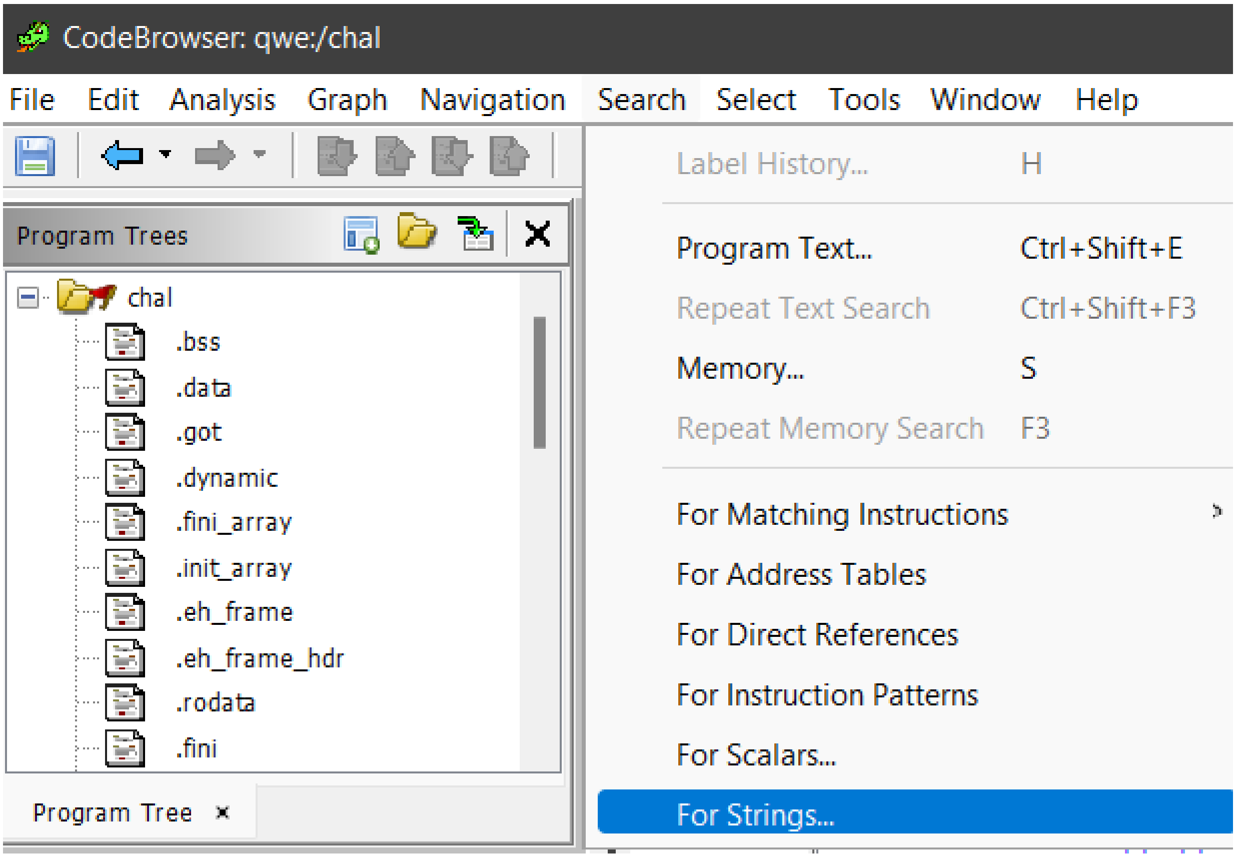
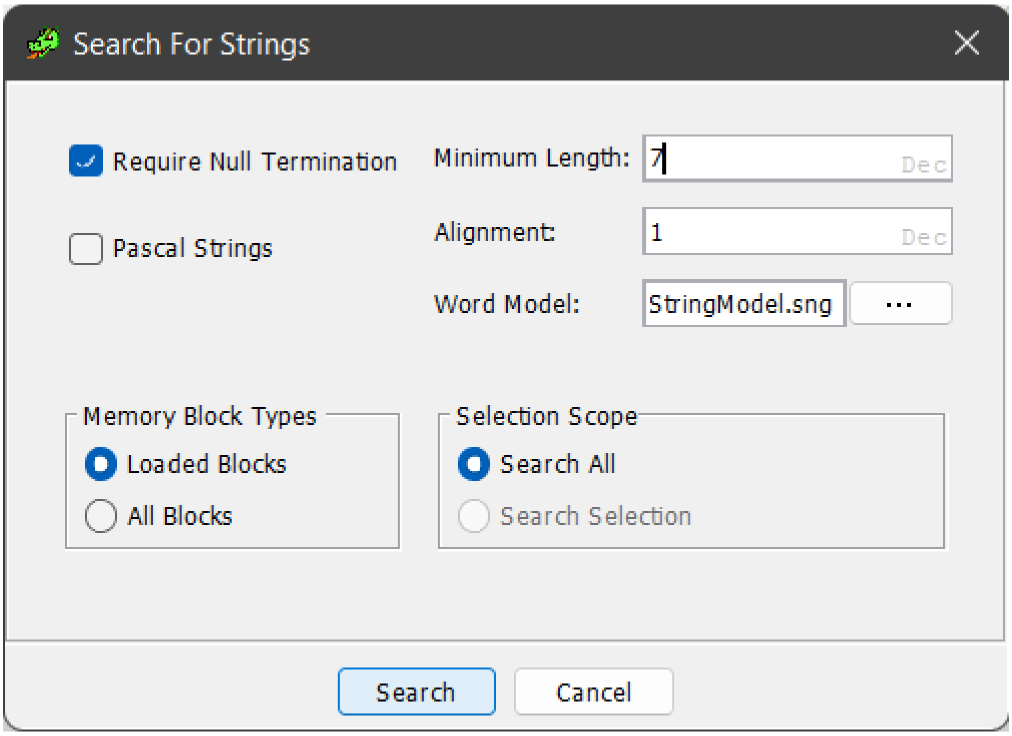
- Debug this shit

The end

- Locate correct string





Search For Strings

☑ Require Null Termination

□ Pascal Strings

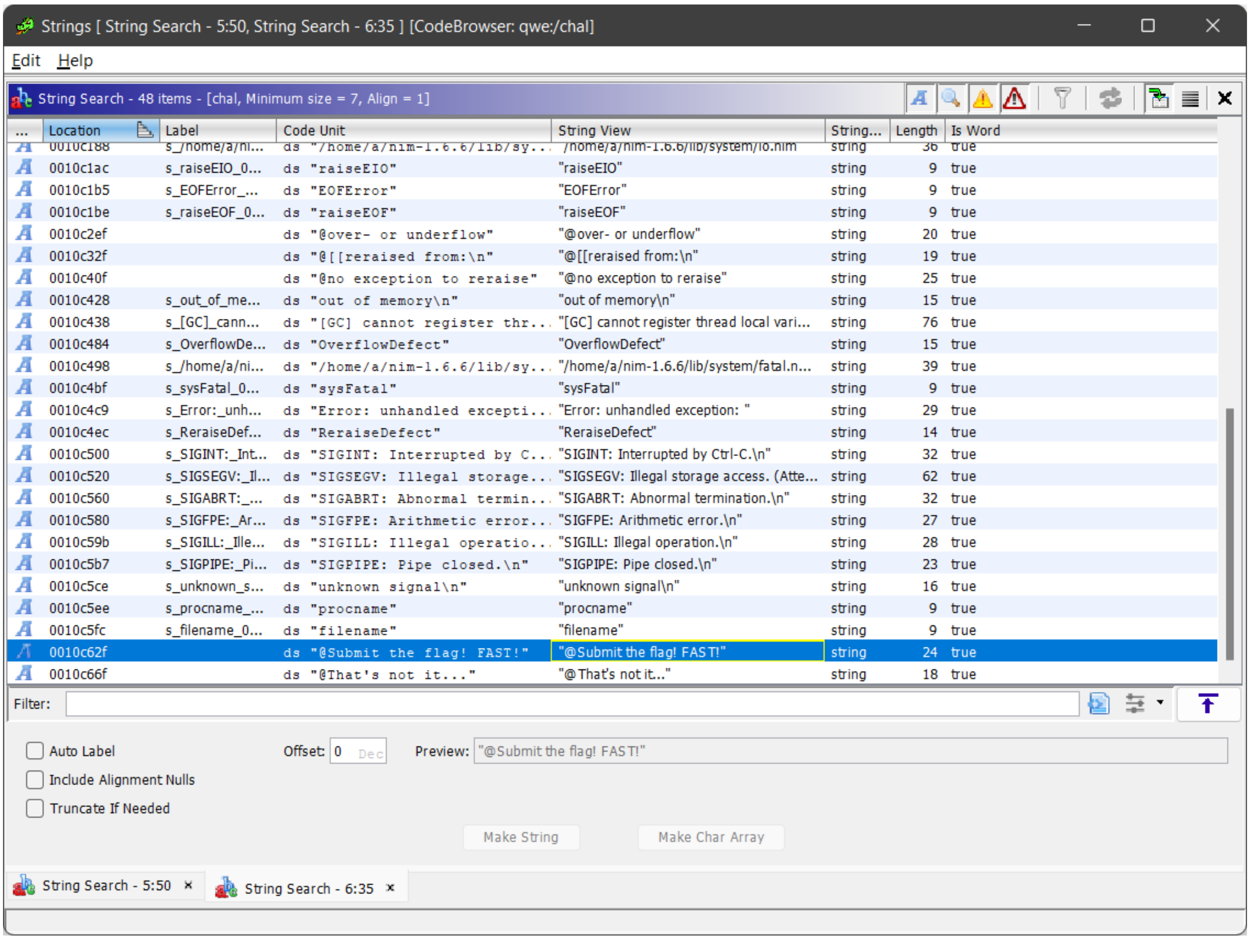
Minimum Length: 7 Dec

Alignment: 1 Dec

Word Model: StringModel.sng

Memory Block Types
● Loaded Blocks
○ All Blocks

Selection Scope
● Search All
○ Search Selection



Strings [String Search - 5:50, String Search - 6:35] [CodeBrowser: qwe:/chal]

String Search - 48 items - [chal, Minimum size = 7, Align = 1]

...	Location	Label	Code Unit	String View	String...	Length	Is Word
	0010c188	s_/home/a/ni...	ds "/home/a/nim-1.6.6/lib/sy...	/home/a/nim-1.6.6/lib/system/io.nim	string	36	true
	0010c1ac	s_raiseEIO_0...	ds "raiseEIO"	"raiseEIO"	string	9	true
	0010c1b5	s_EOFError_...	ds "EOFError"	"EOFError"	string	9	true
	0010c1be	s_raiseEOF_0...	ds "raiseEOF"	"raiseEOF"	string	9	true
	0010c2ef		ds "@over- or underflow"	"@over- or underflow"	string	20	true
	0010c32f		ds "@[[reraised from:\n"	"@[[reraised from:\n"	string	19	true
	0010c40f		ds "@no exception to reraise"	"@no exception to reraise"	string	25	true
	0010c428	s_out_of_me...	ds "out of memory\n"	"out of memory\n"	string	15	true
	0010c438	s_[GC]_cann...	ds "[GC] cannot register thr...	"[GC] cannot register thread local vari...	string	76	true
	0010c484	s_OverflowDe...	ds "OverflowDefect"	"OverflowDefect"	string	15	true
	0010c498	s_/home/a/ni...	ds "/home/a/nim-1.6.6/lib/sy...	"/home/a/nim-1.6.6/lib/system/fatal.n...	string	39	true
	0010c4bf	s_sysFatal_0...	ds "sysFatal"	"sysFatal"	string	9	true
	0010c4c9	s_Error:_unh...	ds "Error: unhandled excepti...	"Error: unhandled exception: "	string	29	true
	0010c4ec	s_ReraiseDef...	ds "ReraiseDefect"	"ReraiseDefect"	string	14	true
	0010c500	s_SIGINT:_Int...	ds "SIGINT: Interrupted by C...	"SIGINT: Interrupted by Ctrl-C.\n"	string	32	true
	0010c520	s_SIGSEGV:_Il...	ds "SIGSEGV: Illegal storage...	"SIGSEGV: Illegal storage access. (Atte...	string	62	true
	0010c560	s_SIGABRT:_...	ds "SIGABRT: Abnormal termin...	"SIGABRT: Abnormal termination.\n"	string	32	true
	0010c580	s_SIGFPE:_Ar...	ds "SIGFPE: Arithmetic error...	"SIGFPE: Arithmetic error.\n"	string	27	true
	0010c59b	s_SIGILL:_Ille...	ds "SIGILL: Illegal operatio...	"SIGILL: Illegal operation.\n"	string	28	true
	0010c5b7	s_SIGPIPE:_Pi...	ds "SIGPIPE: Pipe closed.\n"	"SIGPIPE: Pipe closed.\n"	string	23	true
	0010c5ce	s_unknown_s...	ds "unknown signal\n"	"unknown signal\n"	string	16	true
	0010c5ee	s_procname_...	ds "procname"	"procname"	string	9	true
	0010c5fc	s_filename_0...	ds "filename"	"filename"	string	9	true
	0010c62f		ds "@Submit the flag! FAST!"	"@Submit the flag! FAST!"	string	24	true
	0010c66f		ds "@That's not it..."	"@That's not it..."	string	18	true

Filter:

□ Auto Label

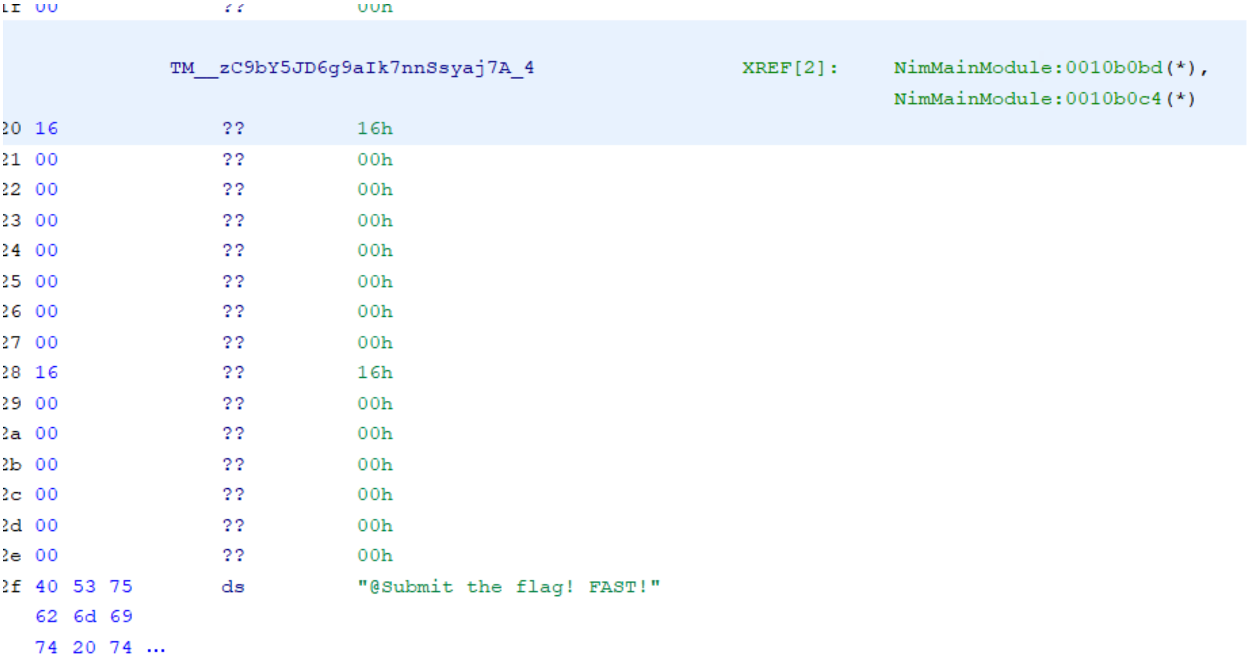
□ Include Alignment Nulls

□ Truncate If Needed

Offset: 0 Dec

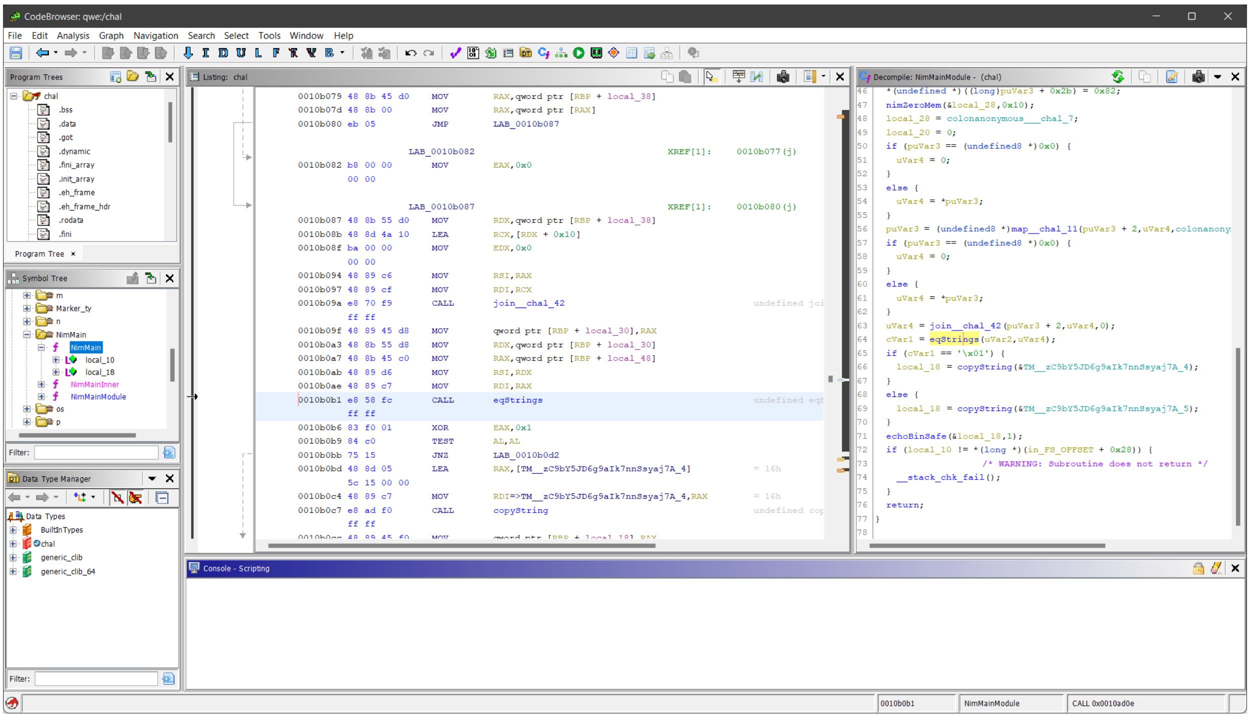
Preview: "@Submit the flag! FAST!"

- Locate string references



```
                TM__zC9bY5JD6g9aIk7nnSsyaj7A_4                  XREF[2]:     NimMainModule:0010b0bd(*),
                                                                             NimMainModule:0010b0c4(*)
20 16           ??          16h
21 00           ??          00h
22 00           ??          00h
23 00           ??          00h
24 00           ??          00h
25 00           ??          00h
26 00           ??          00h
27 00           ??          00h
28 16           ??          16h
29 00           ??          00h
2a 00           ??          00h
2b 00           ??          00h
2c 00           ??          00h
2d 00           ??          00h
2e 00           ??          00h
2f 40 53 75     ds          "@Submit the flag! FAST!"
   62 6d 69
   74 20 74 …
```

- NimMainModule located



```
0010b079 48 8b 45 d0     MOV      RAX,qword ptr [RBP + local_38]
0010b07d 48 8b 00        MOV      RAX,qword ptr [RAX]
0010b080 eb 05           JMP      LAB_0010b087

                 LAB_0010b082                                  XREF[1]:    0010b077(j)
0010b082 b8 00 00        MOV      EAX,0x0
         00 00

                 LAB_0010b087                                  XREF[1]:    0010b080(j)
0010b087 48 8b 55 d0     MOV      RDX,qword ptr [RBP + local_38]
0010b08b 48 8d 4a 10     LEA      RCX,[RDX + 0x10]
0010b08f ba 00 00        MOV      EDX,0x0
         00 00
0010b094 48 89 c6        MOV      RSI,RAX
0010b097 48 89 cf        MOV      RDI,RCX
0010b09a e8 70 f9        CALL     join__chal_42                                  undefined joi
         ff ff
0010b09f 48 89 45 d8     MOV      qword ptr [RBP + local_30],RAX
0010b0a3 48 8b 55 d8     MOV      RDX,qword ptr [RBP + local_30]
0010b0a7 48 8b 45 c0     MOV      RAX,qword ptr [RBP + local_48]
0010b0ab 48 89 d6        MOV      RSI,RDX
0010b0ae 48 89 c7        MOV      RDI,RAX
0010b0b1 e8 58 fc        CALL     eqStrings                                      undefined eqS
         ff ff
0010b0b6 83 f0 01        XOR      EAX,0x1
0010b0b9 84 c0           TEST     AL,AL
0010b0bb 75 15           JNZ      LAB_0010b0d2
0010b0bd 48 8d 05        LEA      RAX,[TM__zC9bY5JD6g9aIk7nnSsyaj7A_4]           = 16h
         5c 15 00 00
0010b0c4 48 89 c7        MOV      RDI=>TM__zC9bY5JD6g9aIk7nnSsyaj7A_4,RAX        = 16h
0010b0c7 e8 ad f0        CALL     copyString                                     undefined cop
         ff ff
```

```
  *(undefined *)((long)puVar3 + 0x2b) = 0x82;
  nimZeroMem(&local_28,0x10);
  local_28 = colonanonymous___chal_7;
  local_20 = 0;
  if (puVar3 == (undefined8 *)0x0) {
    uVar4 = 0;
  }
  else {
    uVar4 = *puVar3;
  }
  puVar3 = (undefined8 *)map__chal_11(puVar3 + 2,uVar4,colonanony
  if (puVar3 == (undefined8 *)0x0) {
    uVar4 = 0;
  }
  else {
    uVar4 = *puVar3;
  }
  uVar4 = join__chal_42(puVar3 + 2,uVar4,0);
  cVar1 = eqStrings(uVar2,uVar4);
  if (cVar1 == '\x01') {
    local_18 = copyString(&TM__zC9bY5JD6g9aIk7nnSsyaj7A_4);
  }
  else {
    local_18 = copyString(&TM__zC9bY5JD6g9aIk7nnSsyaj7A_5);
  }
  echoBinSafe(&local_18,1);
  if (local_10 != *(long *)(in_FS_OFFSET + 0x28)) {
                    /* WARNING: Subroutine does not return */
    __stack_chk_fail();
  }
  return;
}
```

- Start GDB

```
→ nimrod gdb chal
```

- Locate NimMainModule function

```
gdb-peda$ info functions
All defined functions:
```

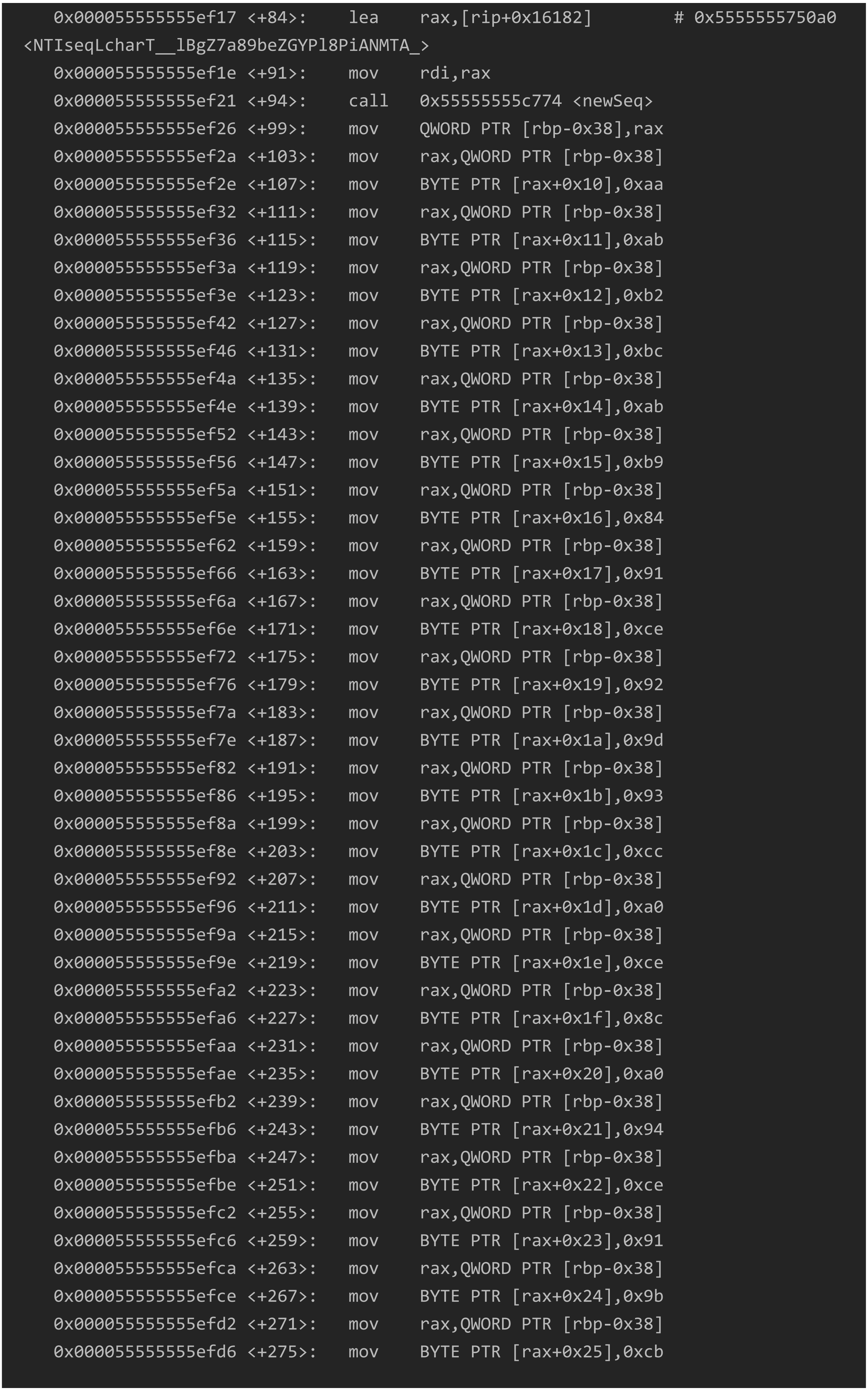
```
Non-debugging symbols:
0x0000000000001000  _init
...
0x000000000000ac6b  colonanonymous___chal_7
0x000000000000ac8b  nimCmpMem
0x000000000000acc5  equalMem__system_1735
0x000000000000ad0e  eqStrings
0x000000000000ad97  initStackBottomWith
0x000000000000adb2  PreMainInner
0x000000000000adbd  PreMain
0x000000000000ae1b  NimMainInner
0x000000000000ae2b  NimMain
0x000000000000ae7f  main
0x000000000000aec3  NimMainModule <-------------This
0x000000000000b10e  chalDatInit000
0x000000000000b154  _fini
```

- Set a breakpoint and tinker around

```
gdb-peda$ b *NimMainModule
Breakpoint 1 at 0xaec3
gdb-peda$ r
...
Breakpoint 1, 0x000055555555eec3 in NimMainModule ()
```

- Disassamble this function

```
gdb-peda$ disassemble
Dump of assembler code for function NimMainModule:
=> 0x000055555555eec3 <+0>:     endbr64
   0x000055555555eec7 <+4>:     push   rbp
   0x000055555555eec8 <+5>:     mov    rbp,rsp
   0x000055555555eecb <+8>:     sub    rsp,0x40
   0x000055555555eecf <+12>:    mov    rax,QWORD PTR fs:0x28
   0x000055555555eed8 <+21>:    mov    QWORD PTR [rbp-0x8],rax
   0x000055555555eedc <+25>:    xor    eax,eax
   0x000055555555eede <+27>:    lea    rax,[rbp-0x10]
   0x000055555555eee2 <+31>:    mov    esi,0x8
   0x000055555555eee7 <+36>:    mov    rdi,rax
   0x000055555555eeea <+39>:    call   0x55555555eb51 <nimZeroMem>
   0x000055555555eeef <+44>:    mov    QWORD PTR [rbp-0x40],0x0
   0x000055555555eef7 <+52>:    mov    rax,QWORD PTR [rip+0x5172]        #
0x555555564070 <stdin@GLIBC_2.2.5>
   0x000055555555eefe <+59>:    mov    rdi,rax
   0x000055555555ef01 <+62>:    call   0x5555555561f3 <readLine__systemZio_271>
   0x000055555555ef06 <+67>:    mov    QWORD PTR [rbp-0x40],rax
   0x000055555555ef0a <+71>:    mov    QWORD PTR [rbp-0x38],0x0
   0x000055555555ef12 <+79>:    mov    esi,0x1c
```



```
   0x000055555555ef17 <+84>:    lea    rax,[rip+0x16182]        # 0x5555555750a0
<NTIseqLcharT__lBgZ7a89beZGYPl8PiANMTA_>
   0x000055555555ef1e <+91>:    mov    rdi,rax
   0x000055555555ef21 <+94>:    call   0x55555555c774 <newSeq>
   0x000055555555ef26 <+99>:    mov    QWORD PTR [rbp-0x38],rax
   0x000055555555ef2a <+103>:   mov    rax,QWORD PTR [rbp-0x38]
   0x000055555555ef2e <+107>:   mov    BYTE PTR [rax+0x10],0xaa
   0x000055555555ef32 <+111>:   mov    rax,QWORD PTR [rbp-0x38]
   0x000055555555ef36 <+115>:   mov    BYTE PTR [rax+0x11],0xab
   0x000055555555ef3a <+119>:   mov    rax,QWORD PTR [rbp-0x38]
   0x000055555555ef3e <+123>:   mov    BYTE PTR [rax+0x12],0xb2
   0x000055555555ef42 <+127>:   mov    rax,QWORD PTR [rbp-0x38]
   0x000055555555ef46 <+131>:   mov    BYTE PTR [rax+0x13],0xbc
   0x000055555555ef4a <+135>:   mov    rax,QWORD PTR [rbp-0x38]
   0x000055555555ef4e <+139>:   mov    BYTE PTR [rax+0x14],0xab
   0x000055555555ef52 <+143>:   mov    rax,QWORD PTR [rbp-0x38]
   0x000055555555ef56 <+147>:   mov    BYTE PTR [rax+0x15],0xb9
   0x000055555555ef5a <+151>:   mov    rax,QWORD PTR [rbp-0x38]
   0x000055555555ef5e <+155>:   mov    BYTE PTR [rax+0x16],0x84
   0x000055555555ef62 <+159>:   mov    rax,QWORD PTR [rbp-0x38]
   0x000055555555ef66 <+163>:   mov    BYTE PTR [rax+0x17],0x91
   0x000055555555ef6a <+167>:   mov    rax,QWORD PTR [rbp-0x38]
   0x000055555555ef6e <+171>:   mov    BYTE PTR [rax+0x18],0xce
   0x000055555555ef72 <+175>:   mov    rax,QWORD PTR [rbp-0x38]
   0x000055555555ef76 <+179>:   mov    BYTE PTR [rax+0x19],0x92
   0x000055555555ef7a <+183>:   mov    rax,QWORD PTR [rbp-0x38]
   0x000055555555ef7e <+187>:   mov    BYTE PTR [rax+0x1a],0x9d
   0x000055555555ef82 <+191>:   mov    rax,QWORD PTR [rbp-0x38]
   0x000055555555ef86 <+195>:   mov    BYTE PTR [rax+0x1b],0x93
   0x000055555555ef8a <+199>:   mov    rax,QWORD PTR [rbp-0x38]
   0x000055555555ef8e <+203>:   mov    BYTE PTR [rax+0x1c],0xcc
   0x000055555555ef92 <+207>:   mov    rax,QWORD PTR [rbp-0x38]
   0x000055555555ef96 <+211>:   mov    BYTE PTR [rax+0x1d],0xa0
   0x000055555555ef9a <+215>:   mov    rax,QWORD PTR [rbp-0x38]
   0x000055555555ef9e <+219>:   mov    BYTE PTR [rax+0x1e],0xce
   0x000055555555efa2 <+223>:   mov    rax,QWORD PTR [rbp-0x38]
   0x000055555555efa6 <+227>:   mov    BYTE PTR [rax+0x1f],0x8c
   0x000055555555efaa <+231>:   mov    rax,QWORD PTR [rbp-0x38]
   0x000055555555efae <+235>:   mov    BYTE PTR [rax+0x20],0xa0
   0x000055555555efb2 <+239>:   mov    rax,QWORD PTR [rbp-0x38]
   0x000055555555efb6 <+243>:   mov    BYTE PTR [rax+0x21],0x94
   0x000055555555efba <+247>:   mov    rax,QWORD PTR [rbp-0x38]
   0x000055555555efbe <+251>:   mov    BYTE PTR [rax+0x22],0xce
   0x000055555555efc2 <+255>:   mov    rax,QWORD PTR [rbp-0x38]
   0x000055555555efc6 <+259>:   mov    BYTE PTR [rax+0x23],0x91
   0x000055555555efca <+263>:   mov    rax,QWORD PTR [rbp-0x38]
   0x000055555555efce <+267>:   mov    BYTE PTR [rax+0x24],0x9b
   0x000055555555efd2 <+271>:   mov    rax,QWORD PTR [rbp-0x38]
   0x000055555555efd6 <+275>:   mov    BYTE PTR [rax+0x25],0xcb
   0x000055555555efda <+279>:   mov    rax,QWORD PTR [rbp-0x38]
   0x000055555555efde <+283>:   mov    BYTE PTR [rax+0x26],0xa0
   0x000055555555efe2 <+287>:   mov    rax,QWORD PTR [rbp-0x38]
   0x000055555555efe6 <+291>:   mov    BYTE PTR [rax+0x27],0x9c
   0x000055555555efea <+295>:   mov    rax,QWORD PTR [rbp-0x38]
   0x000055555555efee <+299>:   mov    BYTE PTR [rax+0x28],0xcf
   0x000055555555eff2 <+303>:   mov    rax,QWORD PTR [rbp-0x38]
   0x000055555555eff6 <+307>:   mov    BYTE PTR [rax+0x29],0xcf
   0x000055555555effa <+311>:   mov    rax,QWORD PTR [rbp-0x38]
   0x000055555555effe <+315>:   mov    BYTE PTR [rax+0x2a],0x93
   0x000055555555f002 <+319>:   mov    rax,QWORD PTR [rbp-0x38]
   0x000055555555f006 <+323>:   mov    BYTE PTR [rax+0x2b],0x82
   0x000055555555f00a <+327>:   lea    rax,[rbp-0x20]
   0x000055555555f00e <+331>:   mov    esi,0x10
   0x000055555555f013 <+336>:   mov    rdi,rax
   0x000055555555f016 <+339>:   call   0x55555555eb51 <nimZeroMem>
   0x000055555555f01b <+344>:   lea    rax,[rip+0xfffffffffffffc49]        #
0x55555555ec6b <colonanonymous___chal_7>
   0x000055555555f022 <+351>:   mov    QWORD PTR [rbp-0x20],rax
   0x000055555555f026 <+355>:   mov    QWORD PTR [rbp-0x18],0x0
   0x000055555555f02e <+363>:   mov    QWORD PTR [rbp-0x30],0x0
   0x000055555555f036 <+371>:   cmp    QWORD PTR [rbp-0x38],0x0
   0x000055555555f03b <+376>:   je     0x55555555f046 <NimMainModule+387>
   0x000055555555f03d <+378>:   mov    rax,QWORD PTR [rbp-0x38]
   0x000055555555f041 <+382>:   mov    rsi,QWORD PTR [rax]
   0x000055555555f044 <+385>:   jmp    0x55555555f04b <NimMainModule+392>
   0x000055555555f046 <+387>:   mov    esi,0x0
   0x000055555555f04b <+392>:   mov    rax,QWORD PTR [rbp-0x38]
   0x000055555555f04f <+396>:   lea    rdi,[rax+0x10]
   0x000055555555f053 <+400>:   mov    rax,QWORD PTR [rbp-0x20]
   0x000055555555f057 <+404>:   mov    rdx,QWORD PTR [rbp-0x18]
   0x000055555555f05b <+408>:   mov    rcx,rdx
   0x000055555555f05e <+411>:   mov    rdx,rax
   0x000055555555f061 <+414>:   call   0x55555555eb9c <map__chal_11>
   0x000055555555f066 <+419>:   mov    QWORD PTR [rbp-0x30],rax
   0x000055555555f06a <+423>:   mov    QWORD PTR [rbp-0x28],0x0
   0x000055555555f072 <+431>:   cmp    QWORD PTR [rbp-0x30],0x0
   0x000055555555f077 <+436>:   je     0x55555555f082 <NimMainModule+447>
   0x000055555555f079 <+438>:   mov    rax,QWORD PTR [rbp-0x30]
   0x000055555555f07d <+442>:   mov    rax,QWORD PTR [rax]
   0x000055555555f080 <+445>:   jmp    0x55555555f087 <NimMainModule+452>
   0x000055555555f082 <+447>:   mov    eax,0x0
   0x000055555555f087 <+452>:   mov    rdx,QWORD PTR [rbp-0x30]
   0x000055555555f08b <+456>:   lea    rcx,[rdx+0x10]
   0x000055555555f08f <+460>:   mov    edx,0x0
   0x000055555555f094 <+465>:   mov    rsi,rax
   0x000055555555f097 <+468>:   mov    rdi,rcx
   0x000055555555f09a <+471>:   call   0x55555555ea0f <join__chal_42>
   0x000055555555f09f <+476>:   mov    QWORD PTR [rbp-0x28],rax
   0x000055555555f0a3 <+480>:   mov    rdx,QWORD PTR [rbp-0x28]
   0x000055555555f0a7 <+484>:   mov    rax,QWORD PTR [rbp-0x40]
   0x000055555555f0ab <+488>:   mov    rsi,rdx
   0x000055555555f0ae <+491>:   mov    rdi,rax
   0x000055555555f0b1 <+494>:   call   0x55555555ed0e <eqStrings>
   0x000055555555f0b6 <+499>:   xor    eax,0x1 <-----------HELLO THERE
   0x000055555555f0b9 <+502>:   test   al,al
   0x000055555555f0bb <+504>:   jne    0x55555555f0d2 <NimMainModule+527>
   0x000055555555f0bd <+506>:   lea    rax,[rip+0x155c]        # 0x555555560620
<TM__zC9bY5JD6g9aIk7nnSsyaj7A_4>
   0x000055555555f0c4 <+513>:   mov    rdi,rax
   0x000055555555f0c7 <+516>:   call   0x55555555e179 <copyString>
   0x000055555555f0cc <+521>:   mov    QWORD PTR [rbp-0x10],rax
   0x000055555555f0d0 <+525>:   jmp    0x55555555f0e6 <NimMainModule+547>
   0x000055555555f0d2 <+527>:   nop
   0x000055555555f0d3 <+528>:   lea    rax,[rip+0x1586]        # 0x555555560660
<TM__zC9bY5JD6g9aIk7nnSsyaj7A_5>
   0x000055555555f0da <+535>:   mov    rdi,rax
   0x000055555555f0dd <+538>:   call   0x55555555e179 <copyString>
   0x000055555555f0e2 <+543>:   mov    QWORD PTR [rbp-0x10],rax
   0x000055555555f0e6 <+547>:   lea    rax,[rbp-0x10]
   0x000055555555f0ea <+551>:   mov    esi,0x1
   0x000055555555f0ef <+556>:   mov    rdi,rax
   0x000055555555f0f2 <+559>:   call   0x5555555562cb <echoBinSafe>
   0x000055555555f0f7 <+564>:   nop
   0x000055555555f0f8 <+565>:   mov    rax,QWORD PTR [rbp-0x8]
   0x000055555555f0fc <+569>:   sub    rax,QWORD PTR fs:0x28
   0x000055555555f105 <+578>:   je     0x55555555f10c <NimMainModule+585>
   0x000055555555f107 <+580>:   call   0x555555555200 <__stack_chk_fail@plt>
   0x000055555555f10c <+585>:   leave
   0x000055555555f10d <+586>:   ret
End of assembler dump.
```

- Locate xor function and set a breakpint

```
gdb-peda$ b *NimMainModule+499
Breakpoint 2 at 0x55555555f0b6

gdb-peda$ c
Continuing.
qwerty
[----------------------------------registers-----------------------------------]
RAX: 0x0
RBX: 0x0
RCX: 0x7ffff7d1857d --> 0x4000000
RDX: 0x7ffff7d170d0 --> 0x1c
RSI: 0x7ffff7d170d0 --> 0x1c
RDI: 0x7ffff7d16050 --> 0x6
RBP: 0x7fffffffdc60 --> 0x7fffffffdc70 --> 0x7fffffffdc90 --> 0x7fffffffdcc0 -->
```

```
0x1
RSP: 0x7fffffffdc20 --> 0x7ffff7d16050 --> 0x6
RIP: 0x55555555f0b6 (<NimMainModule+499>:       xor    eax,0x1)
R8 : 0x0
R9 : 0x5555555762a0 --> 0xa797472657771 ('qwerty\n')
R10: 0x77 ('w')
R11: 0x246
R12: 0x7fffffffddd8 --> 0x7fffffffe03f
("/mnt/d/UTMCTF2022_Proto/rev/nimrod/chal")
R13: 0x55555555ee7f (<main>:    endbr64)
R14: 0x555555563d10 --> 0x5555555553c0 (<__do_global_dtors_aux>:        endbr64)
R15: 0x7ffff7ffd040 --> 0x7ffff7ffe2e0 --> 0x555555554000 --> 0x10102464c457f
EFLAGS: 0x293 (CARRY parity ADJUST zero SIGN trap INTERRUPT direction overflow)
[-------------------------------------code-------------------------------------]
   0x55555555f0ab <NimMainModule+488>:  mov    rsi,rdx
   0x55555555f0ae <NimMainModule+491>:  mov    rdi,rax
   0x55555555f0b1 <NimMainModule+494>:  call   0x55555555ed0e <eqStrings>
=> 0x55555555f0b6 <NimMainModule+499>:  xor    eax,0x1
   0x55555555f0b9 <NimMainModule+502>:  test   al,al
   0x55555555f0bb <NimMainModule+504>:  jne    0x55555555f0d2
<NimMainModule+527>
   0x55555555f0bd <NimMainModule+506>:  lea    rax,[rip+0x155c]        #
0x555555560620 <TM__zC9bY5JD6g9aIk7nnSsyaj7A_4>
   0x55555555f0c4 <NimMainModule+513>:  mov    rdi,rax
[------------------------------------stack-------------------------------------]
0000| 0x7fffffffdc20 --> 0x7ffff7d16050 --> 0x6
0008| 0x7fffffffdc28 --> 0x7ffff7d17050 --> 0x1c
0016| 0x7fffffffdc30 --> 0x7ffff7d17090 --> 0x1c
0024| 0x7fffffffdc38 --> 0x7ffff7d170d0 --> 0x1c
0032| 0x7fffffffdc40 --> 0x55555555ec6b (<colonanonymous___chal_7>:     endbr64)
0040| 0x7fffffffdc48 --> 0x0
0048| 0x7fffffffdc50 --> 0x0
0056| 0x7fffffffdc58 --> 0x1c25dbf8553edc00
[------------------------------------------------------------------------------]
Legend: code, data, rodata, value

Breakpoint 2, 0x000055555555f0b6 in NimMainModule ()
```

- Browse memory stack aet the plaintext flag from memory

```
gdb-peda$ x/50s 0x7ffff7d17050
...
0x7ffff7d170a0: "UTMCTF{n1mbl3_1s_k1nd4_c00l}"
```

Flag: *subject to change*