1212E1519

Candidate's Seat No:____

MSc IT MAUID Sem.-3 Examination

MSCMA 501

Mobile App Security Basic

Time : 2.30 Hours] **December-2025** **[Max.Marks : 70**

Instructions:
1. **Attempt all questions.**
2. **Make suitable assumptions wherever necessary.**
3. **Figures to the right indicate full marks.**
4. **Can't write anything on this paper.**

		Marks
Q 1.	1.Secure Software Development Lifecycle (SSDLC) includes: A) Security considerations at every phase of development B) Security only during testing C) Security only after deployment D) No security requirements 2.M8: Security Misconfiguration in OWASP Mobile Top 10 2024 includes: A) Weak encryption algorithms B) Improper server and API configurations C) Poor binary obfuscation D) Inadequate supply chain vetting 3.What does MASTG stand for in the OWASP mobile security framework? A) Mobile Application Security Training Guide B) Mobile Application Security Testing Guide C) Mobile App Security Threat Guidelines D) Mobile Application Security Technical Guide 4.API security best practices for mobile apps include: A) Using HTTP instead of HTTPS B) Implementing authentication, rate limiting, and input validation C) Removing all authentication requirements D) Sharing API keys in the app code 5.What risk does M4 address in OWASP Mobile Top 10 2024? A) Improper Credential Usage B) Insufficient Input/Output Validation C) Insecure Data Storage D) Inadequate Privacy Controls	**[10]**

P.T.O

SET B

E1519-2

Enrolment No.

	6.What type of attacks are increasingly leveraging AI tech in 2025? A) Basic SQL injection B) AI-driven malware and phishing attacks C) Simple buffer overflow attacks D) Manual brute force attacks 7.What does AI-powered anomaly detection in RASP helps: A) Design user interfaces B) Identify unusual patterns that may indicate security threats C) Optimize database queries D) Manage app updates 8.End-to-end encryption for messaging ensures: A) The server can read all messages B) Only the sender and intended recipient can read the messages C) Messages are stored permanently D) Messages load faster 9.Where does FaceID/TouchID is stored on device Hardware in iPhone: A) RAM B) ROM C) M Chip D) Secure Enclave 10.Zero Trust Architecture for mobile requires: A) One-time authentication B) Continuous authentication and authorization throughout the session C) No authentication D) Biometric authentication only	
Q 2.	**Answer in short:**	**[30]**
a.	What is the purpose of app sandboxing?	**[6]**
b.	What is the main goal of Security by Design methodology?	**[6]**
c.	What is App Tracking Transparency (ATT) in iOS?	**[6]**
d.	What does end-to-end encryption ensure?	**[6]**
e.	Explain what FIDO2/WebAuthn provides for authentication.	**[6]**
	OR	
e.	Explain what runtime permissions are in mobile applications.	**[6]**

SET B	E1519-3	Enrolment No.

Q 3.	**Answer in Detail:**	[30]
a.	Explain M2: Inadequate Supply Chain Security from OWASP Mobile Top 10 2024. What are the risks of third-party libraries and SDKs, and what tools or practices can mitigate these risks?	[7]
b.	Describe in detail the OWASP Mobile Top 10 2024, explaining at least five categories and their significance in modern mobile security. How has this list evolved from the 2016 version?	[7]
c.	Explain secure communication protocols for mobile applications in detail. Cover HTTPS implementation, certificate pinning, API security, secure WebSocket connections, & how to prevent man-in-the-middle attacks.	[8]
d.	Compare and contrast the security models of Android and iOS in 2025. Discuss app sandboxing, hardware-backed security, biometric authentication, and privacy controls specific to each platform.	[8]
	OR	
d.	Explain the iOS Secure Enclave architecture and its role in protecting sensitive operations. Discuss how it integrates with Face ID/Touch ID, secure key storage, and provides isolation from the main processor.	[8]

—x—