Secure Programming
——Course Introduction

胡天磊, Dr. HU Tianlei

Associate Professor

College of Computer Science, Zhejiang Univ.

htl@zju.edu.cn

Course Outline

- Objectives & Contents
- Topics & Materials
- Evaluation & Grading

Objectives

Introduce the concept of security in programming, especially in following 3 aspects:

- Principle of security in software design/implementation/testing
- Vulnerabilities in web application & practice of secure web programming
- Vulnerabilities in C / C++ application & practice of secure high-level language programming

Why to learn this course?

- To be a "true" programmer
- To understand why an application is vulnerable and how to exploit / fix it

Prerequisites

- You must know what is programming and how to program (in at least C programming language)
  - More programming experiences will help you more to learn this course
- You are not required to know how to do web programming
  - During the course and the lab, I will show you how to start
  - But, you should do a lot of after-class work if you want to get a better grade and/or to understand the secure web programming more
- You are not required to know the architecture of computer and the operation system
  - During the course and the lab, I will show you the elemental information
  - However, also you should do a lot of after-class work for a good grade and/or a more sophisticated understanding of security

Course Outline

Part 1. Introduction & Concepts **week 1**

- Introduction of the course
- Introduction of the software security

Part 2. Secure Web Programming **week 1-3**

- Introduction of the web programming
- Introduction of web app vulnerabilities and how to exploit/fix them
  - SQL injection & XSS

Part 3. Secure High-Level Language Programming **week 4-7**

- Introduction of C/C++ vulnerabilities and how to exploit / fix them
  - Buffer overflow & format string overflow
- Secure coding guide for C/C++
- The security model of Java/C#/JavaScript

Part 4. Principle & Practice to be More Secure **week 7-8**

- Introduction of secure software engineering

Course Outline (cont.)

This is a lab-intensive "programming" course, you need do a lot of lab work.

You can do the lab on-site / off-site, with the help of the course website.

Labs:

- Lab 1. Web Application Security — week 1 – 4 — 40 points
  - Setting up a Java web environment
  - Build the first Java web application, using HTML/CSS/JavaScript, JSP/Tomcat/MySQL
  - Using WebGoat to try exploit it and fix the vulnerabilities
- Lab 2. Buffer Overflow — week 4 – 7 — 40 points
  - Setting up a Linux VM environment
  - Build/Debug a C application using GCC / GDB
  - Try exploits and fix buffer overflow vulnerabilities
- Lab 3. Static Analysis — week 8 — 20 points
  - Using splint to analyze programs

Course Materials

- 《软件安全实现——安全编程技术》
  - 郭克华主编，清华大学出版社，2010.6.1
  - http://product.dangdang.com/20862469.html

- Text books are not required for this course.

Logistics & Contact

WEB: http://121.40.131.130/sec_prog_2021_summer

- 教师：胡天磊 / HU Tianlei
  - htl@zju.edu.cn
  - 13958091761
- 助教：王皓波 / WANG Haobo
  - wanghaobo@zju.edu.cn
  - 17816855125
- 助教：刘雨辰 / LIU Yuchen
  - liuyuchen0921@zju.edu.cn
  - 18066331397

Evaluation and Grading

- In Course 10 points
- Lab & Reports 90 points

About the Lab

Week 1 ~Week 4

- Lab 1.1 Web Environment Setup – Java & Tomcat & Eclipse, 5 points
- Lab 1.2 Implementation of Web Application, 10 points
- Lab 1.3 WebGoat Setup & Usage, 5 points
- Lab 1.4 Injection and XSS, 15 points
- Optional: Lab 1.5 Web Attack, 5 points bonus
- **2-3 Deliverables, Deadline: 2021.6.6 23:59:59**

Week 5 – Week 8

- Lab 2.1 Setting up Ubuntu Linux with VMWare Player, 10 points
- Lab 2.2 Running a Hello World Program in C using GCC, 10 points
- Lab 2.3 Buffer Overflow Vulnerability, 15 points
- Optional: Lab 2.4 Format String Vulnerability, 5 points bonus
- Lab 3.1 Using Splint for C Static Analysis, 10 points
- Lab 3.2 Using Eclipse for Java Static Analysis, 10 points
- **4-5 Deliverables, Deadline: 2021.7.4 23:59:59**

Follow the lab guide, and send your deliverables to TA (liuyuchen0921@zju.edu.cn) on time. You will get ZERO if late for 1 second, **I AM NOT KIDDING YOU**