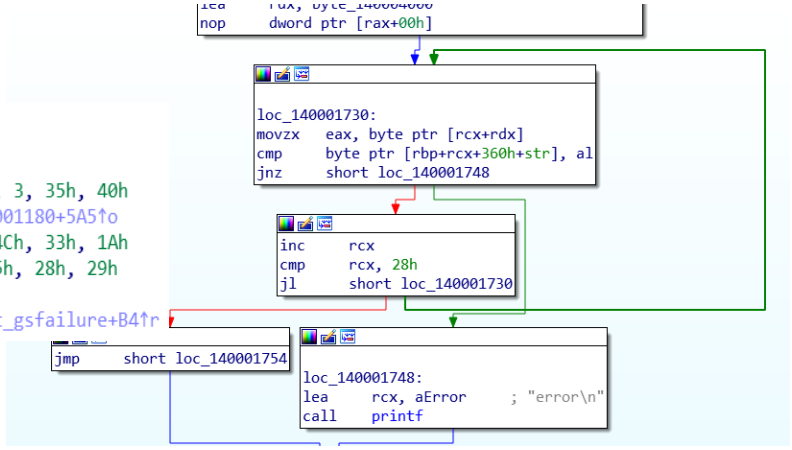
HGAME Week4 WriteUp

RE

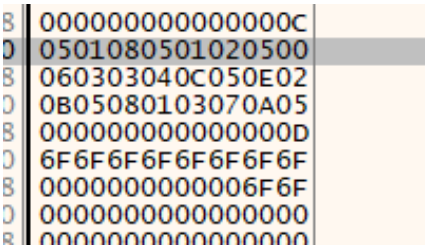
easyVM

1. 通过字符串的查找 通过 error 找到对输入字符的判定 且可以判定字符串长度应为 40

```
assume cs:_data
;org 140004000h
0004000[48]
db 3Ah, 54h, 2Fh, 2Ah, 2Fh, 36h, 13h, 1, 2Eh, 3, 35h, 40h
                        ; DATA XREF: sub_140001180+5A5↑o
db 47h, 0Eh, 5Fh, 59h, 1, 69h, 27h, 8, 3Dh, 4Ch, 33h, 1Ah
db 2Dh, 0Bh, 40h, 0Eh, 4Bh, 24h, 41h, 27h, 25h, 28h, 29h
db 2Ah, 2 dup(2), 5Dh, 24h, 8 dup(0)
dq 0FFFFD466D2205DCDh   ; DATA XREF: __report_gsfailure+B4↑r
```



2. 往上追溯发现有对字符串的加密，是通过对内存里的指令进行的，再与内存中的数值进行比较



3. 带入到 x64dbg 中进行动态调式 发现当指令执行到 0B 时回进行循环返回至 0E，循环里的操作总结起来就是对字符串逐位进行 xor 运算，在内存中可以找到运算的对象，太长就不截出来了。

4. 把数据写进脚本就完事了