NES 755: Web Applications Security

Spring 2019

Instructor	-	Ahmed Shatnawi
Email	-	`ahmedshatnawi@just.edu.jo`
Class Hours	-	Tuesday 1:30-4:30
Office Hours	-	; anytime electronically; by appointment; after class

1 Overview and Goals

This class will provide the theory and practice of software security, focusing in particular on some common software security risks, including buffer overflows, race conditions and random number generation, and on the identification of potential threats and vulnerabilities early in the design cycle. The emphasis is on methodologies and tools for identifying and eliminating security vulnerabilities, techniques to prove the absence of vulnerabilities, and ways to avoid security holes in new software and on essential guidelines for building secure software: how to design software with security in mind from the ground up and to integrate analysis and risk management throughout the software life cycle.

2 Required Text

B. Chess and J. West. Secure Programming with Static Analysis. Addison-Wesley, 2007.
David A. Wheeler, Secure Programming HOWTO Version 3.71

3 Grading

Course letter grades will be determined later.

Course percentage grades are broken down into the following categories.

55% Research paper and presentation

The purpose of the research paper and presentation is to expose you to recent research in secure computing. The report will demonstrate the depth of your understanding of a chosen area of Web Secure. You will write a paper/conduct experiments that investigates recent research on the topic. If you choose to do a paper, it should be at least 10 pages long (excluding the reference list), and written using 11 or 12 point type, single-spaced, with 1 inch or 1.25 inch side margins and 1 inch top/bottom margins. You must cite the work you reference appropriately and include a bibliography (or ”references” section) that is formatted in a reasonable way. If you find a paper on the Web that you believe to have been published in a conference proceedings or journal, you must cite the conference proceedings or journal, not the Web page. Your paper must cite at least 8 papers total.

The paper should investigate in one of predefined ideas that covers a new way to think about the problem or a new design that might be an improvement of an existing ideas in the literature. It should discuss the research contributions have been made in enough detail that a reader who has completed this course is likely to understand the central ideas. The paper should analyze your results and try to integrate those ideas into a coherent summary of current state of the art and directions for future research.

[Date to be determined]You are required to submit a short (1/2 page) summary of exactly which topic you choose. Your half page summary should describe how you will limit or expand the scope of your paper. You will need to have looked at a number of relevant articles in order to see what interests you and what collection of articles would be a good basis for a coherent research report.

5% Quizzes

There will be several announced quizzes throughout the semester. Quiz content will focus on material presented in lecture the week prior. Missed quizzes can not be made up.

20% Assignments

There will be couple of exposing and analyzing assignments of web vulnerabilities. Assignments must be submitted to the eLearning and are be graded on correctness, clarity, and style.

20% Exams

You will have one midterm and one cumulative final (with a strong emphasis on the materials covered after the midterm). Exams will take place according to the department official exam schedules. Exam week lectures will be replaced by an ad-hoc review (you should come prepared with questions, or at the very least a vague sense of wonder).

10%	Midterm
10%	Final

4 Late Policy

Late homework will not be accepted.
Quizzes missed due to unforeseen and extreme circumstances may be made up *within the same week* my office hours.

5 Academic Misconduct

The university has a responsibility to promote academic honesty and integrity and to develop procedures to deal effectively with instances of academic dishonesty. Students are responsible for the honest completion and representation of their work, for the appropriate citation of sources, and for respect of others' academic endeavors. A more detailed description of Student Academic Disciplinary Procedures may be found at `www.just.edu.jo/Deanships/DeanshipofStudentsAffairs/Documents/Deanship%20of%20Students%20Affairs.doc`.

6 Cheating & Collaboration

All graded assignments must be your own work (your own words). For this course, verbal communication and collaboration using non-code text or hand-written code is not permitted.

Automatic copying of assignments (e.g. email, messaging, flash drive copies, printed hard copies, etc) is **strictly** forbidden. At the very least, you must write every word in your assignments. If you are unsure whether something is permitted, please check with me. If you turn in a program/document which is an electronic copy (or a minor variation of a copy) of other peoples work, then the source and people who give credit to the source will receive zero for the assignment, while those who do not give credit may be given an 'F' grade for the course.

7 In-Class Communication

Phone calls, text messages, instant messages, email, and web surfing are highly disruptive to other students and hence **not allowed** during class time. Technology devices may only be used for the class purposes (e.g. following slides) Violators will be asked to leave the room. If you anticipate a call that you simply have to take (yes, that happens), please sit near the door, put your phone on vibrate, and leave quietly at the appropriate time. If you are disrupted by another student's violation of this policy, please bring the matter to my attention.

8 Outline

This course outline is a "living document". It can be changed in response to events in the course. You will be notified if major changes are made.
The lectures will cover the key issues and explain some things that might not be clear otherwise. However, you are responsible for reading and understanding the material in the assigned readings (and not just knowing whats in the lectures). Note that there is a significant amount of reading, especially in the first half of the course; we then move into more specialized topics and application.

Topics

Computer Attack Overview
Input Validation
Buffer Overflows
Error Handling Privacy
Secrets, and Cryptography
Implementing Authentication and Access Control
Web Application Vulnerabilities
Secure Programming Best Practices
Static Code Analysis and Run-time Analysis
Virtual Machines, Usability [phishing], E-Voting, Privilege Separation, Java Security, Network Security & Worms