iGNITE Technologies

Training & Services

www.ignitetechnologies.in

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)

iGNITE Technologies

ABOUT

iGNITE Technologies

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 realtime exposure.
- Get a training certificate of participation.

iGNITE Technologies

HOW WE FUNCTION

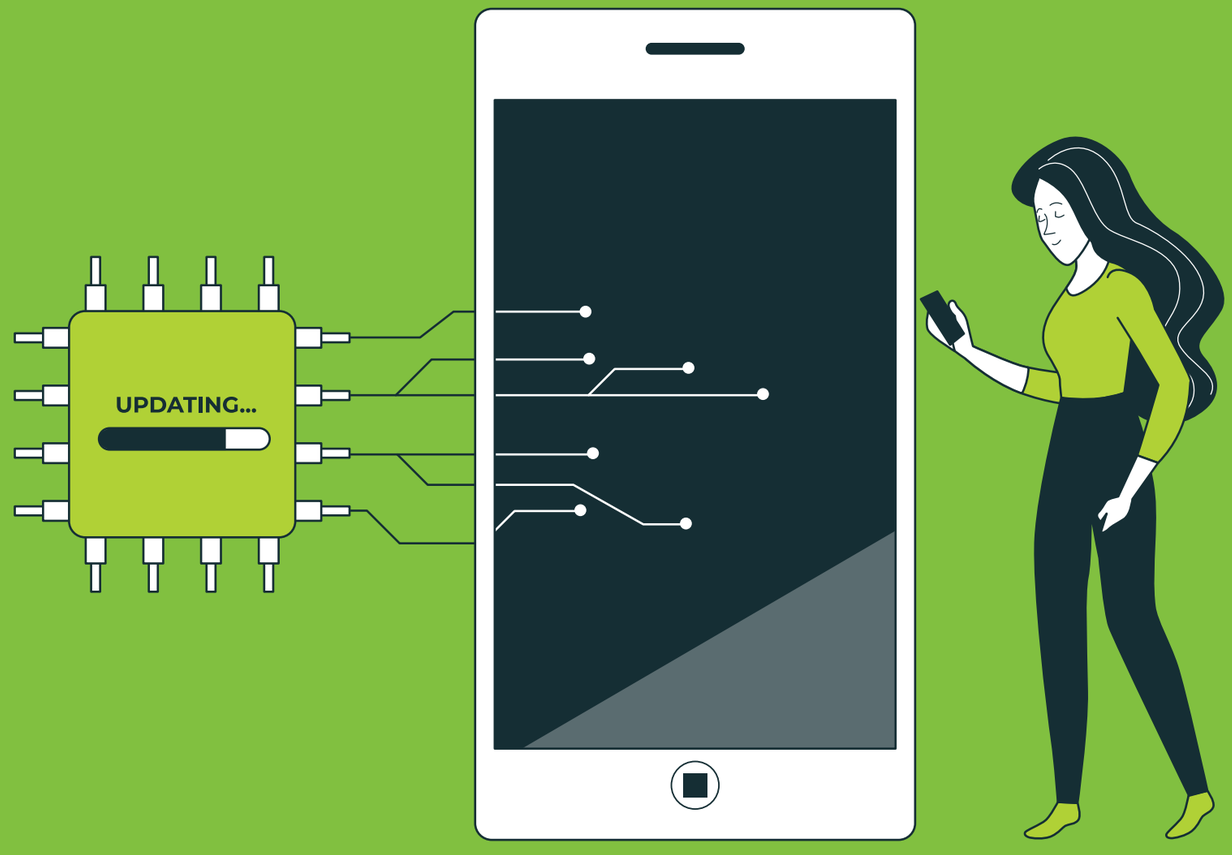
Ignite Trainers

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

APPROACH



In-house lab setup

Implement your own Pentest environment which will help to understand the backend functionality and architecture

Fundamental knowledge Sharing

Learn the fundamentals concept and works flow of Android framework and

Threat & Analysis

Test and identify the misconfiguration and exploitable vulnerabilities as per OWASP

Mitigation

Provide recommendations for patching the vulnerabilities by addressing CVSS Risk score

iGNITE Technologies

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

iGNITE Technologies

CONTENT

Module 1

Module 2

Module 3

iGNITE Technologies

CONTACT US

Phone No.

+91 9599 387 41 | +91 1145 1031 30

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