gdb？！

pwndbg是gdb的一个插件，先来安装它吧

首先对于调试，

设置断点

```Bash
break + 【函数名】
b +
```

启动程序

```Bash
run
```

步过（汇编语句）

```Bash
ni
```

步过（与ni的区别是碰到call某个函数会进入）

```Bash
si
```

快速完成一个函数

```Bash
finish
```

第一关

尝试从对应的地方找到目标的值吧

第二关

如何查看指定地址的值?

```Bash
x/[n][f][u] addr
```

- n：可选，表示要显示的单元数量，默认为1。
- f：可选，表示显示的格式，常见格式包括：
  - d：十进制整数
  - x：十六进制
  - o：八进制
  - c：字符
  - f：浮点数
- u：可选，表示数据单位，常见单位包括：
  - b：字节
  - h：半字（2 字节）
  - w：字（4 字节）
  - g：巨字（8 字节）

```Bash
x 按十六进制格式显示变量。
d 按十进制格式显示变量。
u 按十六进制格式显示无符号整型。
o 按八进制格式显示变量。
t 按二进制格式显示变量。
a 按十六进制格式显示变量。
c 按字符格式显示变量。
f 按浮点数格式显示变量。
s 按字符串显示。
b 按字符显示。
i 显示汇编指令。
```

第三关

如何在调试的时候改变指定地址内存储的值?

```Bash
set? ? ? ?
```

第四关

如何查看堆相关的指令，请试试他们分别是做什么的吧：

```Bash
heap -v
```

```Bash
arena
```

```Bash
bins
```

```Bash
vis
```