




攻防世界 Misc高手进阶区 2分题 Reverse-it

原创

思源湖的鱼  于 2020-10-30 19:48:51 发布  359  收藏

分类专栏: [ctf](#) 文章标签: [网络安全](#) [ctf](#) [攻防世界](#) [misc](#)

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/weixin_44604541/article/details/109390872

版权

CTF

[ctf 专栏收录该内容](#)

200 篇文章 23 订阅

订阅专栏

前言

继续ctf的旅程

攻防世界Misc高手进阶区的2分题

本篇是Reverse-it的writeup

发现攻防世界的题目分数是动态的

就仅以做题时的分数为准了

解题过程

下下来一串乱码

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

?p
国用rc("揭?詛? ~ 疼?1V{Z薔辉箏 # m6?噪?-Xr?:狭□□QG 輕□□閑捲?7v乘□??徹堰膏D?鵠? ~ &紮&□ -佻
孳□□醅17.□□eD l]?! 測鳴隨Mq(nM泓屬攘礮i+@?擲
桐M5闕邢A宝窄幼?□ [e?□]僅?哺k)J^訛□U拮 ?R`k|≤□ J痠{7 越N_?窘Z钏S曷n?惋?□□8湾□受.璈??]m? 氩?橡|
? 回 ?▲暨嚙莪溲.□匪 描f板□=?儻7郝袂布箭璫???鴿泡?'?达砾焯□蒸=k▲璈敦探D消碑_騷?抚□錠?除□?`□J鳩
s□獵 詞5□b襪□q□7@樞#8勳h?M?□台瘕橢鬘?忻??□M 稟孤{y?_GE□#?鵠故钟贛籬0娒?□N繆@踢□鸛鹑Eu|
碗糶椎?蕞5y 9韶醞@%C拊迟S鈉of M8?□京g鶯OS)阡□□?Y妨6板□=) |换? 椅□沂^o%S撵忒gc孺
琉挝+

&F蓀□h後底 x?徑\$L悬 ?w嫖^爆□鍛"佛"炊捺□

□?OO綉後筭薇T鄧S燻

□K琪 □描撒賈E筊]狗縐f0幙?□膊46&*驛迢渲薯 鱗烱灼□餒K??J} ? ^?棘劲`□@2?ふ.YWQ?py□鉞割F顛遺?緹
掣k[E?洩??□ 滄鉞?□ ?? □0□ □0? ?? @ ?{|||||||||||||||||||||||||||||||||||||||(莊竟膾揆己剔□4 ?
UWU任縛勛\$Eo5??15)%?□%n□?□□□□□□□□□□ 魏淦錡滌?預?垣?磨?穿?蠢碣ふ ?故?蚪攤?劫凱?t摺Stod簪
? l ? { + ? ? ? J ? ? ? Y ? h □ ? w ' ? ? ? 6 ? ? ? E ? ? ? T □ ? s # ? ? ? 2 ? ? ? A ? ? ? P @ g'W6 E%4 v? ?
B 段? X{ ? ? ? 0 _ ? *? ? ? 告a□ □□? ?

? □ @

□ □ 0 □

0 #□?C?□ ##?□□□#d □F?V □噠G?噠□ T芴諺鑿7□ ? □ ?

□ @ 杓? A #□' ? □ □ □ 0?? □ P?& □ P? □ □ 0!op € ?裁 f构T- ??□□□ d摠? □

https://blog.csdn.net/weixin_44604541

扔进winhex看看

00000000	9D FF 70 0D B6 DA FC 93 72 63 28 22 22 BD D2 18	ÿp ůü"rc("";ò
00000016	B4 25 D4 7B 8C 00 A1 AB 60 9E E7 07 BB 04 31 56	‘%ô{G i«`žç » 1V
00000032	7B 5A D6 84 BB D4 B9 7E 00 A0 AB 6D 36 CD 31 C9	{ZÖ„»ô¹~ «m6ílÉ
00000048	A4 D1 01 2D 58 72 A9 B5 3A CF C1 04 1B 51 47 00	¤Ñ -Xr@µ:İÁ QG
00007664	A2 00 D4 D4 00 00 66 96 87 54 2D 00 1E FF 00 00	ø ôô f-+T- ŷ
00007680	84 00 84 00 10 10 10 00 64 94 64 A4 01 00 0E FF	„ „ d”d¤ ŷ
00007696	8D FF	ÿ

可以看到开头结尾分别是9DFF70和FF8DFF

查了查

jpg文件文件头和文件尾分别是FFD8FF和FFD9

所以这是个jpg文件的倒序

将十六进制复制

用python反序

再在winhex里建立新文件并保存

得到图片

SECCON{6in_tex7}

https://blog.csdn.net/weixin_44604541

翻转写到flag

SECCON{6in_tex7}

结语

知识点

- jpg文件头
- 十六进制反转