

ANDROID STATIC ANALYSIS REPORT



Anime Al Chat (2.4.0)

File Name:	Anime Chat - Al Chat_2.4.0_Apkpure.apk	
Package Name:	com.animega.music	
Scan Date:	Dec. 3, 2023, 11:13 p.m.	
App Security Score:	49/100 (MEDIUM RISK)	
Grade:		

FINDINGS SEVERITY

派 HIGH	▲ MEDIUM	i INFO	✓ SECURE	® HOTSPOT
3	6	4	2	1

FILE INFORMATION

File Name: Anime Chat - Al Chat_2.4.0_Apkpure.apk

Size: 9.25MB

MD5: 4e1903b9a8a38653b50124bfb95a05d6

SHA1: 809d1e6d803e9b54b2a32c469858918832d9229b

SHA256: 3b26231fe36734f10b2aac4e8ba4e7055bd346d1c79e2c12b8a666ec68da0eaf

1 APP INFORMATION

App Name: Anime Al Chat

Package Name: com.animega.music

Main Activity: com.animega.music.views.activities.SplashActivity

Target SDK: 33 Min SDK: 21 Max SDK:

Android Version Name: 2.4.0 **Android Version Code:** 29

B APP COMPONENTS

Activities: 6
Services: 2
Receivers: 1
Providers: 1

Exported Activities: 0 Exported Services: 0 Exported Receivers: 0 Exported Providers: 0

***** CERTIFICATE INFORMATION

Binary is signed v1 signature: True v2 signature: True v3 signature: False v4 signature: False

X.509 Subject: CN=yunus oruc

Signature Algorithm: rsassa_pkcs1v15 Valid From: 2014-05-09 19:29:17+00:00 Valid To: 2039-05-03 19:29:17+00:00

Issuer: CN=yunus oruc Serial Number: 0x5dd1b42e Hash Algorithm: sha256

md5: 9ad767e3016277cb5468a68ea1d9839b

sha1: 8235b7e21ab72da40fcf9930b07595d1d16f95ab

sha256: 0ccc6cb8d7527736c4af03af813f3f176f79ab6cd5f76f451bc6314d7852afa5

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: ef9cfdd08156fd84da90bc6b118ff7a790621c47f859ed131e249f413a3181b4

Found 1 unique certificates

⋮ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
com.android.vending.BILLING	unknown	Unknown permission	Unknown permission from android reference
com.animega.music.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.

M APKID ANALYSIS

FILE	DETAILS		
	FINDINGS	DETAILS	
classes.dex	Anti-VM Code	Build.FINGERPRINT check Build.MANUFACTURER check	
	Compiler	r8 without marker (suspicious)	

FILE	DETAILS	
classes2.dex	FINDINGS	DETAILS
Classes2.uex	Compiler	r8 without marker (suspicious)

△ NETWORK SECURITY

HIGH: 2 | WARNING: 1 | INFO: 2 | SECURE: 0

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	high	Base config is insecurely configured to permit clear text traffic to all domains.
2	*	info	Base config is configured to trustbundled certs @raw/lets_encrypt_r3.
3	*	info	Base config is configured to trustbundled certs @raw/lets_encrypt_e1.
4	*	warning	Base config is configured to trust system certificates.
5	*	high	Base config is configured to trust user installed certificates.

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.

Q MANIFEST ANALYSIS

HIGH: 1 | WARNING: 2 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version [minSdk=21]	warning	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. Support an Android version > 8, API 26 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.
3	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.

NO	ISSUE	SEVERITY	DESCRIPTION
4	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.

</> CODE ANALYSIS

HIGH: 0 | WARNING: 1 | INFO: 2 | 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/animega/music/network/ApiClient.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/airbnb/lottie/LottieAnimationView.java com/airbnb/lottie/PerformanceTracker.java com/airbnb/lottie/utils/LogcatLogger.java com/animega/music/network/GeneralCallBac k.java
3	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	com/animega/music/views/adapters/Messag eAdapter.java
4	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	com/animega/music/views/activities/Upgrad eActivity.java

■ NIAP ANALYSIS v1.3

NO IDENTIFIER REQUIREMENT FEATURE DESCRIPTION

• OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION
DOMAIN	COUNTRIPREGION

Q DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
api.flow-tech.fun	ok	IP: 51.83.126.129 Country: France Region: Hauts-de-France City: Roubaix Latitude: 50.694210 Longitude: 3.174560 View: Google Map

DOMAIN	STATUS	GEOLOCATION
www.termsofservicegenerator.net	ok	IP: 172.64.80.1 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
play.google.com	ok	IP: 142.251.41.46 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
www.privacypolicygenerator.info	ok	IP: 172.64.80.1 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map



EMAIL	FILE
yunussapps@gmail.com com/animega/music/views/fragments/SettingsFragment.java	



POSSIBLE SECRETS

token=LKNLeTW4BBdlABAcQgno3e42C4O8f9F7

token=e05AM2vGn8WAmWKCYGexkYVFbJ1COeRb

258EAFA5-E914-47DA-95CA-C5AB0DC85B11

5e5398f0546d1d7afd62641edb14d82894f11ddc41bce363a0c8d0dac82c9c5a



Title: Anime Chat - Al Chat

Score: 3.0625 Installs: 100,000+ Price: 0 Android Version Support: Category: Productivity Play Store URL: com.animega.music

Developer Details: Flow., Flow., None, None, yunussapps@gmail.com,

Release Date: Nov 20, 2019 Privacy Policy: Privacy link

Description:

Picture having virtual Al anime companions right on your mobile device, available for chats whenever you desire. The sophisticated Al-powered technology comprehends your inquiries and produces responses that sound like those of an anime character, giving you the impression that you are speaking with an anime girlfriend. Additionally, it can suggest a manga or movie to view. Just ASK anime Al. Key Features: Latest ChatGPT technology from Open Al (GPT3.5 & GPT4) Unlimited questions and answers Ability to have dialogs with the anime chat (Al remembers your full chat history) Different virtual Al anime characters or ai companion to chat with Multi-language support (140+ languages) ASK Anime Al Anything: Here are some ideas you can ask Al Chat, powered by ChatGPT and GPT-3, to write for you: Song lyrics, scripts Anime scenarios or anime spoilers:) How to make an anime music video How to edit AMV Favorite anime series to watch Texting tips for your relationship from anime friends A short story about Tokyo Ghoul or Naruto Which anime to watch or read and many more! or Need a virtual anime friend to have a conversation with? I'm here, Anime Al Chat is also your Al anime friend. You can even have some conversations about the anime series you watch. GET FAST ANSWERS You may get quick responses to any question with "anime Al Chat" and its impressive Al capabilities, powered by ChatGPT and GPT-4 API. Whether you need information right away on issues of historical significance, scientific truths, specialized trivia, or pop culture nuances, anime Al Chat can provide it.

SKILLS \(\text{Looking to improve your current abilities or acquire new ones? You can get information, suggestions, and assistance from "anime AI Chat," which makes use of ChatGPT and GPT-3, on a variety of topics. \(\text{Looking BOOST YOUR CREATIVITY} \) Utilize anime AI Chat powered by ChatGPT and the GPT-4 API, to unleash your creativity. Write a poem, some anime ending lyrics, or a short manga. Ask Kaneki what he ate yesterday Imagine a conversation between Kaneki and a modern-day teenager \(\text{LSEP} \) CURRENT WITH THE LATEST ANIME TRENDS \(\text{LNENDS} \) Never miss the newest news or trends in the anime world. Keep up with everything going on in the anime world with "anime AI Chat," supported by ChatGPT and GPT-3. Our anime AI chatbot has you covered for the most recent technology, fashion, and pop culture. Download the anime AI app today to always have access to your ChatGPT and GPT-4 powered virtual anime assistant. Anime AI Chat utilizes the GPT-3.5 & GPT-4 API from OpenAI for its application, however, it is not directly linked or associated with OpenAI. Furthermore, AI Chat does not hold any affiliations with any governmental or political organizations. The data supplied by the AI is intended solely for informational use, and it should not be deemed as official or authoritative. UNLOCK UNLIMITED ACCESS \(\text{Subscribe to get full, uninterrupted access to all the app's features.} \(\text{The selected subscription plan determines the automatic billing rate.} \)

Report Generated by - MobSF v3.7.9 Beta

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.

© 2023 Mobile Security Framework - MobSF | Ajin Abraham | OpenSecurity.