

pokemon

发表于 2021-01-21 分类于 [Challenge](#) , [2017](#) , [HCTF](#) , [Extra](#)
[Challenge](#) | [2017](#) | [HCTF](#) | [Extra](#) | [pokemon](#)

[点击此处](#)获得更好的阅读体验

WriteUp 来源

<https://xz.aliyun.com/t/1589>

题目考点

解题思路

打开游戏，大木会直接和你疯狂暗示

□

□

大木告诉你，FLAG在第一个道馆，去打败馆主。到研究室领精灵，助手给你20个奇异糖果，让你快速升级。再次提醒打败第一个馆主。

□

□

□

一路打怪升级到第一个道馆

□

打败后

□

□

□

馆主说我不会告诉你的，想知道的话自己去逆向这个rom。
正文开始。用PPRE工具。

□

```
1 text_11="HIIIIIIINT(You-really-want-to-get-the-flag-by-submi  
2 ting-it-one-by-one?) "  
3 text_12="HIIIIIIINT(Try-to-read-the-scrpit-XP) "  
4 text_13="HIIIIIIINT(Don't forget to change Brackets to Curly  
5 Brackets !!!!) "
```

下面是一堆flag，但只有一个是正确的。
提示你去看脚本。锁定脚本

```

1 Fanfare 1500
2 Lockall
3 Faceplayer
4 Checkbadge 0 0x800c
5 If 0x800c 1
6 CheckLR 1 func_5
7 Message 0
8 CloseMsgOnKeyPress
9 TrainerBattle 20 0 0
10 CheckTrainerLost 0x800c
11 If 0x800c 0
12 CheckLR 1 func_6
13 Setbdgtrue 0
14 ActMainEvent 22
15 SetTrainerId 29
16 SetTrainerId 50
17 Setvar 0x4074 1
18 Setflag 402
19 Setvar 16648 6
20 Setflag 244
21 Setflag 403
22 Message 1
23 SetvarHero 0
24 Message 2
25 Soundfr 1189
26 Fadedef
27 Message 3
28 Jump func_7

```

到func_7

```

1 Setvar 0x8004 378
2 Setvar 0x8005 1
3 CheckItem3 0x8004 0x8005 0x800c
4 If 0x800c 0
5 CheckLR 1 func_15
6 Callstd 241 7
7 Setflag 115
8 Clearflag 741
9 Setvar 0x8004 378
10 Setvar 0x8005 1
11 CheckItem3 0x8004 0x8005 0x800c
12 If 0x800c 0
13 CheckLR 1 func_16
14 Message 4
15 WaitButton
16 CloseMsgOnKeyPress
17 Releaseall
18 End

```

分析逻辑可知, func_16永远不会被执行
到func_16

```

1 Message 64
2 WaitButton
3 CloseMsgOnKeyPress
4 Releaseall
5 End

```

发现是使用64号text弹出对话框

text_64="HCTF{6A0A81AB5F9917B1EEC3A6183C614380}"

Flag

```
1 HCTF{6A0A81AB5F9917B1EEC3A6183C614380}
```

- 本文作者: CTFHub
- 本文链接: <https://writeup.ctfhub.com/Challenge/2017/HCTF/Extra/jvmIGHK11vReq8jUFPmAGE.html>
- 版权声明: 本博客所有文章除特别声明外, 均采用 [BY-NC-SA](#) 许可协议。转载请注明出处!

[#Challenge](#) [#2017](#) [#HCTF](#) [#Extra](#)

[big_zip](#)

[New_Love_Song](#)