



Training and Services

PENETRATION TESTING

ANDROID ABOUT COURSE PENTEST

What is the Android Pentest course?

The **OWASP Top 10 Mobile Security** will be focused in this Android Pentest course to create awareness about Android app security issues. If you're familiar with the OWASP Top 10 series, you'll notice the similarities: they are intended for readability and adoption.

Its purpose is to ascertain whether an Android application is vulnerable and then to suggest to the client what patches should be applied.

Who needs Android App Pentest?

Stakeholders, Clients and Vendors should evaluate all areas of an application's security and confirm that no security bugs exist. Each security assessment may include Android penetration testing in their Pentest Cycle. This is related to the devices' and apps' functionality and improper error handling.

Ignite Training Objective

- OWASP Top 10 Android Security
- Android Security Cheat Sheet
- Automating the Android Pentest

Prerequisites

Basic knowledge of Web Application Pentesting as per OWASP top 10 for Web App, ethical hacking, Kali Linux and BurpSuite,

Course Duration: 25 Hours (Tentative)

Price: [Contact us](#)

ABOUT IGNITE

**Well-Known Entity for Offensive Security Training
and Services**

About us

With an outreach to over a million students and over thousand colleges, Ignite Technologies stood out to be a trusted brand in cyber security training and services.

WHO CAN ?

- College Students
- IS/IT specialist, analyst, or manager
- IS/IT auditor or consultant
- IT operations manager
- Network security officers and
- Practitioners
- Site administrators
- Technical support engineer
- Senior systems engineer
- Systems analyst or administrator
- IT security specialist, analyst, manager,
- architect, or administrator
- IT security officer, auditor, or engineer
- Network specialist, analyst, manager,
- Architect, consultant, or administrator

WHY US ?

- Level up each candidate by providing the fundamental knowledge required to begin the Sessions.
- Hands-on Experience for all Practical Sessions.
- Get Course PDF and famous website links for content and Tools
- Customized and flexible training schedule.
- Get recorded videos after the session for each participant.
- Get post-training assistance and backup sessions.
- Common Platform for Group discussion along with the trainer.
- Work-in Professional Trainer to provide real-time exposure.
- Get a training certificate of participation.

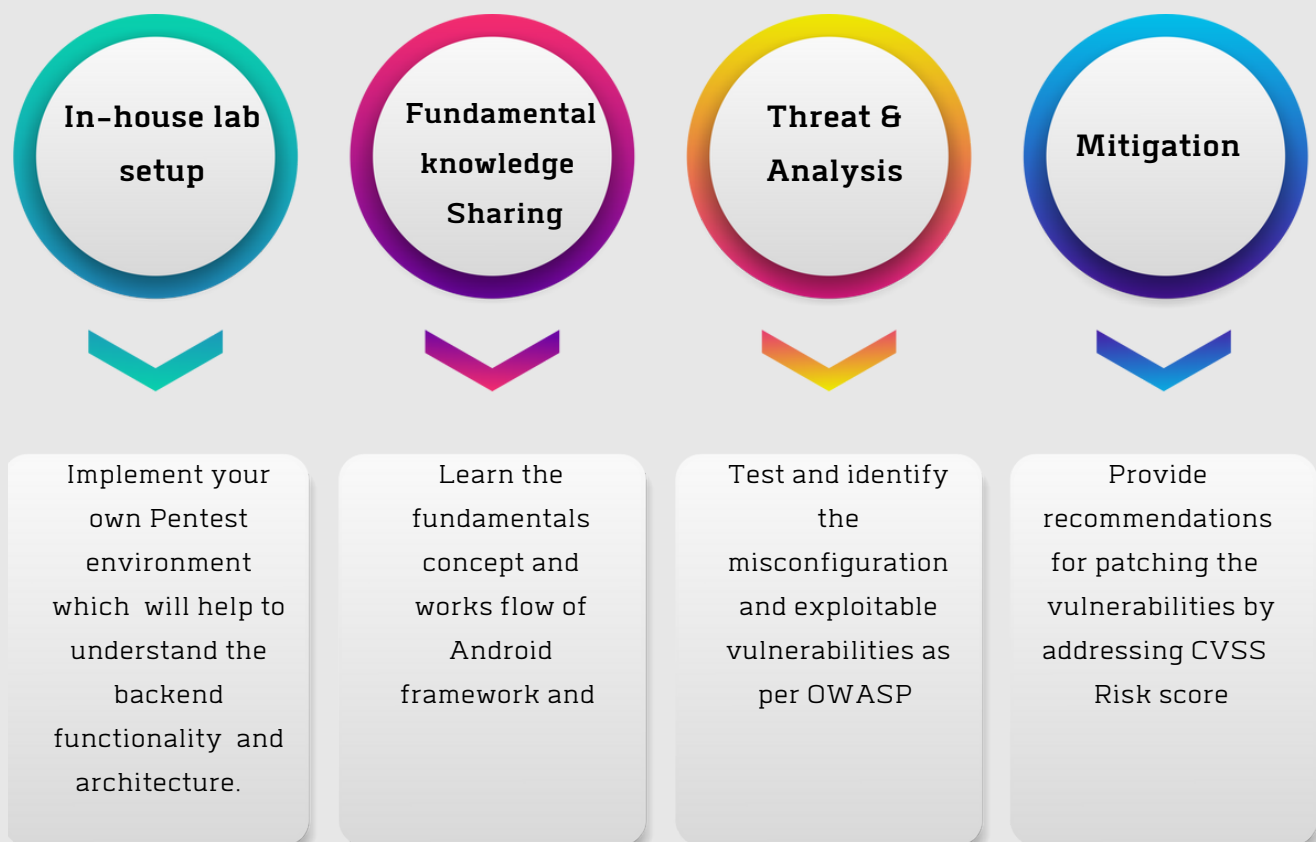
HOW WE FUNCTION

Ignite Trainers

Ignite Trainers are **industry-experienced professionals** and have vast experience with real-time threats thus they provide proactive training by delivering **hands-on practical sessions**.

Had working exposure in Big Fours and MNCs and Fortune 500 companies and clients such as Tata, Facebook, Google, Microsoft, Adobe, Nokia, Paypal, Blackberry, AT&T and many more.

Certified Trainers: CEH, OSCP, OSAP, Iso- Lead Auditor, ECSA, CHFI, CISM



ANDROID PENTEST

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 how to protect themselves, because of this companies are hiring security engineers who know mobile application security.

The strongest part of this course is 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 and you can even mitigate attacks like RCE.

WHAT ARE WE GOING TO LEARN



CONTENTS

Module 1

- 1)-Introduction of Genymotion
- 2)- Creating devices on Emulator
- 3) Setting up the burp proxy
- 4)- Installation of Root Certificate
- 5)- Introduction of Burp Proxy
- 6)- Traffic Analysis with Burp
- 7)- Introduction of adb

Module 2

- 1)- Android Architecture
- 2) Android Security Model
- 3)-Android Application Development Cycle
- 4)- Major Components of Android
- 5)- Android Application Components
- 6)-Android Startup Process

Automated Tool

- 1)- Mobsf
- 2)- Objection and Frida Tool
- 3)- Testing and Exploitation with Dozer Framework

Module 3

- 1)-Android Application Building
- 2)-Decompile With Jadx
- 3)Decompile with Apkeasy Tool
- 4)-Weak Server Side Controls
- 5)-Insecure Data Storage
- 6)-Hardcoding Issues
- 7)- Detection of Insecure Logging
- 8)-Database Insecure Storage
- 9)- Reading Temporary Files
- 10)- SQL Injection in Android
- 11)-Web View Vulnerability
- 12)- Access-Related Issues
- 13)- Authorization Bypass
- 14)- Understanding and Exploitation of Content Providers
- 15)- Input Validation leading to DOS Attack
- 16) Root Detection BYypass
- 17) SSL Pinning Bypass
- 18)Inspection of Certificate and Signing Schema

CONTACT US

PHONE

+91-9599387841 | +91-7805803296

WHATSAPP

<https://wa.me/message/HIOPPNENLOX6F1>

EMAIL ADDRESS

info@ignitetechnologies.in

WEBSITE

www.ignitetechnologies.in

BLOG

www.hackingarticles.in

LINKEDIN

<https://www.linkedin.com/company/hackingarticles/>

TWITTER

<https://twitter.com/hackinarticles>

GITHUB

<https://github.com/Ignitetechnologies>