OWASP MASVS TRAINING

Level - OWASP

Email – contact@DevOpsSchool.com

TRAINING AGENDA

DAY 1

Introduction to Mobile Application Security

- Mobile application threat landscape
- Common attack surfaces in Android & iOS apps
- OWASP Mobile Top 10 overview
- Why mobile security standards are required
- Introduction to OWASP MASVS and MASTG

OWASP MASVS Overview & Structure

- Purpose and scope of MASVS
- MASVS security control categories
- MASVS verification levels (L1, L2, R)
- Relationship between MASVS and MASTG
- Selecting the right MASVS level for applications

Secure Mobile Architecture & Design

- Secure mobile app architecture principles
- Client-side vs server-side responsibilities
- Secure API and backend integration
- Trust boundaries and data flow
- Common architectural mistakes in mobile apps

Authentication & Authorization

- Secure authentication mechanisms for mobile apps
- Token-based authentication and session handling
- Secure authorization models
- Protection against session hijacking and replay attacks
- MASVS verification requirements for identity controls

Secure Network Communication

- Secure communication fundamentals
- TLS configuration and enforcement
- Certificate pinning concepts
- Preventing MITM attacks
- Network security verification using MASVS

Hands-On Discussion & Case Studies

- Real-world mobile app security failures
- Mapping vulnerabilities to MASVS controls
- Group discussion on secure mobile design

DAY 2

Data Storage & Privacy Controls

- Secure local storage techniques
- Handling sensitive data on mobile devices
- Encryption, key management, and keystore usage
- Privacy and data protection considerations
- MASVS verification requirements for data security

Cryptography & Secure Key Management

- Cryptographic fundamentals for mobile apps
- Secure use of cryptographic APIs
- Key storage and lifecycle management
- Common cryptographic mistakes in mobile apps

Platform Interaction & OS Security

- Secure use of platform features (Android & iOS)
- Permissions and sandboxing
- Secure inter-process communication
- Handling intents, deep links, and app extensions

Code Quality & Secure Development Practices

- Secure coding principles for mobile apps
- Input validation and error handling
- Protection against code injection and logic flaws
- Secure update mechanisms

Runtime Protection & Anti-Tampering

- Reverse engineering threats
- Obfuscation and code protection
- Root and jailbreak detection
- Runtime integrity checks
- Advanced MASVS verification requirements

Security Testing, Verification & Compliance

- Using MASVS with security testing tools
- Manual vs automated testing approaches
- MASVS and MASTG mapping
- Integrating MASVS into SDLC and DevSecOps
- Compliance and audit readiness

Final Review & Practical Guidance

- End-to-end MASVS verification walkthrough
- Best practices for enterprise adoption
- Common mistakes and how to avoid them
- Final Q&A and knowledge check