Mobile Application Security Assessment

Project Description:

In this project, you will need to focus on assessing the security of a mobile application, such as an Android or iOS app. Mobile applications often store sensitive user data and can be vulnerable to various security threats. You will perform a comprehensive security assessment of the chosen mobile app, identify vulnerabilities, and provide recommendations for improving its security.

Objective:

This project allows you to dive into the realm of mobile application security, which is highly relevant in today's digital world. You will gain practical experience in identifying vulnerabilities in mobile apps and learn how to provide valuable recommendations to enhance app security.

Requirements:

1. Mobile Device or Emulator:

- You will need access to an emulator for testing. You should select an app to assess, and the app should be installed and running on the device or emulator.

2. Mobile Application Analysis Tools:

- Familiarity with tools for analyzing mobile applications, such as APKTool (for Android apps), JADX (for Java code extraction), and class-dump (for iOS apps). You can choose any kind of tool that is necessary to implement this attack.

3. Static and Dynamic Analysis:

- Static analysis involves examining the app's source code, manifest files, and resources to identify potential vulnerabilities.

- Dynamic analysis involves running the app and monitoring its behavior to detect vulnerabilities.

4. Vulnerability Identification:

- Identify common mobile app vulnerabilities.

- Use specialized tools and techniques to find vulnerabilities.

5. Exploitation:

- After discovering a vulnerability, you are required to attempt the exploitation.

6. Security Report:

- Create a comprehensive security assessment report that includes an executive summary, methodology, findings, recommendations, and references.

- Describe each vulnerability discovered, its potential impact, and provide steps for prevention.

- Include evidence such as screenshots, code snippets, and logs to support findings.

7. Ethical and Legal Considerations:

- Emphasize the importance of responsible and legal hacking practices.

- Ensure to adhere to ethical guidelines.

Submission guidelines:

1) Provide a **recorded video** of your screen while performing this attack (**max**: 5 mins)
2) Create the **security report (min:** 10 pages) mentioned above and include the following:
    a) *Introduction:* provide the scope of your assessment
    b) *Methodology*: include the tools and techniques used and the choice of emulator. Explain the purpose and result of using each tool
    c) *Vulnerability Identification:* list the vulnerabilities that were identified describe how the tools and techniques were used to discover these vulnerabilities
    d) *Exploitation*: discuss any vulnerabilities that were exploited and provide information on the impact and implications of these attacks.
    e) *Recommendations*: offer recommendations on improving the security of the mobile application and suggest the best practices or security measures that could be taken to mitigate these vulnerabilities.
    f) *Conclusion*: summarize your key findings and describe your overall security status of the mobile app
    g) References: APA style (if you’ve used any external sources)
3) Both the video and your report should include your **name and ID**
4) Provide **code snippets** on the report