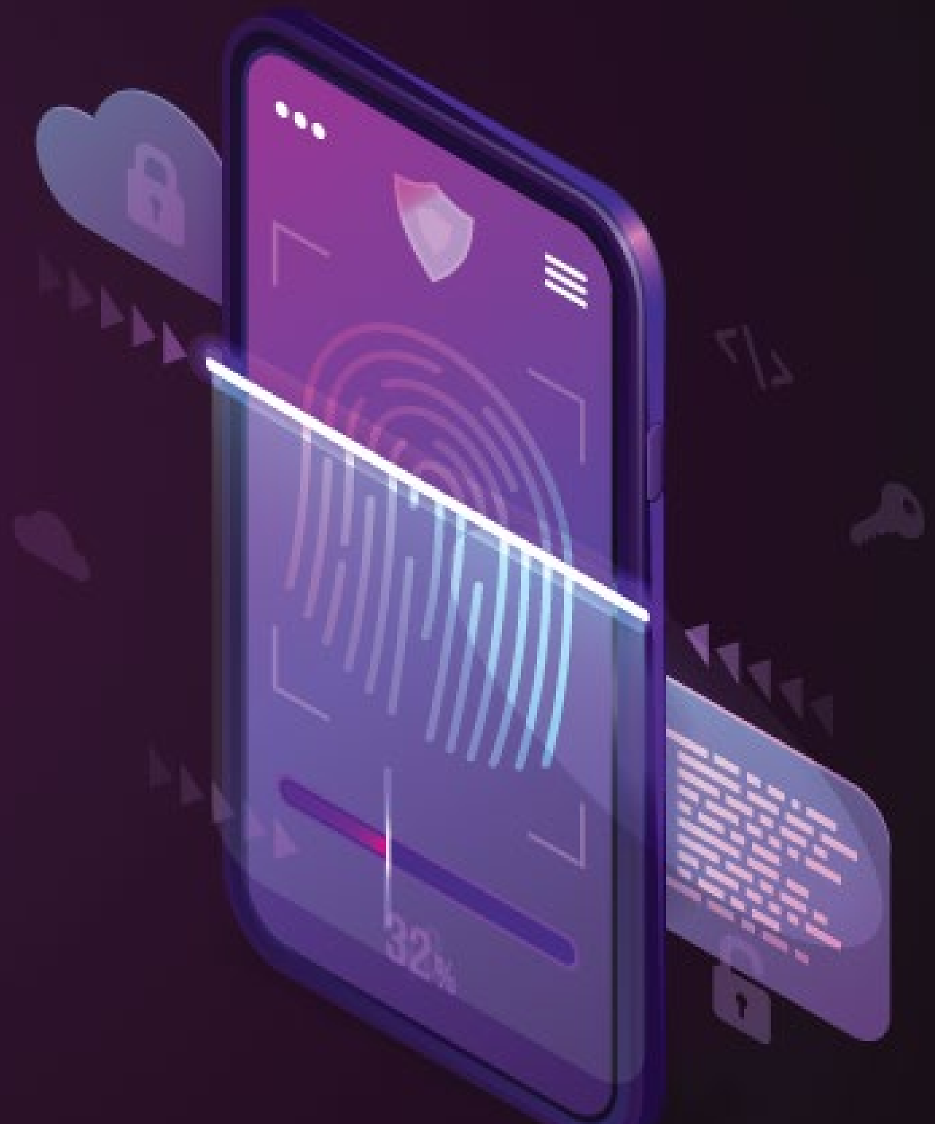
CRAW
ACADEMY

Mobile Pentest 667

Crack the Code, Secure the Device, Your Ultimate Guide to Mobile Pen Testing



Mobile Penetration testing

☎ +91 951 380 5401
training@craw.in
https://www.craw.in

Table of **Content:**

Program **Overview:**

The Mobile Application Security Course with AI offered by Craw Security is designed to equip participants with the knowledge and skills required to secure mobile applications against cyber threats. The course covers a wide range of topics, including mobile application architecture, security best practices, and vulnerability assessment.

Program **Features:**

- ✓ 60 hours of instructor-led training or Live VILT classes.
- ✓ Full implementation of AI fundamentals throughout the course curriculum.
- ✓ Accredited by the FutureSkills Prime, Approved by the Government of India.
- ✓ The course will be in both English and Hindi mediums.
- ✓ Learn from Industry-leading experts with extensive experience in network administration and security.
- ✓ Hands-on practical exercises to learn with real-time problem-solving scenarios.
- ✓ Real-world case studies and practical exercises.
- ✓ Interactive sessions and group discussions.
- ✓ Complete job placement assistance.
- ✓ Cutting-edge curriculum to stay at the forefront of the networking domain.
- ✓ Access Comprehensive course material, resources, and live sessions through both online and offline modes to suit your learning preferences.

Delivery **Mode:**

Online Bootcamp / Offline Classroom Training / Corporate Training Facility

Prerequisites of **Mobile Penetration Testing:**

Participants are required to have a basic understanding of cybersecurity concepts and mobile application development.

Target **Audience:**

- ✓ IT professionals,
- ✓ Students and recent graduates aiming to build a career in IT and mobile app security domain.
- ✓ Professionals from other fields seeking to transition into IT and mobile application security roles.
- ✓ Mobile application developers with a curiosity about how mobile application systems work and how to manage
- ✓ Anyone who is interested in securing mobile applications.

Key Learning **Outcomes:**

This Mobile Application Security Course with AI will help you:

- ✓ **Understanding Mobile Application Security Concepts:** Participants will gain a comprehensive understanding of the key concepts and principles of mobile application security, including common threats and vulnerabilities.
- ✓ **Identifying and Mitigating Security Vulnerabilities:** Participants will learn how to identify and mitigate common security vulnerabilities in mobile applications, such as insecure data storage, insufficient authentication, and improper session handling.
- ✓ Introduction of AI in Mobile App Security Technology: Learners will hone their current mobile application security knowledge with the basics of AI throughout the course curriculum wherever it can be implemented by highly trained instructors.

- ✓ **Implementing Best Practices:** Participants will learn best practices for securing mobile applications, including secure coding practices, encryption techniques, and secure communication protocols.
- ✓ **Conducting Vulnerability Assessments and Penetration Testing:** Participants will learn how to conduct vulnerability assessments and penetration testing on mobile applications to identify and address security weaknesses.
- ✓ **Mobile Device Management (MDM):** Participants will learn about mobile device management (MDM) solutions and how they can be used to enhance the security of mobile applications and devices.
- ✓ **Security Compliance and Regulations:** Participants will gain an understanding of security compliance requirements and regulations relevant to mobile applications, such as GDPR and HIPAA.
- ✓ **Security Incident Response:** Participants will learn how to respond to security incidents involving mobile applications, including incident detection, analysis, and mitigation.
- ✓ **Secure Development Lifecycle:** Participants will learn about the secure development lifecycle (SDLC) for mobile applications and how to integrate security into every phase of the development process.
- ✓ **Mobile Application Security Best Practices:** Participants will learn and apply best practices for securing mobile applications, including secure coding, secure authentication, secure data transmission, and secure storage.
- ✓ **Secure Mobile Application Deployment:** Participants will learn about secure deployment strategies for mobile applications, including app signing, app distribution, and app monitoring.

Certification **Alignment:**

Our Mobile Application Security Course with AI is genuinely accredited to the FutureSkills Prime, a MeitY — NASSCOM, Digital Skilling Initiative, and approved by the Government of India. Moreover, Craw Security is a proud partner of FutureSkills Prime. Learners will get this certificate from FutureSkills Prime after participating in a dedicated exam.

Certification **Details & Criteria:**

Upon successful completion of the course and passing the examination, participants will receive a certification from Craw Security. The examination assesses the participant's ability to apply Mobile Application Security techniques in a controlled environment. Specific criteria for certification include practical assessments and a theoretical exam.

About the **Exam:**

- ✓ **Number of Questions:** 30-35 Questions
- ✓ **Exam Test Duration:** 1 Hour
- ✓ **Exam Provider:** FutureSkills Prime
- ✓ **Test Format:** Multiple Choice Question (MCQ)
- ✓ **Exam Cost:** 600 Inclusive Taxes

Craw Security **Certification Criteria:**

- ✓ Attend 75% of classes and obtain 50% marks in the corresponding examination.
- ✓ Please note that there is an additional fee for the FutureSkills Prime exam related to this course.

100% Placement with **1 Year Cyber Security Course***

There is a specialized set of Terms and Conditions for a 100% Placement with our 1 Year Cybersecurity Diploma that needs to be fulfilled by every student who is willing to benefit from features from Craw Security. However, we have jotted down all the necessary T&Cs that need to be completed to take advantage of 100% Placement Assistance from the Department of Training & Placement by Craw Security:

- ✓ Attendance of 75% should be mandatory.
- ✓ Marks for internal exams should be 80% mandatory.
- ✓ Fees for 1 Year Cybersecurity Diploma Course should be properly paid.
- ✓ Candidate can apply for a job after completion of 6 modules.
- ✓ A candidate is applicable for Mock Interviews/PD Class after completion of 3 modules.

- ✓ Global certifications are required, if needed by companies for jobs.
- ✓ Candidate should be Graduate/Pursuing.
- ✓ One-time job Assistance/Placement will be provided, if the candidate misses any interview, Craw Placement Cell will not be liable to re-arrange the interview, and also Craw Academy will not be liable for any refund or future litigations or claims.
- ✓ Package as per candidate's skills or according to company norms.
- ✓ Ideal Candidates can apply for multiple jobs.
- ✓ The Post Placement Process will be provided by the Placement Cell, highly known as the Department of Training and Placement, which is as follows:
  1. Documentation
  2. Offer Letter
  3. Joining Date/ Timeline of Joining

What to Choose After this **Course:**

A person can choose the 1 Year Cybersecurity Diploma Course after the completion of this course or even switch the current course to this 12-course bundle of 1 Year Cybersecurity Diploma Course by Craw Security whose maximum courses are accredited to the FutureSkills Prime, a MeitY — NASSCOM, Digital Skilling Initiative, and approved by the Government of India. After doing this course, a person would be eligible to choose from a variety of options for a fruitful professional career in the long run.

Course **Curriculum:**

Module 01: Introduction to Mobile Penetration Testing

- ✓ Lesson 01: Scope
- ✓ Lesson 02: Methodology
- ✓ Lesson 03: Tools

Module 02: Lab Setup

- ✓ Lesson 01: Kali lab setup
- ✓ Lesson 02: Burp suite setup
- ✓ Lesson 03: Mobile penetration testing lab setup

Module 03: Android Architecture

- ✓ Lesson 01: Layers of Android architecture
- ✓ Lesson 02: Key Components
- ✓ Lesson 03: Application lifecycle
- ✓ Lesson 04: Security Model

Module 04: ApI File structure

- ✓ Lesson 01: Core components
- ✓ Lesson 02: Common file structure patterns
- ✓ Lesson 03: File structure example

Module 05: Reversing App with Apktool

- ✓ Lesson 01: Overviews
- ✓ Lesson 02: Functionality
- ✓ Lesson 03: Installation
- ✓ Lesson 04: Usage
- ✓ Lesson 05: Common usage case

Module 06: Reversing App with MobSf

- ✓ Lesson 01: Overviews
- ✓ Lesson 02: Functionality
- ✓ Lesson 03: Installation and setup
- ✓ Lesson 04: Feature and Capabilities
- ✓ Lesson 05: Scan the app with mobsf

Module 07: Static Analysis with AI

- ✓ Lesson 01: Types of static analysis
- ✓ Lesson 02: Tools and techniques
- ✓ Lesson 03: Benefits
- ✓ Lesson 04: How to perform static analysis

Module 08: Scanning Vulnerability with Drozer

- ✓ Lesson 01: Overviews
- ✓ Lesson 02: Dynamic analysis
- ✓ Lesson 03: Injection attacks
- ✓ Lesson 04: Exploitation

Module 09: Improper Platform Usage

- ✓ Lesson 01: Definition
- ✓ Lesson 02: attacks
- ✓ Lesson 03: Impact
- ✓ Lesson 04: Mitigation
- ✓ Lesson 05: Tools and resources

Module 10: Insecure Data Storage

- ✓ Lesson 01: Definition
- ✓ Lesson 02: Storing passwords in plain text
- ✓ Lesson 03: Unprotected databases
- ✓ Lesson 04: Impact
- ✓ Lesson 05: Mitigation
- ✓ Lesson 06: Tools and resources

Module 11: Insecure Communication

- ✓ Lesson 01: Definition
- ✓ Lesson 02: Unencrypted protocols
- ✓ Lesson 03: Missing or misconfigured SSL/TLS
- ✓ Lesson 04: Impact
- ✓ Lesson 05: Mitigation
- ✓ Lesson 06: Tools and resources

Module 12: Insecure Authentication

- ✓ Lesson 01: Definition
- ✓ Lesson 02: Weak password policies
- ✓ Lesson 03: Lack of multi-factor authentication
- ✓ Lesson 04: Impact
- ✓ Lesson 05: Mitigation
- ✓ Lesson 06: Tools and resources

Module 13: Insufficient Cryptography

- ✓ Lesson 01: Common vulnerability
- ✓ Lesson 02: Impact
- ✓ Lesson 03: Prevention and Mitigation
- ✓ Lesson 04: Continuous monitoring and updates

Module 14: Insecure Authorization

- ✓ Lesson 01: Common vulnerability
- ✓ Lesson 02: Impact
- ✓ Lesson 03: Prevention and Mitigation

Module 15: Client Code Quality

- ✓ Lesson 01: Important of client code quality
- ✓ Lesson 02: Code structure and Organization
- ✓ Lesson 03: Readability and Maintainability

Module 16: Code Tampering

- ✓ Lesson 01: Objective
- ✓ Lesson 02: Techniques
- ✓ Lesson 03: Detection and Prevention
- ✓ Lesson 04: Implications

Module 17: Reverse Engineering

- ✓ Lesson 01: Purpose
- ✓ Lesson 02: Techniques
- ✓ Lesson 03: Tools
- ✓ Lesson 04: Reversing Malware

Module 18: Extraneous Functionality

- ✓ Lesson 01: Security risks
- ✓ Lesson 02: User Experience (UX) issues
- ✓ Lesson 03: Code review and refactoring
- ✓ Lesson 04: Automated Analysis tools

Module 19: SSL Pinning

- ✓ Lesson 01: Public key Pinning
- ✓ Lesson 02: Certificate Pinning
- ✓ Lesson 03: Benefits of SSL pinning
- ✓ Lesson 04: Certificate Authority (CA)

Module 20: Intercepting the Network Traffic

- ✓ Lesson 01: Packet Capture
- ✓ Lesson 02: Network sniffing
- ✓ Lesson 03: Protocol Analysis
- ✓ Lesson 04: Traffic Decryption

Module 21: Dynamic Analysis

- ✓ Lesson 01: Introduction to Dynamic Analysis
- ✓ Lesson 02: How to perform dynamic analysis
- ✓ Lesson 03: Dynamic Debugging

- ✓ Lesson 04: Dynamic Decomplication

Module 22: **Report Preparation using AI**

- ✓ Lesson 01: Consider the objective of the report
- ✓ Lesson 02: The test compiles a comprehensive report
- ✓ Lesson 03: Detailing their findings of vulnerability

Module 23: **IOS Penetration: Basics**

- ✓ Lesson 01: Introduction to IOS Penetration testing
- ✓ Lesson 02: IOS structure
- ✓ Lesson 03: How to secure you application

Module 24: **Report Writing**

- ✓ Lesson 01: Proof of Concept (POC)
- ✓ Lesson 02: Executive and Management Report
- ✓ Lesson 03: Technical Report For IT and security Department

About **us:**

Craw Security is India's leading cybersecurity training institute, dedicated to developing the next generation of cybersecurity professionals. With a focus on practical, hands-on training, we offer a wide range of courses tailored to all skill levels. Our mission is to enhance the cybersecurity posture of individuals and organizations worldwide.

For more information, please visit our course page website:
https://www.craw.in/mobile-application-security-course-in-delhi/

Contact **us:**

Craw Cyber Security Private Limited, India (Head Office)

1st Floor, Plot no. 4, Lane no. 2, Kehar Singh Estate, Westend Marg, Behind Saket Metro Station,
Said-ula-jab, New Delhi – 110030, India

Email id: training@craw.in | info@craw.in
Contact Number: +91 9513805401
Connect on WhatsApp: +91 8448897124

Visit our website: www.craw.in | www.crawsecurity.com
Get Latest Cyber Security updates: www.nesw4hackers.com

Connect on Social media

Facebook: https://www.facebook.com/CrawSec/
Twitter: https://twitter.com/crawsec
YouTube: https://www.youtube.com/c/crawsecurity
LinkedIn: https://www.linkedin.com/company/crawsec

Join Our Community

WhatsApp Channel: Join Whatsapp Channel
Twitter: Join Twitter Channel