Popa & Kao CS 161 Spring 2023 程序代码域做证5编程辘影Prep 3

Q1 Robin (20 points) Consider the follow void robin (2 char buf 3 int i; if (fread(&i 1, stdin) != 1) 6 return; if (fgets Wfe Chatuf C Stuto FOSLL) return: 10 11 Assignment Project Exam Help 12

Assume that:

- There is no compiler pairly or truit or cost registers 63.com
- The provided line of code in each subpart compiles and runs.
- buf is located at remory address 12 12 19 19 19
- Stack canaries are enabled, and all other memory safety defenses are disabled.
- The stack canary is four completely random bytes (no null byte).

For each subpart, mall whether it is pustible I tak the value of the stack canary. If you put possible, provide an input to Line 5 and an input to Line 8 that would leak the canary. If the line is not needed for the exploit, you must write "Not needed" in the box.

Write your answer in Python syntax.

Q1.1	O Possible 程序代写代做 CS编程辅导
	Not pos Line 5:
	Line 8:
Q1.2	WeChat: cstutorcs (5 points) For this subpart only, enter an input that allows you to leak a single character from memory address 0xffffd8d7. Mark "Not possible" if this is not possible. Line 11 contains printf("%c", buf[i]); O Possible Possible Project Exam Help
	O Not possible Line 5: Line 5: Line 5: 163.com
	QQ: 749389476
	https://tutorcs.com
Q1.3	(6 points) Line 11 contains printf(buf);. O Possible
	O Not possible Line 5:
	Line 8:

Q1.4 (6 points) Line 程 on Print 写 代 做 CS 编程 辅导

O Not	pos and the post of the post o		
Line 5:			
	**		
Line 8:			
	WeChat:	cstutores	

Assignment Project Exam Help

Email: tutorcs@163.com

QQ: 749389476

https://tutorcs.com

Q2 The Way You Look Tonight
Consider the following vulngrable Cos 代故 CS编程辅导 (20 points)

```
typedef struct
      char mon [16]
3
      char chan
4
  } duo;
5
                                  FILE *f) {
  void third_wh
7
      duo mond
8
      duo richa
9
      fgets (ric
10
      strcpy (richard.
11
      int8_t alias = 0;
12
      size_t counter = 0;
13
      while (!richard.mon[15]
14
15
           size_t index = counter / 10;
          if (mandler mon[index] == 'A') {
massingnimento Project Exam Help
16
17
18
19
           alias++;
20
          country++;
          if (Email: tutorcs@163.com
21
22
               richard.chan[alias] = mondler.mon[alias];
23
                    ): 749389476
24
      }
25
      printf("%s\n", richard.mon);
26
      fflush(stdout); // no memory safety vulnerabilities on this line
27
28
               https://tutorcs.com
29
  void valentine(char *tape[2], FILE *f) {
30
31
      int song = 0;
32
      while (song < 2) {
          read_input(tape[song]); //memory-safe function, see below
33
          third_wheel(tape[song], f);
34
35
          song + +;
36
      }
37
```

For all of the subparts, here are a few tools you can use:

You run GDB one, and discover that the address of the RP of thirte when is suffffed 84.

• For your inputs, you may use SHELLCODE as a 100-byte shellcode.

• The number 0 as jmp *esp • The number 0xe4ff is interpreted as jmp *esp

• If needed, you put as OUTPUT, slicing it using Python 2 syntax.

Assume that:

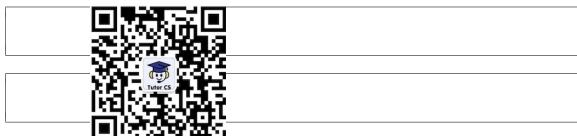
- You are on a l
- There is no other compiler padding or saved additional registers.
- main calls valentine with the appropriate arguments.
- Stack canarie we enabled not no other no metro y safety defenses are enabled.
- The stack canary is four completely random bytes (no null byte).
- read_input(buf) is a memory-safe function that writes to buf without any overflows. Write your exploits in Python Syntax (Just like in Project J.).
- Q2.1 Fill in the following stack diagram, assuming that the program is paused at **Line 14**. Each row should contain a struct men ber, local variable, the struct wheel, or canary (the value in each row does not have to be four bytes long).

Stack

QQ	: 749389476
http	os://tutorcs.com

Q2.2	In the first call to	hird_wheel	, we vant to	leak the val	ue of the stack	canry. 💆	hat should be
~	In the first call to the missing value	es at line 21 in o	rder o make	Mexploi	10%和27王	、拥与	_

Provide a decimal integer in each box.



For the rest of the question, assume that ASLR is enabled in addition to stack canaries. Assume that the code section of memory has not been randomized.

Q2.3 Provide an input of the lines below in project the stack canary in the first call to third_wheel. If you don't need an input, you must write "Not Needed".

Provide a string value for tape[0]:

Assignment Project Exam Help

Email: tutorcs@163.com

Provide an input to fgets in third_wheel: 749389476

https://tutorcs.com

Q2.4 Provide an input to each of the lines below in order to run the maligious shall code in the second call to third_wicel. It you don't need an lung to the way "Not Need to".

Provide a string value for tape[1]:



WeChat: cstutorcs

Assignment Project Exam Help

Email: tutorcs@163.com

QQ: 749389476

https://tutorcs.com