MOBSF

ANDROID STATIC ANALYSIS REPORT

app_icon

TimeSavers

File Name:	TimeSavers.zip
Package Name:	
Scan Date:	Sept. 4, 2024, 2:57 p.m.
App Security Score:	35/100 (HIGH RISK)
Grade:	C

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
4	4	1	1	1

FILE INFORMATION

File Name: TimeSavers.zip
Size: 42.23MB
MD5: ba210927e8e8e016ffe2c9c1947f666f
SHA1: 287bebeb74198a78699c497c0dc2fd9b87f2e130
SHA256: bcb9fa9d43fdda635137d53c6e9f9f46ebc7add28e8b2e5983062bc3ecdbc094

APP INFORMATION

App Name: TimeSavers
Package Name:
Main Activity: .LoginActivity
Target SDK:
Min SDK:
Max SDK:
Android Version Name:
Android Version Code:

APP COMPONENTS

Activities: 6
Services: 0
Receivers: 0
Providers: 0
Exported Activities: 3
Exported Services: 0
Exported Receivers: 0
Exported Providers: 0

CERTIFICATE INFORMATION

Failed to read Code Signing Certificate or none available.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

TITLE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

HIGH: **4** | WARNING: **4** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
2	Activity (.AddEventActivity) is vulnerable to StrandHogg 2.0	high	Activity is found to be vulnerable to StrandHogg 2.0 task hijacking vulnerability. When vulnerable, it is possible for other applications to place a malicious activity on top of the activity stack of the vulnerable application. This makes the application an easy target for phishing attacks. The vulnerability can be remediated by setting the launch mode attribute to "singleInstance" and by setting an empty taskAffinity (taskAffinity=""). You can also update the target SDK version (26) of the app to 29 or higher to fix this issue at platform level.

NO	ISSUE	SEVERITY	DESCRIPTION
3	Activity (.AddEventActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
4	Activity (.LoginActivity) is vulnerable to StrandHogg 2.0	high	Activity is found to be vulnerable to StrandHogg 2.0 task hijacking vulnerability. When vulnerable, it is possible for other applications to place a malicious activity on top of the activity stack of the vulnerable application. This makes the application an easy target for phishing attacks. The vulnerability can be remediated by setting the launch mode attribute to "singleInstance" and by setting an empty taskAffinity (taskAffinity=""). You can also update the target SDK version (26) of the app to 29 or higher to fix this issue at platform level.
5	Activity (.MainActivity) is vulnerable to StrandHogg 2.0	high	Activity is found to be vulnerable to StrandHogg 2.0 task hijacking vulnerability. When vulnerable, it is possible for other applications to place a malicious activity on top of the activity stack of the vulnerable application. This makes the application an easy target for phishing attacks. The vulnerability can be remediated by setting the launch mode attribute to "singleInstance" and by setting an empty taskAffinity (taskAffinity=""). You can also update the target SDK version (26) of the app to 29 or higher to fix this issue at platform level.
6	Activity (.MainActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
7	Activity (.RegistrationActivity) is vulnerable to StrandHogg 2.0	high	Activity is found to be vulnerable to StrandHogg 2.0 task hijacking vulnerability. When vulnerable, it is possible for other applications to place a malicious activity on top of the activity stack of the vulnerable application. This makes the application an easy target for phishing attacks. The vulnerability can be remediated by setting the launch mode attribute to "singleInstance" and by setting an empty taskAffinity (taskAffinity=""). You can also update the target SDK version (26) of the app to 29 or higher to fix this issue at platform level.
8	Activity (.RegistrationActivity) is not Protected. [android:exported=true]	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

CODE ANALYSIS

HIGH: 0 | WARNING: 0 | INFO: 1 | SECURE: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/example/timesavers/ui/tabs/ListFragment.kt

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	2/24	android.permission.READ_EXTERNAL_STORAGE, android.permission.INTERNET
Other Common Permissions	0/45	

Malware Permissions:
Top permissions that are widely abused by known malware.

Other Common Permissions:
Permissions that are commonly abused by known malware.

SCAN LOGS

Timestamp	Event	Error
2024-09-04 14:57:58	Extracting ZIP	OK
2024-09-04 14:57:58	Unzipping	OK
2024-09-04 14:57:58	Detecting source code type	OK
2024-09-04 14:57:58	Source code type - studio	OK
2024-09-04 14:57:58	Generating Hashes	OK
2024-09-04 14:57:59	Getting Hardcoded Certificates/Keystores	OK
2024-09-04 14:57:59	Parsing AndroidManifest.xml	OK
2024-09-04 14:57:59	Extracting Manifest Data	OK
2024-09-04 14:57:59	Fetching Details from Play Store:	OK

2024-09-04 14:58:00	Manifest Analysis Started	OK
2024-09-04 14:58:00	Checking for Malware Permissions	OK
2024-09-04 14:58:00	Guessing icon path	OK
2024-09-04 14:58:00	Code Analysis Started on - java	OK
2024-09-04 14:58:00	Android SAST Completed	OK
2024-09-04 14:58:00	Android API Analysis Started	OK
2024-09-04 14:58:01	Android Permission Mapping Started	OK
2024-09-04 14:58:01	Android Permission Mapping Completed	OK
2024-09-04 14:58:01	Finished Code Analysis, Email and URL Extraction	OK
2024-09-04 14:58:01	Extracting String data from Code	OK
2024-09-04 14:58:01	Extracting String values and entropies from Code	OK

2024-09-04 14:58:01	Performing Malware check on extracted domains	OK
2024-09-04 14:58:03	Updating Trackers Database....	OK
2024-09-04 14:58:03	Detecting Trackers from Domains	OK
2024-09-04 14:58:03	Saving to Database	OK

Report Generated by - MobSF v4.0.7

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.

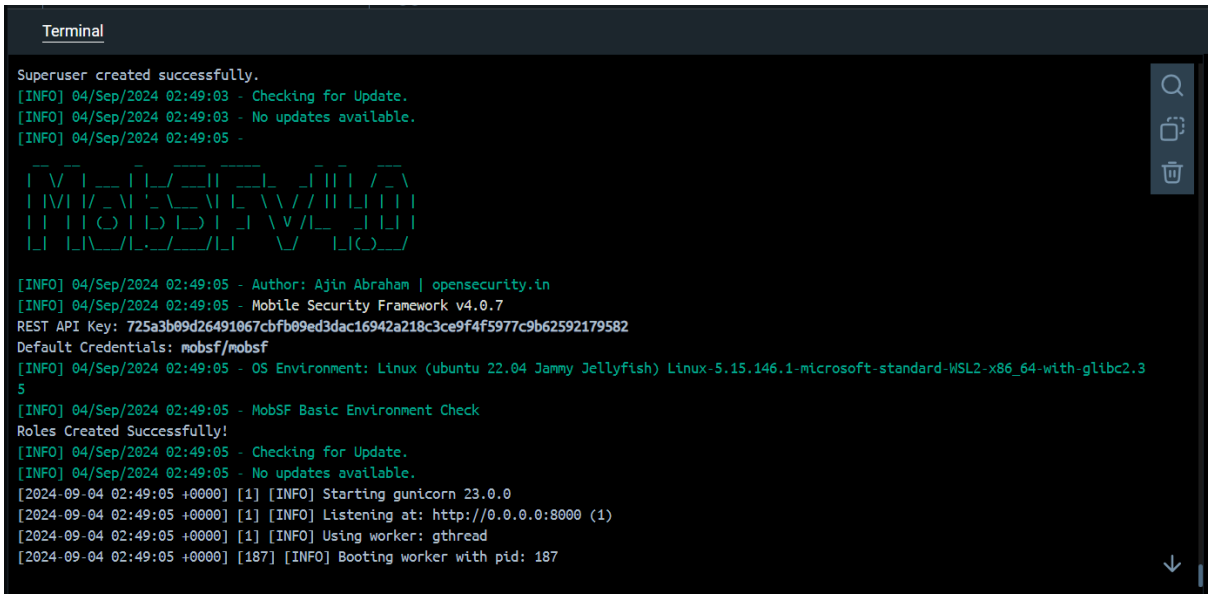
MobSF

Mobile Security Framework (MobSF) is an open-source security tool used when testing mobile applications for vulnerabilities, analysing malware, and assessing security (MobSF, 2024). It supports Android, iOS, and Windows. MobSF can do static analysis, examining the code without running the application; or dynamic analysis, testing the applications in a controlled environment. MobSF enables security teams to detect vulnerabilities, assess the security of applications, and look for probable misconfigurations or malware.

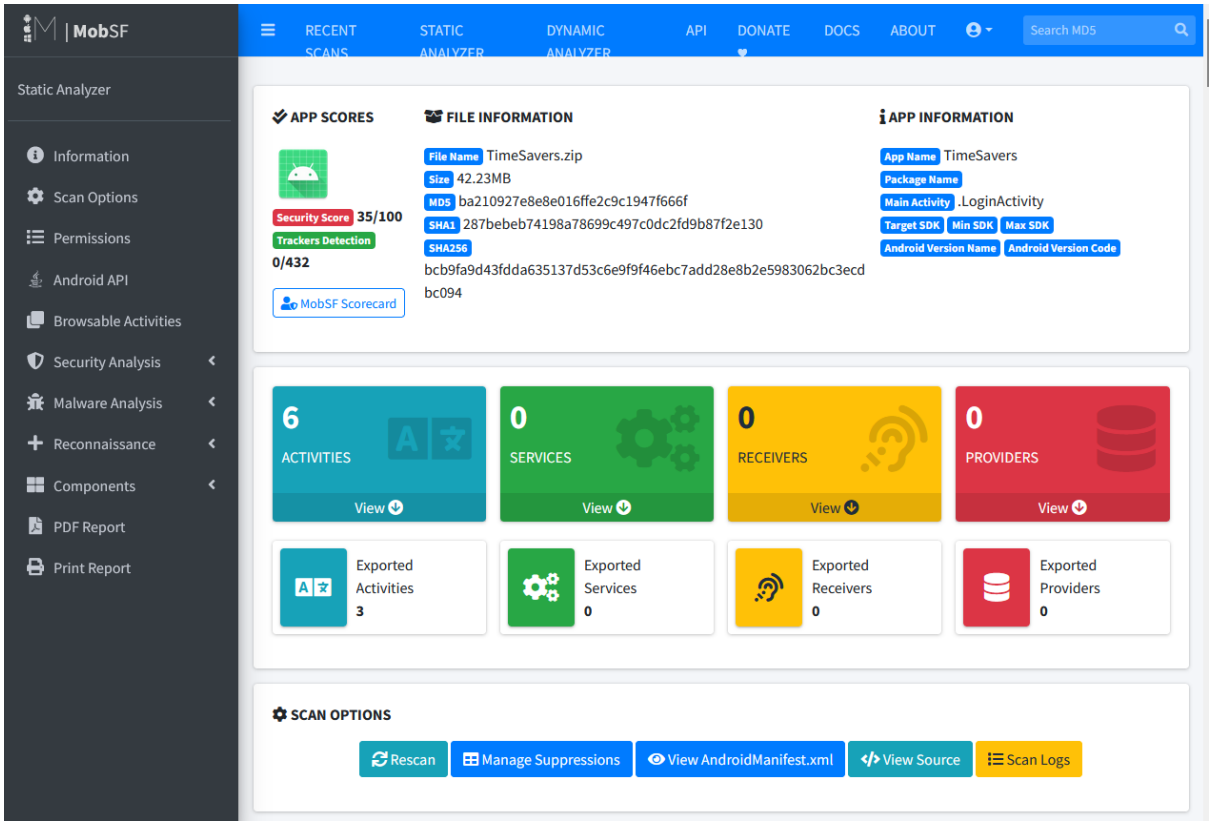
MobSF can be used to ensure their mobile apps follow security best practices. The tool is useful for identifying risks (like insecure app permissions or vulnerabilities), allowing teams to address issues before deploying. (MobSF, 2024).

Running MobSF On Our Android App

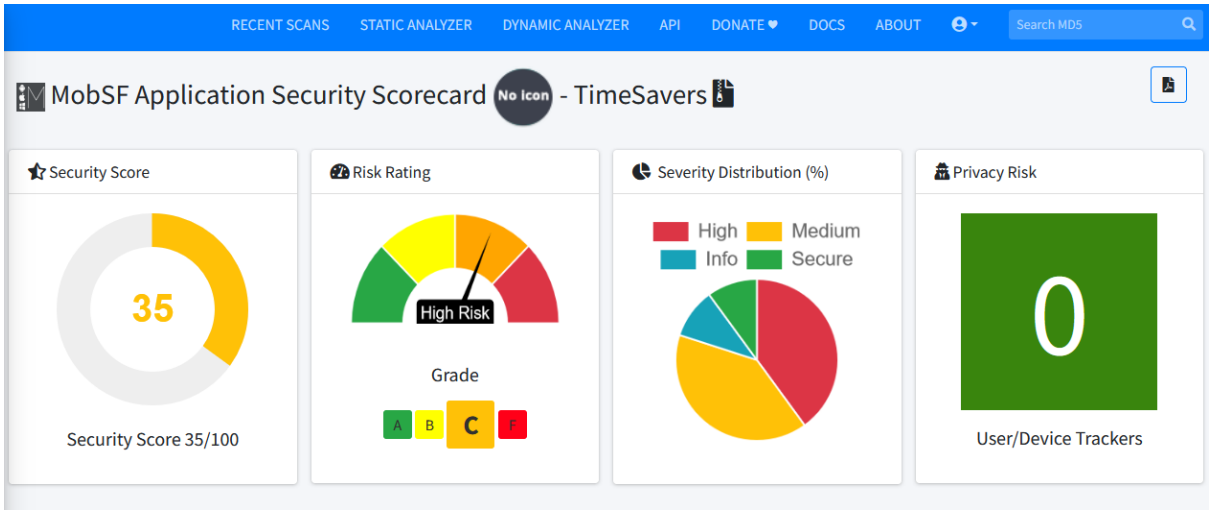
Installing MobSF



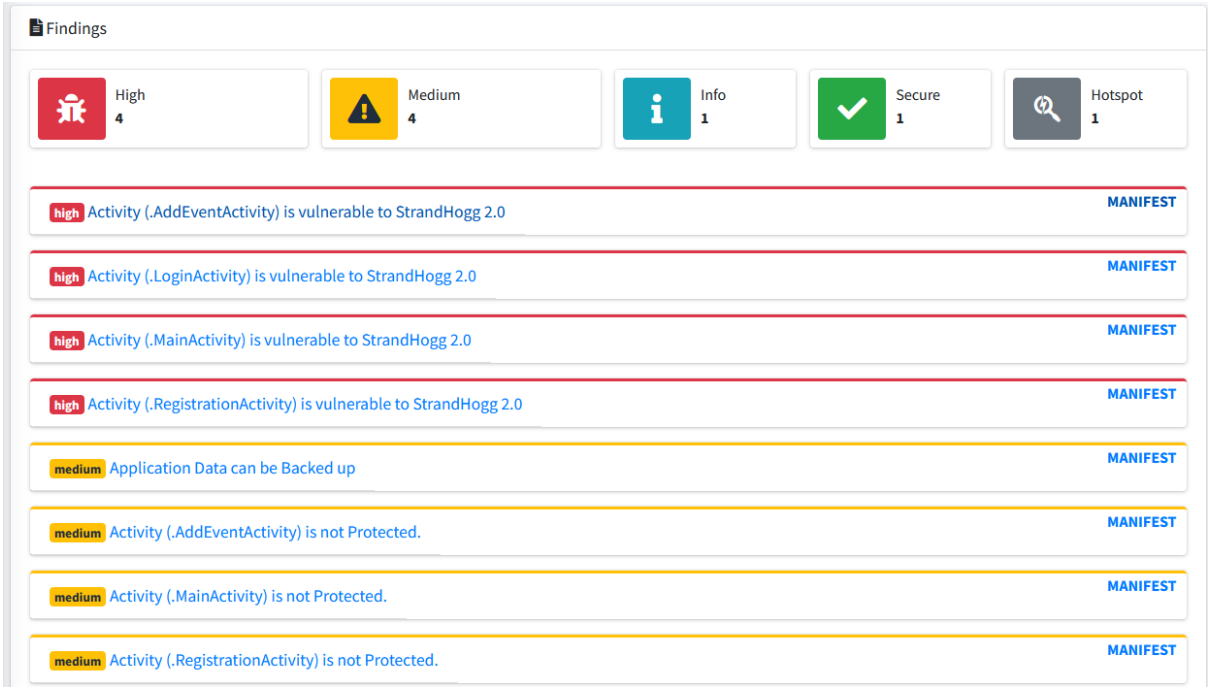
App Analysis



Application Report 1



Application Report 2



Findings Report

The TimeSavers app has been identified to have an App Security Score of 35/100, making it fall under the high-risk category.
These are some of the main findings:

- **StrandHogg 2.0 Vulnerabilities:**
  The app's LoginActivity, AddEventActivity, MainActivity, and RegistrationActivity are all vulnerable to the StrandHogg. This allows malicious apps to overlay the application with a phishing screen. (Android Developers, 2024).
- **Unprotected Activities**:
  The app exposes activities like MainActivity and RegistrationActivity, which can be accessed by other apps on the device. This increases the risk of unauthorized access and security breaches.
- **Dangerous Permissions**:
  READ_EXTERNAL_STORAGE, which could expose user data if not handled securely
  POST_NOTIFICATIONS which allows the app to post notifications, potentially used by malware to deceive users.

Based on the findings from the TimeSavers analysis, MobSF could be an extremely useful tool for our security team. It accurately and quickly found vulnerabilities, it identified unnecessary permissions, and helps ensure that apps follow security best practices.

Given the high-risk issues detected in just the single scan, I recommend that we adopt MobSF for mobile app security assessments to make security testing more efficient and easier, and prevent severe vulnerabilities from being deployed.

REFERENCES

MobSF. 2024. MobSF Documentation. [Online]. Available at: https://mobsf.github.io/docs/#/ [Accessed 8 September 2024].

Android Developers. 2024. StrandHogg Attack / Task Affinity Vulnerability. 28 February 2024. [Online]. Available at: https://developer.android.com/privacy-and-security/risks/strandhogg#resources [Accessed 8 September 2024].