INFOSEC Skills

LIVE BOOT CAMPS

Get live, expert instruction from anywhere.

Secure Coding for C/C++ Boot Camp

Learn the most common programming bugs and their practical mitigation techniques through hands-on exercises that provide full understanding of the root causes of security problems.

Course description

Our Secure Coding in C/C++ Boot Camp covers typical C/C++ security programming bugs and common vulnerabilities. The root causes of the problems are explained through a number of easy-to-understand source code examples that depict how to find and correct the issues. The real strength of the training is the numerous hands-on exercises, which help you understand how easy it is for attackers to exploit these vulnerabilities.

The training also provides an overview of practical protection methods that can be applied at different levels (hardware components, operating systems, programming languages, the compiler, the source code or in production) to prevent the occurrence of various bugs, to detect them during development and before market launch, or to prevent their exploitation during system operation. Through exercises specially tailored to these mitigation techniques, you'll learn how simple it is to eliminate various security problems.

Who should attend

- » C / C++ developers
- » Designers and architects
- » Members or managers of the software development team
- » Anyone who wants to learn more about secure coding in C/C++

Boot camp at a glance

What you'll learn

- ✓ Basic concepts of IT security and secure coding
- ✓ How to identify and correct common programming bugs
- ✓ Architectural protection techniques and their weaknesses

Delivery methods

- ✓ Online
- ✓ Team onsite

Training duration

- ✓ Immediate access to Infosec Skills
- ✓ 2-day boot camp
- ✓ 90-day extended access to all boot camp materials

The hands-on cybersecurity training platform that moves as fast as you do

Infosec Skills boot camps are engineered to match the way today's cybersecurity professionals prefer to learn. In addition to days of live training from an experienced pro, you'll get unlimited access to 100s of additional hands-on cybersecurity courses and cyber ranges to help you advance your skills before, during and after your boot camp. Your Infosec Skills access extends 90 days past your boot camp, so you can take additional time to prepare for your exam, or get a head start on your next certification goal.

Start training immediately

Prepare for your boot camp with immediate access to the Infosec Skills on-demand training library.

Learn by doing in the cyber range

Put what you've learned into practice with 100s of browser-based labs and hands-on projects.

Get unlimited custom practice exams

Uncover knowledge gaps with unlimited practice exams attempts and skill assessments.

700+ IT and security courses

Earn CPEs and build new skills with 100s of additional training courses.

What's included

- Two days of expert, live Secure Coding for C/C++ training
- 100% Satisfaction Guarantee
- Free 90-day Infosec Skills subscription (access to 1,400+ additional courses and labs)
- 90-day extended access to all boot camp video replays and materials
- Hands-on cyber ranges and labs
- Knowledge Transfer Guarantee

Prerequisites

- Knowledge of C / C++ programming languages
- Familiarity with memory management
- Background in OS mechanisms

What you'll learn

This Secure Coding in C/C++ Boot Camp provides two days of training with a real C/C++ security expert. Our instructors have extensive C/C++ development experience as well as years of experience performing security code reviews. You will learn valuable knowledge and skills, including the ability to:

- Understand basic concepts of security, IT security and secure coding
- Realize the severe consequences of non-secure buffer handling
- Understand the architectural protection techniques and their weaknesses
- Learn about typical coding mistakes and how to avoid them
- Be informed about recent vulnerabilities in various platforms, frameworks and libraries

Hands-on exercises

This secure coding boot camp includes a number of easy-to-understand exercises that demonstrate live hacking. You'll learn to analyze vulnerable code snippets and carry out attacks against them in order to fully understand the root causes of certain security problems. All exercises are prepared in a plug-and-play manner by using a pre-set desktop virtual machine, which provides a uniform development environment.

Regularly updated training

Black hat hackers are always changing their tactics to get one step ahead of the good guys. We update our course materials regularly to ensure you learn about the latest C/C++ coding threats — and how to write secure code to prevent those threats.

Skill up and get certified, guaranteed

100% Satisfaction Guarantee

If you're not 100% satisfied with your training at the end of the first day, you may withdraw and enroll in a different online or in-person course.

Knowledge Transfer Guarantee

If an employee leaves within three months of obtaining certification, Infosec will train a different employee for free for up to one year.

What our students are saying

I really appreciate that our instructor was extremely knowledgeable and was able to provide the information in a way that it could be understood. He also provided valuable test-taking strategies that I know not only helped me with this exam, but will help in all exams I take in the future.

Michelle Jemmott

Pentagon

Excellent! Our instructor had a vast background and related the materials to real life. Much better than just teaching the materials to pass an exam ... but he did that as well. He went out of his way in class. The extra materials really benefited us when we returned to our real jobs! Great experience!

John Peck

EPA

Very impressed with Infosec. My instructor did a great job delivering the information strategically and in a way for all to understand. I would definitely take another class/certification prep course.

Sylvia Swinson

Texeltek

The instructor was able to take material that prior to the class had made no sense, and explained it in real-world scenarios that were able to be understood.

Erik Heiss

United States Air Force

The course was extremely helpful and provided exactly what we needed to know in order to successfully navigate the exam. Without this I am not confident I would have passed.

Robert Caldwell

Salient Federal Solutions

Secure Coding for C/C++ details

Our instructors give you 100% of their time and dedication to ensure that your time is well spent. You receive an immersive experience with no distractions! The typical daily schedule is:

	Day 1	Day 2
Morning session	IT security and secure coding	Common coding errors and vulnerabilities
Afternoon session	Security relevant C/C++ programming bugs and flaws Buffer overflow	Advice and principles Knowledge sources
Evening session	Optional group & individual study	Optional group & individual study

Schedule may vary from class to class

Before your boot camp

Start learning now. You'll get immediate access to all the content in Infosec Skills, including an in-depth boot camp prep course, the moment you enroll. Prepare for your live boot camp, uncover your knowledge gaps and maximize your training experience.

During your boot camp

Day 1

IT security and secure coding

- Nature of security
- IT security related terms
- Definition of risk
- IT security vs. secure coding
- From vulnerabilities to botnets and cybercrime
  - Nature of security flaws
  - Reasons of difficulty
  - From an infected computer to targeted attacks
- Classification of security flaws
  - Landwehr's taxonomy
  - The Fortify taxonomy
  - The Seven Pernicious Kingdoms
  - OWASP Top Ten

Security relevant C/C++ programming bugs and flaws

- Exploitable security flaws
- Protection principles
  - Specific protection methods
  - Protection methods at different layers
  - The PreDeCo matrix of software security
- x86 machine code, memory layout, stack operations
  - Main registers
  - Most important instructions
  - Flags
  - Control instructions
  - Stack handling and flow control

- The memory address layout
- The function calling mechanism in C/C++ on x86
- Calling conventions
- The local variables and the stack frame
- Function calls
- Prologue and epilogue of a function
- Stack frame of nested calls
- Stack frame of recursive functions

Buffer overflow

- Stack overflow
  - Buffer overflow on the stack
    - Overwriting the return address
    - Exercise BOFIntro
    - Exercise BOFShellcode
  - Protection against stack overflow
    - Stack overflow – prevention (during development)
    - Stack overflow – detection (during execution)
  - Stack smashing protection
    - Stack smashing protection variants
    - Stack smashing protection in GCC
    - Exercise BOFShellcode
    - Effects of stack smashing protection
    - Bypassing stack smashing protection – an example
  - Address Space Layout Randomization (ASLR)
    - Stack randomization with ASLR
    - Using ASLR
    - Circumventing ASLR: NOP sledding
    - Exercise BOFASLR
    - Circumventing ASLR with NOP sledging
  - Non executable memory areas – the NX bit
    - Protection through virtual
    - memory management
    - Access control on memory segments
    - The Never eXecute (NX) bit
    - Exercise BOFShellcode – enforcing NX memory segments
    - Return-to-libc attack – circumventing the NX bit
    - Arc injection / return-to-libc attack
    - Multiple function calls with return-to-libc
  - Return oriented programming (ROP)
    - Exploiting with ROP
    - ROP gadgets
    - Combining the ROP gadgets
    - Exercise BOFROP
- Heap overflow
  - Memory allocation managed by a doubly-linked list
  - Buffer overflow on the heap
  - Steps of freeing and joining memory blocks
  - Freeing allocated memory blocks
  - TLS Heartbeat Extension
  - Heartbleed – a simple explanation
  - Heartbleed – fix in v1.0.1g
  - Protection against heap overflow

Day 2

Common coding errors and vulnerabilities

- Input validation
  - Input validation concepts
  - Integer problems
  - Representation of negative integers
  - Integer ranges
  - Integer representation by using the two's complement
  - The integer promotion rule in C/C++
  - Arithmetic overflow – spot the bug!
  - Exercise IntOverflow
  - So why ABS(INT_MIN)==INT_MIN?
  - Signedness bug – spot the bug!
  - Widthness integer overflow – spot the bug!
  - A case study – Android Stagefright
  - Stagefright – a quick introduction
  - Some Stagefright code examples – spot the bugs!
  - Integer problem mitigation
  - Avoiding arithmetic overflow – addition
  - Avoiding arithmetic overflow – multiplication

- Dealing with signed/unsigned integer promotion
- Safe integer handling in C
- The SafeInt class for C++
- Printf format string bug – exploitation
- Exercise Printf
- Printf format string exploit – overwriting the return address
- Mitigation of printf format string problem
- Some otherinput validation problems
- Array indexing – spot the bug!
- The Unicode bug
- Directory Traversal Vulnerability
- Shellshock – basics of using functions in bash
- Shellshock – vulnerability in bash
- Exercise – Shellshock
- Shellshock fix and counterattacks
- Exercise – command override with environment variables
- Improper use of security features
- Problems related to the use of security features
- Insecure randomness
- Week PRNGs in C
- Stronger PRNGs in C and Linux
- Hardware-based RNGs
- Password management
- Exercise – Google cracking
- Password management and storage
- Special purpose hash algorithms for password storage
- BDKDF2 and bcrypt implementations in C/C++
- Some other typical password management problems
- Improper error and exception handling
  - Typical problems with error and exception handling
  - Empty catch block
  - Overly broad catch
  - Exercise ErrorHandling – spot the bug!
- Time and state problems
  - Time and state related problems
  - Serialization errors (TOCTTOU)
  - Attacks with symbolic links
  - Exercise TOCTTOU
- Code quality problems
  - Dangers arising from poor code quality
  - Poor code quality – spot the bug!
  - Unreleased resources
  - Type mismatch – spot the bug!
  - Exercise TypeMismatch

Advice and principles

- Matt Bishop's principles of robust programming
- The security principles of Saltzer and Schroeder

Knowledge sources

- Vulnerability databases
- Secure coding sources – a starter kit

After your boot camp

Your Infosec Skills access extends 90 days past your boot camp, so you can take additional time to prepare for your exam, get a head start on your next certification goal or start earning CPEs.

About Infosec

Infosec's mission is to put people at the center of cybersecurity. We help IT and security professionals advance their careers with skills development and certifications while empowering all employees with security awareness and phishing training to stay cyber-safe at work and home. Learn more at infosecinstitute.com.