3/36

0912E994

Candidate's Seat No :________

IM.Sc in CSF Sem.-7 Examination

ICSF-404

Adv. Mobile Application Security

December-2024

Time : 2-30 Hours] **[Max. Marks : 70**

Question 1 Answer the following questions:

i. Explain Android's progress from its origin to its current status, emphasizing major milestones in history. 7Marks

ii. Explain the hardware and software architecture of Android. How do they collaborate to ensure a smooth customer experience? 7Marks

OR

i. Explain the Android security model. How does it secure the security of user data and system integrity? 7Marks

ii. Explain Android's permission model for application security. How does it assist to protect user privacy and prevent unauthorized access? 7Marks

Question 2 Answer the following questions:

i. How has the historical growth of iOS influenced its current functioning and features? Discuss the key upgrades and advances that have taken place throughout time. 7Marks

ii. What are the essential components of iOS architecture, and how do hardware and software pieces work together to provide a safe and efficient operating environment? 7Marks

OR

i. What procedures are used in the iOS security model to protect the confidentiality, integrity, and availability of user data? 7Marks

ii. How does the iOS permissions model control application access to sensitive data and system functions? Provide instances to back up your assessment. 7Marks

Question 3 Answer the following questions:

i. What are the important elements in creating a mobile application penetration testing environment, and how do they assure testing accuracy and security? 7Marks

ii. How can good engagement with mobile devices help identify and exploit possible vulnerabilities during penetration testing? 7Marks

OR

i. Explain Drozer's function in mobile application penetration testing. How does it help with the examination of Android application vulnerabilities? 7Marks

ii. Discuss how important it is to configure Burp Suite for traffic interception. How may traffic interception bypass methods be used to identify and attack mobile application vulnerabilities? 7Marks

Questions 4 Answer the following questions:

i. What are the risks associated with client-side injection vulnerabilities in mobile applications? Explain how such vulnerabilities can be exploited, the potential consequences, and the mitigation measures that can be employed to address them. 7Marks

(P.T.O)

E994-2

ii. What are the implications of improper session handling mechanisms in mobile applications? Explain how attackers might exploit this vulnerability and recommend techniques for effective mitigation. 7Marks

OR

i. How can the use of hardcoded cryptographic keys within a mobile application's source code create vulnerabilities? Discuss the methods an attacker might use to exploit such a weakness and propose strategies for mitigating this issue. 7Marks

ii. How can the use of hardcoded cryptographic keys within a mobile application's source code create vulnerabilities? Discuss the methods an attacker might use to exploit such a weakness and propose strategies for mitigating this issue. 7Marks

Questions 5: Attempt any Seven out of Twelve. 14Marks

1. What is the primary purpose of sandboxing in Android and iOS applications?
   A. To isolate applications from each other for security
   B. To enhance application performance
   C. To enable application debugging
   D. To prevent application updates
2. Which file in an Android application contains critical information such as permissions and application components?
   A. AndroidManifest.xml
   B. MainActivity.java
   C. res/layout/activity_main.xml
   D. strings.xml
3. What is a common risk associated with insufficient transport layer protection in mobile applications?
   A. Unauthorized device access
   B. Man-in-the-middle attacks
   C. Increased battery consumption
   D. Application crashes
4. Describe the purpose of the Android Permission Model and its impact on application security.
5. Which tool is commonly used for traffic interception in mobile application penetration testing?
   A. Burp Suite
   B. Drozer
   C. Wireshark
   D. Nessus
6. Explain how the Android security model ensures the protection of user data and application integrity.
7. What vulnerability allows an attacker to exploit hardcoded cryptographic keys in a mobile application?
   A. Broken cryptography
   B. Improper session handling
   C. Unintended data leakage
   D. Lack of binary protection
8. What is the primary difference between Android and iOS in terms of hardware and software architecture?
9. What is the primary reason for using codesigning in mobile applications?
   A. To ensure the application is free of bugs
   B. To verify the authenticity and integrity of the application
   C. To optimize application performance

E994-3

D. To enable cross-platform compatibility

10 What role does sandboxing play in the security of Android and iOS applications, and how does it prevent unauthorized access?

11 What is the role of the Keychain in iOS security?

A. To store sensitive user data securely

B. To manage application permissions

C. To improve application performance

D. To debug applications

12 What are the risks associated with rooting an Android device or jailbreaking an iOS device, and how can they compromise system security?

........................X...X.......................