This homework is due in class on Wednesday February 13, 2019.

The assignment is to complete the SEED labs on cross-site scripting and on SQL injection, available at

http://www.cis.syr.edu/~wedu/seed/Labs_16.04/Web/Web_XSS_Elgg/
http://www.cis.syr.edu/~wedu/seed/Labs_16.04/Web/Web_SQL_Injection/

Please use the Ubuntu 16.04 VM image for the labs.

**Collaboration policy:** Students are welcome to talk to each other, to the TAs, or to the instructor, about the assignment. Any assistance, though, must be limited to discussion of the problem and sketching general approaches to a solution. Each student must write out his or her own solutions to the homework. Consulting another student’s solution is prohibited, and submitted solutions may not be copied from any source. These and any other forms of collaboration on this assignment constitute cheating. If you have any question about whether some activity would constitute cheating, please feel free to ask.

**Plagiarism policy:** This homework must be solved without accessing the Internet, except as instructed in the assignment itself. Content from any source (other than your brain) has to be properly attributed.

**UNC Honor Pledge:** Your homework solution must include the UNC Honor Pledge, affixed with your signature: “UNC Honor Pledge: I certify that no unauthorized assistance has been received or given in the completion of this work.”

**What to turn in:** Each lab asks for a report where you detail your experience in working through a series of tasks. For each task, provide a 1-2 paragraph explanation of how you performed the task, along with screenshots to illustrate your progress on the task. Be sure to answer the questions asked in each task description.

**Friendly advice from your TAs:** Your friendly TAs have vetted these labs, and offered the following advice.

For the XSS lab: For Task 6,

1. Fetch the needed javascript worm code using the method demonstrated in the DOM approach.
2. Add the needed tags and encode it.
3. POST it to the user, using the same methods already used to modify profiles in task 5.

For the SQL injection lab: The lab’s description of task 2.3 includes, “In SQL, semicolon (;) is used to separate two SQL statements. Please describe how you can use the login page to get the server to run two SQL statements.” This seems to suggest that the task is possible and just requires separating two statements with a semicolon. However, this does not work – try to explain why in your solution.