base64(突然觉得base64又香了不少),没错就是它,它又来了。

请输入要进行 Base64 编码或解码的字符

ZmxhZ3tiZHNjan	nhia3ptbmZyZGhidi	mNraWpuZHNrdmJramRzY	W19	
				1
编码 (Encode)	解码 (Decode)	↓交换 (编码快捷键: c	trl + Enter)	
Base64 编码或解码的	的结果:			□编/解码后自动全选
flag{bdscjhbkzmr	nfrdhbvckijndskvbkj	dsab}		
				napasatagiaanintas Fariana

8. stegano

用火狐打开刚才下载pdf文件,控制台输入

document.documentElement.textContent

然后回车查看

polar bear during a snow storm 🗙 🕂				ø	
\leftarrow \rightarrow C \textcircled{a} \textcircled{v} \textcircled{v} \textcircled{v} file:///C:/Users/yatktm	/Downloads/d802bcf9530b45e0b37170c67b8efcea (1).pdf	··· ☆		5	≡
📄 火狐官方站点 💪 新手上路 📄 常用网址 ᠿ 京东双11 🚺 天猫双11]移ī	加设备上的	书签
	─ 十 自动缩放 ~		<u>p</u> 🖶	Cʻ 🛛	>>
					^
L Volu orci,	orem ipsum dolor sit amet, consectetur adipiscing elit. Cras faucibus odio ut r tpat. Integer nec enim vel arcu porttitor egestas. Vestibulum suscipit lorem sed convallis vitae auctor vehicula, interdum ut mi. Maccenas nec urna at dolo	metus vulputate, id laoreet magna l sem faucibus rutrum. Nunc diam r mattis dictum sit amet at orci.			~
□ ① 查看器 D 控制台 D 调试器 1↓ 网络 {} 样式编辑器 ① 性	第 ① 内存 3日 存储 🕆 无障碍环境 2部 应用程序 ● HackBar			Ŋ	۰×
		错误 警告 日志 信息	调试 CSS >	(HR 请求	☆
NoFlaghere! NoFlaghere! NoFlaghere!XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	t still not here IBABA 888 DA 8BA ABA AB B AAB A ipiscing alit. Cras faucibus odio ut metus vulpu hicula, intendam ut mi. Macenas nee urna er arcu. In facilisis et tortor commodo aliquam. disecto a statuto a statuto a statuto a statuto hogesta, tisique mauris qui pusto. Nu met, consectetur adipiscingelit. Cras fauris ci, convallis vitas auctor vehicula, intendum u buis aget ullamcorper arcu. In facilisis psum dolor sit amet, consectetur adipiscing elit. nu donor sector autor vehicula, intendum u tai. ullamcorper arcu. In facilisis et tortor commodo molor sit amet, consectetur adipiscing elit. un. Nunc diam orti, convullis vita auctor vehi adipiscing dui. Duis eget ullamcorper and seus sollicitudin a felis guis, blandit porta jor eu bibendum metusinterdum in.lorem ipsum dolor sit a, faculis adipiscing dui. Duis egetulamcorpes felis quis, blandit porta ipsum. done sed nibi metus interdum in.lorem ipsum dolor sit asopint lorems de sem faucibus rutrum. Nunc diam stopin verse de sem faucibus rutrum. Nunc diam sopue varius ligula, iaculis adipiscing dui. Duis subilicitudina felis quis. blandit porta ipsum.	AA AB B AA BBB tate, id laon at dolon mm Nulla feugia lla facilisi. us odio ut minimecenas t tortor com ue mauris eu, Cras faucibu maccenas nec u aliquom. Nul maccenas nec u aliquom. Nul utrum justo. . Cras fauci utrum justo. . consectes t amet, conse egestas, trist segt ullamco Donec sed nil	BA AAA eet ttis t, sem et Duis metus metus rna at la Nulla ibus m ut isis et nibh ctetur ehicula, ils vitae per arcu h	

发现一串特殊的编码:

看到有空格隔开,于是猜测摩斯密码 **'A'代替 '·', 'B'代替'--'** 只能一个个打(老工具人了),解密后得到flag。(ps:填flag的时候要注意格式喔)

摩斯密码转换网址: http://moersima.00cha.net/

输入摩尔斯电码,点击"解密",即可将摩尔斯电码翻译成可识别的字符。



congratulations,flag:1nv151bl3m3554g3 推荐:中文摩斯密码翻译>>

解密

9. SimpleRAR

把下载的文件解压后,发现只有一个flag.txt(很显然是假的),用 winhex 打开发现有一个 png 文件。

rar对png的文件类型编码是74,就在flag.txt文件结束,这里是7A,所以要把圈圈里的7A改过来喔,保存再次解压。

🚟 WinHex - [18c5326aada0499eafbe03ad8a52e40c.rar]

🏭 文件(F) 编辑(E) 排	遼索(S) 位置(P)	视图(V)	工具	(T)	专家(I) 选	项(O)	窗口	(W)	帮助(ŀ	H)	
🗅 🚅 🖶 🎒 😭 🕍 🖌) 🖹 📸 🖏 🖏 1012	MA HEX	B HEX	ģ	→ -Ð) 💠 =	⇒	2 🖣		🛯 🔎 🗌	in the second s	🕨 💼 🗌 🤣
2 noname 18c532	6aada0499eafbe0)3ad8a52	e40c	•								
18c5326aada0400aafbe03ad	offset	0 1	2 3	4	5 (5 7	8	9 A	В	C D	E F	· · · · ·
C:\Users\yatktm\Desktop\新建	🗙 00000000	52 61	72 21	1A	07 0	CF CF	90	73 00	00	OD 00	00 00) Rar!Ï.s
	00000010	00 00	00 00	D5	56 7	4 20	90	2D OO	10	00 00	00 10)ÕVt
File size: 5.4 k	B 00000020	00 00	00 02	C7	88 6	7 36	6D (BB 4E	4B	1D 30	08 00)Ç∎g6m≫NK.O
5,569 byte	^{is} 00000030	20 00	00 00	66	6C 6	1 67	2E	74 78	74	00 BO	57 00)flag.txt.°W.
DOS name: 18C532~1.RA	R 00000040	43 66	6C 61	67	20 6	973	20	6E 6F	74	20 68	65 72	2 Cflag is not her
D. (00000050	65 A8	30 7A	20	90 21	7 00	ЗA	15 00	00	42 16	00 00) e~ <z .∕.:b<="" th=""></z>
State: modifie	00000060	02 BC	E9 8	2F	6E 8-	4 4F	4B	1D 33	ΟA	00 20	00 00) .¼é∎∕n∎OK.3
in the second se	00000070	00 73	65 6	72	65 7	4 2E	70	6E 67	00	FO 40	AB 18	3 _ secret.png.ð@«.
Undo level:	0 00000080	11 C1	11 55	08	D1 5	5 80	OD	99 C4	90	87 93	22 1	.Á.U.ÑUL.LÄ.LL".
Chido reverses. Reyboard imp	00000090	4C 58	DA 18	Β1	A4 5	3 16	33	83 08	F 4	3A 18	42 OE	3 LXÚ.±¤X.3∎.ô:.B.
Creation time: 2020/10/3	0A000000 0	04 05	85 96	21	AB 1 <i>i</i>	43	08	66 EC	61	OF AO	10 21	l∎!≪.C.fìa!
21:15:4	2 000000B0	AB 3D	02 80	BO	10 9) C5	8D ,	A1 1E	84	42 <i>B</i> O	43 29	9 ≪=. I °Å.i. I B°C)
Last write time: 2020/11/0	00000000	08 10	DA OF	23	99 C	C F3	9D (C4 85	86	67 73	39 DE	EÚ.#IÌó.ÄIIgs9⊧
20:54:3	000000D0	47 63	91 DE	С4	77 EI) A8	DC	46 F4	C5	54 CD	55 6A	A Gc'ÞÁwi ÜFôÅTÍUj

用winhen打开png文件后发现其实是gif文件。

🚟 WinHex - [secret.png]

🎬 文件(F) 编	辑(E) 捜索	\$(S) 位置(P)	视图	룁(V)		[具(T)	专家	₹(I)	选	项(O)		§□((W)	帮	助(⊦	I)					
🗅 🖻 🖥 🎒 😭	🖄 🛛 🖂	🖹 🛍 🛅 1012	酋	HEX	вн	éx 🏘		-	-	(= =	♦	2	-	(m) [🖬 🖌		_√×	◀) 🚺 🔠	1		
2 noname	e secret.p	ng																				
secreting		Offset	0	1	2	3	4	- 5	6	7	8	- 9	Α	В	C	D	Е	F				
C:\Users\yatktm\De	esktop\新建文	00000000	47	49	46	38	39	61	18	01	18	01	91	02	00	FE	FF	FF	GIF89a.	*	• þÿÿ	
		00000010	FF	FF	FF	FF	$\mathbf{F}\mathbf{F}$	FF	00	00	00	21	FF	ΟB	58	4D	50	.0		!ÿ.>	ΩMP	
File size:	5.6 KB	00000020	44	61	74	61	58	4D	50	ЗC	ЗF	78	70	61	63	6B	د ۲	74	DataXMP	(?xpad	:ket	
	5,698 bytes	00000030	20	62	65	67	69	6E	ЗD	22	EF	BB	BF	22	20	65	64	ЗD	begin=	'ï≫ć"	id=	
Default Edit Mode		00000040	22	57	35	4D	30	4D	70	43	65	68	69	48	7 A	72	65	53	"W5M0Mp(lehiHz	zreS	
State:	original	00000050	7A	4E	54	63	7A	6B	63	39	64	22	ЗF	ЗE	20	ЗC	78	ЗA	zNTczkc?	}d"?>	<x:< td=""><td></td></x:<>	
Lindo lovol:	- 0	00000060	78	6D	70	6D	65	74	61	20	78	6D	6C	6E	73	ЗA	78	ЗD	xmpmeta	xmlns	s:x=	
Undo reverses:	n/a	00000070	22	61	64	6F	62	65	ЗA	6E	73	ЗA	6D	65	74	61	2F	22	"adobe:	is:met	ta∕"	
		00000080	20	78	ЗA	78	6D	70	74	6B	ЗD	22	41	64	6F	62	65	20	x:xmptl	s="Ado	be	
Creation time:	2020/11/01	00000090	58	4D	50	20	43	6F	72	65	20	35	2E	33	2D	63	30	31	XMP Core	: 5.3-	-c01	
	20:54:33	000000A0	31	20	36	36	2E	31	34	35	36	36	31	2C	20	32	30	31	1 66.145	5661 ,	201	

修改了后缀后,按照题目意思把图层给分离出来(用的是ps,还特地下载了个ps学了一下),再用stegsolve查看



把二维码拼起来,然后再把定位符补上就扫描就可以获取flag啦(都快把我整图吐了。。)



< >

10. base64stego



用脚本跑一下,也很轻松得到flag了(前几天的比赛中也遇到了这样的隐写题(base64加密了49次。。))

11. ext3

把下载好的文件,拷贝一份到kali中,挂载到系统上。mount命令用于加载文件系统到指定的加载点。此命令的最常用于挂载 cdrom,使我们可以访问cdrom中的数据。



root@kali:~/桌面

执行完命令后,可以直接访问然后获取flag(要把密文用base64解密)

◎◎文件(F) 动作(A) 编辑(E) 查看(V) 帮助(H)	
root@kali:~/桌面# file f1fc23f5c743425d9e0073887c846d23 f1fc23f5c743425d9e0073887c846d23: Linux rev 1.0 ext3 filesystem data, UUID= cf6d7bff-c377-403f-84ae-956ce3c99aaa root@kali:~/桌面# strings f1fc23f5c743425d9e0073887c846d23 grep flag	
.flag.txt.swp Flag.txtt.swx	
~root/Desktop/file/07avZhikgKgbF/flag.txt 1 访问	
flag.txtt.swx	
Flag. tytt. swy	
/root/果面/temp/O7avZh kgKgbF/flag.txt - Mousepad _ C ×	
文件(F) 编辑(E) 搜索(S) 视图(V) 文档(D) 帮助(H) 数年、你工在使用 $$ 地内 特化工作合相定物的石体	
警告:您止仕使用「COP」账户,操作个当可能会损害您的系统。	
2 获取flag	
https://blog.csdp.pet/Yshshsi	
nupa.//biog.coun.ne/ rananaj	
	_
ZmxhZ3tzYWpiY2lienNrampjbmJoc2J2Y2pianN6Y3N6Ymt6an0=	
编码 (Encode) 解码 (Decode) ↓ 交换 (编码快捷键: Ctrl + Enter)	
Base64 编码或解码的结果:	
flag{sajbcibzskjjcnbhsbvcjbjszcszbkzj} https://blog.osdn.pet/Ys	
mponorogioannior e	
啊,终于又写完一题,看到每一个flag呼之欲出,就会不禁的开心。	

12. 功夫再高也怕菜刀

下载附件,用foremost进行pcapng文件的分离,得到一个zip,打开zip,得到一份加密的flag.txt文件。然后用wireshark打开 pcapng文件,查找flag.txt关键字,

▲ acfff53ce3fa4e2bbe8654284dfc18e1.pcapng 文件(£) 編攝(£) 視圏(M) 競转(5) 捕获(C) 分析(A) 統计(S) 电话(M) 无线(W) 工具(I) 帮助(H)	o	×
文件(E) 编辑(E) 视图(M) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(M) 无线(M) 工具(D) 帮助(H)		
🚄 🧮 🔬 💿 🖡 🖄 🖄 🔍 🗣 🍁 🖀 🖡 💆 📰 🔍 🔍 🏛		
■ 应用显示过滤器 … <ctrl-></ctrl->		1 •
分组字节法 > 宽存 >> □ 区分大小写 字符串 >> flag 查找	取注	肖
No. Time Source Destination Protocol Length Info		1
1143 49.897215668 192.168.25.128 219.216.128.25 TCP 54 58432 → 80 [ACK] Seq=145 Ack=176641 Win=65535 Len=0		
1144 50.098716397 192.168.43.83 192.168.25.128 HTTP 300 HTTP/1.1 200 OK (text/html)		

1145 50.098792302 192.168.25.128 192.168.43.83 1146 50.134447510 192.168.25.128 192.168.43.83	TCP 54 478 TCP 290 478	56 → 80 [ACK] Seq=205239 Ack=247 Win=30016 Len=0 56 → 80 [PSH, ACK] Seq=205239 Ack=247 Win=30016 Len=236 [TCP segment of a reassem	mbled PDU]
1147 50.138633287 192.168.43.83 192.168.25.128	1CP 60.80	→ 4/856 [ACK] Seq=24/ ACK=2054/5 Win=64240 Len=0	
1148 50.138903657 192.168.25.128 192.168.43.83 1140 50 140816842 102 168 42 82 102 168 25 128	HTTP ///PU:	/ /upload/l.pnp Hilp/l.l (application/x-www-torm-urlencoded)	
1149 50.140816842 192.168.45.85 192.168.25.128		→ 47856 [ACK] Seq=247 ACK=206198 Win=64240 Len=0	
1150 0.147576455 192.168.43.83 192.168.25.128	HIIP 515 HI	P/1.1 200 0K (text/ntml)	v
	110 5447		>
[Prev response in frame: 1144]			^
[Request in frame: 1948]			
[Request URI: http://192.168.43.83/upload/1.php]			
File Data: 221 bytes			
Line-based text data: text/html (7 lines)			
-> ./\t2017-12-08 11:42:11\t0\t0777\n			
/\t2017-12-08 11:39:10\t4096\t0777\n			
1.php\t2017-12-08 11:33:16\t33\t0666\n			
6666.jpg\t2017-12-08 11:42:11\t102226\t0666\n			
flag.txt\t2017-12-08 11:35:29\t17\t0666\n			
h-11i-1+2047 42 00 00-22-201+224)+00001-			~
0130 2d 31 32 2d 30 38 20 31 31 3a 34 32 3a 31 31 09	-12-08 1 1:42:11		^
0140 30 09 30 37 37 37 0a 2e 2e 2f 09 32 30 31 37 2d	0 0777/ 2017-		
0150 31 32 2d 30 38 20 31 31 3a 33 39 3a 31 30 09 34	12-08 11 :39:10 4		
0100 30 39 30 09 30 37 37 37 0a 31 22 70 68 70 09 32	096-0777 -1.pnp-2		
01/0 50 51 57 20 51 52 20 50 50 20 51 51 53 55 53 0180 31 36 00 33 33 00 30 36 36 36 36 00 36 36 36 36 36 20	16.33.06 66.6666		
0190 6a 70 67 09 32 30 31 37 2d 31 32 2d 30 38 20 31	ing 2017 -12-08 1		
01a0 31 3a 34 32 3a 31 31 09 31 30 32 32 32 36 09 30	1:42:11 102226 0		
01b0 36 36 36 0a 66 6c 61 67 2e 74 78 74 09 32 30 31	666.flag .txt.201		
01c0 37 2d 31 32 2d 30 38 20 31 31 3a 33 35 3a 32 39	7-12-08 11:55-29		
01d0 09 31 37 09 30 36 36 36 0a 68 65 6c 6c 6f 2e 7a	·17·0666 ·hello.z		
01e0 69 70 09 32 30 31 37 2d 31 32 2d 30 38 20 30 39	ip 2017- 12-08 09		
01f0 3a 33 32 3a 33 36 09 32 32 34 09 30 36 36 36 0a	:32:36 2 24 0666		
0200 7c 3c 2d	<-		~
- ● Z 字节 436-472: Text item (text)		│ 分组: 2139 · 已显示: 2139 (100.0%)	配置: Default

发现有个6666.jpg,右键第1150个数据包,追踪TCP流,复制从FFD8开始到FFD9的内容,到winHex里新建文件粘贴,注意粘贴格式是ASCIIHex。



BEFAC1FCAB3EE7ADFF00FD7083F9C75D0FDD83B74D7D6DCDE565FC3EDBB5FC91B73D2F7A4BCF937D6DCFEC97CECAADB5DD295FE393322E24C6C1183925 BECCAC4F5E7CDBC9BD48DADB41C018E32139C694801447F38DCDE486FF0096F3747B997B08D3076EEF61D9C56A5DFDFB8FFB0745FF00B4EB1E6EABFF00 60E7FE42BCCAD75A76F2B6B74AE97CB4E8BDD4EE9352F630E95A3E76FC545FFEDDD2DBCDAB392E4CD99B0A31FBD05FE4CF2D79723EF48D93930C648EBC 608CE0935893BE771399079983839FB4DD374553FF003CA33D80E79EEC00D49BEF41FF005E32FF0027ACA3D6D3FEB85CFF00296BC6ACF5F9A5F7FB3FFE

4FE6959FC53E6F770E	96AFB5FCB6	E67D366DC3A689B6D2D236C8BA9000DB89705BE798CE679C1E96043EE3CE3EA5BA7191EC158B70E4	1F98643BB0409D9
71F3B7FCB2B58FØ385	5C7CDB4103	9FEEA83A72FDFB3FF7DFFF0066AC83D2D3FEBEA4FF00D0C578F8896CBBC53FBD53767DFF0089D775	5CDFCEEDEEE192B
FA36BE69DAFE5FØE96	DBDDB69046	5CEF8326FE08C7DA197A20E365B47D831C00DE9DF201CE3DCB677866DADB71291FF2C61E8B02FABE	3F1B8638DD83CEE
009F780F1B467A4926	E00FF176E0	B3118731C7CD8D876128A738B780F2646FFA6B2678C1E49E30480356EFEEDCFF00D7D27F37ACAD47	7A5FF00FBF07F23
5E3577A7AB7F85FF00	1F7775B377	56B452F6B0DAB827BC9C75F5F651DB6D39FEE56FB526F0EE1CB30D9F28018C00E3F751F57B8931FF	002D1B191E99E3
2319C999F681B7A90C	6156C60609	DD73276E31F2E7B8183F2F37EE7EFDCFFD7383F9C758F77D65FF00AF78FF00F408EBC6C4DD4ADE4F	5F4EDBD97BBA2E
FE9E65DA5FF81BFF00	2F5FE96BFF	D9HTTP/1.1 200 OK	-rcos/s/rssrbre
Date: Fri, 08 Dec	2017 11:42	07 GMT	
Server: Apache/2.4	.23 (Win64	PHP/5.6.25	
Content-Length: 7	5.0.25		
Keep-Alive: timeou	t=5, max=1	00	
Connection: Keep-A	live		
Content-Type: text	/html; cha	irset=TF-8	
-> 1 <-POST /uploa	d/1.php HT	TP/1.1	
User-Agent: Java/1	.8.0_151		
Host: 192.168.43.8	3 image/gif	$im_{2}\sigma_{2}/im_{2}\sigma_{3}$	
Connection: keep-a	live	, 1mdgc/ JAcg, , 4-,2, / , 4-,2	
Content-type: appl	ication/x-	www-form-urlencoded	
Content-Length: 72	3		
aa=@eval.			
(base64_decode(\$_P	OST[action]));&action=QGuaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCIpO0BzZXRfdGltZV9saW1pdCgwKTtA	Ac2V0X21hZ2ljX3
F1b3R1c19ydW50aW11	KDAp02VjaG	80Ii0%2BfCIpOzskRD1iYXNlNjRfZGVjb2RlKCRfUE9TVFsiejEiXSk7JEY9QG9wZW5kaXIoJEQpO2lm	nKCRGPT10VUxMKX
RikpevROPSRELiIvIi	4kTiskVD1A	ZGF0ZSgiWS1tLW0gSDppOnMiLEBmaWxlbXRpbWUoJFApKTtAJEU9c3Vic3RvKGJhc2VfY29udmVvdCh4	AZmlsZXBlcm1zKC
RQKSwxMCw4KSwtNCk7	JFI9Ilx0Ii	4kVC4iXHQiLkBmaWxlc2l6ZSgkUCkuIlx0Ii4kRS4iCiI7aWYoQGlzX2RpcigkUCkpJE0uPSROLiIvIi	i4kUjtlbHNlICRM
Lj0kTi4kUjt9ZWNoby	AkTS4kTDtA	Y2xvc2VkaXIoJEYpO307ZWNobygifDwtIik7ZGllKCk7&z1=RDpcd2FtcDY0XHd3d1x1cGxvYWRcHTTF	P/1.1 200 OK
Server: Apache/2.4	2017 11:42 .23 (Win64) PHP/5.6.25	
X-Powered-Rv: PHP/	5.6.25	,	~
分组 1144。53 客户端 分组,2 №	【务 <i>器 分组,3 tu</i> r.	n(s). 点面选择。	\+
整个对话(206 kB)		显示和保存数据为 ASCII ◇	流 7 🖵
			▲ → 21:30
			ost/Molo g ics <u>26209</u> 47,shsh sj ~
🚟 WinHex - [noname]			
🎬 WinHex - [noname] 🎆 文件(F) 编辑(E) 搜索	š(S) 位置(P)	视图(V) 工具(T) 专家(I) 选项(O) 窗口(W) 帮助(H)	
 ※ WinHex - [noname] ※ 文件(F) 编辑(E) 搜索 □ ☞ ■ 를 압 當 │ ∽ ■ 	(S) 位置(P) 會 臨 臨 000	视图(V) 工具(T) 专家(I) 选项(O) 窗口(W) 帮助(H) 桷 歳 翁 篆 桷 │ → 관 神 ⇒ │ ② 局 ※ ■ ♀ │ 岱 ◀ ▶ 四 国 │ ◆	
 WinHex - [noname] 文件(F) 编辑(E) 搜索 □ ☞ ■ 叠 督 營 ∞ □ 2 noname secret.pu 	t(S) 位置(P) 電 電 陆 1017 Ing noname	视图(V) 工具(T) 专家(I) 选项(O) 窗口(W) 帮助(H)	
 WinHex - [noname] 文件(F) 编辑(E) 搜索 □ ☞ 目 叠 @ ☞ □ 2 noname secret.pi noname 	(S) 位置(P) 電 電 いい ng noname Offset 0000000	视图(V) 工具(T) 专家(I) 选项(O) 窗口(W) 帮助(H) A 急 導 氯 A → ① 字 ⇒ ◎ 雪 ♀ ◎ 酚 ♀ ◎ 酚 ↓ ◎ 聞 ● ● 0 1 2 3 4 5 6 7 8 9 A B C D E F ■ D B FF E0 00 10 4A 46 49 46 00 01 01 00 78 ¹ / ₉ 0 ¹ / ₂ , JFIFx	
WinHex - [noname] 文件(F) 编辑(E) 搜索 D 译 - 母 留 读 中 日 2 noname c:Usersyatktm/Desktop	(S) 位置(P) 管 陸 いっついの offset 00000000 00000000	视图(V) 工具(T) 专家(I) 选项(O) 窗口(W) 帮助(H)	
WinHex - [noname] 文件(F) 编辑(E) 搜索 □ ▷ □ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	(S) 位置(P) 合 語 哈 ※ ng noname Offset 0000000 0000000 0000000 00000000	视图(V) 工具(T) 专家(I) 选项(O) 窗口(W) 帮助(H) → 熱 急 気 級 ▲ → ① 中 ⇒ ○ □ ○ □ ○ □ ○ □ ○ □ ○ □ ○ □ ○ □ ○ □ ○	
WinHex - [noname] 文件(F) 编辑(E) 搜索 □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	(S) 位置(P) 値 函 ※ noname Offset 0000000 00000010 00000010 00000020 00000000	视图(V) 工具(T) 专家(I) 选项(O) 窗口(W) 帮助(H) A 急 協 絵 A → ① 中 → ② 号 ◇ 回 ♀ │ 益 ↓ ▷ 图 │ ◆ 0 1 2 3 4 5 6 7 8 9 A B C D E F F D8 FF E0 00 10 4A 46 49 46 00 01 01 01 00 78 9 / ジジネJFIFx 10 10 10 10 10 10 10 10 10 10 10 10 10 1	
WinHex - [noname] 文件(F) 编辑(E) 搜索 2 noname secret. proname C:UsersiyatitimDesktop File size: 0.6 MB 614,054 bytes Default Edit Mode state: original	 (S) 位置(P) 回 四 時、 回 nonane Offset O0000000 	视图(V) 工具(T) 专家(I) 选项(O) 窗口(W) 帮助(H)	
WinHex - [noname] 文件(F) 编辑(E) 搜索 文件(F) 编辑(E) 搜索 ① ② □ ◎ ◎ ◎ ◎ ◎	(S) 位置(P) (3) (つうか) (3) (つうか) (1) (つうか) (1) (つうか) (2) (つ) (つ) (2) (0) (0) (0) (0) (0) (0) (0) (0) (0) (0	视图(V) 工具(T) 专家(I) 选项(O) 窗口(W) 帮助(H) (A) 急 輸 公 (A)	
WinHex - [noname] 文件(F) 编辑(E) 搜索 ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○	(S) 位置(P) (空) (空) (空) (空) (空) (空) (空) (空) (空)		
WinHex - [noname] 文件(F) 编辑(E) 搜索 ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○	(S) 位置(P) 國 四 ※ ng nonane 0ffset 0000000 0000000 0000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 000000000 00000000 00000000 000000000 00000000 00000000 000000000 00000000 00000000 000000000 00000000 00000000	祝图(V) 工具(T) 专家(I) 选项(O) 窗口(W) 帮助(H) 講 会 論 → ① 中 → ② 中 → ③ 中 ◇ □ ◇ □ ◇ □ ◇ □ ◇ □ ◇ □ ◇ □ ◇ □ ◇ □ ◇	
WinHex - [noname] 文件(F) 编辑(E) 搜索 ○ ○ ○ ○ ○ ○ 2 noname secret.pp noname C:UsersiyatitmDesktop File size: 0.6 MB 614,054 bytes Default Edit Mode State: 01ginal Undo level: 0 Undo level: 0 Creation time: 2020/11/01 16:48:24 Last write time: 2020/11/01	(S) 位置(P) 國 四 ※ ng nonane 0ffset 00000000 0000000 0000000 00000000 0000000 0000000 00000000 0000000 0000000 00000000 0000000 0000000 00000000 0000000 0000000 00000000 00000000 00000000 00000000 00000000 00000000 000000000 00000000 00000000 000000000 00000000 00000000 000000000 00000000 00000000		
WinHex - [noname] 文件(F) 编辑(E) 搜索 ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○	(S) 位置(P) 通 通 協 ※ nonane Offset 0000000 0000000 0000000 0000000 00000000 0000000 00000000 0000000 00000000 0000000 00000000 0000000 00000000 0000000 00000000 0000000 00000000 0000000 00000000 00000000 00000000 00000000 00000000 00000000 000000000 00000000 000000000 00000000 00000000 00000000		
WinHex - [noname] 文件(F) 编辑(E) 投索 ロ ジー ジ ジ ジ ジ ジ 2 noname 2 noname CiUsersyatktmiDesktop File size: 0.6 MB 614,054 bytes Default Edit Mode Oundo reverses: 0 Undo level: 0 Undo level: 0 Creation time: 2020/11/01 16:48:24 Last write time: 2020/11/01 16:48:24 Attributes: A	(S) 位置(P) (合 (G) (C) (C) (C) (C) (C) (C) (C) (C) (C) (C		
WinHex - [noname] 文件(F) 编辑(E) 投索 ロ ジー ④ 谷 谷 ど い 回 2 noname C:UserstyatktmiDesktop File size: 0.6 MB 614,054 bytes Default Edit Mode State: 0.101 Undo level: 0 Undo level: 0 Undo level: 0 Creation time: 2020/11/01 16:48:24 Last write time: 2020/11/01 16:48:24 Attributes: A Icons: 0 Mode: hexadecimal	(S) 位置(P) (第 略 彩) (可有にないのののののののののののののののののののののののののののののののののののの		
WinHex - [noname] 文件(F) 编辑(E) 搜索 ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○	(S) 位置(P) (第 1% 1%) (1) (1) (1) (1) (2) (1) (1) (2)	umal(v) $I=q(T)$ $e=s(I)$ $b=u(O)$ $a=1(W)$ $a=b(H)$ m $a=s$ $a=b$	
WinHex - [noname] 文件(F) 编辑(E) 搜索 ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○	(S) 位置(P) 國 四 ※ ng nonane 0ffset 0000000 000000 000000 0000000 0000000 0000000 00000000 0000000 0000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 000000000 00000000 00000000 000000000 00000000 00000000 000000000 00000000 00000000 000000000 00000000 00000000 000000000 00000000 00000000 000000000000000000000000000000000000	WB(V) I=(1) $\xi = \langle x \rangle$	
WinHex - [noname] 文件(F) 編辑(E) 授家 文件(F) 編辑(E) 授家 マー マー	(S) 位置(P) 回 四 ※ ng nonane 0ffset 00000000 000000 000000 00000000 0000000 0000000 00000000 0000000 0000000 00000000 0000000 0000000 00000000 00000000 0000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 000000000 00000000 00000000 000000000 00000000 00000000 0000000000 00000000 00000000 0000000000000 00000000 00000000 000000000000000000000000000000000000	$WB(V)$ $I=\{1\}$ $E = \{1\}$ $E = \{2\}$	
WinHex - [noname] 文件(F) 编辑(E) 搜索 ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○	(S) 位置(P) 回 四 100 ng nonane 0000000 00000000 0000000 0000000 00000000 0000000 0000000 00000000 0000000 0000000 00000000 00000000 0000000 00000000 00000000 0000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 000000000 00000000 00000000 000000000 00000000 00000000 000000000 00000000 00000000 000000000 00000000 00000000 000000000 00000000 00000000 0000000000 00000000 00000000 0000000000 00000000 00000000 0000000000000 000000000 00000000 000000000000000000000000 000000000000000000000000000000000000	WB(V) $T=Q(T)$ $E=(V)$ $E=(V)$ $R=U(V)$	
WinHex - [noname] 文件(F) 编辑(E) 搜索 文件(F) 编辑(E) 搜索 ○ ○ ○ ○ ○ ○ ○ ○ ○ 2 noname 2 noname 2 noname 3 or bar bar bar bar bar bar bar bar bar ba	(S) (ひ音(P)) (回) (回) (回) 0000000 0000000 0000000 0000000 00000000 0000000 00000000 0000000 00000000 0000000 00000000 0000000 00000000 0000000 00000000 0000000 00000000 0000000 00000000 0000000 00000000 0000000 00000000 0000000 00000000 0000000 00000000 0000000 00000000 0000000 00000000 0000000 000000000 00000000 000000000 00000000 00000000000 00000000 00000000000000 000000000 000000000000000000000000000000000000	$WB(V)$ I =(I) $\Theta = (I)$ $B = (I)$ $A = (I)$	
WinHex - [noname] マ件(F) 编辑(E) 搜索 ロマーク ロマーク ロの面池 Secret.pr noname C:UsersyatktmDesktop File size: 0.6 MB 614,054 bytes Default Edit Mode State: 0.6 MB 614,054 bytes Creation time: 2020/11/01 16:48:24 Last write time: 2020/11/01 16:48:24 Last write time: 2020/11/01 16:48:24 Attributes: A decimal Offsets: hexadecimal Bytage: 46x16=736 Window #: 2 No. of windows: 4 Clipboard: 99.8 KB TEMP folder: 141 GB free ersiyatktm\AppData\Local\Temp	(S) 位置(P) (G) ゆうかい (G) ゆうかい (F)	$WB(V)$ $I=q(1)$ $\Theta = (1)$ $B = [(W)$ $B = (1)$ $A = (1)$	
Image: Second	(S) 位置(P) (G) (つ) (C) (C) (C) (C) (C) (C) (C) (C) (C) (C	WB(V) Image: Image	
WinHex - [noname] 文件(F) 編編(E) 投索 ロ マースのの面で 2 noname 2 noname C:Userslyatktm/Desktop File size: 0.6 MB 614,054 bytes Default Edit Mode State: 0 iginal Undo level: 0 Undo level: 0 Undo reverses: 0 Creation time: 2020/11/01 16:48:24 Attributes: A Corons: 0 Mode: hexadecimal Ansol Axis=r36 Window #: 2 No. of windows: 4 Clipboard: 99.8 KB TEMP folder: 141 GB free erslyatktm/AppDatal_ocal/Temp	(S) 位置(P) (G) 位置(P) (G)		
WinHex - [noname] 文件(F) 編集(E) 技家 口 のの和限 secret.pl 2 noname secret.pl C:UserslyatktmDesktop File size: 0.6 MB Elie size: 0.6 MB Oldo level: 0 Undo level: 0 Undo level: 0 Creation time: 2020/11/01 16:48:24 16:48:24 Attributes: A Cons: 0 Mode: hexadecimal Character set: ANSIASCI Offsets: hexadecimal Modow #: 2 No. of windows: 4 Clipboard: 99.8 KB TEMP folder: 141 GB free erslyatktmVAppDataUcoal/Temp 141 GB	(S) 位置(P) (G) 位置(P) (G)		
Image: Second	(S) 位置(P) 国 内の 0000000 000000 0000000 000000 0000000 000000 0000000 0000000 0000000 0000000 00000000 0000000 00000000 0000000 00000000 0000000 00000000 0000000 00000000 0000000 00000000 0000000 00000000 0000000 00000000 0000000 000000000 00000000 000000000 00000000 00000000000 00000000 0000000000000 000000000 000000000000000000000000000000000000	UBB(V) I.P.(1) $\overline{\phi}$ as (1) $\overline{bar}(0)$ $\overline{bar}(1)$ $\overline{car}(1)$	
WinHex - [noname] 文件(F) 編年(F) 援索 口 小口 小口 授索 2 noname secret.pi 1 1 1 1 2 noname secret.pi 1 16:4054 bytes Default Edit Mode original Undo level: 0 1 16:48:24 Last write time: 2020/11/01 16:48:24 16:48:24 Attributes: A Icons: 0 Mode: hexadecimal Nex decimal bytes per page: 46x16=736 Window#: 2 Vindow#: 2 4 Clipboard: 99.8 kB TEMP folder: 141 GB free ersiyatkimkkppDataLocal/Temp 141 GB free	(S) (ひ音(P)) (回) (回) (1) (1) (1) </th <th>Umber No. Teq.(1) $\overline{\phi}$ as (1) $\overline{\phi}$ as (2) $\overline{\phi}$ as (2)</th> <th></th>	Umber No. Teq.(1) $\overline{\phi}$ as (1) $\overline{\phi}$ as (2)	
WinHex - [noname] 文件(F) 编辑(E) 搜索 口 口 口 口 口 口 口 口 口 口 口 口 口 口 口 口 口 口 口	(S) (ひ音(P)) (1) (1) 0000000 0000000 00000000 0000000 00000000 0000000 00000000 0000000 00000000 0000000 00000000 0000000 00000000 0000000 00000000 0000000 00000000 0000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 000000000 00000000 00000000 00000000 000000000 00000000 000000000 00000000 000000000000000000 000000000000000000000000000000000000	UBB(V) Image (V)	
WinHex - [noname] 文件(F) 编辑(E) 搜索 口 ご 口 の口加座 2 noname C:UJserslyatktmDesktop File size: 0.6 MB 614,054 bytes Default Edit Mode State: original Undo level: 0 16:48:24 Last write time: 2020/11/01 16:48:24 Attributes: A Character set: ANSIASCII Offsets: hexadecimal Byte per page: 46x16-736 Windows: 4 Clipboard: 99.8 KB TEMP folder: 141 GB free erslyatktmXAppDataU.ocallTemp	(S) (ひ音(P)) (a) (b) (c) 0100000 000000 0000000 000000 0000000 0000000 0000000 0000000 00000000 0000000 00000000 0000000 00000000 0000000 00000000 0000000 00000000 0000000 00000000 0000000 00000000 0000000 00000000 0000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 000000000 00000000 000000000 00000000 00000000000 00000000 0000000000000000000 000000000000000000000000000000000000	UB(V) I=(1) $5 \times (1)$ $2 \times (1) \times (2)$ $2 \times (2) \times (2) \times (2)$ $2 \times (2) \times (2) \times (2) \times (2)$ $2 \times (2) \times (2) \times (2) \times (2) \times (2)$ $2 \times (2) \times (2)$	

保存为jpg格式,可以得到图片,即是flag.txt的密钥,打开flag.txt即可获得flag。



https://blog.csdn.net/Yshshsj