ANDROID STATIC ANALYSIS REPORT

MHealth (1.18.0)

File Name:	com.meditech.PatientPhm_60.apk
Package Name:	com.meditech.PatientPhm
Scan Date:	Aug. 31, 2025, 3:30 a.m.
App Security Score:	52/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	10	1	2	1

FILE INFORMATION

File Name: com.meditech.PatientPhm_60.apk
Size: 10.34MB
MD5: 6c765bdfa0c62b059b37b1ec147ad827
SHA1: b42af09ff35a67440c86382a46705f9fbe48b0da
SHA256: 22ddf93fa9cf12178d733d167decfffbc4abc776f4af4badef58762e59589a1a

APP INFORMATION

App Name: MHealth
Package Name: com.meditech.PatientPhm
Main Activity: com.example.meditech.eVisit.SplashActivity
Target SDK: 34
Min SDK: 29
Max SDK:
Android Version Name: 1.18.0
Android Version Code: 60

APP COMPONENTS

Activities: 11
Services: 0
Receivers: 0
Providers: 1
Exported Activities: 1
Exported Services: 0
Exported Receivers: 0
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: False
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=MA, L=Westwood, O=MEDITECH, OU=MobilDev, CN=JonathanPrince
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2017-03-15 14:46:32+00:00
Valid To: 2042-03-09 14:46:32+00:00
Issuer: C=US, ST=MA, L=Westwood, O=MEDITECH, OU=MobilDev, CN=JonathanPrince
Serial Number: 0xcabef03
Hash Algorithm: sha256
md5: 135620d625519f3748fd68996fce5a47
sha1: 8c0e120f52f02047e6f29235417edf88c58d00b3
sha256: 3b7abc1bf29ac98e4a95eabf600ea09bc6643b3d457f6461149bd5e72c7cf35c
sha512: 8e1f15fb10db7c59e8f79ea065ae6328694e6843f1141e4ce6e977e364c8224cf337b2d66451ec0a53aee720384fcca57e911f623020cb761ac9b3e2e1ffe6cf
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 31769fc1200c32afaaa856ff86f6c00c12f9615992f62e4f1dd3b36281fd1e8b
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_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
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.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.MODIFY_AUDIO_SETTINGS	normal	change your audio settings	Allows application to modify global audio settings, such as volume and routing.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
com.meditech.PatientPhm.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></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.MANUFACTURER check
Build.TAGS check
possible ro.secure check</td></tr>
<tr><td>Compiler</td><td>unknown (please file detection issue!)</td></tr>
</table>
</td></tr>
</table>

FILE	DETAILS
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.example.meditech.eVisit.PortalActivity	Schemes: https://, Hosts: cdn.meditech.cloud, Path Prefixes: /mhealth,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: **0** | WARNING: **0** | INFO: **1**

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate

MANIFEST ANALYSIS

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

NO	ISSUE	SEVERITY	DESCRIPTION
1	Activity (com.example.meditech.eVisit.PortalActivity) 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: **2** | WARNING: **8** | INFO: **1** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/example/meditech/eVisit/AboutApp.java com/example/meditech/eVisit/BaseActivity.java com/example/meditech/eVisit/EncryptUtil.java com/example/meditech/eVisit/LocationViaLocationManager.java com/example/meditech/eVisit/Messenger.java com/example/meditech/eVisit/ModalWebViewFragment.java com/example/meditech/eVisit/PortalActivity.java com/example/meditech/eVisit/ProvidersFileIO.java com/example/meditech/eVisit/SelectorActivity.java com/example/meditech/eVisit/SettingsActivity.java

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/meditech/eVisit/SettingsActivity.java com/example/meditech/eVisit/SiteDistanceComparatorGCF.java com/example/meditech/eVisit/StartActivity.java com/example/meditech/eVisit/UpdateMessageActivity.java com/example/meditech/eVisit/Utilities.java com/example/meditech/eVisit/helpers/DocumentHelper.java com/example/meditech/eVisit/models/CloudLogging.java com/example/meditech/eVisit/services/Azure.java com/example/meditech/eVisit/services/CheckValidAppVersion.java com/example/meditech/eVisit/services/CheckValidAppVersionGCF.java com/example/meditech/eVisit/services/ConfigService$fetch$2.java com/example/meditech/eVisit/services/GetDNSRecord.java com/example/meditech/eVisit/services/GetDNSResolver.java com/example/meditech/eVisit/services/GetImageFromUrl.java com/example/meditech/eVisit/services/GetSite.java com/example/meditech/eVisit/services/GetSiteGCF.java com/example/meditech/eVisit/services/GoogleCloudFunctions.java com/example/meditech/eVisit/services/SearchSites.java com/example/meditech/eVisit/services/SearchSitesGCF.java com/scottyab/rootbeer/RootBeer.java com/scottyab/rootbeer/RootBeerNative.java com/scottyab/rootbeer/util/QLog.java defpackage/dig.java defpackage/jnamed.java defpackage/lookup.java defpackage/update.java org/codehaus/plexus/util/DirectoryScanner.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				org/codehaus/plexus/util/SweeperPool.java org/codehaus/plexus/util/cli/CommandLineUtils.java org/codehaus/plexus/util/cli/Commandline.java org/codehaus/plexus/util/cli/DefaultConsumer.java org/codehaus/plexus/util/xml/pull/XmlPullParserException.java org/xbill/DNS/Client.java org/xbill/DNS/Compression.java org/xbill/DNS/ExtendedResolver.java org/xbill/DNS/Lookup.java org/xbill/DNS/Name.java org/xbill/DNS/ResolverConfig.java org/xbill/DNS/SimpleResolver.java org/xbill/DNS/TSIG.java org/xbill/DNS/ZoneTransferIn.java org/xbill/DNS/spi/DNSJavaNameService.java
2	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/example/meditech/eVisit/services/Azure.java
3	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	org/codehaus/plexus/util/FileUtils.java org/xbill/DNS/Header.java
4	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/example/meditech/eVisit/models/CloudLogging.java com/example/meditech/eVisit/services/CheckValidAppVersion.java com/example/meditech/eVisit/services/CheckValidAppVersionGCF.java defpackage/jnamed.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
5	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/example/meditech/eVisit/PortalActivity.java com/example/meditech/eVisit/helpers/DocumentHelper.java
6	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/example/meditech/eVisit/PortalActivity.java
7	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/example/meditech/eVisit/PortalActivity.java
8	Remote WebView debugging is enabled.	high	CWE: CWE-919: Weaknesses in Mobile Applications OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	com/example/meditech/eVisit/PortalActivity.java
9	Insecure WebView Implementation. WebView ignores SSL Certificate errors and accept any SSL Certificate. This application is vulnerable to MITM attacks	high	CWE: CWE-295: Improper Certificate Validation OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	com/example/meditech/eVisit/ModalWebViewFragment$webViewClient$1.java com/example/meditech/eVisit/PortalActivity.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
10	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	org/xbill/DNS/DNSSEC.java org/xbill/DNS/NSEC3Record.java
11	This App may request root (Super User) privileges.	warning	CWE: CWE-250: Execution with Unnecessary Privileges OWASP MASVS: MSTG-RESILIENCE-1	com/scottyab/rootbeer/Const.java
12	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	com/scottyab/rootbeer/RootBeer.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00163	Create new Socket and connecting to it	socket	org/xbill/DNS/TCPClient.java org/xbill/DNS/UDPClient.java org/xbill/DNS/ZoneTransferIn.java

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	org/codehaus/plexus/util/DirectoryScanner.java org/codehaus/plexus/util/DirectoryWalker.java org/codehaus/plexus/util/FileUtils.java org/codehaus/plexus/util/cli/Commandline.java org/codehaus/plexus/util/cli/shell/Shell.java org/codehaus/plexus/util/xml/XmlUtil.java
00096	Connect to a URL and set request method	command network	com/example/meditech/eVisit/models/CloudLogging.java com/example/meditech/eVisit/services/ConfigService$fetch$2.java com/example/meditech/eVisit/services/GetImageFromUrl.java
00089	Connect to a URL and receive input stream from the server	command network	com/example/meditech/eVisit/helpers/DocumentHelper.java com/example/meditech/eVisit/helpers/UmaHelper.java com/example/meditech/eVisit/services/ConfigService$fetch$2.java com/example/meditech/eVisit/services/GetImageFromUrl.java org/codehaus/plexus/util/xml/XmlReader.java
00109	Connect to a URL and get the response code	network command	com/example/meditech/eVisit/helpers/DocumentHelper.java com/example/meditech/eVisit/helpers/UmaHelper.java com/example/meditech/eVisit/models/CloudLogging.java com/example/meditech/eVisit/services/ConfigService$fetch$2.java com/example/meditech/eVisit/services/GetImageFromUrl.java
00013	Read file and put it into a stream	file	com/example/meditech/eVisit/ProvidersFileIO.java defpackage/jnamed.java defpackage/update.java org/codehaus/plexus/util/Expand.java org/codehaus/plexus/util/FileUtils.java org/codehaus/plexus/util/PropertyUtils.java org/codehaus/plexus/util/ReaderFactory.java org/codehaus/plexus/util/xml/XmlReader.java org/xbill/DNS/ResolverConfig.java org/xbill/DNS/Tokenizer.java

RULE ID	BEHAVIOUR	LABEL	FILES
00030	Connect to the remote server through the given URL	network	com/example/meditech/eVisit/helpers/DocumentHelper.java com/example/meditech/eVisit/helpers/UmaHelper.java com/example/meditech/eVisit/services/GetImageFromUrl.java
00047	Query the local IP address	network collection	defpackage/jnamed.java
00012	Read data and put it into a buffer stream	file	com/example/meditech/eVisit/ProvidersFileIO.java org/codehaus/plexus/util/xml/XmlReader.java org/xbill/DNS/ResolverConfig.java org/xbill/DNS/Tokenizer.java
00094	Connect to a URL and read data from it	command network	org/codehaus/plexus/util/xml/XmlReader.java
00108	Read the input stream from given URL	network command	org/codehaus/plexus/util/xml/XmlReader.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/example/meditech/eVisit/AboutApp.java com/example/meditech/eVisit/PortalActivity.java com/example/meditech/eVisit/UpdateMessageActivity.java com/example/meditech/eVisit/helpers/DocumentHelper$viewDocument$1.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/example/meditech/eVisit/PortalActivity.java com/example/meditech/eVisit/helpers/DocumentHelper$viewDocument$1.java
00162	Create InetSocketAddress object and connecting to it	socket	org/xbill/DNS/UDPClient.java org/xbill/DNS/ZoneTransferIn.java
00091	Retrieve data from broadcast	collection	com/example/meditech/eVisit/PortalActivity.java com/example/meditech/eVisit/SelectorActivity.java
00024	Write file after Base64 decoding	reflection file	com/example/meditech/eVisit/PortalActivity.java

RULE ID	BEHAVIOUR	LABEL	FILES
00137	Get last known location of the device	location collection	com/example/meditech/eVisit/LocationViaLocationManager.java
00115	Get last known location of the device	collection location	com/example/meditech/eVisit/LocationViaLocationManager.java
00016	Get location info of the device and put it to JSON object	location collection	com/example/meditech/eVisit/services/SearchSites.java

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	9/25	android.permission.INTERNET, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.CAMERA, android.permission.RECORD_AUDIO, android.permission.WAKE_LOCK, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE
Other Common Permissions	1/44	android.permission.MODIFY_AUDIO_SETTINGS

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
mt-dev-url-discovery.documents.azure.com	ok	No Geolocation information available.
home.meditech.com	ok	**IP:** 34.107.130.189 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
us-central1-mobile-site-328315.cloudfunctions.net	ok	**IP:** 216.239.36.54 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
xmlpull.org	ok	**IP:** 185.199.109.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.meditech.com	ok	**IP:** 34.107.130.189 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
play.google.com	ok	**IP:** 142.250.188.238 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.w3.org	ok	**IP:** 104.18.23.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

HARDCODED SECRETS

POSSIBLE SECRETS
atWPbBOZEGX2cegi3di1Sm2oAWa9El9nojxhYo5iABbCXoYdlg40HRghiCxdRbqTUXmbyJ04CVDCwhuXg4TdNg==

POSSIBLE SECRETS
AA87CA22BE8B05378EB1C71EF320AD746E1D3B628BA79B9859F741E082542A385502F25DBF55296C3A545E3872760AB7
FFFFFFFF00000000FFFFFFFFFFFFFFFFBCE6FAADA7179E84F3B9CAC2FC632551
1790b201-2570-4bfd-a6a1-d1c3bc637ec3
3CkSYfA1TEcUDPwz5FtYR0bh1bsGTfyeBsuV1es6ZJIjJaHiibitKfMmpPKXpA7Gx92UgNao50ey9KvZF5f2RQ==
4FE342E2FE1A7F9B8EE7EB4A7C0F9E162BCE33576B315ECECBB6406837BF51F5
3617DE4A96262C6F5D9E98BF9292DC29F8F41DBD289A147CE9DA3113B5F0B8C00A60B1CE1D7E819D7A431D7C90EA0E5F
B3312FA7E23EE7E4988E056BE3F82D19181D9C6EFE8141120314088F5013875AC656398D8A2ED19D2A85C8EDD3EC2AEF
5AC635D8AA3A93E7B3EBBD55769886BC651D06B0CC53B0F63BCE3C3E27D2604B
6B17D1F2E12C4247F8BCE6E563A440F277037D812DEB33A0F4A13945D898C296
8D91E471E0989CDA27DF505A453F2B7635294F2DDF23E3B122ACC99C9E9F1E14
87cb6d5d-0c41-42f6-9727-5aae4658e416

PLAYSTORE INFORMATION

Title: MEDITECH MHealth

Score: 3.0732985 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.meditech.PatientPhm

Developer Details: Medical Information Technology, Inc., Medical+Information+Technology,+Inc., None, https://ehr.meditech.com/support/meditech-mhealth, android-developer-group@meditech.com,

Release Date: Jun 12, 2017 **Privacy Policy:** Privacy link

Description:

MHealth is the mobile version of MEDITECH’s Patient and Consumer Health Portal, which offers secure and convenient access to your health information at your fingertips, on your mobile device or tablet. MHealth offers a wide range of results and features that allow you to better manage your and your family’s care. Use your existing Patient Portal logon ID and password to get started with MHealth. With MHealth, you can: • Communicate securely with your care team • Request new appointments and see details for upcoming visits • Pre-register for upcoming appointments • Review laboratory results and radiology reports • Track immunizations, allergies, and conditions • Manage home medications and request prescription renewals • Reference visit history information and forms, including discharge instructions. If you already have a Patient Portal account through your healthcare provider, and your provider has enabled access through MHealth, you are ready to begin. If you do not already have a Portal account with a MEDITECH affiliate, visit your healthcare provider’s web page to learn how to get started.

SCAN LOGS

Timestamp	Event	Error
2025-08-31 03:30:40	Generating Hashes	OK
2025-08-31 03:30:40	Extracting APK	OK
2025-08-31 03:30:40	Unzipping	OK
2025-08-31 03:30:40	Parsing APK with androguard	OK
2025-08-31 03:30:40	Extracting APK features using aapt/aapt2	OK
2025-08-31 03:30:40	Getting Hardcoded Certificates/Keystores	OK

2025-08-31 03:30:42	Parsing AndroidManifest.xml	OK
2025-08-31 03:30:42	Extracting Manifest Data	OK
2025-08-31 03:30:42	Manifest Analysis Started	OK
2025-08-31 03:30:44	Performing Static Analysis on: MHealth (com.meditech.PatientPhm)	OK
2025-08-31 03:30:46	Fetching Details from Play Store: com.meditech.PatientPhm	OK
2025-08-31 03:30:48	Checking for Malware Permissions	OK
2025-08-31 03:30:48	Fetching icon path	OK
2025-08-31 03:30:48	Library Binary Analysis Started	OK
2025-08-31 03:30:49	Reading Code Signing Certificate	OK
2025-08-31 03:30:50	Running APKiD 2.1.5	OK
2025-08-31 03:30:53	Detecting Trackers	OK

2025-08-31 03:30:55	Decompiling APK to Java with JADX	OK
2025-08-31 03:31:09	Converting DEX to Smali	OK
2025-08-31 03:31:09	Code Analysis Started on - java_source	OK
2025-08-31 03:31:14	Android SBOM Analysis Completed	OK
2025-08-31 03:31:19	Android SAST Completed	OK
2025-08-31 03:31:19	Android API Analysis Started	OK
2025-08-31 03:31:25	Android API Analysis Completed	OK
2025-08-31 03:31:26	Android Permission Mapping Started	OK
2025-08-31 03:31:48	Android Permission Mapping Completed	OK
2025-08-31 03:31:50	Android Behaviour Analysis Started	OK
2025-08-31 03:31:55	Android Behaviour Analysis Completed	OK

2025-08-31 03:31:55	Extracting Emails and URLs from Source Code	OK
2025-08-31 03:31:56	Email and URL Extraction Completed	OK
2025-08-31 03:31:56	Extracting String data from APK	OK
2025-08-31 03:31:56	Extracting String data from Code	OK
2025-08-31 03:31:56	Extracting String values and entropies from Code	OK
2025-08-31 03:31:59	Performing Malware check on extracted domains	OK
2025-08-31 03:32:01	Saving to Database	OK

Report Generated by - MobSF v4.4.0

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.