CNT 4419: Secure Coding [Fall 2019]
Test 6

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 and essay questions include guidelines for how much to write. Respond in complete English sentences. Avoid using bullet points and enumerated lists. Responses will be graded as described on the syllabus.

4) This test is closed books, notes, papers, smartphones, laptops, 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. [6 points] [1-3 sentences]
Describe XXE attacks.

2. [6 points] [1-3 sentences]
Describe session fixation, including an example scenario.

3. [6 points] [1-3 sentences]
Describe session hijacking, including an example scenario.

4. [14 points] [Short essay]
Describe CSRF, including an example scenario, possible defenses, and a comparison with the classic attack exploiting compilers, as discussed in class.

5. [18 points] [Short essay]
Describe SQL-injection attacks, including at least 3 example attack scenarios, each illustrating a different high-level type of SQL-injection attack, as discussed in class.

6. [10 points] [1 paragraph]
Describe the CIA classification of policies and its limitations.

7. [10 points]
Categorize the following policy, i.e., whether it is a property, safety, and/or liveness. Formally prove the correctness of your classification at the level of detail discussed in class.

$P = \{\{t^1, t^2, \ldots\} \mid \forall i, j, n, m: (\mathit{input}(n) \in t^i \wedge \mathit{output}(m) \in t^i \wedge \mathit{input}(n) \in t^j) \Rightarrow (\mathit{output}(m) \in t^j)\}$

8. [30 points]
Consider the following tables, which store the names of employees at a company and the departments in which they work. EID and DID are the primary keys.

Employees

EID	Name	DID
1621	Arnold	1
2673	Sara	2
3532	Kenneth	3
4213	Chris	3

Departments

DID	DName
1	Human Resources
2	Engineering
3	Finance

For each of the following tasks, write a single SQL statement to complete the task.

a) Make the Employees table.

b) Insert a new employee with an EID of 5432, named Carl, with a DID of 2.

c) Insert a new employee with an EID of 5 and a DID of 2 but whose name is not given.

d) Retrieve the names of all employees.

e) Retrieve all employees with an ‘r’ in their name.

f) Retrieve all employee name and department pairs, where each returned pair (E, D) corresponds to the department D employee E works in. Use a join clause.

g) Retrieve the names of all employees in the Finance department (by querying both the Employees and Departments tables).

h) Move Chris into the department that has a DID of 1.

i) Add an Address column to the Employees table.

j) Delete the Employees table.