INFOSEC Skills
LIVE BOOT CAMPS

Get live, expert instruction from anywhere.

Mobile and Web Application Penetration Testing Boot Camp

Learn how to conduct penetration tests on mobile and web applications! This boot camp goes in-depth into the tools and techniques used to exploit and defend web and mobile apps with a combination of hands-on labs and expert instruction.

Course description

Infosec's Mobile and Web Application Penetration Testing Boot Camp is a practical, hands-on training focused on teaching you the skills, tools and techniques required for conducting comprehensive security tests of mobile devices and web applications.

You'll learn the secrets of mobile and web app penetration testing in an immersive environment, including exploiting and defending web and mobile apps, performing static and dynamic analysis of iOS and Android apps using popular tools, finding vulnerabilities in source code, exploiting weaknesses in the implementation of mobile security controls and more. The boot camp also prepares you to earn the Certified Mobile and Web Application Penetration Tester (CMWAPT) certification.

Who should attend

- Penetration testers
- Application developers
- Web administrators
- Security analysts

Boot camp at a glance

Hands-on training

- Build your skills with dozens of hands-on labs
- Set up a pentesting platform and discover vulnerabilities
- Exploit web applications and iOS and Android devices

Delivery methods

- Online
- In person
- Team onsite

Training duration

- Immediate access to Infosec Skills
- 5-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

- 5 days of expert, live pentesting training
- Exam Pass Guarantee
- Exam voucher
- Unlimited practice exam attempts
- 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
- Onsite proctoring of exam
- Pre-study learning path
- Knowledge Transfer Guarantee

Prerequisites

Familiarity with penetration testing concepts and at least one year in an information security role, or equivalent experience, is recommended.

Hands-on labs

Get hands-on penetration testing experience in our cloud-hosted lab environment. Typical labs consist of an app demonstrating a vulnerability commonly found in a Web or mobile app. You'll learn how to assess the app like a black hat hacker and exploit the app to demonstrate the true risk of the vulnerability to the app owner. This can involve taking control of the app itself, downloading data the app stores or using the app as a launching pad to attack unsuspecting visitors with a malicious script. You'll also learn remediation steps so that the app owner can properly close the security hole.

What you'll learn

- Web application pentesting
- iOS exploitation
- Android exploitation

Industry-leading exam pass rates

Infosec's courseware materials are always up to date and synchronized with the latest CMWAPT exam objectives. Our industry-leading curriculum and expert instructors have led to the highest pass rates in the industry. More than 93% of Infosec students pass their certification exams on their first attempt.

Learn from experts

We don't just have great instructors, our instructors have years of industry experience and are recognized as experts. Over the past 15 years, we've helped tens of thousands of students get certified and advance their careers.

Skill up and get certified, guaranteed

Exam Pass Guarantee

If you don't pass your exam on the first attempt, get a second attempt for free. Includes the ability to re-sit the course for free for up to one year.

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

Mobile and Web Application Penetration Testing 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	Day 3	Day 4	Day 5
Morning session	Web application (in)security Understanding HTTP protocol	Exploiting web app vulnerabilities (i)	Getting started with iOS pentesting Static and dynamic analysis of iOS apps	Reversing iOS apps Securing iOS apps	Exploiting Android apps
Afternoon session	Web app pentesting tools Finding weaknesses in web apps	Exploiting web app vulnerabilities (ii) Securing web apps	Exploiting iOS applications	Understanding Android architecture Reversing Android apps	Take CMWAPT exam
Evening session	Optional group & individual study	Optional group & individual study	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

Part 1 - Web application pentesting

Module 1

- Web application (in)security
- Setting up a web application pentesting platform
- Installing vulnerable apps
- Burp Suite basics
- Analyzing traffic over HTTP
- Analyzing traffic over HTTPs

Module 2

- Understanding the HTTP protocol
- HTTP headers
- Attacking HTTP basic & digest authentication
- Conducting a brute-force attack

Module 3

- Analyzing the attack surface
- Information gathering
- Finding hidden URLs with dirbuster
- Identifying weak SSL certificates

Module 4

- Cross-site scripting (XSS) — reflected, stored and DOM based
- HTML injection
- Broken authentication and session management
- Insecure direct object references cross-site request forgery (CSRF)

- Insufficient transport layer protection
- Unvalidated redirects and forwards
- Cross origin resource sharing
- Command injection vulnerabilities
- Local file inclusion vulnerability
- Remote file inclusion vulnerability
- Insecure direct object reference
- HTTP response splitting
- SQL injection
- Attaching session management
- HTTP response header injection
- Improper exception handling
- Server side code disclosure
- Chaining XSS with other attacks
- Targeting reset password functionality
- Business logic flaws

Module 5

- Securing Web apps
- Applying input validation
- IP whitelisting
- Implementing access controls
- Removing HTTP headers
- Preventing CSRF with tokens
- Setting login limits
- Removing server configuration errors
- Identifying and fixing business logic issues

Part 2 - iOS exploitation

Module 1

- iOS security model
- App signing, sandboxing and provisioning
- Setting up XCode 9
- Changes in iOS 11
- Primer to iOS 10 security
- Exploring the iOS filesystem
- Intro to Objective-C and Swift
- What's new in Swift 4?
- Setting up the pentesting environment
- Jailbreaking your device
- Cydia, Mobile Substrate
- Getting started with Damn Vulnerable iOS app
- Binary analysis
- Finding shared libraries
- Checking for PIE, ARC
- Decrypting IPA files
- Self signing IPA files

Module 2

- Static Analysis of iOS applications
- Dumping class information
- Insecure local data storage
- Dumping Keychain
- Finding URL schemes
- Dynamic Analysis of iOS applications
- Cycript basics
- Advanced Runtime Manipulation using Cycript
- Method Swizzling
- GDB basic usage
- Modifying ARM registers

Module 3

- Exploiting iOS applications
- Broken cryptography
- Side channel data leakage
- Sensitive information disclosure
- Exploiting URL schemes
- Client side injection
- Bypassing jailbreak, piracy checks
- Inspecting Network traffic
- Traffic interception over HTTP, HTTPs
- Manipulating network traffic
- Bypassing SSL pinning

Module 4

- Introduction to Hopper
- Disassembling methods
- Modifying assembly instructions
- Patching app binary
- Logify

Module 5

- Securing iOS applications
- Where to look for vulnerabilities in code?
- Code obfuscation techniques
- Piracy/jailbreak checks
- iMAS, Encrypted Core Data

Part 3 - Android exploitation

Module 1

- Why Android
- Intro to Android
- Android security architecture
- Android application structure
- Signing Android applications
- ADB — non root
- Rooting Android devices
- ADB — Rooted
- Understanding Android file system
- Permission model flaws

Module 2

- Understanding Android components
- Introducing Android Emulator
- Introducing Android AVD

Module 3

- Proxying Android traffic
- REverse engineering for Android apps
- Smali labs for Android
- Dex analysis and obfuscation
- Android app hooking

Module 4

- Attack surfaces for Android applications
- Exploiting local storage
- Exploiting weak cryptography
- Exploiting side channel data leakage
- Root detection and bypass
- Exploiting weak authorization mechanism
- Identifying and exploiting flawed broadcast receivers
- Identifying and exploiting flawed intents
- Identifying and exploiting vulnerable activity components
- Exploiting backup and debuggable apps
- Dynamic analysis for Android apps
- Analysing ProGuard, DexGuard and other obfuscation techniques

Module 5

- Exploitation using Drozer
- Automated source code analysis
- Exploiting Android embedded applications

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.

INFOSEC