ANDROID STATIC ANALYSIS REPORT

Full Code (3.3.5)

File Name:	com.minerva_medical.minerva_365.apk
Package Name:	com.minerva_medical.minerva
Scan Date:	Aug. 31, 2025, 5:14 a.m.
App Security Score:	52/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	4/432

FINDINGS SEVERITY

HIGH	MEDIUM	ℹ INFO	✓ SECURE	HOTSPOT
2	13	3	2	1

FILE INFORMATION

File Name: com.minerva_medical.minerva_365.apk
Size: 52.64MB
MD5: ce2846f4415ada8d3c46ee0f427bec9c
SHA1: 1d5225b723f84c5b80238247684af431ffc7c82b
SHA256: d4b6557a715745419689de9ed7cb57d24cb4e71dad441949062124f9270c2d1b

APP INFORMATION

App Name: Full Code
Package Name: com.minerva_medical.minerva
Main Activity: com.minerva_medical.minerva.MainActivity
Target SDK: 34
Min SDK: 24
Max SDK:
Android Version Name: 3.3.5

Android Version Code: 365

APP COMPONENTS

Activities: 7
Services: 7
Receivers: 6
Providers: 3
Exported Activities: 1
Exported Services: 0
Exported Receivers: 2
Exported Providers: 0

CERTIFICATE INFORMATION

```
Binary is signed
v1 signature: False
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2018-02-14 20:55:43+00:00
Valid To: 2048-02-14 20:55:43+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0x5e370c74efb974162128f7c6bd31552ef1996cf1
Hash Algorithm: sha256
md5: 954d4276e0e825b45a7140fe55986975
sha1: 0534420847f310210b18eee315944abf0f31965e
sha256: f4d7c2dc44a1a28eca1b89c80d2c3a7da91379e331cf97e543da9b04ba515fa0
sha512: 40a1a3a5cad5ea9e96decddfad00db9f63462c97fcf388c90ad08769f672a2fd9c0fc17fdd0da90405753254775c03b6657057b9a8178aee40f9ba2bee34107e
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: 3d6b2076b401e914a2cbf39584164f2f1bd8bf9f1623739d224a810a2a6d1603
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.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
com.android.vending.BILLING	normal	application has in-app purchases	Allows an application to make in-app purchases from Google Play.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
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.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.minerva_medical.minerva.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>ce2846f4415ada8d3c46ee0f427bec9c.apk</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>possible VM check</td></tr>
</table>
</td></tr>
</table>

<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>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
SIM operator check
network operator name check
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.minerva_medical.minerva.MainActivity	Schemes: fullcode://,
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.com.minerva_medical.minerva,

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: **2** | WARNING: **3** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 7.0, [minSdk=24]	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	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.

NO	ISSUE	SEVERITY	DESCRIPTION
3	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [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.
4	Activity (com.facebook.CustomTabActivity) 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	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: **8** | INFO: **2** | SECURE: **1** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	C2/a.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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	T2/a.java T2/b.java U2/a.java Y/C0300n.java o0/Q.java
				B0/b.java C1/g.java F0/k.java F1/C0212y.java I0/a.java J/a.java M/a.java Q/n.java R0/a.java R0/d.java T/b.java U0/A.java U0/AbstractC0258b.java U0/C0259c.java U0/D.java U0/E.java U0/k.java U0/x.java U0/y.java V0/A.java V0/AbstractC0278n.java V0/C0274j.java V0/C0279o.java V0/E.java V0/J.java V0/O.java V0/r.java X/a.java X0/v.java Y/C0293g.java Y/E.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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	Y/J.java Y/L.java Y/W.java Y0/AbstractBinderC0309a.java Y0/AbstractC0311c.java Y0/AbstractC0332y.java Y0/B.java Y0/S.java Y0/V.java Y0/W.java Y0/X.java Y0/Z.java Y0/f0.java Y0/j0.java Z/C0336c.java Z/C0339f.java Z/L.java Z/m.java Z/r.java a2/C0356b.java b1/C0486b.java b2/c.java c0/l.java c1/AbstractC0505f.java c1/o.java c1/p.java com/minerva_medical/minerva/b.java d0/C1137e.java d0/C1138f.java f0/C1180a.java g1/AbstractC1207d.java h0/C1220f.java h0/i.java h0/j.java h0/m.java i2/C1242B.java i2/C1244D.java i2/C1251g.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				i2/G.java i2/k.java i2/x.java j/c.java j2/C1265a.java k0/C1268a.java k2/C1274c.java k2/f.java o0/C1337F.java o0/C1359w.java o0/Q.java o0/S.java q1/C1389a.java r1/C1402a.java s/d.java s0/c.java v/f.java w/C1477o.java w1/C1485f.java x0/C1499c.java y0/AbstractC1508A.java y0/C1538x.java z1/C1563f.java z1/n.java
4	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	H1/b.java I1/C0230e.java I1/w.java b0/g.java
5	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	Y/C0288b.java Y/L.java Y/O.java Y/W.java f0/C1189j.java l0/C1278b.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
6	MD5 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	Z/C0337d.java h0/m.java
7	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	o0/Q.java
8	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	a2/C0356b.java x0/C1497a.java
9	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	a2/C0357c.java
10	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	M0/M.java M0/W.java
11	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	F1/AbstractC0198j.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00039	Start a web server	control network	C2/a.java
00014	Read file into a stream and put it into a JSON object	file	H1/f.java N1/a.java a2/C0357c.java i0/j.java l0/C1277a.java q0/k.java
00022	Open a file from given absolute path of the file	file	E/m.java H1/f.java com/minerva_medical/minerva/p.java
00013	Read file and put it into a stream	file	E/m.java F1/H.java H1/f.java L1/e.java N1/a.java Z/C0339f.java a2/C0357c.java com/minerva_medical/minerva/p.java h0/m.java i0/j.java l0/C1277a.java q0/k.java
00005	Get absolute path of file and put it to JSON object	file	H1/f.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	V0/C0275k.java com/minerva_medical/minerva/MainActivity.java com/minerva_medical/minerva/k.java o0/C1337F.java o0/C1338a.java o0/Q.java o0/S.java o0/W.java y0/C1517c.java
00089	Connect to a URL and receive input stream from the server	command network	b0/g.java b2/c.java com/minerva_medical/minerva/c.java x0/C1499c.java
00004	Get filename and put it to JSON object	file collection	i0/f.java q0/c.java u0/C1443a.java
00096	Connect to a URL and set request method	command network	Y/E.java b0/g.java b2/c.java com/minerva_medical/minerva/a.java
00109	Connect to a URL and get the response code	network command	R0/d.java b0/g.java b2/c.java com/minerva_medical/minerva/a.java com/minerva_medical/minerva/c.java
00003	Put the compressed bitmap data into JSON object	camera	Y/E.java c0/l.java

RULE ID	BEHAVIOUR	LABEL	FILES
00015	Put buffer stream (data) to JSON object	file	o0/Q.java
00078	Get the network operator name	collection telephony	o0/Q.java
00009	Put data in cursor to JSON object	file	o0/Q.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	V0/C0275k.java o0/Q.java o0/S.java
00191	Get messages in the SMS inbox	sms	o0/C1337F.java o0/C1338a.java o0/Q.java
00036	Get resource file from res/raw directory	reflection	V0/C0275k.java o0/C1338a.java o0/Q.java o0/S.java o0/W.java
00094	Connect to a URL and read data from it	command network	K1/a.java com/minerva_medical/minerva/c.java
00091	Retrieve data from broadcast	collection	com/minerva_medical/minerva/MainActivity.java o0/C1337F.java y0/AbstractC1511D.java
00012	Read data and put it into a buffer stream	file	Z/C0339f.java h0/m.java
00072	Write HTTP input stream into a file	command network file	com/minerva_medical/minerva/c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00030	Connect to the remote server through the given URL	network	com/minerva_medical/minerva/c.java
00108	Read the input stream from given URL	network command	com/minerva_medical/minerva/c.java
00125	Check if the given file path exist	file	i0/f.java
00189	Get the content of a SMS message	sms	o0/C1337F.java
00188	Get the address of a SMS message	sms	o0/C1337F.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	o0/C1337F.java
00200	Query data from the contact list	collection contact	o0/C1337F.java
00187	Query a URI and check the result	collection sms calllog calendar	o0/C1337F.java
00201	Query data from the call log	collection calllog	o0/C1337F.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	o0/C1337F.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
App talks to a Firebase database	info	The app talks to Firebase database at https://full-code.firebaseio.com
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/706243224957/namespaces/firebase:fetch?key=AIzaSyA3W2dgfUmYs8_Wc9gqYCvivISo7QHakyc. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	4/25	android.permission.INTERNET, android.permission.VIBRATE, android.permission.ACCESS_NETWORK_STATE, android.permission.WAKE_LOCK
Other Common Permissions	3/44	com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE, com.google.android.gms.permission.AD_ID

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
graph-video.s	ok	No Geolocation information available.
mike.fullcodemedical.com	ok	**IP:** 18.155.173.21 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
issuetracker.google.com	ok	**IP:** 142.251.40.46 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
.facebook.com	ok	No Geolocation information available.

DOMAIN	STATUS	GEOLOCATION
play.google.com	ok	**IP:** 142.250.179.110 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
services.fullcodemedical.com	ok	**IP:** 44.212.186.183 **Country:** United States of America **Region:** Virginia **City:** Ashburn **Latitude:** 39.043720 **Longitude:** -77.487488 **View:** Google Map
graph.s	ok	No Geolocation information available.
facebook.com	ok	**IP:** 31.13.70.36 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
firebase.google.com	ok	**IP:** 142.250.179.78 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
clinical.fullcodemedical.com	ok	**IP:** 18.238.96.61 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
developers.facebook.com	ok	**IP:** 31.13.70.1 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
pagead2.googlesyndication.com	ok	**IP:** 142.250.72.162 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
ganymede.local	ok	No Geolocation information available.
app.fullcodemedical.com	ok	**IP:** 18.238.96.125 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
staging.fullcodemedical.com	ok	**IP:** 18.238.96.41 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
dev.fullcodemedical.com	ok	**IP:** 18.238.109.62 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
firebase-settings.crashlytics.com	ok	**IP:** 142.250.176.3 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
full-code.firebaseio.com	ok	**IP:** 34.120.160.131 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
logan.fullcodemedical.com	ok	**IP:** 18.155.173.53 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
www.facebook.com	ok	**IP:** 31.13.70.36 **Country:** United States of America **Region:** California **City:** Los Angeles **Latitude:** 34.052231 **Longitude:** -118.243683 **View:** Google Map
luke.fullcodemedical.com	ok	**IP:** 18.238.96.66 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map
dueces.local	ok	No Geolocation information available.

EMAILS

EMAIL	FILE
u0013android@android.com0 u0013android@android.com	V0/z.java

TRACKERS

TRACKER	CATEGORIES	URL
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

HARDCODED SECRETS

POSSIBLE SECRETS
"com.google.firebase.crashlytics.mapping_file_id" : "fc57708900da41948603428888dc0e10"
"facebook_client_token" : "4d5b9e3a33dab89768216443daf63cac"
"firebase_database_url" : "https://full-code.firebaseio.com"

POSSIBLE SECRETS
"google_api_key" : "AIzaSyA3W2dgfUmYs8_Wc9gqYCvivISo7QHakyc"
"google_crash_reporting_api_key" : "AIzaSyA3W2dgfUmYs8_Wc9gqYCvivISo7QHakyc"
c56fb7d591ba6704df047fd98f535372fea00211
8a3c4b262d721acd49a4bf97d5213199c86fa2b9
470fa2b4ae81cd56ecbcda9735803434cec591fa
df6b721c8b4d3b6eb44c861d4415007e5a35fc95
2438bce1ddb7bd026d5ff89f598b3b5e5bb824b3
9b8f518b086098de3d77736f9458a3d2f6f95a37
a4b7452e2ed8f5f191058ca7bbfd26b0d3214bfc
cc2751449a350f668590264ed76692694a80308a

PLAYSTORE INFORMATION

Title: Full Code Medical Simulation

Score: 4.412214 **Installs:** 1,000,000+ **Price:** 0 **Android Version Support:** **Category:** Medical **Play Store URL:** com.minerva_medical.minerva

Developer Details: Full Code Medical Inc., 5421245799174059448, None, https://fullcodemedical.com/, support@fullcodemedical.com,

Release Date: Jul 22, 2018 **Privacy Policy:** Privacy link

Description:

Full Code is an intuitive, mobile-first simulation designed by medical experts for individuals who want to become better medical professionals, including medical students, residents, physicians, nurses, NPs, PAs, EMTs, paramedics, and more. The platform offers over 200 realistic virtual cases and an engaging, gamelike interface. You can choose from hundreds of possible actions as you diagnose and treat acutely sick patients in this open-ended medical simulation. Daily, deliberate practice is the key to maintaining and improving your clinical skills. Download and play a free case today! Interested in bringing Full Code to your organization or institution? Learn more at fullcodemedical.com! Features: • 200+ case library written and peer-reviewed by expert clinicians • Over 30 diagnostic disciplines, including Emergency Medicine, OBGYN, and Pediatrics • 20+ realistic avatars, including pediatric and adult patients • *NEW* EMS cases and pre-hospital environment • Detailed scoring and full case breakdowns - learn your strengths and weaknesses • Patient AI enables practice with history taking • Full Code Pro + CME provides 100+ hours of accredited CME • Frequent new cases and regular updates TRAIN ON YOUR TERMS Full Code’s on-demand simulation training with realistic virtual patients allows you to practice complex cases and enhance your skills whenever you get a break, wherever you happen to be, on the devices you already own. IMPROVE YOUR CONFIDENCE Full Code's infinitely repeatable cases measure skills in both diagnosis and management, allowing you to learn from your mistakes in a risk-free environment. Build competence so you can face complex real-world cases with confidence. PRACTICE MAKES THE PRACTITIONER Frequent, deliberate practice is the key to clinical success and improving your clinical decision-making ability. Full Code can easily fit into any schedule—whether you're a med student or practicing clinician. NEW CHALLENGES Every case presents a new challenge in Full Code: from routine diagnosis to rare diseases. You’re not just limited to the hospital, either—Full Code has expanded into pre-hospital and EMS content. Get out of the ED and into the ambulance for all new scenarios! LEARN FROM TOP MEDICAL EXPERTS Created by medical educators from some of the top hospitals in the U.S. and peer-reviewed by licensed medical professionals, our simulations are designed with industry-standard medical best practices, setting the bar high for medical students and professionals worldwide. EARN CME CREDIT Complete your continuing medical education (CME) requirements with flexible and engaging simulation challenges accredited through the Accreditation Council for Continuing Medical Education (ACCME). With our PRO+CME subscription, you can earn up to 100 CME credits. Subscribe to Full Code Pro+CME to get started. FEATURED GOOGLE PLAY REVIEWS ★★★★★ “Hands down the best medical sim app I've ever played.” —Huw Gyver ★★★★★ “This is not a game! It is the most realistic portrayal of an ER rotation that I have ever seen.” —Caroline K ★★★★★ This game is one of the most detailed, life-like games I have played in a long time […] Obsessed to the point I have all of my family and friends trying to beat each others’ scores. —Anna Douglas ★★★★★ “A great app for medical and nursing students — really engaging, fun, and educational. I love this app.” —Bodhi Watts ★★★★★ “Absolutely the best learning simulation app I've ever come across. Download now! You won't be sorry!” —Rya K FOLLOW FULL CODE Facebook: facebook.com/fullcodemedical Twitter: @fullcodemedical Instagram: @fullcodemedical TikTok: @fullcodemedical Website: fullcodemedical.com Play on desktop: app.fullcodemedical.com

SCAN LOGS

Timestamp	Event	Error
2025-08-31 05:14:40	Generating Hashes	OK
2025-08-31 05:14:40	Extracting APK	OK

2025-08-31 05:14:40	Unzipping	OK
2025-08-31 05:14:41	Parsing APK with androguard	OK
2025-08-31 05:14:41	Extracting APK features using aapt/aapt2	OK
2025-08-31 05:14:41	Getting Hardcoded Certificates/Keystores	OK
2025-08-31 05:14:43	Parsing AndroidManifest.xml	OK
2025-08-31 05:14:43	Extracting Manifest Data	OK
2025-08-31 05:14:43	Manifest Analysis Started	OK
2025-08-31 05:14:43	Performing Static Analysis on: Full Code (com.minerva_medical.minerva)	OK
2025-08-31 05:14:44	Fetching Details from Play Store: com.minerva_medical.minerva	OK
2025-08-31 05:14:47	Checking for Malware Permissions	OK
2025-08-31 05:14:47	Fetching icon path	OK

2025-08-31 05:14:47	Library Binary Analysis Started	OK
2025-08-31 05:14:47	Reading Code Signing Certificate	OK
2025-08-31 05:14:48	Running APKiD 2.1.5	OK
2025-08-31 05:14:53	Detecting Trackers	OK
2025-08-31 05:14:54	Decompiling APK to Java with JADX	OK
2025-08-31 05:15:03	Converting DEX to Smali	OK
2025-08-31 05:15:03	Code Analysis Started on - java_source	OK
2025-08-31 05:15:04	Android SBOM Analysis Completed	OK
2025-08-31 05:15:11	Android SAST Completed	OK
2025-08-31 05:15:11	Android API Analysis Started	OK
2025-08-31 05:15:16	Android API Analysis Completed	OK

2025-08-31 05:15:17	Android Permission Mapping Started	OK
2025-08-31 05:15:22	Android Permission Mapping Completed	OK
2025-08-31 05:15:23	Android Behaviour Analysis Started	OK
2025-08-31 05:15:29	Android Behaviour Analysis Completed	OK
2025-08-31 05:15:29	Extracting Emails and URLs from Source Code	OK
2025-08-31 05:15:30	Email and URL Extraction Completed	OK
2025-08-31 05:15:30	Extracting String data from APK	OK
2025-08-31 05:15:30	Extracting String data from Code	OK
2025-08-31 05:15:30	Extracting String values and entropies from Code	OK
2025-08-31 05:15:31	Performing Malware check on extracted domains	OK

2025-08-31 05:15:36	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.