CSE 565 Solution to Homework 6

1. (30 points total; 7 points for part (a) including correctness, verification, and the minimum number of queries; 8 points for part (b) including correctness and the minimum number of queries; and 15 points for part (c) for correct answer with correct logic) Multiple answers are possible.

   (a) sum(Department=EE AND Position=Faculty AND Sex=F, Salary) = 90
   count(Department=EE AND Position=Faculty AND Sex=F) = 1
   The first query obtains Toner's salary and the second is used to verify that there is only one female EE faculty (who must be Toner).

   (b) sum(Department=EE AND (NOT Position=Student), Salary) = 381
   sum(Department=EE AND Sex=M AND (NOT Position=Student), Salary) = 291
   count(Department=EE AND (NOT Position=Student)) = 3
   count(Department=EE AND Sex=M AND (NOT Position=Student)) = 2
   The first two queries are used to determine the answer as $381 - 291 = 90$, while the last two queries verify that this is the correct answer (note that the last query can be implicit and we know that the count is at least 2 if the second sum query wasn't rejected). That is, there are 3 people in the EE Department who are not students, two of whom are male. This means that the third person must be Toner. Note that all queries comply with the requirement that a query has to match at lest 2 records and thus they are not rejected.

   (c) count(Department=EE AND Sex=F) = 2
   count(Department=EE AND Position=Faculty) = 2
   max(Department=EE AND Sex=F, Salary) = 90
   max(Department=EE AND (NOT Position=Faculty), Salary) = 66
   The first two queries tell us that there are two females in EE and two faculty members. This tell us that one EE faculty member is not female (as otherwise the second query would be rejected) and thus one female in the department is not faculty. The next query tells us that the highest paying female in the department earns 90 and the last query confirms that this is Toner's salary because the highest salary of non-faculty employees is 66.

   All queries comply with the requirements. In particular, the count queries overlap by one record (Toner) and both match more than one record. The max queries match two and three records, respectively, and overlap by one record.

2. (70 points total; 50 points for carrying out the attack with no address randomization and 20 points for partially getting around address randomization) Answers vary. We are looking for the evidence of correct execution of the attack or correct execution of some of the steps (for partial credit) if the attack could not be successfully executed. If `vulnerable.c` is not modified to have extra variables, we expect to require 23 characters before the first address is getting overwritten (and thus $23+15 = 35$ characters are needed to overwrite all 3 addresses). With no address randomization, you could expect addresses such as `0xbfe5f430` for `system`, `0xb7e52fb0` for `exit`, and `0xbffffe78` for the shell string. The most reliable way to extract the last address is by making a call to `getenv` from `vulnerable.c` (even if you later remove the corresponding code). To get around address randomization and reliably determine the address of the shell string, you may retrieve the address in the program and write it to the exploit file, or print the address, modify the exploit file, and have the program read the modified exploit.