National University

Of Computer & Emerging Sciences Faisalabad-Chiniot Campus

Name: **Section:** **Roll:**

Information Security
Quiz 02

Q1: In your own words, what is a buffer overflow? What part of a program's memory is affected when a buffer overflow occurs?

A buffer overflow happens when a program writes more data into a buffer (fixed-size memory space) than it can hold. This extra data spills over into nearby memory locations.

It mainly affects the **stack memory**, where function variables, return addresses, and control data are stored.

For more information refer to **Lecture Buffer Overflow 1 Slide 4.**

Q2: Explain the three portions of a stack frame (arguments, special region, local variables).

When a function is called, the stack frame has three parts:

1. **Arguments** – Passed parameters, located using EBP offsets.
2. **Special Region** – Stores return address and saved EBP.
3. **Local Variables** – Declared inside the function, stored below EBP.

For more information refer to **Lecture Buffer Overflow 1 Slide 7-8.**

Q3: Draw and label the stack frames for main() and foo():

```
void bar(char *in) {
   char buf[16];
   strcpy(buf, in);
}
int main() {
   char msg[256];
   bar(msg);
}
```

Above code is taken from **Lecture Buffer Overflow 1 Slide 11** and only the buffer size, variable names and function name have been changed.