**Lab6** **RE Challenge #2**

1. **实验目的**
   1. 熟悉静态反汇编工具IDA Freeware；
   2. 熟悉反汇编代码、伪代码的逆向分析过程；
   3. 掌握反汇编语言中的数学计算、数据结构、条件判断、分支结构的识别和逆向分析；
   4. 运用熟悉的编程语言，实现简单的脚本编写。
2. **实验原理**
3. 通过IDA Freeware得到ELF文件的反汇编代码，如图1和图2所示。



图 1 reverse的反汇编代码

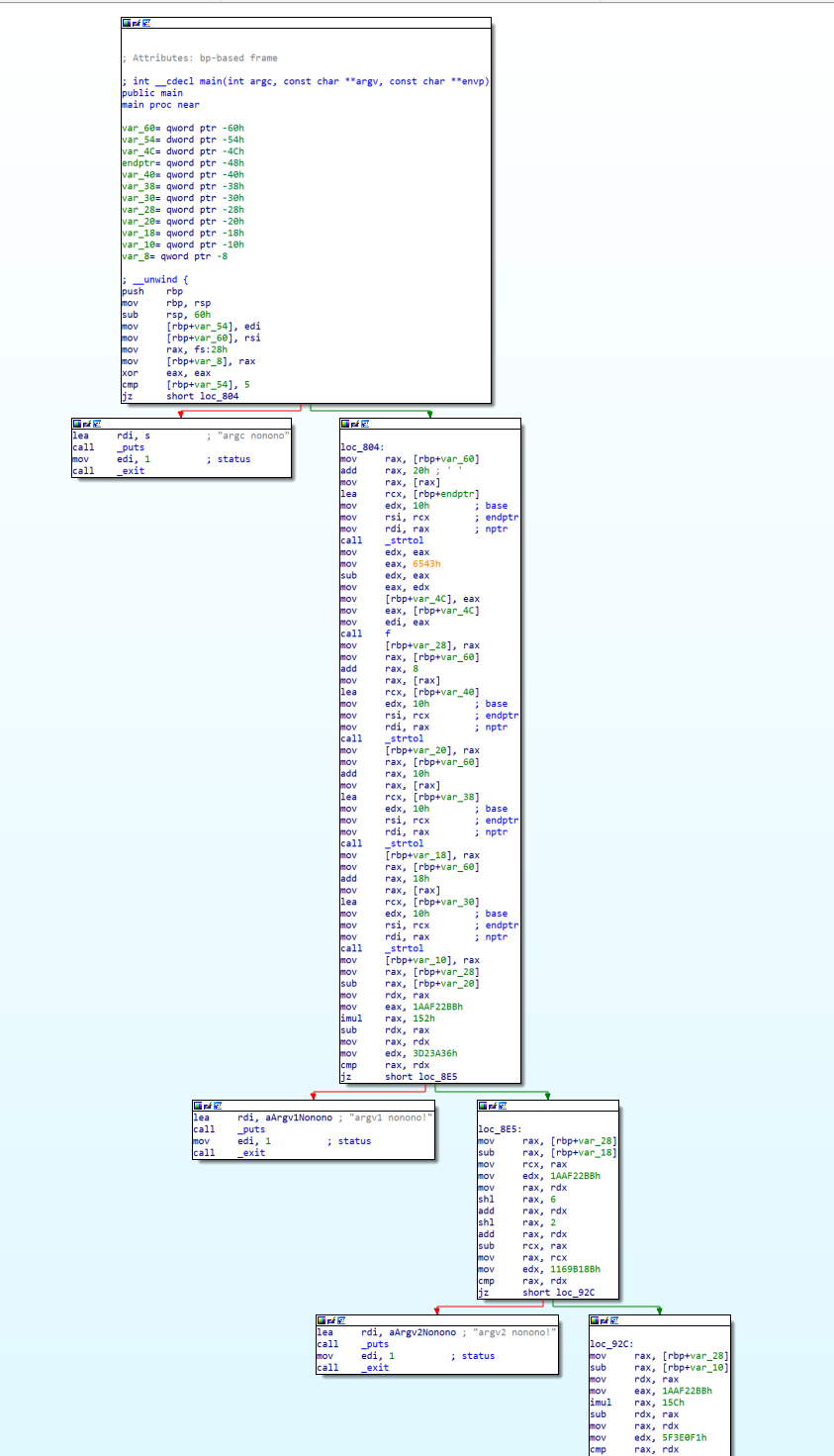


图 2 reverse的反汇编代码的图形化显示

1. 使用IDA的反编译功能（F5）得到伪代码，如图3所示。

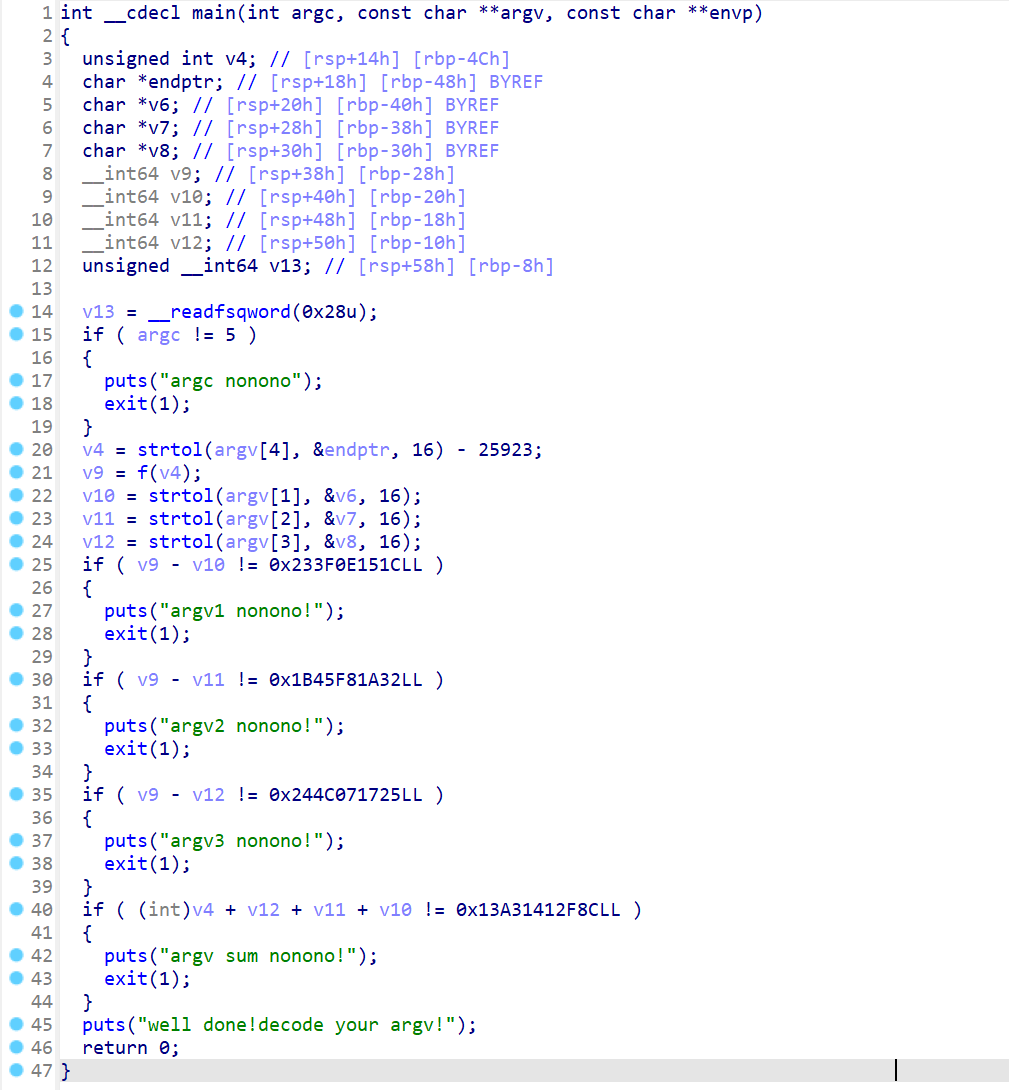


图 3 reverse的反编译伪代码

1. 对汇编代码和反编译伪代码的计算过程、条件判断、分支结构等信息进行分析，逆向推出待解方程组。
2. 编写脚本实现暴力破解，解出方程组，得到参数“V9”、“V10”、 “V11”、“V12”的正确取值，完成逆向分析挑战！
3. **实验报告**
4. 使用IDA Freeware，获得ELF文件的反汇编代码、反编译伪代码，提供截图。
5. 对反汇编代码或反编译伪代码的计算过程、数据结构、条件判断、分支结构等信息进行逆向分析，推理出逆向方程组，在实验报告中记录逆向分析的详细过程。
6. 使用熟悉的编程语言编写脚本，暴力解出方程组，得到正确的参数取值，在实验报告中记录脚本撰写思路和输出结果。

strtol()会将nptr指向的字符串，根据参数base，按权转化为long int, 然后返回这个值

