# ISEC 400 Homework 3

Answer the following questions based on your reading of the text book, any supplemental material, and the instructor’s presentation this week. If you use an external source (i.e. a web-page, the required textbook, or an additional book) to help you answer the questions then be sure to cite that source. Hint: you should probably always be citing a source.

## Questions

1. [5 points] Consider a small business employer who writes web application software for other small businesses. Their approach to security is to perform penetration testing before product release using tools such as Vega, OWASP ZAP, and w3af. When the tools find no more vulnerabilities, the owner ships the software and claim a high level of security for his products. Do you agree? Why or why not? What are the benefits and drawbacks to his approach? If you were running the business, what (if any) additional steps would you take and why?
2. [4 points] Consider the standard software development lifecycle contrasted against a secure software development lifecycle of your choice (e.g. SDL, BSIMM, OpenSAMM). What are the similarities in the lifecycles? What additional activities take place in a secure development lifecycle? Which, in your opinion, are the most critical additional activities and why?
3. [3 points] What is STRIDE and DREAD? How are the two related to one another? How are they used in a secure development context?
4. [8 points] Consider the scenario of user logging in to a web application for e-commerce. Using the Microsoft SDL Threat Modeling Tool (downloadable from <http://www.microsoft.com/en-us/download/details.aspx?id=2955>), do the following:
	1. Create a context diagram for the application
	2. Create a level 1 diagram for the login process
	3. Apply STRIDE to the data flows between the user and the login process *only* (or else you’ll spend too much time).
	4. Show your results from a-c above and explain what you learned through the process.

## Submission instructions

Create a Word document with your solution to the short answer questions. Submit the Word document to the dropbox for the course.