Sense – It
(APK/IPA Package Validation Tool)

[1]Dr. L. Javid Ali, [2]Mr. Gautham S, [3]Mr. Aadithya M

[1]Associate Professor, [2,3]B.Tech Student
Department of Information Technology
St.Joseph's Institute of Technology

***Abstract*- Sense – IT is a static and dynamic security package analyzer developed by us, the authors Gautham.S and Aadithya.M for mobile application evaluation. It breaks the source code and goes through the process of analysis, vulnerability identification, as well as penetration testing for mobile applications on many platforms such as Android, iOS, as well as Windows. This tool enables the developers to evaluate and improvise the application security feature which reduces the overall vulnerability risk and it allows the developers to strengthen their mobile application's resistance to constantly evolving cyberattacks.**

Keywords: **StaticAnalysis, Dynamic Analysis, Endpoint Report.**

I. INTRODUCTION

In today's modern and ever-changing world, Mobile applications play a very important role in helping out various applications, which saves several times for humans. Thus it is important to have security risk-free Mobile applications as they might contain the User's confidential data. Sense – IT (Package Analyzer) is a tool that might become an indispensable tool for strengthening the mobile application's defenses against the almighty cyberattacks. Among other tools, Sense–IT is a dynamic and all-inclusive solution that has a high-level skill at analyzing in-depth security audits for Mobile applications on different platforms such as Android, iOS, and Windows.

Its fundamental architecture is modular and expandable, which enables thorough Analysis, Vulnerability identifications, as well as penetration testing. It's User- friendly and feature-rich UI gives the developers and security experts an easier approach to spot and fix the problems as soon as possible. It is a crucial ally for the developers as it is an ever-expanding and diverse mobile ecosystem because it provides a proactive way to improvise the application's security structures protecting the user data and maintaining the richness of digital experience during the process.

Moreover, Sense–IT is also the universal solution for developers and security experts because of its versatility in supporting a wide range of mobile platforms such as Android, and IOS. It helps in improving throughout the development life cycle in the real world which helps indetecting early vulnerability detections and mitigation.

Furthermore, the idea of Dynamic Analysis which is an intrinsic implementation of validation and verification over the mobile applications for a greater view of possible vulnerabilities if any, tends to minimize the logical errors and loopholes for a better and safer environment throughout execution in Android/IOS applications. The final report submitted over the full validations ensures a particular score for the application is validated and also provides a solutionin minor cases of issues.

II. LITERATURE REVIEW

Finding and reducing any security threats related to mobile applications is the main goal of a dynamic mobile APK verification system. This includes identifying potentially exploitable vulnerabilities, unauthorized data access, and criminal activity.

[1] According to Ailie K.Y. (2021) "A systematic literature review and analysis on mobile apps in m-commerce: Implications for future research" This initiates a proper pathways of important folder validations over the analysis stages .Over the part of Contribution, this study attempts to classify and arrange the subjectivism on mobile apps in Mobile commerce as well as evaluate the current state of the field. This was in fact the newer part of the project, where it was the first form of validation projected over the manifest fields occurring over the background.

[2] Ivano Malavolta's book "Datasets of Android Applications" (2022) is helpful for both seasoned and inexperienced researchers who want to study Android apps. Our study's findings can be used as a guide to help researchers find the best datasets for their goals.

[3] Tejpal Sharma's article from 2022, "Malicious application detection in Android," describes There is an identification of the many methods that are employed tolook into harmful applications.

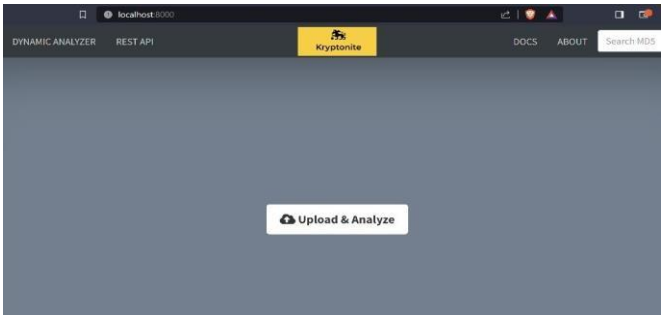


Figure -1 (Startup page)

These above-mentioned literature surveys helped us to create a properly validated application that ensures accurate data handling and implication strategies for creating a mobile validation application that is entirely new to the technological environment and can improve the statistics of applications being used in our society.

In order to indicate the state of novelty in our segment of our project shortly, we have introduced Concurrent data validation over the period of application running in the projected mobile environment, which paves way for a more intrinsic and hard-core method of file validation that can identify the malicious factors more easily.

III. METHODOLOGY

The overall process of the evaluation for the security of the Mobile application is done using a special tool for Package Analysis known as Sense – IT. To find the potential vulnerability points, the tool first scans the Mobile application using Static analysis scanning which carefully analyses the overall source code and binary files. It finds the security flaws by examining the overall structural architecture, permissions required from the user, as well as API usage. Since it offers a detailed approach to finding the potential vulnerability points, Static analysis is very useful for early detection and fixing the flaws in every iteration of the development life cycle which is very useful according to the developer's point of view.

Sense – IT also uses dynamic analysis along with static analysis to provide a detailed evaluation report of the overall behavior of the Mobile application during runtime in real- world scenarios. Through pre-program execution, the Sense

-IT tool Stores the security flaws that might show up during the evaluation process as a detailed report. The overall structure of the mobile application might be evaluated in a complex manner, since, some vulnerabilities cannot be simply found during Static analysis, Thus dynamic analysis approach helps to find these well-hidden vulnerability points for higher efficiency in overall security upgrades in that Mobile application. Thus the combination of both Static and Dynamic analysis helps the developer to completely reduce the cyberattacks by simulating the Mobile application in this tool which helps to find all vulnerability points at any stage of the development life cycle of the Mobile Application.

Furthermore, we have included a factor of validation called Cross-Site scripting validation, where the tendency of validating the extrinsic websites that are being re-directed from the current application being used is implied here.

This is projected as a final and a minor part of file validation, which helps to procure a safe and effective way of approach towards the purpose. The Manifest files are being subjected to a concurrent code alterations such as URL Traversals and finally it tends to procure the actual sitewhich meant to be reached from the source.

Finally, in case of any confusions that occurs over the period, the process formats the existing queries that are done and finally it restarts the progress from initial stage.

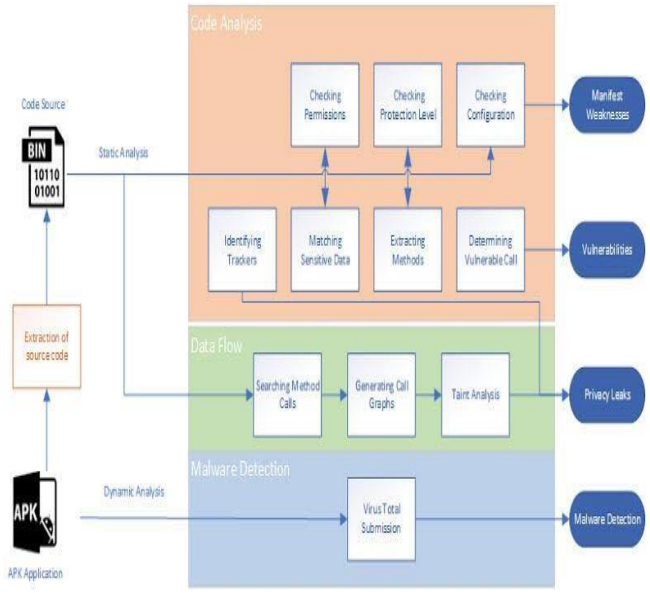


Figure 2 (Backend Process)

The above figure mentions the complete flow of the Sense- IT tool's Coding examination along with both Static Analysis as well as Dynamic Analysis.
Moreover, the additional features provided by the Sense – IT tool improve the richness for the end user to filter out particular security requirements. The tool provides additional plugins and scripts, which help to simulate particular real-world situations. This analysis gives the developer and user more flexibility in usage. Thus, the architecture of Sense–IT makes sure it can constantly change with the overall mobile security threats and cyberattack landscape.
This tool's comprehensive reports and simpler-to-use User Interface facilities make it easier to share the security flaws and encourage the overall cooperation between developer teams and security teams to reduce the overall threats.

IV. STATIC ANALYSIS

The initial validation of the uploaded mobile application file starts with static Analysis, which undergoes a thorough check of the source code and binary files of the mobile application without running the code. This widely helps to remove errors initially in the starting stage of the development life cycle of the application.

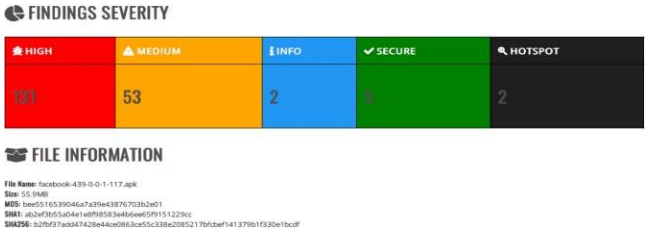
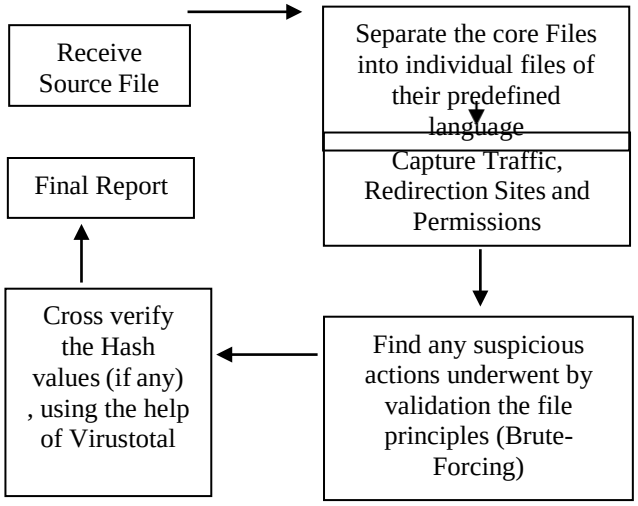


Figure 3 (Validation Report)

During it's first phase, Sense-it identifies if there are no forms of unsafe coding complications and security flaws being prevailed. It ensures the proper usage of uploading user data in the application with the inclusion of administrative privileges, permissions, and data storage techniques. The API check is also a major form of testing strategy available, where the interaction over the backend connectivity of the application is validated thoroughly. This procedure helps to improve access controls and paves the way for data privacy.
The binary code which plays the core factor of an application is examined by checking over the source code's compiled version. Then it continues to check over the interlinks which are in the format of libraries and executable files compiled over it. By following in this way it helps even to find out the hidden vulnerabilities that include hardcoded credentials, encryption techniques, and other configurations that aren't entirely from the source code being specified.
Sense-It's static analysis step includes identifying common security mistakes such poor input validation, insufficient session management, and unsecured data storage. Sense-It helps developers strengthen their code against popular attack vectors by highlighting these problems, which lowers the possibility of security breaches.

This application has the potential to validate over both Android and IOS application software irrespective of the versions which make it flexible and used to a greater extent. In conclusion, the Sens-It's Static Analysis offers complete validation over the given mobile application file, which makes it easy to configure the errors and loopholes if thereare any.

Algorithm / Work Flow :



VI. DYNAMIC ANALYSIS

The major part of the entire project involves the idea of dynamic analysis, which is the concurrent assessment of an application while it's in a running state. This process allows a virtual simulation of how the application works and identifies the stability while attaining greater pressure.

V. SOURCE CODE INSPECTION

Sense-It validates functions of errors and code inspections with every line possible over the application's backend data for which it uses the following mechanisms:

- **Identification of Security Flaws:**

Sense-It has the potential to make sensitive vulnerability checks over the application's environment and identify the loopholes, if available.

- **API Usage Analysis:**

Sense-It keeps an eye over the interactions between API communications to verify if the data processing is safe and secured and also identifies compliance with industrial standards.

- **Permissions and Access Controls:**

The illegal access to permissions for device controls is being handled and stopped with multi-factor authentications.

- **Cryptographic Analysis:**

The idea of key validations of hash values and cryptographic formulations are being administered to be carried out in a more sensible way, which leads toa more secure environment.

- **Custom Checks and Extensibility:**

Sense -It tends to allow the user's own script validations and checks to procure flexibility over the analysis.

Sense-It interacts with a virtual simulation of how the entire application works and over the case this method includes stress testing to a particular extent so that we can easily figure out the load balance that the particular file canhandle and configure the necessary alterations if the particular test-case should be altered.

To find the reaction towards the scenarios of protecting data, session management, and input validation, Sense-It 's Dynamic Analysis enhances the virtue of static analysis implementing a mere accurate usage situation. This helps to identify the actual level of security that the application intends to and reveals the working tendency over its actual use. The final results attained over the process can be a great source of information for the project developers and security experts that help them to fix the vulnerabilities and improve the application's overall security posture to a greater extent.

Upon a wider view, Sense-It's dynamic analysis identifies the working of external services and Third-party APIs that are running in the background environment and so, the matter of flexible communication towards the endpoint is sorted out. Moreover, the idea of runtime interactions is the core idea of the testing strategy which helps to build the live virtual implementation and submit a proper report upon which the application that is tested has the potential to be vulnerable to the loopholes and errors submitted fromthe final report.

VII. CONCLUSION

The tool associates with the important features mentioned below and it continues to improve the quality of validation with each scanning report it undergoes. So this makes it concurrent and a more integrated way predictability.

Security Automation and DevSecOps Integration:

The security Life cycle is an essential component for the entire process of the Sense-It tool's behaviour and analysis and so the concept of DevSecOps is included for the successful integration and deployment of the overall Analysis process. This includes the initial process of uploading and analysis over static validations until the integration between the virtual system for dynamic validation and report submission criteria.

Threat Intelligence Integration:

The implementation of course has a set of pre-stored data sets for making decisions regarding the assessment of the application's integrity. By providing the necessary information, we can configure a certain set of patterns for the overall process of analysis and the state of unusual activity pretending to be carried out in the execution phase of the application.

Behavioural Analysis and Anomaly Detection:

The anomaly detection techniques being provided are a form of a pre-set act of execution where the use cases are defined ideally and so when a certainty takes place according to the scenario specified in the use case it is immediately alerted and noted out so that the application is again turned out to be proceeding over a rightful behavior. This includes suspicious network traffic being mitigated when the application connects over the internet.

Secure Communication and Data Protection:

Currently, we have built an application that entirely focuses on robust encryption mechanisms and heavy data security. When it comes to future development, this application surely provides a safer part of communication over the provided environment from both the endpoint to ensure that the data is only used over the given source of validations and strictly not used beyond the course of action.

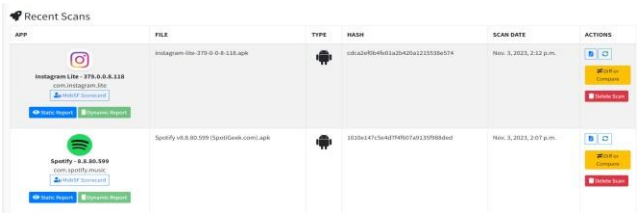


Figure -4 (Successful executions)

REFERENCES:

1. Karthi Vignesh. S; Abhilash. N 2023. Screening Ransomware Through APK Analysis: Implementation of CNN Models.
2. Mohammad Al-Fawa'reh 2020. Malware Detection byEating a Whole APK.
3. Nitesh Kumar 2021 Banking Trojans APK Detection using Formal Methods Published in: 2019 4th InternationalConference on Information Systems and Computer Networks (ISCON)
4. W Enck, M Ongtang and P. Mc Daniel, "On lightweight mobile phone application certification", *Proceedings of the 16th ACM conference on Computer and communications security*, pp. 235-245, 2021.
5. M Y Su and W C. Chang, "Permission-based malware detection mechanisms for smart phones Information Networking (ICOIN)", *2014 International Conference on*,pp. 449-452, 2022.
6. S.H Seo, A Gupta and A. Mohamed Sallam, "Detecting mobile malware threats to homeland security through staticanalysis", *J. Netw. Comput.*, vol. 38, no. 22, pp. 43-53, 2023.
7. https://www.hindawi.com/journals/scn/2021/9964224/
8. APK Auditor: Permission-based Android malwaredetection system - ScienceDirect
9. Afonso, V. M., M. F. de Amorim, A. R. A. Grégio, G. B. Junquera, and P. L. de Geus. 2015. Identifying Android malware using dynamically obtained features. *Journal of Computer Virology & Hacking Techniques* 11 (1):9–524. 2021
10. Android malware detection based on image-based features and machine learning techniques | SN Applied Sciences (springer.com)
11. https://www.synacktiv.com/sites/default/files/2022-07/PTS2022-Talk-19 -for-penetration-testers_0.pdf