## Popa & Kao CS 161 Spring 2023 程序代码域做证65编程辘影 Prep 2

Q1 Indirection (0 points) Consider the follow #include < sto struct log\_en char title [8 6 char \* msg; 7 **}**; 8 void log\_event(char \*title , char \*msg) { 10 size\_t len = strnlen(msg, 256); if (len == 256) return: Message too long Fixamtr Help struct log entry e 11 12 13 entry -> msg = malloc (256); strcpy(entry->title, title); add\_to\_log(entry); \* implementation 163.com 15 16 17

Assume you are on a little-indian 42 bit x868 spring in memory safety defenses are enabled.

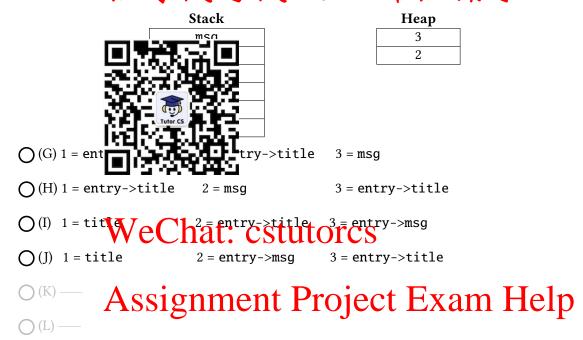
- Q1.1 (3 points) Which of the following lines contains a memory safety vulnerability?
  - O(A) Line 10 https://tutorcs@om 15
  - (B) Line 13

(E) —

(C) Line 14

(F) ---

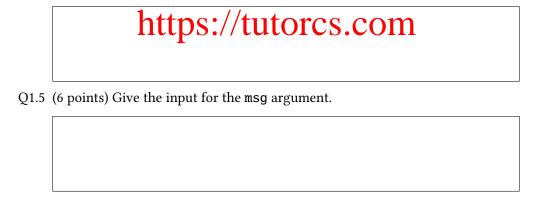
Q1.2 (3 points) Fill in the numbered blanks on the following stack and here diagrammer log\_event. Assume that lower-numbered addresses that a the bottom of the hid rain.



## Email: tutorcs@163.com Using GDB, you find that the address of the rip of log\_event is 0xbfffe0f0.

Let SHELLCODE be a 40-byte shellcode. Construct an input that would cause this program to execute shellcode. Write all your arswers in Python 2syptax (just like Project 1).

Q1.4 (6 points) Give the input for the title argument.



Q2 Stack Exchange Consider the following will real of to CS编程辅导 (19 points)

```
#include <byteswap.h>
  #include <inttypes
  #include < std
 5
  void prepare
 6
       char buff
 7
       int64 t
 8
9
       printf (
10
       fread (buf
11
       printf("What is the pointer?\n");
12
       fread (& ptr VIP ( iz pf ( fuin o Stut O gt S);
13
14
       if (ptr < buffer || ptr >= buffer + 68) {
15
           printf Pointer is outside Puffer!");
return SS1gnment Project Exam Help
16
17
18
19
       * ptr = bs Eaph all; tutores to 163.com
20
21
22
23
       main (void prepare_input); 749389476
  int main (void)
24
25
26
       return 0;
27
```

The bswap\_64 function takes in 8 bytes and returns the 8 bytes in reverse order.

Assume that the code is run on a 32-bit system, no memory safety defenses are enabled, and there are no exception handlers, saved registers, or compiler padding.

Q2.1 (3 points) Fill in the numbered blanks on the following stack diagram for prepare\_input.

	1	(0xbffff494)
	2	(0xbffff490)
	3	(0xbfffff450)
	4	(0xbffff44c)
O(A) 1 = sfp, 2 = rip, 3 = buffer, 4 = ptr		O(D) 1 = rip, 2 = sfp, 3 = ptr, 4 = buffer
O(B) 1 = sfp, 2 = rip, 3 = ptr, 4 = buffer		(E) ——
(C) 1 = rip, 2 = sfp, 3 = buffer, 4 = ptr		(F) ——

Q2.2	(4 points) Which of these values on the stack can that apply.	the attacker wite te thing 1 a # 13? Select all
	☐(G) buffer	$\square$ (J) rip
	□(H)ptr	$\square$ (K) None of the above
	□(I) sfp	□ (L) ——
Q2.3	(3 points) Give these bytes:	ogram to execute shellcode. At line 10, first input
	(A) 64-byte shellcode	$O(D) \xbf\xff\xf4\x50$
	O(B)\xbf\x\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	EX50\xf4\xff\xbf
	$\bigcirc$ (C) \x4c\xf4\xff\xbf	(F) ——
Q2.4	(3 points) Thermos Sispinement P	Project Exam Help
	(G) 64-byte shellcode	$O(J) \xbf\xff\xf4\x50$
	O(H)\xbf\x Fmail: tutores	SA 1x63f4GAM
	$\bigcirc (I) \x4c\xf4\xff\xbf$	(L) —
Q2.5	QQ: 7493894 (3 points) At line 13, input these bytes:	6/6
	$O(A) \times ff \times ff \times f4 \times 50$	$O(D) \x90\xf4\xff\xbf$
	O(A)\xbf\xff\xf4\x50 https://tutorcs	$O(E) \times f(xf4) \times 94$
	$O(C) \xbf\xff\xf4\x90$	$O(F) \x94\xf4\xff\xbf$
Q2.6	(3 points) Suppose you replace 68 with 64 at line 1	10 and line 15. Is this modified code memory-safe?
	(G) Yes (H) No (I) —	$\bigcirc (J) \qquad \bigcirc (K) \qquad \bigcirc (L)$

This is the end of Q2. Leave the remaining subparts of Q2 blank on Gradescope, if there are any. You have reached the end of the exam.