ANDROID STATIC ANALYSIS REPORT

app_icon

OTP (1.0)

File Name:	OTP.apk
Package Name:	com.example.otp
Scan Date:	Dec. 27, 2024, 3:23 p.m.
App Security Score:	52/100 (MEDIUM RISK)
Grade:	
Trackers Detection:	1/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	8	1	1	0

FILE INFORMATION

File Name: OTP.apk
Size: 7.08MB
MD5: 4dd99b1b78ee9863fbdae04004bd754a
SHA1: 21ae182c264d5772334d3e9bc46109189c126294
SHA256: bf822f590f15a821fd96167bccf8ff34b4f4b48fe6c36091feeb08065952952a

APP INFORMATION

App Name: OTP
Package Name: com.example.otp
Main Activity: com.example.otp.MainActivity
Target SDK: 34
Min SDK: 23
Max SDK:
Android Version Name: 1.0

Android Version Code: 1

APP COMPONENTS

Activities: 7
Services: 5
Receivers: 2
Providers: 2
Exported Activities: 2
Exported Services: 1
Exported Receivers: 1
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: O=Universitas Udayana
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2024-12-27 15:20:31+00:00
Valid To: 2049-12-21 15:20:31+00:00
Issuer: O=Universitas Udayana
Serial Number: 0x1
Hash Algorithm: sha256
md5: 2be067cee933a86c9dbe7f768387dfb9
sha1: 64aac99747c8fce2918025554d5753588c440cb8
sha256: 7201378eb647de188d9bbfe9bb7d738c2e088cb426fbe3ed44983970bedf2707
sha512: 072f04799ef9f90b47afb784fe5d54bc2a166fdf0e685137192672830d56d2296069bd445176e42d77d5e112cac31c8b539ade8d8c4ccd3c15347e3299e0d876
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 6aecf156380a4d4dc7d0bfc9be43924f8e09b753d9f0526a67ecd52ff4e9477d
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.

PERMISSION	STATUS	INFO	DESCRIPTION
com.google.android.providers.gsf.permission.READ_GSERVICES	unknown	Unknown permission	Unknown permission from android reference
com.example.otp.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check Build.MANUFACTURER check Build.TAGS check FINDINGS: Compiler — DETAILS: r8 without marker (suspicious)
classes2.dex	FINDINGS: Compiler — DETAILS: unknown (please file detection issue!)

FILE	DETAILS
classes3.dex	<table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check Build.TAGS check</td></tr><tr><td>Compiler</td><td>r8 without marker (suspicious)</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: 0 | WARNING: 1 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.

MANIFEST ANALYSIS

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

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 6.0-6.0.1, [minSdk=23]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
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.

NO	ISSUE	SEVERITY	DESCRIPTION
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: **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/otp/MainActivity.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/1083717578381/namespaces/firebase:fetch?key=AIzaSyBDcvcXItXkdAc1teKFCStIfx1iABb8flY. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	3/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.WAKE_LOCK

TYPE	MATCHES	PERMISSIONS
Other Common Permissions	2/44	com.google.android.gms.permission.AD_ID, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

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

TRACKERS

TRACKER	CATEGORIES	URL
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

HARDCODED SECRETS

POSSIBLE SECRETS
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Password"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"
"google_api_key" : "AIzaSyBDcvcXItXkdAc1teKFCStIfx1iABb8flY"
"google_crash_reporting_api_key" : "AIzaSyBDcvcXItXkdAc1teKFCStIfx1iABb8flY"

POSSIBLE SECRETS
"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" : "■■■■■"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "■■■■■■■■■■■"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "■■■■■■■■■■"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Passord"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Tilgangsnøkkel"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Пароль"

POSSIBLE SECRETS
"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]"
"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]"

POSSIBLE SECRETS
"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"
"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"

POSSIBLE SECRETS
"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" : "□□□"
"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"

POSSIBLE SECRETS
"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" : "Lozinka"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Şifre"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "[redacted]"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "[redacted]"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Lozinka"
"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"

POSSIBLE SECRETS
"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" : "■■■■■■■"
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "■■■■■"
"android.credentials.TYPE_PASSWORD_CREDENTIAL" : "Jelszó"
"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"

POSSIBLE SECRETS
"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"
"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" : "□□"

POSSIBLE SECRETS
"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"
"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"

POSSIBLE SECRETS
"androidx.credentials.TYPE_PUBLIC_KEY_CREDENTIAL" : "Passkey"
ChNjb20uYW5kcm9pZC52ZW5kaW5nCiBjb20uZ29vZ2xlLmFuZHJvaWQuYXBwcy5tZWV0aW5ncwohY29tLmdvb2dsZS5hbmRyb2lkLmFwcHMubWVzc2FnaW5n
36864200e0eaf5284d884a0e77d31646
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
3940200619639447921227904010014361380507973927046544666794690527962765939911326356939895630815229491355443365394264 3
8081828384858687888 98a8b8c8d8e8f909192939495969798999a9b9c9d9e9f
1157920892103562487626974469494075735300861434152903141955336313088670978539 51
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
3940200619639447921227904010014361380507973927046544666794829340424572177149687032904726608825893800186161606973112319
af60eb711bd85bc1e4d3e0a462e074eea428a8
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
23456789abcdefghjkmnpqrstvwxyz

POSSIBLE SECRETS
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
a0784d7a4716f3feb4f64e7f4b39bf04
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
115792089210356248762697446949407573529996955224135760342422259061068512044369
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
bae8e37fc83441b16034566b
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151

SCAN LOGS

Timestamp	Event	Error
2024-12-27 15:23:33	Generating Hashes	OK
2024-12-27 15:23:33	Extracting APK	OK

2024-12-27 15:23:33	Unzipping	OK
2024-12-27 15:23:33	Parsing APK with androguard	OK
2024-12-27 15:23:34	Extracting APK features using aapt/aapt2	OK
2024-12-27 15:23:35	Getting Hardcoded Certificates/Keystores	OK
2024-12-27 15:23:39	Parsing AndroidManifest.xml	OK
2024-12-27 15:23:39	Extracting Manifest Data	OK
2024-12-27 15:23:39	Manifest Analysis Started	OK
2024-12-27 15:23:39	Performing Static Analysis on: OTP (com.example.otp)	OK
2024-12-27 15:23:39	Fetching Details from Play Store: com.example.otp	OK
2024-12-27 15:23:40	Checking for Malware Permissions	OK

2024-12-27 15:23:40	Fetching icon path	OK
2024-12-27 15:23:40	Library Binary Analysis Started	OK
2024-12-27 15:23:40	Reading Code Signing Certificate	OK
2024-12-27 15:23:41	Running APKiD 2.1.5	OK
2024-12-27 15:23:46	Detecting Trackers	OK
2024-12-27 15:23:52	Decompiling APK to Java with JADX	OK
2024-12-27 15:24:51	Converting DEX to Smali	OK
2024-12-27 15:24:51	Code Analysis Started on - java_source	OK
2024-12-27 15:24:53	Android SBOM Analysis Completed	OK
2024-12-27 15:25:08	Android SAST Completed	OK

2024-12-27 15:25:08	Android API Analysis Started	OK
2024-12-27 15:25:14	Android API Analysis Completed	OK
2024-12-27 15:25:15	Android Permission Mapping Started	OK
2024-12-27 15:25:21	Android Permission Mapping Completed	OK
2024-12-27 15:25:22	Android Behaviour Analysis Started	OK
2024-12-27 15:25:28	Android Behaviour Analysis Completed	OK
2024-12-27 15:25:28	Extracting Emails and URLs from Source Code	OK
2024-12-27 15:25:29	Email and URL Extraction Completed	OK
2024-12-27 15:25:29	Extracting String data from APK	OK
2024-12-27 15:25:29	Extracting String data from Code	OK
2024-12-27 15:25:29	Extracting String values and entropies from Code	OK

2024-12-27 15:25:35	Performing Malware check on extracted domains	OK
2024-12-27 15:25:35	Saving to Database	OK

Report Generated by - MobSF v4.2.9

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.