SYLLABUS

CYBER SECURITY · COURSE HANDOUT 2026

MOBILE SECURITY

NDROID . IOS . APP STORAGE
STATIC . DYNAMIC . TRAFFIC
OWASP MASVS . HARDENING

DURATION	LEVEL	MODULES	MODE
45 Hours	**Intermediate to Advanced**	**8**	**Classroom · Online · Hybrid**

01 COURSE OVERVIEW

A mobile application security course covering Android and iOS assessment against OWASP MASVS. Learners set up instrumented devices and emulators, decompile and review applications, intercept and manipulate traffic, examine insecure storage and authentication, and test platform-specific controls.

Each learner completes an assessment of a deliberately vulnerable application and reports findings.

WHO IT IS FOR

- Mobile developers
- Application security analysts
- Penetration testers extending to mobile
- QA engineers on mobile products

PREREQUISITES

Basic Android or iOS development awareness, networking and Linux command line.

02 LEARNING OUTCOMES

01 Set up a mobile testing environment with proxying.

02 Decompile and review Android and iOS applications.

03 Find insecure data storage and logging.

04 Intercept and modify API traffic despite pinning.

05 Test authentication, session and biometric flows.

06 Assess platform permissions and IPC surfaces.

07 Report findings against OWASP MASVS.

03 MODULE STRUCTURE

8 MODULES

01 MOBILE THREAT MODEL

- Platform architectures
- Permission models
- OWASP Mobile Top 10
- Sandboxing
- Threats and attackers

02 TEST ENVIRONMENT

- Emulators and real devices
- Proxy setup
- Rooting and jailbreaking basics
- Certificate installation

TOOLS

BURP SUITE | FRIDA | MOBSF

03 ANDROID STATIC ANALYSIS

- APK structure
- Decompilation
- Third-party SDKs
- Manifest review
- Hardcoded secrets

TOOLS

JADX | APKTOOL

04 ANDROID DYNAMIC ANALYSIS

- Runtime hooking
- Insecure storage
- Deep links and exported components
- Logcat
- WebView issues

LAB

VULNERABLE APP ASSESSMENT

05 IOS ASSESSMENT

- IPA structure
- Plist and cache data
- Runtime instrumentation
- Keychain
- Class dumping

06 API AND TRAFFIC SECURITY

- TLS validation
- Authentication tokens
- Backend authorisation
- Certificate pinning bypass
- Rate limiting

07 HARDENING AND DEFENCE

- Secure storage APIs
- Root and tamper detection
- Play Integrity and DeviceCheck
- Obfuscation
- Secure update paths

08 REPORTING

- Severity rating
- Developer-ready remediation
- MASVS mapping
- Evidence capture
- Retesting

PROJECT

MOBILE APP SECURITY ASSESSMENT REPORT

04 ASSESSMENT & CERTIFICATION

Module assignments and labs	**25%**
Mini projects	**20%**
Internal assessments	**15%**
Final project and review	**40%**

CERTIFICATION

Learners who complete all modules, submit the final project and clear the review receive a course completion certificate from Kaizen Infinities Private Limited. Project work is documented for the learner's portfolio, and interview preparation is included in the closing sessions.

05 CAREER OUTCOMES

ROLES THIS PROGRAMME PREPARES FOR

MOBILE SECURITY ANALYST · **APPLICATION SECURITY ENGINEER** · **PENETRATION TESTER (MOBILE)** · **SECURE MOBILE DEVELOPER** · **PRODUCT SECURITY ENGINEER**

CALL US
+91 73051 33996

EMAIL US
apply@kaizeninfinities.com

VISIT OUR WEBSITE
www.kaizeninfinities.com