

# DEMYSTIFYING ANDROID APP SECURITY

The course delves into the Security Analysis of critical security flaws prevalent in Android app development, emphasizing the importance of robust security practices. Participants will explore common vulnerabilities as identified by OWASP Top 10 and MASVS covering areas such as reverse engineering, improper platform usage, insecure communication, and insufficient cryptography.



## Objectives

- **Set Up an Android Analysis Environment:** Equip participants with the necessary tools and knowledge to establish a comprehensive analysis environment for examining Android applications.
- **Understand Android Application Fundamentals:** Provide a foundational understanding of Android applications, covering the essential concepts needed for security analysis.
- **Learn Basic Principles of Android Secure Coding Practices:** Introduce participants to the basic principles of Android security, including common vulnerabilities and threats.
- **Reverse Engineering Android Apps:** Guide participants through the process of reverse engineering Android applications, even with little to no prior knowledge in the field.
- **Apply Security Analysis Techniques:** Enable participants to apply various techniques for analyzing and securing Android applications, preparing them for more advanced security challenges.



## Expected Outcomes

- **Establishment of Security Analysis Environment and Secure Coding Practices:** Participants will have successfully set up a complete environment for analyzing Android applications.
- **APK Analysis Skills:** Participants will acquire the skills needed to analyze APK files and assess their security.
- **Enhanced Security Awareness:** Participants will be equipped with the knowledge to identify and understand basic security vulnerabilities in Android apps.

## Duration

**5 days**

- **2 Days:** Essentials Module Self-Paced Online
- **2 Days:** Physical
- **1 Day:** CTF/Hackathon

## Dates

- **Start Date:** 2<sup>nd</sup> December 2024
- **End Date:** 6<sup>th</sup> December 2024

## Participant Prerequisites

- Basic understanding of Android app development and familiarity with Android Studio.
- Knowledge of Java or Kotlin programming languages.
- Awareness of general cybersecurity concepts, including encryption, authentication, and secure communication.

## Modules/Topics to be Covered

- Introduction to Android Apps
- Setting up of Android Pentesting Environment
- Latest Mobile Application Security Threats and Vulnerabilities
- OWASP Top 10 Mobile threats
- Secure Coding Practices
- Android Application Reverse Engineering & Security Analysis
- Static analysis of Android applications
- Dynamic analysis of Android applications
- Security Analysis of Android applications - Case Studies
- Challenges in performing analysis of Mobile applications & probable research approaches

**Target Participants**

**Students**

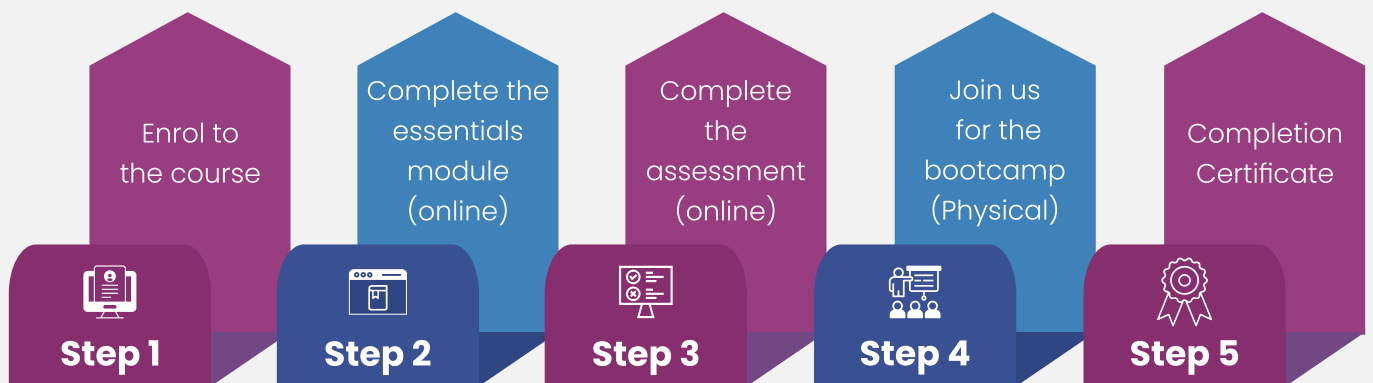
**Expected No. of Participants**

**100**

**Mode of Delivery**

**Essentials Module: Online  
Bootcamp : Offline**

## Process Flow



**Coordinated by**  
**M K Chaithanya**  
Scientist E

**Contact details :**

mkchaithanya@cdac.in | 9160441112

Register at : ▶▶▶▶

<https://bootcamps.isea.app/register>