

owo_whats_this's Very Special Number v1

Link: <https://crackmes.one/crackme/5e6ac90233c5d4439bb2de39>

Platform: Unix/linux etc.

Language: C/C++

```
$ file OwO_vsn_1
```

```
OwO_vsn_1: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked,  
interpreter /lib64/ld-linux-x86-64.so.2,
```

```
BuildID[sha1]=238174dec0aed75b00dcbf9bbccfc7ce7cc799da, for GNU/Linux 3.2.0, not  
stripped
```

```
$ strings OwO_vsn_1
```

```
/lib64/ld-linux-x86-64.so.2
```

```
Libstdc++.so.6
```

```
Hi! Can you guess my Special Number?
```

```
You must be psychic :O
```

```
Wrong! Try again :)
```

```
GCC: (GNU) 9.2.1 20200130
```

```
GCC: (Arch Linux 9.2.1+20200130-2) 9.2.1 20200130
```

```
init.c
```

```
crtstuff.c
```

```
crackme.cpp
```

```
main
```

The binary was compiled on Arch Linux.

VirusTotal Report

Link: <https://www.virustotal.com/gui/file/c8990006a610e4a28e6eb2d78b5d923ecbd0ed7a6da146a8a9444cd590976640/detection>

MD5: 6bd06c2526aa73a8ff61806e38533d86

SHA-1: b8241680c92d07a28e34fa5669659a67d640ca40

Radare2 Analysis

```
radare2 -d -e io.cache=true OwO_vsn_1
```

```

0x561deb00b339 e816fdffff call sym std::ostream::operator<<(std::ostream& (*)(std::ostream&)) ;[2]
0x561deb00b33a 48d45f0 lea rax, [var_10h]
0x561deb00b33e 48b9c6 mov rsi, rax
0x561deb00b341 48d3db82e00. lea rdi, reloc.std::cin ; 0x561deb00e200
0x561deb00b348 e823fdffff call sym std::istream::operator>>(long long&) ;[3]
0x561deb00b34d e872fdffff call sym generate() ;[4]
0x561deb00b352 48b55f0 mov rdx, qword [var_10h]
0x561deb00b356 4839d0 cmp rax, rdx
0x561deb00b359 0f94c0 sete al
0x561deb00b35c 84c0 test al, al
0x561deb00b35e 742a je 0x561deb00b38a
0x561deb00b360 48d35e60c00. lea rsi, str.You_must_be_psychic:_0 ; 0x561deb00c04d ; "You must be psychic :0"
0x561deb00b367 48d3d722d00. lea rdi, reloc.std::cout ; 0x561deb00e0e0
0x561deb00b36e e8cdfcffff call sym std::basic_ostream<char, std::char_traits<char> >> std::operator<< <std::char_traits<char> >(std::b
0x561deb00b373 48b9c2 mov rdx, rax
0x561deb00b376 488b05532c00. mov rax, qword [method.std::basic_ostream_char_std::char_traits_char____std::endl_char__std.char_traits_cha
0x561deb00b37d 48b9c6 mov rsi, rax
0x561deb00b380 48b9d7 mov rdi, rdx
0x561deb00b383 e8c8fcffff call sym std::ostream::operator<<(std::ostream& (*)(std::ostream&)) ;[2]
0x561deb00b388 eb28 jmp 0x561deb00b3b2
0x561deb00b38a 48d35d30c00. lea rsi, str.Wrong_Try_again:_ ; 0x561deb00c064 ; "Wrong! Try again :)"
0x561deb00b391 48d3d482d00. lea rdi, reloc.std::cout ; 0x561deb00e0e0

```

0x561deb00b341 ~ Get the users input.

0x561deb00b34d ~ Calls the function generate().

0x561deb00b352 ~ The variable var_10h is moved into register rdx.

0x561deb00b356 ~ The number generated is being compared with the inputted number

[0x55ae44bbc2fb]> db 0x55ae44bbc352

[0x55ae44bbc2fb]> db 0x55ae44bbc356

[0x55ae44bbc2fb]> dc

Hi! Can you guess my Special Number?

12

hit breakpoint at: 0x55ae44bbc352

[0x55ae44bbc352]> drr

role	reg	value	refstr
R0	rax	198b6e17cf	109713430479 rax

The secret number is 109713430479.

[0x55ae44bbc352]> dc

hit breakpoint at: 0x55ae44bbc356

[0x55ae44bbc356]> drr

role	reg	value	refstr
R0	rax	198b6e17cf	109713430479 rax
A2	rdx	c	12 rdx

[0x55ae44bbc356]> dr rdx = 109713430479

Set the rdx register to the magic number

[0x55ae44bbc356]> dc

You must be psychic :0

\$./OwO_vsn_1

Hi! Can you guess my Special Number?

109713430479

You must be psychic :O