Q1 *Antares* (0 points)

This problem is a (very) simplified variant of Question 6 of Project 1 , with the intention of introducing you to `printf` *vulnerabilities.*

Consider the following vulnerable code.

```
1  #include <stdio.h>
2  #include <string.h>
3
4  void echo(char *buf) {
5      char padding[12];
6      fgets(buf, 48, stdin);
7      printf(buf);
8  }
9
10 int main() {
11     char buf[48];
12     echo(buf);
13     return 0;
14 }
```

1. Which line of code contains the memory safety vulnerability? Briefly explain this vulnerability.

2. Complete the stack diagram if the code were executed until a breakpoint set on line 8. Assume normal (non-malicious) program execution. You do not need to write the values on the stack, only the names. There are no extraneous boxes, and each box represents one item in memory. The bottom of the page represents the lower addresses.

main's RIP
main's SFP

3. Construct an input to Line **6** that would result in a successful execution of `SHELLCODE`. Assume that echo's `RIP` is stored at `0xffff8e0` and that you have a `SHELLCODE` script stored at `0xffffbeef`.

   Hint: You will find the following directives useful

   `%_u`*: Treats* `args[i]` *as a VALUE. Print a variable-length number of bytes starting from* `args[i]` *(set _ to the desired length).*

   `%hn`*: Treats* `args[i]` *as a POINTER. Write the number of bytes that have been currently printed (as a two-byte number) to the memory address* `args[i]`*.*

   _____ * _____ + \x ___ \x ___ \x ___ \x ___ + _____ * _____ +

   \x ___ \x ___ \x ___ \x ___ + '%c' * _____ + '%_____u' + _____ +

   '%_____u' + _____ + '\n'

Q2 *IV-e got a question for ya* **(24 points)**

Determine whether each of the following schemes is IND-CPA secure. This question has 6 subparts.

Q2.1 (6 points) AES-CBC where the IV for message M is chosen as HMAC-SHA256(k_2, M) truncated to the first 128 bits. The MAC key k_2 is distinct from the encryption key k_1.

Provide a short justification for your answer on your answer sheet.

◯ (A) Insecure ◯ (C) —— ◯ (E) ——

◯ (B) Secure ◯ (D) —— ◯ (F) ——

Q2.2 (6 points) AES-CTR where the IV for message M is chosen as HMAC-SHA256(k_2, M) truncated to the first 128 bits. The MAC key k_2 is distinct from the encryption key k_1.

Provide a short justification for your answer on your answer sheet.

Clarification made during the exam: You can assume that IV refers to the nonce for CTR mode.

◯ (G) Insecure ◯ (I) —— ◯ (K) ——

◯ (H) Secure ◯ (J) —— ◯ (L) ——

Q2.3 (3 points) AES-CBC where the IV for message M is chosen as SHA-256(x) truncated to the first 128 bits. x is a predictable counter starting at 0 and incremented *per message*.

◯ (A) Insecure ◯ (C) —— ◯ (E) ——

◯ (B) Secure ◯ (D) —— ◯ (F) ——

Q2.4 (3 points) AES-CTR where the IV for message M is chosen as SHA-256(x) truncated to the first 128 bits. x is a predictable counter starting at 0 and incremented *per message*.

Clarification made during the exam: You can assume that IV refers to the nonce for CTR mode.

◯ (G) Insecure ◯ (I) —— ◯ (K) ——

◯ (H) Secure ◯ (J) —— ◯ (L) ——

Q2.5 (3 points) AES-CBC where the IV for message M is chosen as HMAC-SHA256(k_2+x, M) truncated to the first 128 bits. The MAC key k_2 is distinct from the encryption key k_1 and x is a predictable counter starting at 0 and incremented *per message*.

◯ (A) Insecure ◯ (C) —— ◯ (E) ——

◯ (B) Secure ◯ (D) —— ◯ (F) ——

Q2.6 (3 points) AES-CTR where the IV for message M is chosen as HMAC-SHA256(k_2+x, M) truncated to the first 128 bits. The MAC key k_2 is distinct from the encryption key k_1 and x is a predictable counter starting at 0 and incremented *per message*.

Clarification made during the exam: You can assume that IV refers to the nonce for CTR mode.

◯ (G) Insecure ◯ (I) —— ◯ (K) ——

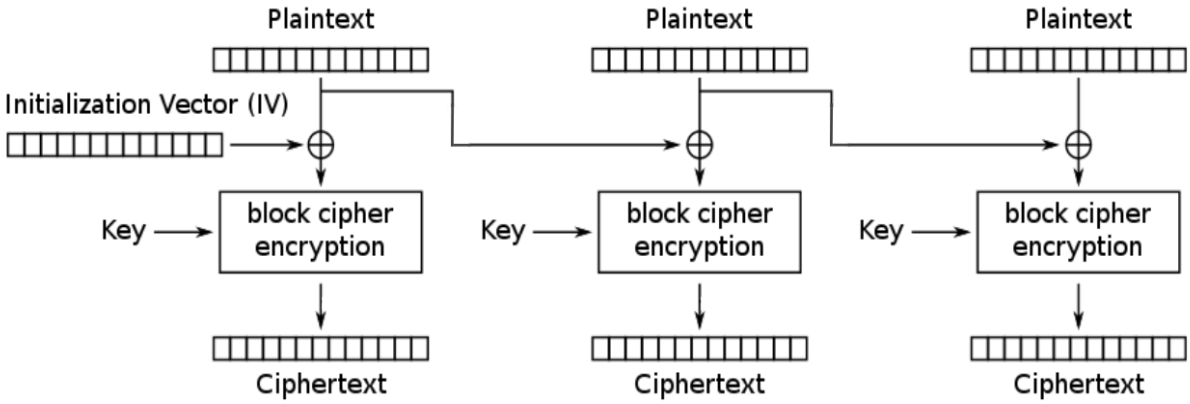
◯ (H) Secure ◯ (J) —— ◯ (L) ——

Q3 *Block Ciphers* **(15 points)**

Consider the following block cipher mode of operation.

M_i is the ith plaintext block. C_i is the ith ciphertext block. E_K is AES encryption with key K.

$$C_0 = M_0 = IV$$
$$C_i = E_K(M_{i-1} \oplus M_i)$$



Q3.1 (5 points) Which of the following is true about this scheme? Select all that apply.

☐ (A) The encryption algorithm is parallelizable

☐ (B) If one byte of a plaintext block M_i is changed, then the corresponding ciphertext block C_i will be different in exactly one byte

☐ (C) If one byte of a plaintext block M_i is changed, then the next ciphertext block C_{i+1} will be different in exactly one byte

☐ (D) If two plaintext blocks are identical, then the corresponding ciphertext blocks are also identical

☐ (E) The encryption algorithm requires padding the plaintext

☐ (F) None of the above

Q3.2 (4 points) TRUE or FALSE: If the IV is always a block of all 0s for every encryption, this scheme is IND-CPA secure. Briefly justify your answer.

◯ (G) True ◯ (H) False ◯ (I) —— ◯ (J) —— ◯ (K) —— ◯ (L) ——

Q3.3 (6 points) TRUE or FALSE: If the IV is randomly generated for every encryption, this scheme is IND-CPA secure. Briefly justify your answer.

◯ (A) True ◯ (B) True ◯ (C) —— ◯ (D) —— ◯ (E) —— ◯ (F) ——