Student ID: ______________________________________

This sheet will not be graded (feel free to write on it), but you must turn it in at the end of the exam.

## C Function Definitions

```
size_t fread(void *ptr, size_t size, size_t nmemb, FILE *stream);

      The  function  fread() reads nmemb items of data, each size bytes long,
      from the stream pointed to by stream,  storing  them  at  the  location
      given by ptr.

      Note that fread() does not add a null byte after input.

int printf(const char *format, ...);

      printf() produces output according to the format string format.

      Conversion specifiers:

      %s   String (pointer to a character array). Treats corresponding
           argument as an address, dereferences that address, and
           outputs bytes at that address until null terminator.

      %Nu  Unsigned integer, padded to N bytes of output, where N is
           some number.

      %hn  Treats corresponding argument as an address, and writes
           the number of bytes printed so far (as a 2-byte integer) to that address.

      Each of the above conversion specifiers reads a 4-byte argument on the stack.

int strcmp(const char *s1, const char *s2);

      The  strcmp()  function compares the two strings s1 and s2.  It returns
      an integer less than, equal to, or greater than zero if  s1  is  found,
      respectively, to be less than, to match, or be greater than s2.
```

## JavaScript Function Definitions

The JavaScript function `post(URL, data)` sends a POST request to the given URL with the given `data`.

# SQL Function Definitions

In SQL, strings are 1-indexed. For example, in the word `pancake`, the letter `p` is at index 1.

`SUBSTRING(string, start_index, length)`

- Slices the given string starting at `start_index` and includes up to `length` characters.
- Example: `SUBSTRING("EvanBot", 5, 3)` returns `"Bot"`.
- Example: `SUBSTRING("EvanBot", 1, 1)` returns `"E"`.

`CHARINDEX(substring, string)`

- Returns the index where `substring` is found in `string`, or 0 if it isn't found.
- Example: `CHARINDEX("Bot", "EvanBot")` returns 5.
- Example: `CHARINDEX("Coda", "EvanBot")` returns 0.

# General Exam Assumptions

Unless otherwise specified, you can assume these facts on the entire exam:

- Memory safety:
  - You are on a little-endian 32-bit x86 system.
  - There is no compiler padding or saved additional registers.
  - If stack canaries are enabled, they are four completely random bytes (no null byte).
  - You can write your answers in Python syntax (as seen in Project 1).
  - Unless otherwise specified, all other memory safety defenses are disabled.
  - Each x86 instruction is 4 bytes long in machine code.
- Cryptography:
  - The attacker knows the algorithms being used (Shannon's maxim).
  - $\|$ denotes concatenation.
  - H refers to a secure cryptographic hash function.
  - $g$ and $p$ refer to a public generator element and large prime modulus, respectively.
  - $IV$s are randomly generated per encryption unless otherwise specified.
- Networking:
  - DNSSEC does not use ZSKs/KSKs, unless otherwise specified.