



# ANDROID PENTESTING

POWERED BY IGNITE TECHNOLOGIES



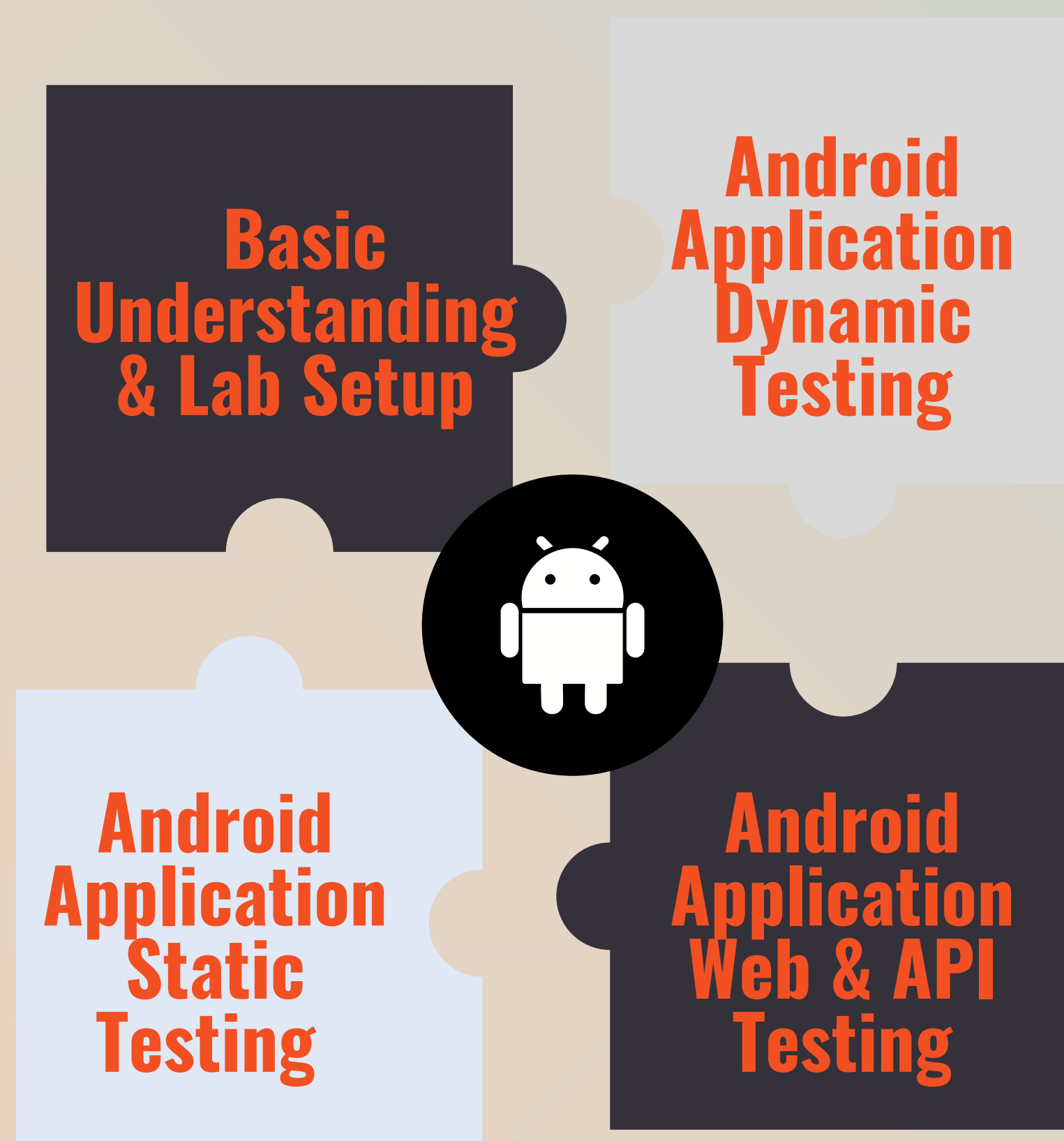


# ANDROID PENTESTING

In this modern world where our main concern is privacy and protection, we know in our hands that we have the greatest assets and the greatest threat. Yes, we're talking about the smartphone, Now phone isn't just a tool to call somebody it has become a part of life. Mobile phones now have more personal information, such as banking & social identity numbers, etc and people don't know to how to protect, because of this company's are hiring security engineers who knows mobile application security.

The strongest part of this course that it includes code-level security means you will understand the working of codes from there you can determine what attacks can be formed on the application by that you can even mitigate attacks like Instagram\_RCE.

## WHAT WE ARE GOING TO LEARN



**COURSE DURATION: 25 to 30 HOURS**

## Why to choose Ignite Technologies?

Ignite believes in “Simple Training makes Deep Learning” which help us in Leading International CTF market.

- Ignite Technologies is leading Institute which provides Cyber Security training from Beginner to Advance as mention below:

1. Networking
2. Ethical hacking
3. Bug Bounty
4. Burp Suite for Pentester
5. Windows for Pentester
6. Linux for Pentester
7. Computer Forensic
8. CTF-2.0
9. Privilege Escalation
10. Red Team Operations
11. Infrastructure Penetration Testing
12. API Penetration Testing
13. Android Penetration Testing

- World RANK -1st, in Publishing more than 400 walkthroughs (Solution) of CTFs of the various platform on our reputed website “[www.hackingarticles.in](http://www.hackingarticles.in)”.
- We Provide Professional training that includes real-world challenges.
- Ignite’s Students are placed in a TOP reputed company in the overworld.
- Hands-on Practice with 80% Practical and 20% Professional Documentation.
- ONLINE classes are available

## Career in IT Security Domain:

Chief Information Security  
Senior Security Consultant  
Cryptographer  
Penetration Tester  
Researcher


Officer Incident Analyst | Responder  
Software code Analyst  
Risk Controller  
Security Architect  
Exploit Developer

Information Security Analyst  
Digital Forensic Expert  
International Trainer  
Security Engineer  
Ethical Hacker



# COURSE OVERVIEW

## UNIT-1: INTRODUCTION

- 
- 
1. Android Architecture
  2. Android Permissions
  3. Android Application Package
  4. Android Compilation and Decompilation
  5. Android Pentest Lab Setup
  6. ADB
  7. Insecure logging
  8. SQLite DBs
  9. Drozer Introduction
  10. OWASP TOP 10

## UNIT-2: STATIC ANALYSIS

1. Improper Platform Usage
2. Insecure Data Storage
3. Broken Cryptography (through decompilation)

4. Code Analysis

5. Reverse Engineering and Frida

## UNIT-3: DYNAMIC ANALYSIS

1. Unintended Data Leakage:

a. Copy Paste Buffer

b. Crash Logs Analysis

c. Analytics Data Analysis

2. Hooking to snoop sensitive data including Crypto APIs

3. Objection and XPosed framework - Automated Hooking

4. Root Detection Bypass and prevention

5. Traffic Analysis

6. Insufficient Transport Layer Protection

a. Lack of Certificate Inspection

b. Weak Handshake Negotiation

c. Privacy Information Leakage

7. SSLPinning and Unpinning/MiTM attacks

8. Android Debugging Based Vulnerabilities



- 
- 
9. Crafting malicious APKs to exploit:
    - a. Activities
    - b. Services
    - c. Content Providers
    - d. Broadcast Receivers
    - e. Android DeepLinks and Exploitation
  10. Client-Side Injections:
    - a. SQLi
    - b. XSS
    - c. LFI
    - e. Eternal Cookies
  11. Android WebViews and Exploitation

## UNIT-4: AUTOMATED ANALYSIS

1. MobSF
2. QARK
3. Xposed framework
4. Objection 2.0