



ANDROID STATIC ANALYSIS REPORT



 FamPay (2.2.3)

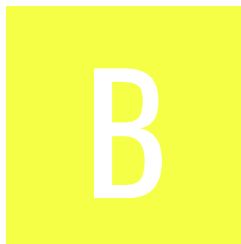
File Name: com.fampay.in_2.2.3-323_minAPI22(arm64-v8a,armeabi,armeabi-v7a,mips,mips64,x86,x86_64)(nodpi)_apkmirror.com.apk

Package Name: com.fampay.in

Scan Date: Dec. 20, 2022, 10:24 a.m.






App Security Score: **47/100 (MEDIUM RISK)**

Grade:



Trackers Detection: **11/428**

FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
2	8	0	1	2

FILE INFORMATION

File Name: com.fampay.in_2.2.3-323_minAPI22(arm64-v8a,armeabi,armeabi-v7a,mips,mips64,x86,x86_64)(nodpi)_apkmirror.com.apk

Size: 37.76MB

MD5: 68c4593a2401de400da929a608fa0b6c

SHA1: 120ba02affcc6df3100638aff2d4eb79b3193ea4

SHA256: bc9251ca3e4641fa659b1539e3d365f81ac3002bcbfec4a78cf1a24b6a91491b

APP INFORMATION

App Name: FamPay

Package Name: com.fampay.in

Main Activity: com.fampay.in.ui.splash.SplashActivity

Target SDK: 31

Min SDK: 22

Max SDK:

Android Version Name: 2.2.3

Android Version Code: 323

APP COMPONENTS

Activities: 157

Services: 28

Receivers: 23

Providers: 10

Exported Activities: 8

Exported Services: 7

Exported Receivers: 7

Exported Providers: 0

CERTIFICATE INFORMATION

APK is signed

v1 signature: True

v2 signature: True

v3 signature: True

Found 1 unique certificates

Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android

Signature Algorithm: rsassa_pkcs1v15

Valid From: 2019-06-30 05:48:58+00:00

Valid To: 2049-06-30 05:48:58+00:00

Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android

Serial Number: 0xaf1ba50f3c7ea4a5e6c308a4c103b31dfc519ae0

Hash Algorithm: sha256

md5: ac39109c327fe7fb447eec623328f449

sha1: 43a2bd6824215be3454b203be7ec9e5a926bdde7

sha256: 50591d2cb6cf057d6728f9e6c2d63f2ec38bca945683d89363ef782930b9c0ce

sha512: 98bd65b80fbee673e8be48dab1e404e6cd45a110f1ffa8643b8f7b4b7e1513b13030e57454a3b1a60671aafc578965b38420db09a8be272959ec92bba84aa163

PublicKey Algorithm: rsa

Bit Size: 4096

Fingerprint: 047b9048f4766ecbc546c31524737dca44d31c4deafc361443a11602c35559f2

☰ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
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.AUTHENTICATE_ACCOUNTS	dangerous	act as an account authenticator	Allows an application to use the account authenticator capabilities of the Account Manager, including creating accounts as well as obtaining and setting their passwords.
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
android.permission.MANAGE_ACCOUNTS	dangerous	manage the accounts list	Allows an application to perform operations like adding and removing accounts and deleting their password.
android.permission.READ_SYNC_SETTINGS	normal	read sync settings	Allows an application to read the sync settings, such as whether sync is enabled for Contacts.
android.permission.USE_CREDENTIALS	dangerous	use the authentication credentials of an account	Allows an application to request authentication tokens.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.WRITE_SYNC_SETTINGS	normal	write sync settings	Allows an application to modify the sync settings, such as whether sync is enabled for Contacts.
android.permission.READ_SYNC_STATS	normal	read sync statistics	Allows an application to read the sync stats; e.g. the history of syncs that have occurred.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
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.FLASHLIGHT	normal	control flashlight	Allows the application to control the flashlight.
android.permission.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.
android.permission.WRITE_CONTACTS	dangerous	write contact data	Allows an application to modify the contact (address) data stored on your phone. Malicious applications can use this to erase or modify your contact data.
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.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
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.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.SEND_SMS	dangerous	send SMS messages	Allows application to send SMS messages. Malicious applications may cost you money by sending messages without your confirmation.
android.permission.READ_SMS	dangerous	read SMS or MMS	Allows application to read SMS messages stored on your phone or SIM card. Malicious applications may read your confidential messages.
android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.

PERMISSION	STATUS	INFO	DESCRIPTION
BIND_GET_INSTALL_REFERRER_SERVICE	unknown	Unknown permission	Unknown permission from android reference
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.USE_BIOMETRIC	normal		Allows an app to use device supported biometric modalities.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
com.google.android.c2dm.permission.RECEIVE	signature	C2DM permissions	Permission for cloud to device messaging.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	unknown	Unknown permission	Unknown permission from android reference
com.google.android.gms.permission.AD_ID	unknown	Unknown permission	Unknown permission from android reference
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
android.permission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.
android.permission.BROADCAST_CLOSE_SYSTEM_DIALOGS	unknown	Unknown permission	Unknown permission from android reference

FILE	DETAILS	
classes.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.TAGS check network operator name check ro.hardware check ro.kernel.qemu check possible ro.secure check possible VM check
	Anti Debug Code	Debug.isDebuggerConnected() check
	Compiler	r8

FILE	DETAILS	
classes2.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check possible Build.SERIAL check Build.TAGS check SIM operator check
	Compiler	r8 without marker (suspicious)

FILE	DETAILS	
classes3.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.BOARD check possible Build.SERIAL check Build.TAGS check network operator name check device ID check
	Anti Debug Code	Debug.isDebuggerConnected() check
	Compiler	r8 without marker (suspicious)

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.fampay.in.deeplink.DeepLinkActivity	Schemes: fp://, https://, http://, upi://, Hosts: fampay.in, fam.one, pay,
com.facebook.CustomTabActivity	Schemes: fbconnect://, Hosts: cct.com.fampay.in,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION
1	westeros.fampay.in	secure	Certificate pinning does not have an expiry. Ensure that pins are updated before certificate expire. [Pin: ++MBgDH5WGvL9Bcn5Be30cRcL0f5O+NyoXuWtQdX1aI= Digest: SHA-256,Pin: f0KW/FtqTjs108NpYj42SrGvOB2PpxlVM8nWxjPqJGE= Digest: SHA-256,Pin: NqvDJlas/GRcYbcWE8S/IceH9cq77kg0jVhZeAPXq8k= Digest: SHA-256,Pin: 9+ze1cZgR9KO1kZrVDxA4HQ6voHRCSVNz4RdTCx4U8U= Digest: SHA-256,Pin: KwccWaCgrnaw6tsrrSO61FgLacNgG2MMLq8GE6+oP5I= Digest: SHA-256]

CERTIFICATE ANALYSIS

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

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
----	-------	----------	-------------

NO	ISSUE	SEVERITY	DESCRIPTION
1	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.
2	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
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.

NO	ISSUE	SEVERITY	DESCRIPTION
4	Service (co.hyperverge.crashguard.services.CrashIntentService) 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.
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.
6	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.

NO	ISSUE	SEVERITY	DESCRIPTION
7	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.

</> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
----	-------	----------	-----------	-------

🚩 SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
----	---------------	----	-----------------	-------	---------	---------	---------------------

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	lib/mips/libduktape.so	<p>True info</p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This shared object 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.</p>	<p>None info</p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The shared object does not have RUNPATH set.</p>	<p>False warning</p> <p>The shared object 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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
2	lib/mips/libaudio-processor.so	<p>True info</p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>False high</p> <p>This shared object does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries.</p>	<p>None info</p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The shared object does not have RUNPATH set.</p>	<p>False warning</p> <p>The shared object 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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
3	lib/armeabi-v7a/libduktape.so	<p>True info</p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This shared object 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.</p>	<p>None info</p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The shared object does not have RUNPATH set.</p>	<p>False warning</p> <p>The shared object 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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	lib/armeabi-v7a/libtool-checker.so	<p>True info</p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>False high</p> <p>This shared object does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries.</p>	<p>None info</p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The shared object does not have RUNPATH set.</p>	<p>False warning</p> <p>The shared object 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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
5	lib/armeabi-v7a/libaudio-processor.so	<p>True info</p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>False high</p> <p>This shared object does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries.</p>	<p>None info</p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The shared object does not have RUNPATH set.</p>	<p>False warning</p> <p>The shared object 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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
6	lib/armeabi-v7a/libimage_processing_util_jni.so	<p>True info</p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This shared object 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.</p>	<p>None info</p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The shared object does not have RUNPATH set.</p>	<p>False warning</p> <p>The shared object 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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
7	lib/armeabi-v7a/libndp-detector.so	<p>True info</p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>False high</p> <p>This shared object does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries.</p>	<p>None info</p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The shared object does not have RUNPATH set.</p>	<p>False warning</p> <p>The shared object 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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
8	lib/armeabi-v7a/libbarhopper_v3.so	<p>True info</p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This shared object 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.</p>	<p>None info</p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The shared object does not have RUNPATH set.</p>	<p>False warning</p> <p>The shared object 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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
9	lib/armeabi/libduktape.so	<p>True info</p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This shared object 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.</p>	<p>None info</p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The shared object does not have RUNPATH set.</p>	<p>False warning</p> <p>The shared object 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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
10	lib/armeabi/libaudio-processor.so	<p>True info</p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>False high</p> <p>This shared object does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries.</p>	<p>None info</p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The shared object does not have RUNPATH set.</p>	<p>False warning</p> <p>The shared object 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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
11	lib/x86/libduktape.so	<p>True info</p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This shared object 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.</p>	<p>None info</p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The shared object does not have RUNPATH set.</p>	<p>False warning</p> <p>The shared object 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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
12	lib/x86/libtool-checker.so	<p>True info</p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This shared object 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.</p>	<p>None info</p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The shared object does not have RUNPATH set.</p>	<p>False warning</p> <p>The shared object 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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
13	lib/x86/libaudio-processor.so	<p>True info</p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This shared object 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.</p>	<p>None info</p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The shared object does not have RUNPATH set.</p>	<p>False warning</p> <p>The shared object 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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
14	lib/x86/libimage_processing_util_jni.so	<p>True info</p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This shared object 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.</p>	<p>None info</p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The shared object does not have RUNPATH set.</p>	<p>False warning</p> <p>The shared object 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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
15	lib/x86/libndp-detector.so	<p>True info</p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This shared object 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.</p>	<p>None info</p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The shared object does not have RUNPATH set.</p>	<p>False warning</p> <p>The shared object 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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
16	lib/x86/libbarhopper_v3.so	<p>True info</p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This shared object 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.</p>	<p>None info</p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The shared object does not have RUNPATH set.</p>	<p>False warning</p> <p>The shared object 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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
17	lib/arm64-v8a/libduktape.so	<p>True info</p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This shared object 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.</p>	<p>None info</p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The shared object does not have RUNPATH set.</p>	<p>False warning</p> <p>The shared object 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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
18	lib/arm64-v8a/libtool-checker.so	<p>True info</p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>False high</p> <p>This shared object does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries.</p>	<p>None info</p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The shared object does not have RUNPATH set.</p>	<p>False warning</p> <p>The shared object 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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
19	lib/arm64-v8a/libaudio-processor.so	<p>True info</p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>False high</p> <p>This shared object does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries.</p>	<p>None info</p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The shared object does not have RUNPATH set.</p>	<p>False warning</p> <p>The shared object 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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
20	lib/arm64-v8a/libimage_processing_util_jni.so	<p>True info</p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This shared object 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.</p>	<p>None info</p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The shared object does not have RUNPATH set.</p>	<p>True info</p> <p>The shared object has the following fortified functions: ['__memmove_chk', '__memcpy_chk']</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
21	lib/arm64-v8a/libndp-detector.so	<p>True info</p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>False high</p> <p>This shared object does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries.</p>	<p>None info</p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The shared object does not have RUNPATH set.</p>	<p>False warning</p> <p>The shared object 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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
22	lib/arm64-v8a/libbarhopper_v3.so	<p>True info</p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This shared object 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.</p>	<p>None info</p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The shared object does not have RUNPATH set.</p>	<p>True info</p> <p>The shared object has the following fortified functions: ['__strlen_chk', '__vsprintf_chk', '__read_chk']</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
23	lib/x86_64/libduktape.so	<p>True info</p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This shared object 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.</p>	<p>None info</p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The shared object does not have RUNPATH set.</p>	<p>False warning</p> <p>The shared object 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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
24	lib/x86_64/libtool-checker.so	<p>True info</p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>False high</p> <p>This shared object does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries.</p>	<p>None info</p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The shared object does not have RUNPATH set.</p>	<p>False warning</p> <p>The shared object 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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
25	lib/x86_64/libaudio-processor.so	<p>True info</p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>False high</p> <p>This shared object does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries.</p>	<p>None info</p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The shared object does not have RUNPATH set.</p>	<p>False warning</p> <p>The shared object 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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
26	lib/x86_64/libimage_processing_util_jni.so	<p>True info</p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This shared object 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.</p>	<p>None info</p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The shared object does not have RUNPATH set.</p>	<p>True info</p> <p>The shared object has the following fortified functions: ['__memcpy_chk']</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
27	lib/x86_64/libndp-detector.so	<p>True info</p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This shared object 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.</p>	<p>None info</p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The shared object does not have RUNPATH set.</p>	<p>False warning</p> <p>The shared object 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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
28	lib/x86_64/libbarhopper_v3.so	<p>True info</p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This shared object 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.</p>	<p>None info</p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The shared object does not have RUNPATH set.</p>	<p>True info</p> <p>The shared object has the following fortified functions: ['__strlen_chk', '__vsprintf_chk', '__read_chk']</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
29	lib/mips64/libduktape.so	<p>True info</p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>True info</p> <p>This shared object 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.</p>	<p>None info</p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The shared object does not have RUNPATH set.</p>	<p>False warning</p> <p>The shared object 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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NO	SHARED OBJECT	NX	STACK CANARY	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
30	lib/mips64/libaudio-processor.so	<p>True info</p> <p>The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.</p>	<p>False high</p> <p>This shared object does not have a stack canary value added to the stack. Stack canaries are used to detect and prevent exploits from overwriting return address. Use the option -fstack-protector-all to enable stack canaries.</p>	<p>None info</p> <p>The shared object does not have run-time search path or RPATH set.</p>	<p>None info</p> <p>The shared object does not have RUNPATH set.</p>	<p>False warning</p> <p>The shared object 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.</p>	<p>True info</p> <p>Symbols are stripped.</p>

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
----	------------	-------------	---------	-------------

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
192.168.19.137	ok	IP: 192.168.19.137 Country: - Region: - City: - Latitude: 0.000000 Longitude: 0.000000 View: Google Map
fampayandroid.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
www.tensorflow.org	ok	IP: 142.250.74.78 Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
friends.fampay.in	ok	IP: 52.21.33.16 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map

DOMAIN	STATUS	GEOLOCATION
test.cashfree.com	ok	IP: 15.207.171.179 Country: India Region: Maharashtra City: Mumbai Latitude: 19.014410 Longitude: 72.847939 View: Google Map
626b6e45.ngrok.io	ok	IP: 3.134.125.175 Country: United States of America Region: Ohio City: Columbus Latitude: 39.961182 Longitude: -82.998787 View: Google Map
www.cashfree.com	ok	IP: 13.235.230.74 Country: India Region: Maharashtra City: Mumbai Latitude: 19.014410 Longitude: 72.847939 View: Google Map
fampay.in	ok	IP: 65.9.44.98 Country: United States of America Region: Washington City: Seattle Latitude: 47.606209 Longitude: -122.332069 View: Google Map

FIREBASE DATABASES

FIREBASE URL	DETAILS
<code>https://fampayandroid.firebaseio.com/.json</code>	high Firebase DB is exposed publicly.

EMAILS

EMAIL	FILE
android-sdk-releaser@vopo7.prod	lib/armeabi-v7a/libbarhopper_v3.so
android-sdk-releaser@vopo7.prod	lib/x86/libbarhopper_v3.so
android-sdk-releaser@vopo7.prod	lib/arm64-v8a/libbarhopper_v3.so
android-sdk-releaser@vopo7.prod	lib/x86_64/libbarhopper_v3.so

TRACKERS

TRACKER	CATEGORIES	URL
AppsFlyer	Analytics	https://reports.exodus-privacy.eu.org/trackers/12
CleverTap	Analytics, Profiling, Location	https://reports.exodus-privacy.eu.org/trackers/174

TRACKER	CATEGORIES	URL
Facebook Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/66
Facebook Login	Identification	https://reports.exodus-privacy.eu.org/trackers/67
Facebook Share		https://reports.exodus-privacy.eu.org/trackers/70
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49
MixPanel	Advertisement, Analytics	https://reports.exodus-privacy.eu.org/trackers/118
Segment	Analytics, Profiling	https://reports.exodus-privacy.eu.org/trackers/62
SmartLook	Profiling, Location	https://reports.exodus-privacy.eu.org/trackers/291

HARDCODED SECRETS

POSSIBLE SECRETS
"content_authority" : "com.android.contacts"
"facebook_client_token" : "26fe5767297386e9e2d02b3316cb0ab8"
"firebase_database_url" : "https://fampayandroid.firebaseio.com"

POSSIBLE SECRETS
"freshchat_file_provider_authority" : ""
"google_api_key" : "AlzaSyBGRhHxZjeKuInp6D3SBca_FXCdlad-1m0"
"google_crash_reporting_api_key" : "AlzaSyBGRhHxZjeKuInp6D3SBca_FXCdlad-1m0"
"password" : "Password"

PLAYSTORE INFORMATION

Title: FamPay : Teen UPI Payment App

Score: 4.39 **Installs:** 10,000,000+ **Price:** 0 **Android Version Support:** **Category:** Finance **Play Store URL:** [com.fampay.in](https://play.google.com/store/apps/details?id=com.fampay.in)

Developer Details: FamPay, 8507326308533346818, None, <https://fampay.in/>, support@fampay.in,

Release Date: None **Privacy Policy:** [Privacy link](#)

Description:

India's first UPI and card payments for teenagers is here! Introducing the best prepaid card and UPI app for teenagers (13-19-year-olds). FamPay helps teens to make payments, online and offline through the FamCard & UPI ID, exclusively for teenagers. Our aim is to drive the smart generation from cash to digital, all without a bank account, through a family-friendly, safe app. Teenagers can now make secure payments, after ensuring their parents and they themselves have completed their KYC verification. FamPay ensures the highest safety and security for its users. □□ Make your own payments as a teenager → Create your own UPI ID for teens and make easy money transfer. → Send money to and request money from friends and family with UPI payments. → Make lightning-fast payments with FamPay for teenagers. → Make easy online and offline payments at your favorite stores using the FamCard & UPI for teenagers. → Pay with your numberless FamCard - the best prepaid card for teens. → Scan and pay through QR Codes for digital payments through your UPI ID. □ Get Rewarded → Earn rewards for making digital payments through Scan & Pay and UPI ID for teens → Win rewards up to 10000 for referring and paying your friends on the FamPay app for teenagers → Use your rewards to redeem exclusive offers, discounts, gift cards, cashbacks, participate in exciting giveaways, and more! □ Save money and earn through fun challenges → Earn extra pocket money and double your savings on FamPay's in-app gamified savings challenge! □ Shop the best brands from within the app → Exclusive discounts and offers available on the most popular brands, for FamPay users. → Make easy payments with your UPI ID or prepaid card and get rewarded for every payment. □ Get things done with the FamPay Store → Recharge your prepaid mobile with our multiple operators: Airtel, Jio, Vodafone Idea. → Order food and groceries from the best delivery apps: Swiggy, Zomato, Dunzo, Big Basket. → Top-up in-game currencies through Codashop on the FamPay Store. □ The most convenient payments app for parents → Being an online app, with FamPay you can send money to your child whenever you want, from wherever you are - the benefit of digital money transfer. → Pay or request money easily using a personal UPI ID for teens

that allows convenient money transfers. → Set limits and control the expenses of your child by transferring the amount you wish into their FamPay account. → Experience true transparency and manage your child's finances by tracking their expenses. → Help your child become financially independent and experience savings and money through practical experience. → FamPay is the most secure app for teenagers to make payments and follows required guidelines, which is why both you and your child must complete KYC verification before you attain complete access to the app. □ Unmatched security → FamPay is a marketing and distribution partner of IDFC FIRST Bank Prepaid Card. Using the FamPay app does not require linking of a bank account. → We've gathered the best engineers to detect frauds, prevent hacking, and keep your money safe. Every transaction is protected with a device lock, such as fingerprint, face ID, pattern lock, or PIN. → Our numberless card ensures that your important card details are stored safely within the FamPay app. You can also block, pause or change the pin of the card at your fingertips - anytime, anywhere. → FamPay enables secure UPI payments for teens through a UPI ID that can be easily personalized as per your requirements. → Our help center is available 24x7, so you can chat with us whenever you wish to. ☺ Experiencing FOMO? Don't worry! You can join the app and start making payments even if you are not a teenager. Got any questions or feedback for us? We'd love to hear from you! Write to us at <http://lnk.fampay.in/support>

Report Generated by - MobSF v3.6.2 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.

© 2022 Mobile Security Framework - MobSF | [Ajin Abraham](#) | [OpenSecurity](#).