CIS 4930: Secure Coding [Fall 2018]
Test VI

NAME: _____

Instructions:

1) This test is 5 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. [4 points]
What is a DBMS? What does it do? [1-2 sentences]

2. [5 points]
Contrast DMLs and DDLs. [1-2 sentences]

3. [18 points]
Consider the Employees table shown below.

PID	**Name**	**Salary**
1	Alice	10.2
2	Bob	22
3	Eve	35
4	Mallory	10.6

a) Define a logical schema for the Employees table.

b) Write a SQL statement to define (but not populate) the Employees table.

c) Write a SQL statement to populate the first row in the Employees table.

d) Write a SQL statement to retrieve the names of all the employees having a salary less than 30.

e) Write a SQL statement to retrieve all the information in the Employees table.

f) Write a SQL statement to delete the Employees table.

4. [9 points]
What are 3 example web-application frameworks, and what is a security benefit such frameworks provide? [2-3 sentences]

5. [20 points] [Essay]
Describe how SQLIAs can leak database schema. Exact code need not be shown, but please discuss all the main ideas presented in class.

6. [10 points]
A4 in the "OWASP Top 10 Application Security Risks" is "XML External Entities (XXE)".
a) What does XML stand for? [1 point]

b) What are the 3 types of XML tags described in class? [2 points]

c) At the level of detail discussed in class, how do XXE attacks work?

7. [11 points]
A8 in the "OWASP Top 10 Application Security Risks" is "Insecure Deserialization".
a) What are serialization and deserialization? [4 points]

b) At the level of detail discussed in class, how do insecure-deserialization attacks work, or what is a high-level example of how such an attack could proceed?

8. [5 points]
What is the formal requirement for a property to be safety? [1-2 sentences]

9. [4 points]
What is the main difference between Mandatory and Discretionary Access Control? [1 sentence]

10. [4 points]
Contrast the Bell-LaPadula and Biba Integrity models. [2-4 sentences]

11. [10 points]
Describe how a session-fixation attack may proceed. [2-5 sentences]