Homework 1 (Due: Nov. 18)

Submission Requirement:

- Your homework needs to be typed; handwritten submission will not be accepted.
- If you need to draw diagrams, you can hand-draw them, scan them (e.g. using your smartphone or digital camera), and insert them into your document.
- For on-campus students, you need to submit the hardcopy as well as the softcopy before the lecture starts on Nov. 18.
- For online students, you only need to submit a softcopy, but make sure that your submission is before 12:30pm on Nov. 18.
- No late homework will be accepted, because we will discuss the answers in class on Nov. 18. You will receive zero points if you don't submit the homework before I start my lecture on Nov. 18. The Blackboard's submission system will close on 12:30pm on Nov. 18, so nobody can submit after that.

Question 1: I have shown you that if mobile apps are written using the HTML5-based technologies (such as PhoneGap apps), they may be vulnerable to code injection attacks. For example, if you use such apps to scan a 2D barcode, you may be attacked. (1) Please describe why such attacks are possible? (2) Why the native apps (i.e., apps that are written using Java in Android and Object C in iOS) are immune to such attacks?

Question 2: What do the following attacks have in common?

- SQL Injection attack
- Cross-Site Scripting attack
- Attack on `system(command)`

Question 3: Why do the cross-site Ajax request need to be restricted, while the normal cross-site request needs not?

Question 4: Please watch the "ClickJacking" video from the following URL, and explain what the ClickJacking attack is:

- http://www.cis.syr.edu/~wedu/education/websec3.html (you only need to watch the ClickJacking section; the other sections are already covered in lectures).

Question 5: Please watch the "data integrity", "workflow", and "workflow attack" sections of the following video, and explain why stateless nature of the web has led to the data integrity and workflow problems. In your explanation, you need to explain why these are not problems in the traditional stateful client-server programs.

- http://www.cis.syr.edu/~wedu/education/websec2.html

Question 6: This is assigned in the lecture on Nov. 6. Describe how you can add the "disable" and "enable" functionalities to the file-descriptor's capability mechanism. Namely, if a process disables a file-descriptor capability, the process will not able to use the capability to access the corresponding file, until the process specifically enables the capability again. This is meant for discussing your concrete idea, and there is no need to implement it.