iGNITE Technologies

Training and Services

PENETRATION TESTING

ANDROID 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

iGNITE Technologies

COURSE OVERVIEW

iGNITE Technologies

UNIT-1: INTRODUCTION

1. Android Architecture
2. Android Permissions
3. Android Application Package
4. Android Compilation and Decomplication
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: AUTOMATED ANALYSIS

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

UNIT-4: 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

CONTACT US

PHONE

+91-9599387841 | +91 9599387845

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

iGNITE Technologies