CIS 4930: Secure Coding [Fall 2018]
Test VII

NAME: _____

Instructions:

1) This test is 6 pages in length.

2) You have 40 minutes to complete and turn in this test.

3) Short answer questions include a guideline for how many sentences to write. Respond in complete English sentences. Responses will be graded as described on the syllabus.

4) This test is closed books, notes, papers, friends, neighbors, etc.

5) Use the backs of pages in this test packet for scratch work. If you write more than a final answer in the area next to a question, circle your final answer.

1. [18 points]
Consider the tables shown below.

Students

SID	Name	Major
1	Alice	Civil Engineering
2	Bob	Electrical Engineering
3	Eve	Mechanical Engineering
4	Mallory	Medicine

Classes

CID	SID	Class
1	1	Calculus
2	1	Programming
3	2	Calculus
4	3	Programming
5	4	Anatomy

a) Write a SQL statement to retrieve all student names in the Students table.

b) Write a SQL statement to retrieve all student names that are majoring in engineering in Students table. Use a LIKE clause.

c) Write a SQL statement to retrieve all of Alice's classes in the Classes table.

d) Write a SQL statement to retrieve all student name and class pairs from the Students and Classes tables, where each returned pair (S,C) corresponds to a class C taken by student S.

e) Write a SQL statement to retrieve all student names that are taking the Programming class from the Students and Classes tables.

f) Write a SQL statement to add Age as a new column to the Students table.

2. [14 points]
Describe, and provide an example of, second order SQL injection attacks. [1 paragraph]

3. [10 points]
Identify and briefly describe the two primary types of XSS attacks. [3-4 sentences]

4. [10 points]
Explain how prepared statements mitigate injection attacks. [1 paragraph]

5. [8 points]
What is taint tracking? What are example mechanisms that use taint tracking? [2-3 sentences]

6. [8 points]
What are the primary tradeoffs between using stream versus block ciphers? [2-3 sentences]

7. [2 points]
What are metadata and metavariables? [1-2 sentences]

8. [24 points]
Consider the following portion of a web application.

```
1   String input = request.getParameter("input");
2   Connection conn = DriverManager.getConnection("MyDB");
3   String ins = "INSERT INTO simpleLedger VALUES ('user1', - " + input + " - 4)";
4   ins = ins + " ; INSERT INTO simpleLedger VALUES ('user2', " + input + " + 2)";
5   conn.executeUpdate(ins);
```

This program records data about a money transfer between accounts. It takes a transfer amount as the `input` and subtracts that amount from the `user1` account and adds that amount to the `user2` account. The program also applies a $4 transaction fee to the `user1` account and, due to a spectacular Cyber Monday sale, adds half of this fee as a bonus to the `user2` account.

a) Write, as we did in class (including using underlines where appropriate), the output SQL statement when the input is 6. Explain the output statement.

b) Write, as we did in class (including using underlines where appropriate), the output SQL statement when the input is 6E. Explain the output statement.

c) Write, as we did in class (including using underlines where appropriate), the output SQL statement when the input mounts a SQL injection attack using a SQL comment (--).

d) Rewrite the program to use a prepared statement, as with JDBC. Please do not worry about getting the method names exactly correct; we just want to see that you understand all the main ideas of coding with prepared statements.

9. [6 points]
Briefly explain the classic example of a confused-deputy attack on a compiler. [2-3 sentences]