APP SCORES

Security Score 57/100

Trackers Detection 0/432

FILE INFORMATION

File Name polavaram_release_v1.apk

Size 10.66MB

MD5 dd991407dd43c25aaec13ea188502e20

SHA1 09ef589a7bb55a55e1f2d62956c2b9c434ef7435

SHA256 b7fd9b29636b503a43852f7642131a3a72be477ec39644459adeb03b082e88ff

APP INFORMATION

App Name Polavaram

Package Name com.example.polavaram

Main Activity com.example.polavaram.SplashActivity

Target SDK 34 Min SDK 25 Max SDK

Android Version Name 1.0 Android Version Code 1

2 / 7

EXPORTED ACTIVITIES

View All

1 / 5

EXPORTED SERVICES

View All

2 / 10

EXPORTED RECEIVERS

View All

0 / 1

EXPORTED PROVIDERS

View All

SCAN OPTIONS

DECOMPILED CODE

SIGNER CERTIFICATE

```
Binary is signed
v1 signature: False
v2 signature: True
v3 signature: False
v4 signature: False
X.509 Subject: CN=Abhijeet, OU=A, O=A, L=A, ST=A, C=91
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2025-07-03 12:24:38+00:00
Valid To: 2050-06-27 12:24:38+00:00
Issuer: CN=Abhijeet, OU=A, O=A, L=A, ST=A, C=91
Serial Number: 0x1
Hash Algorithm: sha256
md5: 21683dbf65fd35c3f4bbc61d91fc3e5c
sha1: f8c666e2a2b0a6aa8fcc1dd1606b4fa74245649c
sha256: fb5b0b57224403636edb358159da6d839af17013881f52456325d8c4f76420a5
sha512:
95d37ea1b601f931b9d8405529c11347a467f75d40042a1c33f27cb266cb0f84d5c7a4626c52c72e90ad4b4365f58f74dada3216448658f7e6c2832405f17524
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 807732ea1095a812b12cab7f815054fc72b4a63996f1b6f3c03ded492b316b2b
Found 1 unique certificates
```

APPLICATION PERMISSIONS

Search:

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
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.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.	
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.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.	
android.permission.FOREGROUND_SERVICE_DATA_SYNC	normal	permits foreground services for data synchronization.	Allows a regular application to use Service.startForeground with the type "dataSync".	

PERMISSION	STATUS	INFO	DESCRIPTION	CODE MAPPINGS
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.	
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications	
android.permission.READ_MEDIA_IMAGES	dangerous	allows reading image files from external storage.	Allows an application to read image files from external storage.	
android.permission.READ_MEDIA_VIDEO	dangerous	allows reading video files from external storage.	Allows an application to read video files from external storage.	

Showing 1 to 10 of 15 entries

Previous 1 2 Next

ANDROID API

Search:

API	FILES
Android Notifications	
Base64 Decode	
Crypto	
Get System Service	
GPS Location	

API	FILES
HTTP Connection	
Inter Process Communication	
Java Reflection	
Local File I/O Operations	
Message Digest	

Showing 1 to 10 of 14 entries

Previous 1 2 Next

BROWSABLE ACTIVITIES

Search:

ACTIVITY	INTENT
No data available in table	

Showing 0 to 0 of 0 entries

Previous Next

NETWORK SECURITY

HIGH	WARNING	INFO	SECURE
1	1	0	1

Search:

NO	SCOPE	SEVERITY	DESCRIPTION
1	*	secure	Base config is configured to disallow clear text traffic to all domains.
2	*	warning	Base config is configured to trust system certificates.
3	10.0.0.131	high	Domain config is insecurely configured to permit clear text traffic to these domains in scope.

Showing 1 to 3 of 3 entries

Previous 1 Next

CERTIFICATE ANALYSIS

HIGH	WARNING	INFO
0	0	1

Search:

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

Showing 1 to 1 of 1 entries

Previous 1 Next

MANIFEST ANALYSIS

HIGH	WARNING	INFO	SUPPRESSED
1	5	0	0

Search:

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
1	App can be installed on a vulnerable unpatched Android version Android 7.1-7.1.2, [minSdk=25]	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	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.	
3	**Activity** (com.example.polavaram.MainActivity) 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.example.polavaram.CameraXActivity) 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	OPTIONS
5	**Service** (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. **Permission:** android.permission.BIND_JOB_SERVICE [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.work.impl.diagnostics.DiagnosticsReceiver) 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.	

NO	ISSUE	SEVERITY	DESCRIPTION	OPTIONS
7	**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.	

Showing 1 to 7 of 7 entries

Previous 1 Next

</> CODE ANALYSIS

HIGH	WARNING	INFO	SECURE	SUPPRESSED
0	3	1	1	0

Search:

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
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		

NO	ISSUE	SEVERITY	STANDARDS	FILES	OPTIONS
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		
3	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	**OWASP MASVS:** MSTG-NETWORK-4	com/example/polavaram/CallBack/APIClient.java	
4	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		
5	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	com/airbnb/lottie/network/NetworkCache.java	

Showing 1 to 5 of 5 entries

Previous 1 Next

SHARED LIBRARY BINARY ANALYSIS

Search:

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYM STR

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYM STR
1	arm64-v8a/ libimage_processing_util_jni.so	**True** info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	**Dynamic Shared Object (DSO)** info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	**True** info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	**Full RELRO** info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	**None** info The binary does not have run-time search path or RPATH set.	**None** info The binary does not have RUNPATH set.	**True** info The binary has the following fortified functions: ['__memcpy_chk']	**Tru** inf Syn stri

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYM STR
2	arm64-v8a/ libsurface_util_jni.so	**True** info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	**Dynamic Shared Object (DSO)** info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	**True** info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	**Full RELRO** info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	**None** info The binary does not have run-time search path or RPATH set.	**None** info The binary does not have RUNPATH set.	**False** warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/ Flutter libraries.	**Tru** inf Syn stri

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYM STR
3	x86/ libimage_processing_util_jni.so	**True** info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	**Dynamic Shared Object (DSO)** info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	**True** info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	**Full RELRO** info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	**None** info The binary does not have run-time search path or RPATH set.	**None** info The binary does not have RUNPATH set.	**True** info The binary has the following fortified functions: ['__memcpy_chk']	**Tru** info Syn stri

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYM STR
4	x86/libsurface_util_jni.so	**True** info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	**Dynamic Shared Object (DSO)** info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	**True** info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	**Full RELRO** info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	**None** info The binary does not have run-time search path or RPATH set.	**None** info The binary does not have RUNPATH set.	**False** warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/ Flutter libraries.	**Tru** inf Syn stri

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYM STR
5	armeabi-v7a/ libimage_processing_util_jni.so	**True** info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	**Dynamic Shared Object (DSO)** info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	**True** info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	**Full RELRO** info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	**None** info The binary does not have run-time search path or RPATH set.	**None** info The binary does not have RUNPATH set.	**True** info The binary has the following fortified functions: ['__memcpy_chk']	**Tru** inf Syn stri

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYM STR
6	armeabi-v7a/ libsurface_util_jni.so	**True** info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	**Dynamic Shared Object (DSO)** info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	**True** info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	**Full RELRO** info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	**None** info The binary does not have run-time search path or RPATH set.	**None** info The binary does not have RUNPATH set.	**False** warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/ Flutter libraries.	**Tru** inf Syn stri

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYM STR
7	x86_64/ libimage_processing_util_jni.so	**True** info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	**Dynamic Shared Object (DSO)** info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	**True** info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	**Full RELRO** info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	**None** info The binary does not have run-time search path or RPATH set.	**None** info The binary does not have RUNPATH set.	**True** info The binary has the following fortified functions: ['__memcpy_chk']	**Tru** inf Syn stri

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYM STR
8	x86_64/libsurface_util_jni.so	**True** info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	**Dynamic Shared Object (DSO)** info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	**True** info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	**Full RELRO** info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	**None** info The binary does not have run-time search path or RPATH set.	**None** info The binary does not have RUNPATH set.	**False** warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/ Flutter libraries.	**Tru** inf Syn stri

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYM STR
9	arm64-v8a/ libimage_processing_util_jni.so	**True** info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	**Dynamic Shared Object (DSO)** info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	**True** info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	**Full RELRO** info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	**None** info The binary does not have run-time search path or RPATH set.	**None** info The binary does not have RUNPATH set.	**True** info The binary has the following fortified functions: ['__memcpy_chk']	**Tru** info Syn stri

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYM STR
10	arm64-v8a/ libsurface_util_jni.so	**True** info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	**Dynamic Shared Object (DSO)** info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	**True** info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	**Full RELRO** info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	**None** info The binary does not have run-time search path or RPATH set.	**None** info The binary does not have RUNPATH set.	**False** warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/ Flutter libraries.	**Tru** inf Syn stri

Showing 1 to 10 of 16 entries

Previous 1 2 Next

NIAP ANALYSIS v1.3

Search:

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
No data available in table				

Showing 0 to 0 of 0 entries

Previous Next

FILE ANALYSIS

Search:

NO	ISSUE	FILES
No data available in table		

Showing 0 to 0 of 0 entries

Previous Next

FIREBASE DATABASE ANALYSIS

Search:

TITLE	SEVERITY	DESCRIPTION
No data available in table		

Showing 0 to 0 of 0 entries

Previous Next

MALWARE LOOKUP

VirusTotal Report | Triage Report | MetaDefender Report | Hybrid Analysis Report

APKiD ANALYSIS

Search:

DEX	DETECTIONS
classes.dex	

Search:

FINDINGS	DETAILS
Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check
Compiler	r8 without marker (suspicious)

Showing 1 to 2 of 2 entries

Previous 1 Next

DEX	DETECTIONS
classes2.dex	Search:

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

Showing 1 to 2 of 2 entries

Previous 1 Next

Showing 1 to 2 of 2 entries

Previous 1 Next

BEHAVIOUR ANALYSIS

Search:

RULE ID	BEHAVIOUR	LABEL	FILES
00004	Get filename and put it to JSON object	file collection	com/airbnb/lottie/LottieCompositionFactory.java
00005	Get absolute path of file and put it to JSON object	file	com/airbnb/lottie/LottieCompositionFactory.java
00013	Read file and put it into a stream	file	
00022	Open a file from given absolute path of the file	file	
00024	Write file after Base64 decoding	reflection file	com/airbnb/lottie/LottieCompositionFactory.java

RULE ID	BEHAVIOUR	LABEL	FILES
00030	Connect to the remote server through the given URL	network	com/airbnb/lottie/network/DefaultLottieNetworkFetcher.java com/bumptech/glide/load/data/HttpUrlFetcher.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	com/example/polavaram/SettingsActivity.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	com/example/polavaram/SettingsActivity.java com/example/polavaram/fragments/sor_progress/SorReportUploadFragment.java
00075	Get location of the device	collection location	com/example/polavaram/commonObjects/AppLocationService.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/bumptech/glide/load/data/mediastore/ThumbFetcher.java

Showing 1 to 10 of 17 entries

Previous 1 2 Next

ABUSED PERMISSIONS

Top Malware Permissions **8**/25

android.permission.ACCESS_FINE_LOCATION, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_NETWORK_STATE, android.permission.INTERNET, android.permission.CAMERA, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.WAKE_LOCK, android.permission.RECEIVE_BOOT_COMPLETED

Other Common Permissions **2**/44

com.google.android.gms.permission.AD_ID, android.permission.FOREGROUND_SERVICE

Malware Permissions are the top permissions that are widely abused by known malware.

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

SERVER LOCATIONS

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

Search:

DOMAIN	COUNTRY/REGION
No data available in table	

Showing 0 to 0 of 0 entries

Previous Next

DOMAIN MALWARE CHECK

Search:

DOMAIN	STATUS	GEOLOCATION
android.googlesource.com	ok	**IP:** 172.217.194.82 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
ppa.wapcos.co.in	ok	**IP:** 49.249.224.52 **Country:** India **Region:** Delhi **City:** Delhi **Latitude:** 28.666670 **Longitude:** 77.216667 **View:** Google Map
tsecl.wapcos.co.in	ok	**IP:** 49.249.224.45 **Country:** India **Region:** Delhi **City:** Delhi **Latitude:** 28.666670 **Longitude:** 77.216667 **View:** Google Map

Showing 1 to 3 of 3 entries

Previous 1 Next

URLS

Search:

URL	FILE
data:image	com/bumptech/glide/load/model/DataUrlLoader.java
file:///android_asset/	com/bumptech/glide/load/model/AssetUriLoader.java
http://localhost/	retrofit2/Response.java
https://android.googlesource.com/toolchain/llvm-project	lib/arm64-v8a/libsurface_util_jni.so
https://android.googlesource.com/toolchain/llvm-project	lib/x86/libsurface_util_jni.so
https://android.googlesource.com/toolchain/llvm-project	lib/armeabi-v7a/libsurface_util_jni.so
https://android.googlesource.com/toolchain/llvm-project	lib/x86_64/libsurface_util_jni.so
https://android.googlesource.com/toolchain/llvm-project	apktool_out/lib/arm64-v8a/libsurface_util_jni.so
https://android.googlesource.com/toolchain/llvm-project	apktool_out/lib/x86/libsurface_util_jni.so
https://android.googlesource.com/toolchain/llvm-project	apktool_out/lib/armeabi-v7a/libsurface_util_jni.so

Showing 1 to 10 of 13 entries

Previous 1 2 Next

EMAILS

Search:

EMAIL	FILE
polavaram-auth@gov.in	com/example/polavaram/SettingsActivity.java

Showing 1 to 1 of 1 entries

Previous 1 Next

TRACKERS

Search:

TRACKER NAME	CATEGORIES	URL
No data available in table		

Showing 0 to 0 of 0 entries

Previous Next

POSSIBLE HARDCODED SECRETS

▼ Showing all **23** secrets

"google_maps_key" : "AIzaSyCo3HPzxbWJXHgB49k0kPVcIcaaKiLdzWA"

11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650

b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef

d4e3f0a221d53aa8a05c1bac1aadbc9f

86254750241babac4b8d52996a675549

394020061963944792122790401001436138050797392704654466679469052796276593991132635693989563081522949135544336539426 43

aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7

686479766013060971498190079908139321726943530014330540939446345918554318339765605212255964066145455497729631139148085803712198799971664381257 4

028291115057151

115792089210356248762697446949407573529996955224135760342422259061068512044369

a-95ed6082-b8e9-46e8-a73f-ff56f00f5d9d

4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
1cbd3130fa23b59692c061c594c16cc0
3940200619639447921227904010014361380507973927046544666794829340424572177149687032904726608825893800186161606973112319
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372
808892707005449
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
11579208921035624876269744694940757353008614341529031419553363130886709785395 1
16a09e667f3bcc908b2fb1366ea957d3e3adec17512775099da2f590b0667322a
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
640947142a3c917a7d8904471f0c7bbb

A STRINGS

From APK Resource

▸ Show all **9191** strings

From Code

▸ Show all **20571** strings

From Shared Objects

lib/arm64-v8a/libimage_processing_util_jni.so

▸ Show all **5** strings

lib/arm64-v8a/libsurface_util_jni.so

▸ Show all **40** strings

lib/x86/libimage_processing_util_jni.so

▾ Showing all **4** strings

Failed to get ANativeWindow
Failed to get JPEG bytes array pointer.
Failed to lock window.
YuvToRgbJni

lib/x86/libsurface_util_jni.so

▶ Show all **42** strings

lib/armeabi-v7a/libimage_processing_util_jni.so

▶ Show all **9** strings

lib/armeabi-v7a/libsurface_util_jni.so

▶ Show all **46** strings

lib/x86_64/libimage_processing_util_jni.so

▼ Showing all **4** strings
Failed to get ANativeWindow
Failed to get JPEG bytes array pointer.
Failed to lock window.
YuvToRgbJni

lib/x86_64/libsurface_util_jni.so

▶ Show all **43** strings

apktool_out/lib/arm64-v8a/libimage_processing_util_jni.so

▶ Show all **5** strings

apktool_out/lib/arm64-v8a/libsurface_util_jni.so

▶ Show all **40** strings

apktool_out/lib/x86/libimage_processing_util_jni.so

▼ Showing all **4** strings

Failed to get ANativeWindow
Failed to get JPEG bytes array pointer.
Failed to lock window.
YuvToRgbJni

apktool_out/lib/x86/libsurface_util_jni.so

▶ Show all **42** strings

apktool_out/lib/armeabi-v7a/libimage_processing_util_jni.so

▶ Show all **9** strings

apktool_out/lib/armeabi-v7a/libsurface_util_jni.so

▶ Show all **46** strings

apktool_out/lib/x86_64/libimage_processing_util_jni.so

▼ Showing all **4** strings
Failed to get ANativeWindow
Failed to get JPEG bytes array pointer.
Failed to lock window.
YuvToRgbJni

apktool_out/lib/x86_64/libsurface_util_jni.so

▶ Show all **43** strings

ACTIVITIES

▼ Showing all **7** activities
com.example.polavaram.SplashActivity
com.example.polavaram.MainActivity
com.example.polavaram.LoginActivity
com.example.polavaram.SettingsActivity
com.example.polavaram.SyncActivity

com.example.polavaram.CameraXActivity
com.google.android.gms.common.api.GoogleApiActivity

SERVICES

▼ Showing all **5** services
androidx.camera.core.impl.MetadataHolderService
androidx.work.impl.background.systemalarm.SystemAlarmService
androidx.work.impl.background.systemjob.SystemJobService
androidx.work.impl.foreground.SystemForegroundService
androidx.room.MultiInstanceInvalidationService

RECEIVERS

▼ Showing all **10** receivers
com.example.polavaram.SyncCompletedReceiver
androidx.work.impl.utils.ForceStopRunnable$BroadcastReceiver
androidx.work.impl.background.systemalarm.ConstraintProxy$BatteryChargingProxy
androidx.work.impl.background.systemalarm.ConstraintProxy$BatteryNotLowProxy
androidx.work.impl.background.systemalarm.ConstraintProxy$StorageNotLowProxy
androidx.work.impl.background.systemalarm.ConstraintProxy$NetworkStateProxy
androidx.work.impl.background.systemalarm.RescheduleReceiver
androidx.work.impl.background.systemalarm.ConstraintProxyUpdateReceiver
androidx.work.impl.diagnostics.DiagnosticsReceiver
androidx.profileinstaller.ProfileInstallReceiver

PROVIDERS

▼ Showing all **1** providers
androidx.startup.InitializationProvider

LIBRARIES

▼ Showing all **4** libraries
androidx.camera.extensions.impl
org.apache.http.legacy
androidx.window.extensions
androidx.window.sidecar

SBOM

▼ Showing all **82** Versioned Packages
androidx.activity:activity-ktx@1.8.1
androidx.activity:activity@1.8.1
androidx.annotation:annotation-experimental@1.4.1
androidx.appcompat:appcompat-resources@1.7.1
androidx.appcompat:appcompat@1.7.1
androidx.arch.core:core-runtime@dynamic
androidx.asynclayoutinflater:asynclayoutinflater@1.0.0
androidx.camera:camera-camera2@1.4.2
androidx.camera:camera-core@1.4.2
androidx.camera:camera-extensions@1.4.2
androidx.camera:camera-lifecycle@1.4.2
androidx.camera:camera-video@1.4.2
androidx.camera:camera-view@1.4.2
androidx.cardview:cardview@1.0.0
androidx.constraintlayout:constraintlayout@2.2.1
androidx.coordinatorlayout:coordinatorlayout@1.1.0
androidx.core:core-ktx@1.16.0
androidx.core:core-viewtree@1.0.0
androidx.core:core@1.16.0
androidx.cursoradapter:cursoradapter@1.0.0

androidx.customview:customview-poolingcontainer@1.0.0
androidx.customview:customview@1.1.0
androidx.databinding:viewbinding@8.11.0
androidx.documentfile:documentfile@1.0.0
androidx.drawerlayout:drawerlayout@1.1.1
androidx.dynamicanimation:dynamicanimation@1.0.0
androidx.emoji2:emoji2-views-helper@1.3.0
androidx.emoji2:emoji2@1.3.0
androidx.exifinterface:exifinterface@1.3.6
androidx.fragment:fragment-ktx@1.8.8
androidx.fragment:fragment@1.8.8
androidx.interpolator:interpolator@1.0.0
androidx.legacy:legacy-support-core-ui@1.0.0
androidx.legacy:legacy-support-core-utils@1.0.0
androidx.legacy:legacy-support-v4@1.0.0
androidx.lifecycle:lifecycle-extensions@2.2.0
androidx.lifecycle:lifecycle-livedata-core-ktx@2.9.0
androidx.lifecycle:lifecycle-livedata-core@2.9.0
androidx.lifecycle:lifecycle-livedata@2.9.0
androidx.lifecycle:lifecycle-process@2.9.0
androidx.lifecycle:lifecycle-runtime-ktx@2.9.0
androidx.lifecycle:lifecycle-runtime@2.9.0
androidx.lifecycle:lifecycle-service@2.9.0
androidx.lifecycle:lifecycle-viewmodel-ktx@2.9.0
androidx.lifecycle:lifecycle-viewmodel-savedstate@2.9.0
androidx.lifecycle:lifecycle-viewmodel@2.9.0
androidx.loader:loader@1.0.0
androidx.localbroadcastmanager:localbroadcastmanager@1.0.0
androidx.media:media@1.0.0
androidx.navigation:navigation-common@2.9.1
androidx.navigation:navigation-fragment-ktx@2.9.1
androidx.navigation:navigation-fragment@2.9.1
androidx.navigation:navigation-runtime@2.9.1
androidx.navigation:navigation-ui-ktx@2.9.1
androidx.navigation:navigation-ui@2.9.1
androidx.preference:preference@1.2.1
androidx.print:print@1.0.0

androidx.profileinstaller:profileinstaller@1.4.0
androidx.recyclerview:recyclerview@1.4.0
androidx.room:room-ktx@2.7.2
androidx.room:room-runtime@2.7.2
androidx.savedstate:savedstate-ktx@1.3.0
androidx.savedstate:savedstate@1.3.0
androidx.security:security-crypto@1.1.0-beta01
androidx.slidingpanelayout:slidingpanelayout@1.2.0
androidx.sqlite:sqlite-framework@2.5.1
androidx.sqlite:sqlite@2.5.1
androidx.startup:startup-runtime@1.1.1
androidx.swiperefreshlayout:swiperefreshlayout@1.0.0
androidx.tracing:tracing-ktx@1.2.0
androidx.tracing:tracing@1.2.0
androidx.transition:transition@1.5.0
androidx.vectordrawable:vectordrawable-animated@1.1.0
androidx.vectordrawable:vectordrawable@1.1.0
androidx.versionedparcelable:versionedparcelable@1.1.1
androidx.viewpager2:viewpager2@1.1.0-beta02
androidx.viewpager:viewpager@1.0.0
androidx.window:window@1.0.0
androidx.work:work-runtime@2.10.2
com.google.android.material:material@1.12.0
org.jetbrains.kotlinx:kotlinx-coroutines-android@1.7.3
org.jetbrains.kotlinx:kotlinx-coroutines-core@1.7.3

▼ Showing all **21** Packages

a
android.app
android.graphics
android.os
android.telephony
android.view
android.window
b
com.airbnb.lottie
com.bumptech.glide
com.example.polavaram

com.github.mikephil.charting
com.mikhaellopez.circularfillableloaders
d
javax.inject
me.relex.circleindicator
okio
org.intellij.lang.annotations
org.jetbrains.annotations
org.jspecify.annotations
retrofit2

FILES

▸ Show all **1222** files

 Version v4.4.0