UNSW CANBERRA | Cyber

Code Review

Location	UNSW Canberra
Duration	5 days
Standard Price	$4,550.00
Defence Price	$4,095.00

Description

This 5 day course will look at reviewing C/C++ code for security issues. The course is heavily based around practical auditing of actual C/C++ programs. Common coding bugs will be identified in set lectures and then students will apply the theory by reviewing real programs and identifying vulnerabilities. In addition to manual code review, automated means of vulnerability discovery will be briefly discussed, including fuzz testing and static analysis.

Topics covered include:

- C/C++ Programming Language
- Vulnerability discovery
- Dynamic Program Analysis
- C/C++ Bug Patterns
- Open Source OS Kernel Auditing
- Automating Code Review with Coccinelle
- Secure Coding

Learning Outcomes

On completion of this course, participants should be able to:

- Perform secure programming and identify potential flaws in codes to mitigate vulnerabilities.
- Understand the auditing and review process of technical systems using code analysis tools.
- Use security testing tools including ‘fuzzing’ static-analysis code scanning to perform code reviews.
- Perform secure program testing, review, and assessment to identify potential flaws in codes and mitigate vulnerabilities.
- Understand countermeasures and mitigations against potential exploitations of programming language weaknesses and vulnerabilities in systems and elements.

Who Should Attend

This course is aimed at technical staff. It is suitable for vulnerability researchers looking to discover bugs in C/C++ software. It is equally suitable for software developers aiming to improve the security of their code.

NICE Framework mapping

This course maps to the highlighted work categories:

Securely Provision | Oversee & Govern | Analyse | Investigate

Operate & Maintain | Protect & Defend | Collect & Operate

To find out more about the NICE Framework go to: niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework

Course Day Breakdown

Day 1

Review of C/C++ Programming Language

Day 1 starts off with a comprehensive review of C code language and commonly called functions. We'll then move onto basic Debugging Functions, Pointers, Strings and Arrays and Dynamic Memory management techniques.

Topics

Type and Variables, Control Flow, Functions, Bitwise Arithmetic, Debugging, GDB, Changing a Register, Types of Arrays, Dereferencing, Pointer Operations, Buffer Functions, Strings, Allocating Memory, Buffer Overflows, Calloc, Dynamic Data Structures.

Day 2

C/C++ Bug Patterns

The session will introduce the concept of fuzzing in order to find unique crashes and exploitable cases, followed by an in-depth discussion around Static Program Analysis and advantages and limitations of Symbolic Execution processes.

Topics

Dumb Fuzzing, Generative Fuzzing, Fuzzing Internals, Lexical Analysis, Parsing, Intermediate Representations, Control Flow Analysis, Data Flow Analysis, Compiler Optimisations, SMT, Symbolic Execution.

Day 3

C/C++ Bug Patterns cont.

Day 3 will delve into numerous examples of C Language Problems and Standard C Libraries. Unix APIs and Problems will be discussed and the day will conclude with an Introduction to Exploitation followed by several practical exercises.

Topics

Integers, Floating Point Numbers, printf, Stream IO, Tmpnam/ access, Pthreads, Strings, Common Unix and Linux APIs, Vulnerable Program, Stack Layouts.

Day 4

Open Source OS Kernel Auditing

The session will start with an overview of how to navigate the Linux Kernel and will also touch on Memory Bugs in OS Kernels and examine different types of OS Kernel Attack Surfaces.

Topics

Source Code Structure, Useful APIs, Memory Allocation, Memory Copying, File Systems, System Calls, Device Drivers.

Day 5

Secure Coding

The final day of the course will go over SMT Solving, Reverse Engineering and Code Review Strategies. Students will get to put their newly acquired skills and knowledge into practice through hands on exercises.

Topics

SMT-Lib, Z3, BitVectors, Small Programs, Large Programs, Symbol & Data Structure Recovery, Decompilation, Code Review.

"The course really opened my eyes to the real threats posed in cyber. Provided me the tools to conduct threat assessments and how to consider mitigation strategies."

Course participant

CRICOS No. 00098G • 337361580

UNSW Canberra Cyber

UNSW Canberra Cyber is a unique, cutting-edge, interdisciplinary research and teaching centre, working to develop the next generation of cyber security experts and leaders. The centre is based in Canberra at the Australian Defence Force Academy and provides professional, undergraduate and post graduate education in cyber security. Our air-gapped, state of the art cyber range offers a secure environment where we deliver a number of technical and highly specialised learning opportunities. Our courses are designed to give the next generation of cyber security professionals the skill sets needed to thrive in the industry. We can also create bespoke professional education programs tailored to your organisation's needs. Contact us at cyber@adfa.edu.au to discuss how.

Find out more

cyber@adfa.edu.au
unsw.adfa.edu.au/cyber