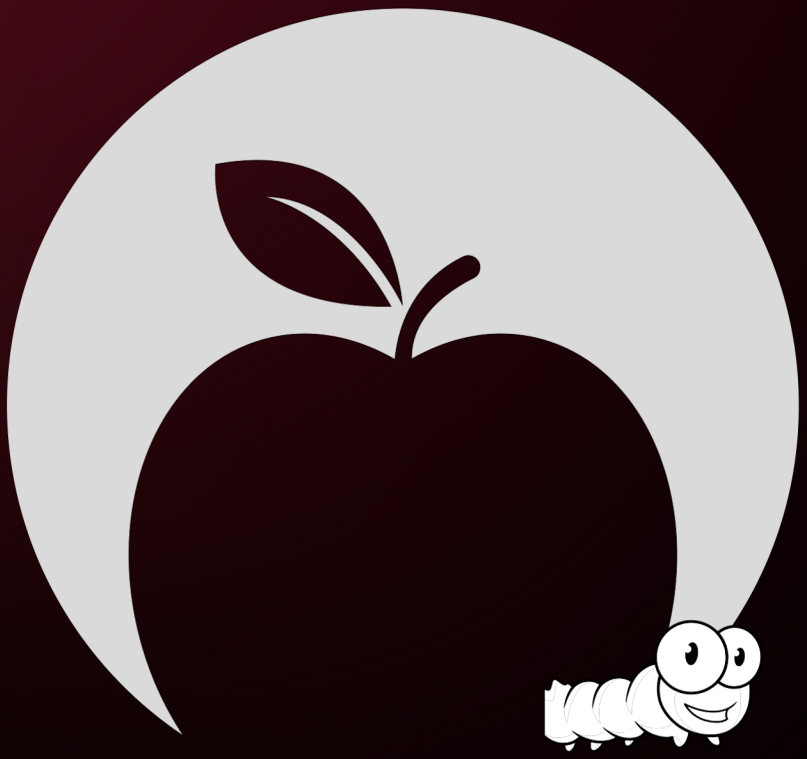

Penetration Testing

IOS APP

Training Program & Services

iGNITE Technologies

IOS PENTEST

ABOUT COURSE

What is IOS Pentest course?

The OWASP Top 10 Mobile Security will be focused in this IOS Pentest course to create awareness about modern IOS 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 IOS is vulnerable and then to suggest to the client what patches should be applied.

Who needs IOS 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 iOS penetration testing in their Pentest Cycle. This is related to the devices' and apps' functionality

Ignite Training Objective

OWASP Top 10 IOS Security
IOS Security Cheat Sheet
IOS Jailbreaking & Security Assessment

Prerequisites

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

Course Duration: 30 Hours (Tentative)

Price: Contact us

iGNITE Technologies

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

In-house lab setup	Fundamental knowledge Sharing	Threat & Analysis	Mitigation
Implement your own Pentest environment which will help to understand the backend functionality and architecture.	Learn the fundamentals concept and work flow of IOS framework and	Test and identify the misconfiguration and exploitable vulnerabilities as per OWASP	Provide recommendations for patching the vulnerabilities by addressing CVSS Risk score

iGNITE Technologies

COURSE CONTENT

IOS LAB SETUP

1. Xcode
2. Jailbreaking of IOS device
3. Installing Cydia
4. Installing tools

INSTALLATION OF VULNERABLE APPLICATIONS

1. Installing vulnerable applications
2. Installation of app sync

CONNECTING DEVICE VIA SSH

1. Installation of SSH
2. Connecting the devices through wifi network
3. Installing packages

VULNERABILITIES TO BE COVERED

1. Insecure data storage
2. Creation of new IOS project
3. Check signing certificates, device identifiers, bundle id
4. Installation of test application
5. Connecting physical device with Xcode
6. Installation of burp suite
7. Data storage in plist files
8. Data storage in nsuser defaults
9. SQL databases
10. Core data
11. Keychain data
12. Local data storage
13. Installation of objection and Frida
14. SQL injection
15. XML injection
16. Lack of rate limiting
17. Finding hidden APIs
18. Sensitive data exposure
19. Privilege escalation
20. volatile memory
21. Sensitive data in the clipboard
22. Web view XSS
23. Obfuscation
24. Jailbreak detection bypass
25. SSL pinning bypass

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