ANDROID STATIC ANALYSIS REPORT

app_icon

KineticPulseMobileApp (1.0)

File Name:	app-debug.apk
Package Name:	com.example.kineticpulsemobileapp
Scan Date:	Nov. 20, 2024, 10:48 a.m.
App Security Score:	55/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
3	6	1	3	1

FILE INFORMATION

File Name: app-debug.apk
Size: 17.88MB
MD5: 97bd19d4d1780499b1c56770df0d5cd1
SHA1: 3bc6dfd6d25ba4622f8bdfa4e9e302ae5c33fbd7
SHA256: 6f2683bb7a844185e38ac5f3de1a5c521e9fecbd63aac7f14bec5a422077cbba

APP INFORMATION

App Name: KineticPulseMobileApp
Package Name: com.example.kineticpulsemobileapp
Main Activity: com.example.kineticpulsemobileapp.LoginScreen
Target SDK: 34
Min SDK: 30
Max SDK:
Android Version Name: 1.0
Android Version Code: 1

APP COMPONENTS

Activities: 8
Services: 4
Receivers: 1
Providers: 2
Exported Activities: 2
Exported Services: 1
Exported Receivers: 1
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: CN=Android Debug, O=Android, C=US
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2024-02-29 14:39:06+00:00
Valid To: 2054-02-21 14:39:06+00:00
Issuer: CN=Android Debug, O=Android, C=US
Serial Number: 0x1
Hash Algorithm: sha256
md5: c6e65f17fc788add9626cf7d21cdf594
sha1: 18bc17fa0097437b8855ba0a2fbc307cbb9d933b
sha256: 5316776cee771dc61aed5cc5784d983318271cbaa57a0107a52dc2a51bada070
sha512: 230345a05c78cb362f4a3f990331c6a8280b91f96e07b5e3e534c627805ab3d0a01e6989c5554368cfdb21bd2a0be20f974b5a7c7ced8e6c23748f439fec7967
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: bbb102994ca9d8d4e093c6271ab64418ab0cd3962d897f792a95bc22e029629d
Found 1 unique certificates

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.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.FOREGROUND_SERVICE_REMOTE_MESSAGING	normal	allows foreground services for remote messaging.	Allows a regular application to use Service.startForeground with the type "remoteMessaging".
android.permission.FOREGROUND_SERVICE_CONNECTED_DEVICE	normal	enables foreground services with connected device use.	Allows a regular application to use Service.startForeground with the type "connectedDevice".
android.permission.BLUETOOTH	normal	create Bluetooth connections	Allows applications to connect to paired bluetooth devices.
android.permission.BLUETOOTH_ADMIN	normal	bluetooth administration	Allows applications to discover and pair bluetooth devices.
android.permission.BLUETOOTH_CONNECT	dangerous	necessary for connecting to paired Bluetooth devices.	Required to be able to connect to paired Bluetooth devices.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
com.example.kineticpulsemobileapp.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes4.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.TAGS check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

FILE	DETAILS
classes3.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr><tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr></table>
classes2.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>yara_issue</td><td>yara issue - dex file recognized by apkid but not yara module</td></tr><tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr></table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.google.firebase.auth.internal.GenericIdpActivity	Schemes: genericidp://, Hosts: firebase.auth, Paths: /,
com.google.firebase.auth.internal.RecaptchaActivity	Schemes: recaptcha://, Hosts: firebase.auth, Paths: /,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 1 | WARNING: 0 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application signed with debug certificate	high	Application signed with a debug certificate. Production application must not be shipped with a debug certificate.

MANIFEST ANALYSIS

HIGH: 1 | WARNING: 5 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	Debug Enabled For App [android:debuggable=true]	high	Debugging was enabled on the app which makes it easier for reverse engineers to hook a debugger to it. This allows dumping a stack trace and accessing debugging helper classes.

NO	ISSUE	SEVERITY	DESCRIPTION
2	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.
3	Activity (com.google.firebase.auth.internal.GenericIdpActivity) 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 (com.google.firebase.auth.internal.RecaptchaActivity) 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.
5	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
6	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

CODE ANALYSIS

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

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/example/kineticpulsemobileapp/RetrofitInstance.java
2	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/kineticpulsemobileapp/LoginScreen.java com/example/kineticpulsemobileapp/TerminalFragment.java
3	Debug configuration enabled. Production builds must not be debuggable.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	com/example/kineticpulsemobileapp/BuildConfig.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	okio/Okio__JvmOkioKt.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/example/kineticpulsemobileapp/BluetoothUtil.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/64191478664/namespaces/firebase:fetch?key=AIzaSyCEm7SPgfdZ6yqK2yA6M2auEyQq60gZl1Y. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	2/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE
Other Common Permissions	3/44	android.permission.FOREGROUND_SERVICE, android.permission.BLUETOOTH, android.permission.BLUETOOTH_ADMIN

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

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

! OFAC SANCTIONED COUNTRIES

This app may communicate with the following OFAC sanctioned list of countries.

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
kinecticpulseapi.onrender.com	ok	**IP:** 216.24.57.252 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
kineticpulseproject-default-rtdb.europe-west1.firebasedatabase.app	ok	**IP:** 34.107.226.223 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

HARDCODED SECRETS

POSSIBLE SECRETS
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Password"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"
"firebase_database_url" : "https://kineticpulseproject-default-rtdb.europe-west1.firebasedatabase.app"
"google_api_key" : "AIzaSyCEm7SPgfdZ6yqK2yA6M2auEyQq60gZl1Y"
"google_crash_reporting_api_key" : "AIzaSyCEm7SPgfdZ6yqK2yA6M2auEyQq60gZl1Y"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Contrasenya"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Adgangskode"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Adgangsnøgle"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "گذرواژه"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "گذرکلید"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "□□□□□"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "□□□□"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "პაროლი"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "■■■■■■"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "■■■■■"

POSSIBLE SECRETS
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "[redacted]"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "[redacted]"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Passord"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Tilgangsnøkkel"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Пароль"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Passwort"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "[redacted]"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "[redacted]"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "[redacted]"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "[redacted]"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Wagwoord"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Wagwoordsleutel"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Парола"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "[redacted]"

POSSIBLE SECRETS
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "[redacted]"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Salasana"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Avainkoodi"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "[redacted]"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "[redacted]"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "[redacted]"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "[redacted]"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Лозинка"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Heslo"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Пароль"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Contrasinal"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "[redacted]"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "[redacted]"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Wachtwoord"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Toegangssleutel"

POSSIBLE SECRETS
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Hasło"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Klucz"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Geslo"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Password"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "[redacted]"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "[redacted]"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "[redacted]"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "[redacted]"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Sandi"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "[redacted]"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "[redacted]"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "□□□□"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "□□□"

POSSIBLE SECRETS
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "ລະຫັດຜ່ານ"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "ກະແຈຜ່ານ"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Parolă"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Fjalëkalimi"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Zaporka"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "■■■■■■■"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "■■■■■"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "■■■■■■■■"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "■■■■■"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Лозинка"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Lozinka"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Şifre"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "■■■■■■■"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "■■■■■"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Lozinka"

POSSIBLE SECRETS
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Heslo"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Contraseña"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Aðgangsorð"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Aðgangslykill"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Parool"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Pääsuvõti"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Password"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Slaptažodis"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Pasahitza"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Sarbide-gakoa"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "[redacted]"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "[redacted]"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Jelszó"

POSSIBLE SECRETS
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Azonosítókulcs"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Пароль"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Iphasiwedi"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Parole"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Lösenord"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Nyckel"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "סיסמה"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Nenosiri"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Գաղտնաբառ"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Անցաբառ"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Сырсөз"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "■■■■■□■□"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "■□□■■■■□■□■■■"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Parol"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Parol"

POSSIBLE SECRETS
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Kod"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Password"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "□□"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "□□"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "□□"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "□□□□"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Senha"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Contraseña"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Palavra-passe"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "□□"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "□□□□"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Senha"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Password"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"

POSSIBLE SECRETS
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Password"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Password"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Password"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650

POSSIBLE SECRETS
115792089210356248762697446949407573529996955224135760342422259061068512044369
bae8e37fc83441b16034566b
a0784d7a4716f3feb4f64e7f4b39bf04
23456789abcdefghjkmnpqrstvwxyz
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
af60eb711bd85bc1e4d3e0a462e074eea428a8
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
36864200e0eaf5284d884a0e77d31646
808182838485868788898a8b8c8d8e8f909192939495969798999a9b9c9d9e9f
394020061963944792122790401001436138050797392704654466679469052796276593991132635693989563081522949135544336539426 43
115792089210356248762697446949407573530086143415290314195533631308867097853951
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
394020061963944792122790401001436138050797392704654466679482934042457217714968703290472660882589380018616069731123 19

SCAN LOGS

Timestamp	Event	Error
2024-11-20 10:48:32	Generating Hashes	OK
2024-11-20 10:48:32	Extracting APK	OK
2024-11-20 10:48:32	Unzipping	OK
2024-11-20 10:48:32	Getting Hardcoded Certificates/Keystores	OK
2024-11-20 10:48:32	Parsing APK with androguard	OK
2024-11-20 10:48:34	Parsing AndroidManifest.xml	OK
2024-11-20 10:48:34	Extracting Manifest Data	OK
2024-11-20 10:48:34	Manifest Analysis Started	OK
2024-11-20 10:48:34	Performing Static Analysis on: KineticPulseMobileApp (com.example.kineticpulsemobileapp)	OK

2024-11-20 10:48:34	Fetching Details from Play Store: com.example.kineticpulsemobileapp	OK
2024-11-20 10:48:35	Checking for Malware Permissions	OK
2024-11-20 10:48:35	Fetching icon path	OK
2024-11-20 10:48:35	Library Binary Analysis Started	OK
2024-11-20 10:48:35	Reading Code Signing Certificate	OK
2024-11-20 10:48:35	Running APKiD 2.1.5	OK
2024-11-20 10:48:43	Updating Trackers Database....	OK
2024-11-20 10:48:43	Detecting Trackers	OK
2024-11-20 10:48:44	Decompiling APK to Java with JADX	OK
2024-11-20 10:49:11	Converting DEX to Smali	OK
2024-11-20 10:49:11	Code Analysis Started on - java_source	OK

2024-11-20 10:49:17	Android SAST Completed	OK
2024-11-20 10:49:17	Android API Analysis Started	OK
2024-11-20 10:49:21	Android API Analysis Completed	OK
2024-11-20 10:49:21	Android Permission Mapping Started	OK
2024-11-20 10:49:24	Android Permission Mapping Completed	OK
2024-11-20 10:49:24	Android Behaviour Analysis Started	OK
2024-11-20 10:49:27	Android Behaviour Analysis Completed	OK
2024-11-20 10:49:27	Extracting Emails and URLs from Source Code	OK
2024-11-20 10:49:27	Email and URL Extraction Completed	OK
2024-11-20 10:49:27	Extracting String data from APK	OK
2024-11-20 10:49:27	Extracting String data from Code	OK

2024-11-20 10:49:27	Extracting String values and entropies from Code	OK
2024-11-20 10:49:29	Performing Malware check on extracted domains	OK
2024-11-20 10:49:30	Saving to Database	OK

Report Generated by - MobSF v4.2.3

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.

© 2024 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.