Computer Systems Security / Computer Systems Security Lab
CS166 / CS162

Collaboration Policy

Spring 2019

Important: Please indicate your understanding and agreement to these course policies by completing this Google form: `https://goo.gl/forms/OadJIJHz6RhrGw7O2`. You will not receive any grades until we have your form response on file.

This document outlines the CS166 and CS162 policies regarding collaboration and the acceptable use of skills taught in this course. We expect that you read this document carefully and understand all of its concepts. Please consult with the course staff if you have any confusions about this policy. Assume that this policy applies unless otherwise specified by the assignment. **If you violate this policy, you may be subject to university disciplinary action.**

Collaboration Policies

Collaboration on Lecture Content

You may discuss material covered in lecture (and any associated readings) and high level concepts with anyone, including the course staff, students in the course, and others.

Collaboration on Homework

You may discuss homework problems with other students. However, you must write up your final solution independently. Once you start writing up your solutions, you may not discuss the homework with anyone except for the CS166/162 course staff. Also, you may not share your write-up with anyone.

Clinic is not exempt from this. You may not write anything while collaborating with other students: whiteboards are provided to allow for a temporary work space. You may not take pictures of whiteboards at clinic, nor walk away with any materials from collaboration sessions. Your time at clinic is meant to provide you with an understanding of the problem: you should then demonstrate that understanding by doing your write-up individually.

You may consult outside sources, but you must cite them, and you may only rely on outside sources for concepts, not for solutions to actual problems - all analysis must be your own. *Note: this has been adapted from the CS22 Collaboration Policy.*

Collaboration on Programming Projects

Course Staff You may discuss any aspect of the projects with the TAs or the Professors.

Current CS166/162 Students You should do your own thinking, your own design of attacks, and your own coding. You may consult with other students regarding technical issues about the languages, frameworks, or systems involved in the assignments, as long as the issues are narrow and do not help with the problem-solving process at large. You may help another student debug their code if they are stuck on a specific low-level problem that has been impeding progress on the work. In essence, you may not let yourself be led by another student to the extent that your task becomes significantly less challenging because of your

discussion with them. Finally, you may never copy code from another student, and you should be sure to protect your files using appropriate Linux permissions.

Outside Sources You may only consult outside sources to look up technical details about the languages, frameworks, or systems involved in the assignments, but you may not consult outside sources that describe specific attacks. You should never copy code from an outside source.

The following table summarizes the collaboration policy:

	CS166/162 Staff	**CS166/162 Students**	**Outside Sources**
Homeworks	May discuss any aspect	May discuss any aspect. However, you must write up your final solution independently.	May consult if cited. Analysis must be your own.
Programming Assignments	May discuss any aspect	May consult only for narrow questions about systems, languages, or frameworks involved as long as it does not help with the problem-solving process.	May consult outside sources to look up technical information about the languages, frameworks, or systems involved, but not about specific attacks.
Lecture Content	May discuss any aspect	May discuss any aspect	May consult

Piazza

CS166 and CS162 will be using Piazza to facilitate intra-course communication. When posting questions to Piazza, students must consider whether to post the question publicly or privately, as descriptive questions can disclose the solutions to the assignments. Please follow these guidelines when posting to Piazza:

- *Please post or answer publicly:* Misunderstandings of the assignment, clarifications about the requirements, bugs in the assignment spec or support code, small, specific questions about the languages, frameworks, or systems involved with an assignment that do not refer to any potential vulnerabilities.
- *Please post or answer privately:* More than a few lines of code, explanations of the attacks involved in your solutions, questions about your grade, etc.

Please use your best judgement when deciding whether to post publicly or privately. If you post privately, please let us know whether or not it would be OK to make the post public if we feel that it would be beneficial to the class.

Ethical and Legal Issues

Some of the techniques covered in this course for educational purposes are unethical and/or illegal to use and apply in contexts beyond the course itself. Breaking into, misusing, or harming computer systems or networks is illegal and punishable by law if done without the explicit authorization of the owner. There are various legal restrictions applicable to removing DRM protection from copyrighted content without prior authorization by the copyright owner. Attacking computers at Brown (whether owned by Brown or by others), except as specifically assigned in this course, is a violation of Browns Computer Policy and may lead to disciplinary action.