

i春秋之坚持60s

原创

金崑  于 2022-02-17 16:41:23 发布  2255  收藏

分类专栏: [攻防世界Misc](#) 文章标签: [wp](#)

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/I2872253606/article/details/122985457>

版权



[攻防世界Misc](#) 专栏收录该内容

7 篇文章 0 订阅

订阅专栏

是个jar文件, 打开看看



居然是个游戏，有点难，玩了好久，都坚持不了60s



还是换种方法吧

文件用notepad++打开

文件(F) 编辑(E) 搜索(S) 视图(V) 编码(N) 语言(L) 设置(T) 工具(O) 宏(M) 运行(R) 插件(P) 窗口(W) ?

9dc125bf1b84478cb14813d9bed6470c.jar

Address	0	1	2	3	4	5	6	7	8	9
00000000	50	4b	03	04	14	00	08	08	08	00
00000010	00	00	00	00	00	00	00	00	00	00
00000020	54	41	2d	49	4e	46	2f	4d	41	4e
00000030	4d	46	fe	ca	00	00	f3	4d	cc	cb
00000040	4b	2d	2a	ce	cc	cf	b3	52	30	d4
00000050	2c	2e	d6	0d	48	2c	c9	b0	52	d0
00000060	d3	05	8b	59	29	24	e7	e9	25	65
00000070	24	e6	a5	ea	05	80	48	f7	c4	dc
00000080	c5	cb	05	00	50	4b	07	08	81	91
00000090	53	00	00	00	50	4b	03	04	0a	00
000000a0	52	4b	00	00	00	00	00	00	00	00
000000b0	00	00	63	6e	2f	50	4b	03	04	0a
000000c0	86	52	4b	00	00	00	00	00	00	00
000000d0	00	00	00	63	6e	2f	62	6a	73	78
000000e0	0a	00	00	08	00	00	35	86	52	4b
000000f0	00	00	00	00	00	00	0f	00	00	00
00000100	78	74	2f	70	6c	61	6e	65	2f	50
00000110	08	08	00	35	86	52	4b	00	00	00
00000120	00	00	00	1f	00	00	00	63	6e	2f
00000130	70	6c	61	6e	65	2f	47	61	6d	65
00000140	2e	63	6c	61	73	73	75	51	6b	8f
00000150	42	e9	2e	ec	a3	2c	8f	75	7d	63
00000160	7c	91	a8	24	44	13	35	24	7e	2c
00000170	ba	eb	9f	f0	b7	68	b4	d9	44	13
00000180	68	16	a3	b1	c9	cc	bd	33	77	ee

查看文件的十六进制

CSDN @金 帛

发现文件头50 4b 03 04，说明这个文件也是zip文件

改一下后缀为zip，解压

名称	修改日期	类型	大小
cn	2022/2/17 16:08	文件夹	
images	2022/2/17 16:08	文件夹	
META-INF	2022/2/17 16:08	文件夹	



里面有许多文件的

用工具grepwin，搜索一下该文件夹的flag



发现有个文件里面放有flag，还说编码是2进制的

继续用notepad++打开看看，先以16进制的形式查看

复制过去解码

在线base64解码/编码工具

转换内容:

RGFqaURhbGlfSmlud2FuQ2hpamk=

Base64编码

Base64解码

转换结果:

DajiDaji JinwanChiji

CSDN@金帛

再加一下格式就OK了

这应该是考察jar的反编译，class文件就是，正常操作应该是修改游戏的代码直接通关，或者是查看过了60秒后会输出啥

建议参考：

[攻防世界 - MISC - 07 - 坚持60s_古月浪子的博客-CSDN博客_攻防世界坚持60s](#)