INSTITUTE FOR ADVANCED COMPUTING
AND
SOFTWARE DEVELOPMENT
AKURDI, PUNE

DOCUMENTATION ON

"MOBILE SECURITY ASSESSMENT"

PG-DITISS SEPT-2023

SUBMITTED BY

Group No: 14

Ruchira Warke (239434)

Sakshi Chaudhari (239437)

MRS. SUSHMA HATTARKI
PROJECT GUIDE

MR. ROHIT PURANIK
CENTRE CO-ORDINATOR

ABSTRACT

Mobile devices have become ubiquitous in modern society, facilitating communication, productivity, and access to information. However, their widespread usage also presents significant security risks, as mobile applications often handle sensitive data and connect to various networks. To address these concerns, this project focuses on mobile security assessment, aiming to enhance the security posture of mobile applications and devices. The project encompasses a comprehensive evaluation of mobile application security using a combination of static and dynamic analysis techniques, vulnerability scanning, penetration testing, and threat modeling. Additionally, it involves the implementation of security best practices and mitigation strategies to harden mobile applications against common attack vectors, such as data leakage, unauthorized access, and network-based attacks. Through systematic assessment and proactive measures, this project aims to mitigate security risks, safeguard user privacy, and bolster the resilience of mobile ecosystems against evolving threats.

In the realm of mobile security, this assessment project endeavors to comprehensively evaluate the resilience of mobile applications against a spectrum of potential cyber threats. Employing a multi-faceted approach, the project encompasses static analysis for scrutinizing source code vulnerabilities, dynamic analysis to simulate real-world scenarios, and penetration testing to emulate malicious attacks. Emphasis is placed on identifying and mitigating risks associated with data security, user authentication, and secure communication channels. Leveraging a combination of automated tools and manual inspection, the project not only detects vulnerabilities but also assesses the effectiveness of existing security controls. With the ultimate goal of fortifying mobile applications against evolving cyber threats, this project serves as a vital initiative in enhancing the overall security posture of mobile ecosystems.

INDEX

1. INTRODUCTION

In the contemporary digital landscape, the proliferation of mobile devices has revolutionized the way individuals and organizations interact with information, services, and each other. As mobile applications continue to play a pivotal role in daily life, from financial transactions to personal communications, the security of these applications becomes paramount. The Mobile Security Assessment Project emerges as a proactive response to the escalating cybersecurity challenges posed by the increasing reliance on mobile technology.

In the contemporary digital landscape, the proliferation of mobile devices has revolutionized the way individuals and organizations interact with information, services, and each other. As mobile applications continue to play a pivotal role in daily life, from financial transactions to personal communications, the security of these applications becomes paramount. The Mobile Security Assessment Project emerges as a proactive response to the escalating cybersecurity challenges posed by the increasing reliance on mobile technology.

Background and Rationale:

The ubiquity of smartphones and tablets has brought about a paradigm shift in how peopleaccess and share information. However, this technological evolution has not been without its drawbacks. Mobile applications, serving as conduits for a myriad of functionalities, often handle sensitive data, making them lucrative targets for malicious actors. The rise in mobile cyber threats, ranging from data breaches to unauthorized access, necessitates a robust and systematic approach to assess and fortify the security of mobile applications.

This project seeks to address the multifaceted security concerns associated with mobile applications by employing a comprehensive framework for assessment. By integrating a combination of static and dynamic analysis techniques, vulnerability scanning, penetration testing, and threat modeling, the project aims to identify and mitigate vulnerabilities before they can be exploited. The rationale behind this initiative lies in the need to establish a proactive defense against evolving mobile security threats, safeguard user privacy, and ensure the resilience of mobile ecosystems.

The Mobile Security Assessment project is a comprehensive initiative aimed at ensuring the robust security posture of mobile applications in the ever-evolving digital landscape. With theubiquitous use of smartphones and the increasing reliance on mobile apps for sensitive transactions, safeguarding user data and thwarting potential cyber threats have become imperative. This project leverages cutting-edge tools and methodologies, including Mobile Security Framework (MobSF) for in-depth vulnerability analysis, the Social-Engineer Toolkit (SET) to simulate social engineering attacks, and the Metasploit Framework (msfconsole) fordynamic penetration testing.

The project encompasses a systematic approach, beginning with defining the scope and objectives, analyzing mobile applications for security vulnerabilities, employing social engineering tactics, and utilizing penetration testing techniques. Subsequently, the identified vulnerabilities are addressed through the implementation of robust hardening measures, fortifying the mobile applications against potential exploits. Through meticulous documentation, continuous monitoring, and proactive updates, this project aims to elevate the overall security resilience of mobile applications, ensuring user data confidentiality, integrity, and availability in the face of evolving cybersecurity challenges.

1.1 PROBLEM STATEMENT

As the usage of mobile applications continues to surge, concerns related to the security of these applications intensify. Mobile devices store sensitive personal and corporate information, making them attractive targets for cyber threats. The pervasive use of mobile devices and the increasing reliance on mobile applications have exposed users and organizations to a growing array of security threats. Mobile applications often handle sensitive data and connect to diverse networks, making them susceptible to vulnerabilities and exploitation. The lack of robust security measures in mobile applications poses a significant risk, leading to unauthorized access, data breaches, and potential compromise of user privacy. Moreover, the rapid evolution of mobile technologies introduces new attack vectors, requiring a proactive approach to assess and address security concerns.

Therefore, there is a critical need for a systematic and comprehensive mobile security assessment project that employs advanced techniques, tools, and methodologies to identify vulnerabilities, evaluate risks, and implement effective countermeasures. This project aims to contribute solutions to enhance the security posture of mobile applications, ultimately safeguarding user data and maintaining the integrity of mobile ecosystems in the face of evolving cyber threats.The objective of this project is to address the growing challenges associated with mobile application security by conducting a comprehensive Mobile Security Assessment initiative.

1.2 ADVANTAGES

- Enhances overall security posture of mobile applications.
- Identifies and mitigates vulnerabilities, reducing the risk of unauthorized access.
- Provides insights into potential security threats, enabling proactive risk mitigation.
- Enhances user awareness through education on mobile security best practices.

2. LITERATURE SURVEY

The integration of mobile devices into daily life has indeed transformed the way people work, communicate, and access information, offering numerous benefits such as flexibility, efficiency, and instant connectivity. This societal shift towards mobile technology has been extensively studied in the literature. Chan et al. (2016) highlights the increasing reliance on mobile devices for various activities, including email communication and social media engagement. The surge in mobile video consumption, as observed by the rise in YouTube and Facebook mobile usage, underscores the widespread adoption of these devices for multimedia content (Chan et al., 2016). This trend has not only altered user behavior but has also introduced security challenges, particularly in safeguarding sensitive information stored on mobile devices.

Security concerns associated with mobile devices are extensively explored in scholarly works. Alimardani and Nazeh (2018) shed light on the evolving landscape of mobile security, emphasizing the vulnerabilities introduced by the storage of sensitive information, such as credit card details and passwords, on these devices. The convenience of mobile banking, allowing users to access financial information on the go, has made mobile devices an attractive target for cyber attackers (Alimardani & Nazeh, 2018). Jin et al. (2020) and Vaghela (2020) delve into the rising threat landscape surrounding mobile devices, where attackers exploit less meticulous security practices compared to traditional computing platforms.

In the context of mobile app vulnerabilities, the literature addresses the increasing risks associated with the vast ecosystem of mobile applications. Researchers have identified diverse vulnerabilities, ranging from insecure data storage and transmission to inadequate authentication mechanisms. The work by Felt et al. (2011) highlights the prevalence of insecure data storage practices in Android apps, while Enck et al. (2011) emphasize the significance of addressing vulnerabilities related to inter-app communication. The expansive user base and diverse app functionalities contribute to the complexity of securing mobile applications, making it imperative to implement robust security measures and conduct thorough assessments to identify and mitigate potential risks. Overall, the literature emphasizes the need for a holistic approach to mobile security, encompassing both device-level and application-level considerations.

3. SURVEY OF TECHNOLOGY

SEToolkit

The Social-Engineer Toolkit (SET) stands as a versatile and robust open-source framework designed for ethical hackers, security professionals, and penetration testers. Developed by TrustedSec, SET focuses on simulating real-world social engineering attacks to evaluate the security posture of systems and networks. SET's rich toolkit encompasses a variety of modules and attack vectors, allowing users to craft sophisticated social engineering scenarios. It includes functionalities such as spear-phishing, credential harvesting, and the creation of malicious payloads. Its modular architecture facilitates customization, enabling security experts to tailor attacks based on specific testing requirements. SET serves as a comprehensive platform for both education and practical assessment, offering an environment where users can understand, emulate, and defend against social engineering threats prevalent in today's dynamiccybersecurity landscape.

At its core, SET is built to enhance the skills and awareness of security practitioners by providing a hands-on experience with the tactics employed by malicious actors. The framework assists in identifying and addressing vulnerabilities related to human behavior, emphasizing the human element as a critical aspect of overall security. SET's utility extends to not only uncovering weaknesses in technical defenses but also in educating users about the importance of vigilance, awareness, and adherence to security best practices. Through its continuous development and integration of the latest attack techniques, SET remains an invaluable resource for the security community, contributing to the ongoing efforts in fortifying digital landscapes against social engineering threats.

MobSF

Mobile Security Framework (MobSF) is an open-source, extensible, and scalable mobile application security testing framework designed to assist security professionals, developers, and penetration testers in comprehensively assessing and enhancing the security of mobile applications. Offering support for both Android and iOS platforms, MobSF integrates a wide array of security testing tools and techniques into a unified framework, providing a holistic approach to mobile application security analysis. MobSF facilitates static analysis by scrutinizing the application's source code for potential vulnerabilities and dynamic analysis by executing the application in a controlled environment to observe its runtime behavior.
Additionally, it aids in the identification of common security issues such as insecure data storage, improper session handling, and insecure communication.

With a modular architecture, MobSF allows users to extend its functionality by integrating additional tools and plugins. Its user-friendly web interface streamlines the assessment process, making it accessible even for users with varying levels of expertise in mobile security.
MobSF's capabilities encompass static analysis, dynamic analysis, malware analysis, and forensic analysis, providing a comprehensive toolkit for the assessment of mobile applications throughout the development lifecycle. By empowering security professionals with robust testing capabilities, MobSF plays a crucial role in fostering the development of secure mobile applications in an ever-evolving threat landscape.

msfconsole

The Metasploit Framework, commonly accessed through its command-line interface known as msfconsole, is a robust and versatile penetration testing tool used in cybersecurity. Developed by Rapid7, Metasploit provides a comprehensive platform for security professionals and ethical hackers to assess and exploit vulnerabilities in computer systems, networks, and applications.

Offering a vast array of pre-built exploits, payloads, and auxiliary modules, MSF facilitates the identification of weaknesses in target systems, enabling security experts to evaluate and strengthen defenses. Its modular architecture allows users to create, customize, and automate complex attack scenarios, making it an indispensable tool for penetration testing, vulnerability research, and ethical hacking. The continually updated and expansive Metasploit community ensures a dynamic and evolving toolset that aligns with the latest security challenges and threatlandscapes.

MSFConsole, as the primary user interface for the Metasploit Framework, provides an interactive and powerful environment for security practitioners. It enables users to navigate through various modules, configure exploit options, and execute attacks seamlessly. The console allows for real-time interaction with exploits, payloads, and post-exploitation modules, providing detailed information on the progress of penetration tests.

4. REQUIREMENT & ANALYSIS

Software Requirement:

Software configurations used are:

- Operating System: Kali Linux, Android

Hardware Requirement:

- Minimum RAM: 512MB.
- Recommended RAM: 2GB.
- Hard Drive Space: 10 GB.
- Minimum 1GHz Pentium processor.

5. METHODOLOGY

1. Define Scope and Objectives:

Clearly outline the scope of the project, including the specific mobile applications, platforms, and network environments to be assessed. Define the project's objectives, such as identifying vulnerabilities, assessing security controls, and implementing effective hardening measures.

2. Setup Environment:

Prepare the testing environment, including the setup of a controlled network and virtualized mobile devices using platforms like Genymotion. Ensure that you have a dedicated testing environment for security assessments.

3. MobSF Analysis:

Utilize MobSF to conduct static and dynamic analysis of the mobile applications. Identify vulnerabilities such as insecure data storage, improper session handling, insecure communication, and other security issues. Analyze the results to prioritize and understand the potential impact of the vulnerabilities.

4. Social Engineering Assessments (SET):

Employ the Social-Engineer Toolkit (SET) to simulate social engineering attacks against mobile users and test their awareness of phishing, malicious links, and other social engineering techniques. Evaluate the effectiveness of security awareness training.

5. Metasploit Framework (msfconsole):

Utilize msfconsole from the Metasploit Framework to perform dynamic penetration testing on the mobile applications. Use pre-built exploits, payloads, and auxiliary modules to simulate attacks and assess the application's resistance to common security threats.

5.1 PROPOSED SYSTEM

The proposed system for the project on Mobile Security Assessment integrates several key tools, including MobSF (Mobile Security Framework), SET (Social-Engineer Toolkit), and MSF (Metasploit Framework), to comprehensively address the security landscape of mobile applications. MobSF serves as the initial analysis tool, leveraging static and dynamic analysis techniques to identify vulnerabilities within the mobile app's code, communication protocols, and storage mechanisms. Once potential weaknesses are identified, SET comes into play, offering a range of social engineering attacks to assess the application's resistance to user manipulation and unauthorized access.

Finally, MSF, accessible through the **msfconsole**, provides a dynamic and extensive framework for penetration testing and exploit development. It aids in probing for vulnerabilities discovered during the earlier stages, allowing security professionals to simulate real-world attacks and assess the application's resilience. By combining these tools, the proposed system not only detects vulnerabilities but also empowers security experts to harden mobile applications against potential threats, ultimately enhancing the overall security posture of the mobile ecosystem.

6. IMPLEMENTATION

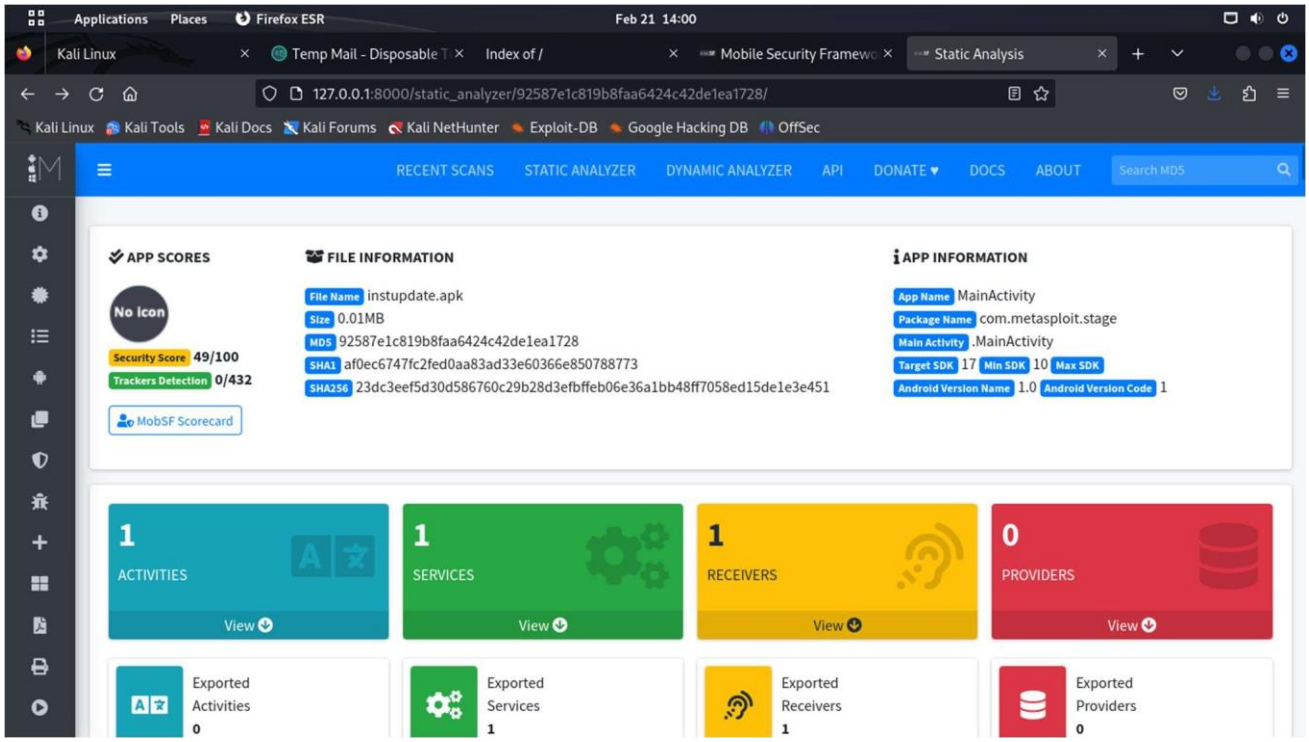


Fig. 7.1 MobSF generated result of scanning an app

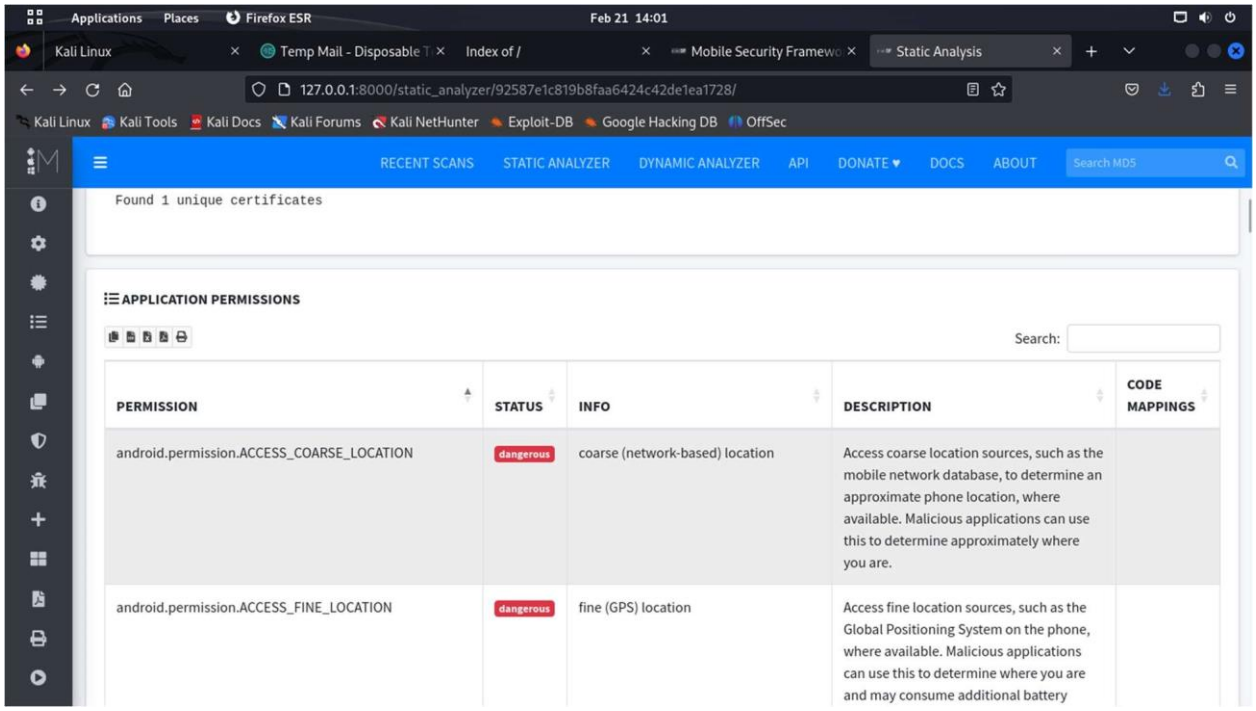
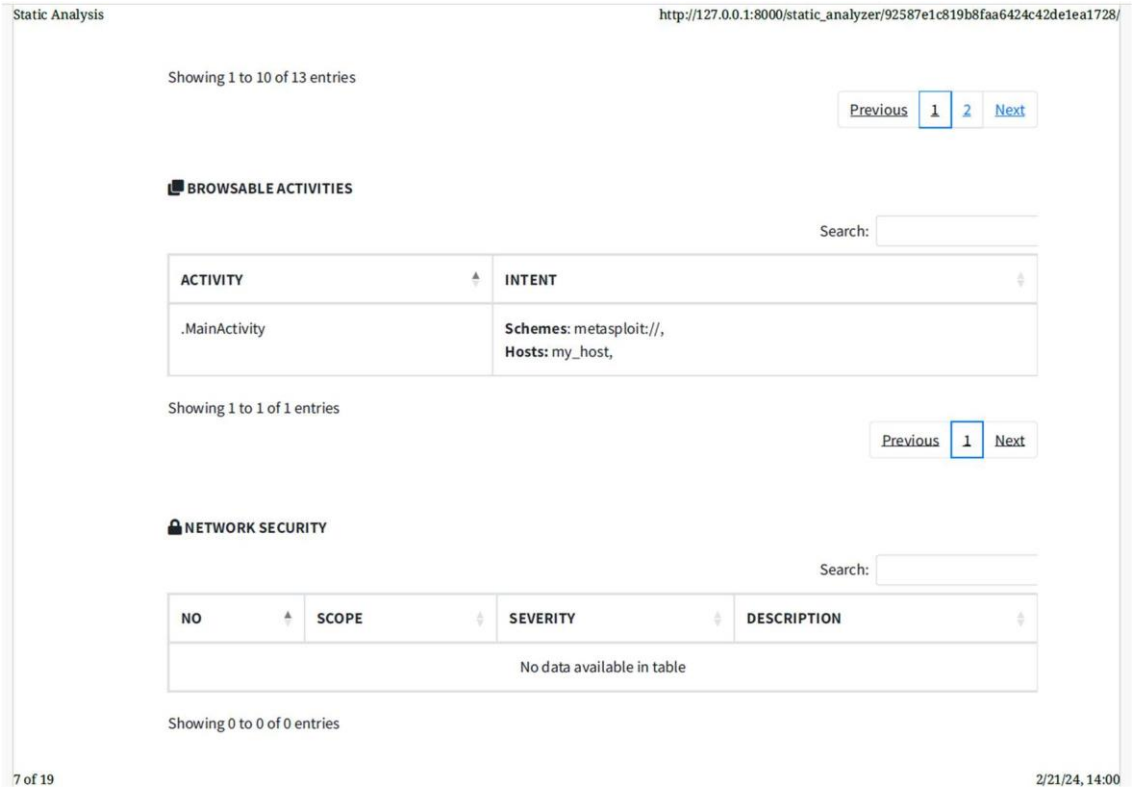
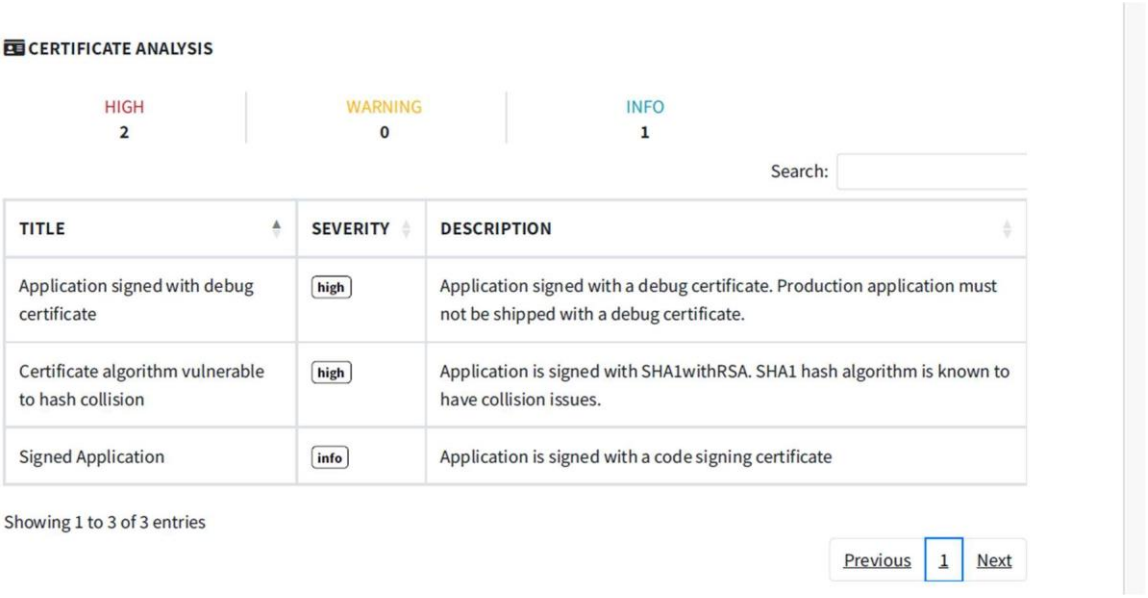


Fig 7.2 Static Analysis report using MobSF

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
android.permission.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.	
android.permission.CHANGE_WIFI_STATE	normal	change Wi-Fi status	Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks.	
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.	
android.permission.READ_CALL_LOG	dangerous	grants read access to the user's call log.	Allows an application to read the user's call log.	


Static Analysis
http://127.0.0.1:8000/static_analyzer/92587e1c819b8faa6424c42de1ea1728/
Showing 1 to 10 of 13 entries
Previous 1 2 Next
BROWSABLE ACTIVITIES
Search:
ACTIVITY
INTENT
.MainActivity
Schemes: metasploit://,
Hosts: my_host,
Showing 1 to 1 of 1 entries
Previous 1 Next
NETWORK SECURITY
Search:
NO
SCOPE
SEVERITY
DESCRIPTION
No data available in table
Showing 0 to 0 of 0 entries
7 of 19
2/21/24, 14:00


CERTIFICATE ANALYSIS
HIGH
2
WARNING
0
INFO
1
Search:
TITLE
SEVERITY
DESCRIPTION
Application signed with debug certificate
high
Application signed with a debug certificate. Production application must not be shipped with a debug certificate.
Certificate algorithm vulnerable to hash collision
high
Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues.
Signed Application
info
Application is signed with a code signing certificate
Showing 1 to 3 of 3 entries
Previous 1 Next

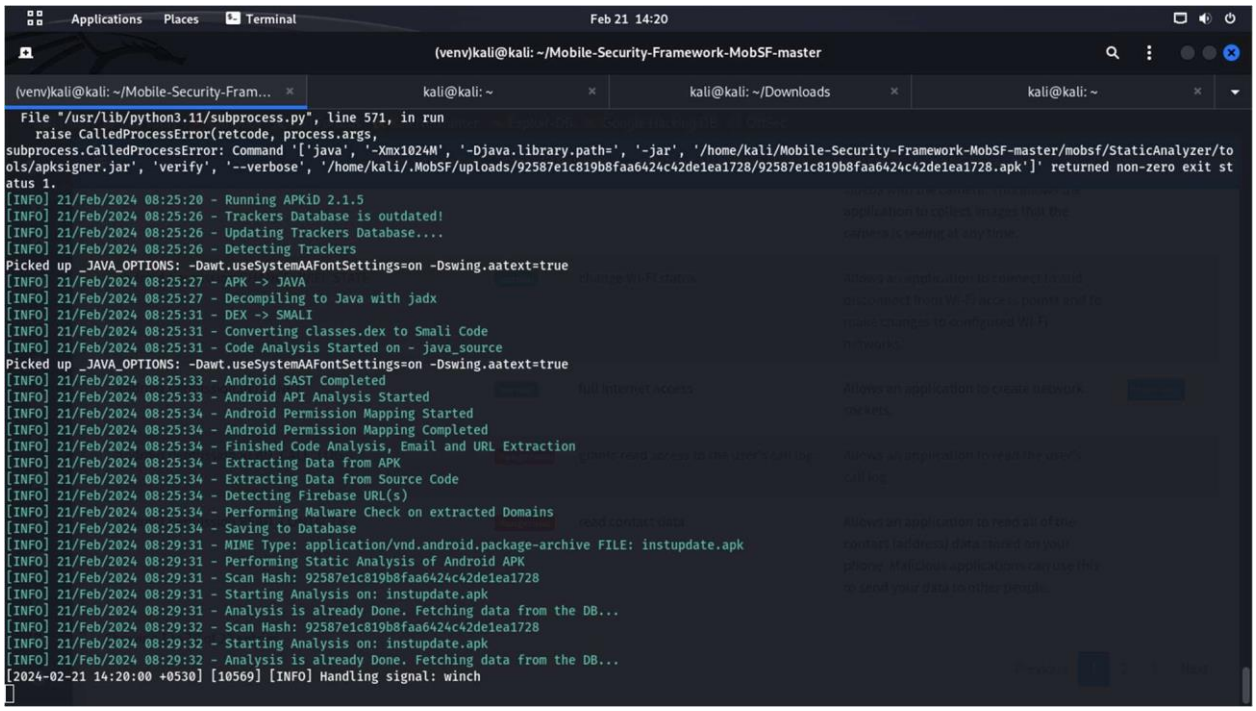


Fig 7.3 MobSF Running

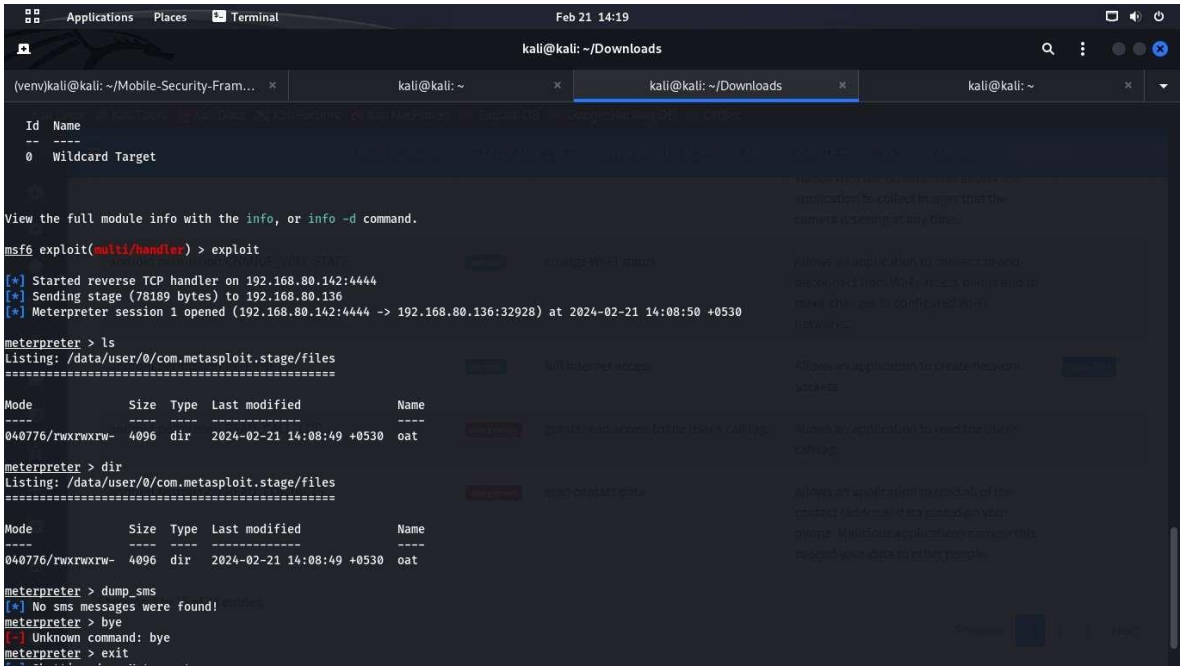


Fig 7.4 Exploit

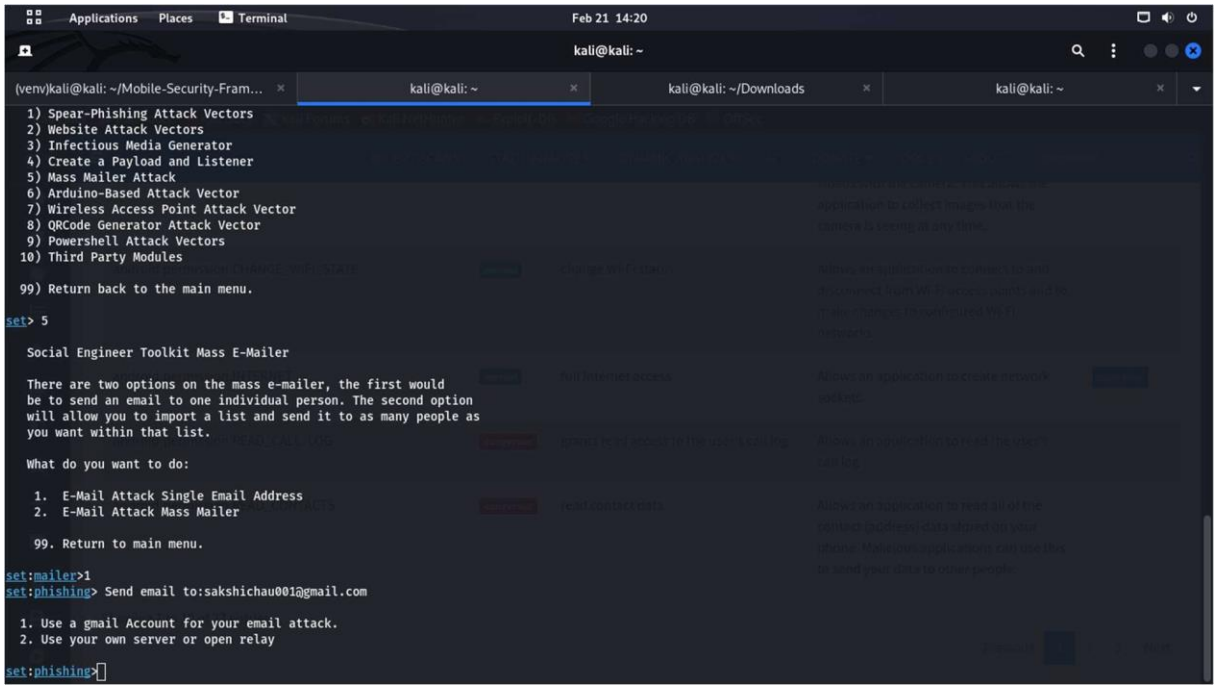


Fig 7.5 Using SEToolkit

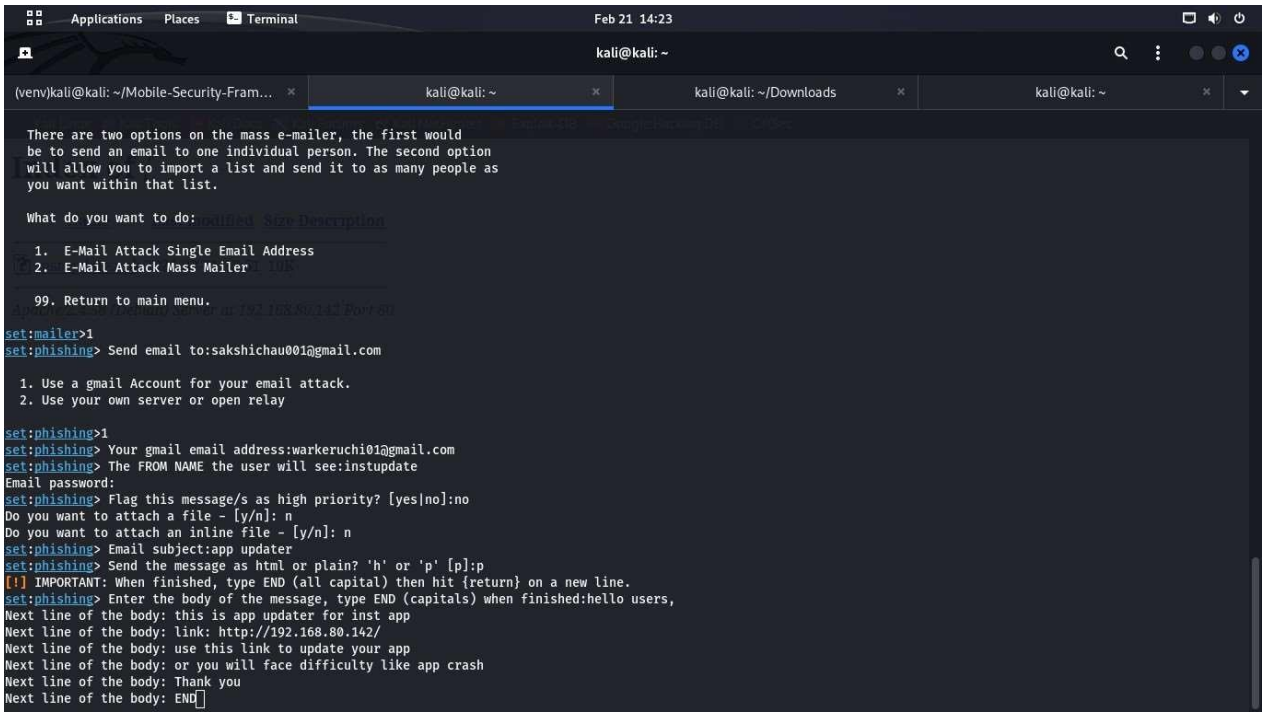


Fig 7.6 Tried email attack single mail address

7. FUTURE SCOPE

The future scope for Mobile Security Assessment projects is vast, considering the ever-evolving landscape of mobile technology and the increasing sophistication of cyber threats. Several areas present opportunities for enhancement and implementation in the future. Firstly, the integration of Artificial Intelligence (AI) and Machine Learning (ML) algorithms can be explored to automate the identification and classification of emerging mobile threats. This would enable quicker and more accurate detection of vulnerabilities, allowing security professionals to proactively address risks. Additionally, the inclusion of advanced anomaly detection mechanisms can improve the real-time monitoring of mobile application behavior, identifying deviations from expected norms and triggering alerts for potential security incidents.

Furthermore, the future of mobile security could witness the development of more sophisticated tools for runtime application self-protection (RASP). These tools can dynamically defend mobile applications against various attacks by detecting and responding to malicious activities in real- time. As mobile applications increasingly rely on cloud-based services and APIs, future projects could focus on assessing the security of these integrations and ensuring the resilience of mobile apps in distributed and interconnected environments.

8. CONCLUSION

The mobile security assessment project have been instrumental in fortifying the resilience of mobile applications against potential cyber threats. The comprehensive analysis conducted using tools like Mobile Security Framework (MobSF) has allowed for the identification and remediation of vulnerabilities, ensuring a robust defense mechanism. Leveraging Social-Engineer Toolkit (SET) and Metasploit Framework (msfconsole) has added a layer of sophistication to the project, enabling the simulation of real-world attack scenarios and enhancing the overall security posture. The project emphasizes a proactive and systematic approach to mobile security, addressing challenges through rigorous assessments and implementing effective hardening measures. By integrating these tools, the project contributes significantly to creating secure mobile applications capable of withstanding the dynamic landscape of cybersecurity threats.

9. REFERENCES

https://github.com/MobSF/Mobile-Security-Framework-MobSF
https://github.com/trustedsec/social-engineer-toolkit
https://www.offsec.com/metasploit-unleashed/msfconsole-commands/