CS674 Secure Software Development

HW 2: Secure Design

**Name:**

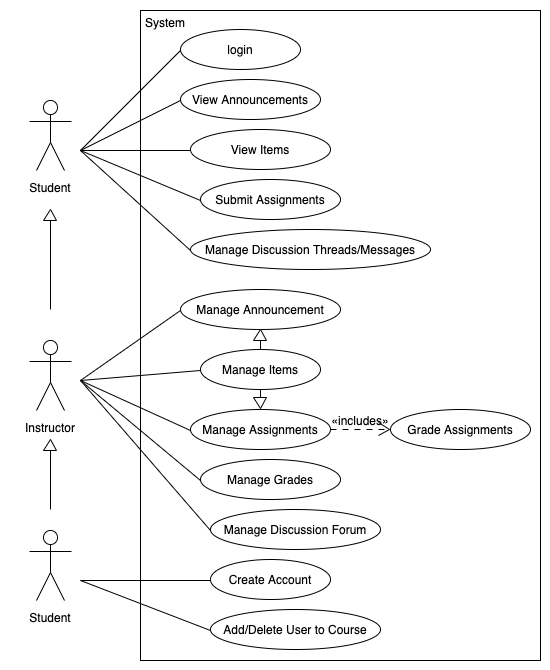
**Instructions:**

1. Please name your file as CS763\_yourusername\_hw2.
2. All questions must be answered on an INDIVIDUAL basis. If your answer is inspired by the discussion with other students, you need to mention their names in your acknowledgement section.
3. State clearly all your assumptions if anything is ambiguous. Always ask if you have any questions.
4. Please **correctly cite and list any (online) references. Please pay attention to the academic conduct code, particularly the definition of plagiarism**.
5. Please submit your homework through Blackboard on time.
6. Thank You!

**Questions (100%):**

1. Based on the use case diagram provided below for the blackboard system, identify 1 or more possible adversaries (as additional actors). Add 5 abuse cases that may threaten existing use cases and additional use cases that can mitigate these abuse cases. Make sure that a use case (or an abuse case) should be written as a short, active verb phrase that defines the goal of the use case. (Not the techniques used to achieve the goal. E.g. “SQL Injection” is not a good abuse case). (40%)

(The following use case diagram is created using UMLet. <http://www.umlet.com/umletino/umletino.html> You can import the attached file (BlackboardUseCases.uxf) in UMlet to modify the diagram if you want.



1. Choose one of the abuse cases you added in the above problem, and create an attack tree to show possible ways to achieve that goal. The attack tree should have at least 3 levels and 6 nodes. (30%)
2. Suppose we have the following simplified data flow diagram for the ProjectPortal project, focusing on the project data flow. Apply STRIDE on each of the following elements: project owner, general user, project data, web client, web server, database. Identify at least 6 possible threats and for each threat, propose 1 or 2 mitigations. (30%)

