华维帝皇铠甲Week3 wp

patchme

超纲difficult

不过在answer哥的帮助下还是做出来了

核心的漏洞就是gets带来的栈溢出以及printf不使用占位符带来的格式化字符串漏洞

一开始我的想法是把gets换成fgets，从汇编和反编译形成的伪代码来看么有任何问题

但是跑起来就是非法指令或者段错误

询问answer学长也无果

最终选择了scanf来读入字符串

有个知识点就是因为scanf和printf都是需要占位符的

占位符的实质其实是字符串

所以可以在程序中相对无关的地方改掉一点数据

看了answer发的那篇hint之后改了

eh_frame段的数据

查询之后知道eh_frame段是异常处理段（error handle frame）

所以程序没有抛出异常的话是不会影响程序运行的

但是改的时候遇到了地址对齐之类的pwn的东西就很异或了

空间不足也是采用了jmp的方法直接跳到了其他地方继续执行操作

但是我直接找了一个没有被引用到的函数

虽然交叉引用的结果是no refer

但是如果坏坏的出题人干一点坏事也是可以用到的

下次谨慎吧

做完这题patch的熟练度确实高了不少

对于汇编以及elf文件格式之类杂七杂八的东西也是有了新学到的东西

还是不错的题目的