CIS 6373: Foundations of Software Security [Spring 2024]
Test II

NAME: _____

Instructions:

1) This test is 7 pages in length.

2) You have 75 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. Responses will be graded as described on the syllabus. Respond at the level of detail discussed in class. Avoid using bullet points and enumerated lists.

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

1. [3 points] What are the 2023 CWE top 3 “most dangerous software weaknesses”? [1 sentence]

2. [2 points] Describe heterogeneity as it relates to computer security. [1 sentence]

3. [2 points] What is OWASP? [1 sentence]

4. [5 points] How can attackers circumvent stack canaries? [2-4 sentences]

5. [5 points] Explain XXE vulnerabilities. [2-4 sentences]

6. [5 points] Explain use-after-free vulnerabilities. [2-4 sentences]

7. [5 points] Explain deserialization-of-untrusted-data vulnerabilities. [2-4 sentences]

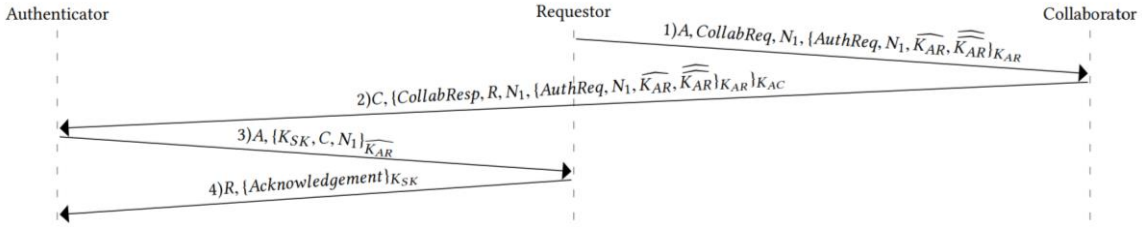
8. [5 points] Explain CSRFs. [2-4 sentences]

9. [6 points] [Short essay] Explain the primary data structures used to implement authorization, as discussed in class.

10. [9 points] [Short essay] How are passwords typically stored? Why? Hit all the main points discussed in class.

11. [13 points] [Essay] What are the primary properties enforced by cryptographic mechanisms, what does each of those properties mean, and which sorts of cryptographic mechanisms enforce each of those properties?

12. [20 points] [Essay] Explain the protocol shown below and the guarantees it provides.



13. [20 points]
(a) How are gray policies, gray properties, gray safety, and gray liveness defined?
(b) Formally state and prove the theorem that "trivial" is the only gray property that is both gray safety and gray liveness.